Review on Security Analysis in Cyber Physical Systems

[1]**AbneyWilliam**
[1]School of Design, University of Washington, Seattle, WA.
[1]williamabney@hotmail.com

ArticleInfo
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202202018
Received 31 January 2022; Revised form 30 March 2022; Accepted 25 May 2022.
Available online 05 July 2022.

Abstract – Cyber-Physical Systems (CPS) have seen a dramatic increase in research and real-world application in recent years. Many parts of our everyday lives have been affected, including electrical power systems, oil and gas delivery, transportation networks, medical equipment, home appliances, and a host of other areas. For example, many critical infrastructure and life support equipment are relying on these kinds of systems. As a result, they are required to be completely secure and resistant to all forms of assaults, which is almost unachievable for any real-world system. This paper focuses on security analysis in CPSs, whereby security in CPSs, security threats in CPSs, and security challenges in CPSs, have been discussed

Keywords – Cyber-Physical Systems (CPS), Industrial Control Systems (ICS), Information Technology (IT)

I. INTRODUCTION

Cyber-Physical Systems (CPSs) [1] are a new study topic that has the potential to bring together the physical and digital worlds. In order to integrate the physical and digital worlds, these systems use integrated components to perform tasks collectively. CPSs have grown more dispersed as a result of the Internet of Things (IoT) and the increased complexity of jobs, thus it is vital to design ubiquitous CPSs capable of providing timely service delivery. A distributed CPS with multiresolution dynamism and connectivity allows for the efficient, reliable, safe and secure administration of monitoring and management of physical objects in the real world. Innovations such as Service-Oriented Architecture (SOA), interactive platforms, and cloud technology have emerged in the construction of CPSs after the merger of CPSs and IoT.

The potential of service-oriented CPSs has been highlighted by the need of devices in CPSs to work together on both a cyber and a physical scale. While the service-oriented methodology may be used to create dispersed real-time CPSs that can interact with real-world objects in real-time, it is not adequate to fully realise complete distributed CPSs that take into consideration the interrelations between virtual and real elements. A distributed embedded computing framework depends on agents that are aware of their context is therefore more appealing because it is possible to incorporate various attributes into agents and achieve distributed cloud computing with improved coordination and interconnectivity between independent and inhomogeneous agents. When it comes to CPSs, context-awareness is a must, since this new technology relies heavily on sensors, resources, adaptability, and augmentation. Partial observability in CPSs is a given, given the dynamic nature of distributed CPSs domains. As a result, in order to get high model performance while using ontology as the underlying semantic technology, it is necessary to use uncertainty modelling methodologies.

There are substantial challenges to the security and privacy protection of CPS because of the complexity of CPS and its heterogeneity. Cyber-physical interactions have made assessing threats and vulnerabilities more challenging, and new security concerns have arisen. Because the assaults may come from various CPS components, tracing and examining them is particularly complex. The construction of defensive systems requires an in-depth study of the vulnerabilities, threats, and assaults. Identifying gaps, weak linkages, and new avenues for investigation will be made possible by a review of current CPS privacy and security measures. This paper focuses on security analysis in CPSs, whereby security in CPSs, security threats in CPSs, and security challenges in CPSs, have been discussed. The remaining part of the paper has been organized as follows. Section II focusses on the background analysis of the paper. Section III focuses on a critical survey of the security of CPSs. Section IV finally draws conclusions to the paper and presents suggestions for future studies.

II. BACKGROUND ANALYSIS

CPSs (Cyber Physical Systems) are IT structures integrated into real-world applications. There are sensors and actuators included in these systems. Advances in information and communications technology (ICTs) have resulted in a rise in the interconnection between physical processes.

Real-life Application of CPSs

It is the current iteration of instrumentation and control systems that can constantly monitor the physical environment. CPSs are becoming more important in a wide range of industries, including energy, aviation, and healthcare. As a very significant and symbolic consideration, it is contingent on the technology used. An example of a CPS is the SCADA, which is employed in CI, e.g., smart/intelligent grids and industrial control systems, and wearable and implanted gadgets (utilized in medical care). There are so many versions of CPSs that it would be impossible to mention them all here, but in this article, we'll focus on four examples (see **Table 1**) of how CPSs might be used.

