Chapter 2
Classification of Vulnerabilities in Cyber Physical Systems: Approach, Security and Challenges

Anju Gandhi, Stuti Mehla, Shivani Gaba, Alankrita Aggarwal, and Shally Napgal

2.1 Introduction

Cyber Physical System integrates cyberspace and real space in a dynamic environment. A CPS is a feedback loop mechanism involving a set of physical devices (sensors and actuators) controlled by computer-based algorithms. With the help of CPS, service providers demonstrate their products to their customers and gain a better understanding. It is used to model many real-time applications such as automotive, factory, healthcare, agriculture, and my monitoring. The main goal of CPS is to maximise the implementation of large systems by improving their adaptability, flexibility, performance, functionality, reliability, protection, and accessibility. CPSs have the following two main elements.

- Actual Time data collecting from the internet intelligence feedback and real world are made possible by advanced technologies.
- Cyberspace relies on intelligent data processing, analysis, and computing power.

Cyber physical systems use IoT as its foundational or enabling technology. Cyber physical systems are the IoT's advancement in terms of full conception and perception, and they have a significant capacity for physical world control. Traditional embedded and control techniques are also a part of cyber physical systems,

A. Gandhi (✉) · S. Mehla · S. Gaba · A. Aggarwal · S. Napgal
Panipat Institute of Engineering and Technology, Panipat, India
e-mail: anjugandhi.cse@piet.co.in

S. Mehla
e-mail: stutimehla.cse@piet.co.in

A. Aggarwal
Computer Science & Engineering—Apex Institute of Technology, Chandigarh University,
Mohali 140413, India

N. Sharma et al. (eds.), *Big Data Analytics in Intelligent IoT and Cyber-Physical Systems*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-99-4518-4_2

which have evolved them into cutting-edge techniques. For dependable transmission and information processing, IoT links information acquiring devices including sensors, Cloud Computing and RFID (Radio Frequency Identification) wireless sensor networks technology. In contrast, CPS is a control technique that combines computation, communication, and IoT control. It is scalable and reliable. IoT, on the other hand, focuses on information processing and transmission, whereas CPS not only has the capacity to perceive but also has a potent ability to control. Cyber and physical aspects are related to one another in CPS on both a geographic and temporal scale, revealing a variety of distinct behavioural processes and cooperating with one another in a variety of ways that change the context.

Next generation engineered systems are referred to as CPS. In 2006, Helen Gill at the NSF (National Science Foundation) introduced the term "Cyber-Physical System". The terms "cyber-physical system" and "cyber-security," which have no connection to physical processes, are frequently used interchangeably. The close integration of computations, algorithms, and physical devices is known as CPS. The technologies are seen as connecting the information world with the real world. CPS communicates via well-known technologies including the Industrial Internet of Things (IoT), Industry 4.0, Intelligent Internet of Things (IIoT) and Machine to Machine (M2M).

CPS is a cutting-edge technique that can demonstrate the behaviour of tightly coupled, dispersed physical systems that were previously unthinkable, greatly enhancing the effectiveness and productivity of large-scale systems. In the area of computational meditation systems, it aids in the generation of novel theories. It uses a network of actuators and sensors to continuously manage, monitor and improve physical control systems. The integration of embedded systems with the physical environment is what CPS is, in other words (Fig. 2.1 CPS-based technologies raise the standard of living and make advancements possible in sectors like healthcare, medical crises, and other areas.

Extensive implementation of Cyber Physical Systems due to its characteristics refers to the "Industry 4.0", which combines technology and knowledge to achieve autonomy, reliability, systemization, and innovation without the need for human intervention. It represents process control. The technologies like Smart Technology, Cloud Computing, IoT and many more are the key technology trends driving the CPSs.

CPSs working architecture as shown in Fig. 2.2 supports development in extents like Smart Medication, Smart Constructions and infrastructure, Smart Cities, Smart and unmanned Vehicles, Wearable gadgets, Smart Engineering, Mobility systems, Smart and Powerful defence Systems, and Smart technology meteorology. But the fast evolution of applications of cyber physical system raises several security and privacy concerns.

Information security upholds the information's availability, confidentiality, and integrity. The expanding usage of non-wired technologies for data collection, transmission, and reception as well as control orders via wireless sensor networks has increased the need for information security system development in the industry (WSNs). Due to their independence, equipment in CPSs is inaccessible, which raises

