Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.

Microprocessors and Microsystems 77 (2020) 103201

Contents lists available at ScienceDirect

Microprocessors and Microsystems

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

Cyber-physical systems security: Limitations, issues and future trends

Jean-Paul A. Yaacoub[a], Ola Salman[b,*], Hassan N. Noura[a], Nesrine Kaaniche[c], Ali Chehab[b], Mohamad Malli[a]

[a] Arab Open University, Department of Computer Sciences, Beirut, Lebanon
[b] American University of Beirut, Electrical And Computer Engineering, Lebanon
[c] University of Sheffield, Department of Computer Science, United Kingdom

ARTICLE INFO

Article history:
Received 1 November 2019
Revised 30 April 2020
Accepted 2 July 2020
Available online 8 July 2020

Keywords:
Cyber-physical systems
Cyber-security threats
attacks and issues
Cyber-physical vulnerabilities and challenges
Security
privacy and forensics solutions
Security and performance analysis

ABSTRACT

Typically, Cyber-Physical Systems (CPS) involve various interconnected systems, which can monitor and manipulate real objects and processes. They are closely related to Internet of Things (IoT) systems, except that CPS focuses on the interaction between physical, networking and computation processes. Their integration with IoT led to a new CPS aspect, the Internet of Cyber-Physical Things (IoCPT). The fast and significant evolution of CPS affects various aspects in people's way of life and enables a wider range of services and applications including e-Health, smart homes, e-Commerce, etc. However, interconnecting the cyber and physical worlds gives rise to new dangerous security challenges. Consequently, CPS security has attracted the attention of both researchers and industries. This paper surveys the main aspects of CPS and the corresponding applications, technologies, and standards. Moreover, CPS security vulnerabilities, threats and attacks are reviewed, while the key issues and challenges are identified. Additionally, the existing security measures are presented and analyzed while identifying their main limitations. Finally, several suggestions and recommendations are proposed benefiting from the lessons learned throughout this comprehensive review.

© 2020 Elsevier B.V. All rights reserved.

1. Introduction

Cyber Physical Systems (CPS) are designated as essential components of the Industrial Internet of Things (IIoT), and they are supposed to play a key role in Industry v4.0. CPS enables smart applications and services to operate accurately and in real-time. They are based on the integration of cyber and physical systems, which exchange various types of data and sensitive information in a real-time manner [1]. The development of CPS is being carried out by researchers and manufacturers alike [2]. Given that CPS and Industry v4.0 offer a significant economic potential [3], the German gross value will be boosted by a cumulative of 267 billion Euros by 2025 upon the introduction of CPS into Industry v4.0 [4].

A CPS is identified as a network of embedded systems that interact with physical input and output. In other words, CPS consists of the combination of various interconnected systems with the ability to monitor and manipulate real IoT-related objects and processes. CPS includes three main central components: sensors, aggregators and actuators. Moreover, CPS systems can sense the surrounding environment, with the ability to adapt and control the physical world [5]. This is mainly attributed to their flexibility and capability to change the run-time of system(s) process(es) through the use of real-time computing [6]. In fact, CPS systems are being used in multiple domains (see Fig. 1), and embedded in different systems such as power transmission systems, communication systems, agricultural/ecological systems, military systems [7,8], and autonomous systems (drones, robotics, autonomous cars, etc.) [9,10]. That, in addition to medical care domains to enhance the medical services [11]. Moreover, CPS can be used in supply chain management to enable echo-friendly, transient, cost efficient, and safe manufacturing process.

1.1. Problem formulation

Despite their numerous advantages, CPS systems are prone to various cyber and/or physical security threats, attacks and challenges. This is due to their heterogeneous nature, their reliance on private and sensitive data, and their large scale deployment. As such, intentional or accidental exposures of these systems can result into catastrophic effects, which makes it critical to put in place robust security measures. However, this could lead to unacceptable network overhead, especially in terms of latency. Also, zero-day vulnerabilities should be minimized with constant software, applications and operating system updates.

* Corresponding author.
E-mail address: oms15@mail.aub.edu (O. Salman).

https://doi.org/10.1016/j.micpro.2020.103201
0141-9331/© 2020 Elsevier B.V. All rights reserved.

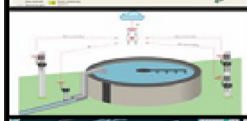
Naming	Classification	Description
Smart House	Industrial-Consumer IoT	• Control Smart Devices • Homeowner Security & Comfort
Oil Refinery	Industrial-Transportation IoT	• Naphta, Gasoline, Diesel • Asphalt, Petroleum, Fuel, Oil
Smart Grid	Industrial IoT	• Smart Efficient Energy • Energy Control & Management
 Water Treatment	Industrial-Consumer IoT	• Improved Water Quality • Overcome Contamination & Undesirable Components
Medical Devices	Medical-Wearable IoT	• Improved Patients Life • Enhanced Medical Treatment • Remote Patient Monitoring
SCADA	Industrial IoT	• Control & Monitor Telecoms. • Control & Monitor Industries
Smart Cars	Industrial-Transportation IoT	• Echo Friendly • Enhanced Driver Experience • Advanced Safety Features
Supply Chains	Industrial-Transportation IoT	• Real-Time Delivery Source/Destination • Less Delays & Echo Friendly

Fig. 1. CPS description & classification.

1.2. Related work

Recently, several research works addressed the different security aspects of CPS: the different CPS security goals were listed and discussed in Chen [12], Miller and Valasek [13], Bou-Harb [14], Sklavos and Zaharakis [15]; maintaining CPS security was presented in Humayed et al. [16]; CPS security challenges and issues were presented in Yoo and Shon [17], Alguliyev et al. [18]; some of the security issues were reviewed, including big data security [19,20], IoT storage issues [21], and Operating System vulnerabilities [22]; several security and privacy solutions using cryptographic algorithms and protocols were discussed in Kocabas et al. [23], Lai et al. [24]. However, none of the existing works presented a comprehensive view of CPS security in terms of threats, vulnerabilities, and attacks based on the targeted domain (cyber, physical, or hybrid). Hence, this paper presents a detailed overview of the existing cyber, physical and hybrid attacks, and their security solutions including cryptographic and non-cryptographic ones. Moreover, for the first time, CPS forensics are discussed as an essential requirement for the investigation of the causes of CPS-related crimes and attacks.

1.3. Motivation

CPS systems have been integrated into critical infrastructures (smart grid, industry, supply chain, healthcare, military, agriculture, etc.), which makes them an attractive target for security attacks for various purposes including economical, criminal, military, espionage, political and terrorism as well. Thus, any CPS vulnerability can be targeted to conduct dangerous attacks against such systems. Different security aspects can be targeted including confidentiality, integrity, and availability. In order to enable the wide adoption and deployment of CPS systems and to leverage their benefits, it is essential to secure these systems from any possible attack, internal or/and external, passive or active.

The main motivation of this work is to identify the main CPS security threats, vulnerabilities and attacks, and to discuss the advantages and limitations of the existing security solutions, with the aim to identify the requirements for a secure, accurate, reliable, efficient and safe CPS environment. Moreover, the security solutions are analyzed in terms of the associated computational complexity. Note that CPS systems require innovative security solutions that can strike a good balance between security level and system performance.

1.4. Contributions

In this work, we conduct a comprehensive overview and analysis of the different cyber-physical security aspects of CPS. The contributions entail the following:

- **General Background** about CPS including their main layers, components and model types.
- **Cyber-Physical Attacks** are presented in relation to the targeted cyber and/or physical system/device, and the corresponding vulnerabilities of each such domain.
- **Risk Assessment:** a qualitative risk assessment method is presented to evaluate the risk and exposure levels for each CPS system, while proposing suitable security countermeasures.

- **Security Measures** and their limitations are discussed and analyzed, including recent cryptographic and non-cryptographic solutions.
- **Forensics** solutions are also presented and discussed about securely extracting evidence and thus, to improve forensics investigations.
- **Lessons:** various lessons are learnt throughout this survey including how to protect real-time data/information communication among resource-constrained CPS devices, and how to achieve protection of CPS security goals such as confidentiality, integrity, availability and authentication.
- **Suggestions & Recommendations** are presented about how to mitigate and overcome various cyber, physical and hybrid threats, vulnerabilities, attacks, challenges and issues for a safe CPS environment.

1.5. Organization

Aside from the introduction, this paper is divided into six main sections as follows. Section 2 presents some background about CPS including their layers, components, and models. Section 3 discusses and details the key CPS threats, attacks and vulnerabilities in addition to listing and describing several real-case CPS attacks, and the main persistent challenges and issues. Section 5 assesses and evaluates the risks associated with CPS security attacks, especially in a qualitative risk assessment manner. Section 5 presents and analyzes the main CPS security solutions including cryptographic, non-cryptographic, and forensics ones. Section 6 highlights the lessons learnt throughout this study. Section 7 provides key suggestions and recommendations for a safe and secure CPS environment. Section 8 concludes the presented work.

2. CPS - background

In this section, we present the CPS architecture, its main layers and components, as well as the main CPS models.

2.1. CPS layers & components

The architecture of CPS systems consists of different layers and components, which rely on different communication protocols and technologies to communicate among each other across the different layers.

2.1.1. CPS layers

The CPS architecture consists of three main layers, the perception layer, transmission layer, and application layer, which are presented and described in Fig. 2. The analysis of the security issues at the various CPS layers is based on the work in Ashibani and Mahmoud [25].

- **Perception Layer:** It is also known as either the recognition or the sensing layer [26]. It includes equipment such as sensors, actuators, aggregators, Radio-Frequency IDentification (RFID) tags, Global Positioning Systems (GPS) along with various other devices. These devices collect real-time data in order to monitor, track and interpret the physical world [27]. Examples of such collected data include electrical consumption, heat, location, chemistry, and biology, in addition to sound and light signals [28], depending on the sensors' type [29]. These sensors generate real-time data within wide and local network domains, before being aggregated and analyzed by the application layer. Moreover, securing actuators depends on authorized sources to ensure that both feedback and control commands are error-free and protected [30]. Generally, increasing the security level requires an end-to-end encryption scheme at each layer [31]. Therefore, heavyweight computations and large memory requirements would be introduced [32]. In this context, there is a need for the design of efficient and lightweight security protocols, which take into consideration the devices capabilities and the security requirements.
- **Transmission Layer:** It is also known as the transport layer or network layer, and it is the second CPS layer [29]. This layer interchanges and processes data between the perception and application layers. Data transmission and interaction is achieved through the Internet using Local Area Networks (LANs) and communication protocols including Bluetooth, 4G and 5G, InfraRed (IR) and ZigBee, Wi-Fi, Long Term Evolution (LTE), along with other technologies. For this purpose, various protocols are used to address the increase in the number of internet-connected devices, such as the Internet Protocol version 6 (IPv6) [33]. This layer also ensures data routing and transmission using cloud computing platforms, routing devices, switching and internet Gateways, firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) [34,35]. Before outsourcing data contents, it is essential to secure their transmission to prevent intrusions and malicious attacks including malware, malicious code injection [36], Denial of Service/Distributed Denial of Service (DoS/DDoS), eavesdropping, and unauthorised access attacks [37]. This introduces a challenge, especially for resource-constrained devices due to the imposed overhead in terms of the required processing and power resources [38].
- **Application Layer:** It is the third and most interactive layer. It processes the received information from the data transmission layer and issues commands, which are executed by the physical units including sensors and actuators [39]. This is done by implementing complex decision-making algorithms based on the

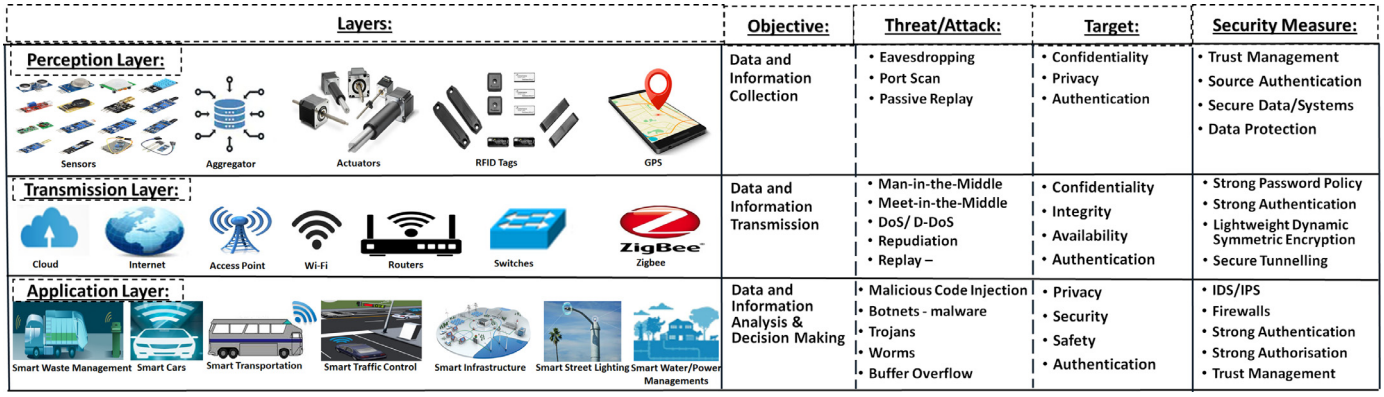


Fig. 2. CPS layers.

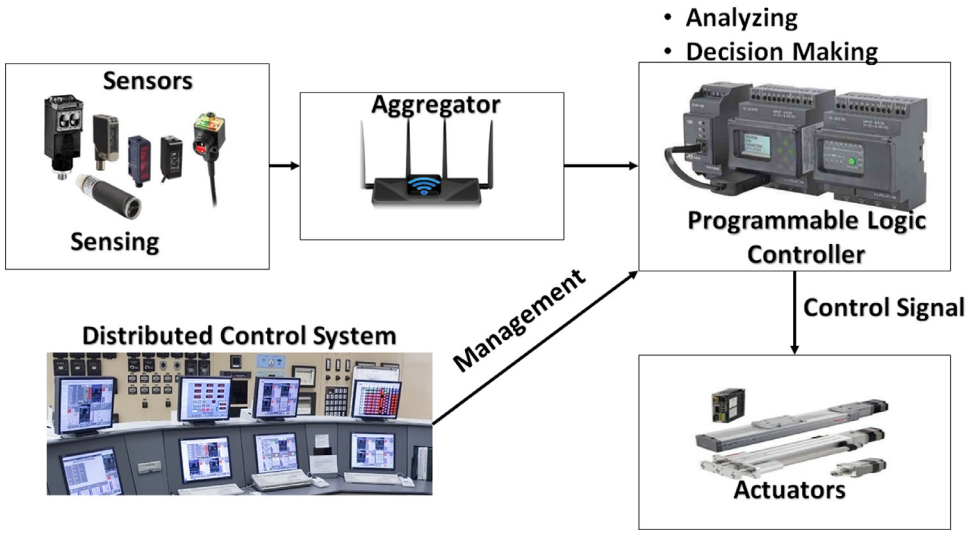


Fig. 3. Infrastructure of CPS.

aggregated data [40]. Moreover, this layer receives and processes information from the perception layer before determining the rightly invoked automated actions [29]. In fact, cloud computing, middleware, and data mining algorithms are used to manage the data at this layer [41]. Protecting and preserving privacy requires protecting private data from being leaked. The most known protective approaches include anonymization, data masking (camouflage) [42,43], privacy-preserving, and secret sharing [31]. Moreover, this layer also requires a strong multi-factor authentication process to prevent unauthorised access and escalation of privilege [44]. Due to the increase in the number of Internet-connected devices, the size of the generated data has become a significant issue [21]. Therefore, securing big data calls for efficient protection techniques to process huge amounts of data in a timely and efficient manner [45].

2.1.2. CPS components

CPS components are used for sensing information [5], or for controlling signals (Fig. 3). In this regard, CPS components are classified into two main categories: **Sensing Components (SC)** that collect and sense information, and **Controlling Components (CC)** that monitor and control signals.

- **Sensing Components:** are primarily located at the perception layer and consist of sensors that collect data/information and forward them to aggregators. Then, this data/information is sent to the actuators for further analysis to ensure accurate decision making. In the following, we list the main CPS sensing components.
  - **Sensors:** collect and record real-world data following a correlation process named "calibration", to assess the correctness of the collected data [46]. Sensing data is essential since the decisions that will be made are based on the analysis of this data.
  - **Aggregators:** are primarily located at the transmission layer (i.e routers, switches and gateways) to process the received data/information from sensors, before issuing the corresponding decision(s). In fact, data aggregation is based on the collected information about a specific target, where this information is gathered and summarized following a statistical analysis. Online Analytical Processing (OLAP) is a prime data aggregation type used as an online reporting mechanism for processing information [46].
  - **Actuators:** are located at the application layer to make the information visible to the surrounding environment based on the decisions made by the aggregators. Since actuators highly depend on other network nodes, then each action performed by the CPS relies on an earlier data aggregation sequence [5]. Also in terms of operations, actuators process electrical signals as input and generate physical actions as output [46].
- **Controlling Components:** are used to control Signals and they play a key role in signal control, monitoring and management to achieve higher levels of accuracy and protection against malicious attacks or accidents, mainly signal jamming, noise and interference. As a result, the reliance on Programmable Logic Controllers (PLCs) and Distributed Control System (DCSs) along with their components (i.e Programmable Automation Controller (PAC) [47], Operational Technology/Information Technology (OT/IT) [48], Control Loop/Server [49], and Human-Machine Interface (HMI)/Graphical User Interface (GUI) [50]) has become highly essential. Next, we list the different types of control systems that are used in CPS systems:
- **Programmable Logic Controllers (PLC):** were initially developed to replace hard-wired relays, and are considered as industrial digital computers that control the manufacturing processes such as robotic devices performance and/or fault diagnosis processing; hence achieving better flexibility and resiliency.
- **Distributed Control Systems (DCS):** are computerized control systems that allow the autonomous controllers' distribution throughout the system using a central operator supervisory control. As a result of the remote monitoring and supervision process, the DCS's reliability is increased, whilst its installation cost is reduced. In some cases, DCS can be similar to Supervisory Control and Data Acquisition (SCADA) systems.
- **Remote Terminal Units (RTU):** or "Remote Telemetry Unit" [51], are electronic devices controlled by a microprocessor such as the Master Terminal Unit (MTU) [52]. Unlike the PLC, they do not support any control loop nor control algorithm(s). Thus, making them more suitable for wireless communications over wider geographical telemetry areas. RTU's main task is to interface SCADA to the physical object(s) using a supervisory messaging system that controls these objects through the system's transmission of telemetry data.

In fact, both RTUs and PLCs use a small computerized "artificial brain" (Central Processing Unit (CPU)) to process inputs and

Table 1
PLC vs. RTU.

PLC (Programmable Logic Controller)	RTU (Remote Terminal/Telemetry Units)
Sold with RTU like features	Sold with PLC-like features
Digital computers designed for output arrangements and multiple inputs	Electronic device controlled by a microprocessor
Automates electro-mechanical processes	Interfaces SCADA physical objects
Physical media with process, relays, motion control and networking	Uses supervisory system messages to control objects
Does support control loops and algorithms	Does not support control loops and algorithms
Immune to electrical noise, resistant to vibration	Low to null immunity against electrical noise and vibration
Suitable for local geographical areas	Suitable for wider geographical telemetry areas
Mainly IEC Standards	Wired/Wireless Communications

outputs from sensing devices and pumping equipment [53]; hence using IEDs (Intelligent Electronic Devices) to transmit data flow or trigger an alarm in case of any intrusion. Table 1 a comparison of the common points and differences between PLCs and RTUs. Concerning the relation between components and layers, it can be seen that sensing components are mainly deployed at the perception and transmission layers, while the controlling components are deployed at the application layer.

2.2. CPS model types

CPS models can be divided into three main types:

- **Timed Actor CPS:** This model focuses on the functional aspects based on behaviour and correctness, along with the non-functional aspects that are based on performance and timing. A theory was introduced in Geilen et al. [54] with a functional and classical refinement that restricts certain behaviour set, improving efficiency while reducing complexity. The main focus is on the refinement based on the "earlier-the-better" principle since it offers the ability to identify deterministic abstractions of non-deterministic systems [55]. In fact, these time-deterministic models are less prone to state explosion problems, with the ability to derive analytical bounds easier [56].
- **Event-Based CPS:** In such models, an event must be sensed and detected by the proper CPS components, before the actuation decisions are made. However, individual component timing constraints vary depending on the non-deterministic system delay, which is caused by the different CPS actions including sensing, actuating, communication and computing [57]. In [58], Hu et al. stated that time constraints can be handled through the use of an event-based approach, which uses CPS events to ensure the system's communication, computation, and control processes. This allows the CPS to be more suitable and more useful for spatio-temporal information.
- **Lattice-Based Event Model** In [59], the CPS events are represented according to the event type, along with the internal and external event attributes. If these events are combined, they can be used to define a spatio-temporal property of any given event, while also identifying all the components that were observing the event.
- **Hybrid-Based CPS Model** Hybrid CPS systems are heterogeneous systems that are made up of two distinct interactive system types, continuous state (physical dynamic systems) and discrete-state (discrete computing systems) [60,61]. Both development and evolution depend on the response of discrete transient events represented by finite state machines, and the the dynamic behaviour represented by differential/difference equation(s) [62]. Unlike other CPS models, hybrid CPS is interconnected via a network, which makes it prone to delays. Moreover, hybrid CPS systems do not support any hierarchical modeling, and are not suitable for modeling concurrent systems. Hence, hybrid systems modeling challenges caused by CPS were discussed by Benveniste et al. [63]. In fact, CPS system network latency issues were addressed and solved by Kumar et al. using a real-time hybrid authentication method [64], while a configurable real-time hybrid structural testing for CPS was presented by Tidwell et al. [65]. Finally, an event driven monitoring of CPS based on hybrid automata was presented by Jianhui [66].

3. CPS vulnerabilities, threats, attacks & failures

In a similar manner to most networking systems, security services were not incorporated into CPS systems by design, leaving the door open for various vulnerabilities and threats to be leveraged by attackers to launch security attacks. This is also due to the heterogeneous nature of CPS devices since they operate in different IoT domains and communicate using different technologies and protocols.

3.1. CPS security threats

CPS security threats can be classified as cyber or physical threats, as explained below, and if combined, these can result into cyber-physical threats.

3.1.1. Cyber threats

The main attention on Industrial IoT security was highly focused on cyber threats rather than physical threats for many reasons, as cited in Alguliyev et al. [18]. This includes the electrical grid evolution into an Advanced Metering Infrastructure (AMI), which resulted into the rise of newly unknown cyber threats aside from SCADA vulnerabilities [67–69]. Electronic attacks are now easier to launch from any device, unlike physical attacks that require physical presence and physical tools. Moreover, the smart meter interfacing and interconnection with other meters in the Near-me Area Network (NAN) and Home Area Network (HAN) increase its exposure to various remote threats. Finally, electronic attacks are difficult to mitigate and overcome in the absence of the right prevention and defensive countermeasures. For further details on cyber threat intelligence, a brief survey of CPS security approaches was presented in Bou-Harb [14]. For further information about cyber security threats, more details can be found in Cleveland [70], Metke and Ekl [71].

Since cyber security is not limited to a single aspect, it can be considered from different perspectives, such as:

- **Centring Information:** which requires protecting the data flow during the storage phase, transmission phase, and even the processing phase.
- **Oriented Function:** which requires integrating the cyber-physical components in the overall CPS.
- **Oriented Threat:** which impacts data confidentiality, integrity, availability, and accountability [70].

The above issues make CPS systems prone to:

- **Wireless Exploitation:** It requires knowledge of the system's structure and thus, exploiting its wireless capabilities to gain

remote access or control over a system or possibly disrupt the system's operations. This causes collision and/or loss of control [72].

- **Jamming:** In this case, attackers usually aim at changing the device's state and the expected operations to cause damage by launching waves of de-authentication or wireless jamming signals, which would result into denial of device and system services [73].
- **Reconnaissance:** An example of such a threat is where intelligence agencies continuously perform operations targeting a nation's Computational Intelligence (CI) and Industrial Control System (ICS) mainly through a malware spread [74]. This results in violating data confidentiality due to the limitation of traditional defenses [75,76].
- **Remote Access:** This is mainly done by trying to gain remote access to the CPS infrastructure, for example, causing disturbances, financial losses, blackouts, as well as industrial data theft and industrial espionage [77]. Moreover, Havex Trojans are among the most dangerous malware against ICSs, as they can be weaponized and used as part of cyber-warfare campaign management against a nation's CPS [78].
- **Disclosure of Information:** Hackers can disclose any private/personal information through the interception of communication traffic using wireless hacking tools [16], violating both privacy and confidentiality [79].
- **Unauthorised Access:** Attackers try to gain an unauthorized access through either a logical or physical network breach and to retrieve important data, leading to a privacy breach [80].
- **Interception:** Hackers can intercept private conversations through the exploitation of already existing or new vulnerabilities leading to another type of privacy and confidentiality breach [72].
- **GPS Exploitation:** Hackers can track a device or even a car by exploiting (GPS) navigation systems, resulting in a location privacy violation [72,81].
- **Information Gathering:** software manufacturers covertly gather files and audit logs stored on any given device in order to sell this huge amount of personal information for marketing and commercial purposes in an illegal manner.

3.1.2. Physical threats

CPS systems are recently evolving into the industrial domain by introducing an Advanced Metering Infrastructure (AMI), and Neighbourhood Area Networks (NANs), along with data meter management systems to maintain the robustness of CPS in industrial domains [82]. In fact, physical threats might be classified according to the following three factors:

- **Physical Damage:** since different facility types implement different levels of protection, power-generating stations (E.g power grid, power plants, base stations) are well protected. This is due to the fact that these stations are well-manned and well-guarded based on the implementation of access controls, authorisation and authentication mechanisms such as usernames and passwords, access cards, biometrics and video surveillance. However, the main concern is related to the less protected power-generating sub-stations since transmission lines are vulnerable to sabotage attacks and disruption. In fact, smart meters are also vulnerable to a number of threats as explained in Chen et al. [83]. To address this problem, smart meters must be tamper-resistant by relying on outage detection or even host-based intrusion detection. However, it is almost impossible to prevent physical tampering or theft by adversaries (such as Advanced Persistent Threats (APTs)), except that it is possible to mitigate the risk and reduce its impact.
- **Loss:** the most worrying scenario is having more than a single substation failure caused by a malicious attacker. In case of a severe damage in the smart grid, a total blackout of major metropolitan areas may occur for several hours [84]. A real-case scenario includes the cascading blackout that managed to hit the U.S. on August 14th, 2003 [85], caused by the People Liberation Army (PLA), which is a Chinese politically-motivated group [86].
- **Repair:** it can be based on a self-healing process [87], which is based on the ability to either sense faults or disruptions, whilst isolating the problem and sending alerts to the corresponding control system to automatically reconfigure the back-up resources in order to continuously provide the necessary service. The aim is to ensure a fast recovery in as short of a time as possible. However, critical components do suffer from either a lack or a limited backup capability. Therefore, self-healing can respond faster to a severe damage.