Table 1. Examples of CPSs applications

Application	Details
Industrial Control Systems (ICS)	Nuclear power facilities, water and sewage treatment plants, and irrigation systems all use ICS (SCADA or distribution systems) to better their control and output. We use a variety of controllers in ICS, including PLCs (Programmable Logic Controller) [2]. You may use this gadget to accomplish a variety of goals by combining its many features. A variety of actuators and sensors are being employed to link this gadget to the real-world. This system has both wireless and cable communication capabilities that may be employed depending on the environment. Using PC systems, it is also possible to monitor and control systems in a control centre.
Smart Grid Systems	Smart grids are the next generation of grids for producing energy, even though they have been in use for decades. By giving consumers more control over their energy use at the local scale, it is both economically and ecologically viable. In addition, it improves pollution management, global load balance, and saves energy at the national scale.
Clinical Devices	In an aim to render between medical care, clinical gadgets have been enhanced with a combination of cyber and physical capabilities. In order to help patients, these medical gadgets may either be implanted in the body or worn as wearable devices. These gadgets are intelligent, and they can connect with other gadgets using wireless technology. A programmer is responsible for establishing this line of communication, which is necessary for performing software updates and configuration changes on the devices. Patients who use a wearable gadget are more likely to keep track of their daily routines.
Smart Vehicles	Sustainable, fuel-efficient, cleaner and more convenient: these are the characteristics that distinguish smart cars from traditional automobiles. Electronic Control Units (ECUs), a system of up to 70 computer networks, allowed these improvements. ECUs are responsible for overseeing and controlling a variety of functions, including machine emission controls, recreation controls (audiovisual and radio players), braking control, and recreational elements (cruise control, and closing and window opening). To help alleviate traffic congestion and prevent accidents on the road and in the area, these kinds of advancements are critical in the present era's technological landscape.

Developments in Clinical CPSs

We have analysed the wearable technology and IMDs, and now it's time to talk about the relevance of CPSs in clinical uses, such as insulin pumps, ventilation systems, and patient surveillance systems that are software-intensive. Many individuals are interested in these medical gadgets because they promise to make their lives more comfortable and stress-free (via determining causal factors of diseases or treating diseases). Because of this, new difficulties and possibilities for the scientific community arise when big changes are made to these devices. The following (see **Table 2**) are some of the most common developments in medical instruments:

Overdosing should not be possible with a properly set PCA device since it is meant to only deliver a certain number of doses, no matter how frequently the button is pushed. This safety system, on the other hand, is insufficient to meet the needs of all patients. Misprogrammed pumps, pump developers who overestimate a patient's maximal dosage, drugs placed incorrectly into the device, and PCA-by-proxy are just a few of the possible causes of overdoses that may lead to death or serious illness in many patients. It is not possible to address all of the clinical practise situations that PCA infusion pumps are implicated in, even with established precautions like medication libraries and programmable thresholds. Because of this, we'll need more effective medical gadgets to examine people in the near future (equipment are also required to

determine the patient's medication concentration). Medical gadgets are also increasingly being used to monitor a patient's heart rate, respiratory rate, sugar levels, perceived stress, and body temperature. Despite this, since they lack real-time diagnostic ability, these instruments are limited to a store-and-forward mode of operation and performance. Vital signs can be monitored in real time using closed-loop technologies in physiology, although this requires continual attention.

Table 2. Common developments in medical instruments

Development	Details
New software-enabled functionality	Embedded system concepts [3] are used to bring new technology into medical equipment, such as robotic surgery and proton therapy treatment, using software-based design. Real-time processing of high-resolution pictures and haptic feedback is required for this (robotic surgery). In contrast, proton therapy treatment is one of the most digital therapies and requires one of the biggest clinical device systems in the world. Patients with cancer get precise treatment directions from a cyclotron using a proton beam that give exact dosages of radiation. Beam planning and projecting might potentially be disrupted by the fact that the same beam is disseminated to several patients and must be transferred from place to site. Research on the safety of proton beam machines has mostly focused on one type in the last decade, namely, devices that must be turned off in an emergency. One of the key issues confronting medical device makers and the industry is how to properly analyse and evaluate such massive and complicated structures.
Enhanced connectivity of clinical gadgets	Nowadays, health gadgets are connected with network connections since they increasingly depend on software. The usage of such interconnected healthcare devices allows the creation of more decentralized structures of clinical devices, which have to be planned properly and structured to perform particular functions. Electronic health records (EHRs) might be employed to save patient data via the localized or distant interconnection of these clinical devices for tracking patients or for tele-ICU telemonitoring in Electronic Health Records (EHR). As a consequence of these limitations, novel treatment approaches and enhanced patient safety may be achieved via the use of such healthcare devices in the present context. Medical Device Plug-and-and-Play (MD PnP) interoperability approach is a standard open framework for scalable and safe interconnections of clinical devices, and for enhancing patient safety and efficacy within the healthcare system.
Physiologically closed-loop systems	In most clinical facilities, a nurse is assigned to keep an eye on the systems (or more than one). During an operation, an anaesthesiologist manages the patient's sedation and decides when to alter the sedative stream. This reliance on "person in the loop" may jeopardise patient safety, which is why some in the clinical community worry about it. Nurses who are often overburdened and under tremendous time constraints may overlook a critical warning sign. There may be times when nurses are unable to care for numerous patients simultaneously; however, they can operate a device, which will be a significant assistance to the nurse and enhance patient safety and care. Nonetheless, even though the machine (computer) can never replace the caregivers (in emotion), it may significantly reduce the caregiver's labour by bringing attention to the caregiver only when anything out of the normal occurs. The medical device industry has long employed case-based on closed-loop physiologic control. PCA (Patient-Controlled Analgesia) is a medical condition that takes use of the closed loop technique [4]. Pain treatment after surgery is usually achieved using PCA infusion pumps. PCA pumps allow patients to request a dosage at any time, rather than relying on a caregiver's set schedule for delivery.
Continuous Monitoring and Care	Residential care, supported living, telehealth, and medical monitoring of sports activities are becoming more popular as an alternative to in-hospital treatment because of their lower cost. Remote monitoring of patient and bodily functions is feasible via mobile surveillance and home automation.