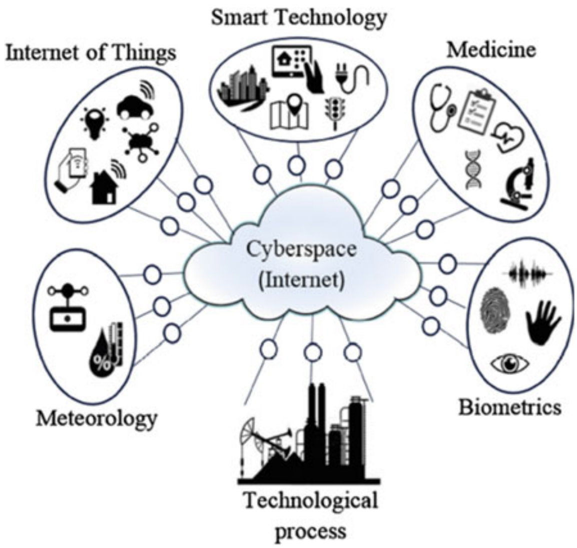

Fig. 2.1 Cyber physical system

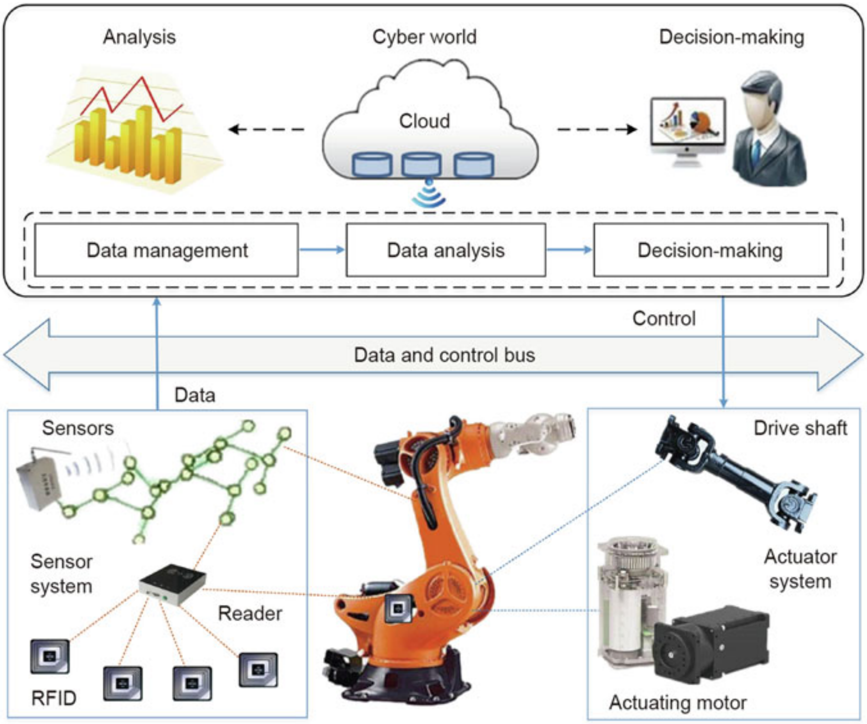

Fig. 2.2 Cyber-physical system architecture and its applications

the possibility of intrusion and attack. When working with many device groups, certain devices can be in danger. New challenges are presented by CPS security. Working with numerous tactics at once can put some of them in jeopardy. The CPS security presents the following new difficulties:

- As the number of IoT devices increases, these systems become more vulnerable to cyberattacks (such as DDoS).
- Modelling of the security intimidations.
- Advancement to assess CPS vulnerabilities approaches.
- Development of highly consistent and fault-tolerant designs to address quickly developing cyber and physical intimidations.

Thus, new techniques are created to satisfy the demands of the cyber physical system for data security, dependability, confidentiality, and specific data. This chapter makes an effort to aggregate and scrutinise the available research on cyber physical system architecture, security, and related topics.

2.2 Cyber Physical System

Helen Gill suggested the term in 2006 at the workshop of US NSF's National Science Foundation. CPSs are now on the US and numerous European countries' priority innovation lists.

- CPS differentiates from existing systems, such as embedded and automated systems, in terms of quality despite having comparable exterior looks. This is made possible by the incorporation of cybernetic, hardware, and software technologies as well as new actuators. Because CPS are a part of their ecosystem, they can recognise changes in it, react to them, note how they were handled, and adjust going future.
- From the standpoint of computer science (Lee 2008). The integration of physical and computational processes is what makes up CPS. These gadgets frequently include feedback and include controllers, network monitors, and embedded computers, among others, where computations are affected both directly and indirectly by physical processes.
- Under the perspective of automation technology, CPSs are customised systems whose functions are governed by computer and communication (Johansson 2014).
- According to US NSF, the future of CPS will perform better than the currently available systems based on efficiency, flexibility, fault tolerance, security, and usability.

2.2.1 History of Cyber Physical Systems

- As embedded systems proliferate, there is a greater requirement for storage space and more memory.
- The complexity and dependability of the CPS algorithm can be influenced by its quality, which raises the computational workload's intensity.
- The response time describes the feedback delay. With longer feedback delays, the accompaniments' quality assurance suffers.
- IoT, smart environments, and other technical trends together in huge systems.
- As information volumes increase, it is vital to outsource some CPS control while maintaining human oversight (Stankovic 2014).

2.2.2 Features of CPS Systems

The main characteristics of CPS as shown in Fig. 2.3 make the system rigid and reliable.

