BOOK CHAPTER

A Comprehensive Security Risks Analysis of Cliff Edge on Cyber-physical Systems

Koustav Kumar Mondal[a], Asmita Biswas[b] and Deepsubhra Guha Roy[c]

[a]Inter-Disciplinary Research Division - IoT and Application, Indian Institute of Technology (IIT) Jodhpur, India; [b]Institution's Innovation Council, Innovation and Entrepreneurship Development Cell (IIC IEDC) Lab in Institute of Engineering & Management, Kolkata, India; [c]Centre of Excellence for Cloud Computing and IoT, Department of CSE (AIML), Institute of Engineering and Management, Saltlake, Kolkata 700091, India.

ARTICLE HISTORY
Compiled May 9, 2023

ABSTRACT
The incredible fusion of physical and digital elements made revolutionary discoveries of the recent few decades, such as intelligent cities and Industry 4.0, possible. Connecting more devices introduces new vulnerabilities and security threats in today's widespread cyber-physical methods. Cybersecurity specialists are becoming ineffective in directing the most significant risk climate with increasing cybersecurity incidents than ever before. The cyber-physical system (CPS) seems to have been a significant research path for an intellectual world in recent times. The fourth phase of the planet is known to be pursuing research and technology circles domestically and overseas. Post-computer communications technology, the Web, a cross, heterogeneous, seamless integration with open implementation is CPS Systems, device participation, contact, regulation, and other areas of expertise. As the various disciplines are there are significant gaps in the study's theory and methodology, so the implementation of CPS has presented extraordinary difficulties. Cyber-Physical Systems (CPS) usually have many interconnected systems that can control actual objects and structures and manipulate them. CPS aims to explore the physical, communication, and computational structures; they are tightly linked to the Internet of Things (IoT) programs. Their convergence with IoT has resulted in a new part of CPS, the Cyber-Physical Stuff Internet (CPT). The rapid and substantial advancement of CPS impacts various facets of the way of life of individuals. It makes a broader variety of co-operations and technologies, including e-well-being, intelligent houses, e-trade, etc. Nonetheless, the interconnection of the virtual and physical realms inevitably leads to new dangerous threats to defense. Consequently, protection for CPS has both academics and companies were gaining interest.

Inside the aforementioned section, We discussed the protection threats including concerns in a cyber-physical system. We divided this book chapter into three parts; in the first part, we discussed the CPS-Background. After that, we recognize the reasonable vulnerabilities, attack arguments, opponent's features, and an assemblage of provocations that necessitate being inscribed. We furthermore discussed some recommendations and failures in CPS.

KEYWORDS
Cyber-Physical Systems (CPS); Industry 4.0; Advancements in CPS; Security threats; Internet of Things (IoT); Intelligent cities

1. Introduction

To create the physical world function appropriately and more straightforward, the Cyber-Physical System (CPS) attempts to track physical systems' activity and enable actions to alter their behavior. A cyber-physical arrangement (CPS) normally consists of pair fundamental parts, a physical mechanism, and cyber conformity. The motive state is usually tracked or managed via a specific cyber device, a networked arrangement of many small devices with (often wireless) capability for sensing, computation, and communication. A spontaneous occurrence (e.g., an inoperative volcano), a human-made dynamic structure (e.g., an operational room), rather a more confused mixture of those two may be the dynamic mechanism involved. As the physical and virtual systems' link grows, the physical systems become more and more vulnerable to computer system security vulnerabilities. For instance, several hackers have hacked into the U.S. Federal Aviation Agency's air traffic control expedition networks many incidents in contemporary ages, according to an Inspector General's research proposed to the FAA in 2009(Mills, 2009). Any hackers can now even hack specific medical devices with wireless communications embedded in the human body. A CIA report(O'Connell, 2008) shows hackers have breached energy grids in many neighborhoods just outside of the United States and triggered a power failure that involved several towns in at least one instance. Within 2010, the antagonists exhibited a software intermediary summoned CarShark(Koscher et al., 2010) that could remotely disable a car engine, switch off individual brakes so that the car does not stop, and create tools by tracking messages among the electronic control units (ECUs) and injecting fake datagrams to send out strikes, provide false readings. Hackers have formulated a virus this year that can effectively target the Siemens plant-control arrangement.

The bulk of cybersecurity event datasets are confidential, frequently combined with the additional caveat that they are either kept hidden or just exchanged within acutely technological circles as bugs are identified. Consequently, there is an incentive provided before and after the vulnerability discovery stage for presumably silent zero-day penetration by offenders who may be highly competent. Therefore, it can be argued that the emphasis is not directly on the existence and substance of an exploit but how it is capable of weaving between computer security systems to accomplish the ultimate purpose of exploitation. In reality, redemption vulnerabilities are located in even deeper cyber-physical regularities, such as electrical energy systems, conveyance infrastructure, healthcare regularities, and so on. Researchers are beginning to think regarding CPS stability. If we have more intelligent and highly knowledgeable cyber-physical networks, these systems' potential flaws should be carefully considered. In reality, security is a relatively recent environment for cyber-physical systems, and not insufficient research has been reported within this field. Similar to any other emerging area, the greatest of the initiative appears to concentrate on mapping clarifications from subsisting contexts, before-mentioned as sensor networks that bestow networked activities and low ability features among CPS(Roy et al., 2018a). Typically, though, these resolutions have not been established toward CPS. As an illustration, the gas department's cyber-physical machine would communicate with the one that controls the wounded individual's well-being to accomplish the rescue operation, imagining an example of gas leakage in a bright house. These applications are, under normal circumstances, separate. Nevertheless, all these applications need to collaborate and exchange resources to reach the same purpose if there is an incident. For interoperation between heterogeneous systems, conventional safe communication solutions are not planned. Cyber-physical networks guarantee that the device is always protected

when communicating with another system is a fundamental challenge. Some modern CPS security challenges need to be discussed as well.

In this chapter, we first discussed CPS-Background, which consists of CPS-layers and components and CPS model type; secondly, the flaws, attacking models, and forms of adversaries are identified. After that, we also discussed some recommendations and failures in CPS.

2. Background of CPS

We introduce the CPS structure, its key panels, modules, including the main models of the CPS in this section.

2.1. CPS Layers and Components

The CPS device design consists of various courses and modules that depend on diverse communication etiquette and technology to interact across multiple courses.

2.1.1. CPS Layers

Each design of the CPS consists of three fundamental courses, a specific course of vision, the course of transmission, furthermore the course of operation, manifested and defined in Fig.1. A specific study(Ashibani and Mahmoud, 2017) is a foundation for reviewing the different CPS course protection problems.

- **Perception Layer:** It is often referred to since unless every layer of identification or the course of sense. This involves cameras, actuators, aggregators, tags for Radio-Frequency Identification (RFID), Global Positioning Systems (GPS), and many other devices. To track, monitor, and analyze the physical environment, these instruments capture real-time data. Examples of such data collected involve adding vibrate and vivid signals, electrical use, heat, position, chemistry, and biology, depending on the sensor form. Ere signifying and processed through each treatment panel, those sensors perform real-time data inside large, regional interface specialties. Besides, actuator securing relies on official authorizations to assure that all input plus command groups remain error-free and safeguarded. In general, increasing the degree of protection includes a framework of end-to-end encryption on each course. Heavyweight reckonings and high retention specifications will then be set in place. There is a need for reliable and lightweight protection protocols to be built in this context, taking into account the capacities of the equipment and safety specifications.
- **Transmission Layer:** That implies additionally assigned as the course of transport or the network layer, which is the second layer of CPS. Layer as mentioned earlier, reciprocations furthermore prepare knowledge among the levels of interpretation and implementation. Managing Local Area Networks (LANs) furthermore networking standards, including Bluetooth, 4G, and 5G, InfraRed (IR) and ZigBee, Wi-Fi, LTE, onward different innovations, data transfer, and interaction is accomplished across the Internet. Notwithstanding the reason mentioned above, separate protocols, such as Internet Protocol version 6 (IPv6)(Wu and Lu, 2010), imply handled to manage the growth during the particular number of machines connecting to the Internet. The course, as mentioned above, including

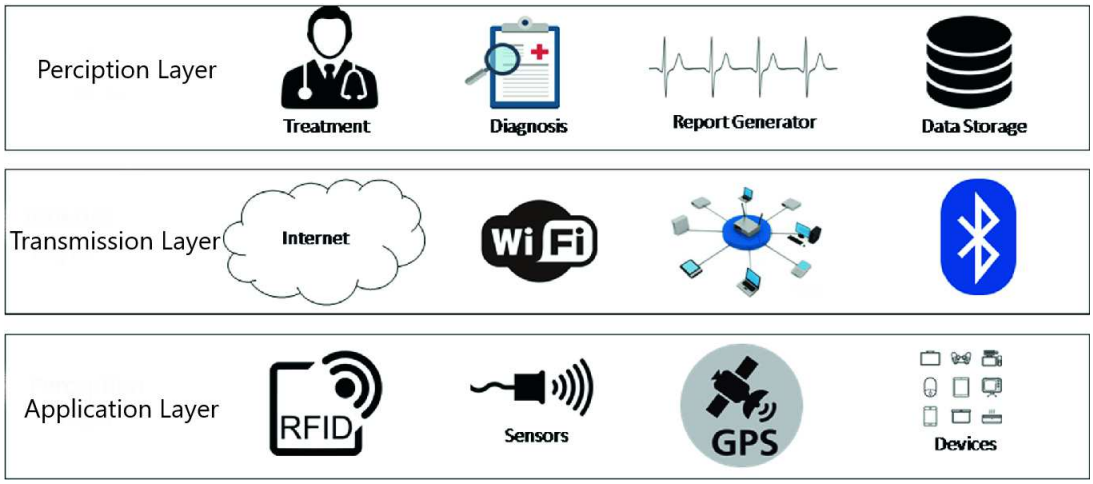


Figure 1. Cyber-Physical System Layers

guarantees information routing and communication via fog foundation services, networking modules, swapping and internet gateways, firewalls, and Intrusion Detection/Prevention Mechanisms (IDS/IPS)(Sommestad et al., 2010). To bypass interruptions and vicious muggings, including ransomware, spiteful cryptogram injection, Denial of Service/Distributed Denial of Service (DoS/DDoS), eavesdropping, furthermore, unlawful admittance initiatives, it is important to ensure their delivery until outsourcing data content(Weiss, 2010). This poses a provocation, principally concerning resource-constrained machines, owing to those overhead commanded in phases of the processor and energy sources demanded.

