Computers in Industry 100 (2018) 212–223

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Cyber-physical systems and their security issues

Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat*

Institute of Information Technology, Azerbaijan National Academy of Sciences, 9A, B. Vahabzade Street, Baku AZ1141, Azerbaijan

ARTICLE INFO

Keywords:
Cyber-physical system
Cyber-physical system security
Cyber-physical system attacks
Cyber-physical system security threats
Philosophical issues
Tree of attacks

ABSTRACT

The creation of cyber-physical systems posed new challenges for people. Ensuring the information security of cyber-physical systems is one of the most complex problems in a wide range of defenses against cyber-attacks. The aim of this paper is to analyse and classify existing research papers on the security of cyber-physical systems. Philosophical issues of cyber-physical systems are raised. Their influence on the aspects of people's lives is investigated. The principle of cyber-physical system operation is described. The main difficulties and solutions in the estimation of the consequences of cyber-attacks, attacks modeling and detection and the development of security architecture are noted. The main types of attacks and threats against cyber-physical systems are analysed. A tree of attacks on cyber-physical systems is proposed. The future research directions are shown.

1. Introduction

Cyber-Physical System (CPS) is a system that can effectively integrate cyber and physical components using the modern sensor, computing and network technologies [1,2].

A new computing paradigm, known as cyber-physical-social or physical-cyber-social computing [3], has been originated from CPS and cyber-social system (CSS). Cyber-physical-social systems (CPSSs) expand CPSs and include social space and signs of people's participation and interaction [4].

The widespread adoption of CPS is connected with the concept “Industry 4.0” [4], which forms the process of combining technologies and knowledge, providing autonomy, reliability, systematicity, and control without human participation. Key technological trends underlying CPS include Internet of Things (IoT), Big Data, smart technologies, cloud computing, etc.

CPSs are the basis for the development of the following areas: smart manufacturing, smart medicine, smart buildings and infrastructures, smart city, smart vehicles, wearable devices, mobile systems, defense systems, meteorology, etc. (Fig. 1). The rapid growth of CPS applications leads to a number of problems with security and confidentiality.

According to ISO/IEC 27001:2013, information security is the preservation of confidentiality, integrity, and availability of information.

Confidentiality – property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Integrity is the property of accuracy and completeness. Availability – property of being accessible and usable upon demand by an authorized entity.

Other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Due to the widespread use of wireless technologies for data collection and transmission and control commands, where a wireless sensor network (WSN) is used, there is a growing need to develop information security systems in the industry. The remote location of CPS devices and their autonomy lead to the risk of intrusions and attacks.

Working with large groups of devices can cause some of them to be compromised. CPS security raises a number of new challenges [5]:

- the rising number of IoT devices leads to an increasing vulnerability of such systems to cyber-attacks (for example, DDoS);
- security threats modeling;
- development of a formal approach to CPS vulnerabilities assessment;
- designing reliable and fault-tolerant architectures for processing of rapidly developing cyber and physical threats.

Therefore, new methodologies and technologies (such as people-centric sensing, wireless and quantum sensors, wearable biosensors, 2D/3D multi-sensor systems, etc.) should be developed to meet CPS requirements in terms of security, reliability, and confidentiality of personal data. The aim of this paper is to analyse and classify existing studies in CPS security in order to better understand how the security of such systems is actually carried out. The objectives of this study are to provide a picture of the state of the CPS security, helping researchers and practitioners to find limitations and shortcomings in modern research of CPS architecture, intrusion detection, their future potential, and their practical applicability in the context of real projects.

* Corresponding author at: 9A, B. Vahabzade Street, Baku AZ1141, Azerbaijan.
E-mail addresses: rasim@science.az (R. Alguliyev), yadigar@lan.ab.az (Y. Imamverdiyev), lsuhostat@hotmail.com (L. Sukhostat).

https://doi.org/10.1016/j.compind.2018.04.017
Received 6 July 2017; Received in revised form 29 April 2018; Accepted 30 April 2018

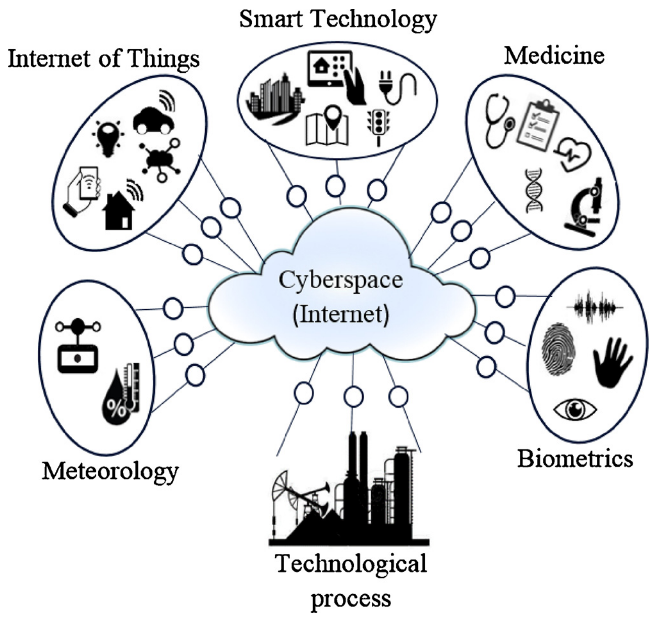

Fig. 1. Cyber-physical systems.

The rest of the paper is organized as follows. Section 2 describes CPS features that differ from other systems. The philosophical issues of the CPS are examined in Section 3. In section 4, the operation of CPS systems is described. Section 5 is devoted to the architecture of CPS. In Section 6 the threats to these systems are presented. A tree of attacks on the CPS is proposed in Section 7. Section 8 considers the research papers in the field of information security, which offers various strategies and measures to maintain the desired level of CPS security. Open issues are outlined for future research in Section 9. Finally, some final conclusions on CPS security are presented.

2. About cyber-physical systems

2.1. What is a cyber-physical system?

This term was proposed by Helen Gill in 2006 at the National Science Foundation (NSF) CPS Workshop conducted by the US NSF. Now CPSs are included in the priority lists of innovations of the US and several European countries.

- The novelty and fundamental difference of CPS from existing embedded systems or automated process control systems (APCS), even though they are similar in appearance, is that CPS integrate the cybernetic beginning, computer hardware and software technologies, qualitatively new actuators, embedded in their environment and able to perceive its changes, respond to them, learn and adapt themselves.
- From the computer science point of view [6] CPS are the integration of computing and physical processes. They include embedded computers, network monitors, and controllers, usually with feedback, where physical processes affect computations and vice versa.
- From the automation technologies point of view [7], CPSs are specialized systems which activities are controlled by computing and communication cores embedded in objects and structures of the physical environment.
- According to the US NSF, the CPS of the future will far exceed the existing systems in performance, adaptability, fault tolerance, security, and ease of use.

2.2. Technical background of cyber-physical systems

1) A large number of devices based on embedded processors and, consequently, increasing memory for data storage.
2) The quality of the CPS control algorithm can affect its complexity and reliability, which increases the intensity of the computing workload.
3) The response time characterises feedback delay. The more feedback delay, the worse the quality control of the object.
4) Combination of different technological trends in large systems: IoT, Smart environment, etc.
5) With the growth of information volumes, it is necessary to transfer part of the CPS control by keeping a human in the loop [8].

2.3. Distinctive features of CPS systems (CPSs) [9,10]

- Embedded and mobile sensing.
- Cross-domain sensor sources and data flows.
- Interaction of cyber- and physical components.
- Ability to train and adapt.
- Interoperability through the Internet (such as IoT).
- Ensuring the reliable operation of the systems (such as ATM and POS) with centralized automatic control.
- The presence of a common cyberspace, which provides exchange both within systems and with the environment, as well as information security, in the form of cryptosystems, firewalls, antiviruses, etc.
- The operation must be dependable and certified in some cases.
- System robustness is ensured by automated intellectual control.
- Human in/outside the loop.

3. Philosophical issues of CPSs

The world of modern people is rapidly changing, and their entity has also changed. “Things” begin to lose their “materiality” and increasingly become “virtual” [11]. The economy is also becoming increasingly virtual: online banking and online crediting are developing, purchases are made in online stores where a person can only see a photo or an image – a sign of the product that he will receive in the end.

Information overflow is increased by new information generated by the nodes and the collaborative network of nodes. This information is generated as a result of the ability of the nodes and the collaborative network to learn and adapt and autonomously interact with their environment, which includes humans. And since it’s interaction, humans might be tempted to, or even need to, react, leading to even more information and more challenges, also in security.