- Mobile and embedded sensing devices.
- Data flows and sensor sources that span domains.
- Cyber and physical components interconnections.
- The capacity for understanding and adaptation.
- Internet of Things
- Employing centralised automatic control to ensure the consistent performance of the systems

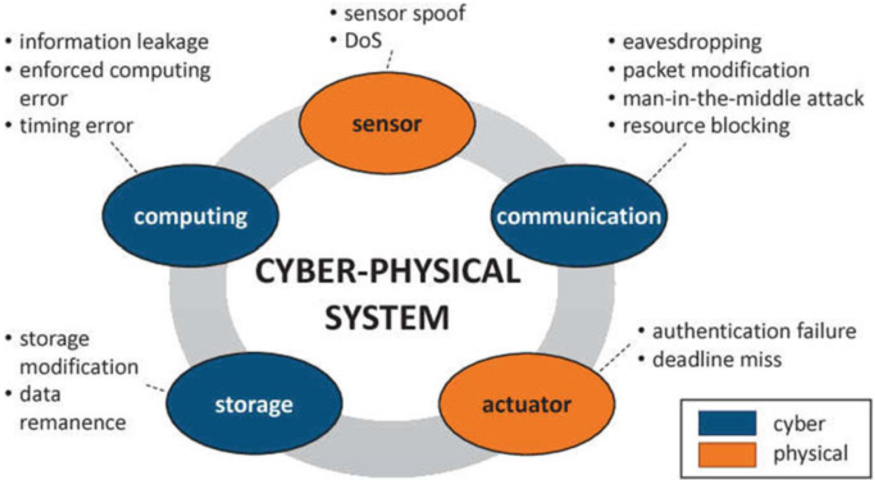

Fig. 2.3 Characteristics of CPS main components

- Communication security via cryptosystems, firewalls, antivirus software, etc., as well as the existence of a shared cyberspace that permits communication between systems and with the outside world.
- In some situations, the operation needs to be dependable and certified.
- Automated intellectual control ensures system robustness.
- Human in/outside the loop.

2.2.3 Key Attributes of Cyber Physical Systems

On the web, as shown in Fig. 2.3, physical systems not only act as the bridge between physical and computational approaches, but they also have all physical characteristics that come from the union of two different system types. Some crucial CPS components include (Kumar and Patel 2014):

- Every physical thing has a cyber capacity that is heavily influenced by IT.
- In CPSs, every action is anticipated.
- CPSs use sophisticated sensing.
- All employed software and systems have high levels of confidence and trust.
- There are always one or more feedback loops between a CPS's input and output.
- CPSs self-optimise, self-document, and self-monitor.
- CPSs need to be safely connected to international networks.

2.3 Essential Layers in CPS

Three separate levels and sections make up the game strategy for the CPS structures. These levels and sections communicate with one another through a variety of correspondence advances and shows. The CPS contains three important tiers. Figure 2.4 depicts and describes the Perception, Transmission, and Application Layers. The security breaches at the various CPS divisions are outlined in the study by Ashibani and Mahmoud (Sobhrajan and Nikam 2014).

It is widely termed as the interest layer or the clear layer (Ashibani and Mahmoud 2017). In close proximity to many devices, it connects hardware like sensors, Global Positioning System (GPS), actuators, aggregators and RFID tags. These devices provide clear information to screen, track, and loosen up this ongoing reality (Mahmoud et al. 2015). Depending on the type of sensors, these instances amounted to data coordination for electrical consumption, heat, area, science, and science, giving little attention to sound and light signals (Gaddam et al. 2008). Prior to being integrated and assessed by the application layer, these sensors produce clear data within extensive and nearby connection districts. In order to guarantee that both appraisal and control orders are accurate and secure, purchasing actuators also depend on remaining source awareness (Khan et al. 2012). Overall, it is estimated that young people should terminate the encryption scheme through each degree in accordance

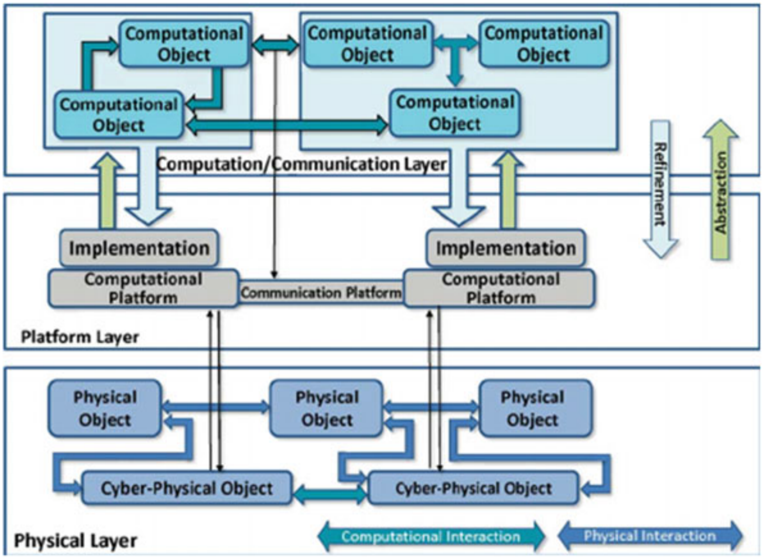

Fig. 2.4 CPS Layers and their interconnections

with the security level (Geng et al. 2006). Along these lines, heavyweight assessments and goliath memory stray pieces would be introduced (Jing et al. 2014). In this situation, there is crucial for a game plan of consistent and lightweight security shows, which contemplate the contraption's abilities and security necessities.