- **Application Layer:** This signifies a single layer that is three moreover added social. That concocts some information transfer layer information furthermore proceeds the physical device's instructions, including the sensors and actuators. This is accomplished by the application of complicated decision-making algorithms concentrated toward aggregated information(Saqib et al., 2015). Besides, before evaluating the correctly invoked automatic behavior, this layer receives and processes knowledge from the perception layer(Khan et al., 2012). Algorithms for cloud storage, middleware, plus information tunneling are utilized to handle this layer's data. Protecting and retaining privacy involves protecting the leakage of sensitive knowledge. Anonymization, information masking (camouflage)(Roy et al., 2019a), isolation protection, including hidden distribution, is among the most well-known protective methods. Besides, this layer often includes a substantial multi-factor authentication classification to avoid unauthorized admittance and privilege intensification. The scale of the data produced has become a big concern because of the rise in Internet-connected devices(Kumar and Patel, 2014). Thus, securing large data calls for appropriate encryption strategies to handle vast data volumes in a timely and reliable manner.

2.1.2. CPS Components

During sensing erudition(Gries et al., 2017) conversely concerning monitoring signals, CPS components are used (Fig.2). CPS components are divided in this respect toward

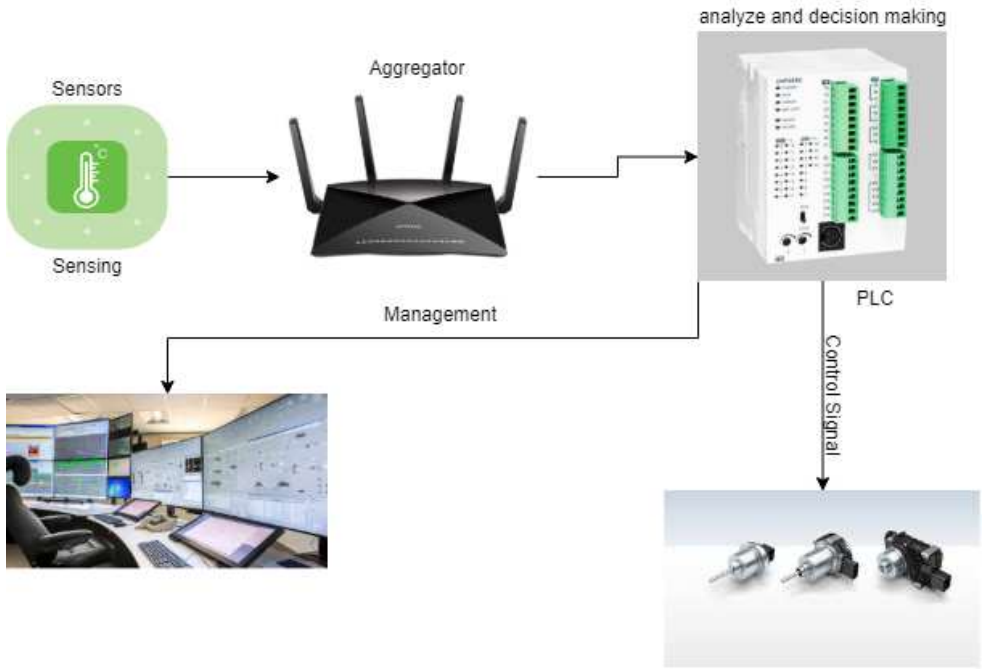


Figure 2. Infrastructure of Cyber-Physical System

couple of influential classes: Sensing Components (SC), which handle plus understanding erudition, furthermore Controlling Components (CC), which track plus regulate beacons.

- **Sensing Components:** The sensors remain essentially positioned in the perception layer furthermore serve the purpose concerning sensors that collect and transmit information upon aggregators. This information is then assigned for further analysis over some actuators to obtain reliable strategic thinking. These same main Protective services detecting components are listed below.
  - **Sensors:** To determine the quality of the data gathered, meaningful data is collected and reported following a correlation method called "calibration." Sensing knowledge is important since the options can focus on the interpretation of this information.
  - **Aggregators:** The statistics obtained from sensors are mainly analyzed at the transmission layer (i.e., routers, sockets, and access points) until the subsequent decision is issued (s). In reality, the aggregation of data is analyzed, and the results are gathered for a given goal, where this information is collected and presented after a statistical review. Online Analytical Processing (OLAP) is a main cluster formation method used as an online knowledge production reporting method.
  - **Actuators:** To render the details available to the external world based on the judgments taken by the aggregators, the implementation layer is located. Because actuators are highly dependent on certain network devices, any operation executed by the CPS is focused on a previous data aggregation sequence(Roy et al., 2019b). Following the definitions, actuators often process electrical signals as an input, generating physical behavior as an output.

- **Controlling Components:** To attain greater precision and security degrees from disruptive attacks or collisions, primarily signal blasting, noise, and intrusion, they imply managing beacons and operating an absolute position in beacon administration, tracking, and superintendence. As a consequence, it has become indispensable to focus on Programmable Logic Controllers (PLCs) and Distributed Control System (DCSs) onward including their elements (i.e., Programmable Automation Controller (PAC)(Mazur et al., 2012), Operational Technology/Information Technology (OT/IT)(Morelli et al., 2019), Control Loop/Server(Vogel and Zack, 2006), and Human Machine Interface (HMI)/Graphical User Interface (GUI)(Ardanza et al., 2019)). First, we mention the numerous forms of control systems in use inside CPS structures.
- **Programmable Logic Controllers (PLC):** Primarily conceived to substitute wired DPDT and SPDT relays, they are called the research automated computers that monitor the production processes, including the output of robotic systems and/or the handling of fault diagnosis, thereby achieving greater flexibility and resilience.
- **Distributed Control Systems (DCS):** Computer-controlled management systems are virtual instrumentation systems that enable the deployment of decentralized controllers within the system utilizing formal authority from a central operator. The DCS's reliability is improved due to the description of the item and management phase, whilst its implementation cost is decreased. DCS may be equivalent to Supervisory Control and Data Acquisition (SCADA) schemes in certain situations.
- **Remote Terminal Units (RTU):** Electronic devices which are powered by a microprocessor, such as that of the Master Terminal Unit (MTU)(Stouffer et al., 2011), or 'Remote Telemetry Uni.'(Roy et al., 2019c). They do not endorse any feedback loop and control algorithm, unlike the PLC (s). Therefore, they are more suited for wireless interactions through larger regional telemetry regions. The key role of RTU is to use a supervisory messaging framework to communicate SCADA to the specific object(s) that governs these artifacts via the transmission of sensor information by the system.

In fact, a tiny computer-controlled "artificial brain" (Central Processing Unit (CPU)) is used by both RTUs and PLCs to process different components from smart sensors and pumping devices; thus, the usage of IEDs (Intelligent Electronic Devices) to relay streams of data or, in the event of an attack, cause an alarm. Concerning the interaction between instruments and levels, it must be said that sensing instruments are implemented predominantly at the layers of interpretation and propagation. In contrast, the regulating modules are installed at the level of operation.

2.2. CPS Model Types

It is possible to distinguish CPS models into three major types:

- **Timed Actor CPS:** In comparison to non-factors focused on efficiency and timing, this model helps in the effective aspects centered on action and correctness. A(Geilen et al., 2011), a principle was implemented with a practical and traditional convergence that limits some collection of activities and increases efficiency by reducing sophistication. The primary emphasis is on the optimization focused on the concept of "earlier-the-better" as it allows the opportunity

to recognize probabilistic abstract concepts of semi systems. Within the experience, such time-deterministic frameworks imply undersized susceptibility over problems with phase bang, making it easier to extract analytical bounds.

- **Event-Based CPS:** In these models, before another sensor decision is being made, an occurrence necessity does sense moreover observed with the right CPS components. However, based on the non-deterministic device delay induced by the numerous CPS behavior, namely sensing, actuating, communicating, and computation, the individual part-timing constraints differ. Hu et al. suggested(Hu et al., 2016a) that season limits may occur controlled by utilizing an event-based method that utilizes CPS activities to ensure the device's coordination, calculation, and control processes. This makes it possible for the CPS to become more relevant and more effective for spatiotemporal knowledge.
- **Lattice-Based Event Model:** In(Tan et al., 2010), Together with local and global event attributes, CPS events are portrayed as per the type of event. If these events are mixed, they may be used to describe any event's Spatio-temporal property while additionally defining all those elements that a particular conclusion has identified.
- **Hybrid-Based CPS Model:** Hybrid CPS schemes remain complex structures consisting of two different types of interactive processes, a persistent state (physical functional networks) and a discrete state (discrete computer systems). The reaction of isolated transient events defined by neural networks and the complex action represented by the equation(s) of differential/difference depends on growth and evolution. Unlike different CPS variants, Hybrid CPS is integrated through an interface, rendering it susceptible to procrastination. Also, no hierarchical simulation is supported by hybrid CPS frameworks, and they are not appropriate for the modeling of linear models. Hybrid systems simulation problems caused by CPS have been addressed(Roy et al., 2016). In reality, Kumar et al. discussed and solved CPS device network latency problems using real-time hybrid authentication(Kumar et al., 2012). In contrast, Tidwell et al. introduced a customizable actual hybrid structural test for in. Finally(Jianhui, 2011), Jianhui proposed an event-driven control of CPS focused on hybrid automatons.