Cyber, Network and Data/Information Security

Data security, of which cyber-security is a subset, encompasses a broader range of concerns. Many different methods, technologies or practises may be utilised to safeguard a firm’s networks and computers against unauthorized accessibility, damage or hazards. When it comes to protecting both real and virtual material, InfoSec ensures that no one can get their hands on it. In contrast to cyber-security, the objective of information security (InfoSec) is to safeguard data in any format. When it comes to cyber dangers like viruses, malware, and Trojan horses, network security is responsible for protecting the company's IT infrastructure from all types of cyberattacks including hacker and denial-of-service attacks, hosts and

spyware. Various elements of the network security framework work collaboratively to keep us safe. A firewall, Intrusion Detection/Prevention System (IDS/IPS), Virtual Private Network (VPN), and anti-virus, are all shared security measures on most systems.

III. SECURITY ANALYSIS IN CYBER-PHYSICAL SYSTEMS (CPS)

Security in CPSs

In this section, we provide various instances to demonstrate the criticality of safety to the CPS process. Cryptography, access management, penetration testing, and a slew of other concepts fall under the umbrella of security control (used in IT models). When it concerns safeguarding an ICT's infrastructure, they play a critical role [5]. There will be a lot of demand for error-free cyber physical systems in the near future. There will be many more assaults like these in the future, therefore it's important to be prepared now. Uses of CPSs as shown in **Table 3** need various levels of security.

Table 3. Security breach of CPSs Applications

CPSs Application	Details
Nuclear energy	Based on the facts, it might be disastrous if the CPS lacks enough protection. In the case of a nuclear facility, for example, the safety of the CPS might be compromised, posing a global security risk. As recently as 2010, Iran's nuclear power reactors were targeted by an assault known as Stuxnet. Big industrial control systems also have a large number of outdated systems. In fact, this also holds true. Over the past decade, several individuals have worked on "lightweight cryptographic mechanisms" (mechanisms that make data safe, accessible, and secure). However, much work remains to be done in each of these areas. Make sure to take into account that some security level is preferable to none at all. An ICS's security is critical, and researchers must do their share to ensure it.
Smart Grid Security	If smart grid security is breached, users might lose particular services and the utility agencies might lose particular funds. It is also possible to target smart grids from a distance, which might result in widespread power outages. For example, malfunctioning medical devices, information loss at the data center, and also enhanced crime rate might occur if there are power or energy shortages. As a result, the security of Smart Grid CPSs is fundamental (also to safeguard user data within a system)
Patient safety	The safety of patients might be jeopardised if hacker-targeted wearables and IMDs are not adequately guarded. Licensing authorities must be able to gain access to and utilize datasets, they have to have the capabilities to recognize, modifying, updating and ensuring that gadgets are accessible to them. As a result, ensuring the safety of a medical app's users' and patients' personal information is of paramount importance.
Automobile industry	Automobile manufacturers are always looking for innovative ways to improve the usability and comfort of their vehicles for their consumers. Researchers aren't always thinking about safety when they create vehicles, but that's a good thing to keep in mind. Security safeguards the vehicle's capacity to continue operating in the event of a minor collision. In contrast, safety was not a segment of the design, but rather an added feature. For the vehicle's novel element to work, they must be able to connect wirelessly and physically. For the most part, smart cars rely on these two technologies to protect them from most security breaches or attacks. We must find ways to defend ourselves that are both secure and effective.

In order to adequately safeguard CPSs, the underlying technologies should accomplish particular performance necessities. This allows for the implementation of proven safety systems and standards.

Security Parameters

For CPSs, there are a number of variables to consider in order to ensure, which the system they protect are safe enough (actual-work application). In order to protect CPSs, we must adhere to strict security guidelines.