Some of the threats associated with CPS systems include:

- **Spoofing:** it consists of masquerading the identity of a trusted entity by a malicious unknown source. In this case, attackers are capable of spoofing sensors, for example, by sending misleading and/or false measurements to the control center.
- **Sabotage:** Sabotage consists of intercepting the legal communication traffic and redirecting it to malicious third party or disrupting the communication process. For example, attackers can sabotage physically exposed CPS components across the power grid, to cause a service disruption or even denial of service that leads to either total or partial blackout.
- **Service Disruption or Denial:** Attackers are capable of physically tampering with any device to disrupt a service or to change the configuration. This has serious effects, especially in the case of medical applications.
- **Tracking:** Since devices are physically exposed, an attacker can gain access to a given device, and/or even attach a malicious device or track the legal ones.

In the following, we present the main CPS vulnerabilities that can be targeted by the above-mentioned threats.

3.2. CPS vulnerabilities

A vulnerability is identified as a security gap that can be exploited for industrial espionage purposes (reconnaissance or active attacks). Hence, a vulnerability assessment includes the identification and analysis of the available CPS weaknesses, while also identifying appropriate corrective and preventive actions to reduce, mitigate or even eliminate any vulnerability [88].

In fact, CPS vulnerabilities are divided into three main categories:

- **Network Vulnerabilities:** include weaknesses of the protective security measures, in addition to compromising open wired/wireless communication and connections, including man-in-the-middle, eavesdropping, replay, sniffing, spoofing and communication-stack (network/transport/application layer) [89], back-doors [90], DoS/DDoS and packet manipulation attacks [91].
- **Platform Vulnerabilities:** include hardware, software, configuration, and database vulnerabilities [36].
- **Management Vulnerabilities:** include lack of security guidelines, procedures and policies.

Vulnerabilities occur due to many reasons. However, there are three main causes of vulnerabilities:

- **Assumption and Isolation:** It is based on the "security by obscurity" trend in most CPS designs. Therefore, the focus here is

to design a reliable and safe system, taking into consideration the implementation of necessary security services, without assuming that systems are isolated from the outside world.

- **Increasing Connectivity:** More connectivity increases the attack surfaces. Since CPS systems are more connected nowadays, manufacturers have improved CPS through the implementation and usage of open networks and open wireless technologies. Most ICS attacks were based on internal attacks up until 2001. This was before utilizing the internet which shifted attacks to external ones [92].
- **Heterogeneity:** CPS systems include heterogeneous third party components which are integrated to build CPS applications. This has resulted in CPS becoming a multi-vendor system, where each product is prone to different security problems [93].
- **USB Usage:** this is a main cause of CPS vulnerabilities, such as the case of the Stuxnet attack that targeted Iranian power plants, since the malware is inside the USB. Upon plugging it, the malware spread across several devices through exploitation and replication.
- **Bad Practice:** is primarily related to a bad coding/weak skills that lead to the code to execute infinite loops, or to become too easy to be modified by a given attacker.
- **Spying:** CPS systems are also prone to spying/surveillance attacks, mainly by using spyware (malware) types that gain a stealthy access and remain undetected for years with the main task to eavesdrop, steal and gather sensitive/confidential data and information.
- **Homogeneity:** similar cyber-physical system types suffer from the same vulnerabilities, which once exploited, can affect all the devices within their vicinity, a prime example is the Stuxnet worm attack on Iranian nuclear power plants [94].
- **Suspicious Employees:** can intentionally or inadvertently damage or harm CPS devices, by sabotaging and modifying the coding language, or granting remote access to hackers through the opening of closed ports or plugging in an infected USB/device.

Thus, CPS vulnerabilities can be of three types, including cyber, physical, and when combined, they result into a cyber-physical threat.

3.2.1. Cyber vulnerabilities

Since ICS heavily relies on open standard protocols including Inter-Control Center Communications Protocol (ICCP) [95] and Transmission Control Protocol/Internet Protocol (TCP/IP) [96], ICS applications are prone to security attacks. In fact, ICCP suffers from a critical buffer overflow vulnerability [89] and also lacks the basic security measures [97]. In fact, the Remote Procedure Call (RPC) protocol [98] and ICSs are prone to various vulnerabilities including the Stuxnet (1 & 2) [99–101] and Duqu malware (1.0, 1.5 & 2.0) attack types [102–104], Gauss malware [102,105,106], and RED October malware [107,108], as well as Shamoon Malware (1, 2 & 3) [109–111], Mahdi malware [112–114], and Slammer Worm [115].

Open/Non-secure wired/wireless communications such as Ethernet are vulnerable to interception, sniffing, eavesdropping, wiretapping and wardialing and wardriving attacks [116–118] and meet-in-the-middle attacks [119]. Short-range wireless communications are also vulnerable, since they can be captured, analysed, damaged, deleted or even manipulated by insiders [120]. Moreover, employees' connected devices to ICS wireless network, if not secure, are prone to botnet, remote access Trojan and rootkit attacks, where their devices will be remotely controlled by an attacker [121]. Long-range wireless communications are vulnerable to eavesdropping, replay attacks, and unauthorized access attacks. Yet, SQL injection remains the most Web-related vulnerability since attackers can access any server database without authorization through the injection of a malicious code that keeps on running endlessly once executed without the user's knowledge [122].

Since many medical devices heavily rely on wireless communications, they are prone to a large number of wireless attacks including jamming, modification and replay attacks due to the lack of encryption. Moreover, GPS and the device's microphone are now becoming a tracking tool, allowing the identification of the target's location, or intercepting the in-car conversations through eavesdropping [13].

By default, ICS relies on Modbus and DNP3 protocols to monitor and send control commands to sensors and actuators. In [16], Humayed et al. stated that the Modbus protocol lacks basic security measures such as encryption, authentication and authorization. This has made it prone to eavesdropping, wiretapping, and portscan [123], with the risk of the controller being spoofed through false data injection [124]. The DNP3 protocol is also prone to the same vulnerabilities and attacks, with one main difference which is the integration of Cyclic Redundancy Check (CRC) as an integrity measure [125]. Moreover, Windows Server Services were vulnerable to remote code execution [99], with more attacks being achieved through the exploitation of buffer overflow vulnerabilities in any running Operating System (OS).

Moreover, power system infrastructure of smart grids is prone to the same vulnerabilities as ICS, Modbus and DNP3, since they are based on the same protocols. As a result, IEC 61850 protocol was introduced in substations' communications, which lack security properties and are prone to eavesdropping attacks. Therefore, leading to interference attacks [126], or false information injection attacks [127]. In [128], Santamarta et al. analysed the available documentation of smart meters, and located a "factory login" account used to perform basic configurations. This gives the user full control over a smart meter and leads to power disruption, wrong decision making and targeting neighbouring smart meters within the same network. In addition, many devices are prone to battery exhausting attacks [73].

Gollakota et al. [129] and Halperin et al. [130] exploited the Implantable Cardioverter Defibrillator (ICD) wireless vulnerabilities through injection attacks. The authors also showed that Smart cars are vulnerable to various attack types. In [131], Radcliffe, revealed another vulnerability with Continuous Glucose Monitoring (CGM) devices being vulnerable to replay attacks. The CGM device was spoofed with the injection of incorrect values. This is due to the fact that security considerations were not made when the smart cars were designed [132]. In fact, the Controller Area Network (CAN) protocol suffers from many vulnerabilities, which if exploited could result in attacks against smart cars. This will increase the likelihood of a DoS attack [133]. A Tire-Pressure Monitoring System (TPMS) is also vulnerable to eavesdropping and spoofing due to the lack of encryption [134]. In addition, Adaptive Cruise Control (ACC), which forms a part of the CAN network can be directly exploited [13]. In fact, a well-equipped attacker is able to interrupt ACC sensors' operations by adding noise or spoofing. Thus, controlling the car by either reducing, increasing its speed or even causing collisions.

3.2.2. Physical vulnerabilities

Physical tampering may result into misleading data in cyber-physical components. In fact, physical attacks with cyber impact were studied in MacDonald et al. [135]. The physical exposure of ICS components is classified as a vulnerability due to the insufficient physical security provided to these components. Thus, making them prone to physical tampering, alteration, modification or even sabotage. CPS field devices (i.e smart grids, power grids, supply chains etc.) are prone to the same ICS vulnerabilities since a large number of physical components is exposed without physi-

cal security, making them prone to physical destruction. Therefore, in Mo et al. [136], Mo et al. stressed on detection and prevention solutions. In [16], Humayed et al. stated that medical devices are vulnerable to physical access along with the possibility of installing malware into them, or even modifying the device's configurations, risking the patient's health. Moreover, a physical access to any medical device is also a vulnerability since an attacker can retrieve the device's serial number to launch targeted attacks [131].

As listed above, CPS systems suffer from various vulnerabilities making them prone to different types of attacks, which are discussed next.

3.3. Cyber-physical system attacks

In this section, we present the different types of attacks that target the different aspects of CPS systems, including cyber and physical ones:

3.3.1. Physical attacks

Physical attacks were more active in past years, especially against industrial CPS systems [137,138]. Many of these attacks were already presented in Al-Mhiqani et al. [139]. Nonetheless, this paper presents a broader range of physical attack types:

- **Infected Items:** this includes infected CDs, USBs, devices and drives such as the case of the Stuxnet worm [140], which upon their insertion into a cyber-physical device, a covert malware is installed containing a malicious software.
- **Abuse of Privilege:** this attack occurs when rogue or unsatisfied employees access the server rooms and installation areas within the CPS domain. This allows them to insert a rogue USB for infection through the installation of malicious malware/code or as keystroke, or to capture confidential data.
- **Wire Cuts/Taps/Dialing:** since communication lines including telephony and Wi-Fi of many cyber-physical headquarters (HQs) are still physically visible, attackers can cut the wires or wiretap into them to intercept the communicated data [117].
- **Fake Identity:** this attack occurs when attackers masquerade themselves as legitimate employees, with enough experience to fool the others. They mainly act as cleaners to gain an easier access and better interaction with other employees. A prime example of that is Australia's Maroochy Water Breach in 2000 [141].
- **Stalkers:** these are usually legal employees who act curious (with malicious intents) by being on the shoulder of CPS administrators and engineers to acquire their credentials to blackmail or sell them to other competing CPS organisations.
- **CCTV Camera Interception:** this includes intercepting the footage of Closed-circuit television cameras that are securing entry and key points within CPS areas. This can be done by distorting the signals of cameras, cutting off the communication wires, deleting the footage, gaining access to the remote control and monitoring area, etc., before performing a physical attack in an undetected manner.
- **Key-Card Hijacking:** this includes cloning legitimate cards that are stolen from employees, or creating look-alike genuine copies to gain full/partial access and to compromise the CPS domain.
- **Physical Breach:** this attack requires gaining an illegal physical access to the system, mainly through a physical breach such as the case of the Springfield Pumping Station in 2011 [142], a backdoor such as the case of US Georgia Water Treatment Plant in 2013 [143], or an exploited security gap such as the case of the Canadian Telvent Company in 2012 [144]. This allows an attacker to damage and shut-down network-connected manufacturing systems and CPS devices, resulting into loss of availability and productivity.
- **Malicious Third Party Software Provider:** the main purpose of this attack is to target the company's CPS by compromising the legitimate "Industrial Control Systems" software, such as the case of the Georgia Nuclear Power Plant Shutdown in 2008 [145]. This includes replacing legitimate files in their repositories with a malware that will be installed to offer remote access functionalities to control or compromise a given system.
- **Abuse of Privilege:** is mainly led by insiders or "whistleblowers" to perform or help perform a (cyber)-attack from within. Such high privilege grants them the ability to conduct these attacks by exposing valuable knowledge on CPS systems' vulnerabilities and weaknesses. This abuse of privilege can take many forms.
  - **Physical Tampering:** including gaining unauthorised or masqueraded authorised access to restricted areas to damage CPS systems, devices, modify their operational mode, inject malicious data/information or steal confidential documents.
  - **Unauthorised Activities:** are based on performing suspicious tasks, such as opening/closing pumping stations, increasing/decreasing power voltage, opening closed ports, communicating with an external entity, network traffic redirection or information leakage.
- **Social Engineering:** can take many deceptive forms [91] such as reverse engineering (impersonating a techy-savvy), baiting (selling malicious USBs or software), tailgating (following authorised personnel) or Quid Pro Quo (impersonating technical support teams), and is based on the art of manipulating people (either mentally or emotionally) to reveal confidential information by manipulating their emotions to gain their trust to reveal sensitive information related to a CPS, PLC or ICS system.

Recently, CPS systems became the new target of hackers for espionage, sabotage, warfare, terrorism, and service theft [146], mainly as part of cyber-warfare [147], cyber-crimes [148,149], (cyber)-terrorism [150–152], (cyber)-sabotage [153] (such as cyber-attacks against Estonia in 2007 [154], and Georgia in 2008 [155]), or (cyber)-espionage [156,157]. The lack of (cyber)-security revealed a serious issue with possibly drastic effects [12], especially in countries like Lebanon [158,159].

3.3.2. Cyber attacks

In recent years, there was a rise in the rate of cyber-attacks targeting CPS and IoCPT with very devastating consequences. According to current studies carried out by [160,161], CPS is highly prone to malicious code injection attacks [162] and code-reuse attacks [163], along with fake data injection attacks [164], zero-control data attacks [165], and finally Control-Flow Attestation (C-FLAT) attacks [160]. Such attacks can result into a total blackout targeting CPS industrial devices and systems as presented in Table 2.

- **Eavesdropping:** eavesdropping includes the interception of non-secure CPS network traffic to obtain sensitive information (passwords, usernames, or any other CPS information). Eavesdropping can take two main forms:**passive** by listening to CPS network message transmission, and **active** by probing, scanning or tampering the message by claiming to be a legitimate source.
- **Cross-Site Scripting:** or XSS occurs when third-party web resources are used to run malicious scripts in the targeted victim's web browser (mainly a targeted CPS engineer, contractor, workers, etc.) by injecting malicious Coding Script into a website's database. XSS can achieve session hijacking, and in some cases, can log key strokes along and remotely accesses a victim's machine.

Table 2
Real CPS attacks.

Country	Target	Attack Nature	Type	Date	Motives
United States of America	Ohio Nuke Plant Network [215]	Slammer Worm	Malware-DoS	January 25, 2003	Criminal
	Taum Sauk Hydroelectric Power Station Failure [216]	Sensors Failure	Accident	December 14, 2005	N/A
	Georgia Nuclear Power Plant Shutdown [145]	Installed Software Update	Undefined Software	March 7, 2008	Unclear
	US Electricity Grid [217]	Reconnaissance	Undefined Software Programs	April 8, 2009	Political
	Springfield Pumping Station [142]	Backdoor	Unauthorised Access	November 8, 2011	Criminal
	Georgia Water Treatment Plant [143]	Physical Breach	Unauthorised Access	April 26, 2013	Criminal
Iran	Iranian nuclear facilities	Stuxnet [218]	Worm	November, 2007	Political
	power plant and other industries	Stuxnet-2	worm	December 25, 2012	Political
	Iranian Infrastructure (nuclear,oil) and communications companies	DDoS	Disruptive	October 03, 2012	Political
	Iranian key oil facilities	Computer Virus	Malware	April 23, 2012	Political
Saudi Arabia	Saudi infrastructure in the energy industry	Shamoon-1	Malware	August 15–17, 2012	Religio-Political
	Saudi government computers and targets	Shamoon-2	Malware	November 17, 2016	Religio-Political
	Tasnee and other petrochemical firms, National Industrialization Company, Sadara Chemical Company	Shamoon-3	Malware	January 23, 2017	Religio-Political
Qatar	Qatar's RasGas	Shamoon	Malware	August 30, 2012	Political
United Arab Emirates	UAE energy sector	Trojan Laziok	Malware	January-February 2015	Political
Australia	Maroochy Water Breach [141]	Remote Access	Unauthorised Access	March, 2000	Criminal
Canada	Telvent Company [144]	Security Breach	Exploited Vulnerability	September 10, 2012	Criminal
Ukraine	Ukrainian Power-grids [219]	BlackEnergy Malware	DDoS	December 23, 2015	Political
	Ukramian Electricity Firms [220]	Petya [221]	Ransomware	June 27, 2017	Political

- **SQL Injection:** or SQLi targets CPS database-driven websites to read and/or modify sensitive data, along possibly executing administrative operations such as database shutdown, especially when CPS systems are still relying on SQL for data management [166].
- **Password Cracking:** aim to target the authenticity of CPS users [167,168] (mainly engineers and managers) by trying to crack their passwords using brute-force [169], dictionary [170] (mitigated by using key exchange [171]), rainbow table [172], birthday (mitigated by hashing) [173] or online/offline password guessing attacks [174] to gain access to the password database, or to the incoming/outgoing network traffic. Therefore, it is important to prevent such escalation from taking place [175,176].
- **Phishing:** has many types such as e-mail phishing, vishing, spear phishing or whaling that target some or all CPS users (such as engineers, specialists, businessmen, Chief Executive Officers (CEOs), Chief Operations Officers (COO), or/and Chief Financial Officers (CFO)), through impersonation of business colleagues or service providers.
- **Replay:** includes intercepting transmitted/received packets between ICSs, RTUs, and PLCs through impersonation to cause delays that affect CPS's real-time operations and affect their availability. In some cases, these intercepted packets can be modified, which would seriously hinder normal operations.
- **DoS/DDoS:** DoS attacks target the cyber-physical system resources and are launched from a large number of locally infected devices. DDoS attacks are usually exploited by Botnets, whereby a large number of infected devices simultaneously launch a DDoS attack from different geographical locations. DoS attacks can take many forms (i.e blackhole [177], teardrop [178]), while DDoS can take the following forms (i.e ping-of-death [179], smurf [180] and Black Energy series (BE-1, BE-2 and BE-3 [181–183]), all targeting CPS systems.
  - **TCP SYN Flood:** exploits the TCP handshake process by constantly sending requests without responding back to the server, causing the server to constantly allocate space awaiting a reply [184]. This leads to a buffer overflow and causes the cyber-physical system to crash.
- **Malicious Third Party:** includes software that covertly exploit data aggregation network and compromises them, mainly using botnets, Trojans or worms to infiltrate information through a CPS encrypted channel from an internal system (i.e PLC, ICS or RTU) through the reliance on Trusted Third Party in disguise, to a botnet Command-and-Control server. Thus, targeting CPSs [185] and AMIs [186].
- **Watering-hole Attack:** The attacker scans for any cyber-physical security weakness. Once a weakness is identified, the chosen CPS website will be manipulated by a "watering hole" where a malware will delivered by exploiting the targeted CPS system mainly through backdoor, rootkits or zero-day exploit [187].
- **Malware:** is used to compromise CPS devices in order to steal/leak data, harm devices or bypass access control systems. The malware can take many forms, however, the main forms that target CPS are briefly listed and presented in the following.
  - **Botnets:** this includes exploiting CPS devices vulnerabilities to turn them into bots or zombies, mainly to conduct hardly-traceable DDoS attacks (i.e Ramnit (2015) [188], Mirai (2016) [189], Smominru botnet (2017) [188], Mootbot (2020) [190], WildPressure and VictoryGate (2020).)
  - **Trojan:** is a disguised malware that seems legitimate and tricks users to download it. Upon download, the Trojan infects the device and offers a remote access to steal data credentials and monitor users activities. This also includes Remote Access Trojans which in turn, can be used to turn a device into a bot (i.e Turla (2008) [191], MiniPanzer/MegaPanzer (2009) [192], Gh0st RAT (2009) [193], Shylock (2011) [194], Coreflood (2011) [195], DarkCornet (2012) [196], MEMZ (2016) [197], TinyBanker (2016) [198] and Banking.BR Android Botnet (2020)).

  - **Virus:** it can replicate and spread to other devices through human/non-human intervention. Viruses spread by attaching themselves to other executable codes and programs to harm CPS devices and steal information.
  - **Worms:** spread by exploiting operating system vulnerabilities to harm host networks by carrying payloads to steal, modify and delete data, or overload to web-servers (aside Stuxnet, Flame and Duqu, i.e aCode Red/Code Red II (2001) [199], Nimda (2001) [200], Triton (2017 [201])).
  - **Rootkit:** is designed to remotely and covertly access or control a computer to execute files, access/steal information or modify system configurations (i.e Moonlight Maze (1999) [202], and Blackhole exploit kit (2012) [203]).
  - **Polymorphic Malware:** constantly and frequently changes its identifiable to evade being detected to become unrecognizable against any pattern-matching detection technique.
  - **Spyware:** is a malicious software covertly installed on a device without the user or authorization knowledge, for spying purposes (e.g surveillance, reconnaissance, or scanning). In fact, they can be used for future cyber-attack purposes (i.e ProjectSauron (2011) [204], Dark Caracal (2012) [205], Red October (2013) [107], WarriorPride (2014) [206], FinFisher (2014) [207], and COVID-19 spyware.)
  - **Ransomware:** is a malicious software that holds and encrypts CPS data as a ransom by exploiting CPS vulnerabilities, targeting oil refineries, power grids [208], manufacturing facilities, medical centers and encrypting all data-backups until a ransom has been paid. A prime example of that is the Siskey (2016), SamSam (2016), Locky (2016), Jigsaw (2016) [209], Hitler-Ransomware (2016) [210], WannaCry (2017), Petya (2017), Bad-Rabbit (2017), Maze (2019) and Ekans (2020) ransomware [211–214].
- **Side-Channel:** is based on the information gained from the implemented CPS system such as timing information, power consumption and electromagnetic leaks that can be exploited.

For this reason, some of the most infamous cyber-attacks deserve being mentioned (Table 2). Moreover, for further details, you can refer to [139]. In fact, Do et al. presented a much more detailed attack description as early as 1980s in Fillatre et al. [142]. However, this paper aims to classify the occurrence of these attacks as early as 2000 and based on, but not limited to, political, religious, and criminal motives.

After reviewing the main CPS attacks, it is essential to assess their associated risks to design the convenient counter-measures. In the next section, the risks associated with the different CPS security attacks are evaluated.

3.4. CPS failures

Given the different threats, attacks and vulnerabilities that the CPS domain suffers from, it is important to highlight the main failures than CPs systems suffer from. These failures can either be minor (limited damage) or major (severe damage). In fact, further details can be found in Avizienis et al. [222], where Avizienis et al. presented a well-defined and detailed explanation in this regards.

- **Content Failure:** means that the content of the delivered information is inaccurate, which would result into some functional system failure. Content failure can be either numerical or non-numerical (i.e alphabets, graphics, sounds or colours).
- **Timing Failure:** means that the timing of information delivery (transmission/receiving) is delayed or interrupted (received/transmitted too early or too late). This would affect the decision making process and may cause data management issues.
- **Sensors Failure:** means that the sensors are no longer functioning properly, and would seriously hinder the decision making process due to misinformation, or bringing a CPS system to a sudden halt. A similar case occurred in 2005, at Taum Sauk Hydroelectric Power Station [216].
- **Silent Failure:** occurs when there is no message sent or received in a distributed system.
- **Babbling Failure:** occurs when the information is delivered, causing the system to malfunction and to operate in a babbling manner.
- **Budget Failure:** occurs when the cost of implementing a cyber-physical system outweighs the budget set, before ever reaching the testing level. This is mainly caused by poor planning.
- **Schedule Failure:** occurs when the schedule set for planning, testing and evaluating a given CPS is not achieved due to further upgrades, additional testing, or inadequacy for users needs.
- **Service Failure:** occurs when having an error propagates through the service interface and affects its decision making or/and normal performance ability. This failure can either cause a partial or full CPS system failure either temporarily or permanently.
- **Consistent/Inconsistent Failures:** a consistent failure occurs when a given service is identically perceived by all CPS users. An inconsistent failure takes place when all CPS users differently perceive an incorrect service (i.e bohrbugs, mandelbugs, heisenbugs and Byzantine failures) [223].

4. Evaluating risks

Evaluating risks is essential to assess the risk's economic impact of an attack on any CPS system, before managing it. Such management is based on assessing and analysing the risk before mitigating it, then deploying the right security measures according to the level of severity and risk impact (see Fig. 4).

4.1. Risk identification & management

Risk Management is implemented in order to identify, analyse, rank, evaluate, plan and monitor any possible risk through risk assessment.

- **Identifying Risks:** identification is based on uncovering and recognising risks that can negatively affect a project/project outcome and describing it [224].
- **Analysing Risks:** risks likelihood and consequence must be determined once they are identified, to understand the nature of a risk.
- **Ranking Risks:** risks rank is evaluated according to the risk magnitude, based on the combination of both risk likelihood and consequence in case it occurred.
- **Evaluating Risks:** based on their ranks, risks are either deemed as acceptable or require serious treatment and urgent attention.
- **Planning Risks Response:** highest ranked risks are assessed to treat, modify and mitigate them to once again achieve an acceptable risk level. Therefore, risk mitigation strategies are created, along with the deployment of preventive and contingency plans.
- **Monitoring and Reviewing Risks:** risks are constantly monitored, tracked and reviewed. In case of any suspicious activity, these risks are mitigated before any serious threat occurs.