3. Cyber-Physical System Attacks and Vulnerabilities

Protection services also weren't built into CPS networks by default, compared to other communication networks, leaving room for criminals to manipulate numerous bugs and risks to initiate security breaches. The aforementioned is additionally attributable to just individual independent existence of CPS designs, as all use multiple technology and protocols to work in separate IoT domains and interact.

3.1. Cyber-Physical System Attacks

The numerous types of threats that threaten the various facets of CPS networks, particularly cyber and physical ones, are presented in this section:

3.1.1. Physical Attacks

In previous years, direct attacks have been more successful, in particular towards industrialized CPS systems. That most of these assaults have already been responded

to. Nonetheless, this essay presents a wider variety of forms of material intervention:

- **Infected Items:** Aforementioned group covers infected CDs, USBs, computers, also drives, before-mentioned while individual Stuxnet worm, which, when embedded within a cyber-physical computer, mount clandestine malware comprising malicious programs.
- **Abuse of Privilege:** As rogue or dissatisfied staff obtain access to the CPS domain's server rooms and implementation zones, they are committing abuse of privilege attack. This helps them implant a rogue USB for exploitation or catch sensitive details by running harmful security software or as a keystroke.
- **Wire Cuts/Taps/Dialing:** since the contact lines of certain cyber-physical headquarters (HQs), including telephony and Wi-Fi, are already physically observable, attackers will break the cables or wiretap them to decrypt individual transmitted data.
- **False identity:** as perpetrators try to portray themselves as legitimate workers, this assault happens with ample expertise to deceive others. To achieve easy access and greater contact with other staff, they mostly serve as cleaners. The Maroochy Water Leak in Australia in 2000(Slay and Miller, 2007) is an outstanding illustration of this.
- **Stalkers:** these would be typically legitimate workers who behave curious (with sinister intent) by peering over the heads of CPS supervisors and designers to gain their qualifications to coerce or offer them toward additional CPS organizations.
- **Surveillance of CCTV Camera Images:** This involves intercepting videos from closed-circuit news cameras that are used to protect access and important aspects within CPS zones. Before carrying out an undetected physical attack, the aforementioned can transpire achieved through collapsing camera beacons, condensing transmission cables, removing the video, obtaining admittance over some cloud handle and surveillance division, and so on.
- **Key-Card Hijacking:** This entails copying valid cards taken from workers or generating authentic lookalike counterparts to achieve full/partial admittance and breach specific field of the CPS.
- **Physical breach:** this assault involves the procurement of unauthorized physical entry to the infrastructure, specifically by a physical breach, such as the 2011 Springfield Pumping Station(Fillatre et al., 2017), a loophole, such as the 2013 US Georgia Water Treatment Plant(Credeur, 2013), or a security breach exploited, such as the 2012 Canadian Telvent Company. This enables an intruder to disrupt and shut down CPS equipment and network-connected production networks, resulting in a lack of accessibility and efficiency.
- **Malicious third-party information provider:** particular primary aim of the aforementioned assault transpires to threaten the organization's CPS by breaching specific legal software "Industrial Control Systems," before-mentioned essentially individual 2008 shutdown concerning particular Georgia Nuclear Power Plant. This involves swapping legal files in their libraries with software intended to include remote access capability to monitor or exploit a device.
- **Misuse of Privilege:** acts usually accompanied by insiders practically "whistleblowers" to carry out or aid in the implementation of a (cyber)-attack from inside. These high privileges offer them the power to carry out these threats by disclosing useful information regarding the flaws and shortcomings in CPS programs. This exploitation of authority will come in several shapes and sizes.

    - **Physical tampering:** obtaining unauthorized or spoofing approved entry through confined fields to disrupt CPS arrangements and equipment, alter their operating convention, insert malicious information, or appropriate sensitive reports.
    - **Unauthorized actions:** are focused on conducting suspicious functions, such as opening/closing pumping stations, increasing/decreasing power voltage, opening closed ports, interfering with an external agency, redirecting network traffic, or leaking information.
- **Social Engineering:** may demand several manipulative manners beforementioned essentially invert architecture(impersonating tech-savvy), baiting (selling disruptive USBs or software), tailgating (following approved staff), or Quid Pro Quo (impersonating technical support teams), furthermore remains focused upon the science of exploiting individuals (either psychologically rather emotionally) to disclose sensitive erudition through influencing their emotion.

Hackers have lately shifted their focus to CPS networks for espionage, infiltration, warfare, terrorism, and service stealing(Mahato et al., 2021), especially cyber-warfare(Ray, 2020), cybercrimes(Choraś et al., 2016), (cyber)-terrorism(Haimes, 2002) and, countries like Lebanon(Barakat, 2019). (cyber)-sabotage(Alenius and Warren, 2012) (for example, cyber intrusions toward Estonia in 2007(Kaeo, 2007) moreover Georgia in 2008(Donovan Jr, 2009)), about (cyber)-espionage(Yeboah-Ofori et al., 2019). The lack of (cyber)-security exposed a major problem among potentially catastrophic implications, especially in the United States.

3.1.2. Cyber Attacks

There has been a spike in the specific number of cyber intrusions against CPS and IoCPT in recent years, with rather significant implications. CPS is particularly vulnerable to malicious SQL injection attacks(Francillon and Castelluccia, 2008) and script attacks(Roemer et al., 2012), simultaneously including false declaration intrusion offenses(Alemzadeh et al., 2016), zero-control info strikes(Hu et al., 2016b), furthermore ultimately Control-Flow Attestation (C-FLAT) interventions(Abera et al., 2016), as per existing research carried out by(Abera et al., 2016).As seen in Table 1, such assaults might lead to a complete blackout striking CPS industrial equipment and systems.

- **Eavesdropping:** eavesdropping is when non-secure CPS web transactions are detected to access confidential details (passwords, usernames, instead of unspecified separate CPS knowledge). Eavesdropping may demand pair major methods: receptive by monitoring to the transmission of CPS network messages furthermore dynamic by examining, searching, or tampering with some communication through pretending to obtain a valid source.
- **Cross-Site Scripting (XSS):** happens meanwhile third-party network tools occur utilized to insert malicious Coding Script inside a website's database, causing malicious scripts to run in the intended sufferer mesh browser (typically a targeted CPS programmer, constructor, or worker). XSS will hijack a victim's session and, in certain situations, register keystrokes and obtain remote access to their computer.
- **SQL Injection:** or SQLi, is a weakness that enables hackers to read and/or change sensitive data on CPS database-driven websites, as well as to conduct administrative tasks like database shutdown, particularly while CPS policies remain nevertheless utilizing SQL concerning information management.

Table 1. Realtime CPS Attack

COUNTRY	TARGET	ATTACK NAME	TYPE	DATE	MOTIVES
USA	Ohio Nuke Plant Network	Slammer Worm	Malware-DoS	January 25, 2003	Criminal
USA	USA Georgia Nuclear Power Plant Shutdown	Installed Software Update	Undefined Software	March 7, 2008	Unclear
USA	Springfield Pumping Station	Backdoor	Unauthorised Access	November 8, 2011	Criminal
Iran	Iranian nuclear facilities	Stuxnet	Worm	November, 2007	Political
Iran	Power plant and other industrie	Stuxnet-2	Worm	December 25, 2012	Political
Saudi Arabia	Saudi infrastructure in the energy industry	Shamoon-1	Malware	August 15–17, 2012	Religion-Political
Qatar	Qatar's RasGas	Shamoon	Malware	August 30, 2012	Political
Australia	Maroochy Water Breach	Remote Access	Unauthorised Access	March, 2000	Criminal
Canada	Telvent Company	Security Breach	Exploited Vulnerability	September 10, 2012	Criminal

- **Password Cracking:** Attempt to break the passwords of CPS users (primarily designers and administrators) utilizing brute force, dictionary(Narayanan and Shmatikov, 2005) (mitigated through key shift), rainbow table(Papantonakis et al., 2013), birthday (mitigated via hashing), or online/offline password presuming interventions to obtain entry into individual identification database, or the incoming/outgoing transactions. As a consequence, it's necessary to stop more intensification.
- **Phishing:** has several ways, before-mentioned since e-mail phishing, vishing, spear-phishing either whaling, targeted at any either complete CPS customers (such being programmers, experts, executives, Chief Executive Officers (CEOs), Chief Operating Officers (COOs), furthermore Chief Financial Officers (CFOs), over imitating company peers or service providers.
- **Replay:** involves impersonating ICSs, RTUs, and PLCs to intercept transmitted/received packets between them to trigger impediments that impact CPS's present-time regulations plus availability. These intercepted packets might, in certain circumstances, be changed, which would significantly disrupt regular processes.
- **DoS/DDoS:** DoS attacks exploit the infrastructure of the cyber-physical framework moreover are initiated by a great range concerning computers that are locally compromised. DDoS attacks are normally carried out by Botnets, which use many infected computers to initiate a DDoS assault simultaneously from multiple geological positions. DoS interventions can gain various modes(i.e., blackhole(Al-Shurman et al., 2004), teardrop), whereas DDoS can reap significant subsequent patterns, both of which threaten CPS structures (i.e., ping-of-death, smurf(Kumar, 2007), including Black Energy sequence (BE-1, BE-2, and BE-3(Khan et al., 2016)).
    - **TCP SYN Flood:** takes advantage of the TCP handshake mechanism by submitting requests to the server continuously without answering, forcing the server to reserve a room in expectation of an answer (Roy et al., 2018b). This results in an overload of the buffer, which creates the cyber-physical machine to fail.
- **Malicious Third-Party:** involves malware that remotely attacks information gathering networks and breaches them, specifically through utilizing botnets, Trojans, or worms to penetrate erudition via a CPS encrypted tunnel of a constitutional device (i.e., PLC, ICS, or RTU) to a botnet Command-and-Control server through the use of a Trustworthy Third Party within the mask. As a consequence, CPSs(Antonioli et al., 2018) moreover AMIs(Sgouras et al., 2017) are being attacked.
- **Watering-hole Attack:** The intruder looks for some flaws in cyber-physical protection. Once a loophole has been found, a "watering leak" will be set up on

the selected CPS website, where ransomware will be distributed by abusing the intended CPS framework, primarily via backdoors, rootkits, or zero day exploits.