In recent years, it has become more evident that the reliability of control functions is a critical component. The most significant distinction between control schemes and IT security is the absence of patching or updating requirements for control systems. The process of upgrading a computer may take months, for example. Stopping an industrial computer every time a new security patch is released is not worth the effort. After a software upgrade on March 7, 2008, a gadget designed to monitor chemical data and diagnostic datasets from the plant's corporate systems began operations again. This resulted in the shutdown of a nuclear power facility by accident. There was no evidence that water reservoirs had decreased, which meant that nuclear fuel rods could not be kept cold. When the machine was rebooted, it generated this error. Autonomy is critical, but so is the requirement for decision-making that occurs in real time (another management

system component). Much attention has been paid to availability as a security concern. The real-time operational environment, on the other hand, is more stringent than that of most other IT systems.

The last portion of the report discusses the various security factors and standards for CPSs (i.e., in intelligent control system, intelligent grid system, etc.). In the sub-section below, we will discuss the various forms of security threats in CPSs (i.e., intelligent grid system, intelligent clinical devices, intelligent control schemes, etc.).

Security Threats in CPSs

Our discussion of the security standards for four distinct CPS applications may be found in the preceding section. For each of these applications, we will now discuss some probable attacks. In this sub-section, we're going to discuss about various different cyber physical assaults.

Real-world cyber physical threats

CPSs systems could be attacked by Physical (P), Cyber-Physical (CP) and Cyber (C) threats, and how to prevent them [6]. There are just a few recorded public assaults, and it's quite difficult to get back or figure out exactly what occurred in the immediate aftermath. In this chapter, attacks are categorised according to the location of the injuries. The term "cyber" refers to assaults on computers that do not compromise sensors or actuators. The term "physical" refers to assaults that target specific physical components. When it comes to cyber-physical threats, on the contrary, they are threats that attack physical elements through the employment of cyber elements. But extortion control systems have been around for a long time, so this is nothing new. Terrorism and physical violence are being employed as a means of extortion in many nations. Because they are quicker, cheaper, and do not have to be constricted by distances, cyberattacks are a logical next stage in the development of physical assaults. The following are examples of cyber and physical assaults against CPS that may now be documented:

Cyber attacks on cyber physical systems

Table 4 presents the cyber-attacks of CPSs.

Table 4. Cyber-attacks of CPSs.

Attack	Details
Industrial Control System Attacks	Iran was hit by a "Stuxnet" assault in 2010 that damaged many nuclear reactors. Iran has recently been the target of many cyberattacks by cybercriminals from the United States. There have been two kinds of attacks discovered against ICS. 1. Communication protocols: In several cases, attackers exploited holes in communication systems. A SCADA system [7], for instance, demonstrated how to evade the domain resolution protocol. 2. Espionage: Hacking ICS hacks like DuQu and Flame may be exploited to spy on individuals. A number of ICS networks were detected in the Mideast in 2012 by Flame, for example The primary purpose of this spyware was to steal confidential information from businesses, such as their locations and the passwords they entered into their computers. In many nations, intruders who are not authorized are attacking them on a daily basis. At this point, governments are employing these assaults as a weaponry to inflict maximum harm on their adversary (the enemy).
Smart Grid CPS Attack	CPS assault on a Central Processing System (CPS). The most frequent occurrence is a total power outage. Smart grids are vulnerable to cyberattacks, which might result in a complete blackout in a nation. It was quite significant whenever it happened in USA and Europe a few times over the past 10 years.
Clinical CPS attack	In a distributed framework, insider threats, spies and other types of threats are probable. This is a major danger. Medical gadgets may be tampered with or hacked by an insider, allowing him to control the machinery in any way he sees fit. The wireless transmissions that medical gadgets use to keep individuals healthier might easily be jammed by an invader. In this case, the gadget would be rendered useless and would not be able to render the necessary treatments.
Intelligent Vehicles Attack	Taking control of a motor vehicle or automobiles from a specific distance or through an assault from the outside is a major security issue. An assailant might take control of any car, which could result in a major traffic incident.

Physical Threats on CPSs

Physical assaults that were popular in the past include the following: i) A Pennsylvania (USA) water filtration facility was hacked by intruders in 2006 and employed as its own unlicensed application distribution system or spam, which was later

shut down. ii) Machines compromised with the Slammer worm at the Davis Besse power company in Ohio, took down security surveillance system in January 2003. iii) the Maroochy Shire Council in Queensland, Australia, was attacked in 2000, on the sewage control system (that was undertaken by disgruntled ex-worker of the contractor company, which has established the control systems). In this part, we'll look at an example of a threat framework in CPS.