4.2. Risk assessment

Risk Assessment is implemented to minimize the impact of a given attack [225]. In fact, risks are evaluated based on calculating the average loss in each occurring event [226]. Additionally,

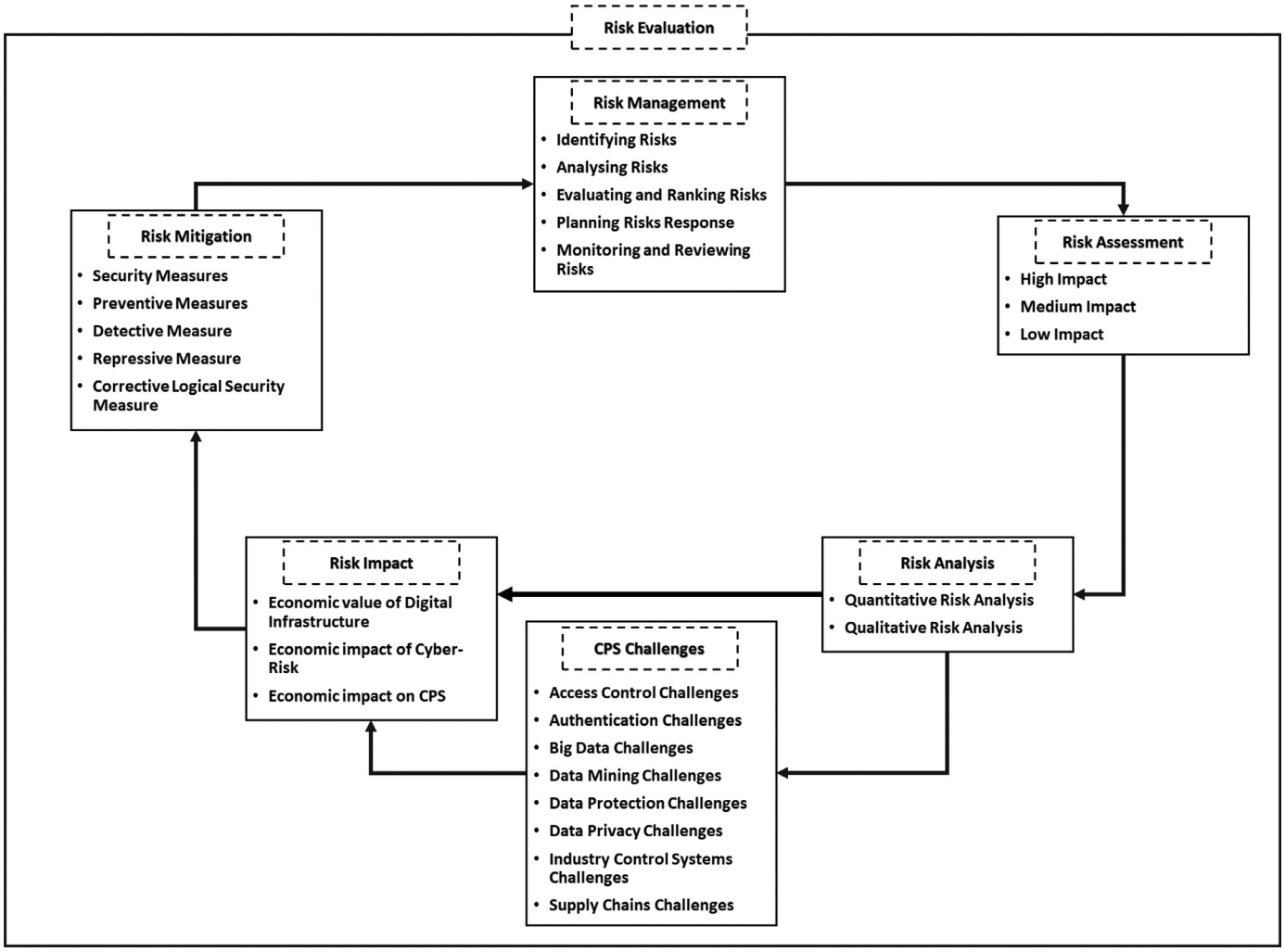


Fig. 4. CPS risk evaluation.

several risk assessment methods, as well as various techniques to secure CPS were revealed in Ashibani and Mahmoud [25]. In fact, since most studies are focused on securing enterprise systems in order to assess risks, security became an emerging issue that imposes a serious risk on CPS [227]. As a result in Lu et al. [228,229], Lu et al. presented an adequate risk assessment method. The main security focus was based on transferring it from risk assessment, to Computer Risk Assessment (CRA), to Network Risk Assessment (NRA) with a heavy reliance on the internet [230]. **Asset Identification:** is also important, since it is a resource value that can either be tangible, or intangible that impacts daily transactions and services [231]. In fact, CPS assets can be divided between cyber assets, physical assets, and cyber-physical assets. Finally, since asset quantization is estimated from both direct and indirect economic losses [232], it is important to determine the Asset Value (AV).

4.3. Risk impact

Risk is assessed based on its possible impact on CPS systems. It is divided into three main types:

- **High Impact:** in case the risk has occurred, this can result in devastating and damaging effects on CPS systems. It is used to evaluate and mitigate persistent advanced threats [233].
- **Medium Impact:** in case of its occurrence, the impact is less severe. However, it also imposes a serious threat against CPS. It is used to evaluate and mitigate advanced threats [234].
- **Low Impact:** in case this risk has occurred, its impact is not severe, nor has damaging effects. As a result, its impact is very limited and can be easily mitigated. It is used to evaluate and mitigate basic threats [235].

4.4. Risk mitigation

Risk mitigation requires the adaptation and implementation of a well-built management strategy in addition to cyber and physical security in order to counter-espionage, theft, or/and terrorist attacks. Such a mitigation model also requires, data security and protection, as well as anti-counterfeit and supply chain risk management [236]. These models should also be supported by both forensic and recovery plans. This can help in analyzing cyber-attacks whilst coordinating and cooperating with the responsible agencies to identify external cyber-attack vectors [237]. Therefore, preventive, detective, repressive and corrective logical security measures can be adopted.

As a result, a qualitative risk assessment table is presented (see Table 3) where the exposure is either Low (L), Moderate (M) or High (H), the risk level is either Major (Ma), Minor (Mi) or Critical (Cr), and the security measures are Detective (D), Repressive (R), Preventive (P) and Corrective (C), respectively.

Table 3
Qualitative CPS risk assessment.

Attack		System/Data Exposure		Evaluation	Risk Mitigation		Targeted Security Goals			
Type	Impact	Protected	Unprotected	Risk Level	Security Measures	Countermeasures	Confident-iality	Integrity	Availability	Authent-ication
Malware	High	L/M/H	H	Ma/Cr	D, P, C & R	IDS, Firewalls, Anti-Malware, Anti-Virus	✓	✓	X	✓
Spyware	Moderate	M	H	Ma/Mi	D, P & R	Anti-Spyware, Defence in Depth	✓	X	X	X
Ransomware	High	M/H	H	Ma/Cr	D, R & C	Honeypot, Verified Backup/Update, Lesson Learnt	✓	✓	✓	✓
Botnets	High	M/L	H	Ma	D, C & P	IDS, Anti-Malware	✓	✓	✓	X
DoS/DDoS	High	H	H	Ma/Mi	D, P & R	Backups, Secondary Devices, IDS, Leverage to Clouds	X	X	✓	X
Eavesdrop	Low	L	H	Mi	D & P	HTTPS/SSH Encryption, Personal Firewalls, VPNs [238]	✓	X	X	X
Side-Channel	Moderate	M/L	H	Ma	D, P & R	Ultra-Low Power Processors, Faraday Cage, Obfuscating Timing/Power Information [239]	✓	X	X	X
Zero-Day	High	H	H	Cr	D, C & R	Real-Time Threat Intelligence, Rapid Incident Response Teams, Constant Updates	✓	✓	✓	✓
Malicious Data Injection	Moderate	L	H	Ma	D, P & C	Hybrid IDS, ML, BYOD Policy [240]	✓	✓	X	X
Social Engineering	Low	L	M/H	Mi	D & P	Employee Training & Awareness	✓	✓	X	X
Phishing	Moderate	L	H	Ma	D & P	IDS, Anti-Phshing Software/Training	✓	✓	X	X
Password Cracking	Moderate	L	M	Ma	P & C	Password Policy, Periodic Password Changing	✓	✓	X	✓
Replay	Low	L	M	Mi	D & P	Timestamp, Filtering, Random Session Keying	X	X	✓	X
XSS	High	L	H	Cr	D & P	Validate & Sanitize User Input	✓	✓	X	✓
SQLi	Moderate	L	H	Ma/Mi	D, C & P	Least Privilege, Strong Code, Whitelisting	✓	✓	✓	X

4.4.1. Attack cost & impact

The cost of security attacks can take many forms, and the main ones are highlighted as follows:

- **Delays:** CPS systems may be prone to service delays, which may affect their performance and render them inactive (blackout, burnout) until the issue is sorted either through maintenance or back up.
- **Affected Performance:** system delays due to a malicious (cyber-attack)/non-malicious (accident) event can gradually affect the CPS performance and cause it to operate in an abnormal manner which can seriously affect the decision making process.
- **Cascading Failures:** such as sensor failures, software bugs or nuclear power plant overheating, which can cause environmental catastrophes such as the case of Chernobyl (1986) and Fukushima (2011), natural gas pipeline explosion in Belgium (2004), series of TransCanada Corporation's natural gas leakage and explosion in Canada (between 2000 and 2018) [241] as well as similar incidents in the US [242], Mexico, China and other countries, oil spilling, water pipeline incidents, flooding, blackouts, and so on.
- **Financial Losses:** malware attacks such as ransomware (i.e Ekans snake malware) targeting Industrial Control Systems (ICMs) can lead to huge loss of information beyond recovery if the backup is not maintained, or if the ransom is not paid. This leads to huge financial losses over short and long terms especially if the information is deleted beyond recovery. CPS systems might take months and even years to recover.
- **Additional Spending:** may be required to tackle the advanced persistent threat attempts and zero-day attacks, which require additional spending in terms of security protection in a defense-in-depth manner.
- **Loss of Life:** can be the result of flooding, radioactivity, fire or electric shock due to hazardous or intentional acts.
- **Disclosure of Information:** can affect CPS businesses and business trades and put the privacy of users at risk of having their personal information being exposed.

Before proceeding any further, it is important to classify CPS components as critical, moderate and non-critical, to identify the risk of an event occurrence (malicious/hazard) along its impact to define the proper security measures (basic, standard or advanced), as seen in Fig. 5.

While adopting all possible security measures might be costly in all terms (i.e. complexity, financial cost, delay, etc.), risk management is key for selecting the convenient security solutions. In the next section, the different security solutions proposed to defend the security issues are reviewed. While these security solutions aim at preventing, detecting or correcting system damage, the CPS forensics aim at knowing the system issues causes, which help in reducing and preventing future attacks. Thus, the main CPS forensics solutions are also reviewed.

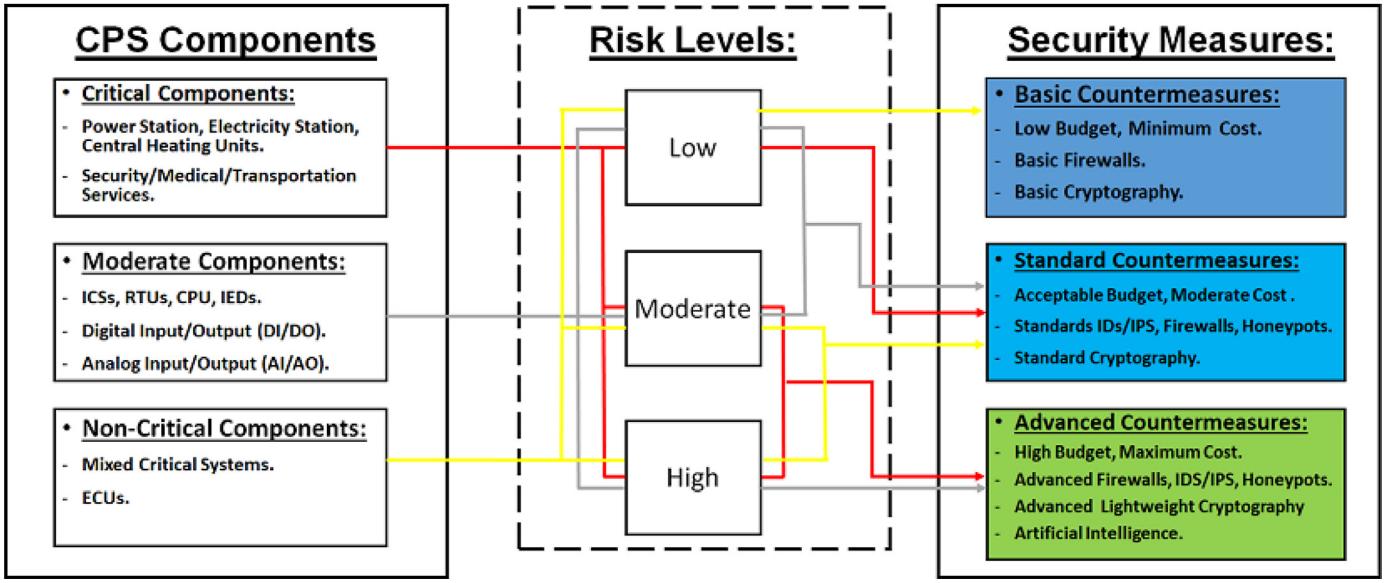


Fig. 5. CPS component classification & protection.

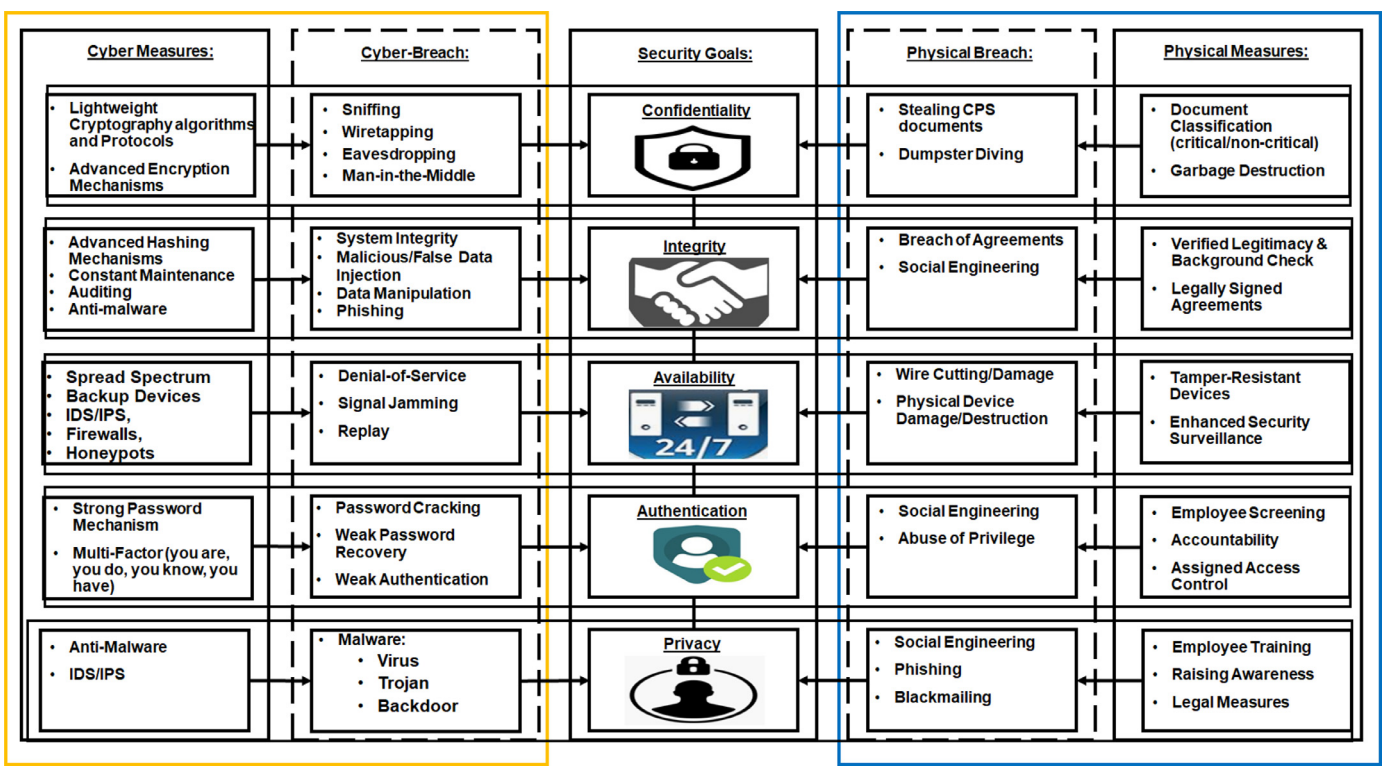


Fig. 6. Targeting CPS security goals.

5. Securing CPS

Securing CPS is not a straightforward task. For this reason, various existing solutions are mentioned and discussed in this section. Already existing testing tools are also introduced. All of these schemes are presented to protect CPS domains against attacks that target the confidentiality, integrity, availability, authentication and privacy of both data and systems as seen in Fig. 6.

5.1. CPS security requirements

According to National Institute of Standards and Technology (NIST) guidelines [243,244], ensuring trust between IoT and CPS, should consist of various multi-factors. This is due to both IoT and CPS systems relying on safety, security, privacy, consistency, dependability, resiliency, reliability, interaction and coordination, all of which are combined to form a well-designed and trustworthy system. If this condition is satisfied, a perfect CPS mechanism is

Table 4
CPS testing tools.

Tools	Origins	Nature	Description
Achilles	[246]	uniquely designed for embedded and industrial control devices	uses Wurldtech proprietary fuzzing algorithms to generate tests of known and unknown vulnerabilities, provides the analysis of the attack impact, monitors the whole system
BreakingPoint	[247]	designed as the industry's first cyber tomography machine	a 4 RU rack-mountable, modular system that accurately recreates a live network environment and identifies network devices "Breaking-Points". It measures and hardens the resiliency of CI component against crippling attacks
beSTORM	[248]	automated tool	programmed to make an excessive search of all possible input combinations, tests any product for potential weaknesses
Codenomicon Defensics	[249]	a specialized fuzzing tool which supports the security of industrial protocols	sends to the system invalid or unexpected inputs that expose software defects and vulnerabilities, ensures a broader test coverage, can be used to test digital media, wireless infrastructures and network protocols. Easy integration. Proactive testing. Integrated online documentation
Mu-8000	[250]	Mu Studio Security, built on a powerful automation platform that provides extensive automation, monitors hardware/software-based restarters, and reports capabilities	consists of four types of tests, Protocol Mutation Tests including DNP3, IEC 61850, MMS, and MODBUS/TCP industrial protocols, generates test cases packets containing protocol mutations secure targets handles them successfully, non-secure targets might respond abnormally
Peach	[251]	Smart Fuzzing tool that performs generation and mutation based fuzzing	requires the creation of PeachPit files to define the structure and type of information in the to be fuzzed data, allows the configuration of a fuzzing run including data transport and interface logging
Sully	[252]	is a fuzzer development and fuzz testing framework	It consists of multiple extensible components, it also supports ICCP, modbus and DNP3 fuzzing modules
SPIKE	[253]	designed to focus on finding exploitable bugs	It is a fuzzer creation kit, it provides an API to allow users to create their own fuzzer for network based protocols, allows the use of the C programming language

Table 5
CPS security certifications.

CPS security certifications		
Certification name	Levels	Description
WST Achilles Certification [246]	1	includes basic testing Layer 2–4 Industrial Protocols
	2	includes in-depth testing Layer 2–4 Industrial Protocols
Exida Certification [254]	N/A	includes three main types which are functional safety, functional integrity, and cyber security
ISASecure EDSA Certification [255]	N/A	consists of Functional security assessment (FSA), Software development security assessment (SDSA), and Communication robustness testing (CRT)
MuDynamics MUSIC Certification [250]	Foundation	includes various protocols such as ARP, IPv4, TCP, UDP, and IEEE 802.lp/Q
	Advanced	includes various protocols such as DNP3, FTP, HTTP, MODBUS/TCP, and Telnet

achieved. As a result, several CPS testing tools were used to evaluate the security of Industrial Control devices upon their development (see Table 4). For further details, these tools are explained in Zhao et al. [245]. Moreover, several security certifications are also discussed, reviewed, analysed and compared according to their different aspects [245] (see Table 5).

In the following, the main CPS security requirements are defined and discussed.

- **Privacy:** In CPS, a huge data collection process is constantly taking place, and this is what most people are not aware of [256,257]. Therefore, a person has the right to access his own data, along with being given the right to know what type of data is being collected about them by data collectors, and to whom these data is being given or sold to. However, this also requires preventing the illegal/unauthorised access to the user's personal data and their information disclosure [258,259].
- **Dependability:** Intelligent Physical World (IPW) ensures that the CPS adaptive behaviour is achieved to bring a higher dependability and ensure the right Quality of Service (QoS) through the adoption of fault-tolerance mechanisms in a timely manner. Dependability includes two other qualities, safety and reliability. Safety is often an objective defined in terms of the organisation's goals [243]. This is due to the negative impact of cyber-security risks, where vulnerabilities can be compromised and exploited by a hacker, or due to CPS failure. Hence, safety is of a high concern for IoT, CPS and (Internet of Cyber-Physical Things) IoCPT users alike. While reliability is based on the ability to adapt to changing conditions to overcome and recover from any possible disruption either based on cyber or/and physical attacks led by adversaries, in addition to natural disasters [243].
  Physical systems rely on timing and proper functionality. However, in case of any possible mismatch, unreliability and uncertainty can cause problems and disruptions for CPS services. Therefore, maintaining a high reliability requires reducing the uncertainty levels. In fact, it is also recommended to implement error-correction algorithms to sort electronic components imperfect reliability [260]. As a result, Rajamäki et al. [260] stated that CPS behaviour can be predictable through the implementation and use of artificial intelligence or/and even Machine Learning (ML) schemes. This allows the prediction of the so called "next-time system state".
- **Resiliency:** CPS must be resilient to overcome accidents and malicious attacks. Therefore, CPS logical and physical systems are prone to cyber security vulnerabilities from a security aspect. This included the demonstration of Carshark software tools that control a car in Koscher et al. [133], along with the successful design of a virus in 2010 which attacked Siemens plant-control systems [261], along with how hackers broke into

the United States Federal Aviation Administration (US FAA) air traffic control system in 2009 [262]. Resiliency is achieved by each CPS component in a Base Architecture (BA) presented in Rajhans et al. [263], where each communication and physical connection path between elements is granted access by the BA's connectors. This requires the BA system to know and identify every possible path, while overcoming any connection disruption. Moreover, in case the elements were inconsistent, a multi-view editor will be deployed to make corrections.

- **Interaction and Coordination:** are essential to maintain an all-time operational CPS security. In [58], Hu et al. stated that CPS interaction and coordination between cyber and physical system elements are a key aspect. In fact, the main physical world characteristics are based on the constant system change over time. However, the cyber world characteristics are based on sequence series with no temporal semantics. Moreover, two basic approaches are presented to study and analyse this problem. These approaches are based on the "cyberizing" the physical (CtP) aspect through the introduction of cyber-properties and interfaces into physical systems, and "physicalizing" the cyber (PtC) where cyber-software components are to be represented in real-time [264].
- **Operational Security (OpSec):** Operational Security (OpSec) was introduced in 1988 to ensure physical security, information security, and personnel security [265] through careful planning, risk assessment and risk management [266]. Its primary task is to ensure operational effectiveness by denying any adversary access to public/private information; hence controlling information and observable actions about a given cyber-physical system, especially in hostile environments/areas [265]. One of its key benefits is providing means to develop cost-effective security measures to overcome a given threat. To achieve this task, OPSEC involves five main steps:
  - **Critical Information Identification:** includes identifying which information, if targeted, can effectively degrade a CPS's operational effectiveness or place its potential organizational success at risk, and develop an initial plan to protect it.
  - **Threat Analysis:** includes determining an adversary's potential and capabilities to gather, process, analyze, and use the needed information.
  - **Vulnerability Analysis:** includes studying the weaknesses of a given cyber-physical system and the strengths of an adversary. Thus, building a possible view over how a potential adversary might exploit this security gap to perform a security breach.
  - **Risk Assessment:** risks are assessed based on the threat and vulnerability levels combined, depending on how high or how low these levels are. Risk assessment levels include evaluating the cost of implementing the right security measures by ensuring a trade-off between the effective cost and benefit balance.
  - **Appropriate Application Countermeasures:** once the trade-off is achieved in the earlier phase, the appropriate countermeasures are then developed to offer the best protection of CPS against these ongoing threats in terms of feasibility, cost, and effectiveness.
- **System Hardening:** System hardening can be used to defend a wider range of threats. Therefore, it is highly recommended to isolate critical applications that lack the proper security measures, from any OS that is not trusted in order to boost the IoCPT and CPT security. In [267], Shepherd et al. analysed different trust-computing technologies along with their applications in the CPS domain. According to [268], such analysis included a Trusted Platform Module (TPM), Trusted Execution Environments (TEE), Secure Elements (SE), and Encrypted Execution Environment (E3), to increase the OS's integrity. Moreover, the authors' work in Almohri et al. [269] has successfully achieved a higher security level in the presence of untrustworthy components. This allowed the improvement of CPS by enhancing system's integrity. However, if the Graph-based optimization was combined with parameters, it can provide a reasoning basis to ensure an overall system integrity [270]. Therefore, it is essential to set the right privileges (task-based, role-based, rule-based, etc..) and strong password complexity policies in order to enhance the security level. Moreover, this also includes getting rid of old unused accounts and open yet unused ports to reduce the exposure to remote wireless attacks. As a result, CPS nature must be considered before achieving any design. In [136], Mo et al. presented a Cyber-Physical security by combining systems-theoretic with Cyber-Physical security controls.

5.2. CPS security challenges

The adoption of security measures has many benefits when it comes to protecting CPS components, layers and domains. However, despite these advantages, CPS systems are impacted by the application of these security measures, which can be summarized as follows:

- **Reduced Performance:** security measures can partially or fully affect the performance of a given CPS, in the absence of careful consideration for a balanced security-performance trade-off. This can affect normal operations and requires more human interventions to manually assign services and domains.
- **Higher Power Consumption:** is a serious issue, especially for resource-constrained and battery-limited CPS end devices. A higher power consumption means a shorter lifespan and a higher cost to maintain their availability.
- **Transmission Delays:** transmitted/received data is prone to delays due to the additional encryption process that is being added to thwart passive/active eavesdropping and sniffing attacks. Despite the protective advantage that is offers, this is unacceptable in a real-time CPS systems.
- **Higher Cost:** higher security levels are associated with higher computational costs, which are not limited to the initial capital spending phase, but also include training, update, and operational phases.
- **Compatibility Issues:** some CPS systems are not compatible with the employed security measures and vice versa. This can be due to the software in-use, firmware, Operating System, etc.
- **Operational Security Delays:** upon the deployment of any security service, there is a training phase that precedes the full operational security mode, and during which the service is temporarily ineffective or basic and thus, prone to attacks.

5.3. CPS security solutions

Maintaining a secure CPS environment is not an easy task due to the constant increase of challenges, integration issues and limitation of the existing solutions including the lack of security, privacy and accuracy. Nonetheless, this can be mitigated through different means including cryptographic and non-cryptographic solutions as seen in Fig. 7.

5.3.1. CPS criticality

CPS systems can be divided into four main types based on the aspect of their criticality:

- **Safety Critical:** in such a CPS type, an attack can lead to loss of life or to chronic deadly diseases, with significant damage to the environment such as fire, floods, radioactivity (e.g. Chernobyl in 1986 and Fukushima in 2011) incidents [271,272].