On the one hand, the abundance of new information allows a person to transform it into knowledge, however, on the other hand, this entails an increase in information noise. If earlier such noise was most often found only in the virtual world, for example, in spam letters, pop-up windows, contextual advertising, etc., now with the advent of CPS, when each object contains and transmits a large amount of information, such noise starts to exceed the limits of the framework of virtual reality and acquires its features in the real world. A large amount of information also leads to the fact that the information itself begins to depreciate, and the search for necessary information becomes a difficult task.

Thus, the development of CPSs and their impact on the contours of the life of modern people are extremely controversial. On the one hand, CPS, like any innovation, was originally conceived as a means of improving human life, an innovation that could make life more comfortable, relieve a person and allow him to get rid of routine work [12]. On the other hand, the development of CPS, like any socio-technical innovation, posed new challenges for the person, the main of which is the transformation of life and the partial loss of its completeness, connected with mass distribution, virtualization of practices, and increased information noise. The consequence of these processes is the inability to identify the main priorities and benchmarks in the virtual information space [13].

Barriers of CPS include a variety of protocols and standards, security issues, power supply devices, a psychological barrier. Also, there are smart contracts that are computer programs that make it easier to automate compliance with various types of contracts/transactions. In the conditions of CPS and Big data, a special legal structure should be provided to simplify the cırculation of information as a subject of transactions.

One of the issues with security, in general, is that there always are multiple stakeholders involved. They all have different goals and perceive different security risks and threats. Regulations and standards can be used as part of security countermeasures, but an important focus should be to provide and ensure sufficient levels of security for each of the specific stakeholders and also for specific information in specific contexts and environments. The words “sufficient” and “specific” are key in security. The emergence of decentralized cryptocurrencies has opened new opportunities and also allowed to solve some of the fundamental problems related to the efficiency, security, and autonomy of payment systems.

The humanitarian expertise of CPS realities and technologies and its bioethical support is a non-trivial task and requires complex interdisciplinary teams of developers, researchers, philosophers. Rethinking these issues is one of the most important tasks of the information technology philosophy and philosophy in general.

4. Principle of CPS operation

The CPS architecture often consists of two main layers [14,15]: the cyber layer and the physical layer. The current state of the CPS includes variables that represent data obtained by sensors and control variables representing control signals [16]. The normal value of a certain process parameter is called a set point. In CPS, the distance between the values of the process variables and the corresponding control points is calculated by the controllers. After calculating this offset, the controllers, using a complex set of equations, develop a local actuation, and compute new actuation and control variables. The received control value is sent to the corresponding actuator to keep the process closer to a specific set point [17].

Controllers also send the received measurements to the main control servers and execute the selected commands from them. In CPS, system operators should be aware of the current status of the controlled objects. Thus, the graphical user interface (GUI), called the human-machine interface (HMI), provides the current state of the controlled object to the human operator.

In general, the CPS process can be divided into the following stages [14]: 1) monitoring; 2) networking; 3) computational processing; 4) actuation. The cyber layer often uses industrial protocols such as DNP3 [18], 61 850 [19] and Modbus [20] to communicate with physical layer devices.

5. CPS architecture

A CPS may consist of multiple static/mobile sensor and actuator networks integrated under an intelligent decision system [21]. CPSs are characterized by cross-domain sensor cooperation, heterogeneous information flow, and intelligent decision making.

Different types of CPS components integration are based on effective connectivity. CPS includes various combinations of key functions and depends on their applications. CPS considers computational components that use common knowledge and information from physical processes. Depending on the field of application, the issue arises which of the characteristics should be used and to what extent.

The CPS architecture can be considered at various levels. The most common architecture of CPS is divided into seven fundamental levels of ISO/OSI model [22,23]: from the physical layer to the application layer.

5.1. Physical layer

The physical layer lays the groundwork for the CPS architecture. The physical layer consists of sensors, actuators, which are connected to each other via wireless or wired networks. For example, 2G/3G/4G, Wi-Fi, ZigBee, Bluetooth, WiMAX, RFID readers and tags and wired technologies (PLC, NC, etc.). 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) is a network layer protocol and can be used with any physical and data link layer. This layer is used to connect ZigBee, Bluetooth and other systems to the Internet (acts as a router). The devices at this level usually have little memory and processing power. Attacks on this layer mainly come from external sources.

5.2. Data link layer

The data link layer provides the creation, transmission, and reception of data frames. This layer serves the network layer requests and uses the physical layer service to receive and send packets. The data link layer is divided into logical channel management (LLC) sublayer and media access control (MAC) sublayer. LLC provides network layer service, and the MAC sublayer regulates access to a shared physical environment. An attack on this layer can lead to disruption of MAC addresses, which could result in a failure of the device identification.

5.3. Network layer

At this layer, packets are routed based on converting MAC addresses to network addresses. It uses the IPv4/IPv6 and RPL (“Ripple” routing) protocols. The attacks that lead to the failure of sensors and actuators, in turn, lead to a change of information and source from which it was obtained. This can subsequently lead to a mechanical failure.

5.4. Transport layer

At this layer, packets are broken into small fragments. The most common transport layer protocols include TCP, UDP, and ICMP. Attacks on this level lead to a decrease in the speed of network equipment and the failure of services.

5.5. Session layer

The session layer manages the conversation (communication session). It monitors the order of message transmission over the network; in case of a fault, not to start from the beginning again, inserts labels into long messages. Session-level protocols are usually an integral part of the functions of the top three layers of the model.

5.6. Presentation layer

Presentation level coordinates the data presentation (syntax) in the interaction of two application processes: data transformation from the external format to internal one; data encryption and decryption. An example of such a protocol is the Secure Socket Layer (SSL) protocol, which provides secret message exchange for the application-layer protocols of the TCP/IP stack.

5.7. Application layer

The application layer covers different domains (Fig. 1). This layer stores, analyses and updates information received from previous layers. It makes control decisions that can be visualized using the virtual prototype interface. The protection of data privacy is the most important issue of this level.

Data confidentiality is provided by various security mechanisms (for

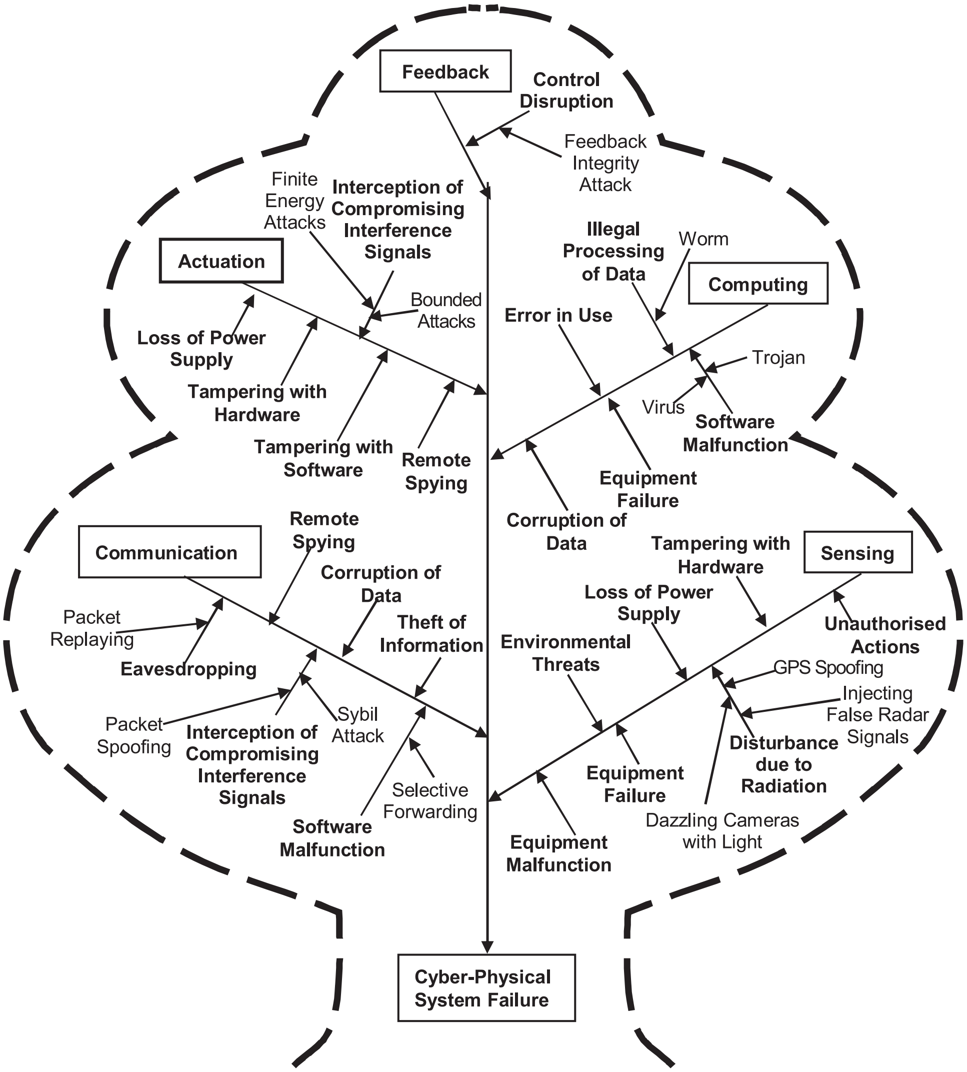

Fig. 2. A tree diagram of attacks and threats on cyber-physical systems.

example, data encryption, two-factor authentication, etc.). This protects CPS sensor data from their disclosure and transferring to an unauthorized party.