- ***Transmission Layer***:

The vehicle layer, also known as the association layer, is the layer that comes after the CPS layer (Zhao and Ge 2013). Through this layer, data is exchanged and cycled between the data layer and the application layer. Local Area Networks, communication technologies including Bluetooth, Wi-Fi, InfraRed (IR), and ZigBee, as well as various additional advancements, are used to send data and do tasks via the Internet. These are employed to deal with the development of web-related technology, including IPv6 (Internet Protocol Version 6) (Wood and Stankovic 2008). This layer also ensures data sorting and transmission using spread controlling platforms, trade and web Gateways, firewalls, arrangement devices, and intrusion prevention or intrusion detection systems (IDS/IPS) (Wu et al. 2010; Sommestad et al. , 2010). In order to avoid obstacles and damaging attacks like malware, dangerous code injection, Denial of Service (DoS)/Distributed Denial of Service (DDoS), tuning in, and malicious users attacks (Sridharan 2012), it is desperately attempting to obstruct the transport of the data before reclaiming its contents. Given how severely the principal operating and power capabilities are constricted above (Weiss 2010), this is a problem, especially for devices with minimal resources.

- ***Application Layer***:

The third and base layer is this one. It analyses the data acquired from the data communication layer and generates commands for real hardware, such as sensors and actuators (Hu et al. 2013). Strong regions for complicated reasoning about the amount of data are implemented to achieve this (Gao et al. 2013). Additionally, this layer obtains and maintains data from the data layer operating before selecting the appropriately referred motorised rehearsals (Zhao and Ge 2013). Middleware and information mining evaluations are used to handle the information at this tier to ensure proper figuring (Saqib et al. 2015). Protecting confidential information from leakage is necessary for protecting and saving security. The most well-known cautious tactics combine anonymization, information concealment (cover), assurance of security, and mystery sharing (Geng et al. 2006). To prevent unauthorised access and raise honour, this layer also needs strong areas for section endorsement cooperation (Pomroy et al. 2011). The magnitude of the created information has grown to be a major problem because of the development in the number of Internet-related devices (Raza 2013). As a result, obtaining vast amounts of information necessitates the use of valuable security frameworks that can consider these vast amounts of information in a helpful and appropriate manner (Konstantinou et al. 2015).

2.4 Types of Vulnerabilities in Cyber Physical Systems

It is necessary to assess a system's robustness about internal (such as human error) and external (such as power system design failure, software system design faults, and threats (e.g., adversary, environment, and other system threats). Cyber Physical Systems may get affected in three phases' development, maintenance and operation as shown below in Fig. 2.5.

Physiological vulnerabilities in CPS devices (Nagpal et al. 2022) are expanding into the industrial sector due to the provision of an Advanced Metering Infrastructure and Neighbourhood Area Networks along with data metering management devices to ensure the sturdiness of CPS in industrial domains.

In reality, the following three criteria could be used to distinguish physical threats.

Physical Disruption: The electricity grid, power stations, and ground stations are all completely protected since different infrastructure types call for different levels of security. These stations are well-equipped and safeguarded as a result of the implementation of access limitations, authorization, and authentication systems including usernames and access cards, passwords biometrics, and surveillance cameras. However, the main problem is associated with the less secured power-generating sub-stations since transmission lines are vulnerable to sabotage attacks and disruption. There are numerous concerns with smart metres.

In order to tackle this problem, monitoring systems must be challenging to meddle with and may rely on host-based vulnerability scanning or outage monitoring. It

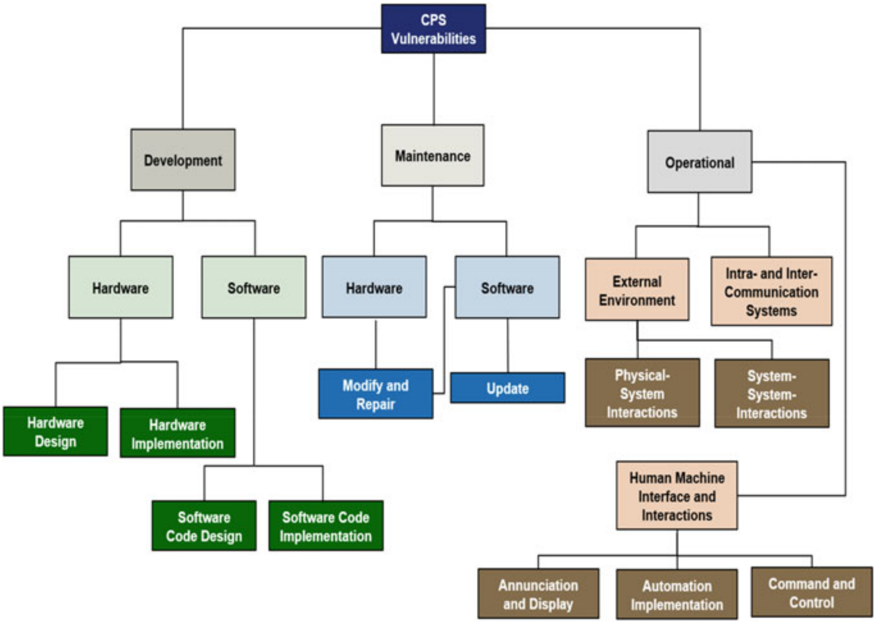

Fig. 2.5 Three levels of vulnerabilities in CPS- development, maintenance and operation

is nearly difficult to avoid physical manipulation or abduction when combating adversaries like Advanced Persistent Threats (APTs).