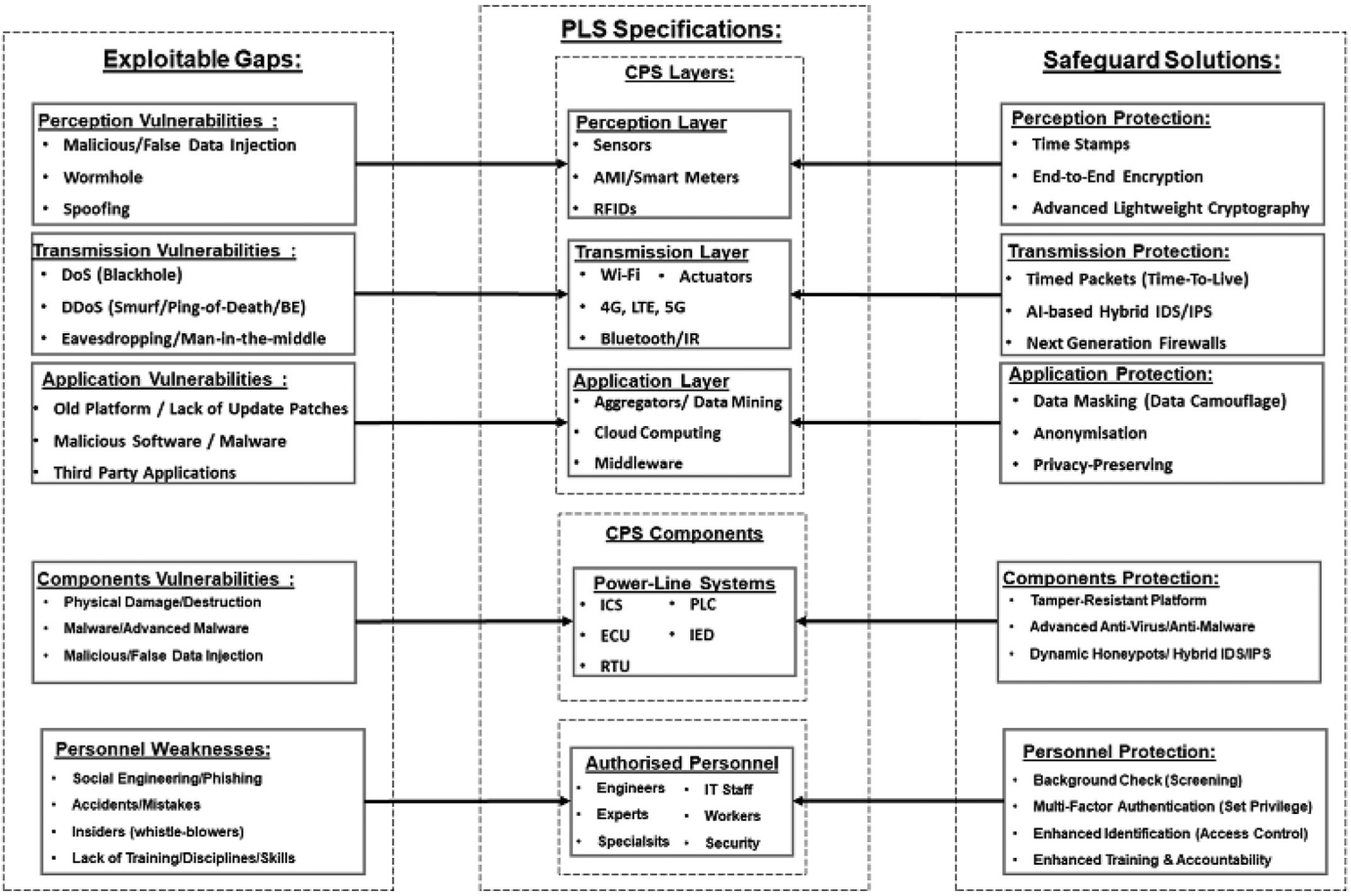


Fig. 7. Protecting CPS layers, components & personnel.

- **Mission Critical:** for this type of CPS, an attack can result into a fatal/non-fatal, total/partial failure of a CPS to achieve its objectives [273].
- **Business Critical:** in such a CPS type, an attack can result into huge financial and economic losses, damaged reputation and loss of CPS contractors and clients.
- **Security Critical:** for this type of CPS, an attack can result into a security breach of the cyber-physical system (security gap, exploitable vulnerability, rootkits, backdoors, etc.).

5.3.2. Cryptographic-based solutions

Cryptographic measures are mainly employed to secure the communication channel from active/passive attacks, along any unauthorized access and interception, especially in SCADA systems [274]. In fact, traditional cryptography approaches based on utilizing ciphers and hash function are not easily applied to CPS including IoCPT due to power and size constraints. As a result, the main focus should be limited to data security alone, instead it should maintain and ensure the efficiency of the overall system process along. Therefore, various solutions were presented. In [23] Kocabas et al. conducted their own survey which was dedicated to conventional and emerging encryption schemes which could be employed to offer secure data storage and sharing. In [24], Lai et al. reviewed and discussed prominent cryptographic authentication and encryption methods [275] to secure Distributed Energy Resources (DER) systems, while providing recommendations on applying cryptography to DER systems. In [276], Ding et al. presented an overview of recent advances on security control and attack detection of industrial CPS, especially against denial-of-service, replay, and deception attacks. In [15], Sklavos et al. presented a tutorial that discusses the implementation efficiency of communications confidentiality, user authentication, data integrity and services availability, along attacks and modern threats with their countermeasures.

Many solutions were presented to maintain a secure CPS environment by fulfilling its main security goals. In [277], Adam et. al. presented a novel framework to understand cyber-attacks and CPS risks. Their framework offers a novel approach to ensure a comprehensive study of CPS attack elements, including the attacker and his objectives, cyber exploitation, control-theoretic and physical system properties. In [232], Stouffer et al. provided a comprehensive ICS security guideline that is related to technical controls including Intrusion Detection Systems (IDS), Access Controls (AC), firewalls, and operational controls including training, awareness and personnel security. In [97], security experts were able to gain the employees' credentials due to their lack of awareness and training, using phishing and social engineering techniques through a simulated attack. In [34], Sommestad et al. conducted a keyword mining comparison, and concluded that the main focus was either on operational controls, or technical controls only. In [278], Sharma et al. presented a novel multi-level Network Security Evaluation Scheme (NSES) that represent five different levels of security. Therefore, providing a holistic view over whether NSES is suitable for Wireless Sensor Networks (WSN) security for IoT/CPS/IoCPT applications. NSES offers recommendation for network administrators on early design phases to achieve the right security needs. As a result, this paper classifies these solutions in terms of them fulfilling one of the following security goals:

- **Confidentiality:** securing CPS communication lines is essential. As a result, various cryptographic solutions were presented. In [279], the authors presented a solution based on the use

of compression techniques before being encrypted. Their solution reduces the overhead and mitigates the problem. Since, lightweight cryptography became the centre of attention with various lightweight block ciphers being presented by different authors, including an ultra-lightweight block cipher by Bogdanov et al. [280] and a low-latency block cipher for pervasive computing applications [281]. This was due to their low-cost and low-latency with the ability to provide cryptographic blocks for any resource constrained, normal, industrial, or even medical devices. In [282], Shahzad, et al. suggested the installation of encryption-decryption modules at both ends of non-secure Modbus communication to protect its connection from confidentiality attacks. Thus, requiring an additional overhead to convert plaintexts into ciphertexts and vice versa. In [283], The American Gas Association (AGA) presented its AGA-12 standard to provide "bump-in-the-wire" encryption services for CPS, but at the expense of large latency overheard [284]. In [285], Vegh et al. described a hierarchical cryptosystem method obtained through the ElGamal algorithm that protects CPS communications. To fix decryption issues, WSO2 Complex Event Processor (WSO2-CEP) was presented in Jayasekara et al. [286], Perera et al. [287] and used in to sort different challenges. Results ensure the ability to ensure confidentiality, privacy and availability in a secure and reliable CPS environment.

In [288], Zhou et al. presented a novel lightweight encryption scheme for real-time requirement in CPS including Vehicular ad hoc networks (VANETs) [289,290]. Results revealed that this scheme is secure, reliable and efficient. In [291], He et al. presented a Lightweight Attribute Based Encryption Scheme (LABE) for mobile cloud-assisted CPS. Security analysis revealed that LABE is secure with fine grained access control and users revocation capability, with low overhead. In [292], Zhao et al. presented a new architecture called Secure Pub-Sub (SPS) that is based on blockchain. Hybrid encryption was used to ensure data confidentiality. Therefore, ensuring data confidentiality and reliability, while achieving anonymity of subscribers and payment fairness between subscribers and publishers. In [293], Sepulveda et al. presented a feasible post-quantum enhanced Datagram Transport Layer security (DTLS) by using Public Key Cryptography (PKC) based on traditional Elliptic-Curves (ECC) to secure communication channels between different parties.

- **Integrity:** maintaining the integrity of CPS devices require preventing any physical or logical modification of incoming/outgoing real-time data. Hence, different solutions are presented. In [294], Omkar et. al. addressed the problems of software reconfiguration and network attacks on ICS through the description of their presented approach called Trustworthy Autonomic Interface Guardian Architecture (TAIGA). TAIGA offers protection against the attacks that originate from both supervisory and plant control nodes, whilst integrating a trusted safety-preserving backup controller. In [295], Tiago et al. introduced the Shadow Security Unit "SSU" as a low-cost device used in parallel with a PLC or Remote Terminal Unit (RTU) to secure SCADA systems [296].

  SSU is complementary to the existing SIEM architectures, and it can transparently intercept its communication control channels along with its physical process Input/Output lines to constantly assess both security and operational status of PLC or RTU. Another approach was also presented in Ghaleb et al. [297], by Asem et. al to overcome MITM, replay and command modification attacks by providing an encryption level for the transferred packets, along with the use of hardware cipher models. In [298], Cao et al. presented a layered approach with the aim of protecting sensitive data. Their techniques relied on hash chains that provide a layered protection for both high and low security levels zones along with a lightweight key management mechanism. Thus, preventing attackers from intercepting data from a higher security level zone. Therefore, ICS applications vendors should work on releasing compatible versions of their applications to ensure that the ICS operators will not resort to older versions of vulnerable OS [22].
- **Availability:** maintaining the availability of CPS devices is a must. Hence, different solutions are presented to mitigate and overcome availability issues. For this reason, the Tennessee-Eastman Process Control System (TE-PCS) model is used to test integrity and DoS attacks [299]. Upon testing, this model reveals how DoS attacks are ineffective against sensor networks. Thus, requesting to prioritize security defences against integrity attacks due to their effectiveness to overcome DoS attacks only [300]. In [39], Gao et al. designed and presented the network ICS testbed based on Emulation, Physical, and Simulation (EPS-ICS testbed) as a control process for corporate and SCADA network emulations through the use of PLCs, RTUs, and DCS controllers to interact with the process. In [301], Thiago et. al. combined an open source PLC with a machine learning-based IPS design to secure the OpenPLC version and render it immune against a wide range of attacks. Their presented approach revealed the ineffectiveness of interception, injection and denial of service attacks, along with the ability of their OpenPLC project to overcome man-in-the-middle attacks through data encryption, without interfering with its own real-time characteristics.
- **Authentication:** authentication is the first line of defense that should be well-built, designed and maintained [259,302–304]. As a result, in Halperin et al. [130], Halperin et al. presented a public key-exchange authentication mechanism to prevent unauthorized parties from gaining access. Their mechanism relies on external radio frequency rather than batteries as an energy source. In fact, out-of-band authentication were deployed in certain wearable devices, where the authentication mechanism uses additional channels including audio and visual channels [73]. On the other hand, Medical CPS (MCPS) biometrics, including mainly heart rates and blood pressure [305], can possibly be used to generate a key to encrypt and secure the body sensor network communication [73]. In [306], Ankarali et al. presented a physical layer authentication technique which relies on pre-equalization. In [307], Ibrokhimov et al. presented a five high-level features categories of user authentication in the gadget-free world, including security, privacy, and usability aspects.

  In [308], Chen et al. presented an authentication scheme that applies Authenticated Identity-Based Cryptography Without Key-Escrow (AIBCwKE) mechanism to protect user's privacy and property from illegal attacks on Machine-to-Machine (M2M) communications. Making it secure and suitable for safe sessions between mobile devices with an acceptable overhead. In [309], Haroon et. al. detailed how recent versions of PLCs (2016) are prone to various vulnerabilities, especially password-based mechanisms. The authors revealed that passwords stored in a PLC memory can be intercepted and cracked. Thus, allowing them to carry out advanced attacks including replay attacks and memory corruption attacks. In [310], Choi et al. presented an ICS-specific key management solution with no delays.
- **Privacy Preserving** Preserving the privacy of users' big data is not an easy task. As a result, various privacy preserving techniques were presented to solve this issue including differential privacy and homomorphic encryption.
  - **Differential Privacy:** limits the disclosure of private real-time big-data and information during its transmission. in [311], Keshk et al. studied the feature reduction role along privacy protection levels using Independent Component Analysis (ICA) as a technique on big power CPS data. Results

revealed that ICA is more secure without breaching confidential data and offers a better privacy preservation and data utility. In [312], J. Feng et al. presented a lightweight privacy-preserving high-order Bi-Lanczos scheme in integrated edge-fog-cloud architectural paradigm for big data processing. User's privacy is achieved using an homomorphic cryptosystem, while computation overheads are offloaded using privacy-preserving tensor protocols. In [313], Ye et al. presented a secure and efficient outsourcing Differential Privacy (DP) scheme to solve data providers issues related to being vulnerable to privacy attacks. In [314], Zhang et al. presented a practical lightweight identity-based proxy-oriented outsourcing with public auditing scheme in cloud-based MCPS, by using elliptic curve cryptography to achieve storage correctness guarantee and proxy-oriented privacy-preserving property.

– **Homomorphic Encryption:** for a better data confidentiality and privacy protection, homomorphic encryption techniques were adopted. In [315], Zhang et al. presented a Secure Estimation based on Kalman Filtering (SEKF) using a multiplicative homomorphic encryption scheme with a modified decryption algorithm to reduce network overhead and enhance the confidentiality of the communicated data. In [316], Kim et al. a fully homomorphic encryption (FHE) as an advanced cryptographic scheme to directly enable arithmetic operations on the encrypted variables without decryption. Moreover, a tree-based computation of sequential matrix multiplication is introduced to slow down the decrease of the lifespan. In [317], Min et al. presented a parallel fully homomorphic encryption algorithm that supports floating-point numbers to achieve an efficient ciphertext operation without decryption. Results revealed that the ability to limited application problems while meeting the efficient homomorphic encryption requirements in cloud computing environment.

5.3.3. Non-cryptographic-based solutions

Many non-cryptographic solutions were also presented to mitigate and eliminate any possible cyber-attack or malicious event. This was done by implementing Intrusion Detection Systems (IDS), firewalls and honeypots. As a result, various solutions presented by various authors are mentioned and discussed.

- **Intrusion Detection Systems** Various IDS methodology types are available due to the availability of different network configurations [318]. Each IDS methodology is characterised by its own advantages and drawbacks when it comes to detection, configuration, cost, and their placement in the network. In [268], Almohri et al. stated that various research activities were implemented to detect attacks against the CPS. These attacks are split into two main models. **Physics-Based** model, which defines normal CPS operations in CPS through anomaly detection. **Cyber-Based** model which is used in order to recognize potential attacks as listed in Shu et al. [319], Xu et al. [320]. In fact, existing approaches were mainly designed to detect specific attacks against specific applications, including Unmanned Aerial Vehicles (UAV) [321], Industrial Control Processes [322], and smart grids [323]. In [324], Zimmer et al. exploited the possibility of a worst case execution time, through obtaining information using a static application analysis in order to detect malicious code injection attacks in CPS. In [325], Mitchell et al. analysed a behaviour-rule specification-based technique to employ IDS mainly in Medical CPS. The authors also presented the transformation of behaviour rules in a state machine, which can detect any suspicious deviation initiated from any medical device behaviour specification.

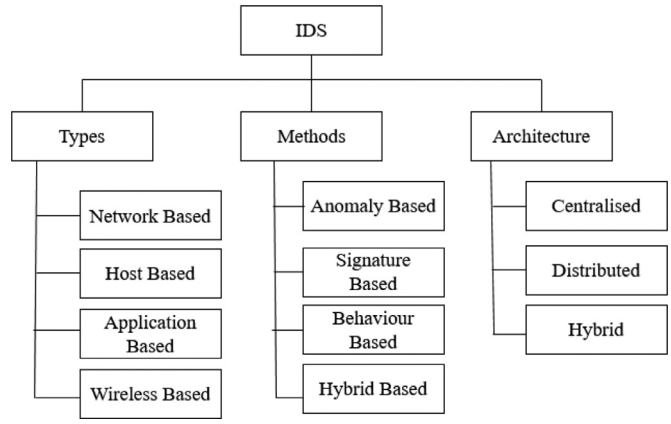


Fig. 8. IDS structure.

- **Intrusion Detection System Placement:** IDS can be placed at the border router of any given IoT network, in one or many given hosts, or in every physical object to ensure the required detection of attacks. Simultaneously, IDS may be able to generate a communication overhead between the LLN (Low Power Lossy Networks) nodes and the border router due to the IDS ability to frequently query the network state. In fact in Zarpelão et al. [326], Zarpel at al. described three main IDS placement strategies (see Fig. 8):
  – **Distributed IDS:** D-IDSs are being employed in every physical LLN object, whilst being optimized in each resource-constrained node. Therefore, a lightweight distributed IDS was presented. In [327], Oh et al. identified a lightweight algorithm matching the attack signatures, and the packet payloads, while suggesting other techniques that require less matching numbers to detect any possible attack. In [328], Lee et al. suggested their own lightweight method that allows them to monitor a node's energy consumption by assigning nodes to monitor their neighbours in the distributed placement. These nodes are defined as "watchdogs". In [329], Cervantes et al., presented a solution called "Intrusion detection of Sinkhole attacks on IPv6 over Low -Power Wireless Personal Area Networks (6LoWPAN) for IoT" (INTI), which combines their concepts of trust and reputation with the watchdogs nodes to mainly detect and mitigate sinkhole attacks. This included the node's role possibly changing every time a network is reconfigured or an attack event has occurred.
  – **Centralized IDS:** C-IDS is mainly deployed in centralized components. This allows all data to be gathered and transmitted by the LLN to the Internet across the border. Therefore, Centralised IDS can analyse all of the exchanged traffic between the LLN and the Internet. In fact, it is not enough to only detect attacks involving nodes within the LLN, since it is difficult to monitor each node during an occurring attack [330]. In [331], Cho et al. presented their solution which is based on analysing all the packets that pass through the border router between physical and network domains. However, the main task is based on how to overcome a botnet attack. In [332,333], Kasinathan et al. deployed a centralized placement that allows them to take into consideration the possibility of overcoming DoS attacks, where in case of a DoS attack, the IDS data transmission would not be affected. In [334], Wallgren et al. employed their cen-

tralized approach which is placed in the border router to detect the attacks that target the physical domain.

- **Hybrid IDS:** H-IDS utilizes both concepts of centralized and distributed placements, by combining their advantages and overcoming their drawbacks. The initial approach allows the network to be organised into clusters with the main node of each cluster being able to host an IDS instance before taking the responsibility for monitoring other neighbouring nodes. Therefore, Hybrid IDS placements can be designed in order to consume more resources than a distributed IDS placement.
  In [335], Le et al. followed the same approach, through the use of a hybrid placement using a relatively small number of "watchdogs" nodes covering the network. This offered them the ability to sniff the communication of its surrounding neighbours in order to indicate whether a node was compromised or not. Therefore, reducing the communication overhead. In [336], Le et al. also managed to organize the network into smaller clusters with a cluster head for each, using the same number of nodes. This allowed an IDS instance to be placed in each cluster head, with each cluster member reporting its own related information and other neighbours related information to the cluster head. In the second approach, IDS modules were placed in, both the border router and other network nodes with the presence of a central component. In [337], Raza et al. presented their own IDS named as SVELTE, where the border router hosts are given the task of processing intensive IDS modules that are responsible for detecting any intrusion attempt by analysing the Routing Protocol Low-power and Lossy device's (RPL) network data. Based on Pongle et al.'s work [338], network nodes were responsible for any detectable changes in their neighbourhood. Moreover, network nodes were also responsible for sending information about their surrounding neighbours to their centralized module which is deployed in the border router having the main assigned responsibility of storing and analysing data. Thus, making it easier to detect and intrusion while identifying attacks in their early stages.
  In [339], Thanigaivelan et al. presented an IDS, which allocates different responsibilities to the network nodes and also to the router's border. Thus, ensuring a cooperative combined work amongst them, with the IDS module monitoring neighbouring nodes, detecting any intrusion attempt, and sending notifications to the IDS modules.

- **Intrusion Detection Methods:** The four main IDS methods are signature-based, anomaly-based, behaviour-based and hybrid based. In fact in Zarpelão et al. [326], these methods were presented, while testing methods and techniques were classified into five main categories, depending on their detection mechanism.
  - **Signature Based:** Such a detection technique is very fast and easy to configure. However, it is only effective for detecting known threats. Thus, showing a high weakness against unknown threats mainly polymorphic malwares and crypting services. Despite its limited capability, Signature Based IDS is very accurate, and also very effective at detecting known threats, with an easy way to understand mechanism. However, this approach is ineffective against the detection of both new and variants of known attacks, due to their matching signature remaining unknown, and constantly updating its signature patches [340,341]. In [327], Oh et al.'s aimed to reduce the computational cost by comparing attack signatures and packet payloads. In [342], Liu et al. presented a signature-based IDS that employs an "Artificial Immune System" (AIS) mechanism with detectors being modelled as immune cells with an ability to classify any datagram as malicious or non-malicious according to the matching signature. Such approach can evolve into the adaptation ability new conditions in new environments that are being monitored. In [332], Kasinathan et al. integrated a signature-based IDS into the network framework, with the objective of being able to detect DoS Attacks against 6LoWPAN-based networks. This IDS was implemented through the adaptation of "Suricata4" used for 6LoWPAN networks, with the main objective of reducing the false alarm rate. In [333], Kasinathan et al. presented a signature-based approach as an extension of their presented approach in Kasinathan et al. [332].
  - **Behaviour Based:** Behaviour Based can be classified as a set of rules and thresholds implemented to define the expected behaviour of the network's components including both nodes and protocols. This approach is capable of detecting any intrusion as soon as the network behaviour deviates from its original behaviour. Behaviour-based acts in the same way as the Anomaly-based detection with a slight difference from specification-based systems where a human expert is needed to manually define each specification rule. Thus, providing a lower false-positive rate than the anomaly based detection [343,344]. Therefore, there will be no need for any training phase, since they are implemented to operate instantly. However, such an approach is not fit for all scenarios, and may become time consuming and error prone. In [345], Misra et al. presented their new approach to protect the IoT middleware from DDoS attacks, by triggering an alert whenever the request number exceeds the threshold line. In [335], Le et al. presented a different specification-based approach, aimed at detecting RPL attacks [346], by specifying the RPL behaviour through network monitoring operation and malicious action detection.
    In [336], Le et al.'s work was extended. Their experimentation resulted in a high true-positive rate, where false positive rates were low throughout their experimentation, whilst also causing an energy overhead compared to a typical RPL network as stated in Zarpelão et al. [326]. In [347], Amaral et al. presented a specification-based IDS that grants the network administrator the ability to create and maintain rules in order to detect any potential attack. Whenever the rule is violated, the IDS would right away send an alert to the Event Management System (EMS) that correlates these alerts for different available nodes in a given network. The success of Misra et al. [345] and Amaral et al. [347] approaches highly relied on the expertise of the network administrator, as well as his experience and skills combined. Therefore, in case of any wrong specifications, it will cause an excessively high false-positive rate and/or a high false-negative rate, leading to a possibly serious risk that threatens the network's security.
  - **Anomaly Based:** This type compares system's activities instantly with the ability to generate an alert whenever a deviation from normal behaviour is detected. However, such a detection method suffers from a high false positive rate [343,348,349]. In [331], Cho et al. presented a botnet detection scheme using the anomaly-based method, by computing an average for each three metrics composing the normal behaviour profile. This was achieved before the system monitors the network's

traffic and raises the alert whenever a metric violates the already defined computed averages. In [350], Gupta et al. presented their own architecture for a wireless IDS, by applying the necessary Computational Intelligence algorithms which are used in order to a construct normal profile behaviour. Moreover, a distinct normal behaviour profile will be implemented for each different IP address being assigned. In [328], Lee et al. suggested that energy consumption should be classified as parameter in order to be used in analyzing each node's behaviour. Thus, defining a regular energy consumption model for each mesh-under routing scheme and route-over routing scheme, where each node will monitor its own energy consumption. In case the node deviates, the IDS classifies the node as malicious and removes it.

In [351], Summerville et al. successfully managed to develop a deep-packet anomaly detection approach aimed at reducing the run on resource constrained IoT devices, by using a bit-pattern matching technique which performs a feature selection. In their experimental evaluation, they used internet enabled devices against four main attack types (including SQLi, worms, etc..), and results have shown low false-positive rates. In [339], Thanigaivelan et al. successfully introduced an IoT distributed internal anomaly detection system, that monitors the node's data rate and packet size. Moreover, in Pongle and Chavan [338] Pongle and Chavan presented an IDS that is designed specifically in order to detect wormhole attacks in IoT devices, in addition to presenting three main algorithms to detect network anomalies. As a result, their experiment revealed that the system has achieved a true positive rate of 94% when tested against wormhole detection, whilst scoring an 87% when it came to detecting both, the attack, and the attacker launching it. In [352], K. Demertzis et al. presented an advanced Spiking One-Class Anomaly Detection Framework (SOCCADF) based on the evolving Spiking Neural Network algorithm. This algorithm implements a One-class classification methodology in an innovative applicable way, due to it being exclusively trained with data to characterise normal ICS operations. Moreover, this algorithm can detect any divergence in behaviours and abnormalities that are associated with APT attacks. The authors stated that SOCCADF is highly suitable for difficult problems, and applications with a huge amount of data. According to their results, the authors stated that SOCCADF has a better performance at a very fast learning speed, with higher accuracy, reliability, and efficiency, and it outperforms the other approaches.

– **Radio-Frequency Based:** In [353], Stone et al. presented a Radio-frequency based anomaly detection method for programmable logic controllers in the critical infrastructure [354]. Their experimental results have demonstrated that the use of a single collected waveform response provides sufficient separability to enable the differentiation between anomalous and normal operational conditions. However, in case of using multi-time domain waveform response, their performance significantly degrades. To solve this problem, the authors presented anomaly detection method based on RF fingerprint feature retrieved from the waveform amplitude, phase, and frequency response to ensure a qualitative differentiation between an anomalous and normal operating conditions.

  In [355], Stone et al. also presented an RF-based methodology to detect anomalous programmable logic controller behaviours with a superior time-domain RF emissions performance. The Cincinnati Bell Any Distance (CBAD) approach reached a Threat Agent Detection and Response (TADR) detection rate higher than 90% benchmark realised at an Signal Power Ratio (SNR) higher or equal to 0 dB. Despite these results, this approach is prone to RF noise, signal degradation and coding loops. In [356], Stephen et al. presented a timing-based side channel analysis technique to help control system operators in detecting any firmware and ladder logic programs modification to the programmable logic controllers. This approach allows a field device to be fingerprinted upon deployment to create an supplicate baseline fingerprint. Various fingerprints of the device are taken and compared to the baseline in order to detect and alert operators of both intentional and unintentional modifications in programmable logic controllers.