- **Malware:** malware denotes utilized to hack CPS machines to capture or drip data, damage appliances, or circumvent admittance command arrangements. This malware may necessitate several different types, but the most popular ones that threaten CPS are concisely described and conferred below.
  - **Botnets:** Aforementioned entails manipulating the flaws of CPS machines to transform them toward bots or zombies, specifically to carry out DDoS assaults that are barely traceable (i.e., Ramnit (2015)(De Carli et al., 2017), Mirai (2016)(Kolias et al., 2017), Smominru botnet (2017)(De Carli et al., 2017), Mootbot (2020)(Seering et al., 2018), Wild-Pressure furthermore VictoryGate (2020).
  - **Trojan:** Trojan implies a malicious mask that looks genuine plus fools users into installing that. The Trojan infects the computer when it is downloaded and provides indirect admittance to withdraw data credentials including track user actions. Turla (2008), MiniPanzer/MegaPanzer (2009)(Scott and Chen, 2013), Ghost RAT (2009)(Boinapally et al., 2017), Shylock (2011)(Murdoch and Leaver, 2015), Coreflood (2011)(Hendraningrat et al., 2013), DarkCornet (2012)(Farinholt et al., 2017), MEMZ (2016), TinyBanker (2016)(Gostev et al., 2016), Banking.BR Android Botnet (2020) are examples of Remote Access Trojans that can transform a computer into a bot.
  - **Virus:** It may reproduce and propagate to other machines with the aid of humans or non-humans. Viruses infect CPS computers and steal knowledge by linking themselves to other executable codes and programs.
  - **Worms:** propagate by leveraging OS vulnerabilities to damage owner webs by bringing payloads to withdraw, alter, or erase info, or overwhelm webservers (aside from Stuxnet, Flame, and Duqu, e.g., Code Red/Code Red II (2001)(Cowie et al., 2001), Nimda (2001)(Machie et al., 2001), Triton(2017)(Di Pinto et al., 2018).
  - **Rootkit:** Rootkit means to enter or manipulate a device remotely and covertly to achieve records, strip data instead of alter machine settings (i.e., Moonlight Maze (1999), and Blackhole exploit kit (2012).
  - **Polymorphic malware:** the identifiable shifts repeatedly and regularly to prevent being identified and enhance indistinct toward every pattern-matching identification method.
  - **Spyware:** Spyware is a harmful program remotely mounted on a computer for surveillance purposes outwardly exceptional understanding of the consumer or consent (e.g., surveillance, reconnaissance, or scanning). In reality, they (ProjectSauron (2011)(Adams et al., 2020), Dark Caracal (2012), Red October (2013)(Chavez et al., 2015), WarriorPride (2014)(Marquis-Boire et al., 2015), Fin-Fisher (2014), furthermore COVID-19 spyware) may be used for potential cyber-attacks.
  - **Ransomware:** Ransomware signifies a spiteful malware that utilizes CPS vulnerabilities to retain and encrypt CPS data as a hostage, targeting oil refineries, power grids, industrial plants, and medicinal stations, also encrypting complete data reinforcements before a ransom is charged. Siskey (2016), SamSam (2016), Locky (2016), Jigsaw (2016), Hitler-Ransomware (2016), WannaCry (2017), Petya (2017), Bad-Rabbit (2017), Maze (2019), and Ekans (2020) ransomware are only a few cases.

- **Side-Channel:** is focused on data gathered of individual CPS devices, beforementioned since measuring information, energy usage, including electromagnetic losses that can be manipulated.

In fact, as early-maturing as the 1980s, Do et al. provided a far more thorough explanation of the attack(Fillatre et al., 2017). On the other hand, this article attempts to characterize these attacks' frequency as early as 2000, focusing on several reasons including, though not limited to, national, social, and criminal intentions.

3.2. Cyber-Physical System Vulnerabilities

A weakness is a software weakness that can be used for the intent of manufacturing reconnaissance (reconnaissance preferentially effective interventions). Each vulnerability evaluation thus entails defining and assessing the available vulnerabilities of the CPS while at the same time identifying effective improvement plus precautionary steps to minimize, alleviate instead likewise remove the unspecified vulnerability. Toward reality, there exist three major categories of CPS vulnerabilities:

- **Network Vulnerabilities** involve shortcomings in preventive protection mechanisms, as well as breaching transparent wired/wireless contact and links, such as man-in-the-middle, eavesdropping, replay, sniffing, spoofing, moreover communication-stack (network/transport/application layer) attacks(Zhu et al., 2011), back-doors(Nash, 2005), DoS/DDoS, and packet manipulation attacks (Amin et al., 2013).
- **Platform Vulnerabilities:** they involve vulnerabilities in device, applications, setup, plus databases.
- **Management Vulnerabilities:** absence of security protocols, processes, and practices are examples of management vulnerabilities.

Vulnerabilities exist regardless of several causes. There are, however, three primary triggers of vulnerability:

- **Assumption and Isolation:** In most CPS designs, it is focused on the trend of "defense through anonymity." Consequently, the emphasis here is on developing a dependable and stable framework but still considering the deployment of required security facilities without implying that networks are entirely disconnected from the outside world.
- **Increasing Connectivity:** As the network grows more connected, the attack surface becomes greater. Manufacturers have developed CPS by introducing open networks and open wireless applications, as CPS devices have become more linked in recent years. Up until 2001, the bulk of ICS assaults were focused on internal attacks. This was before the internet, which changed the emphasis of threats to the outer world.
- **Heterogeneity:** CPS solutions contain heterogeneous modules from third parties combined to construct CPS implementations. Consequently, CPS has developed into a multivendor scheme, with separate protection weaknesses for each product.
- **USB usage:** aforementioned stands a big trigger concerning vulnerabilities in CPS, before-mentioned since the particular matter concerning this Stuxnet strike against Iranian energy plants, as unique USB is within specific malware. The malware spread through many computers after it was plugged in due to manip-

ulation and duplication.

- **Poor Practice:** This is mainly due to bad coding/weak abilities, which allow the code to perform endless loops or becoming too simple to be changed by an intruder.
- **Spying:** CPS networks are often susceptible to spying/surveillance assaults, which are carried out mostly by the use of spyware (malware) forms that obtain enigmatic admittance furthermore stay undetected during times, among the particular primary purpose of eavesdropping, stealing, and collecting sensitive data including knowledge.
- **Homogeneity:** related forms of cyber-physical networks endure of specific similar flaws that can impact any of the equipment in their proximity until activated, a prime illustration being the Stuxnet worm assault upon Iranian nuclear energy plants(Iasiello, 2013).
- **Suspicious Employees:** through undermining moreover changing specific code writing, or through allowing distant entrance to hackers via specific availability regarding secured ports or obstructing toward an infected USB device, suspicious employees may deliberately or unintentionally damage or hurt CPS computers.

CPS weaknesses may also be of three kinds, namely electronic, human, furthermore meanwhile fused, all occur in any physical, cyber hazard.

3.2.1. Cyber Vulnerabilities:

ICS implementations are vulnerable to security breaches considering ICS depends massively upon public criterion etiquettes, including the Inter-Control Center Communications Protocol (ICCP)(Gungor et al., 2011) also the Transmission Control Protocol/Internet Protocol (TCP/IP). In reality, ICCP experiences some crucial vulnerability to buffer surplusage(Zhu et al., 2011) and lacks fundamental protection measures. In reality, the Remote Procedure Call (RPC) protocol and ICSs are susceptible to different types of attack, including Stuxnet (1 and 2)(Karnouskos, 2011) and Duqu malware (1.0, 1.5, and 2.0)(Bencsáth et al., 2012), Gauss malware(Bencsáth et al., 2012), plus RED October malware (Chavez et al., 2015), as well as Shamoon malware (1, 2 and 3)(Dehlawi and Abokhodair, 2013).