- *Reduction*: The situation that raises the most alarm is when a malicious attacker repeatedly fails sub-stations. Major urban areas may experience a total shutdown for several hours if the smart grid suffers serious damage. A real-life example is the cascading blackout that the Chinese political structure People Liberation Army (PLA) managed to bring upon the United States.
- *Repair*: It may be built around a self-healing mechanism that examines errors or interruptions, pinpoints the problem, and notifies the connected control system to automatically rebuild the backup resources to meet the demand for the service. The objective is to recover quickly in the lowest amount of time possible. For crucial components, there is, however, either no backup capacity or one that is just partially present. Self-healing can therefore respond to a severe injury more quickly.

2.4.1 Threats Associated with CPS Systems

There are some threats that are associated with CPS systems such as spooling, tracking and many more, as shown in Fig. 2.6.

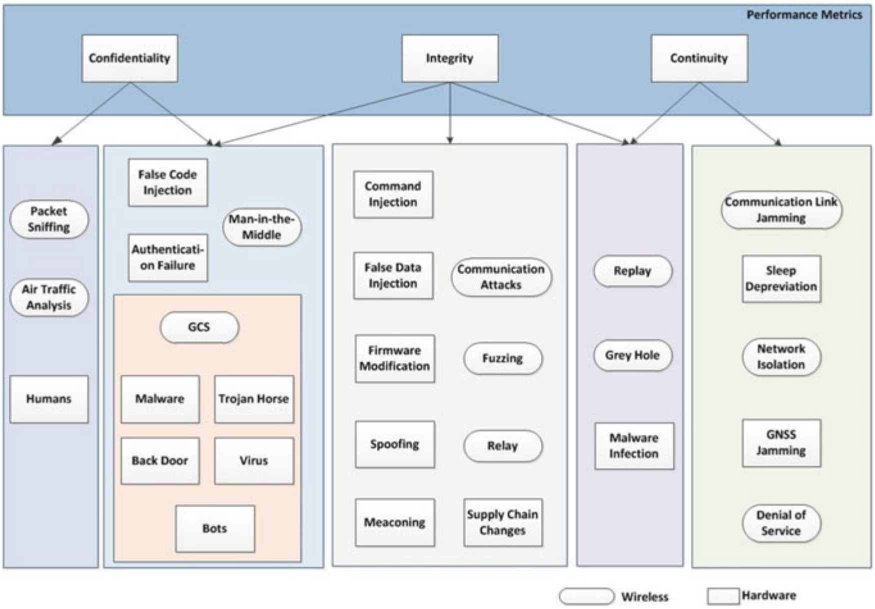

Fig. 2.6 Scope of CPS vulnerabilities and their classification of level phases

1. *Spoofing*: It entails a harmful, unidentified source disguising itself as a reputable entity. Attackers can spoof sensors in this situation, for instance, by providing incorrect or misleading measurements to the control centre.
2. *Sabotage*: Sabotage includes actions like diverting lawful communication traffic and sending it to a malicious party or tampering with the intercultural communication. An attacker might, for example, harm physically vulnerable CPS components dispersed throughout the power system to cause a technical glitch or even a failure of delivery. This can cause a whole or partly blackouts.
3. *Service denial or interruption*: Any device can be physically hacked by an attacker to alter the settings or disrupt a service. This has detrimental implications, particularly when applied to medicinal applications.
4. *Tracking*: Since devices may be physically accessed, an attacker can attach a malicious device, access them, or even track the safe ones. We list the primary CPS weaknesses that the attackers can exploit in the paragraphs that follow.
5. *Tunnelling and encryption (Internet protocol interoperability)*: Ground-anchored communication infrastructure, which are becoming increasingly prevalent, offer measurements of development that require ongoing construction to keep them safe from attack. For these approaches to function effectively, the indications being analysed by avionics systems must have trust in their accuracy, integrity, and availability (continuity). Attacks on networks and software-based firmware are two instances of hazards which could gravely impair upcoming systems.

CPS vulnerabilities are a security flaw that can be exploited for corporate espionage–reconnaissance or we can say active attacks. To discover and analyse the CPS flaws that are currently in place, as well as to determine the best corrective and preventative measures to lessen, alleviate, or even completely remove any vulnerabilities, a vulnerability assessment is necessary. The three major categories of CPS vulnerabilities are as follows:

1. *Network Vulnerabilities*: Unsecured wireless and wireless wired communication and connections are put at risk by man-in-the-middle, espionage, playback, sniffing, masquerading, and connectivity (routing level) attacks. Backdoors, DDoS/DoS, and protocol manipulating assaults are some additional dangers.
2. *Launch Pad (Platform) Flaws*: Vulnerabilities in configuration, System Components (Both hardware and software), and databases are all included (Sztipanovits et al. 2012).
3. *Management Constraints*: Inadequate security measures, protocols, and policies are among them. Numerous factors might lead to vulnerabilities.