Real-time digital data processing and its capture are carried out by sensors. The CPS sensors can measure physical properties and convert them into a signal. There are different types of sensors that perform different functions and are used in different areas. In some cases, they can also have a certain degree of memory, which allows them to register a certain number of measurements.

Sensors with a low data transfer rate form WSNs, which are increasing in popularity, as they can have more sensor nodes than wired sensor networks and work offline for a long time. For example, machine-to-machine (M2 M) communications, which are subject to additional security measures, based on their characteristics associated with different protocols and their applications.

There are several security design principles that can be useful in constructing control systems that can survive attacks [24–26]: redundancy, diversity, a principle of least-privilege, and separation of privilege.

Architecture helps to define and explain the overall structure of CPS, to describe the interaction of its components. Security should be performed on all layers of the CPS architecture, from the physical layer to the application layer.

A higher level of security reduces the risk of confidential information disclosure, provides data anonymity, and hides important information details. CPSs security protects the system from intrusions and reduces the likelihood of risks.

6. Security threats of CPSs

Cyber threats affect: 1) the confidentiality that is necessary to maintain the security of user's personal data in the CPS and prevent an attacker from attempting to change the state of the physical system by "eavesdropping" communication channels between the sensors and the controller, and between the controller and the actuator; 2) the integrity, when data or resources can be changed without permission; 3) the availability, when there are failures in computer technology, management, communication, equipment; 4) the reliability, when it is necessary to confirm that both parties involved are really the ones they pretend to be [27,28]; 5) the authenticity, when the identity of a subject or resource can be proved to be the one claim; 6) the non-repudiation, when actions or events can be proven to have taken place so that they cannot be repudiated later; 7) the accountability, when the actions of an entity can be traced uniquely to the entity.

One of the main characteristics of cyber threats is that they are scalable, i.e. they are easily automated and replicated, and you should expect that they are distributed freely through unreliable domains. Cyber-physical threats are threats that originate in cyberspace but have an impact on the physical space of the system. Cyber-physical threats emerge from cyberspace and affect the physical space of the CPS.

Classification of CPS threats includes [29]: Spoofing identity, Tampering with data, Repudiation of origin, Information disclosure, Elevation of privilege, Denial of service (DoS).

In [30], key problems were identified for CPS security: 1) understanding the threats and possible consequences of attacks; 2) determining the unique properties of CPS and their difference from traditional information technology security, and 3) discussion of the security mechanisms applicable to CPS.

On the other hand, in order to understand the new classes of CPS threats, for example, on the smart network and SCADA (Supervisory for Control and Data Acquisition) systems, it is useful to characterize the interactions between the area that is the source of the threat and the area that has been affected [31].

7. Tree of attacks on CPSs

According to the ISO/IEC 27001:2013 standard, threats may be deliberate, accidental or environmental. The examples of typical threats include: physical damage, natural events, loss of essential services, radiation malfunctions, compromise of information (for example, eavesdropping, tampering with software, etc.), technical failures, unauthorized actions (for example, data corruption), compromise of functions (for example, forging and abuse of rights).

Based on the results of the analysis of existing studies in security in Fig. 2, a "tree" of attacks and threats based on the functional model of CPS [14] is proposed. Branches of the "tree" include the following types of attack: a) attacks on sensor devices (*Sensing*); b) attacks on actuators (*Actuation*); c) attacks on computing components (*Computing*); d) attacks on communications (*Communication*); e) attacks on feedback (*Feedback*).

a) The researchers identified threats and vulnerabilities that affect CPS sensors (such as Injecting false radar signals, Dazzling cameras with light, GPS Spoofing, etc.) [32]. Since CPS is closely related to the physical process in which they are embedded, the reliability and accuracy of the data acquisition process must be ensured. Sensor security needs methods to encourage physical authentication so that any data received from a physical process can be trusted [33].

b) Djouadi et al. [34] analysed the impact of cyber-attacks on actuators and considered two classes that cover a wide range of potential attacks: the *Finite Energy Attack*, which includes, for example, the loss and modification of personal packets, the Finite Time Attack, and Impulse attacks, and the *Bounded Attack*, which leads to the suppression of the control signal.

The actuation control security refers to the fact that during a passive-active or active mode of operation, no action can take place without the appropriate permission. The specification of permissions must be dynamic, as the CPS requirements change over time.

c) Attacks on computing resources have been discussed in detail in the paper and include Trojans, Viruses, Worms and DoS attacks [35]. In [36], information is provided on methods of data mining (DM) that can be used to increase cybersecurity.

A malicious attack can secretly damage the CPS. Since there are violations and measurement errors in control systems, the detection mechanisms must ensure that these regular errors will not cause a false alarm. This gives the attacker a space to hide.

If an attacker changes real data by obtaining a key for secure communication (*communication key*) or capturing some network devices, this is called an *integrity attack*. Storage security includes the development of solutions to ensure the security of stored data in CPS platforms from physical or cyber hacking. From the attacker's point of view, the construction of a strategy of false attacks, as a rule, deals with a number of factors, resources and security constraints.

d) Communication attacks include *Selective Forwarding, Packet Spoofing, Packet Replaying, Sybil,* etc. attacks (can be used to disrupt resource allocation between nodes in favor of malware) that violate the routing of system packages [33]. Any intervention in the data may lead to errors in future requirements for their processing. If an attacker can only capture and forward real data packets, then an effective attack method is to record some "normal" data and play it back to avoid detection.

Communication security requires the development of protocols to provide links between interference sources (active) and eavesdroppers (passive) between and within CPS.

e) In [14], a three-layered logical model of CPS and a *meta*-model of cyber-attacks, where the system is attacked by *Feedback Integrity Attack* (while only part of the control signals retains its integrity), were proposed. Feedback Security refers to the fact that the control systems in CPS, which provide the necessary feedback for actuation, are protected. Modern security solutions are focused only on data security, but their impact on evaluation and management algorithms should be studied to provide in-depth protection for CPS [37].

8. Main research areas

Analysis of state-of-the-art publications on this topic has shown the relevance and prospects of CPSs [27,38]. Scientists from different countries (Germany, China, the USA, etc.) have devoted thousands of publications to this technology that investigate the creation of such systems [39].

In [40] the systematic map of research on the CPS security was presented. This paper showed the leading universities in some developed countries that are engaged in research on this issue.

To analyse the latest research in the field of CPS security, we have identified four research categories. As can be seen from Tables 1–4, the proposed classification scheme is based on the estimation of cyber-attack consequences, modeling of CPS attacks, CPS attacks detection and development of security architecture.

A number of state-of-the-art publications have been studied. They were summarized in the tables according to the criteria.

The tables list the main contributions and concepts of the approaches considered in each document. Moreover, the future research directions of each paper were indicated.

And according to our analysis, the first five research universities dealing with this problem include University of California at Berkeley (USA), University of Science and Technology Beijing (China), KTH Royal Institute of Technology (Sweden), Politecnico di Milano (Italy) and Hamburg University of Technology (Germany).

The development of attack detection for industrial CPSs is reviewed according to the categories of detection approaches [41]: 1) Bayesian detection with binary hypothesis; 2) weighted least square (WLS) approaches; 3) χ^2-detector based on Kalman filters; and 4) quasi-FDI (fault detection and isolation) techniques. Robustness, security, and resilience, as well as stability, have been discussed to govern the capability of weakening various attacks.

According to [42] any CPS security model should include security defense layers with the following characteristics: difficult penetration; robust authentication and access control mechanism; high response time; upgrade capability and attack mitigation abilities. This paper presents an analysis of the security issues at the various layers of CPS architecture, risk assessment, and techniques for securing CPS.