– **Hybrid Based:** It is based on using a specification-based techniques of signature-based, and anomaly-based detection in order to maximize their advantage whilst minimizing their drawbacks. In [337], Raza et al. presented a hybrid IDS known as SVELTE which offers the right trade-off between storage cost of signature-based methods, and computational cost of anomaly-based methods. In [357], Krimmling et al. tested their anomaly and signature-based IDS using the IDS evaluation framework that they presented. Their results revealed the failure of each approach in detecting certain attacks alone. As a result, the authors combined these approaches to cover and detect a wider attack range. In [329], Cervantes et al. presented the Intrusion Detection of SiNkhole attacks on 6LoWPAN for Internet of Things (INTI), to detect and isolate sinkhole attacks by combining the anomaly-based approach which ensures a packet exchange between these nodes. This was done by using the specification-based method in order to extract the evaluation node based on both trust and reputation. However, when comparing SVELTE [337] to INTI IDS, Cervantes et al. simulated a scenario where INTI IDS achieved a sinkhole detection with a rate up to 92%. In case of a fixed scenario, the rate has only reached 75%. Either ways, it has shown a low rate of false-positives and false-negatives compared to SVELTE.

- **Firewalls** Firewalls saw rare use of employment in CPS domain due to the advancement of IDS and Artificial Intelligence technologies. Therefore, a handful number of firewall-based solutions were presented. In [358], Jiang et al. mentioned the use of paired Firewalls between enterprise and manufacturing zones to enhance the cyber security of servers. Their choice of paired firewalls is due to the stringent security and clear management separation. In [359], Nivethan et al. presented a novel methodology that uses iptables as an effective powerful open-source network-level firewall for SCADA systems that inspects and filters SCADA protocol messages. In [360], Adepu et al. presented Argus as a framework for defending a public utility against cyber-physical attacks. Its implementation tests revealed its effectiveness in detecting single and complex multi-component deception attacks. In [361], Ghosh et al. presented their approach towards predicting real-time failures of network devices including load balancers and firewalls using event data. Their focus was on raw device event data. Results revealed that a low failure rate of devices, while achieving a precision rate of 77% and recall network device failure prediction of 67%. In [362], Javed et al. presented a novel security architecture that localizes the cyber-attack in a timely manner, and simultaneously recovers the affected cyber-physical system functionality. Results revealed its effectiveness against system availability attacks only.

- **Honeypots & Deception Techniques** Deception is a key defensive security measure that CPS rely on as a decoy to hide and protect their system. This can be mainly done using honeypots. However, other deceptive solutions also exist. In [363], Cohen presented how honeypot deception can be made more effective upon employment, while discussing different ranges of deception tactics. In [364], Antonioli et al. presented the design of a virtual, high-interaction, server-based ICS honeypot to ensure a realistic, cost-effective, and maintainable ICS honeypot that captures the attackers activities. Such implementation aims to target Ethernet/IP based ICS honeypots. In [365], Litchfield et al. presented HoneyPhy, a physics-aware framework for complex CPS honeypots that monitor the originating behaviour from the CPS process and the device that controls the CPS itself. Results reveal that HoneyPhy can be employed to simulate these behaviours in a real-time manner. In [366], Irvene et al. leverage HoneyPhy framework to create the HoneyBot. HoneyBot is the first software hybrid interaction honeypot specifically designed for networked robotic systems. Simulations reveal that HoneyBot can fool attackers into believing that their exploits are successful.
  In [367], Fraunholz et al. set up a medium interaction honeypot offering telnet and Secure Shell (SSH) services to capture data from attack sessions. This data was analysed to allow the classification of attacker types and sessions, respectively. In [368], Tian et al. presented a honeypot game model with both low/high-interaction modes to mainly improve CPS security. Simulation results revealed that optimal human analysis cost allocation and defensive strategy are obtained. Making their method suitable for CPS data protection. In [369], Duan et al. presented a framework called "CONCEAL" as a new deception as a service paradigm that is effective and scalable. This was done by combining m-mutation for address anonymization, k-anonymity for fingerprint anonymization, and l-diversity for configuration diversification. CONCEAL's proxies save can reach as high as 90%. In [370], Bernieri et al. presented a modular framework called Deep Detection Architecture (DDA) to provide cyber-physical security for industrial control systems. A cyber-physical simulation methodology was also presented and exploited to analyse the security modules under several different attack scenarios. Moreover, DDA will be extensively used for the next ICS generation and implemented into the Industry v4.0 paradigm. In [371], Sayin et al. introduced a deceptive signalling framework as a new defence measure against advanced adversaries in CPS. This framework relies on information that is strategically accessible to adversaries to indirectly control their actions.

5.4. CPS forensics

It is not enough to encrypt, detect and protect against passive and active attacks. In fact, aside from identifying the source of the attack, it is also important to know how the attack was performed despite of the challenges [372]. Hence, there an urgent need for the forensics domain to enhance the forensics tools and techniques to retrieve and analyze logs of events that took place before, during and after the incident. In fact, CPS forensic analysis is still in its early stages of development, due to the ICS specialized nature along with its proprietary and poorly documented protocols [373]. In [374], Awad et al. surveyed the digital forensics applied to SCADA systems and covered the challenges that surround them. Therefore, presenting the current state-of-the-art device and network-specific tools. In [375], Grispos et al. presented a forensic-by-design framework that ensure the integration of forensics principles and concepts in MCPS. In [376], H. Al-Khateeb et al. shed a light on a new approach where a Blockchain-based Chain-of-Custody may be simultaneously established to the generated pre-identified data (data of interest) by an IoT device. In [377], Chan et al. described a novel security block method for detecting memory variable changes that may affect the integrity of programmable logic controllers and efficiently and effectively enhancing security and forensics. This is done by by adding monitoring and logging mechanisms to PLCs. Therefore, ensuring faster anomaly detection with higher accuracy, less overhead and adjustable impact.

In [378], Ahmadi et al. presented a federated Blockchain (BC) model that achieves forensic-readiness by establishing a digital Chain-of-Custody (CoC) and a CPS collaborative environment to qualify as Digital Witnesses (DW) to support post-incident investigations. In [379], Parry et al. presented a high speed hardware-software network forensics tool that was specifically designed for capturing and replaying data traffic in SCADA systems. Experimental results guaranteed preserving the original packet ordering with improvement in data capture and replay capabilities. In [380], Cebe et al. presented a blockchain infrastructure by integrating a Vehicular Public Key Infrastructure (VPKI) to achieve membership establishment and privacy along a fragmented ledger related to detailed vehicular data. Moreover, identities pseudonyms were used to preserve users' privacy. In [381], P. Taveras presented a high level software application that detects critical situations like abnormal changes of sensor reads and traffic over the communication channel, mainly. Therefore, helping by improving critical infrastructure protection and providing appropriate SCADA forensics tools for incident response and forensics analysis. In [382], Ahmed et. al. presented a testbed of three IPPs (Industrial Physical Processes) using real-world industrial equipment including PLC. The authors stated that their presented testbed is useful in cyber-security, education (SCADA systems) and forensics research including PLC analysis and programming. Moreover, their testbed includes fully functional physical processes which are deemed very essential for both research and pedagogical efforts.

In [383], Yau and Chow presented a novel methodology which logs relevant memory address values, that are being used by programmable logic controller programs, in addition to their timestamps. This methodology can be extremely valuable in a forensic investigation in case of an ICS incident. This is realized by applying machine learning techniques to the logged data in order to identify any anomalous programmable logic controller operation. In [384] Saman et. al. combined symbolic execution with model checking to analyse any malicious PLC code bound injection. Their combined approach can also be used for forensic purposes including the identification of the areas where the code injection took place, along with which part of the code caused its execution. In [385], McMinn et al. presented a firmware verification tool used for the forensics analysis of trials of the altered firmware codes to gain unauthorised access over ICS networks. Such verification is achieved either though the analysis of the PLC's captured data to check whether the PLC's firmware is modified or not. In [386], Kleinmann et al. presented an accurate IDS that utilizes a deterministic finite automaton that models the network traffic with a 99.26% accuracy, after analysing and observing the highly periodic network traffic of Siemens S7 PLC. In [387], Saranyan et al. provided a comprehensive forensic analysis of network traffic generated by the PCCC (Programmable Controller Communication Commands) protocol, and also presented prototype tool that extracts updates of the programmable logic and crucial configuration information. Authors also stated that their proof-of-concept tool, "Cutter", which is capable of parsing the content of PCCC messages, extracts and presents digital artifacts in a human-readable form such as Simple Mail Transfer Protocol (SMTP) configuration. Moreover, the SMTP configuration can be retrieved from the network log and can be parsed, too.

In [377], Chan et. al. presented a novel security block method that enhances ICS security and forensics by adding monitoring and logging mechanisms to PLCs, and ICS's key components. Their results demonstrated that their approach increased the anomaly detection range, speed and accuracy with a slight performance impact and a reduced network overhead. Thus, ensuring a more enhanced, efficient and effective forensic investigation procedure. In [388], Yua et al. described the design and implementation of a novel PLC logging system. To overcome the inadequacy of information in forensics investigations, their logging system is used to extract data from Siemens S7 communications protocol traffic. This logging system also helps in recording the evidence based on the exchanged data between the PLC and other network devices. Thus, providing key information about the attack source, actions and timelines. The choice of Simatic S7 PLC is due to their widespread use [389] and successful exploitation by insidious Stuxnet malware. In [390], Chan et al. focused on the logging mechanism of a Siemens PLC, including the Siemens Total Integrated Automation Portal V13 program (Siemens TIA Portal, known as Siemens Step-7). The author's methodology performs an effective and practical forensics analysis of the PLC. Moreover, it focuses on Siemens PLC along with an installed computer workstation with the Siemens TIA Portal (previously targeted by Stuxnet).

5.5. Limitations

During the evaluation and analysis of the existing presented security solutions, several limitations can be deduced, presented and discussed as follows:

- **Asymmetric Cryptography:** introduces overhead in terms of latency and resources. The asymmetric nature of certain cryptographic work [285,292] leaves CPS's real-time communication prone to network latency and overhead due to delays in the encryption/decryption process.
- **Weak Device/User Authentication Scheme:** many of the presented authentication techniques [73,130,306,308] are not very suitable for a secure appliance, due to the lack of multi-factor authentication schemes to protect CPS systems from unauthorised users and access.
- **CPS Forensics Field:** are still prone to many challenges including the lack of tools, skills and responses against any potential anti-forensics activity [372,373].
- **Inefficient Honeypot & Deception System:** despite of the recently proposed techniques in Irvene et al. [366], Tian et al. [368], Bernieri et al. [370], Sayin and Basar [371], there are no appropriate honeypot techniques that can be specifically adopted to protect CPS systems, especially in the wake of Industry v4.0.
- **Lack of Firewall Protection:** firewall solutions including [358,359] are not very applicable and suitable for employment into the CPS domain, nor they offer an effective protection. The best solution requires dynamic firewalls, as well as application and next generation firewall types.
- **Inefficient Intrusion Detection Systems:** despite the availability of various IDS types such as anomaly-based [352], behaviour-based [345] and signature-based [333], these are generally applied within IoT-based domains and not specifically designed to protect CPS systems.

6. Learnt lessons

To secure CPS, many lessons were learnt as how to maintain and achieve their required security goals. Among such lessons:

1. **Maintaining Security Services:** new lightweight cryptographic solutions are required to secure CPS and IoCPT in real-time operations but with minimum computational complexity. These cryptographic solutions can help ensure the following security services:
   - **Confidentiality:** there is a need for a new class of lightweight block or stream cipher algorithms to secure CPS resource-constrained real-time communications. Recently, a new approach was presented, and it is based on the dynamic key-dependent cipher structure and it requires two or one iteration with few operations [391–394]. A set of these solutions can be applied at the physical layer [393–395].
   - **Message/Device Integrity:** this includes the protection of CPS data and devices' integrity from any physical/logical alteration(s). This can be done by ensuring that the Operating System, applications, and software are securely designed and without any flaws to prevent tampering, with strong cryptographic hash functions (SHA256, SHA384 and SHA512). In this end, a new lightweight hash function was presented in Noura et al. [396] and it requires a single round compared to the existing ones.
   - **Device/Data Availability:** requires the need for computational resources along with verified backups, and a self-healing ability of CPS in such a way to recover immediately from availability attack types. Also, maintaining data availability is as necessary [397], and this can be done by defining a multi-secure connection [398–403].
2. **Strong Device/user Authentication:** An efficient device/user mutual multi-factor authentication scheme is necessary, along with enhancing verification and identification phases based on attribute access-control privileges (least-privilege) to ensure non-repudiation and stronger accountability.
3. **Protecting Digital Evidences:** this is highly important since most of the advanced attacks focus on eliminating any source of evidence that traces back to the attack source, such as the case of Shamoon, Duqu, Flame and Stuxnet malware types [75,109,404]. Furthermore, modern digital forensics solutions should define new countermeasures to preserve digital forensics logs.
4. **Enhancing Security Policy:** in many cases, CPS attacks occurred by insiders (by accident or on purpose). Accordingly, all employees must undergo a screening process before recruitment, and have their privileges suspended outside working hours and monitored their actions in the case of advanced tasks. This means that CPS security policy should be contain new rules to limit access and to reduce the potential damage.
5. **Smart Cooperation with non-cryptographic solutions:** Intrusion detection systems should be hybrid in all terms and should be coordinated in an efficient manner with firewalls and dynamic honeypot systems.
6. **Enforcing Compliance:** by respecting users' privacy through ensuring data access regulatory compliance that processes CPS's big data via clouds, especially when stored by utility providers (Trusted Third Party (TTP)) to prevent any data leakage and users privacy violations. Therefore, maintaining a suitable trade-off between users privacy and systems' security and performance, while also ensuring firmer accountability measures [405,406].
7. **Achieving Trade-Off:** is essential for maintaining systems' availability, safety and security [407,408]. Therefore, such a trade-off must be achieved based on the combination of these three key requirements while taking into consideration available budget and cost requirements in terms of risk assessment:
   - **Availability & Safety:** both features are linked together since issues related to the safety of a CPS system also affect its operational availability. To ensure this trade-off, verified backups of computational devices must always be considered in the planning phase, as a second line of defense to handle

any sudden service/system disruption (power cuts, blackouts, pumping stoppage), or maintenance (updates, renovation, installation, etc.).

- **Availability & Security:** since availability is very crucial for all real-time CPS operations, securing them is a top priority. For this reason, a trade-off is to be established between availability and security (Frequency Hopping/Shifting, Signal-to-Noise Ration, Backup devices, Firewalls, IDS, Traffic Monitoring, etc.) especially against wireless jamming attacks.
- **Safety & Security:** having a secure CPS does not always mean that it is protected. In fact, a trade-off must be achieved to maintain both safety and security features in any CPS domain, where a safety feature is meant to protect the CPS from any accidental failure/hazard (system failure, miscalculations, abnormal activities, etc.), while a security feature (IDS, Firewalls, Artificial Intelligence (AI), etc.) ensures protection against intentional cyber-physical attacks.

7. Suggestions & recommendations

Different security measures could be adopted and enhanced to enhance the protection against various threats and attacks. These include:

- **Prioritization & Classification:** of critical CPS components and assets before assessing, managing and analysing risks to ensure the proper budget spending on the right choice of security measures (basic, standard or advanced) in accordance to their costs compared to the likelihood of the occurrence of a given incident and its impact.
- **Careful Financial Planning & Management:** must be conducted in terms of available budget and needed costs/resources to protect critical/non-critical CPS assets and components.
- **Lightweight Dynamic Key Dependent Cryptographic Algorithms:** These solutions can be used to to ensure several security services such as message confidentiality, integrity and authentication, which are mandatory during any secure CPS communications. This can be done by using new generation of cryptographic algorithms, which were presented in Noura et al. [392,409,410]. The advantage of these solutions that it can reach a good balance between security and performance level. The robustness against attacks were proved since a dynamic key is used per message (or a set of messages; depend of application constraints and requirements). Moreover, this dynamic key is used to produce a set of cryptographic primitives and update cryptographic primitives. This means different ciphertext can be obtained for the same plaintext since different cryptographic primitives are used. While, the effectiveness is validates since these algorithms require only one round iteration and uses simple operations in addition to avoid diffusion operation. The new generation of these cryptographic algorithms reduce the required latency, resources and computation overhead, which help CPS devices to preserve better their main functionalities.
- **Defining Privileges:** This should be considered as the most suitable access control policy, which assigns permissions and rights depending on the users' roles/tasks/attributes when it comes to accessing CPS, and removing these access rights upon completing the task or upon the employee's leave. This also includes the use of the least privilege policy. Therefore, the definition of privilege should be done based on Attribute Based Access Control (ABAC), where policies combined with attributes specify access authorizations. Note that ABAC makes access control decisions based on Boolean conditions of attribute values. It provides a high level of granularity, which is necessary to make CPS control access scheme more secure.
- **Strong Entity Multi-Factor Authentication:** Unfortunately, entity authentication schemes that are based on a single factor of authentication (you have, you know, you do or you are) are not resistant enough against authentication attacks, which are increasingly becoming more dangerous. The first line of defense in any system is the entity authentication scheme since any entity authentication attack can lead to confidentiality, integrity and/or availability attack. Recently, the concept of multi-factor authentication was applied by combining two or more factors: (1) "you are" which includes device fingerprint, user fingerprint, hand geometry, iris scan, retina scan, etc., and (2) "you have" which includes cryptographic keys to increase its robustness against authentication attacks such as the ones described in Melki et al. [411], Noura et al. [412].
  This mechanism should be an essential requirement in CPS systems, in addition to the use of the geographical location. The advantage of these solutions is their ability to reduce false positives, and to complicate the authentication attacks since several factors should be broken instead of one. Consequently, this limits the access only to authorised entities and personnel (devices/users).
- **Strong Password & dynamic Hashing Process:** Passwords are considered as the "you know" authentication factor. However, several attacks such as rainbow and hash table attacks can be applied. In order to prevent them from occurring, after a periodic interval, passwords must be re-hashed with a new dynamic Nonce for each user. Moreover, a secure cryptographic hash function should be used such as SHA-3 and SHA-2 (variant 512). This avoids birthday attacks and reduces rainbow/hash table attacks.
- **Secure and Protected Audit:** can be done by using an Audit manager system that collects and stores logs in a distributed system. A possible solution that can be applied in this context was presented recently in Noura et al. [413]. This limits any insider attempt against a cyber-physical system and it preserves the digital evidence of internal and external attacks to trace them back.
- **Enhanced Non-Cryptographic Solutions:** require the need for hybrid IDS/IPS systems or AI-based IDS/IPS (using Machine Learning algorithms), along with advanced firewalls (i.e Application and Next Generation Firewalls) [414], and dynamic honeypots [415] to prevent any future security breach based on a vulnerability exploit. This can be done by employing lightweight IDS/IPS and especially the anomaly-based ones. In fact, one should select the anomaly detection algorithm according to the CPS device constraints, which can be statistical for limited ones or based on machine algorithm, such as random forest, for powerful CPS devices. On the other hand, signature-based techniques can be applied at the Gateway (GW) where all network traffic can be analyzed.
- **Secure & Verified Backups:** this is essential to maintain the CPS data availability and to avoid data destruction or alteration by ensuring robustness against DoS/DDoS and Ransowmare attacks, especially that such attacks may result in total blackouts as in the case of the US. This can be done by using lightweight data protection solutions such as the ones presented in Noura et al. [399].
- **Forensic Efforts:** are essential to retrieve the traces of any occurring attack. Also, new solutions against anti-forensic techniques should be introduced to preserve any digital evidence [413]. This is realized by recovering logs and monitoring network and system behaviour, which can successfully limit various reconnaissance attempts. However, the newly introduced forensics tools must be compatible with different

CPS devices' software/hardware, especially resource constrained devices, and must also be resistant against anti-forensics attempts.

- **Enhanced Incident Response:** includes the ability to identify, alert and respond to a given incident. Moreover, incident recovery and incident investigation plans should be put in place to mitigate attacks. This provides protection against non-intentional technical and operational failures (power shortage, blackout) through back-up plans, and from intentional failures (cyber-attacks), through CERT (Computer Emergency Response) [416], CSIRT (Computer Security Incident Response) [417], and IRCF (Incident Response And Computer Forensics) teams [418,419]. As such, CPS scientists and engineers must undergo further education and training to ensure an enhanced and efficient cyber, physical and computational environment with secure computing and communications.
- **Real time Monitoring:** running real-time systems using specialised forensics or non-forensics tools and methods is essential to prevent any cyber-physical system accidental or non-accidental failure. This enables constant checking and monitoring of CPS devices' behaviour and hence, the detection of any cyber-attack attempt in its early stages.
- **Security Check:** and employee screening must be done for each employee before and during the job to eliminate and contain any possible insider/whistle-blower attempt. Therefore, signing agreements [420] such as Non-Disclosure Agreement (NDA), Confidentiality Agreement (CA), Confidential Disclosure Agreement (CDA), Proprietary Information Agreement (PIA) or Secrecy Agreement (SA) is highly recommended. Such security checks are essential especially in critical areas such as nuclear power plants [421].
- **Periodic Employee Training:** includes periodic awareness training of ICS and PLC employees on the best cyber-security practices based on their level and knowledge, with the ability to detect any suspicious behaviour or activity. Moreover, employees must be trained over various security threats and wrong practices such as avoiding the installation of any software update, how to counter social-engineering and phishing attempts, while also maintaining accountability in case of wrong doings.
- **Periodic Pen Testing & Vulnerability Assessment:** must be maintained in a periodic manner to enforce system auditing, detecting threats, and mitigating them in a real-time manner before they are discovered and exploited by an attacker under the zero-day exploit conditions.
- **Periodic Risk Assessment:** must also be enforced to study the likelihood and impact of a given risk against a critical/non-critical cyber-physical system based on a qualitative or/and quantitative risk assessment and a Cost" Benefit Analysis (CBA), to classify the risk based on acceptable/non-acceptable level and to mitigate it as early as possible.
- **Up-to-Date Systems:** cyber-physical systems must be kept up-to-date in terms of software, firmware and hardware through constant verified patches and updates [422]. Moreover, such systems must be secured at different levels of their implementations (layered protection), with the ability to mitigate and tackle a given attack to reduce its impact and prevent further escalation and damage. Furthermore, USB ports must be physically and logically removed to prevent any payload injection, and PLC systems behaviour and activities must be constantly monitored for any suspicious/abnormal behaviour [422].
- **AI Security Solutions:** Artificial Intelligence is used in IDS/IPS anomaly detection schemes or in "you are" or "you do" entity authentication schemes. In fact, AI is now being considered as a game-changing solution against a variety of cyber-physical attacks targeting CPS systems, devices and communication points. Despite the time consuming process of training an AI system, the accuracy of detection and prevention are much higher than any human intervention. Recent advancements in machine learning, and especially in deep learning, can make CPS systems more secure, robust and resistant against cyber-physical attacks.
- **Defense In-Depth:** most of the existing solutions offer protection against a single attack aspect or a security requirement. Instead, there is need for a multi-purpose security solution that ensures the best protection at each operational layer (perception, transmission and application) of CPS. For example, the two most known international standards for functional safety in the automotive industry, the ISO 26262 [423] and IEC 61508/Edition2 [424,425] should be respected and applied. This ensures a safe CPS implementation based on the Functional safety, which includes the Safety Integrity Level (SIL) basics [426] which in turn, rely on the Probability of Failure on Demand (PoFoD) and the Risk Reduction Factor (RRF) to ensure a much more accurate and efficient Hazard and Risk Analysis (HRA) [424,426], mainly in the Electronic Control Units (ECU) [427,428]).
- **CPS Security & Privacy Life-cycle:** finally, to sum up this work, our paper presents a combined Operational and Functional Safety/Security (OFSS) life-cycle that ensures a successful and safe CPS employment as seen in Fig. 9). This framework is derived from ISO 26262 and IEC 61508/Edition2 protocols and their approach towards ensuring the CPS Functional safety/security. The framework consists of six main phases:
  - **Phase 1:** Devising a plan to design a CPS system by following a well-defined time-table and schedule in accordance to the needed budget and corresponding costs. This also requires the assistance of humans (businessmen, engineers, workers, etc.) and non-human assets (vehicles, machines, etc.).
  - **Phase 2:** requires a careful risk and hazard analysis, which consists of a proper risk management and asset classification, as well as the mutual connection between the two to ensure an accurate decision-making over the adoption of the right security measures/counter-measures.
  - **Phase 3:** defines the right functional safety, security and dependability requirements along their key components/mechanisms that are essential to mitigate a risk/hazard and to reduce their likelihood and impact in case of their occurrence.
  - **Phase 4:** consists of evaluating the performance of CPS in terms of the recently introduced functional safety, security and dependability measures in an operational manner where a performance management and analysis will be conducted to ensure a proper/mutual security-performance, safety-performance and dependability-performance trade-offs.
  - **Phase 5:** once the performance is evaluated, the cyber-physical system is tested and validated to detect any remaining software/hardware bug, security gap, or performance issue to apply the required modifications before being commissioned. If the testing is unsuccessful, the process restarts again to find where the issue took place. If successful, the CPS will head towards further commissioning before being officially deployed.
  - **Phase 6:** upon successful testing, the deployed CPS system will undergo a trial phase to evaluate its operational status, while monitoring its behaviour and performance before becoming fully operational.