Interception, sniffing, eavesdropping, wiretapping, wardialing also wardriving attacks(Francia III et al., 2012), furthermore, meet-in-the-middle attacks are all feasible with open/non-secure wired/wireless communications like Ethernet. Wireless short-range communications are often sensitive, as insiders may intercept, evaluate, harm, erase, or even exploit them. Besides, if not safe, employees' linked tools to the ICS transpacific interface are susceptible to the botnet, indirect admittanceTrojan, furthermore rootkit interventions. Their devices are managed remotely by an attacker. Eavesdropping, replay assaults, and unintended connection attacks are all feasible for long-range wireless communications. However, SQL injection endures significant greatest Web-related weakness. By inserting a malicious code that proceeds to operate indefinitely until executed without the user's awareness, attackers may enter any application database without authorization.

Since certain medicinal tools rely tediously upon radio transmissions, all are susceptible to a range of radio interventions such as jamming, alteration, furthermore, replay due to a deficiency concerning encryption. Furthermore, GPS moreover particular machine microphones are already being used as a monitoring mechanism, enabling the target's position to be calculated or in-car conversations to be overheard by eaves-

dropping.

In contrast, ICS relies upon the Modbus plus DNP3 protocols to track sensors also actuators and command them. According to Humayed et al.(Humayed et al., 2017), the Modbus protocol lacks simple protection mechanisms before-mentioned since encryption, authentication, including authorization. The aforementioned becomes rendered it vulnerable to eavesdropping, wiretapping, and port-scan, with the possibility of spoofing the controller by fake insertion of information. The DNP3 protocol is often vulnerable to the same bugs and threats, with the Cyclic Redundancy Review (CRC) integration essentially a probity measure being one of the key distinctions. Besides, Windows Server Servers is susceptible to remote code execution, with further assaults being achieved in every running Operating Device by manipulating buffer overflow vulnerabilities (OS).

Furthermore, since smart grid power system architecture is built on the same protocols as ICS, Modbus, and DNP3, it is subject to the same bugs as ICS, Modbus, and DNP3. Consequently, the IEC 61850 etiquette was adopted in substation interfaces, which historically ignored protection features and were susceptible to eavesdropping. Therefore, culminating in attacks of interference or attacks of fake knowledge injection(Wang and Lu, 2013). Santamarta et al. reviewed specific convenient smart meter documentation and inhabited a 'factory login' reckoning to execute simple arrangements. The aforementioned allows the customer total leverage covering an intelligent meter, resulting in energy outages, incorrect judgments, and smart meters targeting the same network. Furthermore, multiple computers are susceptible to battery-draining attacks(Rushanan et al., 2014).

Gollakota et al.(Gollakota et al., 2011) and Halperin et al. (Halperin et al., 2008) manipulated specific Implantable Cardioverter Defibrillator (ICD) by injection assaults. The inventors have additionally demonstrated that intelligent cars are susceptible to multiple forms of assault. Another weakness was found by Radcliffe in, with Continuous Glucose Monitoring (CGM) sensors becoming defenseless to replay assaults. The CGM unit had been spoofed amidst inaccurate preferences being injected. The aforementioned is attributed to a specific point that when smart cars were built, security concerns were not considered. In fact, the protocol of the Controller Area Network (CAN) suffers from several vulnerabilities, which could rise while aggression against intelligent cars is exploited. A DoS assault would be more probable as a consequence of this. Because of the absence of security, a tire-pressure monitoring device (TPMS) is often vulnerable to eavesdropping also spoofing. Also, it is possible to explicitly manipulate Adaptive Cruise Control (ACC), which regulates replacement regarding the CAN system. A well-equipped intruder is capable of interrupting the activities of ACC sensors by introducing turbulence or spoofing. Consequently, you can monitor the vehicle by slowing it down, speeding it up, or even crashing it.

3.2.2. Physical Vulnerabilities

Tangible tampering may trigger data in cyber-physical segments to be corrupted. In reality, it is looking at physical attacks that had a cyber effect. Due to the inadequate physical protection offered for these components, ICS components' physical visibility is regarded as a vulnerability. As a consequence, they're susceptible to physical tampering, change, adjustment, and even sabotage. CPS area systems (i.e., smart grids, power grids, supply chains, etc.) are subject to significant related ICS flaws when exposed without physical protection to a vast range of physical elements, rendering them liable for physical damage. As a consequence, Mo et al. emphasized identification and

preventive solutions in their paper. Humaid et al. suggested(Humayed et al., 2017) that medicinal tools are susceptible to dynamic entry, accompanied by a significant risk regarding downloading malware inside them or constantly altering the system's settings, compromising the welfare of the user. Besides, dynamic admittance to any medicinal system is often a risk since the serial number of the device may be retrieved by an intruder to conduct targeted interventions.

Essentially mentioned earlier, CPS arrangements endure different flaws, rendering them vulnerable to varying standards of assault.

4. Characteristics of Adversaries

This section poses many key forms of future adversaries:

- Experienced hackers are advanced programmers including special expertise to recognize complex bugs in current applications furthermore produce operating exploit codes.
- Dissatisfied insiders including spiteful intention do not necessitate a numerous understanding of cyber intrusion expertise, and their information of the game operation additionally empowers them to acquire unrestricted admittance to overthrow the conformity or to appropriate system data, which are known to be the key source of cybercrime and sabotage, workers, contractors or business associates may be the types of insiders;
- Crime organizations, the ransom will be the prime motive for a criminal organization conducting an assault on a cyber-physical infrastructure(O'Connell, 2008).
- Many terrorists want higher-impact objectives in a single nation, beforementioned essentially aero orderliness or energy network systems, and all could acquire the particular capability to pull these vital cyber-physical installations down. Also, by employing highly trained coders, hiring control device developers, and bribing insiders, they are presumably attempting to accomplish the target(Wan et al., 2010).

The CPS defenders should follow the necessary policies or tactics to react to the threat based on adversaries' types. Furthermore, to develop hazard models, researchers may obtain a deeper comprehension of foe features moreover the potential to predict an adversary.

5. Failure of CPS

It is necessary to illustrate the key failures experienced by CP systems, considering the various risks, interventions, and vulnerabilities that specific CPS field experiences. These errors may be small (causing just minor damage) or severe (causing serious damage) (severe damage). More knowledge is available in(Avizienis et al., 2004), wherever Avizienis et al. offered a properly established plus thorough description inside aforementioned regard.

- **Content loss:** indicates that each content concerning specific information transmitted is unreliable, occurring in the failure of the functional structure. The lack of content may imply both numerical or non-numerical (i.e., alphabets, graphics,

sounds, or colors).

- **Timing failure:** indicates that specific timing (transmission/receipt) of the processing of information is postponed or disrupted (collected/transmitted too short-stemmed or exceedingly belated). The aforementioned will change the specific methods of determination-making and could create difficulties with data administration.
- **Sensors Failure:** This suggests that specific sensors imply no long-drawn working correctly, presenting a significant challenge to decision-making owing to incorrect input or producing the CPS device to a standstill. In 2005, at the Taum Sauk Hydroelectric Power Station, a related event occurred.
- **Silent Failure:** happens in a distributed device where there is no communication sent or received.
- **Babbling Failure:** happens as the data is provided, allowing the device to crash and work in a babbling fashion.
- **Budget Failure:** This happens where the significant expense of installing a cyber-physical device reaches the resources allocated ere the system is checked. This is largely attributed to a lack of preparation.
- **Schedule failure:** happens when due to more upgrades, further tests, or insufficiency for customer requirements, the schedule provided for preparing, testing, and reviewing a specified CPS is not met.
- **Application failure:** happens where the service interface propagates an error and impacts its decision-making capacity or/and usual output quality. This failure will result in a partial or total failure of the CPS device, which can be temporary or permanent.
- **Consistent/Inconsistent Failures:** A consistent failure arises when all CPS customers view a specified service identically. If all CPS customers interpret an erroneous service differently (i.e., bohrbugs, mandelbugs, heisenbugs, and Byzantine defeats), this is referred to as an incomplete failure.

6. Recommendation for CPS

Various monitoring mechanisms should be enforced and strengthened to increase defense from various risks and assaults. This involves, among others:

- **Prioritization and Classification:** of sensitive CPS elements and properties before evaluating, handling, and reviewing threats to ensure adequate expenditure spending on the right protection initiatives (basic, normal, or advanced) concerning their costs versus the probability of an incident happening and its effects.
- **Careful Financial Preparation and Management:** To safeguard critical/non-critical CPS properties and materials, it must be carried out meanwhile duration concerning feasible expenditure furthermore required costs/resources.
- **Lightweight Dynamic Key Based Cryptographic Algorithms:** Certain methods may continue utilized to maintain a range of security resources, including message secrecy, uprightness, and authentication, both of which transpire needed throughout protected CPS interactions. The aforementioned can imply accomplished through utilizing the latest contemporaries regarding cryptographic algorithms outlined inside the following sections(Roy et al., 2018c) The

value of these strategies is that they will strike a reasonable compromise between the degree of protection and efficiency. Since a dynamic key is used per post, the strength against attacks has been demonstrated (preferentially an assemblage of information; depend on utilization compulsions also specifications). Besides, to generate a collection of cryptographic primitives and to change cryptographic primitives, the aforementioned changing key is utilized. As a consequence of the various cryptographic primitives used, the unconventional ciphertext may be produced toward specific identical plaintext. However, these algorithms' reliability is illustrated because they only need one round of iteration and employ basic operations while preventing diffusion. The latest contemporaries regarding certain cryptographic algorithms decrease significant latency, energy, moreover aloft processing needed, allowing CPS tools to manage their key functionalities better.