Consequently, the various research communities are very active in the direction of CPS security, which confirms the importance of this problem. However, there are still many unresolved issues. As a result, the following CPS security studies are highlighted in this paper:

1) Estimation of cyber-attack consequences. Complex and sophisticated attacks are designed to cause significant damage to the cyber and physical characteristics of CPS. For example, Stuxnet [43,44], which is the first malicious software specifically designed to inflict physical damage on industrial infrastructures (reprogramming control systems by modifying the PLC code). Thus, it is necessary to assess the impact of cyber-attacks on the normal functioning of

Table 1
A literature overview on the estimation of cyber-attacks consequences.

References	Proposed approach	Main contribution	Future directions
Ashok et al. (2014) [65]	Identification of some of the pertinent issues in the cyber-physical security of WAMPAC.	● Modeling of dynamic cyber-attack scenarios depending on the attacker/defender model. ● Application of the game theory to model cyber-attack threats, which cannot be modeled using traditional risk assessment approaches.	Extension of this framework to more complicated scenarios.
Genge et al. (2014) [66]	Evaluation of the impact of network and installation-specific parameters on cyber-attacks targeting CPSs.	Two key parameters (control code task scheduling and the speed of control valves) that could be adopted at design-time to increase the resilience of physical processes confronted with cyber-attacks were identified.	This solution should be taken into account at process design time, which will lead to a more resilient physical process.
Genge et al. (2015) [50]	A novel methodology for assessing the impacts of cyber-attacks on critical infrastructures.	Works better than graph-theoretic methodologies and electrical centrality measures.	Evaluation of CAIA applicability to production systems and integration of CAIA results in control network design methodologies.
Huang et al. (2009) [54]	● Analysis of how attacks on control systems can affect the physical environment in order to: understand the consequences of attacks, estimate the possible losses, estimate the response time required by defenders, and identify the most cost-effective defenses. ● Threat models for control systems.	● The influence of various cyber-attacks (DoS and integrity attacks) on CPS was investigated. ● It was found that the attacks on control signals are more serious than attacks on sensor signals.	Evaluation of the impact of attack combination on CPS.
Orojloo and Abdollahi Azgomi (2017) [45]	A method for evaluating the consequences of security attacks on physical processes.	● The proposed method provides the possibility of comparing the behavior of CPSs at the different time instants, and under different disturbances on different control parameters. ● The approach can be applied to a combination of attacks.	Analysis of the proposed method to various CPSs.
Sicari et al. (2016) [74]	Assignment a level of robustness to each data source according to integrity, confidentiality, privacy.	An algorithm has been developed in order to assess the trustworthiness of registered and non-registered IoT data sources.	The introduction of a key management system in the platform.
Wasicek et al. (2014) [82]	Application of aspect-oriented modeling (AOM) to CPSs security assessment.	Enables assessing system models and associated attacks within the same model environment.	Development of the executable attack models for CPS and more general attack patterns.
Wu et al. (2015) [73]	Risk assessment method and algorithm.	● The proposed risk change curve helps to better understand the systemic risk in real time and get a response to the risk timely. ● The risk curve can be used to predict risk in the future time.	The automatic identification and quantitative analysis methods to deal with a large number of real-time update information of assets, threats, and vulnerabilities of CPS for the risk assessment.
Yampolskiy et al. (2014) [61]	Cyber-Physical Attack Description Language (CP-ADL) to capture cyber-physical attacks.	Qualitative and quantitative analyses of attacks on CPSs.	Development and population of a knowledge base containing known attacks on CPSs.

physical processes. In such situations, it is extremely important not only to demonstrate and evaluate the destructive impact of cyber-attacks, but also to quantify the consequences and, ultimately, to ensure the availability of specific cyber activities. In order to provide a systematic review of the papers and perform an analysis of cyber-attacks consequences, each work was represented in Table 1.

2) Modeling of CPS attacks. Attack and vulnerability models are used to identify weaknesses in CPS systems to support their search

Table 2
A literature overview of CPS attacks modeling.

References	Proposed approach	Main contribution	Future directions
Khalil (2016) [48]	A probabilistically timed dynamic model for simulating physical security attacks on CPSs.	Applying visual flowcharting as a programming language.	● Adjusting the attacker's mission success probability depending on the time when the attack is launched. ● Incorporating a defender's countermeasures. ● Validating probability predictions of the proposed model.
Martins et al. (2015) [83]	Systematically identify the potential threats at the design phase of building CPSs.	A tool to perform systematic threat modeling for CPS using a real-world railway temperature monitoring system as the case study was presented.	Merging of the different threat modeling techniques in order to enable the expansion of threat identification and system vulnerabilities.
Mavani and Asawa (2017) [71]	Description of IPv6 spoofing attack, which corrupts the border router's routing table of the 6LoWPAN network.	● It is shown that path loss exponent affects the probability of attack success. ● The systematic mathematical analysis using an attack tree model was performed.	Assessment of the impact of multiple attackers on the network communication in CPS and to propose a countermeasure.
Mitchell and Chen (2015) [58]	An analytical model based on SPN techniques for modeling and analysis of attacks and countermeasures for CPSs.	The analytical model allows the optimal design parameter settings for maximizing the mean time to failure (MTTF) of the CPS.	Investigation of countermeasures for improving CPS survivability.
Srivastava et al. (2013) [64]	● The attack modeling using the vulnerability of information, communication, and electric grid network ● Cyber vulnerability index based on discovery, feasibility, access, detection threat and connection speed	Integration of cyber and physical vulnerability models given incomplete information	Development of mitigation techniques to avoid coordinated cyber-physical attacks on the smart grid.

Table 3
A literature overview of CPS attacks detection.

References	Proposed approach	Main contribution	Future directions
Finogeev and Finogeev (2017) [46]	Classification of external attacks and intrusion detection in sensor networks.	The existing routing procedures for the simultaneous exchange of key information allow reducing energy consumption during the information transmission.	Carry out a covert transfer of open or encrypted key information by the steganographic methods.
Friedberg et al. (2015) [51]	A novel anomaly detection approach that utilizes log-lines produced by various systems and components in ICT networks.	● APT detection approach. ● Anomaly detection model. ● Real-World evaluation.	Development of a more intelligent approach for the generation of event classes.
Giani et al. (2013) [49]	An efficient algorithm to find all unobservable attacks in Energy Management Systems.	● Detection of irreducible attacks that involve the compromise of exactly two power injection meters. ● Countermeasures against arbitrary unobservable attacks using known-secure PMUs.	A comprehensive and realistic analysis of cybersecurity threats to electricity grids under normal and contingency operations.
Li et al. (2016) [47]	An approach for modeling the false sequential logic attack (which can disrupt the physical process or cause physical damage by cyber assaults).	● Can be used to establish the rule base for detecting the false sequential logic attacks. ● The proposed approach can be considered as an enhancement of the existing IDS in the detection of the false sequential logic attack.	Other physical processes controlled by SCADA systems investigation.
Li et al. (2016) [63]	A novel distributed host-based collaborative detection (DHCD) method to identify and mitigate false data injection attacks in smart grid CPS.	● Distributed detection significantly mitigates control center's computation burden. ● The effectiveness of the proposal is demonstrated by real-time measurement data.	Extending the proposed approach to capture power system faults (e.g., voltage disturbance, open circuit, and short circuit).
Liu et al. (2015) [62]	A novel cyber-physical fusion approach for attack detection in Smart Grid using ATSE.	Demonstrates a low-cost and easy-implement solution to integrate heterogeneous data in Smart Grids.	● The correlation and interaction between the cyber network and power system investigation. ● IDS tools and abnormal detection methods in computer network integration in ATSE.
Mo et al. (2013) [59]	The model-based techniques capable of detecting integrity attacks on the sensors of a control system.	Countermeasures that optimize the probability of detection by conceding control performance.	Extending the proposed techniques to more sophisticated attack models and to distributed control systems.
Ntalampiras (2016) [52]	A novel methodology for automatic identification of the type of the integrity attack affecting a CPS.	● A framework encompassing a novel feature set and customized pattern recognition algorithms for identifying integrity attacks affecting CPSs. ● The fusion of characteristics belonging to two diverse signal representations (frequency and wavelet) for identifying integrity attacks.	Development of online clustering algorithm for data detected as a novel.
Sakiz and Sen (2017) [57]	A holistic view of previous research works on intrusion/misbehavior detection in VANETs.	A survey of different detection mechanisms (along with the advantages and disadvantages).	Attack/misbehavior detection in VANETs.
Vincent et al. (2015) [67]	A novel product/process design approach to enable real-time attack detections to supplement the shortcomings of quality control systems.	A quick detection of compromised manufactured parts without significantly disrupting the manufacturing process flow.	Development of new manufacturing specific approaches for detecting cyber-attacks that incorporate the physical nature of the manufacturing systems.
Yang et al. (2013) [56]	● Investigation of false data injection attacks against Kalman filtering in the dynamic state estimation of power systems. ● Countermeasures to defend against these attacks.	The enhanced unscented Kalman filter (UKF) technique achieved the best performance than other Kalman filtering techniques and reduced the impact of attacks to some extent.	Studying the impact of false data injection attacks against the state estimation of power grid systems.