2.4.2 Principal Proxies for Vulnerabilities

1. *Confidence and Alienation*: Its foundation is the common “security by obscurity” tendency in CPS architectures. To design a trustworthy and secure system, taking into account the implementation of necessary security services, without assuming that systems are isolated from the outside world, J.A. Yaacoub et al./ Microprocessors and Microsystems 77 (2020) 103,201 7 are focussed here.
2. *Increasing Connectivity*: The attack surfaces grow as connectivity increases. Manufacturers have enhanced CPS through the adoption and use of open networks and open wireless technologies as CPS systems have become more networked in recent years. Up until 2001, most ICS assaults were internal. This was before the use of the internet, which changed attacks to ones from the outside.
3. *Heterogeneity:* CPS applications are created by integrating a variety of third-party components into CPS platforms. Due to this, The CPS system currently has vendor support, and each product is susceptible to distinct security flaws.
4. *USB Utilisation*: Similar to the scenario with the Stuxnet assault that struck Iranian power facilities, the spyware being inside the USB is a significant contributor to CPS risks. When it was plugged in, the malware used replication and exploitation to spread to several devices.
5. *Bad Practise*: It is generally connected to poor coding or insufficient programming skills that caused the code to run indefinitely or become too simple to be altered by a specific attacker.
6. *Spying*: Most spying/surveillance assaults on CPS systems use spyware (malware) types that enter the system covertly and operate for years without being discovered in order to capture delicate or private data.

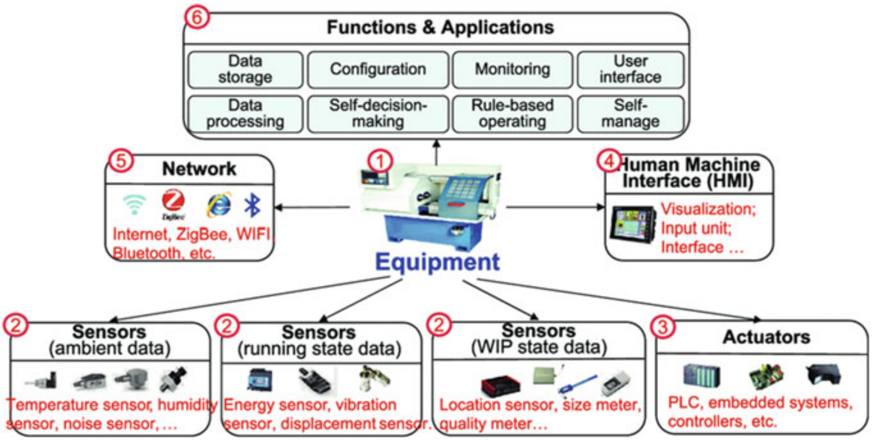
6
Functions & Applications
Data storage
Configuration
Monitoring
User interface
Data processing
Self-decision-making
Rule-based operating
Self-manage
5
Network
Internet, ZigBee, WIFI Bluetooth, etc.
1
Equipment
4
Human Machine Interface (HMI)
Visualization; Input unit; Interface ...
2
Sensors (ambient data)
Temperature sensor, humidity sensor, noise sensor, ...
2
Sensors (running state data)
Energy sensor, vibration sensor, displacement sensor.
2
Sensors (WIP state data)
Location sensor, size meter, quality meter...
3
Actuators
PLC, embedded systems, controllers, etc.

Fig. 2.7 Basic components of CPS prone to threats

7. *Assimilation*: Comparable malware systems have vulnerabilities that, if taken advantage of, might affect the entire surrounding infrastructure. A good example of this is the Stuxnet worm assault targeting Iranian nuclear power installations.
8. *Suspicious Employees*: By undermining and altering the code language, or by providing remote access to hackers by unlocking closed ports or inserting in an infected USB/device, it can purposefully or unintentionally damage or harm CPS equipment. As a result, there are three different kinds of CPS vulnerabilities, including cyber-physical risks (Fig. 2.7). The different activities responsible leading to threats are visualized in the diagram more understanding and analyzing.

2.5 Related Works

The literature work on CPS originates from the integration of physical processes, computational resources, and capabilities of communication; processing units monitor and control physical processes (Ghazani et al. 2012) using sensor and actuator networks. Examples of such systems are transportation networks, water and gas distribution systems, distribution networks, communication systems, control systems and power generation.

The infrastructure based on cyber physical systems (CPS) is one of the important critical structures based on industrial control systems for the last many years and accordingly, there are many cases of computer-based (cyber) attacks (Report: Cyber-Physical Systems Summit. 2008).

A control structure's main purposes are to keep operational goals safe by reducing the likelihood of undesirable behaviour, to meet production demands by maintaining specific process values within established limits, and, finally, to maximise and enhance production profit. Networked agents including sensors, actuators, control processing units like programmable logic controllers (PLCs), and communication devices make up the majority of control systems (Ashibani and Mahmoud 2017). The most significant cyberattack on industrial control systems was Stuxnet, which took place in 2010. It was a sizable piece of malware with numerous features that targeted Siemens industrial control systems and took advantage of four Windows operating system zero-day vulnerabilities (Gaddam et al. 2008). Due to zero-day vulnerabilities, Stuxnet is not only difficult to detect but also has significant implications (Mahmoud et al. 2015). With time, the Iranian nuclear infrastructure began engaging in cyberwarfare. Attacks cannot be stopped by basic antivirus software, but the problems were partially resolved by firms like Kaspersky.