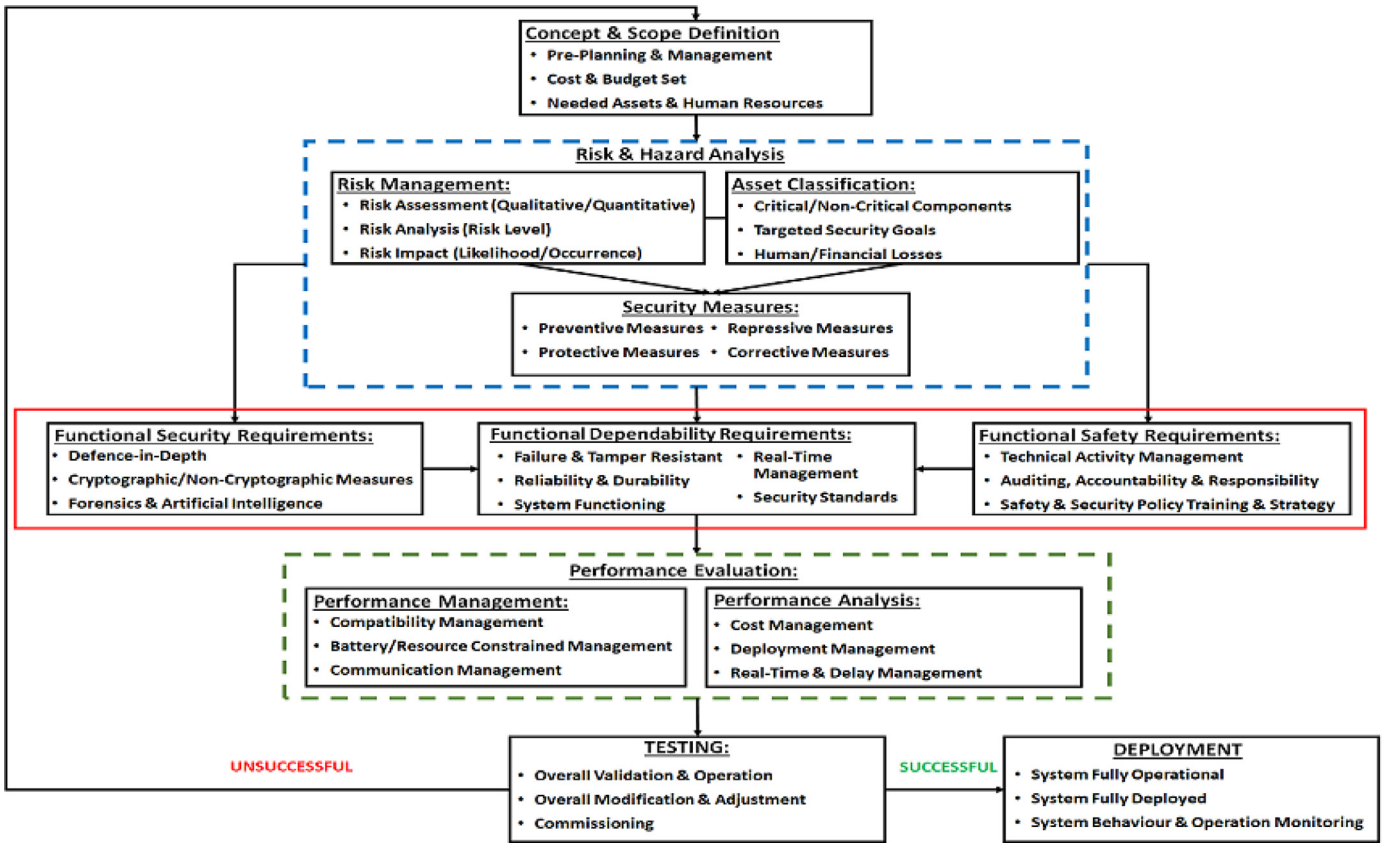


Fig. 9. CPS-OFSS life-cycle framework.

8. Conclusion

CPS systems are key components of Industry v4.0, and they are already transforming how humans interact with the physical environment by integrating it with the cyber world. The aim of implementing CPS systems, either within or outside IoT (IoCPT), is to enhance the products' quality and systems' availability and reliability. However, CPS systems suffer from various security and privacy issues that can degrade their reliability, safety, efficiency, and possibly hindering their wide deployment. In this paper, we first overview all components within CPS systems and their interconnections including IoT systems, and we focus on the main CPS security threats, vulnerabilities and attacks, as related to the components and communication protocols being used. Then, we discuss and analyze the recently available CPS security solutions, which can be categorized as cryptographic and non-cryptographic solutions. Next, we highlight the important lessons learnt throughout, and accordingly, we present suggestions and recommendations with respect to the various security aspects, services, and best practices that must be put in place to ensure resilient and secure CPS systems, while maintaining the required performance and quality of service.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This paper is supported with funds from the Maroun Semaan Faculty of Engineering and Architecture at the American University of Beirut.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.micpro.2020.103201.

References

[1] J. Lee, B. Bagheri, H.-A. Kao, A cyber-physical systems architecture for industry 4.0-based manufacturing systems, Manuf. Lett. 3 (2015) 18–23.
[2] Y. Lu, Industry 4.0: a survey on technologies, applications and open research issues, J. Ind. Inf. Integr. 6 (2017) 1–10.
[3] J. Lee, E. Lapira, S. Yang, A. Kao, Predictive manufacturing system-trends of next-generation production systems, IFAC Proc. Vol. 46 (7) (2013) 150–156.
[4] S. Heng, Industry 4.0: huge potential for value creation waiting to be tapped, Deutsche Bank Res. (2014) 8–10.
[5] S. Gries, M. Hesenius, V. Gruhn, Cascading data corruption: about dependencies in cyber-physical systems: poster, in: Proceedings of the 11th ACM International Conference on Distributed and Event-Based Systems, ACM, 2017, pp. 345–346.
[6] A. Di Ferdinando, P. Ezhilchelvan, M. Dales, J. Crowcroft, Ninth IEEE international symposium on object and component-oriented real-time distributed computing.
[7] I. Chun, J. Park, W. Kim, W. Kang, H. Lee, S. Park, Autonomic computing technologies for cyber-physical systems, in: 2010 The 12th International Conference on Advanced Communication Technology (ICACT), 2, IEEE, 2010, pp. 1009–1014.
[8] C.-R. Rad, O. Hancu, I.-A. Takacs, G. Olteanu, Smart monitoring of potato crop: a cyber-physical system architecture model in the field of precision agriculture, Agric. Agric. Sci. Procedia 6 (2015) 73–79.
[9] T. Haidegger, G.S. Virk, C. Herman, R. Bostelman, P. Galambos, G. Györök, I.J. Rudas, Industrial and medical cyber-physical systems: tackling user requirements and challenges in robotics, in: Recent Advances in Intelligent Engineering, Springer, 2020, pp. 253–277.
[10] B. Siddappaji, K. Akhilesh, Role of cyber security in drone technology, in: Smart Technologies, Springer, 2020, pp. 169–178.
[11] J.-P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, Securing internet of medical things systems: limitations, issues and recommendations, Future Gener. Comput. Syst. 105 (2020) 581–606.
[12] T.M. Chen, Survey of cyber security issues in smart grids, in: Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II, 7709, International Society for Optics and Photonics, 2010, p. 77090D.

[13] C. Miller, C. Valasek, A survey of remote automotive attack surfaces, Black Hat USA 2014 (2014) 94.
[14] E. Bou-Harb, A brief survey of security approaches for cyber-physical systems, in: 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2016, pp. 1–5.
[15] N. Sklavos, I.D. Zaharakis, Cryptography and security in internet of things (IoTs): models, schemes, and implementations, in: 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2016, pp. 1–2.
[16] A. Humayed, J. Lin, F. Li, B. Luo, Cyber-physical systems security-a survey, IEEE Internet of Things J. 4 (6) (2017) 1802–1831.
[17] H. Yoo, T. Shon, Challenges and research directions for heterogeneous cyber—physical system based on IEC 61850: vulnerabilities, security requirements, and security architecture, Future Gener. Comput. Syst. 61 (2016) 128–136.
[18] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, Cyber-physical systems and their security issues, Comput. Ind. 100 (2018) 212–223.
[19] H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao, C. Cheng, A survey of security and privacy in big data, in: Communications and Information Technologies (ISCIT), 2016 16th International Symposium on, IEEE, 2016, pp. 268–272.
[20] H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao, C. Cheng, A survey of security and privacy in big data.
[21] J.S. Kumar, D.R. Patel, A survey on internet of things: security and privacy issues, Int. J. Comput. Appl. 90 (11) (2014).
[22] R.E. Johnson, Survey of SCADA security challenges and potential attack vectors, in: Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, IEEE, 2010, pp. 1–5.
[23] O. Kocabas, T. Soyata, M.K. Aktas, Emerging security mechanisms for medical cyber physical systems, IEEE/ACM Trans. Comput. Biol. Bioinform. 13 (3) (2016) 401–416.
[24] C. Lai, P. Cordeiro, A. Hasandka, N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, M. Martin, Cryptography considerations for distributed energy resource systems, in: 2019 IEEE Power and Energy Conference at Illinois (PECI), IEEE, 2019, pp. 1–7.
[25] Y. Ashibani, Q.H. Mahmoud, Cyber physical systems security: analysis, challenges and solutions, Comput. Secur. 68 (2017) 81–97.
[26] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, Internet of things (IoT) security: current status, challenges and prospective measures, in: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2015, pp. 336–341.
[27] N. Gaddam, G.S.A. Kumar, A.K. Somani, Securing physical processes against cyber attacks in cyber-physical systems, in: Proc. Nat. Workshop Res. High–Confidence Transp. Cyber-Phys. Systems, Autom., Aviation Rail, 2008, pp. 1–3.
[28] K. Zhao, L. Ge, A survey on the internet of things security, in: 2013 Ninth International Conference on Computational Intelligence and Security, IEEE, 2013, pp. 663–667.
[29] R. Khan, S.U. Khan, R. Zaheer, S. Khan, Future internet: the internet of things architecture, possible applications and key challenges, in: 2012 10th International Conference on Frontiers of Information Technology, IEEE, 2012, pp. 257–260.
[30] Y. Geng, C.-m. Rong, C. Veigner, J.-T. Wang, H.-B. Cheng, Identity-based key agreement and encryption for wireless sensor networks, J. China Univ. Posts Telecommun. 13 (4) (2006) 54–60.
[31] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wirel. Netw. 20 (8) (2014) 2481–2501.
[32] A.D. Wood, J.A. Stankovic, Security of distributed, ubiquitous, and embedded computing platforms, Wiley Handb. Sci. Technol. Homel. Secur. (2008) 1.
[33] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, H.-Y. Du, Research on the architecture of internet of things, in: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 5, IEEE, 2010, pp. V5–484.
[34] T. Sommestad, G.N. Ericsson, J. Nordlander, SCADA system cyber security-a comparison of standards, in: Power and Energy Society General Meeting, 2010 IEEE, IEEE, 2010, pp. 1–8.
[35] B. Zhu, S. Sastry, SCADA-specific intrusion detection/prevention systems: a survey and taxonomy, in: Proceedings of the 1st Workshop on Secure Control Systems (SCS), 11, 2010, p. 7.
[36] V. Sridharan, Cyber security in power systems, Georgia Institute of Technology, 2012 Ph.D. thesis.
[37] J. Weiss, Protecting Industrial Control Systems from Electronic Threats, Momentum Press, 2010.
[38] W. Hu, J. Oberg, J. Barrientos, D. Mu, R. Kastner, Expanding gate level information flow tracking for multilevel security, IEEE Embed. Syst. Lett. 5 (2) (2013) 25–28.
[39] H. Gao, Y. Peng, K. Jia, Z. Dai, T. Wang, The design of ICS testbed based on emulation, physical, and simulation (EPS-ICS testbed), in: 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2013, pp. 420–423.
[40] A. Saqib, R.W. Anwar, O.K. Hussain, M. Ahmad, M.A. Ngadi, M.M. Mohamad, Z. Malki, C. Noraini, B.A. Jnr, R. Nor, et al., Cyber security for cyber physcial systems: atrust-based approach, J. Theor. Appl. Inf. Technol. 71 (2) (2015) 144–152.
[41] B. Zhang, X.-X. Ma, Z.-G. Qin, Security architecture on the trusting internet of things, J. Electron. Sci. Technol. 9 (4) (2011) 364–367.
[42] J. Clause, A. Orso, Camouflage: automated anonymization of field data, in: 2011 33rd International Conference on Software Engineering (ICSE), IEEE, 2011, pp. 21–30.
[43] S.P. Pomroy, R.R. Lake, T.A. Dunn, Data masking system and method, 2011. US Patent 7,974,942.
[44] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, Y. Jin, Cyber–physical systems: a security perspective, in: 2015 20th IEEE European Test Symposium (ETS), IEEE, 2015, pp. 1–8.
[45] S. Raza, Lightweight security solutions for the internet of things, Mälardalen University, Västerås, Sweden, 2013 Ph.D. thesis.
[46] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[47] D.C. Mazur, R.D. Quint, V.A. Centeno, Time synchronization of automation controllers for power applications, in: 2012 IEEE Industry Applications Society Annual Meeting, IEEE, 2012, pp. 1–8.
[48] U. Morelli, L. Nicolodi, S. Ranise, An open and flexible cybersecurity training laboratory in it/ot infrastructures, in: Computer Security, Springer, 2019, pp. 140–155.
[49] S.R. Vogel, S.J. Zack, Method and apparatus providing remote reprogramming of programmable logic devices using embedded jtag physical layer and protocol, 2006, US Patent 7,155,711.
[50] A. Ardanza, A. Moreno, Á. Segura, M. de la Cruz, D. Aguinaga, Sustainable and flexible industrial human machine interfaces to support adaptable applications in the industry 4.0 paradigm, Int. J. Prod. Res. 57 (12) (2019) 4045–4059.
[51] J.R. Saunders, Automated remote telemetry paging system, 1989, US Patent 4,856,047.
[52] K. Stouffer, J. Falco, Guide to Supervisory control and data acquisition (SCADA) and industrial control systems security, National Institute of Standards and Technology, 2006.
[53] R.E. Zapolin, Remote terminal industrial control communication system, 1992, US Patent 5,122,948.
[54] M. Geilen, S. Tripakis, M. Wiggers, The earlier the better: a theory of timed actor interfaces, in: Proceedings of the 14th International Conference on Hybrid Systems: Computation and Control, ACM, 2011, pp. 23–32.
[55] P.A. Vicaire, E. Hoque, Z. Xie, J.A. Stankovic, Bundle: a group-based programming abstraction for cyber-physical systems, IEEE Trans. Ind. Inform. 8 (2) (2012) 379–392.
[56] A. Canedo, E. Schwarzenbach, M.A. Al Faruque, Context-sensitive synthesis of executable functional models of cyber-physical systems, in: Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, ACM, 2013, pp. 99–108.
[57] Z. Zhang, J. Porter, E. Eyisi, G. Karsai, X. Koutsoukos, J. Sztipanovits, Co-simulation framework for design of time-triggered cyber physical systems, in: Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, ACM, 2013, pp. 119–128.
[58] 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 Gener. Comput. Syst. 56 (2016) 449–475.
[59] Y. Tan, M.C. Vuran, S. Goddard, Y. Yu, M. Song, S. Ren, A concept lattice-based event model for cyber-physical systems, in: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, ACM, 2010, pp. 50–60.
[60] R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine, The algorithmic analysis of hybrid systems, Theor. Comput. Sci. 138 (1) (1995) 3–34.
[61] P.J. Antsaklis, J.A. Stiver, M. Lemmon, Hybrid system modeling and autonomous control systems, in: Hybrid Systems, Springer, 1992, pp. 366–392.
[62] Y. Yalei, Z. Xingshe, Cyber-physical systems modeling based on extended hybrid automata, in: 2013 International Conference on Computational and Information Sciences, IEEE, 2013, pp. 1871–1874.
[63] A. Benveniste, T. Bourke, B. Caillaud, M. Pouzet, Hybrid systems modeling challenges caused by cyber-physical systems, Cyber-Phys. Syst. (CPS) Found. Chall. (2013). Available on-line: http://people.rennes.inria.fr/Albert.Benveniste/pub/NIST2012.pdf
[64] P. Kumar, D. Goswami, S. Chakraborty, A. Annaswamy, K. Lampka, L. Thiele, A hybrid approach to cyber-physical systems verification, in: DAC Design Automation Conference 2012, IEEE, 2012, pp. 688–696.
[65] T. Tidwell, X. Gao, H.-M. Huang, C. Lu, S. Dyke, C. Gill, Towards configurable real-time hybrid structural testing: a cyber-physical system approach, in: 2009 IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, IEEE, 2009, pp. 37–44.
[66] M. Jianhui, Event driven monitoring of cyber-physical systems based on hybrid automata, Natl. Univ. Defense Technol. Changsha (2011).
[67] C.-W. Ten, C.-C. Liu, G. Manimaran, Vulnerability assessment of cybersecurity for SCADAsystems, IEEE Trans. Power Syst. 23 (4) (2008) 1836–1846.
[68] R. Godreau, SCADA systems and their vulnerabilities within the Smart Grid: Can they be defended from a cyber attack, Utica College, 2013 Ph.D. thesis.
[69] K. Coffey, R. Smith, L. Maglaras, H. Janicke, Vulnerability analysis of network scanning on SCADAsystems, Secur. Commun. Netw. 2018 (2018).
[70] F.M. Cleveland, Cyber security issues for advanced metering infrasttructure (AMI), in: Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, IEEE, 2008, pp. 1–5.
[71] A.R. Metke, R.L. Ekl, Smart grid security technology, in: Innovative Smart Grid Technologies (ISGT), 2010, IEEE, 2010, pp. 1–7.
[72] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al., Comprehensive experimental analyses of automotive attack surfaces., in: USENIX Security Symposium, San Francisco, 2011, pp. 77–92.

[73] M. Rushanan, A.D. Rubin, D.F. Kune, C.M. Swanson, Sok: security and privacy in implantable medical devices and body area networks, in: 2014 IEEE Symposium on Security and Privacy (SP), IEEE, 2014, pp. 524–539.
[74] R. de Oliveira Albuquerque, L.J.G. Villalba, A.L.S. Orozco, R.T. de Sousa Júnior, T.-H. Kim, Leveraging information security and computational trust for cybersecurity, J. Supercomput. 72 (10) (2016) 3729–3763.
[75] K. Munro, Deconstructing flame: the limitations of traditional defences, Comput. Fraud Secur. 2012 (10) (2012) 8–11.
[76] B. Miller, D. Rowe, A survey SCADA of and critical infrastructure incidents, in: Proceedings of the 1st Annual Conference on Research in Information Technology, ACM, 2012, pp. 51–56.
[77] P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Secur. Priv. 7 (3) (2009) 75–77.
[78] J. Vávra, M. Hromada, An evaluation of cyber threats to industrial control systems, in: International Conference on Military Technologies (ICMT) 2015, IEEE, 2015, pp. 1–5.
[79] D. Halperin, T.S. Heydt-Benjamin, K. Fu, T. Kohno, W.H. Maisel, Security and privacy for implantable medical devices, IEEE Perv. Comput. (1) (2008) 30–39.
[80] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. Mullen–Fortino, S. Park, A. Roederer, et al., Challenges and research directions in medical cyber-physical systems, Proc. IEEE 100 (1) (2012) 75–90.
[81] R. Brooks, S. Sander, J. Deng, J. Taiber, Automotive system security: challenges and state-of-the-art, in: Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, ACM, 2008, p. 26.
[82] H. Zeynal, M. Eidiani, D. Yazdanpanah, Intelligent substation automation systems for robust operation of smart grids, in: 2014 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA), IEEE, 2014, pp. 786–790.
[83] T.M. Chen, J.C. Sanchez-Aarnoutse, J. Buford, Petri net modeling of cyber–physical attacks on smart grid, IEEE Trans. Smart Grid 2 (4) (2011) 741–749.
[84] S.M. Amin, Securing the electricity grid, Bridge 40 (1) (2010) 19–20.
[85] T. Force, Final report on the august 14, 2003 blackout in the United States and Canada: Causes and recommendations, US-Canada power system outage task force, 2004.
[86] Y.-S. Eun, J.S. Aßmann, Cyberwar: taking stock of security and warfare in the digital age, Int. Stud. Perspect. 17 (3) (2016) 343–360.
[87] C.M. Davidson, M.J. Santorelli, Realizing the smart grid imperative, 2011.
[88] J. Moteff, Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Library of Congress Washington DC Congressional Research Service, 2005.
[89] B. Zhu, A. Joseph, S. Sastry, A taxonomy of cyber attacks on SCADA systems, in: 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, IEEE, 2011, pp. 380–388.
[90] T. Nash, Backdoors and holes in network perimeters, 2005. Online]: http://ics-cert.us-cert.gov/controlsystems
[91] S. Amin, X. Litrico, S. Sastry, A.M. Bayen, Cyber security of water SCADA systems-part I: Analysis and experimentation of stealthy deception attacks, IEEE Trans. Control Syst. Technol. 21 (5) (2012) 1963–1970.
[92] E. Byres, J. Lowe, The myths and facts behind cyber security risks for industrial control systems, in: Proceedings of the VDE Kongress, 116, 2004, pp. 213–218.
[93] S. Amin, G.A. Schwartz, A. Hussain, In quest of benchmarking security risks to cyber-physical systems, IEEE Netw. 27 (1) (2013) 19–24.
[94] E. Iasiello, Cyber attack: a dull tool to shape foreign policy, in: 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE, 2013, pp. 1–18.
[95] V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G.P. Hancke, Smart grid technologies: communication technologies and standards, IEEE Trans. Ind. Inform. 7 (4) (2011) 529–539.
[96] J.W. Jorgensen, Transmission control protocol/internet protocol (TCP/IP) packet-centric wireless point to multi-point (PTMP) transmission system architecture, 2005, US Patent 6,862,622.
[97] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of cyber-warfare, Comput. Secur. 31 (4) (2012) 418–436.
[98] R. Srinivasan, Rpc: remote procedure call protocol specification version 2 (1995).
[99] M. Dondo, J. Risto, R. Sawilla, Reliability of exploits and consequences for decision support, Tech. Rep. (2015) 1–16.
[100] S. Karnouskos, Stuxnet worm impact on industrial cyber-physical system security, in: IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2011, pp. 4490–4494.
[101] T.M. Chen, S. Abu-Nimeh, Lessons from stuxnet, Computer 44 (4) (2011) 91–93.
[102] B. Bencsáth, G. Pék, L. Buttyán, M. Felegyhazi, The cousins of stuxnet: duqu, flame, and gauss, Future Internet 4 (4) (2012) 971–1003.
[103] B. Bencsáth, G. Ács-Kurucz, G. Molnár, G. Vaspöri, L. Buttyán, R. Kamarás, Duqu 2.0: a comparison to duqu, Budapest. Retriev. 27 (February 2015) 2016.
[104] B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi, Duqu: a stuxnet-like malware found in the wild, CrySyS Lab Tech. Rep. 14 (2011) 1–60.
[105] D. Storm, Gauss malware: nation-state cyber-espionage banking trojan related to flame, stuxnet, Computerworld 9 (2012).
[106] A. Leedom, Stuxnet-risk & uncertainty in the first salvo of global cyber warfare, SAIS Europe J. Glob. Aff. (2016).
[107] R. Chavez, W. Kranich, A. Casella, Red october and its reincarnation, Bost. Univ.| CS558 Netw. Secur (2015).
[108] H. Mwiki, T. Dargahi, A. Dehghantanha, K.-K.R. Choo, Analysis and triage of advanced hacking groups targeting western countries critical national infrastructure: Apt28, red october, and regin, in: Critical Infrastructure Security and Resilience, Springer, 2019, pp. 221–244.
[109] S. Zhioua, The middle east under malware attack dissecting cyber weapons, in: 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops, IEEE, 2013, pp. 11–16.
[110] Z. Dehlawi, N. Abokhodair, Saudi arabia's response to cyber conflict: a case study of the shamoon malware incident, in: 2013 IEEE International Conference on Intelligence and Security Informatics, IEEE, 2013, pp. 73–75.
[111] A. Alabdulatif, Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia, 2018 Ph.D. thesis.
[112] K. Geers, D. Kindlund, N. Moran, R. Rachwald, World war c: understanding nation-state motives behind today's advanced cyber attacks, Tech. Rep., FireEye, Milpitas, CA, USA, Sep 2014.
[113] G. Wangen, The role of malware in reported cyber espionage: a review of the impact and mechanism, Information 6 (2) (2015) 183–211.
[114] M. Gaietta, The Trajectory of Iran's Nuclear Program, Springer, 2016.
[115] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, Inside the slammer worm, IEEE Secur. Priv. (4) (2003) 33–39.
[116] A. Simmonds, P. Sandilands, L. Van Ekert, An ontology for network security attacks, in: Asian Applied Computing Conference, Springer, 2004, pp. 317–323.
[117] G. Francia III, D. Thornton, T. Brookshire, Cyberattacks on SCADA systems, in: Proc. 16th Colloquium Inf. Syst. Security Educ, 2012, pp. 9–14.
[118] P.S. Ryan, War, peace, or stalemate: wargames, wardialing, wardriving, and the emerging market for hacker ethics, Va. JL Tech. 9 (2004) 1.
[119] H. Demirci, A.A. Selçuk, A meet-in-the-middle attack on 8-round AES, in: International Workshop on Fast Software Encryption, Springer, 2008, pp. 116–126.
[120] A. D'Amico, C. Verderosa, C. Horn, T. Imhof, Integrating physical and cyber security resources to detect wireless threats to critical infrastructure, in: Technologies for Homeland Security (HST), 2011 IEEE International Conference on, IEEE, 2011, pp. 494–500.
[121] G. Francia III, D. Thornton, T. Brookshire, Wireless vulnerability of SCADA systems, in: Proceedings of the 50th Annual Southeast Regional Conference, ACM, 2012, pp. 331–332.
[122] T. Paukatong, SCADA security: a new concerning issue of an in-house egat-SCADA, in: Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES, IEEE, 2005, pp. 1–5.
[123] I.N. Fovino, A. Carcano, M. Masera, A. Trombetta, An experimental investigation of malware attacks on SCADA systems, Int. J. Critical Infrastruct. Prot. 2 (4) (2009) 139–145.
[124] R. Tsang, Cyberthreats, vulnerabilities and attacks on scada networks, University of California, Berkeley, Working Paper, 2010. http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf(as of Dec. 28, 2011)
[125] P. Huitsing, R. Chandia, M. Papa, S. Shenoi, Attack taxonomies for the modbus protocols, Int. J. Critical Infrastruct. Prot. 1 (2008) 37–44.
[126] D. Mashima, A.A. Cárdenas, Evaluating electricity theft detectors in smart grid networks, in: International Workshop on Recent Advances in Intrusion Detection, Springer, 2012, pp. 210–229.
[127] W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges, Comput. Netw. 57 (5) (2013) 1344–1371.
[128] R. Santamarta, Here be backdoors: a journey into the secrets of industrial firmware, Black Hat USA (2012).
[129] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu, They can hear your heartbeats: non-invasive security for implantable medical devices, in: ACM SIGCOMM Computer Communication Review, 41, ACM, 2011, pp. 2–13.
[130] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W.H. Maisel, Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses, in: Security and Privacy, 2008. SP 2008. IEEE Symposium on, IEEE, 2008, pp. 129–142.
[131] J. Radcliffe, Hacking medical devices for fun and insulin: breaking the human SCADA system, in: Black Hat Conference Presentation Slides, 2011, 2011.
[132] U.E. Larson, D.K. Nilsson, Securing vehicles against cyber attacks, in: Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, ACM, 2008, p. 30.
[133] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al., Experimental security analysis of a modern automobile, in: Security and Privacy (SP), 2010 IEEE Symposium on, IEEE, 2010, pp. 447–462.
[134] R.M. Ishtiaq Roufa, H. Mustafaa, S.O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, I. Seskarb, Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study, in: 19th USENIX Security Symposium, Washington DC, 2010, pp. 11–13.
[135] D. MacDonald, S.L. Clements, S.W. Patrick, C. Perkins, G. Muller, M.J. Lancaster, W. Hutton, Cyber/physical security vulnerability assessment integration, in: Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES, IEEE, 2013, pp. 1–6.
[136] Y. Mo, T.H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber–physical security of a smart grid infrastructure, Proc. IEEE 100 (1) (2012) 195–209.