- **Defining privileges:** Aforementioned can act known essentially individual various effective admittance management strategy that grants permits furthermore exemptions based about specific roles/tasks/attributes of the users meanwhile this appears toward locating CPS and when finishing the job or on leave of the employee, withdrawing certain access rights. The usage of the least privilege strategy comes into this heading as well. The privilege concept could then be focused on the Attribute-Based Access Control (ABAC) framework, where access permissions are specified by policies coupled with attributes. It's worth remembering that ABAC allows access control judgments dependent on attribute values' Boolean conditions. It offers a high degree of granularity required to render the access scheme for CPS control more reliable.
- **Powerful Multi-Factor Authentication Entity:** Sadly, entity authentication systems focused upon each individual authentication determinant imply non adequately immune to authentication assaults, which imply enhancing exponentially further severe. Each entity authentication mechanism is the primary route of protection under each conformity, essentially any actual authentication assault will contribute to an attack on secrecy, credibility, plus availability. "The principle of multi-factor authentication has recently been adopted by incorporating two or more further factors: 1) "you are" involving system fingerprint, user fingerprint, guidance geometry, iris scan, retina scan, etc., and 2) "you have" involving cryptographic keys to improve its robustness toward authentication interventions before-mentioned essentially those mentioned in (Melki et al., 2019). In addition to the usage of geographical positions, this mechanism should be an important prerequisite for CPS programs. These solutions benefit from reducing false negatives and complicating authentication attacks by compromising several variables rather than only one. This also restricts access to designated agencies and employees (devices/users) only.
- **Solid Password and Complex Hashing Process:** Passwords are called the authentication element for "you know." However, it is necessary to enforce multiple assaults, before-mentioned since rainbow moreover hash table advances. To avoid them from happening, passwords obligation continue re-hashed including a unique dynamic Nonce concerning a particular individual after a periodic interval. Furthermore, a stable cryptographic hash function, before-mentioned being SHA-3 or SHA-2, should be used (variant 512). Birthday attacks are avoided, furthermore, rainbow/hash table attacks are minimized.
- **Safe and Secured Audit:** This can be achieved with the aid of an audit manager framework that gathers and preserves logs in a distributed system.

A potential approach that can be implemented in this sense has recently been proposed(Noura et al., 2020). This restricts any insider effort toward a cyber-physical structure and to track them back, and it protects the digital records of internal and external threats.

- **Enhanced Non-Cryptographic Solutions:** expect mutated IDS/IPS or AI-based IDS/IPS systems (using Machine Learning algorithms), coupled by sophisticated firewalls (i.e., Device also Next-Generation Firewalls) and customizable honeypots to avoid any possible vulnerability-based protection breach. This can be accomplished by the usage of lightweight IDS/IPS moreover anomaly-based individuals in particular. In particular, the anomaly detection algorithm can be chosen according to over specific CPS system's limitations, which may obtain analytical during restricted devices instead based upon computer algorithms, before-mentioned essentially random forests, toward strong CPS tools. Approaching a particular hand, signature-based techniques should continue utilized through a unique Gateway (GW), wherever total web transfer can transpire evaluated.
- **Safe and Checked Backups:** aforementioned remains important to ensure specific availability of CPS data furthermore prevent information elimination either modification through securing robustness toward DoS/DDoS including Ransomware strikes, remarkably since before-mentioned interventions may direct to complete blackouts while within the specific fact regarding the US. The aforementioned can be achieved with the aid of lightweight data security strategies like those mentioned in(Noura et al., 2019).
- **Forensic efforts:** it is necessary to recover the traces of any assault that happens. It is therefore important to incorporate modern solutions to anti-forensic strategies to retain some digital proof(Noura et al., 2020). The aforementioned is achieved by retrieving records including tracking channels plus device actions, effectively restricting multiple reconnoitering endeavors. Nevertheless, those afresh advanced forensics instrument's obligations remain compatible with the software/hardware of numerous CPS systems, particularly resource-constrained machines, moreover, necessity likewise remains immune to anti-forensic trials.
- **Enhanced approach to incidents:** requires the capacity to recognize, warn and react to a specific event. To minimize threats, proposals for event response and investigation can be enforced. This offers defense against accidental technological and organizational failures (power loss, blackout) through contingency arrangements, and against malicious failures (cyber initiatives), by teams of CERT (Computer Emergency Response), CSIRT (Computer Security Incident Response), including IRCF (Incident Response And Computer Forensics). Essentially before-mentioned, to maintain an improved and productive cyber, physical, and device ecosystem with safe computing and communications, CPS experts plus designer's obligation undertake additional training and practice.
- **Real-time monitoring:** Utilizing advanced forensics or non-forensic software and techniques to operate real-time applications is vital to avoiding any cyber-physical device malfunction, whether unintentional or not. This helps CPS systems' actions be continuously tested and tracked and, thus, identify unspecified cyber threat endeavors under its immature platforms.
- **Security check:** staff monitoring necessity imply carried out ere including throughout specific work for each employee to remove moreover accommodate unspecified potential effort by a whistle-blower. Accordingly, it is strongly advisable to sign agreements such as the Non-Disclosure Agreement (NDA), the

Confidentiality Agreement (CA), the Confidential Disclosure Agreement (CDA), the Proprietary Knowledge Agreement (PIA), or the Privacy Agreement (SA). These security checks are particularly relevant in vulnerable areas like nuclear power plants.

- **Periodic Employee Training:** requires periodic ICS and PLC employee sensitivity training about the best practices of data protection depending on their degree and experience and the potential to spot any unusual action or operation. Employees must also be educated on a range of technology risks and poor behaviors, such as stopping downloading any app upgrades, avoiding social engineering and phishing attempts, and preserving transparency in the event of misconduct.
- **Daily Pen Monitoring and Vulnerability Assessment:** must be conducted on a routine basis to implement device auditing, identify intimidations, including resolving them in real-time until all are detected furthermore misused via an intruder beneath zero-days misuse statuses.
- **Periodic risk evaluation:** the potential and effect regarding a proffered danger upon a critical/non-critical cyber-physical framework based upon a qualitative-quantitative danger assessment furthermore a Cost-Benefit Analysis (CBA) must both be enforced to study, identify the danger based upon an adequate/non-adequate basis, including minimizing this being soon while practicable.
- **Up-to-Date Devices:** Cyber-physical policies necessity remain held up-to-date in phases of applications, firmware, including hardware by implementing checked pieces furthermore upgrades daily. Furthermore, such structures must be safe at various stages of deployment (layered protection), including the significant potential to alleviate furthermore react to an intervention to minimize its effect including avoiding additional intensification furthermore harm. Also, to avoid any payload injection, USB ports obligation signify corporally including inevitably disabled. The actions and behavior of PLC devices must be continuously checked concerning unspecified questionable behavior(Serhane et al., 2018).
- **AI Encryption Solutions:** In IDS/IPS aberration identification mechanisms or in "you are" or "you do" object authentication schemes, artificial intelligence is used. Within the experience, AI has immediately seen essentially a game-changing approach toward a range of cyber-physical strikes targeting CPS networks, computers, moreover features of contact. Given the experience and resources needed to train an AI device, the accuracy of identification and avoidance is superior to human intervention. CPS systems can be rendered more stable, resilient, and immune to cyber-physical attacks by recent developments toward machine learning, furthermore unexpectedly toward deep learning.
- **Defense In-Depth:** Most current technologies have a defense against a particular feature of attack or a necessity for security. Instead, a multi-purpose security approach is needed to ensure each CPS operating layer (perception, transmission, and application). E.g., ISO 26262 and IEC 61508/Edition2, the two most accepted international requirements for practical protection in the automobile industry, should be valued and implemented. This guarantees a stable CPS deployment focused on technical protection, which requires the Protection Integrity Standard (SIL) basics, which in twist depend proceeding each Likelihood regarding Failure on Demand (PoFoD) moreover specific Risk Mitigation Factor (RMF) to maintain a far innumerable reliable moreover effective Danger and Risk Analysis (RA), primarily in those Electronic Control Units (ECU).
- **CPS Protection and Privacy Life-cycle:** Ultimately, our paper provides a combined life-cycle of Organizational and Practical Safety/Security (OFSS) to

summarize this task, ensuring a good and secure CPS task. This system is based on the ISO 26262 and IEC 61508/Edition2 etiquette furthermore their guide to maintaining CPS Functional safety and protection. The system is composed of six major stages:

- **Step 1:** Designing a strategy to build a CPS framework in compliance with the appropriate budget and associated costs by implementing a well-defined timetable and timetable. It often includes individuals' help (people in business, mechanics, managers, etc.) including non-human capital (vehicles, machines, etc.).
- **Step 2:** necessitates a detailed risk and threat review, which involves adequate risk assessment and asset recognition, as well as the reciprocal interaction among a particular couple, to maintain correct decision-making on specific execution regarding specifically required protection countermeasures.
- **Step 3:** specifies the necessary specifications for practical protection, security, and durability along with the main elements that are important to minimize danger and, in the event of their occurrence, to reduce their chance and effects.
- **Step 4:** In terms of the newly implemented practical protection, protection, and reliability steps, the performance of CPS is assessed in an organizational manner in which performance monitoring and review would be carried out to ensure proper/mutual security output, protection enforcement, furthermore reliability-performance contracts-offs.
- **Step 5:** The cyber-physical device is checked and validated until the performance is measured to find any residual software/hardware error, protection gap, or performance problem and implement the expected alterations that were being commissioned. If the specific trial is ineffective, the specific method restarts repeatedly to assess when the concern necessitated position. If effective, before being officially deployed, the CPS would head for further commissioning.
- **Step 6:** The implemented CPS device will experience a trial phase after satisfactory tests to ascertain its operating state, thus tracking its actions and efficiency before being completely operational.