Adversary Framework in CPS

Identifying potential threats to a system's security requires an in-depth investigation. An adversary model can be used to assess the scope and severity of a problem. Cybercriminals have been breaking into computers all over the world for the better part of the last decade or so (even in control models). Control systems compromised with malware might not work as planned. From a safety perspective, these attacks are critical because they are the result of unauthorised access to control systems' computers and networks. Attacks by insiders can occur even when control networks are completely isolated from the public Internet and other networks. Currently, targeted computer attacks are primarily perpetrated by disgruntled employees. Most of the time, these employees don't collaborate with each other. " Larger, better-coordinated groups can do more damage, but these individuals may not. As a major issue in CPS, this one necessitates a solution that is both practical and realistic.

Criminal groups and terrorists may try to access the security models. Presently, there are no proofs that terrorists and activists have used computer threats to access controllers. Although criminal clusters may be involved, there is some evidence. CPS initiatives aren't new, but they're gaining in popularity these days because of how much money they can make. Iran and Iraq, for example, have been subjected to physical attacks in the last few years as a result of this tactic. Cyberattacks on other nations' physical infrastructure will become more commonplace in the near future. **Table 5** depicts the concept of attacks and consequences of attacks.

Table 5. Concepts of Attacks and Consequences

Concept	Details
Attacks	Resonance assaults on control systems may be used by attackers to gain access (i.e., threats that are non-feasible in more conventional information technology schemes). Someone tampered with some of the sensors or controls, causing physical systems to oscillate at a natural frequency.
Consequences of Attacks	We're not aware of anybody who's done research on the potential consequences of assaults on critical infrastructures. A person may get entry to a control scheme that does not correspond to them via SCADA security reports, which may look like overreaction. The majority of controllers have safeguards in place to prevent catastrophic failures.

Security challenges in cyber physical systems

All of these terms, as well as others, are intertwined in this piece of writing (paper). We define challenges as unanswered problems, and our goal is to entice individuals to do more investigation to discover solutions. An internal (security) weakness that may be exploited by intruders is referred to as a "vulnerability." Things that potentially harm a system are known as threats.

Overall CPSs security Isues

Security based on Design

Since most CPS are not linked to other systems like the web, they are not meant to be secure. CPS are not linked to other networks, which implies that cybersecurity isn't taken into concern while designing them. Keeping people secure, then, was mostly a matter of physical security.

Cyber Physical Security

Keeping people secure, then, was mostly a matter of physical security. Designers of CPSs must rethink security from a cyber and physical perspective if they are to succeed. Our ability to foresee and prevent new cyber-attacks which have physical implications should be improved. There is a need to develop infrastructure for resolution components (cyber-physical technologies), which have hitherto been dismissed.

Real-Timeliness Nature

In case a certain criterion in real-time is not reached, it has a direct impact on the condition of defence. In order to survive an assault, networks rely on CPS to make timely judgments. CPS security that considers the interplay between real and virtual factors may be shown to the whole globe. Better risk evaluation and threat detection may be achieved by using this method. Since cryptographic techniques must be put on top of these approaches to facilitate real-time interoperability, which is what ought to occur.

Uncoordinated Changes

The CPS employs a large number of employees. Those who manufacture, use, own, and operate goods are all included, as are those who work for them. They need to be well managed, even if their jobs and responsibilities are distinct. This shift will need the attention of many personnel and several CPS divisions (an issue that we must not ignore). Stakeholders in a CPS community should coordinate their efforts at some point. Upgrading hardware, upgrading or modifying software, and introducing new features are all examples of methods to improve things. A country's security may be jeopardised if unanticipated improvements to CPSs security (i.e., novel flaws) were to occur.

Industrial Control System Issues

Change Management

Numerous Internet of Things (IoT) gadgets must be removed or modified in ICS environments. Replacement, modification, or deletion of these systems is required (at one place). ICS system updates, for example, must be scheduled meticulously in order to minimise issues. The ICS system's security plan may change without the awareness of many investors; therefore, we must organize change controls in order to monitor and prevent security-based changes within CPSs.

Malicious Insider

Due to the fact that the assault originates from inside the organisation, tracking down and stopping a hostile insider are very difficult tasks. Internal attacks like those in Maroochy's sewage system and water supply, or Stuxnet, might be launched by an insider who has the trust and inside knowledge necessary to carry out the attack. This is only one illustration of what may be accomplished (via a USB stick). Insiders may unintentionally utilise virus-attacked computers or USB sticks, amounting in ICS entry points being made available to unauthorised users. Finding out who is an internal attacker has been the main difficulty that many independent researchers have neglected or ignored.

Secure Integration

To prevent new security issues, new components must be integrated into existing systems in a secure manner. It's important to keep in mind that the ICS depends heavily on out-of-date technology that might be susceptible. In order to make ICS as safe as possible, all of the old components must be removed and new, safer ones installed. So, short-term fixes are needed to avoid any difficulties with ICS.

Smart grids challenges

Table 6 presents the challenges in the smart grid.