Table 4
A literature overview of security architecture development.

References	Proposed approach	Main contribution	Future directions
Chen et al. (2014) [68]	A general theoretic framework for network robustness analysis and enhancement in large-scale networks (IoT, CPS, and M2 M communications).	● A fusion-based defense mechanism to mitigate the damage caused by intentional attacks. ● Novel avenues to the theoretical analysis and network robustness enhancement for IoT.	This work can be extended to a multistage hierarchical network structure composed of several autonomous fusion centers.
Hu et al. (2016) [55]	A comprehensive survey of the principle of building a resilient CPS.	● A comprehensive survey of the entire design process. ● Qualitative and quantitative descriptions of CPS resilience. ● Detailed investigation of sensor-actuator interactions, as well as CPS security issues.	Critical research issues unsolved in terms of building a resilient CPS have been discussed.
Moosavi et al. (2015) [69]	Development of a secure and efficient authentication and authorization architecture for IoT-based healthcare.	● Architecture for IoT-based healthcare using distributed smart e-health gateways (SEA). ● Any malicious activity can be blocked before entering into a medical constrained domain.	The presented architecture is a promising solution to provide a scalable and reliable end-to-end security for IoT-based healthcare systems.
Venkitasubramaniam et al. (2015) [70]	An analytical framework grounded in information-theoretic security.	A methodological framework to address the challenges, and delineates recent advances utilizing the framework.	This research can be viewed as a launching pad for deeper exploration of cyber-secure control and more generally, cyber-physical security.
Yoo and Shon (2016) [60]	Security requirements and architectures in the heterogeneous CPS environment.	Classification of the security issues that can occur in an environment, where heterogeneous protocols are connected based on IEC 61850, into six security layers, and suggested security countermeasures.	Further study of concrete security techniques is needed, including a method to verify whether a protocol conversion was accomplished in a normal fashion.

strategy and understanding of the attacks. It is necessary to develop attack models to assess them and take adequate countermeasures to ensure CPS security (Table 2). The attacker needs to understand the failure conditions of the equipment, control principles, process behavior, etc. [45].

3) CPS attacks detection. It is important to develop detection algorithms and countermeasures for all well-known attacks in advance to reduce the impact of attacks for a limited time and minimize system damage. Table 3 summarizes the papers on CPS attacks detection, the main contributions, and future research directions.
4) Development of security architecture. The development of CPSs is constrained by security factors. The main task of designing complex CPS architectures is to test and validate "secure design" to ensure the security and reliability of physical and cyber components. It is necessary to develop new reliable control and evaluation algorithms that consider more realistic attack models from a security perspective. Table 4 shows a summary of the literature on the development of security architecture.

By classifying the publications under consideration, we have grouped them into four categories related to SCADA systems security and Smart Grid security, countermeasures against cyber-attacks and communication security.

8.1. SCADA systems security

The problems of detecting attacks in WSN of SCADA systems were introduced in [46]. Authors developed the detailed classification of external attacks and intrusion detection in sensor networks and brought a detailed description of attacking impacts on components of SCADA systems in accordance with the selected directions of attacks. Information security problems are often caused not so much by external attacks, but the staff non-compliance with regulations and rules of the enterprise information security policy. It may result in an unauthorized infection by computer viruses, Trojans, and worms. Finding the infection in the SCADA system may cause a need of hard reset to clean the virus and will stop the most of the enterprise's processes, but it is not always feasible from the economic standpoint.

Li et al. proposed a new type of cyber-physical attacks on SCADA systems [47]. Even though this paper was focused on the neutralization process, many other physical processes controlled by SCADA systems could also be the targets.

A model that simulates attempts by a highly skilled attacker to execute a premeditated malevolent scheme and calculates the probability of attacker's mission success was proposed in [48]. Attacker's mission success probability is dependent on the quality of intelligence gathered prior to launching his attack. The proposed model can be used for simulating what-if scenarios for security drills to better understand vulnerabilities in critical infrastructures.

In [49], the authors presented and characterized the unreasonable cyber-attacks using intentionally secure phasor measurement units (PMUs). It has been shown that $(p + 1)$ PMUs are quite effective for disabling p attacks. A deeper problem with the investigation of the cybersecurity of SCADA/EMS components of the power grid is related to grid operations. Therefore, a complete and realistic analysis of the cybersecurity threats of electrical networks should include both the normal technological regime and emergency situations.

In [50], a new methodology for assessing the effects of cyber-attacks on physical processes was proposed. The study is based on the behavioral evaluation of physical processes and sensitivity analysis. For this, the covariance of the observed variables before and after performing individual attacks against control variables was calculated. One of the main features of this methodology is its applicability to situations where the physical process is unavailable. It only considers individual attacks on control signals.

In [51] an approach for anomaly detection that is the result of the impact of Advanced Persistent Threats (APTs) (for example, direct access to database servers, copying large amounts of data) was proposed. Anomaly detection in this approach is possible only through the use of a combination of different rules describing the model. It was concluded that the proposed approach performs very well in the limited SCADA dataset. Despite this, according to the authors, the proposed approach can work well on real data.

The paper [52] presented a framework encompassing a novel feature set and customized pattern recognition algorithms for identifying integrity attacks affecting CPSs. It is important to make informed decisions regarding accommodation actions and future usage of the infrastructure. Frequency and wavelet values were used to train a Random Forest for identifying integrity attacks. The proposed method is able to detect previously unseen data reducing potential misclassifications.

In [45], a method for estimating the consequences of the attacks spread in CPSs, assessing the direct and indirect consequences of attacks on control parameters, including measurements of CPS sensors and controller signals was proposed. The proposed approach was considered for a Boiling Water Power Plant (BWPP). The "normal" behavior of the system is compared without any malfunctions with the abnormal behavior during the attacks (DoS and deviation attacks). The system parameters are divided into two classes of cause-and-effect parameters, which may be the same or may differ from each other. New indicators that can be used to quantify the level of importance of each parameter in a physical process were proposed. The priorities in the sensors and control signals readings were determined to depend on their attacks sensitivity using the obtained quantitative values. Unlike most of the proposed methods that are applicable to attacks that cause a physical process to shut down (for example, [53,54]); the proposed method can consider attacks that do not necessarily lead to SCADA system outage.

In [55], the authors discussed the concept and strategies for creating a reliable and fault-tolerant CPS. They defined fault tolerance as a 3S-oriented model (Stability, Security, and Systematicness). They also pointed out the problems associated with CPS modeling.

8.2. Countermeasures against cyber-attacks

Countermeasures to improve the stability of Kalman filtering to defend against false data injection attacks were developed in [56]. The proposed countermeasures have been implemented on IEEE 14-bus, 30-bus, and 118-bus systems. Unscented Kalman filter (UKF) approach achieves the best performance on random benign noise and reduces the impact of attacks. According to authors, the proposed temporal-based detection technique can identify compromised meters accurately and quickly.

Due to the increasing use of IoT and Internet of Autonomous Vehicles in the near future VANETs (Vehicular ad hoc networks) develop continuously and attract increased attention. An attacker could compromise some vehicles and turn them into zombie vehicles, awaiting orders from a command and control server. In [57] the approaches for intrusion/misbehavior detection were provided. Proactive and reactive solutions that could be employed as countermeasures to attacks were also discussed.

Attack has consequences only when the network operator is misled, which leads to data compromise. The countermeasures against arbitrary unobservable attacks using known-secure PMUs were proposed [49].

In [58], an approach was proposed to model and evaluate attacks and defensive actions for CPS. The model is based on stochastic Petri nets (SPNs). In this approach, attrition, pervasion and exfiltration failures were considered. Determining the optimal model of conditions in CPS, such as the intrusion detection interval and the modeling of the redundancy level, are the results of this study.

In [59], the model of the replay attack on CPS was determined, and the effectiveness of the control system was analysed. The relationship between loss of performance, detection rate and the strength of the authentication signal has been described. A technique for optimizing noisy authentication signals based on a trade-off between the desired detection efficiency and permissible loss of control performance was also presented. In the paper, it was suggested to introduce an authentication signal into the system at random intervals of time, rather than continuously, thus, only affecting performance for some time.

Yoo and Shon [60] discussed vulnerabilities, security requirements, CPS architecture and presented countermeasures. The suggested security architecture for IEC 61850-to-DNP3 conversion environment model, suggested by IEC 61850 80-2/IEEE 1815.1, was applied and its potential was verified.