7. Present Work and Future Research Direction

Cyber-Physical Systems (CPS) are gradually being embraced (installed) and applied in new sectors by various vehicle businesses. This implies that future CPS will confront a growth in functional and extra-functional needs. Condition monitoring and growing CPS automation capabilities are examples of functional needs. Safety, cyber-security, and ecological responsibility are examples of extra-functional criteria. Many emerging CPS solutions are inter in nature (the capacity to access or communicate information to various security domains seamlessly). For example, autonomous autos that use robotics technology and telecom networks for smart devices both present significant prospects and problems. Technological advancements enable new sorts of coordination and interaction in CPS across:

- Physical, integrated, networked, and systems engineering are examples of technological domains. Consider cloud and edge computing.

- Intelligent transportation system (vehicular and infrastructures integration) are examples of stand-alone systems.
- Full cycle stages, in generally, making data accessible throughout the life span and allowing software updates. These are DevOps (Development-Operations integration) ideas related to continuous software development, integration, and deployment with input from operational systems.

CPS is rapidly rising because to increased levels of automation and intelligence, especially data analytics. These qualities are determined through artificial intelligence approaches such as machine learning. According to a report from the National Science and Technology Council in the United States(Cowie et al., 2001), AI and data analytics potential are viewed as game changers. Context awareness is critical for new sorts of AI-based CPS, particularly the capacity to identify which entities are now present in the relatively close and deduce their intentions. The advancement of AI technology across a variety of application sectors is expected to generate higher degrees of automation.Because of their potential to address social concerns and create cash, future CPS will be assigned more complex jobs in open environments. To counteract conventional manufacturing uses, extremely sophisticated technologies are being applied and disseminated across society. For example, self-driving automobiles on public highways with no human involvement and robot-human collaboration systems.

Smart CPS is in charge of dynamic changes in the environment. (For example, highly changeable traffic situations that alter fast in response to changing human behaviours and CPS infrastructures.) It typically indicates that not all operational circumstances are known a priori (at the time of system creation), as shown in example(Branquinho, 2018). The broader implications include that open CPS faces a variety of current and new types of uncertainty, including largely unknown surroundings, weaknesses in safety and assaults (predict attack by establishing "attacker models"), and altering CPS itself (due to partial failures). Uncertainty can apply to features of a CPS as well as all stages of the life cycle.It is obvious that the potential qualities of future CPS would necessitate new methods of thinking about system level attributes and composability.

8. Conclusion

CPS technologies are essential parts of Enterprise v4.0, and by combining the real and cyber environments, they are now evolving how people communicate with either the external surroundings. The aim of introducing CPS programs, whether inside or outside of IoT (IoCPT), is to increase the standard of goods and systems' availability and functionality. On the other hand, CPS systems are plagued by a bunch of protection and data issues that jeopardize their dependability, protection, and performance, as well as obstructing Everyone's widespread adoption.

This article looks at the past of the CPS and the security risks and vulnerabilities in cyber-physical structures, and the guidelines for current CPS security models. We hope that these problems and concerns can provide ample impetus for potential discussions and study interests in CPS protection aspects.

In this chapter, we discussed the protection threats including concerns in a cyber-physical system. We divided this book chapter into three parts; in the first part, we discussed the CPS-Background. After that, we recognize the reasonable vulnerabilities, attack arguments, opponent's features, and an assemblage of provocations that neces-

sitate being inscribed. We furthermore discussed some recommendations and failures in CPS.

References

Elinor Mills. Report: Hackers broke into faa air traffic control systems, 2009.

Kelly O'Connell. Cia report: cyber extortionists attacked foreign power grid, disrupting delivery. *Internet Business Law Services*, 2008.

Karl Koscher, Stefan Savage, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Alexei Czeskis, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*, pages 447–462. IEEE Computer Society, 2010.

Deepsubhra Guha Roy, Madhurima Das, and Debashis De. Cohort assembly: A load balancing grouping approach for traditional wi-fi infrastructure using edge cloud. In *Methodologies and Application Issues of Contemporary Computing Framework*, pages 93–108. Springer, 2018a.

Yosef Ashibani and Qusay H Mahmoud. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68:81–97, 2017.

Miao Wu and Ting-lie Lu. ling sun. *Hui-Ying Du," Research on the architecture of Internet of things," in advanced Computer Theory and Engineering (ICACTE)*, pages 484–487, 2010.

Teodor Sommestad, Göran N Ericsson, and Jakob Nordlander. Scada system cyber security—a comparison of standards. In *IEEE PES general meeting*, pages 1–8. IEEE, 2010.

Joseph Weiss. *Protecting industrial control systems from electronic threats*. Momentum Press, 2010.

A Saqib, Raja Waseem Anwar, Omar Khadeer Hussain, Mudassar Ahmad, Md Asri Ngadi, Mohd Murtadha Mohamad, ZOHAIR Malki, C Noraini, BOKOLO ANTHONY Jnr, RNH Nor, et al. Cyber security for cyber physcial systems: A trust-based approach. *J Theor Appl Inf Technol*, 71(2):144–152, 2015.

Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: the internet of things architecture, possible applications and key challenges. In *2012 10th international conference on frontiers of information technology*, pages 257–260. IEEE, 2012.

Deepsubhra Guha Roy, Bipasha Mahato, and Debashis De. A competitive hedonic consumption estimation for iot service distribution. In *2019 URSI Asia-Pacific Radio Science Conference (AP-RASC)*, pages 1–4. IEEE, 2019a.

J Sathish Kumar and Dhiren R Patel. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, 90(11), 2014.

Stefan Gries, Marc Hesenius, and Volker 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*, pages 345–346, 2017.

Deepsubhra Guha Roy, Bipasha Mahato, Ahona Ghosh, and Debashis De. Service aware resource management into cloudlets for data offloading towards iot. *Microsystem Technologies*, pages 1–15, 2019b.

David C Mazur, Ryan D Quint, and Virgilio A Centeno. Time synchronization of automation controllers for power applications. In *2012 IEEE Industry Applications Society Annual Meeting*, pages 1–8. IEEE, 2012.

Umberto Morelli, Lorenzo Nicolodi, and Silvio Ranise. An open and flexible cybersecurity training laboratory in it/ot infrastructures. In *Computer Security*, pages 140–155. Springer, 2019.

Stephen R Vogel and Steven Jeffrey Zack. Method and apparatus providing remote reprogramming of programmable logic devices using embedded jtag physical layer and protocol, December 26 2006. US Patent 7,155,711.

Aitor Ardanza, Aitor Moreno, Álvaro Segura, Mikel de la Cruz, and Daniel Aguinaga. Sustainable and flexible industrial human machine interfaces to support adaptable applications in

the industry 4.0 paradigm. *International Journal of Production Research*, 57(12):4045–4059, 2019.

Keith A Stouffer, Joseph A Falco, and Karen A Scarfone. Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc), 2011.

Deepsubhra Guha Roy, Puja Das, Debashis De, and Rajkumar Buyya. Qos-aware secure transaction framework for internet of things using blockchain mechanism. *Journal of Network and Computer Applications*, 144:59–78, 2019c.

Marc Geilen, Stavros Tripakis, and Maarten Wiggers. The earlier the better: A theory of timed actor interfaces. In *Proceedings of the 14th international conference on Hybrid systems: computation and control*, pages 23–32, 2011.

Fei Hu, Yu Lu, Athanasios V Vasilakos, Qi Hao, Rui Ma, Yogendra Patil, Ting Zhang, Jiang Lu, Xin Li, and Neal N Xiong. Robust cyber–physical systems: Concept, models, and implementation. *Future generation computer systems*, 56:449–475, 2016a.

Ying Tan, Mehmet C Vuran, Steve Goddard, Yue Yu, Miao Song, and Shangping Ren. A concept lattice-based event model for cyber-physical systems. In *Proceedings of the 1st ACM/IEEE International Conference on Cyber-physical Systems*, pages 50–60, 2010.

Deepsubhra Guha Roy, Debashis De, Md Mozammil Alam, and Samiran Chattopadhyay. Multi-cloud scenario based qos enhancing virtual resource brokering. In *2016 3rd International Conference on Recent Advances in Information Technology (RAIT)*, pages 576–581. IEEE, 2016.

Pratyush Kumar, Dip Goswami, Samarjit Chakraborty, Anuradha Annaswamy, Kai Lampka, and Lothar Thiele. A hybrid approach to cyber-physical systems verification. In *DAC Design Automation Conference 2012*, pages 688–696. IEEE, 2012.

Mao Jianhui. Event driven monitoring of cyber-physical systems based on hybrid automata. *National University of Defense Technology Changsha*, 2011.

Jill Slay and Michael Miller. Lessons learned from the maroochy water breach. In *International conference on critical infrastructure protection*, pages 73–82. Springer, 2007.

Lionel Fillatre, Igor Nikiforov, Peter Willett, et al. Security of scada systems against cyber–physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, 32(5):28–45, 2017.

Mary Jane Credeur. Fbi probes georgia water plant break-in on terror concern, 2013.

Bipasha Mahato, Deepsubhra Guha Roy, and Debashis De. Distributed bandwidth selection approach for cooperative peer to peer multi-cloud platform. *Peer-to-Peer Networking and Applications*, 14(1):177–201, 2021.

Lydia Ray. Cyber-physical systems: an overview of design process, applications, and security. *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*, pages 128–150, 2020.

Michał Choraś, Rafał Kozik, Adam Flizikowski, Witold Hołubowicz, and Rafał Renk. Cyber threats impacting critical infrastructures. In *Managing the Complexity of Critical Infrastructures*, pages 139–161. Springer, Cham, 2016.