Table 6. Smart grid challenges

Challenge	Details
Change Management	Smart grid adjustments aren't any simpler to cope with than ICS updates, but they're also not much easier. Even while smart grids are increasingly complex and include a greater number of people, they are unable to adapt to changes. It necessitates the use of change management in order to keep smart grids healthy.
Two-Way Communications	The Advanced Metering Infrastructure (AMI) [8] in an intelligent grid allows for two-way communication. Consumers' residences are less of a target for physical attacks since AMI smart metres can connect with utility providers that are nearby, unlike the power grid. Since the introduction of smart grids, keeping these gadgets secure has grown increasingly complex.
Access Control Mechanisms	With a vast reach and many investors, smart grids require strong access control systems to keep them safe. It is critical to keep watch on and regulate any potential accessibility to the smart grid system, data, or gadgets. Whenever possible, it is important to empower the individuals or organisations that are meant to assist.
Privacy Concerns	Anxieties about the usage of personal information are common. Increasing use of smart grids has made this an issue for many individuals. Moreover, it is essential to provide anonymization strategies to prevent attackers from deducing trends or encrypted information to disclose sensitive information. The term for this is "anonymization." As a result, we must ensure that the methods we design can encode and consolidate data securely.
Explicit Trust	We should just not put any faith in the perceived data or directives that have been transmitted in this circumstance. Instead, new methods must be devised to recognise bogus data and actions that are not permitted. Because smart grids are so big, it might be difficult to employ algorithms that just search for faults to identify FDI assaults.
Comprehensive Security	Smart grids benefit from having high levels of security. Even at the lowest levels, it's a problem (as a result of limited capacities in devices on the lower level). There might be variations in the number of securities, which has to be in place at every level as a consequence. Several academic researchers have to come up with compact technologies in order to achieve this. Encryption is also critical for maintaining the privacy and security of data at all layers of the smart grid. This is to ensure that there is no security breach at any time.

Medical devices challenges

Table 7 presents the medical device challenges.

Table 7. Medical devices challenges

Challenge	Details
Usability vs. Security	When the patient's condition is serious, changing the unit would be impossible. Someone with IMD may find himself in a position where another medical professional need immediate assistance. So, if the providers will not have the cryptography credentials or access credentials, which permit them to transform IMD, thereby having IMD might be problematic.
More Code vs. Add-On Security	It's critical to have security, but it shouldn't be prohibitively expensive to install. In order to make IMDs more secure, their code may grow in size, making them more susceptible to be seized. Because of this, it is imperative that the cryptographic processes affecting the functionality and cost of medical equipment (that are accessible to patients) be as low as feasible.
Limited Resources	It takes a lot of power (a finite resource) to run cryptographic methods, and that power must be maintained for a long period (long time). Surgery-dependent implants, for example, should last no more than a decade or two before they need to be replaced (at least). Additionally, many assaults attempt to deplete a device's battery, which is known as a Denial of Service (DoS) threats, to prevent it from effective operations. It is fundamental to remember that gadget receiver and evaluates signals from users who do not want to receive all of it. This could be a discharge on the battery system and could possible be problematic. In order to prevent medical equipment from responding to any harmful interactions, new control methods must be developed.

Smart Vehicles challenges

- The security assumptions that manufacturers make when integrating COTS and third-party elements in intelligent vehicles are at an odd. Automobile producers could ensure that COTS incorporation is stabilized and that various elements operate effectively before going into production. Make sure the maker of a vehicle doesn't compromise on security.
- Many various forms of attacks (such as circumventing it and entering restricted bandwidths) may be employed against the gateway Electronic Control Units (ECU) [9]. To improve our vehicles, we may separate important and non-critical ECU by utilizing IP/Ethernet connection and replacing gateways and Master ECUs.
- Other companies in the automotive sector manufacture or purchase (import) automobile parts and components. Buyers and sellers should pay greater attention to security, evaluation, and testing requirements to ensure there aren't any flaws. Manufacturers must consider safety from the outset of the design process.
- The CAN network is susceptible because it is assumed to be isolated. There is a need for new protocols that take into account the possibility of hostile attackers.
- New security issues will arise in the next several years for V2I (Vehicle-2-Infrastructure) and V2Vs (Vehicle-2-Vehicle) connections. In order to prevent ineffective solutions from being implemented, it is necessary to use threats.

As a result, this section examines many recently recognised key difficulties in smart cars, smart healthcare devices, and industrial control systems, among other areas of smart technology development. For medical cyber physical systems, the following part will focus on a number of issues.