The language for describing possible attacks on CPS and their consequences was proposed in [61]. The main advantage of this language is the definition and description of features describing attacks and countermeasures. Although they are not considered in the security assessment process, the authors believe that the proposed attack description language can be used to assess the level of security.

8.3. Smart grid security

In [62] a novel cyber-physic fusion approach by developing an abnormal traffic-indexed state estimation (ATSE) method for attack detection in Smart Grid was described. ATSE was applied to detect the attacks, including IDS (Snort) and bad data detection algorithm (Chi-square Test). The basic idea of ATSE is that the discrete event is quantified as the index of a physical system model. It demonstrates a low-cost and easy-implement solution to integrate heterogeneous data in Smart Grids. ATSE could be extended to detect other attacks in various CPS.

A novel distributed host-based collaborative detection (DHCD) method to identify and mitigate FDI attacks in smart grid CPS was proposed in [63]. A rule specification based real-time collaborative detection system was designed to identify the anomalies of measurement data. In addition, a new reputation system with an adaptive reputation updating (ARU) algorithm was presented to evaluate the overall running status of the PMUs, which can be used to identify compromised PMUs.

The authors in [64] turned to the attack modeling, using the vulnerability of information, communication, and the electrical network, analysed the vulnerabilities of the electrical network with incomplete information using an approach from graph theory. In addition, a comprehensive cyber vulnerability index was introduced and used to model in real time while demonstrating the impact of the Aurora attack.

The game theory approach to the security assessment of smart networks was proposed in [65]. First of all, the authors focused on the cyber-physical security (monitoring, protection, and control in terms of coordinated cyber-attacks) of the vast territory. The main focus of this paper is to study pertinent issues in the cyber-physical security of WAMPAC (Wide-Area Monitoring, Protection and Control).

8.4. Communication security

Genge et al. [66] have described the problem of how network parameters, such as packet loss, communication delay, timing management logic, and network traffic can affect the consequences of attacks. The main contribution of the authors is that the most important parameters that could affect the stability of physical processes were identified. The authors noted that communication parameters (for example, communication delay) have a limited impact on the result of the attacks and the scheduling parameters of the tasks can affect the stability of physical processes.

Attacks can alter a manufacturing system, resulting in impaired communication, functionality or reduced performance [67]. An approach proposed in this paper combines the key principles of modern methods for Trojans detection that affect the physical changes of manufactured parts in the industry. It incorporates the use of structural health monitoring techniques to detect changes in a part's intrinsic behavior and brings manufacturing cybersecurity considerations to the product/process design stages.

The vulnerability of IoT infrastructure under intentional attacks has been investigated in [68]. The network robustness of the Internet-oriented network and the CPS-oriented network were analysed. Both analytical and empirical results showed that the proposed mechanism enhances the robustness of IoT, even in the weak local detection capability and fragile network structure regime.

In [69], an architecture for IoT-based healthcare (where the most devices and their communications are wireless) using distributed smart e-health gateways was proposed. It is more secure than the centralized delegation based architecture because it is more resistant to DoS attacks and uses a more secure key management technique.

Two broad challenges in CPSs information security (preventing retrieval of internal physical system information through monitored external cyber communication links, and limiting the modification of physical system functioning through compromised cyber communication links) were analysed in [70]. Information-theoretic approaches against passive and active security attacks were developed.

Authors in [71] have attempted to describe IPv6 spoofing attack that impacts on network communication, which corrupts the border router's routing table of the 6LoWPAN network. This study uses Attack Tree (where the nodes of the tree represent attacks, and the root of the tree is the global goal of an attacker) [72] as an attack modeling tool to dissect it into micro-attacks and analyse each of them.

The estimation of communication, computing and control attacks consequences on CPS can be successfully implemented in accordance with the risk assessment model and the algorithm proposed in [73], which calculates the overall risk of CPS based on attack severity and attack success probability. The weight was given to each system node (that was under attack). A risk curve can help users better understand and respond to systemic risk in time. In addition, it can also be used to predict future risks.

The work [74] is aimed at minimizing the associated risks by letting users and applications be aware of the security and data quality level. The solution is integrated into IoT middleware and is called as NetwOrked Smart objects (NOS). It is used to dynamically specify the level of security and data quality. This solution is better than conventional one-size-fits-all approaches that often do not consider consumers' requirements in terms of security, privacy and data quality.

Table 5
Summary of the importance of CPS security issues.

Domain	Authenticity	Confidentiality	Reliability	Resilience	Integrity
SCADA systems security	[45], [49], [46], [55]	[51], [55]	[45], [50], [48], [51], [52], [55]	[45], [50], [48], [49], [55]	[45], [50], [49], [51], [52], [47], [46], [55]
Countermeasures against cyber-attacks	[61], [58], [59], [49], [57], [60]	[58], [59], [57]	[58], [59], [56], [57], [60]	[61], [49], [56]	[59], [49], [57], [60]
Smart Grid security	[65], [64], [62]	[64], [62]	[65], [64], [63], [62]	[62]	[65], [64], [62]
Communication security	[73], [74], [71], [69], [70]	[73], [74], [71], [69], [70]	[73], [74], [69], [68], [70]	[73], [66], [74], [71], [67], [69], [68]	[73], [66], [74], [71], [67], [69]

Table 5 discusses the above categories in terms of security issues, including authenticity, confidentiality, reliability, resilience, and integrity. The table provides an overview of the trends in CPSs security research. It shows that information security goals have been touched in almost all of the considered papers.

9. Open issues

CPSs have a high potential for creating new markets and solutions to social risks, but impose high demands on quality, safety, security and privacy [75–78]. Fundamental scientific research is necessary to achieve a predictable level of verification and measurement quality, to effectively combat external and internal changes.

Based on the above analysis of the latest CPS security studies, the future research directions include the following tasks:

1) The development of methods for CPS components authentication. The presence of component authentication mechanisms, as well as a secure channel between sensors and controllers, makes it possible to increase the security of CPS from any tampering [79].
2) The development of metrics to determine the level of trust in CPS components. According to Table 5 from the previous section, ensuring the authenticity, confidentiality, reliability, resilience, and integrity of CPS against various attacks must be performed at a certain level of trust, depending on the level of risks. CPS uses data from several sensors for full information. There is a conflict between reliable in case of a failure of one sensor and faulty sensors, and therefore the user may receive false information [80].
3) The development of methods for ensuring the security of personal data. The growing popularity and development of DM technologies pose a serious threat to the security of confidential personal information. Data privacy may be violated due to unauthorized access to personal data. The wide application of DM and machine learning algorithms allow malicious users to use intelligent data analysis to access private information. This problem can be solved with the help of two aspects: ethical and technological. Security through transparency is one of the solutions [81].
4) The development of CPS security architecture. Analysis of the main CPS problems arising with the growth of rapidly developing cyber and physical threats shows that it is necessary to create a reliable and fault-tolerant architecture that ensures a high level of security and cost-effectiveness.
5) The development of countermeasures to increase the survivability of CPS. The development of countermeasures is an urgent task in order to minimize the number of vulnerabilities in the CPS. Analysis of recent work to improve the reliability and resiliency of CPS has shown the need to develop defensive mechanisms and evaluate their impact on the survivability of CPSs.
6) Security protocol development. The growing number of devices in CPSs raises many questions about the suitability and adaptability of state-of-the-art security standards and protocols to ensure the confidentiality and integrity of data. The use of smart security protocols, which allow the self-adopting and self-controlling of CPS architecture, and their integration into innovative, state-of-the-art devices are among the priority tasks. The interaction between security technologies of CPS components leads to interoperability issues. Providing built-in security and privacy from components to the CPS as a whole requires special attention.

10. Conclusion

CPSs are a promising paradigm for the development of current and future engineering systems and are expected to have an important impact on the real world. The idea of CPS focuses on the design of complex systems, not the cyber or physical system separately.

This paper gives a definition and background of CPS. The technical background and distinctive features of CPS, the principle of CPS operation and philosophical issues were discussed in detail. It was noted that the development of CPS and their impact on the life of modern people is extremely contradictory.

The problems of attacks in the cyberspace, which have different consequences and goals (such as to change some safety attributes, to cause catastrophic damage to system equipment and resources, to lead to production losses, to endanger life and safety of people, and to cause damage to the environment), were investigated. We considered the impact of cyber threats on authenticity, confidentiality, reliability, resilience, and integrity. This was reflected as a tree of attacks and threats on sensor devices, actuators, computing components, communications, and feedback.

