Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 165 (2019) 647–655

Procedia Computer Science

www.elsevier.com/locate/procedia

INTERNATIONAL CONFERENCE ON RECENT TRENDS IN ADVANCED COMPUTING 2019, ICRTAC 2019

Medical Cyber Physical Systems and Its Issues

Meghna Manoj Nair[1], Amit Kumar Tyagi[1], Richa Goyal[2]
[1,]

[1]Vellore Institute of Technology, Chennai Campus,
Chennai, 600127, Tamilnadu, India.
[2]Pt. J.L.N. Govt. College, Faridabad, Haryana, India

Abstract.

In the previous decade, many technologies have attracted attention from several research communities. Internet of Things (IoT) is main invention of the recent/ past decade. When these smart devices or internet connected devices are interact together, then they create a cyber infrastructure. These cyber infrastructures face several serious concerns privacy, trust, security, etc. These smart devices make an automatic environment (executed without the intervention of a human) in applications likedefense, manufacturing, e-healthcare, etc. In e-healthcare, these devices built the structure of Medical Cyber Physical System (MCPS). MCPS are facing several critical issues and challenges in current era, i.e., several attacks, issues and challenges which we require to overcome in current and next decade to provide efficient and reliable service to patients. MCPS is need of smart healthcare and require attention from several research communities towards its raised issue. Hence, this article provides a detailed study about CPS, MCPS, mitigated attacks on same architecture (CPS and MCPS), issues and challenges in CPS/ MCPS, including several research gaps in CPS/ MCPS (with opportunities for future researchers).

Keywords:Cyber Physical System; Medical Cyber Physical System; Smart Devices; Cyber Security in E-healthcare; Issues and Challenges in MCPS.

* Corresponding author. Tel.: 9487868518.
E-mail address: amitkrtyagi025@gmail.com

10.1016/j.procs.2020.01.059

1. INTRODUCTION

Cyber Physical Systems (CPSs) are considered to be an integration of computation, networking and numerous physical processes as shown in fig 1. With an advent in technology and advanced sciences, CPS is put to use in a variety of fields including automotive, industries, medical arena, aerospace and much more. It basically is an interlink between the internet and its users and involves a multidisciplinary approach facilitating the need of a physical input and output. However, the medical field has been attaining much of importance in this present decade (in current/ smart era) and innovations and developments in this field are developing gradually. One daily life example has been mentioned in [1], in which authors discussed the human life activities/ living with intelligence (or internet connected things). But this critical application is also facing serious attacks on IoT based infrastructure. For the already existing systems, the major drawbacks of attack on these systems are either financial in nature or have been related to privacy. The preliminary stage in preventing such attacks from recurring would be to identify the safety related domains and integrate the fast-evolving technologies into these physical systems. In general terms, Cyber physical systems and Medical Cyber Physical System can be discussed as:

Cyber Physical Systems: Cyber Physical Systems are feedback systems which have been widely used in the realms of health care, automation, communication, energy, robotics, smart building, transportation, physical security, etc. CPS is very often regarded under the field of engineering with a great deal of abstractions. Note that it is the core subjects of computer science and mathematics over the decades. Usually, it focuses on dynamics and the processes of transforming data and algorithm respectively. Also, it supports communication and storage capabilities with monitoring and controls the enhanced entities in the physical world. Some popular issues (mitigated) in CPS are incorporating dependability, safety, security and efficiency in the real time and virtual world. We can include some characteristics of CPS as:

- Cyber capability in every physical component and resource constraint.
- Closely integrated.
- Networked at multiple and extreme scales.
- Complex multiple temporal and spatial scales.
- Dynamically reorganizing/reconfiguring.
- Closed-loop control and high degrees of automation.
- Operation must be dependable and certified in some cases.

Medical Cyber Physical Systems (MCPS): Systems which successfully incorporate the design of medical implementations in health care with CPS. They face numerous challenges related to privacy/security, inoperability, and high assurance of system software design to prevent MCPS attacks and destructions. MCPS systems are used in hospitals and clinics to automate the devices and machines used there and to provide personalized, customized and quality health care services for the patients. It whole heartedly embraces the potential of embedded software and network connectivity. Some of the applications of CPS in this field include intelligent operating rooms and devices, image and visually guided surgeries, therapies and operations, automated fluid flow controls to be used while injecting therapeutic medicines, development in physical and neural prostheses, etc. Clinical examinations and surveys, treatments and monitorings, and other devices generate complex heterogonous data [2] which may be structured, semi structured or non-structured. In general, CPS in applications like healthcare units are broadly divided as assisted and controlled. The architecture and design framework for the healthcare requires perspectives from the server based and cloud-based ones.

Hence, the organization of this article is followed as (in further sections): Section II discusses several attempts, made in previous decade (towards CPS/ MCPS). Further, section III discusses the motivation behind (working in) this area. In this section, we explain how MCPS is useful to our society/ industries? In continuation to next section, Importance of CPS and MCPS is being discussed in section IV. Further, popular attacks will be discussed in section V. Section VI discusses several popular issues and challenges countermeasures in CPS and MCPS. Then, solutions to measure/ mitigated attacks are discussed in next section VII, i.e., several better enhancements which have been made in previous decade towards MCPS, discussed in section VII. Then, section VIII discusses several modern solutions and opportunities (possible in near future) in CPS and MCPS (or other types of cyber-physical system). In the end, this article (or work) is concluded with several interested future remarks in section IX.