Challenges in Medical CPS

Scientists and researchers will need to address a number of challenges in the Medical Cyber Physical Systems (MCPSs), some of which have already been raised in the preceding section. Note that Ref. [33] has some important information, such as the usage, unresolved problems, and difficulties of (in) MCPS. Other important issues with MCPS are highlighted in **Table 8** below:

Table 8. Medical CPS challenges

Challenge	Details
High Assurance Software	In order to automate hardware (such as security gates) and other functions on medical equipment, technology is used There is no doubt that software engineering is fundamental to make MCPS secure.
Interoperability	It is fundamental to ensure that medical instrument that operate in linkage are effective, secured, precise, certified and safe.
Context awareness	Data about the patient provided during system interaction may assist identify illness early and trigger alarms in crises, to provide good rationale of the general health of a patient.

Autonomy	The device's analytical expertise may be utilised to make it more adaptable by enabling it to treat people in the most appropriate method for them at the moment. The loop should be securely and swiftly closed in this manner.
Security and Privacy	Because MCPSs gather health records and organize the information they acquire, security and privacy are of the utmost importance. As a result, it's critical that no unauthorised party has access to or alters their data. A patient's privacy, discrimination, abuse, or even physical harm might result from such an act.
Certifiability	MCPS requires a low-cost method of demonstrating that biomedical device software is safe and dependable, e.g., clinical device certifications.
Executable clinical workflows	MCPS may be built and deployed fast in order to deliver effective medical services for a (particular) patient since more and more healthcare systems are connecting and working together. With MCPS, patients' security is the foremost concern. Consequently, we must guarantee patient safety in these cases by employing medical protocols that are legitimate and effective.
Model-based Development	Prior to building or developing a software system, we will be able to determine how safe the situation is for patients, and we will be able to establish requirements for safe equipment and their connections. To ensure that the application is safe, these standards may be inspected during deployment. Take note of the way scenario analysis is carried out using MCPS model-based growth. Static and dynamic vulnerability checks are the most difficult to understand.
Physiological close-loop control	Many individuals dislike employing automated control in medical treatment for a variety of reasons, including regulating an application to a specific location, doing many treatments at once that might influence a variety of bodily system in patients. It should be noted that experiences will be unique.
Patient Simulation and Modelling	Patient modelling is essential if we are to analyse how distinct conditions and closed-loop controls operate. It is fundamental to keep watch on elements such as clients' respiratory and heart rates in closed-loop PCA circumstances, as well as how much medication is being absorbed. More basic ways are needed to assist us in solving the difficulty of developing and analysing things. These techniques have the potential to simplify certain complex models.
Adaptive Patient and smart alarms	The majority of medical equipment is designed for use with several patients (having the same medical clinical conditions). In MCPS, patients may have a wide range of reactions to therapy, which may lead to confusion and loss of time. Most medical gadgets, for example, will sound an alert if a potentially harmful situation is discovered. Medical gadgets might potentially mistakenly send out false alerts. They don't have to deal with stuff like this in their line of work. For the benefit of patients and the collection of data for use in the creation of EHR Systems, healthcare systems are now establishing reliable network connections to accomplish this goal. In such situation, we'll need algorithms that can be customised to meet the unique requirements of each patient. Using the patient's activity record in EHR, we aim to alter alert settings so that there are less false alarms as well. Using "smart alarm services" in medical equipment in the near future will reduce the number of false alerts.
User Centred Design	If the caregiver is overworked or anxious or has difficulty operating a piece of equipment, they may make errors in their care. There are a number of ways that medical devices may be designed to be more user-friendly, such as providing interactive methods to learn how to operate the device in the event that the user gets stuck, and providing means for users to rectify errors so that they are satisfied with their gadgets.
Infrastructure for Medical-Device Integration and Interoperability	Distributed MCPS that use an exclusive network communication are currently being developed by just one business (lessening inter-device communication's advantages, while making regulatory clearance more straightforward). Open standards (interconnectivity) are the standard in the MCPS industry (establishing the foundation for medical device interoperability). It's still necessary for these standards to be utilised on systems that are simple to create and use. They must follow specific guidelines while making their goods so that they may function together and interface with each other in order to obtain the greatest benefit from them.
Compositionality	Using methods like contextual induction, it is possible to better understand how linked devices interact with one another, hence enhancing the security of MCPS systems. Figuring out how medical gadgets could interact in unexpected ways is the most challenging thing to