In case of PLC controllers, the victims identify the changes in embedded controllers and code cannot be seen because Stuxnet hides its modifications with sophisticated PLC rootkits and validates the drivers with trusted certificates (Ghazani et al. 2012; Mahmoud et al. 2015).

People use their skillset and mind in cyberattack illegal activities by using vivid ideas to crack a cyber system and are full proof rather can prove advantageous for their nation or for themselves for gaining money. The physical attacks in Cyber physical systems are employed for blackmail or terrorism. Cyberattacks are usually inheritors to physical attacks because of cheap and risky to the attacker (Ashibani and Mahmoud 2017), and additionally, they are easy to replicate and can be coordinated well if at a distance.

2.6 Security Issues in Cyber Physical Systems (CPS)

A combination of societal, specific, and systematic deterrents limits CPS's options. CPS combines a significant number of diverse genuine items and materials with presented and dispersed frameworks that, when combined, should effectively play out the common positions in accordance with the show subtleties (Klesh et al. 2012). The lack of powerful language and expression that must exist to represent computerised genuine affiliation may be the most disturbing problem that such trade-offs face. However, there aren't any crucial first stages for a central affiliation point among structures, real objects, and people, which makes it more difficult for the entire mixture to be interchangeable (Aggarwal et al. 2022).

Human association with CPSs frequently encounters a fundamental barrier while analysing the human–machine collaborative efforts and producing genuine models that consider the present situational measures and natural modifications. These progressions are crucial to the cycle, especially in structures like flying power and military systems (Klesh et al. 2012). Additionally, in complicated CPSs where problematic behaviour should be dealt with promptly employing AI approaches, findings and exercises shouldn't be astonishing or dubious. However, the portions currently prepared for query distribution are currently irrelevant, and the problem is made worse by bad programming strategies, unstable associate connections, and flawed genuine articles (Gaba et al. 2022b).

Additionally, there are difficulties managing the interdependencies between programming and system planning, stresses with compositionality and disengagement for such structures, and difficulties staying aware of a comparable required degree of precision, unwavering quality, and execution of all system components. Security, assurance, and trust are essentially stressed in every cutting-edge development. Politically contentious difficulties include maintaining a CPS's security and constancy and protecting its own data from any usual control. There are security plans in place for a few CPS tiers, including establishment, people, safeguarded development, and items. Since there is a big gap between ensuring that an attack is computerised and real, it is attempting to develop a security system that can swiftly identify both (Sztipanovits et al. 2012).

2.7 Types of Challenges Faced in Cyber Physical Systems

2.7.1 Measures and Challenges in CPS

An examination of the various model kinds, layers, and essential components that make up cyber and physical security. When such attacks are made against any targeted physical or cybernetic system or device, as well as the related vulnerabilities of each such domain, cyber-physical attacks are taken into consideration and analysed. The criteria on which the security is judged are listed below. To estimate the risk and exposure levels for CPS to suggest security countermeasures, a qualitative risk assessment must be conducted (Zhang et al. 2016).

To extract evidence, security measures and their limitations, including the newest cryptographic and non-cryptographic techniques, must be analysed. Cyber forensics techniques are being researched to improve forensics investigations. Numerous life lessons are learned in order to protect authentic data/information communication across CPS devices with limited resources and to achieve CPS security objectives including secrecy, authenticity, reliability, and identification (Gaba et al. 2022a).

For a secure CPS environment, it is advised to minimise and mitigate all threats—cyber, physical, and hybrid–as well as difficulties and problems.

2.8 Conclusion

This chapter paves the way for future advancements in CPS technology. Applications of CPS are better and more versatile because of the improved security parameters. To determine the potential for improvement, the levels of the CPS Architecture were examined. The weaknesses, threats, and attacks related to CPS security are examined.

The serious problems and difficulties encountered are acknowledged. The current security measures are also discussed, and their primary limitations are identified.

References

Aggarwal A, Gaba S, Nagpal S, Arya A (2022) A deep analysis on the role of deep learning models using generative adversarial networks. In: Blockchain and deep learning. Springer, Cham, pp 179–197

Ashibani Y, Mahmoud QH (2017) Cyber physical systems security: analysis, challenges and solutions. Comput Secur 68:81–97

Gaba S, Budhiraja I, Makkar A, Garg D (2022b) Machine learning for detecting security attacks on blockchain using software defined networking. IEEE Int Conf Commun Workshops (ICC Workshops) 2022:260–264. https://doi.org/10.1109/ICCWorkshops53468.2022.9814656

Gaba S, Budhiraja I, Kumar V, Garg S, Kaddoum G, Hassan MM (2022a) A federated calibration scheme for convolutional neural networks: models, applications and challenges. Comp Commun

Gaddam N, Kumar GSA, Somani AK (2008) Securing physical processes againstcyber attacks in cyber-physical systems. In: Proceedings of the national workshop for research on high-confidence transportation cyber-physical systems: automotive. Aviation & Rail, Tyson's Corner, VA, USA, pp 1–3