In order to shed light on the current security problems of CPS, the paper presented a review of relevant literature on the discussion of practical applications in the areas of SCADA and Smart Grid security, countermeasures against cyber-attacks and communication security and the dominant areas of research.

The tables provide the main contributions and concepts of approaches in the areas of cyber-attack consequences estimation, modeling of CPS attacks, CPS attacks detection and development of security architecture, discussed in the papers and outline the future research directions of each article.

Finally, based on the latest CPS security research, we have identified future research areas for CPS deployment, including the development of methods for CPS components authentication, to determine the level of trust in CPS components, for ensuring the security of personal data, the development of countermeasures to increase the survivability of CPS and security protocol development. We hope that this work will help researchers in the field of CPS security.

References

[1] S. Zeadally, N. Jabeur, Cyber-Physical System Design with Sensor Networking Technologies, The Institution of Engineering and Technology, London UK, 2016.
[2] S.H.H.N. Ghazani, J.J. Lotf, R.M. Alguliev, A study on QoS models for mobile adhoc networks, Int. J. Model. Optim. 2 (5) (2012) 634–636.
[3] A. Sheth, P. Anantharam, C. Henson, Physical-cyber-social computing: an early 21 st century approach, IEEE Intell. Syst. 28 (1) (2013) 78–82.
[4] J. Zeng, L.T. Yang, M. Lin, H. Ning, J. Ma, A survey: cyber-physical-social systems and their system-level design methodology, Future Gener. Comput. Syst. (2016), http://dx.doi.org/10.1016/j.future.2016.06.034.
[5] C.H. Liu, Y. Zhang, Cyber Physical Systems: Architectures, Protocols and Applications, CRC Press, Taylor & Francis Group Florida, 2016.
[6] E.A. Lee, Cyber physical systems: design challenges, 11th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, Orlando, Florida, USA, 2008.
[7] K.H. Johansson, Control of cyber-physical systems: fundamental challenges and applications to transportation networks, 27th International Conference on Architecture of Computing Systems, Lübeck Germany, 2014.
[8] J.A. Stankovic, Research directions for the Internet of Things, IEEE IoT J. 1 (1) (2014) 3–9.
[9] L. Wang, X.V. Wang, Cloud-Based Cyber-physical Systems in Manufacturing, Springer International Publishing, London, 2018.
[10] P. Sobhrajan, S.Y. Nikam, Comparative study of abstraction in cyber physical system, Int. J. Comput. Sci. Inf.Technol. (IJCSIT) 5 (1) (2014) 466–469.
[11] R. Davies, The Internet of Things Opportunities and Challenges, European Parliamentary Research Service, 2015 PE 557.012 http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf).
[12] A. Hakansson, R. Hartung, E. Moradian, Reasoning strategies in smart cyber-physical systems, Procedia Comput. Sci. 60 (2015) 1575–1584.
[13] H. Ning, Q. Li, D. Wei, H. Liu, T. Zhu, Cyberlogic paves the way from cyber philosophy to cyber science, IEEE IoT J. 4 (3) (2017) 783–790.
[14] A. Hahn, R.K. Thomas, I. Lozano, A. Cardenas, A multi-layered and kill-chain based security analysis framework for cyber-physical systems, Int. J. Crit. Infr. Prot. 11 (2015) 39–50.
[15] M. Krotofil, J. Larsen, Are you threatening my hazards? 9th International Workshop on Security, Hirosaki Japan, 2014.
[16] M. Krotofil, A. Cardenas, Resilience of process control systems to cyberphysical attacks, 18th Nordic Conference on Secure IT Systems, Ilulissat Greenland, 2013.
[17] H. Kopetz, Real-Time Systems Design Principles for Distributed Embedded Applications, Springer, USA, 2011.
[18] M. Majdalawieh, Security Framework for DNP3 and SCADA, VDM Verlag, Saarbruken, Germany, 2008.
[19] C.R. Ozansoy, A. Zayegh, A. Kalam, Time synchronisation in a IEC 61850 based