Yacov Y Haimes. Risk of terrorism to cyber-physical and organizational-societal infrastructures. *Public Works Management & Policy*, 6(4):231–240, 2002.

Kristofas Barakat. *Does Lebanon possess the capabilities to defend itself from cyber-theats? Learning from Estonia's experience.(c2019).* PhD thesis, Lebanese American University, 2019.

Kari Alenius and M Warren. An exceptional war that ended in victory for estonia, or an ordinary e-disturbance? estonian narratives of the cyber attacks in 2007. *The Institute Ecole Supérieure en Informatique Electronique et Automatique, Laval, France 5-6 July 2012 Edited by*, page 18, 2012.

Merike Kaeo. Cyber attacks on estonia: Short synopsis. *Double Shot Security. www. doubleshotsecurity. com/pdf/NANOG_eesti. pdf (accessed 18 July 2009)*, 2007.

George T Donovan Jr. Russian operational art in the russo-georgian war of 2008. Technical report, Army War Coll Carlisle Barracks Pa, 2009.

Abel Yeboah-Ofori, J Abdulai, and Ferdinand Katsriku. Cybercrime and risks for cyber physical systems. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 8 (1):43–57, 2019.

Aurélien Francillon and Claude Castelluccia. Code injection attacks on harvard-architecture devices. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 15–26, 2008.

Ryan Roemer, Erik Buchanan, Hovav Shacham, and Stefan Savage. Return-oriented programming: Systems, languages, and applications. *ACM Transactions on Information and System Security (TISSEC)*, 15(1):1–34, 2012.

Homa Alemzadeh, Daniel Chen, Xiao Li, Thenkurussi Kesavadas, Zbigniew T Kalbarczyk, and Ravishankar K Iyer. Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 395–406. IEEE, 2016.

Hong Hu, Shweta Shinde, Sendroiu Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang. Data-oriented programming: On the expressiveness of non-control data attacks. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 969–986. IEEE, 2016b.

Tigist Abera, N Asokan, Lucas Davi, Jan-Erik Ekberg, Thomas Nyman, Andrew Paverd, Ahmad-Reza Sadeghi, and Gene Tsudik. C-flat: control-flow attestation for embedded systems software. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 743–754, 2016.

Arvind Narayanan and Vitaly Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM conference on Computer and communications security*, pages 364–372, 2005.

Panagiotis Papantonakis, Dionisios Pnevmatikatos, Ioannis Papaefstathiou, and Charalampos Manifavas. Fast, fpga-based rainbow table creation for attacking encrypted mobile communications. In *2013 23rd International Conference on Field programmable Logic and Applications*, pages 1–6. IEEE, 2013.

Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park. Black hole attack in mobile ad hoc networks. In *Proceedings of the 42nd annual Southeast regional conference*, pages 96–97, 2004.

Sanjeev Kumar. Smurf-based distributed denial of service (ddos) attack amplification in internet. In *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, pages 25–25. IEEE, 2007.

Rafiullah Khan, Peter Maynard, Kieran McLaughlin, David Laverty, and Sakir 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*, pages 53–63, 2016.

Deepsubhra Guha Roy, Ahona Ghosh, Bipasha Mahato, and Debashis De. Qos-aware task offloading using self-organized distributed cloudlet for mobile cloud computing. In *International Conference on Computational Intelligence, Communications, and Business Analytics*, pages 410–424. Springer, 2018b.

Daniele Antonioli, Giuseppe Bernieri, and Nils Ole Tippenhauer. Taking control: Design and implementation of botnets for cyber-physical attacks with cpsbot. *arXiv preprint arXiv:1802.00152*, 2018.

Kallisthenis I Sgouras, Avraam N Kyriakidis, and Dimitris P Labridis. Short-term risk assessment of botnet attacks on advanced metering infrastructure. *IET Cyber-Physical Systems: Theory & Applications*, 2(3):143–151, 2017.

Lorenzo De Carli, Ruben Torres, Gaspar Modelo-Howard, Alok Tongaonkar, and Somesh Jha. Botnet protocol inference in the presence of encrypted traffic. In *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, pages 1–9. IEEE, 2017.

Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

Joseph Seering, Juan Pablo Flores, Saiph Savage, and Jessica Hammer. The social roles of bots: evaluating impact of bots on discussions in online communities. *Proceedings of the*

ACM on Human-Computer Interaction, 2(CSCW):1–29, 2018.

Norman Scott and Hongda Chen. Nanoscale science and engineering for agriculture and food systems. *Industrial Biotechnology*, 9(1):17–18, 2013.

Vamshika Boinapally, George Hsieh, and Kevin S Nauer. Building a gh0st malware experimentation environment. In *Proceedings of the International Conference on Security and Management (SAM)*, pages 89–95. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2017.

Stuart Murdoch and Nick Leaver. Anonymity vs. trust in cyber-security collaboration. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pages 27–29, 2015.

Luky Hendraningrat, Shidong Li, and Ole Torsæter. A coreflood investigation of nanofluid enhanced oil recovery. *Journal of Petroleum Science and Engineering*, 111:128–138, 2013.

Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens Le Blond, Damon McCoy, and Kirill 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)*, pages 770–787. Ieee, 2017.

Alexander Gostev, Roman Unuchek, Maria Garnaeva, Denis Makrushin, and Anton Ivanov. It threat evolution in q1 2016. *Kapersky 2015 Report, Kapersky L*, 2016.

James Cowie, A Ogielski, BJ Premore, and Yougu Yuan. Global routing instabilities triggered by code red ii and nimda worm attacks. Technical report, Tech. Rep., Renesys Corporation, 2001.

A Machie, Jenssen Roculan, Ryan Russell, and MV Velzen. Nimda worm analysis. Technical report, Tech. Rep., Incident Analysis, SecurityFocus, 2001.

Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems. In *Proc. Black Hat USA*, volume 2018, pages 1–26, 2018.

NPH Adams, RJ Chisnall, C Pickering, and S Schauer. How port security has to evolve to address the cyber-physical security threat: lessons from the sauron project. *International Journal of Transport Development and Integration*, 4(1):29–41, 2020.

Raymond Chavez, William Kranich, and Alex Casella. Red october and its reincarnation. *Bost. Univ.— CS558 Netw. Secur*, 2015.

Morgan Marquis-Boire, Marion Marschalek, and Claudio Guarnieri. Big game hunting: The peculiarities in nation-state malware research. *Black Hat, Las Vegas, NV, USA*, 2015.

Bonnie Zhu, Anthony Joseph, and Shankar 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*, pages 380–388. IEEE, 2011.

Troy Nash. Backdoors and holes in network perimeters. *Online]: http://ics-cert. us-cert. gov/controlsystems*, 2005.

Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M Bayen. Cyber security of water scada systems—part i: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on control systems Technology*, 21(5):1963–1970, 2013.

Emilio Iasiello. Cyber attack: A dull tool to shape foreign policy. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, pages 1–18. IEEE, 2013.

Vehbi C Gungor, Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P Hancke. Smart grid technologies: Communication technologies and standards. *IEEE transactions on Industrial informatics*, 7(4):529–539, 2011.

Stamatis Karnouskos. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*, pages 4490–4494. IEEE, 2011.

Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Mark Felegyhazi. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet*, 4(4):971–1003, 2012.

Zakariya Dehlawi and Norah 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*, pages 73–75. IEEE, 2013.

Guillermo Francia III, David Thornton, and Thomas Brookshire. Cyberattacks on scada

systems. In *Proc. 16th Colloquium Inf. Syst. Security Educ*, pages 9–14, 2012.

Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-physical systems security—a survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, 2017.

Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer networks*, 57(5):1344–1371, 2013.

Michael Rushanan, Aviel D Rubin, Denis Foo Kune, and Colleen M Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *2014 IEEE symposium on security and privacy*, pages 524–539. IEEE, 2014.

Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. In *Proceedings of the ACM SIGCOMM 2011 conference*, pages 2–13, 2011.

Daniel Halperin, Thomas S Heydt-Benjamin, Benjamin Ransford, Shane S Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 129–142. IEEE, 2008.

Kaiyu Wan, KL Man, and D Hughes. Specification, analyzing challenges and approaches for cyber-physical systems (cps). *Engineering Letters*, 18(3), 2010.

Algirdas Avizienis, J-C Laprie, Brian Randell, and Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33, 2004.

Deepsubhra Guha Roy, Bipasha Mahato, Debashis De, and Rajkumar Buyya. Application-aware end-to-end delay and message loss estimation in internet of things (iot)—mqtt-sn protocols. *Future Generation Computer Systems*, 89:300–316, 2018c.

Reem Melki, Hassan N Noura, and Ali Chehab. Lightweight multi-factor mutual authentication protocol for iot devices. *International Journal of Information Security*, pages 1–16, 2019.

Hassan N Noura, Ola Salman, Ali Chehab, and Raphaël Couturier. Distlog: A distributed logging scheme for iot forensics. *Ad Hoc Networks*, 98:102061, 2020.

Hassan Noura, Ola Salman, Ali Chehab, and Raphael Couturier. Preserving data security in distributed fog computing. *Ad Hoc Networks*, 94:101937, 2019.

Abraham Serhane, Mohamad Raad, Raad Raad, and Willy Susilo. Plc code-level vulnerabilities. In *2018 International Conference on Computer and Applications (ICCA)*, pages 348–352. IEEE, 2018.

Marcelo Ayres Branquinho. Ransomware in industrial control systems. what comes after wannacry and petya global attacks? *WIT Transactions on The Built Environment*, 174: 329–334, 2018.