[137] H. He, J. Yan, Cyber-physical attacks and defences in the smart grid: a survey, IET Cyber-Phys. Syst. 1 (1) (2016) 13–27.
[138] H. Fawzi, P. Tabuada, S. Diggavi, Secure estimation and control for cyber–physical systems under adversarial attacks, IEEE Trans. Autom. Control 59 (6) (2014) 1454–1467.
[139] M.N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z.Z. Abidin, N.S. Ali, K.H. Abdulkareem, Cyber-security incidents: a review cases in cyber-physical systems, Int. J. Adv. Comput. Sci. Appl. 9 (1) (2018) 499–508.
[140] D. Albright, P. Brannan, C. Walrond, Stuxnet malware and natanz: update of isis december 22, 2010 report, Inst. Sci. Int. Secur. 15 (2011) 739883–739893.
[141] J. Slay, M. Miller, Lessons learned from the maroochy water breach, in: International Conference on Critical Infrastructure Protection, Springer, 2007, pp. 73–82.
[142] L. Fillatre, I. Nikiforov, P. Willett, et al., Security of SCADA systems against cyber–physical attacks, IEEE Aerosp. Electron. Syst. Mag. 32 (5) (2017) 28–45.
[143] M.J. Credeur, Fbi probes georgia water plant break-in on terror concern, 2013.
[144] F.Y. Rashid, Telvent hit by sophisticated cyber-attack, SCADA admin tool compromised, Retrieved from SecurityWeek website:http://www.securityweek.com/telvent-hit-sophisticated-cyber-attack-scada-admin-tool-compromised (2012).
[145] B. Krebs, Cyber incident blamed for nuclear power plant shutdown, Washington Post 5 (2008) June2008.
[146] T. Flick, J. Morehouse, Securing the Smart Grid: Next Generation Power Grid Security, Elsevier, 2010.
[147] L. Ray, Cyber-physical systems: an overview of design process, applications, and security, in: Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications, IGI Global, 2020, pp. 128–150.
[148] M. Chorać, R. Kozik, A. Flizikowski, W. Hołubowicz, R. Renk, Cyber threats impacting critical infrastructures, in: Managing the Complexity of Critical Infrastructures, Springer, Cham, 2016, pp. 139–161.
[149] T. Kiravuo, M. Särelä, J. Manner, Weapons against cyber-physical targets, in: 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops, IEEE, 2013, pp. 321–326.
[150] Y.Y. Haimes, Risk of terrorism to cyber-physical and organizational-societal infrastructures, Public Works Manag. Policy 6 (4) (2002) 231–240.
[151] A. Gupta, M. Kumar, S. Hansel, A.K. Saini, Future of all technologies-the cloud and cyber physical systems, Future 2 (2) (2013).
[152] A. Yeboah-ofori, J.-D. Abdulai, F. Katsriku, Cybercrime and risks for cyber physical systems: a review (2018).
[153] K. Alenius, M. Warren, An exceptional war that ended in victory for estonia or an ordinary e-disturbance? Estonian narratives of the cyber-attacks in 2007, in: Institute Ecole Supérieure en Informatique Electronique et Automatique, Laval, France 5-6 July 2012 Edited by, 2012, p. 18.
[154] M. Kaeo, Cyber attacks on estonia: short synopsis, Double Shot Security. http://www.doubleshotsecurity.com/pdf/NANOG_eesti.pdf (accessed 18 July 2009) (2007).
[155] G.T. Donovan Jr., Russian Operational Art in the Russo-Georgian War of 2008, Technical Report, ARMY WAR COLL CARLISLE BARRACKS PA, 2009.
[156] M.M. Saudi, S. Sukardi, N.A.A.A. Aziz, A. Ahmad, M. Husainiamer, Malware classification for cyber physical system (CPS) based on phylogenetics.
[157] A. Yeboah-Ofori, J.-D. Abdulai, F. Katsriku, Cybercrime and risks for cyber physical systems 2019., Int. J. Cyber-Secur. Digital Forensics 8 (1) (2019) 43–58.
[158] K. Barakat, Does Lebanon possess the capabilities to defend itself from cyber-theats? Learning from Estonia's experience.(c2019), Lebanese American University, 2019 Ph.D. thesis.
[159] A.J. Hejase, H.J. Hejase, J.A. Hejase, Cyber warfare awareness in lebanon: exploratory research, Int. J. Cyber-Secur. Digital Forensics (IJCSDF) 4 (4) (2015) 482–497.
[160] T. Abera, N. Asokan, L. Davi, J.-E. Ekberg, T. Nyman, A. Paverd, A.-R. Sadeghi, G. Tsudik, C-flat: control-flow attestation for embedded systems software, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 743–754.
[161] D.D. Chen, M. Woo, D. Brumley, M. Egele, Towards automated dynamic analysis for linux-based embedded firmware., NDSS, 2016.
[162] A. Francillon, C. Castelluccia, Code injection attacks on harvard-architecture devices, in: Proceedings of the 15th ACM Conference on Computer and Communications Security, ACM, 2008, pp. 15–26.
[163] R. Roemer, E. Buchanan, H. Shacham, S. Savage, Return-oriented programming: systems, languages, and applications, ACM Trans. Inf. Syst. Secur. (TISSEC) 15 (1) (2012) 2.
[164] H. Alemzadeh, D. Chen, X. Li, T. Kesavadas, Z.T. Kalbarczyk, R.K. Iyer, Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation, in: Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on, IEEE, 2016, pp. 395–406.
[165] H. Hu, S. Shinde, S. Adrian, Z.L. Chua, P. Saxena, Z. Liang, Data-oriented programming: on the expressiveness of non-control data attacks, in: Security and Privacy (SP), 2016 IEEE Symposium on, IEEE, 2016, pp. 969–986.
[166] V.N. Gudivada, S. Ramaswamy, S. Srinivasan, Data management issues in cyber-physical systems, in: Transportation Cyber-Physical Systems, Elsevier, 2018, pp. 173–200.
[167] G. Loukas, Cyber-Physical Attacks: A Growing Invisible Threat, Butterworth-Heinemann, 2015.
[168] L. Davi, A. Dmitrienko, A.-R. Sadeghi, M. Winandy, Privilege escalation attacks on android, in: International Conference on Information Security, Springer, 2010, pp. 346–360.
[169] J. Owens, J. Matthews, A study of passwords and methods used in brute-force SSH attacks, USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008.
[170] A. Narayanan, V. Shmatikov, Fast dictionary attacks on passwords using time-space tradeoff, in: Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM, 2005, pp. 364–372.
[171] D.P. Jablon, Extended password key exchange protocols immune to dictionary attack, in: Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE, 1997, pp. 248–255.
[172] P. Papantonakis, D. Pnevmatikatos, I. Papaefstathiou, C. Manifavas, Fast, FPGA-based rainbow table creation for attacking encrypted mobile communications, in: 2013 23rd International Conference on Field programmable Logic and Applications, IEEE, 2013, pp. 1–6.
[173] M. Bellare, T. Kohno, Hash function balance and its impact on birthday attacks, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2004, pp. 401–418.
[174] P.G. Kelley, S. Komanduri, M.L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L.F. Cranor, J. Lopez, Guess again (and again and again): measuring password strength by simulating password-cracking algorithms, in: 2012 IEEE Symposium on Security and Privacy, IEEE, 2012, pp. 523–537.
[175] N. Provos, M. Friedl, P. Honeyman, Preventing privilege escalation., USENIX Security Symposium, 2003.
[176] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, A.-R. Sadeghi, Xmandroid: a new android evolution to mitigate privilege escalation attacks, Technical Report TR-2011-04, Technische Universität Darmstadt, 2011.
[177] M. Al-Shurman, S.-M. Yoo, S. Park, Black hole attack in mobile ad hoc networks, in: Proceedings of the 42nd Annual Southeast Regional Conference, 2004, pp. 96–97.
[178] P. Solankar, S. Pingale, R. Parihar, Denial of service attack and classification techniques for attack detection, Int. J. Comput. Sci. Inf. Technol. 6 (2) (2015) 1096–1099.
[179] F. Yihunie, E. Abdelfattah, A. Odeh, Analysis of ping of death DoS and DDoS attacks, in: 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), IEEE, 2018, pp. 1–4.
[180] S. Kumar, Smurf-based distributed denial of service (DDoS) attack amplification in internet, in: Second International Conference on Internet Monitoring and Protection (ICIMP 2007), IEEE, 2007, p. 25.
[181] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, S. Sezer, Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid, in: 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, 2016, pp. 53–63.
[182] A. Cherepanov, R. Lipovsky, Blackenergy–what we really know about the notorious cyber attacks, Virus Bull. (October 2016).
[183] E. Kovacs, Blackenergy malware used in ukraine power grid attacks, 2016.
[184] J. Lemon, et al., Resisting SYN flood DoS attacks with a SYN cache, in: BSDCon, 2002, 2002, pp. 89–97.
[185] D. Antonioli, G. Bernieri, N.O. Tippenhauer, Taking control: design and implementation of botnets for cyber-physical attacks with cpsbot, arXiv:1802.00152(2018).
[186] K.I. Sgouras, A.N. Kyriakidis, D.P. Labridis, Short-term risk assessment of botnet attacks on advanced metering infrastructure, IET Cyber-Phys. Syst. 2 (3) (2017) 143–151.
[187] F. Shrouf, J. Ordieres, G. Miragliotta, Smart factories in industry 4.0: a review of the concept and of energy management approached in production based on the internet of things paradigm, in: Industrial Engineering and Engineering Management (IEEM), 2014 IEEE International Conference on, IEEE, 2014, pp. 697–701.
[188] L. De Carli, R. Torres, G. Modelo-Howard, A. Tongaonkar, S. Jha, Botnet protocol inference in the presence of encrypted traffic, in: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, IEEE, 2017, pp. 1–9.
[189] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, Ddos in the IoT: mirai and other botnets, Computer 50 (7) (2017) 80–84.
[190] J. Seering, J.P. Flores, S. Savage, J. Hammer, The social roles of bots: evaluating impact of bots on discussions in online communities, Proc.ACM Hum. Comput. Interact. 2 (CSCW) (2018) 1–29.
[191] P. Rascagneres, E. Willems, Regin, an old but sophisticated cyber espionage toolkit platform (2016).
[192] K. Zdravkova, Reconsidering human dignity in the new era, New Ideas Psychol. 54 (2019) 112–117.
[193] V. Boinapally, G. Hsieh, K.S. Nauer, Building a Gh0st malware experimentation environment, in: Proceedings of the International Conference on Security and Management (SAM), The Steering Committee of The World Congress in Computer Science, Computer, 2017, pp. 89–95.
[194] S. Murdoch, N. Leaver, Anonymity vs. trust in cyber-security collaboration, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, 2015, pp. 27–29.
[195] L. Hendraningrat, S. Li, O. Torsæter, A coreflood investigation of nanofluid enhanced oil recovery, J. Pet. Sci. Eng. 111 (2013) 128–138.
[196] B. Farinholt, M. Rezaeirad, P. Pearce, H. Dharmdasani, H. Yin, S. Le Blond, D. McCoy, K. Levchenko, To catch a ratter: monitoring the behavior of amateur darkcomet rat operators in the wild, in: 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 770–787.
[197] S. Hilt, L.A. Remorin, How cybercriminals can abuse chat platform APIs as C&C infrastructures.
[198] A. Gostev, R. Unuchek, M. Garnaeva, D. Makrushin, A. Ivanov, It threat evolution in q1 2016, Kapersky 2015 Report, Kapersky L, 2016.

[199] J. Cowie, A. Ogielski, B. Premore, Y. Yuan, Global routing instabilities triggered by Code Red II and Nimda worm attacks, Technical Report, Tech. Rep., Renesys Corporation, 2001.
[200] A. Machie, J. Roculan, R. Russell, M. Velzen, Nimda worm analysis, Technical Report, Tech. Rep., Incident Analysis, SecurityFocus, 2001.
[201] A.A. Di Pinto, Y. Dragoni, A. Carcano, Triton: the first ICS cyber attack on safety instrument systems, in: Proc. Black Hat USA, 2018, pp. 1–26.
[202] R. Prasad, V. Rohokale, Malware, in: Cyber Security: The Lifeline of Information and Communication Technology, Springer, 2020, pp. 67–81.
[203] D. Desai, T. Haq, Blackhole exploit kit: rise & evolution, Malware Research Team Technical Paper, 2012.
[204] N. Adams, R. Chisnall, C. Pickering, S. Schauer, How port security has to evolve to address the cyber-physical security threat: lessons from the SAURON project, Int. J. Transp. Dev. Integr. 4 (1) (2020) 29–41.
[205] J. Twist, Cyber threat report 16 jan-31 jan 2018(2018).
[206] M. Marquis-Boire, M. Marschalek, C. Guarnieri, Big Game Hunting: The Peculiarities in Nation-State Malware Research, Black Hat, Las Vegas, NV, USA, 2015.
[207] M. Marquis-Boire, B. Marzcak, C. Guarnieri, The smartphone who loved me: finfisher goes mobile(2012).
[208] J.E. Sullivan, D. Kamensky, How cyber-attacks in ukraine show the vulnerability of the us power grid, Electr. J. 30 (3) (2017) 30–35.
[209] D. Byrne, C. Thorpe, Jigsaw: an investigation and countermeasure for ransomware attacks, in: European Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2017, pp. 656–665.
[210] S.I. Popoola, S.O. Ojewande, F.O. Sweetwilliams, S. John, A. Atayero, et al., Ransomware: current trend, challenges, and research directions, 2017.
[211] M.A. Branquinho, Ransomware in industrial control systems. what comes after wannacry and Petya global attacks? WIT Trans. Built Environ. 174 (2018) 329–334.
[212] J.S. Aidan, H.K. Verma, L.K. Awasthi, Comprehensive survey on Petya ransomware attack, in: 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), IEEE, 2017, pp. 122–125.
[213] A.S. Petrenko, S.A. Petrenko, K.A. Makoveichuk, P.V. Chetyrbok, Protection model of pcs of subway from attacks type «wanna cry»,«petya» and «bad rabbit» IoT, in: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), IEEE, 2018, pp. 945–949.
[214] R. Brewer, Ransomware attacks: detection, prevention and cure, Netw. Secur. 2016 (9) (2016) 5–9.
[215] K. Poulsen, Slammer worm crashed ohio nuke plant network, 2003. http://www.securityfocus.com/news/6767
[216] J.D. Rogers, C.M. Watkins, Overview of the Taum Sauk pumped storage power plant upper reservoir failure, Reynolds county, MO (2008).
[217] S. Gorman, Electricity grid in us penetrated by spies, Wall Street J. 8 (2009).
[218] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, S. Todt, Infiltrating Critical Infrastructures with Next-Generation Attacks, Fraunhofer Institute for Secure Information Technology (SIT), Munich, 2010.
[219] T. FoxBrewster, Ukraine claims hackers caused christmas power outage, Forbes Secur. (2016).
[220] P. Katerynchuk, Challenges and threats of Ukraine's national cyber security in hybrid war, *Вісник Маріупольського державного університету. Серія: Історія. Політологія* 21 (2018) 166–173.
[221] V. Zhoghov, The ransomware "Petya" as a challenge to the cybersecurity of Ukraine, main factors of spreading this virus in the focus of Ukraine, the steps taken by the authorities to combat this phenomenon and suggest ways to improve such activities using experience of other countries, Victor Zhoghov The ransomware "Petya" as a challenge to the cybersecurity of, 2017 Ph.D. thesis.
[222] 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) 11–33.
[223] T. Johnson, Fault-tolerant distributed cyber-physical systems: Two case studies, 2010.
[224] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, et al., Challenges for securing cyber physical systems, Workshop on Future Directions in Cyber-Physical Systems Security, 5, 2009.
[225] G. Dondossola, Risk assessment of information and communication systems–analysis of some practices and methods in the electric power industry, CIGRÉ Electra (2008).
[226] C.M. Krishna, I. Koren, Adaptive fault-tolerance fault-tolerance for cyber-physical systems, in: Computing, Networking and Communications (ICNC), 2013 International Conference on, IEEE, 2013, pp. 310–314.
[227] J. Zalewski, S. Drager, W. McKeever, A.J. Kornecki, Threat modeling for security assessment in cyberphysical systems, in: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, ACM, 2013, p. 10.
[228] T. Lu, B. Xu, X. Guo, L. Zhao, F. Xie, A new multilevel framework for cyber–physical system security, First International Workshop on the Swarm at the Edge of the Cloud, 2013.
[229] T. Lu, J. Lin, L. Zhao, Y. Li, Y. Peng, An analysis of cyber physical system security theories, in: 2014 7th International Conference on Security Technology, IEEE, 2014, pp. 19–21.
[230] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, F. Xie, Cyber-physical system risk assessment, in: 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2013, pp. 442–447.
[231] A.M. Gamundani, An impact review on internet of things attacks, in: 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), IEEE, 2015, pp. 114–118.
[232] K. Stouffer, J. Falco, K. Scarfone, Guide to industrial control systems (ICS) security, NIST Spec. Publ. 800 (82) (2011) 16.
[233] N. Virvilis, D. Gritzalis, The big four-what we did wrong in advanced persistent threat detection? in: Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, IEEE, 2013, pp. 248–254.
[234] M. Jouini, L.B.A. Rabai, A.B. Aissa, Classification of security threats in information systems, Procedia Comput. Sci. 32 (2014) 489–496.
[235] A. Ahmad, Type of security threats and it's prevention, Int. J. Comput. Technol. Appl. 3 (2) (2012) 750–752.
[236] S. Ruffle, F. Caccioli, A. Coburn, S. Kelly, B. Leslie, D. Ralph, Stress test scenario: sybil logic bomb cyber catastrophe, in: Cambridge Risk Framework series, Centre for Risk Studies, University of Cambridge, Cambridge Centre for Risk Studies, University of Cambridge Judge Business School, 2014, pp. 1–45.
[237] R. Rajkumar, I. Lee, L. Sha, J. Stankovic, Cyber-physical systems: the next computing revolution, in: Design Automation Conference (DAC), 2010 47th ACM/IEEE, IEEE, 2010, pp. 731–736.
[238] A.N. Kandhil, A study on secure shell (SSH) protocol.
[239] K. Yang, D. Blaauw, D. Sylvester, Hardware designs for security in ultra-low-power IoTsystems: an overview and survey, IEEE Micro 37 (6) (2017) 72–89.
[240] A. Scarfo, New security perspectives around BYOD, in: 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, IEEE, 2012, pp. 446–451.
[241] X. Keystone, C. ENTRIX, Comments of the sierra club, et al., to the department of state on the supplemental draft environmental impact statement for the transcanada keystone xl pipeline.
[242] S. Girgin, E. Krausmann, Historical analysis of us onshore hazardous liquid pipeline accidents triggered by natural hazards, J. Loss Prevent. Process Ind. 40 (2016) 578–590.
[243] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, K. Ueda, Cyber-physical systems in manufacturing, CIRP Ann. 65 (2) (2016) 621–641.
[244] Z. Drias, A. Serhrouchni, O. Vogel, Analysis of cyber security for industrial control systems, in: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), IEEE, 2015, pp. 1–8.
[245] W. Zhao, F. Xie, Y. Peng, Y. Gao, X. Han, H. Gao, D. Wang, Security testing methods and techniques of industrial control devices, in: 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2013, pp. 433–436.
[246] D. Rhoades, Achilles - the world's first man-in-the-middle web security tool, (https://www.mavensecurity.com/about/achilles).
[247] D. Reading, Breakingpoint unveils firestorm cyber tomography, 2011, (https://www.darkreading.com/risk/breakingpoint-unveils-firestorm-cyber-tomography-machine/d/d-id/1135182).
[248] R. Nishimura, R. Kurachi, K. Ito, T. Miyasaka, M. Yamamoto, M. Mishima, Implementation of the CAN-FD protocol in the fuzzing tool beSTORM, in: 2016 IEEE International Conference on Vehicular Electronics and Safety (ICVES), IEEE, 2016, pp. 1–6.
[249] A. MacFarland, Codenomicon defensics finds risks that lurk in your protocols, august 16, 2007, The Clipper Group Navigator, Report# TCG20070811–3.
[250] Mu studio performance suite, (https://www.slideshare.net/aquaphlex/mu-studio-performance-suite).
[251] M. Eddington, Peach fuzzing platform, Peach Fuzzer 34 (2011).
[252] G. Devarajan, Unraveling scada protocols: using sulley fuzzer, Defon 15 Hacking Conf, 2007.
[253] D. Aitel, An introduction to spike, the fuzzer creation kit, Presentation Slides, 1, Aug 2002.
[254] exida certification - IEC 61508, IEC 61511, IEC 62443, ISO 26262, CFSE, 2015, (https://www.exida.com/Certification).
[255] Isasecure - IEC 62443-4-2 - EDSA certification, 2018, (https://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification).
[256] S. Belguith, N. Kaaniche, G. Russello, Pu-abe: lightweight attribute-based encryption supporting access policy update for cloud assisted IoT, in: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), IEEE, 2018, pp. 924–927.
[257] S. Belguith, N. Kaaniche, M. Mohamed, G. Russello, C-ABSC: cooperative attribute based signcryption scheme for internet of things applications, in: 2018 IEEE International Conference on Services Computing (SCC), IEEE, 2018, pp. 245–248.
[258] A.O. Moyegun, Information Security and Innovation; Guide to Secure Technology Innovation Initiatives, 2016 Ph.D. thesis.
[259] N. Kaaniche, M. Laurent, Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms, Comput. Commun. 111 (2017) 120–141.
[260] J. Rajamäki, P. Rathod, A. Ahlgren, J. Aho, M. Takari, S. Ahlgren, Resilience of cyber-physical system: a case study of safe school environment, in: Intelligence and Security Informatics Conference (EISIC), 2012 European, IEEE, 2012, p. 285.
[261] V. Fuhrmans, Virus attacks siemens plant-control systems, Wall Street J. (2010).

[262] E. Mills, Hackers broke into faa air traffic control system, Wall Street J. Page A 6 (2009) 2009.
[263] A. Rajhans, S.-W. Cheng, B. Schmerl, D. Garlan, B.H. Krogh, C. Agbi, A. Bhave, An architectural approach to the design and analysis of cyber-physical systems, Electron. Commun. EASST 21 (2009).
[264] S. Deshmukh, B. Natarajan, A. Pahwa, State estimation in spatially distributed cyber-physical systems: bounds on critical measurement drop rates, in: Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on, IEEE, 2013, pp. 157–164.
[265] K. Van Brabant, et al., Operational Security Management in Violent Environments, Overseas Development Institute London, 2000.
[266] T. Aven, Risk assessment and risk management: review of recent advances on their foundation, Eur. J. Oper. Res. 253 (1) (2016) 1–13.
[267] C. Shepherd, G. Arfaoui, I. Gurulian, R.P. Lee, K. Markantonakis, R.N. Akram, D. Sauveron, E. Conchon, Secure and trusted execution: past, present, and future-a critical review in the context of the internet of things and cyber-physical systems, in: Trustcom/BigDataSE/ISPA, 2016 IEEE, IEEE, 2016, pp. 168–177.
[268] H. Almohri, L. Cheng, D. Yao, H. Alemzadeh, On threat modeling and mitigation of medical cyber-physical systems, in: Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2017 IEEE/ACM International Conference on, IEEE, 2017, pp. 114–119.
[269] H.M. Almohri, D.D. Yao, D. Kafura, Process authentication for high system assurance, IEEE Trans. Dependable Secure Comput. 11 (1) (2013) 1.
[270] H.M. Almohri, L.T. Watson, D. Yao, X. Ou, Security optimization of dynamic networks with probabilistic graph modeling and linear programming, IEEE Trans. Dependable Secure Comput. 13 (4) (2016) 474–487.
[271] K.A. Higley, Environmental consequences of the chernobyl accident and their remediation: twenty years of experience. report of the chernobyl forum expert group 'environment' STI/PUB/1239, 2006, international atomic energy agency, Vienna, Austria ISBN: 92-0-114705-8, 166 pp, 40.00 euros (softbound), Radiat. Protect. Dosim. 121 (4) (2006) 476–477.
[272] Y.-H. Koo, Y.-S. Yang, K.-W. Song, Radioactivity release from the Fukushima accident and its consequences: a review, Progr. Nucl. Energy 74 (2014) 61–70.
[273] A. Banerjee, K.K. Venkatasubramanian, T. Mukherjee, S.K.S. Gupta, Ensuring safety, security, and sustainability of mission-critical cyber–physical systems, Proc. IEEE 100 (1) (2011) 283–299.
[274] A.G. Association, et al., Cryptographic protection of SCADA communications part 1: background, policies and test plan, Technical Report, AGA Report, 2005.
[275] M. Kirkpatrick, E. Bertino, F.T. Sheldon, Restricted authentication and encryption for cyber-physical systems, DHS CPS Workshop Restricted Authentication and Encryption for Cyber-Physical Systems, 2009.
[276] 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 (2018) 1674–1683.
[277] 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. Critical Infrastruct. Protect. 11 (2015) 39–50.
[278] M. Sharma, F. Gebali, H. Elmiligi, M. Rahman, Network security evaluation scheme for WSN in cyber-physical systems, in: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), IEEE, 2018, pp. 1145–1151.
[279] M. Zhang, A. Raghunathan, N.K. Jha, Trustworthiness of medical devices and body area networks., Proc. IEEE 102 (8) (2014) 1174–1188.
[280] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J. Robshaw, Y. Seurin, C. Vikkelsoe, Present: an ultra-lightweight block cipher, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2007, pp. 450–466.
[281] J. Borghoff, A. Canteaut, T. Güneysu, E.B. Kavun, M. Knezevic, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, et al., Prince–a low-latency block cipher for pervasive computing applications, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2012, pp. 208–225.
[282] A. Shahzad, M. Lee, Y.-K. Lee, S. Kim, N. Xiong, J.-Y. Choi, Y. Cho, Real time modbus transmissions and cryptography security designs and enhancements of protocol sensitive information, Symmetry 7 (3) (2015) 1176–1210.
[283] M. Hadley, K. Huston, T. Edgar, AGA-12, part 2 performance test results, Pacific Northwest Natl. Lab. (2007).
[284] J. Rubio-Hernán, L. De Cicco, J. Garcia-Alfaro, Revisiting a watermark-based detection scheme to handle cyber-physical attacks, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 21–28.
[285] L. Vegh, L. Miclea, Secure and efficient communication in cyber-physical systems through cryptography and complex event processing, in: 2016 International Conference on Communications (COMM), IEEE, 2016, pp. 273–276.
[286] S. Jayasekara, S. Perera, M. Dayarathna, S. Suhothayan, Continuous analytics on geospatial data streams with wso2 complex event processor, in: Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems, ACM, 2015, pp. 277–284.
[287] S. Perera, S. Sriskandarajah, M. Vivekanandalingam, P. Fremantle, S. Weerawarana, Solving the grand challenge using an opensource CEP engine, in: Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems, ACM, 2014, pp. 288–293.
[288] T. Zhou, J. Shen, X. Li, C. Wang, H. Tan, Logarithmic encryption scheme for cyber–physical systems employing fibonacci q-matrix, Future Gener. Comput. Syst. (2018) 1307–1313.
[289] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETS): status, results, and challenges, Telecommun. Syst. 50 (4) (2012) 217–241.
[290] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, J. Netw. Comput. Appl. 37 (2014) 380–392.
[291] Q. He, N. Zhang, Y. Wei, Y. Zhang, Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems, Comput. Netw. 140 (2018) 163–173.
[292] Y. Zhao, Y. Li, Q. Mu, B. Yang, Y. Yu, Secure pub-sub: blockchain-based fair payment with reputation for reliable cyber physical systems, IEEE Access 6 (2018) 12295–12303.
[293] J. Sepúlveda, S. Liu, J.M.B. Mera, Post-quantum enabled cyber physical systems, IEEE Embed. Syst. Lett. (2019) 106–110.
[294] O.A. Harshe, N.T. Chiluvuri, C.D. Patterson, W.T. Baumann, Design and implementation of a security framework for industrial control systems, in: 2015 International Conference on Industrial Instrumentation and Control (ICIC), IEEE, 2015, pp. 127–132.
[295] T. Cruz, J. Barrigas, J. Proença, A. Graziano, S. Panzieri, L. Lev, P. Simões, Improving network security monitoring for industrial control systems, in: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE, 2015, pp. 878–881.
[296] M.E. Luallen, Sans SCADA and process control security survey, A SANS Whitepaper, February 2013.
[297] A. Ghaleb, S. Zhioua, A. Almulhem, On plc network security, Int. J. Critical Infrastruct. Protect. 22 (2018) 62–69.
[298] H. Cao, P. Zhu, X. Lu, A. Gurtov, A layered encryption mechanism for networked critical infrastructures, IEEE Netw. 27 (1) (2013) 12–18.
[299] S. Amin, G.A. Schwartz, S.S. Sastry, On the interdependence of reliability and security in networked control systems, in: Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on, IEEE, 2011, pp. 4078–4083.
[300] A.A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, S. Sastry, Attacks against process control systems: risk assessment, detection, and response, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 355–366.
[301] T. Alves, R. Das, T. Morris, Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers, IEEE Embed. Syst. Lett. 10 (3) (2018) 99–102.
[302] S. Belguith, N. Kaaniche, M. Hammoudeh, T. Dargahi, Proud: verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IoT applications, Future Gener. Comput. Syst. (2019) 899–918.
[303] N. Kaaniche, M. Laurent, P.-O. Rocher, C. Kiennert, J. Garcia-Alfaro, Pcs, a privacy-preserving certification scheme, in: Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, 2017, pp. 239–256.
[304] N. Kaaniche, Cloud data storage security based on cryptographic mechanisms, 2014 Ph.D. thesis.
[305] R.M. Seepers, J.H. Weber, Z. Erkin, I. Sourdis, C. Strydis, Secure key-exchange protocol for implants using heartbeats, in: Proceedings of the ACM International Conference on Computing Frontiers, ACM, 2016, pp. 119–126.
[306] Z.E. Ankaralı, A.F. Demir, M. Qaraqe, Q.H. Abbasi, E. Serpedin, H. Arslan, R.D. Gitlin, Physical layer security for wireless implantable medical devices, in: Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015 IEEE 20th International Workshop on, IEEE, 2015, pp. 144–147.
[307] S. Ibrokhimov, K.L. Hui, A.A. Al-Absi, M. Sain, et al., Multi-factor authentication in cyber physical system: A state of art survey, in: 2019 21st International Conference on Advanced Communication Technology (ICACT), IEEE, 2019, pp. 279–284.
[308] S. Chen, M. Ma, Z. Luo, An authentication scheme with identity-based cryptography for m2m security in cyber-physical systems, Secur. Commun. Netw. 9 (10) (2016) 1146–1157.
[309] H. Wardak, S. Zhioua, A. Almulhem, Plc access control: a security analysis, in: 2016 World Congress on Industrial Control Systems Security (WCICSS), IEEE, 2016, pp. 1–6.
[310] D. Choi, H. Kim, D. Won, S. Kim, Advanced key-management architecture for secure SCADAcommunications, IEEE Trans. Power Deliv. 24 (3) (2009) 1154–1163.
[311] M. Keshk, N. Moustafa, E. Sitnikova, B. Turnbull, Privacy-preserving big data analytics for cyber-physical systems, Wirel. Netw. (2018) 1–9.
[312] J. Feng, L.T. Yang, R. Zhang, Practical privacy-preserving high-order Bi-Lanczos in integrated edge-fog-cloud architecture for cyber-physical-social systems, ACM Trans. Internet Technol. (TOIT) 19 (2) (2019) 26.
[313] H. Ye, J. Liu, W. Wang, P. Li, T. Li, J. Li, Secure and efficient outsourcing differential privacy data release scheme in cyber–physical system, Future Gener. Comput. Syst. (2018) 1314–1323.
[314] X. Zhang, J. Zhao, L. Mu, Y. Tang, C. Xu, Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber–physical systems, Pervasive Mob. Comput. 56 (2019) 18–28.
[315] Z. Zhang, J. Wu, D. Yau, P. Cheng, J. Chen, Secure Kalman filter state estimation by partially homomorphic encryption, in: 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS), IEEE, 2018, pp. 345–346.
[316] J. Kim, C. Lee, H. Shim, J.H. Cheon, A. Kim, M. Kim, Y. Song, Encrypting controller using fully homomorphic encryption for security of cyber-physical systems, IFAC-PapersOnLine 49 (22) (2016) 175–180.