Gao H, Peng Y, Jia K, Dai Z, Wang T (2013) The design of ICS testbed based onemulation, physical, and simulation (EPS-ICS testbed). In: 2013 Ninth International conference on intelligent information hiding and multimedia signal processing. IEEE, pp 420–423

Geng Y, Rong C-M, Veigner C, Wang J-T, Cheng H-B (2006) Identity-based keyagreement and encryption for wireless sensor networks. J China Univ Poststelecommun 13(4):54–60

Ghazani SHHN, Lotf JJ, Alguliev RM (2012) A study on QoS models for mobile ad-hoc networks. Int J Model Optim 2(5):634–636

Hu W, Oberg J, Barrientos J, Mu D, Kastner R (2013) Expanding gate level information flow tracking for multilevel security. IEEE Embed Syst Lett 5(2):25–28

Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D (2014) Security of the internet of things: perspectives and challenges. Wirel Netw 20(8):2481–2501

Johansson KH (2014) Control of cyber-physical systems: fundamental challenges and applications to transportation networks. In: 27th International conference on architecture of computing systems, Lübeck Germany

Khan R, Khan SU, Zaheer R, Khan S (2012) Future internet: the internet ofthings architecture, possible applications and key challenges. In: 2012 10th International conference on frontiers of information technology. IEEE, pp 257–260

Klesh AT, Cutler JW, Atkins EM (2012) Cyber-physical challenges for space systems. In: 2012 IEEE/ACM third international conference on cyber-physical systems (ICCPS). Beijing, pp 45–52. https://doi.org/10.1109/ICCPS.2012.13

Konstantinou C, Maniatakos M, Saqib F, Hu S, Plusquellic J, Jin Y (2015) Cyber–physical systems: a security perspective. In: 2015 20th IEEE European TestSymposium (ETS). IEEE, pp 1–8

Kumar JS, Patel DR (2014) A survey on internet of things: security and privacyissues. Int J Comput Appl 90(11)

Lee EA (2008) Cyber physical systems: design challenges. In: 11th International symposium on object/component/service-oriented real-time distributed computing, Orlando, Florida, USA

Mahmoud R, Yousuf T, Aloul F, Zualkernan I (2015) Internet of things (IoT) security:current status, challenges and prospective measures. In: 2015 10th International conference for internet technology and secured transactions (ICITST). IEEE, pp 336–341

Nagpal S, Aggarwal A, Gaba S (2022) Privacy and security issues in vehicular Ad hoc networks with preventive mechanisms. In: Proceedings of International conference on intelligent cyber-physical systems. Springer, Singapore, pp 317–329

Pomroy SP, Lake RR, Dunn TA (2011) Data masking system and method. USPatent 7,974,942

Raza S (2013) Lightweight security solutions for the internet of things. Ph.D. thesis, MälardalenUniversity, Västerås, Sweden

Report: Cyber-Physical Systems Summit. 2008. [online]. https://iccps2012.cse.wustl.edu/_doc/CPS_Summit_Report.pdf

Saqib A, Anwar RW, Hussain OK, Ahmad M, Ngadi MA, Mohamad MM, Malki Z, Noraini C, Jnr BA, Nor R et al (2015) Cyber security for cyber physical systems: atrust-based approach. J Theor Appl Inf Technol 71(2):144–152

Sobhrajan P, Nikam SY (2014) Comparative study of abstraction in cyber physical system. Int J Comput Sci Inf Technol (IJCSIT) 5(1):466–469

Sommestad T, Ericsson GN, Nordlander J (2010) SCADA system cyber security-acomparison of standards. In: Power and energy society general meeting. IEEE, pp 1–8

Sridharan V (2012) Cyber security in power systems. Ph.D. thesis, Georgia Institute of Technology

Stankovic JA (2014) Research directions for the Internet of Things. IEEE IoT J 1(1):3–9

Sztipanovits J, Ying S, Cohen I, Corman D, Davis J, Khurana H, Mosterman PJ, Prasad V, Stormo L (2012) Strategic R&D opportunities for 21st century cyber-physical systems. Technical report for steering committee for foundation in innovation for cyber-physical systems, Chicago, IL, USA

Weiss J (2010) Protecting industrial control systems from electronic threats. Momentum Press

Wood AD, Stankovic JA (2008) Security of distributed, ubiquitous, and embeddedcomputing platforms. Wiley Handb Sci Technol Homel Secur 1

Wu M, Lu T-J, Ling F-Y, Sun J, Du H-Y (2010) Research on the architecture of internet of things. In: 2010 3rd International conference on advanced computer theory and engineering (ICACTE), vol 5. IEEE, pp V5–484

Yaacoub et al. 2020 Yaacoub JPA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M (2020) Cyber-physical systems security: limitations, issues and future trends. Microprocess Microsyst 77. https://doi.org/10.1016/j.micpro.2020.103201

Zhang H, Shu YC, Cheng P, Chen JM (2016) Privacy and performance trade-off in cyber-physical systems. IEEE Netw 30:62–66. https://doi.org/10.1109/MNET.2016.7437026

Zhao K, Ge L (2013) A survey on the internet of things security. In: 2013 Ninth international conference on computational intelligence and security. IEEE, pp 663–667