	undertake in this scenario. Due to their proximity to one another, radio interference may occur between medical equipment that provide various therapies to the same patient. Treatments might conflict with one another if the body's response to them changes. A good example of this is "mixed prioritisation". The sensor's position in regard to the patient determines the MAP measurement's accuracy. The MAP measurement changes when the patient's bed, which is a Class I medical equipment, is elevated, since it is the least significant in the FDA classification. False reports or other undesirable behaviour might result from the sensor's abrupt shift when it is component monitoring things like vital signs. This issue was utilised to provide the monitoring system with more information. Making these gadgets while taking into account is difficult.
Privacy and Security	There are a number of networking capabilities built into medical equipment that, when combined, might contribute to security and privacy concerns. If a hacker gains entry to the MCPS network, they might hurt or even kill individuals (by re-programming devices). Rehired gadgets that may be rehired through the local area network but do not get any requests from the networks might be restricted in this way. There must be a delicate balancing between freedom of travel and the requirement for security. A strategy is needed for coping with EHR system problems.
Verification, Validation and Certification	When the design is complete, verification and validation are performed. Currently, this is how things are going. By using a "design for verification approach," it will be possible to demonstrate the validity of the verification process on an ever-larger scale [10]. It is also possible to do verification earlier in the design process thanks to a technology known as model-based generative approaches. Keep in mind that run-time components may be created from medical devices.
High Assurance Software	Some elements of medical equipment, such as hardware (such as security locks) and other things, are automated with the help of technology. It is commonly accepted that software development is essential to the security of MCPS, however this is not enough.

IV. CONCLUSION AND FUTURE RESEARCH

This paper focuses on security analysis in CPSs, whereby security in CPSs, security threats in CPSs, and security challenges in CPSs, have been discussed. A contemporary Cyber Physical Systems (CPSs) is at its peak in terms of engineering, making it intricate and multi-scale structures that are versatile. The systems are employed in various fields in real-life, and they have significantly attracted the attention of researchers and the academia. CPSs have not become popular, but there are some major segments of the fields, which are not appropriately defined or that not sufficiently studied. It necessitates more efforts to make CPSs function in real-life. This incorporates a broader range of interdisciplinary expertise, as well as tighter integration of important enabling technologies and a focus on environmental and societal concerns. It is essential for networks to have a shared language, abstract structures, modeling techniques, and protocols that function together in a coordinated manner. In order for abstraction to work properly in CPS testing, execution, design, and conceptualization, all of these processes need strong methodologies and theories (also computational and conceptual abstraction, i.e., that are fundamental for both computer and human agents). Computational reasoning has to be employed for autonomous control systems (for the physical system) and for discrete virtual structure (of the physical system) in order to facilitate the writing, connecting, and building of CPSs (with high integration levels). Different concepts, e.g., time-correct controls and operations, compositionality, synergy and goal-centric learning, among others, also require investigation in future studies.

References

[1]. M. Mahmoud and M. Hamdan, "Improved control of cyber-physical systems subject to cyber and physical attacks", Cyber-Physical Systems, vol. 5, no. 3, pp. 173-190, 2019. Doi: 10.1080/23335777.2019.1631889.

[2]. "Programmable logic controller(PLC) in computer numeric controller(CNC)", International Journal of Recent Trends in Engineering and Research, vol. 4, no. 2, pp. 55-60, 2018. Doi: 10.23883/ijrter.2018.4063.fr80v.

[3]. D. Dietrich and H. Garn, "Embedded Vision System", EURASIP Journal on Embedded Systems, vol. 2007, pp. 1-2, 2007. Doi: 10.1155/2007/34323.

[4]. A. BORGEAT, B. SCHAPPI, N. BIASCA and C. GERBER, "Patient-Controlled Analgesia After Major Shoulder Surgery", Survey of Anesthesiology, vol. 42, no. 6, p. 354, 1998. Doi: 10.1097/00132586-199812000-00049.

[5]. S. Maitanmi, S. Ogunlere and A. Adio, "Shaping ICT Infrastructure Through Creativity and Innovation", Indian Journal of Science and Technology, vol. 12, no. 41, pp. 1-6, 2019. Doi: 10.17485/ijst/2019/v12i41/147513.

[6]. J. Park, "Smart Factory and Cyber-Physical Systems: Analysis of CPS Case Study", Regional Industry Review, vol. 44, no. 1, pp. 161-181, 2021. Doi: 10.33932/rir.44.1.7.

[7]. R. Singla and A. Khosla, "Intelligent Security System for HMI in SCADA Applications", International Journal of Modeling and Optimization, pp. 444-448, 2012. Doi: 10.7763/ijmo.2012.v2.160.

[8]. N. Saputro and K. Akkaya, "On preserving user privacy in Smart Grid advanced metering infrastructure applications", Security and Communication Networks, vol. 7, no. 1, pp. 206-220, 2013. Doi: 10.1002/sec.706.

[9]. T. Ehlers, "System integrity in vehicles with networked electronic control units", ATZ worldwide, vol. 105, no. 9, pp. 30-32, 2003. Doi: 10.1007/bf03224629.
[10]. G. Elber and E. Cohen, "A unified approach to verification in 5-axis freeform milling environments", Computer-Aided Design, vol. 31, no. 13, pp. 795-804, 1999. Doi: 10.1016/s0010-4485(99)00047-0.