[317] Z. Min, G. Yang, A.K. Sangaiah, S. Bai, G. Liu, A privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems, EURASIP J. Wirel. Commun. Netw. 2019 (1) (2019) 15.
[318] N. Chakraborty, Intrusion detection system and intrusion prevention system: a comparative study, Int. J. Comput. Bus. Res. (IJCBR) 4 (2013) 2229–6166. ISSN (Online)
[319] X. Shu, D. Yao, N. Ramakrishnan, Unearthing stealthy program attacks buried in extremely long execution paths, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, 2015, pp. 401–413.
[320] K. Xu, K. Tian, D. Yao, B.G. Ryder, A sharper sense of self: probabilistic reasoning of program behaviors for anomaly detection with context sensitivity, in: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, 2016, pp. 467–478.
[321] R. Mitchell, R. Chen, Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, IEEE Trans. Syst. Man. Cybern. 44 (5) (2014) 593–604.
[322] D.I. Urbina, J.A. Giraldo, A.A. Cardenas, N.O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, H. Sandberg, Limiting the impact of stealthy attacks on industrial control systems, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 1092–1105.
[323] S. Sridhar, A. Hahn, M. Govindarasu, et al., Cyber-physical system security for the electric power grid., Proc. IEEE 100 (1) (2012) 210–224.
[324] C. Zimmer, B. Bhat, F. Mueller, S. Mohan, Time-based intrusion detection in cyber-physical systems, in: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, ACM, 2010, pp. 109–118.
[325] R. Mitchell, R. Chen, Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems, IEEE Trans. Dependable Secure Comput. 12 (1) (2015) 16–30.
[326] B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in internet of things, J. Netw. Comput. Appl. 84 (2017) 25–37.
[327] D. Oh, D. Kim, W.W. Ro, A malicious pattern detection engine for embedded security systems in the internet of things, Sensors 14 (12) (2014) 24188–24211.
[328] T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, M.-C. Hsieh, A lightweight intrusion detection scheme based on energy consumption analysis in 6LoWPAN, in: Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Springer, 2014, pp. 1205–1213.
[329] C. Cervantes, D. Poplade, M. Nogueira, A. Santos, Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for internet of things., in: IM, 2015, pp. 606–611.
[330] A.H. Farooqi, F.A. Khan, Intrusion detection systems for wireless sensor networks: A survey, in: Communication and Networking, Springer, 2009, pp. 234–241.
[331] C.S. Hong, T. Tonouchi, Y. Ma, C.-S. Chao, Management enabling the future internet for changing business and new computing services, in: 12th Asia-Pacific Network Operations and Management Symposium, APNOMS 2009 Jeju, South Korea, September 23–25, 2009 Proceedings, 5787, Springer, 2009.
[332] P. Kasinathan, C. Pastrone, M.A. Spirito, M. Vinkovits, Denial-of-service detection in 6LoWPAN based internet of things, in: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2013, pp. 600–607.
[333] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, M.A. Spirito, AnIDS framework for internet of things empowered by 6LoWPAN, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ACM, 2013, pp. 1337–1340.
[334] L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the RPL-based internet of things, Int. J. Distrib. Sensor Netw. 9 (8) (2013) 794326.
[335] A. Le, J. Loo, Y. Luo, A. Lasebae, Specification-basedIDS for securingRPL from topology attacks, in: Wireless Days (WD), 2011 IFIP, IEEE, 2011, pp. 1–3.
[336] A. Le, J. Loo, K.K. Chai, M. Aiash, A specification-basedIDS for detecting attacks on RPL-based network topology, Information 7 (2) (2016) 25.
[337] S. Raza, L. Wallgren, T. Voigt, Svelte: real-time intrusion detection in the internet of things, Ad Hoc Netw. 11 (8) (2013) 2661–2674.
[338] P. Pongle, G. Chavan, Real time intrusion and wormhole attack detection in internet of things, Int. J. Comput. Appl. 121 (9) (2015).
[339] N.K. Thanigaivelan, E. Nigussie, R.K. Kanth, S. Virtanen, J. Isoaho, Distributed internal anomaly detection system for internet-of-things, in: Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual, IEEE, 2016, pp. 319–320.
[340] H.-J. Liao, C.-H.R. Lin, Y.-C. Lin, K.-Y. Tung, Intrusion detection system: a comprehensive review, J. Netw. Comput. Appl. 36 (1) (2013) 16–24.
[341] J.R. Vacca, Computer and Information Security Handbook, Newnes, 2012.
[342] C. Liu, J. Yang, Y. Zhang, R. Chen, J. Zeng, Research on immunity-based intrusion detection technology for the internet of things, in: Natural Computation (ICNC), 2011 Seventh International Conference on, 1, IEEE, 2011, pp. 212–216.
[343] R. Mitchell, I.-R. Chen, A survey of intrusion detection techniques for cyber–physical systems, ACM Comput. Surv. (CSUR) 46 (4) (2014) 55.
[344] I. Butun, S.D. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 266–282.
[345] S. Misra, P.V. Krishna, H. Agarwal, A. Saxena, M.S. Obaidat, A learning automata based solution for preventing distributed denial of service in internet of things, in: Internet of Things (ithings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, IEEE, 2011, pp. 114–122.
[346] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376.
[347] J.P. Amaral, L.M. Oliveira, J.J. Rodrigues, G. Han, L. Shu, Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks, in: Communications (ICC), 2014 IEEE International Conference on, IEEE, 2014, pp. 1796–1801.
[348] H. Debar, An introduction to intrusion-detection systems, Proc. Connect 2002 (2000) 1–18.
[349] K. Scarfone, P. Mell, Guide to intrusion detection and prevention systems (IDPS), NIST Spec. Publ. 800 (2007) (2007) 94.
[350] A. Gupta, O.J. Pandey, M. Shukla, A. Dadhich, S. Mathur, A. Ingle, Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks, in: Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, IEEE, 2013, pp. 1–7.
[351] D.H. Summerville, K.M. Zach, Y. Chen, Ultra-lightweight deep packet anomaly detection for internet of things devices, in: Computing and Communications Conference (IPCCC), 2015 IEEE 34th International Performance, IEEE, 2015, pp. 1–8.
[352] K. Demertzis, L. Iliadis, S. Spartalis, A spiking one-class anomaly detection framework for cyber-security on industrial control systems, in: International Conference on Engineering Applications of Neural Networks, Springer, 2017, pp. 122–134.
[353] S. Stone, M. Temple, Radio-frequency-based anomaly detection for programmable logic controllers in the critical infrastructure, Int. J. Critical Infrastruct. Protect. 5 (2) (2012) 66–73.
[354] A. Hildick-Smith, Security for critical infrastructure SCADA systems, SANS Read. Room GSEC Practical Assign. Version 1 (2005) 498–506.
[355] S.J. Stone, M.A. Temple, R.O. Baldwin, Detecting anomalous programmable logic controller behavior using RF-based hilbert transform features and a correlation-based verification process, Int. J. Critical Infrastruct. Protect. 9 (2015) 41–51.
[356] S. Dunlap, J. Butts, J. Lopez, M. Rice, B. Mullins, Using timing-based side channels for anomaly detection in industrial control systems, Int. J. Critical Infrastruct. Protect. 15 (2016) 12–26.
[357] J. Krimmling, S. Peter, Integration and evaluation of intrusion detection for CoAP in smart city applications, in: Communications and Network Security (CNS), 2014 IEEE Conference on, IEEE, 2014, pp. 73–78.
[358] N. Jiang, H. Lin, Z. Yin, C. Xi, Research of paired industrial firewalls in defense-in-depth architecture of integrated manufacturing or production system, in: 2017 IEEE International Conference on Information and Automation (ICIA), IEEE, 2017, pp. 523–526.
[359] J. Nivethan, M. Papa, On the use of open-source firewalls in ICS/SCADA systems, Inf. Secur. J. 25 (1–3) (2016) 83–93.
[360] S. Adepu, S. Shrivastava, A. Mathur, Argus: an orthogonal defense framework to protect public infrastructure against cyber-physical attacks, IEEE Internet Comput. 20 (5) (2016) 38–45.
[361] T. Ghosh, D. Sarkar, T. Sharma, A. Desai, R. Bali, Real time failure prediction of load balancers and firewalls, in: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2016, pp. 822–827.
[362] Y. Javed, M. Felemban, T. Shawly, J. Kobes, A. Ghafoor, A partition-driven integrated security architecture for cyber-physical systems, arXiv:1901.03018(2019).
[363] F. Cohen, The use of deception techniques: honeypots and decoys, Handb. Inf. Secur. 3 (1) (2006) 646–655.
[364] D. Antonioli, A. Agrawal, N.O. Tippenhauer, Towards high-interaction virtual ICS honeypots-in-a-box, in: Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, ACM, 2016, pp. 13–22.
[365] S. Litchfield, D. Formby, J. Rogers, S. Meliopoulos, R. Beyah, Rethinking the honeypot for cyber-physical systems, IEEE Internet Comput. 20 (5) (2016) 9–17.
[366] C. Irvene, D. Formby, S. Litchfield, R. Beyah, Honeybot: a honeypot for robotic systems, Proc. IEEE 106 (1) (2017) 61–70.
[367] D. Fraunholz, D. Krohmer, S.D. Anton, H.D. Schotten, Investigation of cyber crime conducted by abusing weak or default passwords with a medium interaction honeypot, in: 2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, 2017, pp. 1–7.
[368] W. Tian, X. Ji, W. Liu, G. Liu, R. Lin, J. Zhai, Y. Dai, Defense strategies against network attacks in cyber-physical systems with analysis cost constraint based on honeypot game model, 2019, pp. 193–211.
[369] Q. Duan, E. Al-Shaer, M. Islam, H. Jafarian, Conceal: a strategy composition for resilient cyber deception-framework, metrics and deployment, in: 2018 IEEE Conference on Communications and Network Security (CNS), IEEE, 2018, pp. 1–9.
[370] G. Bernieri, M. Conti, F. Pascucci, A novel architecture for cyber-physical security in industrial control networks, in: 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), IEEE, 2018, pp. 1–6.
[371] M.O. Sayin, T. Basar, Deception-as-defense framework for cyber-physical systems, arXiv:1902.01364(2019).
[372] I. Ahmed, S. Obermeier, M. Naedele, G.G. Richard III, SCADA systems: challenges for forensic investigators, Computer 45 (12) (2012) 44–51.
[373] I. Ahmed, S. Obermeier, S. Sudhakaran, V. Roussev, Programmable logic controller forensics, IEEE Secur. Priv. 15 (6) (2017) 18–24.

[374] R.A. Awad, S. Beztchi, J.M. Smith, B. Lyles, S. Prowell, Tools, techniques, and methodologies: a survey of digital forensics for SCADA systems, in: Proceedings of the 4th Annual Industrial Control System Security Workshop, ACM, 2018, pp. 1–8.
[375] G. Grispos, W.B. Glisson, K.-K.R. Choo, Medical cyber-physical systems development: a forensics-driven approach, in: Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, IEEE Press, 2017, pp. 108–114.
[376] H. Al-Khateeb, G. Epiphaniou, H. Daly, Blockchain for modern digital forensics: the chain-of-custody as a distributed ledger, in: Blockchain and Clinical Trial, Springer, 2019, pp. 149–168.
[377] C.-F. Chan, K.-P. Chow, S.-M. Yiu, K. Yau, Enhancing the security and forensic capabilities of programmable logic controllers, in: IFIP International Conference on Digital Forensics, Springer, 2018, pp. 351–367.
[378] G. Ahmadi-Assalemi, H.M. Al-Khateeb, G. Epiphaniou, J. Cosson, H. Jahankhani, P. Pillai, Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace, in: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), IEEE, 2019, pp. 1–9.
[379] J. Parry, D. Hunter, K. Radke, C. Fidge, A network forensics tool for precise data packet capture and replay in cyber-physical systems, in: Proceedings of the Australasian Computer Science Week Multiconference, ACM, 2016, p. 22.
[380] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles, IEEE Commun. Mag. 56 (10) (2018) 50–57.
[381] P. Taveras, SCADA live forensics: real time data acquisition process to detect, prevent or evaluate critical situations, Eur. Sci. J. 9 (21) (2013).
[382] I. Ahmed, V. Roussev, W. Johnson, S. Senthivel, S. Sudhakaran, A SCADA system testbed for cybersecurity and forensic research and pedagogy, in: Proceedings of the 2nd Annual Industrial Control System Security Workshop, ACM, 2016, pp. 1–9.
[383] K. Yau, K.-P. Chow, Detecting anomalous programmable logic controller events using machine learning, in: IFIP International Conference on Digital Forensics, Springer, 2017, pp. 81–94.
[384] S. Zonouz, J. Rrushi, S. McLaughlin, Detecting industrial control malware using automated plc code analytics, IEEE Secur. Priv. 12 (6) (2014) 40–47.
[385] L. McMinn, J. Butts, A firmware verification tool for programmable logic controllers, in: International Conference on Critical Infrastructure Protection, Springer, 2012, pp. 59–69.
[386] A. Kleinmann, A. Wool, Accurate modeling of the siemens S7 SCADA protocol for intrusion detection and digital forensics, J. Digit. Forensics Secur. Law 9 (2) (2014) 4.
[387] S. Senthivel, I. Ahmed, V. Roussev, SCADA network forensics of the PCCC protocol, Digit. Investig. 22 (2017) S57–S65.
[388] K. Yau, K.-P. Chow, S.-M. Yiu, A forensic logging system for siemens programmable logic controllers, in: IFIP International Conference on Digital Forensics, Springer, 2018, pp. 331–349.
[389] D. Beresford, Exploiting siemens simatic S7 plcs, Black Hat USA 16 (2) (2011) 723–733.
[390] R. Chan, K.-P. Chow, Forensic analysis of a siemens programmable logic controller, in: International Conference on Critical Infrastructure Protection, Springer, 2016, pp. 117–130.
[391] H. Noura, A. Chehab, M. Noura, R. Couturier, M.M. Mansour, Lightweight, dynamic and efficient image encryption scheme, Multimed. Tools Appl. 78 (12) (2019) 16527–16561.
[392] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, M.M. Mansour, One round cipher algorithm for multimedia IoT devices, Multimed. Tools Appl. (2018), doi:10.1007/s11042-018-5660-y.
[393] H.N. Noura, R. Melki, A. Chehab, M.M. Mansour, A physical encryption scheme for low-power wireless M2M devices: a dynamic key approach, Mob. Netw. Appl. 24 (2018) 1–17.
[394] R. Melki, H.N. Noura, M.M. Mansour, A. Chehab, An efficient OFDM-based encryption scheme using a dynamic key approach, IEEE Internet of Things J. (2018).
[395] R. Melki, H.N. Noura, M.M. Mansour, A. Chehab, A survey on OFDM physical layer security, Phys. Commun. 32 (2019) 1–30.
[396] H. Noura, S. Hussein, S. Martin, L. Boukhatem, K. Al Agha, Erdia: an efficient and robust data integrity algorithm for mobile and wireless networks, in: Wireless Communications and Networking Conference (WCNC), 2015 IEEE, IEEE, 2015, pp. 2103–2108.
[397] H. Qiu, G. Memmi, H. Noura, An efficient secure storage scheme based on information fragmentation, in: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2017, pp. 108–113.
[398] H. Noura, S. Martin, K. Al Agha, K. Chahine, ERSS-RLNC: efficient and robust secure scheme for random linear network coding, Comput. Netw. 75 (2014) 99–112.
[399] H. Noura, O. Salman, A. Chehab, R. Couturier, Preserving data security in distributed fog computing, Ad Hoc Netw. 94 (2019) 101937.
[400] K. Kapusta, G. Memmi, H. Noura, Secure and resilient scheme for data protection in unattended wireless sensor networks, in: 2017 1st Cyber Security in Networking Conference (CSNet), IEEE, 2017, pp. 1–8.
[401] K. Kapusta, G. Memmi, H. Noura, Additively homomorphic encryption and fragmentation scheme for data aggregation inside unattended wireless sensor networks, Ann. Telecommun. 74 (3-4) (2019) 157–165.
[402] R. Diba, E. Yaacoub, M. Al-Husseini, H. Noura, K. Abualsaud, T. Khattab, M. Guizani, A simple approach for securing IoT data transmitted over multi-rats, in: 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), IEEE, 2018, pp. 249–254.
[403] H.N. Noura, R. Melki, M. Malli, A. Chehab, Design and realization of efficient & secure multi-homed systems based on random linear network coding, Comput. Netw. 163 (2019) 106886.
[404] J. Demme, M. Maycock, J. Schmitz, A. Tang, A. Waksman, S. Sethumadhavan, S. Stolfo, On the feasibility of online malware detection with performance counters, in: ACM SIGARCH Computer Architecture News, 41, ACM, 2013, pp. 559–570.
[405] N. Kaaniche, M. Laurent, C. Levallois-Barth, Id-based user-centric data usage auditing scheme for distributed environments, Front. Blockchain 3 (2020) 17.
[406] N. Kaaniche, M. Mohamed, M. Laurent, H. Ludwig, Security sla based monitoring in clouds, in: 2017 IEEE International Conference on Edge Computing (EDGE), IEEE, 2017, pp. 90–97.
[407] G. Sabaliauskaite, A.P. Mathur, Aligning cyber-physical system safety and security, in: Complex Systems Design & Management Asia, Springer, 2015, pp. 41–53.
[408] F. Xie, T. Lu, X. Guo, J. Liu, Y. Peng, Y. Gao, Security analysis on cyber-physical system using attack tree, in: 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2013, pp. 429–432.
[409] H.N. Noura, A. Chehab, R. Couturier, Efficient & secure cipher scheme with dynamic key-dependent mode of operation, Signal Process. 78 (2019) 448–464.
[410] H. Noura, R. Couturier, C. Pham, A. Chehab, Lightweight stream cipher scheme for resource-constrained IoT devices, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2019, pp. 1–8.
[411] R. Melki, H.N. Noura, A. Chehab, Lightweight multi-factor mutual authentication protocol for IoT devices, Int. J. Inf. Secur. (2019) 1–16.
[412] H.N. Noura, R. Melki, A. Chehab, Secure and lightweight mutual multi-factor authentication for IoT communication systems, in: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), IEEE, 2019, pp. 1–7.
[413] H.N. Noura, O. Salman, A. Chehab, R. Couturier, Distlog: a distributed logging scheme for IoTforensics, Ad Hoc Netw. 98 (2020) 102061.
[414] S. Thomason, Improving network security: next generation firewalls and advanced packet inspection devices, Glob. J. Comput. Sci. Technol. (2012).
[415] I. Kuwatly, M. Sraj, Z. Al Masri, H. Artail, A dynamic honeypot design for intrusion detection, in: The IEEE/ACS International Conference onPervasive Services, 2004. ICPS 2004. Proceedings., IEEE, 2004, pp. 95–104.
[416] L. Carver, M. Turoff, The human and computer as a team in emergency management information systems, CACM 50 (3) (2007) 33–38.
[417] R. Ruefle, A. Dorofee, D. Mundie, A.D. Householder, M. Murray, S.J. Perl, Computer security incident response team development and evolution, IEEE Secur. Priv. 12 (5) (2014) 16–26.
[418] K. Kent, S. Chevalier, T. Grance, H. Dang, Guide to integrating forensic techniques into incident response, NIST Spec. Publ. 10 (14) (2006) 800–886.
[419] C. Prosise, K. Mandia, M. Pepe, Incident response & computer forensics(2003).
[420] M.M. Klee, The importance of having a non-disclosure agreement, IEEE Eng. Med. Biol. Mag. 19 (3) (2000) 120.
[421] J. Hogan, R. Hogan, How to measure employee reliability., J. Appl. Psychol. 74 (2) (1989) 273.
[422] A. Serhane, M. Raad, R. Raad, W. Susilo, Plc code-level vulnerabilities, in: 2018 International Conference on Computer and Applications (ICCA), IEEE, 2018, pp. 348–352.
[423] Y.-C. Chang, L.-R. Huang, H.-C. Liu, C.-J. Yang, C.-T. Chiu, Assessing automotive functional safety microprocessor with ISO 26262 hardware requirements, in: Technical Papers of 2014 International Symposium on VLSI Design, Automation and Test, IEEE, 2014, pp. 1–4.
[424] R. Bell, Introduction and revision of IEC 61508, in: Advances in Systems Safety, Springer, 2011, pp. 273–291.
[425] R. Bell, Introduction to IEC 61508, in: ACM International Conference Proceeding Series, 162, 2006, pp. 3–12.
[426] C. Miller, J. Kassie, D. Poston, et al., Assessing and computing the safety integrity level (SIL) for turbo machinery protection, in: Proceedings of the 46th Turbomachinery Symposium, Turbomachinery Laboratory, Texas A&M Engineering Experiment Station, 2017.
[427] T. Goto, Electronic control unit, 2001,. US Patent App. 29/132,291.
[428] N. Dellantoni, B. Schinkowitsch, A. Schoenekaes, A. Nix, N.R. Lynam, Scalable integrated electronic control unit for vehicle, 2015, US Patent 9,036,026.

Jean-Paul Yaacoub is a Master student in the department of Electrical and Computer Engineering at the Arab Open University.

Ola Salman is a PhD student in the department of Electrical and Computer Engineering at the American University of Beirut (AUB), Lebanon.

Hassan Noura is a research associate in the department of Electrical and Computer Engineering at the American University of Beirut (AUB), Lebanon.

Nesrine Kaaniche is Lecturer in Cybersecurity and expert in cryptographic solutions at the University of Salford, School of Computing, Science and Engineering, Greater Manchester, England.

Ali Chehab is a professor in the department of Electrical and Computer Engineering at the American University of Beirut (AUB), Lebanon.

Mohamad Malli is a professor in the department of Electrical and Computer Engineering at the Arab Open University.