substation automation system, IEEE −2008 Australasian Universities Power Engineering Conference, IEEE, Sydney Australia, 2008.
[20] Modbus-IDA, Modbus Application Protocol Specification V.1.1b, Modbus-IDA, Hopkinton, Massachusetts, 2016www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf.
[21] W. Fang-Jing, K. Yu-Fen, T. Yu-Chee, Review: from wireless sensor networks towards cyber physical systems, Pervasive Mob. Comput. 7 (4) (2011) 397–413.
[22] H. Li, L. Lai, H.V. Poor, Multicast routing for decentralized control of cyber physical systems with an application in smart grid, IEEE J. Sel. Areas Commun. 30 (2012) 1097–1107.
[23] A. Koubaa, B. Andersson, A vision of cyber-physical internet, 8th International Workshop on Real-Time Networks, Dublin, Ireland, 2009.
[24] A.A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, Challenges for securing cyber physical systems, Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ, 2009.
[25] J.H. Saltzer, M.D. Schroeder, The protection of information in computer systems, Proc. IEEE 63 (9) (1975) 1278–1308.
[26] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE Trans. Dependable Secure Comput. 1 (1) (2004) 11–32.
[27] E.K. Wang, Y. Ye, X. Xu, S.M. Yiu, L.C.K. Hui, K.P. Chow, Security issues and challenges for cyber physical system, IEEE/ACM International Conference on Cyber, Physical and Social Computing, Hangzhou, China, 2010.
[28] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, Comput. Networks 76 (2015) 146–164.
[29] D. Xu, M. Tu, M. Sanford, L. Thomas, D. Woodraska, W. Xu, Automated security test generation with formal threat models, IEEE Trans. Dependable Secure Comput. 9 (4) (2012) 525–539.
[30] Z. Xinlan, H. Zhifang, W. Guangfu, Z. Xin, Information security risk assessment methodology research: group decision making and analytic hierarachy process, Second WRI World Congress on Software Engineering, Wuhan, China, 2010.
[31] C. Neuman, K. Tan, Mediating cyber and physical threat propagation in secure smart grid architectures, Second International Conference on Smart Grid Communications, IEEE, Brussels Belgium, 2011.
[32] Z. Brooks, Hacking Driverless Vehicles, DEFCON, 2016, https://www.defcon.org/images/defcon-21/dc-21-presentations/Zoz/DEFCON-21-Zoz-Hacking-Driverless-Vehicles.pdf.
[33] M. Krotofil, J. Larsen, D. Gollmann, The process matters: ensuring data veracity in cyber-physical systems, 10th ACM Symposium on Information, Computer and Communications Security, ACM Singapore, 2015.
[34] S.M. Djouadi, A.M. Melin, E.M. Ferragut, J.A. Laska, J. Dong, Finite energy and bounded actuator attacks on cyber-physical systems, 14th IEEE European Control Conference, Linz Austria, 2015.
[35] A. Singhal, Data Warehousing and Data Mining Techniques for Cyber Security, Springer Science + Business Media, USA, 2007.
[36] R. Mitchell, I.R. Chen, Effect of intrusion detection and response on reliability of cyber physical systems, IEEE Trans. Reliab. 62 (1) (2013) 199–210.
[37] A.A. Cardenas, S. Amin, S. Sastry, Research challenges for the security of control systems, 3rd Conference on Hot Topics in Security, San Jose, CA, 2008.
[38] K. Wan, K.L. Man, D. Hughes, Specification analyzing challenges and approaches for cyber-physical systems (CPS), Eng. Lett. 18 (3) (2010) 308–315.
[39] L. Sha, J. Meseguer, Design of Complex Cyber Physical Systems with Formalized Architectural Patterns, Software-Intensive Systems and New Computing Paradigms, Springer-Verlag, Berlin, 2008.
[40] Y.Z. Lun, A.D. Innocenzo, I. Malavolta, M.D. Di Benedetto, Cyber-physical Systems Security: a Systematic Mapping Study, (2016) (arXiv preprint arXiv: 1605.09641).
[41] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, X.-M. Zhang, A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing 275 (1) (2018) 1674–1683.
[42] Y. Ashibani, Q.H. Mahmoud, Cyber-physical systems security: analysis challenges and solutions, Comput. Secur. 68 (2017) 81–97.
[43] S. Karnouskos, Stuxnet worm impact on industrial cyber-physical system security, 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, Victoria Australia, 2011.
[44] S. Collins, S. McCombie, Stuxnet: the emergence of a new cyber weapon and its implications, Journal of Policing, Intell. Counter Terror. 7 (1) (2012) 80–91.
[45] M. Krotofil, A.A. Cardenas, J. Larsen, D. Gollmann, Vulnerabilities of cyber-physical systems to stale data-determining the optimal time to launch attacks, Int. J. Crit. Infr. Prot. 7 (2014) 213–232.
[46] A.G. Finogeev, A.A. Finogeev, Information attacks and security in wireless sensor networks of industrial SCADA systems, J. Ind. Inf. Integr. 5 (2017) 6–16.
[47] W. Li, L. Xie, Z. Deng, Z. Wang, False sequential logic attack on SCADA system and its physical impact analysis, Comput. Secur. 58 (2016) 149–159.
[48] Y.F. Khalil, A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures, Process Saf. Environ. Prot. 102 (2016) 473–484.
[49] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla, Smart grid data integrity attacks, IEEE Trans. Smart Grid 4 (3) (2013) 1244–1253.
[50] B. Genge, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures, Int. J. Crit. Infr. Prot. 10 (2015) 3–17.
[51] I. Friedberg, F. Skopik, G. Settanni, R. Fiedler, Combating advanced persistent threats: from network event correlation to incident detection, Comput. Secur. 48 (2015) 35–57.
[52] S. Ntalampiras, Automatic identification of integrity attacks in cyber-physical systems, Expert Syst. App. 58 (2016) 164–173.
[53] H. Orojloo, M. Abdollahi Azgomi, A method for evaluating the consequence propagation of security attacks in cyber?physical systems, Future Gen. Comput. Syst. 67 (2017) 57–71.
[54] Y.L. Huang, A.A. Cardenas, S. Amin, Z.S. Lin, H.Y. Tsai, S. Sastry, Understanding the physical and economic consequences of attacks on control systems, Int. J. Crit. Infr. Prot. 2 (2009) 73–83.
[55] F. Hu, Y. Lu, A.V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, N.N. Xiong, Robust cyber-physical systems: concept, models, and implementation, Future Gen. Comput. Syst. 56 (2016) 449–475.
[56] Q. Yang, L. Chang, W. Yu, On false data injection attacks against kalman filtering in power system dynamic state estimation: int, J. Security Commun. Networks 9 (2016) 833–849.
[57] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: vANETs and IoV, Ad Hoc Networks 61 (2017) 33–50.
[58] R. Mitchell, I.R. Chen, Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems, IEEE Trans. Reliab. 65 (2015) 350–358.
[59] Y. Mo, R. Chabukswar, B. Sinopoli, Detecting integrity attacks on SCADA systems, IEEE Trans. Control Syst. Technol. 22 (4) (2013) 1396–1407.
[60] H. Yoo, T. Shon, Challenges and research directions for heterogeneous cyber–-physical system based on IEC 61850: vulnerabilities, security requirements, and security architecture, Future Gen. Comput. Syst. 61 (2016) 128–136.
[61] M. Yampolskiy, P. Horvath, X.D. Koutsoukos, Y. Xue, J. Sztipanovits, A language for describing attacks on cyber-physical systems, Int. J. Crit. Infr. Prot. 8 (2014) 40–52.
[62] T. Liu, Y. Sun, Y. Liu, Y. Gui, Y. Zhao, D. Wang, C. Shen, Abnormal traffic-indexed state estimation: a cyber–physical fusion approach for Smart Grid attack detection, Future Gen. Comput. Syst. 49 (2015) 94–103.
[63] B. Li, R. Lu, W. Wang, K.K.R. Choo, Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system, J. Parallel Distrib. Comput. 103 (2016) 32–41.
[64] A. Srivastava, T.H. Morris, T. Ernster, C. Vellaithurai, S. Pan, U. Adhikari, Modeling cyber-physical vulnerability of the smart grid with incomplete information, IEEE Trans. Smart Grid 4 (2013) 235–245.
[65] A. Ashok, A. Hahn, M. Govindarasu, Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment, J. Adv. Res. 5 (2014) 481–489.
[66] B. Genge, C. Siaterlis, M. Hohenadel, Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems, Int. J. Comput. Commun. Control 7 (2014) 674–687.
[67] H. Vincent, L. Wells, P. Tarazaga, J. Camelio, Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems, 43rd SME North American Manufacturing Research Conference, Charlotte, North Carolina, 2015.
[68] P.-Y. Chen, S.-M. Cheng, K.-C. Chen, Information fusion to defend intentional attack in Internet of Things, IEEE IoT J. 1 (4) (2014) 337–348.
[69] S.R. Moosavi, T.N. Gia, A.M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, Procedia Comput. Sci. 52 (2015) 452–459.
[70] P. Venkitasubramaniam, J. Yao, P. Pradhan, Information-theoretic security in stochastic control systems, Proc. IEEE 103 (10) (2015) 1914–1931.
[71] M. Mavani, K. Asawa, Modeling and analyses of IP spoofing attack in 6LoWPAN network, Comput. Security 70 (2017) 95–110.
[72] S. Mauw, M. Oostdijk, Foundations of attack trees, in: D.H. Won, S. Kim (Eds.), Information Security and Cryptology − ICISC 2005. ICISC 2005. Lecture Notes in Computer Science, vol. 3935, Springer Berlin, Heidelberg, 2006.
[73] W. Wu, R. Kang, Z. Li, Risk assessment method for cyber security of cyber physical systems, 1 St International Conference On Reliability Systems Engineering, Beijing, China, 2015.
[74] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, A. Coen-Porisini, A secure and quality-aware prototypical architecture for the Internet of Things, Inf. Syst. 58 (2016) 43–55.
[75] S. Barnum, S. Sastry, J.A. Stankovic, Roundtable: reliability of embedded and cyber-physical systems, IEEE Secur. Privacy 8 (5) (2010) 27–32.
[76] K.D. Kim, P.R. Kumar, Cyber-physical systems: a perspective at the centennial, Proc. IEEE 100 (2012) 1287–1308.
[77] P. Derler, E.A. Lee, A. Sangiovanni-Vincentelli, Modeling cyber-physical systems, Proc. IEEE 100 (1) (2012) 1–28.
[78] R. Baheti, H. Gill, Cyber-physical Systems, The Impact of Control Technology vol. 12, (2011), pp. 161–166.
[79] A. Nourian, S. Madnick, A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet, IEEE Trans. Dependable Secure Comput. 99 (2015) 1–19.
[80] L.-A. Tang, X. Yu, S. Kim, Q. Gu, J. Han, A. Leung, T. La Porta, Trustworthiness analysis of sensor data in Cyber-Physical Systems, J. Comput. Syst. Sci. 79 (3) (2013) 383–401.
[81] A. Ouaddah, H. Mousannif, A.A. Elkalam, A.A. Ouahman, Access control in the Internet of Things: big challenges and new opportunities, Comput. Netw. 112 (2017) 237–262.
[82] A. Wasicek, P. Derler, E. Lee, Aspect-oriented modeling of attacks in automotive cyber-physical systems, 51 St Annual Design Automation Conference, San Francisco, CA USA, 2014.
[83] G. Martins, S. Bhatia, X. Koutsoukos, K. Stouffer, C. Tang, R. Candell, Towards a Systematic Threat Modeling Approach for Cyber-physical Systems, Resilience Week (RSW), Philadelphia, PA USA, 2015.

Rasim M. Alguliyev. He is director of the Institute of Information Technology of Azerbaijan National Academy of Sciences (ANAS) and academician-secretary of ANAS. He is full member of ANAS and full professor. He received BSc and MSc in electronic computing machines from the Azerbaijan Technical University in 1979. He received his PhD and Doctor of Science (higher degree after PhD) in Computer Science in 1995 and 2003, respectively. His research interests include: Information Security, E-government, Data Mining, Big Data, Online Social Network Analysis, Cloud Computing, Evolutionary and Swarm Computation, and Scientometrics. He is author more than 580 papers, 4 monographs, 4 patents, several books.

Yadigar N. Imamverdiyev is a Head of Research Lab at Institute of Information Technology, Azerbaijan National Academy of Sciences. He received the M.Sc. degree in 1989 in Applied Mathematics at Azerbaijan State Oil Academy and Ph.D. degree in 2006 in Computer Science at Institute of Information Technology, Azerbaijan. He was a Postdoctoral Research Fellow in 2011.08–2012.08 at Biometric Engineering Research Center of Yonsei Univiversity, South Korea. He was a researcher in more than 10 International and Azerbaijani Research Projects. He has over 100 papers published in international journals and conferences. He is co-author of 6 books, and co-editor of 3 Proceedings Book.

Lyudmila V. Sukhostat works in the Research Lab at Institute of Information Technology, Azerbaijan National Academy of Sciences. She received the M.Sc. degree in 2011 in Applied Mathematics at Azerbaijan State Oil Academy and Ph.D. degree in 2015 in Computer Science at Institute of Information Technology, Azerbaijan.S he has over 20 papers published in international journals and conferences.