2. RELATED WORK

Cyber Physical System is the field in limelight today as it combines a plethora of fields catering to safety, schedulability, efficiency, and most importantly security. Communication network approaches indeed enhance the security protection systems from Supervisory Control and Data Acquisition (SCADA). Ensuring the secure transmission of data over the network and proper machine functioning play an important role in the viability of CPS. [3] Indicated that solving the security issues in CPS's must begin at the very start of the designing and manufacturing phase of it by developing appropriate tools and mechanisms. While in [4], the author's main concern of security is tackled by adopting a complementary approach consisting of approaches for acquiring multi-domain simulation, to provide attack resistivity and procedures and mechanisms that help in detecting the attacked hardware of the CPS. This can be put into practice by trying to identify the harmful sensors by injecting small excitations into the system and by detecting ones that report the wrong sensing values. In [5], let-downs and fault tolerance in CPS are shaped, where such CPS's are treated as widespread algorithms carried out by some agents and the processing of the CPS are abstracted in the form of distinct transitions. There are a number of other attack models including attack trees [6], where the root node adheres to the goal and aim of an attacker and a path from the leaf node to any of the root node denotes an attack instance, like the procedures for executing the attack [7] and so on.

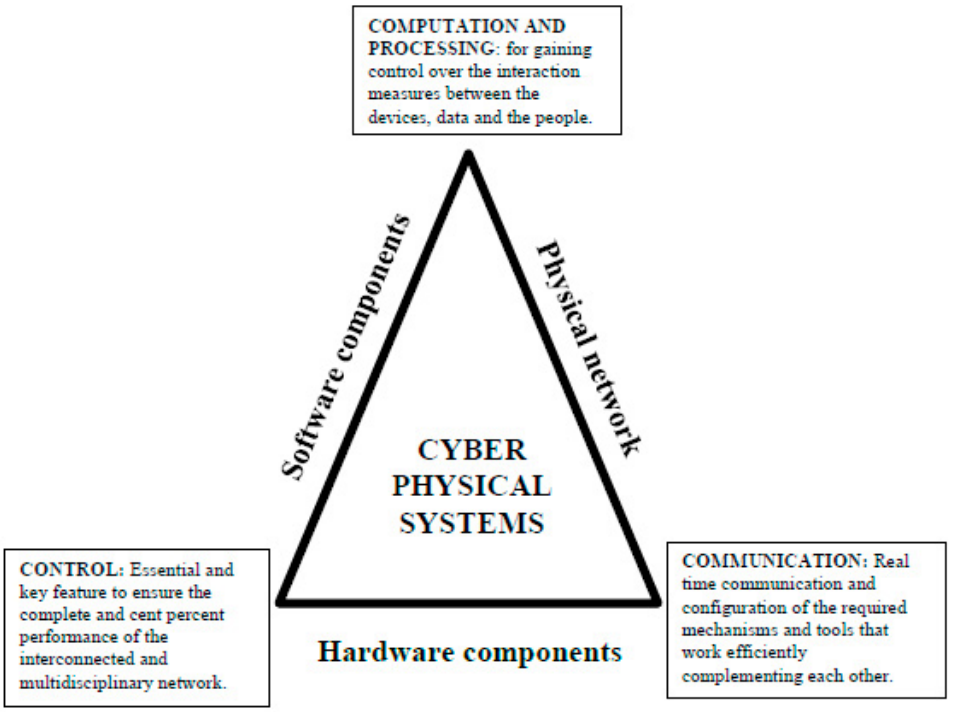

Fig 1: Structure of Cyber Physical System

Hence, this section discusses various terms, components related to control systems and cyber physical systems, etc. Now, next section will discuss our motivation behind this work or area (in brief).

3. MOTIVATION

Today we are entering into the age of innovative technical solutions. These solutions play a very important role in the growth of the nation, for example, cyber infrastructure using internet of things devices are being used in many applications/ sectors like control systems, smart cars, smart grid, e-healthcare, etc.But cybercriminals can

compromise these devices/ computers from anywhere/ control them from anywhere (according to their wish). Further, Terrorists, activists, and organized criminal groups areanother potential threat to this CPS/internet connected control systems. Also, nation states may also be a possible threat to control systems. Hence, designing of novel attack-detection algorithms, new attack-resilient algorithms and architectures are necessary things in CPS. We need to protect and avoid any compromise of attacks on such control systems. As a result, our main aim is to save as many human lives.Hence, this section discusses the motivation behind this work in brief. Now, the next section will discuss the scope and importance or necessity of control systems or cyber physical systems in 21st century.

4. IMPORTANCE OF CYBER PHYSICAL SYSTEMS (CPS) AND MEDICALCYBER PHYSICAL SYSTEMS (MCPS)

It has been identified as the core enabling disruptive technology essential to secure economic and social leadership in embedded systems and in the field of Information Technology (IT). These systems would play an important role in tackling a plethora of societal problems in the present and in the future. Here, it is considered to be the next generation of engineering systems pulling across great attention to itself. The fact that CPS acts as the point of convergence of several disciplines, evolving technologies in numerous fields and the need to build large scale systems to fulfil the societal needs emphasize on throwing light on the importance of CPS. They bridge the cyber world of computing, communications and virtuality with the physical or manual world known as CPS.

4 Importance of MCPS

The developments and design manufacture of CPS in the medical field has been on the rise since the last decade. It is because of the success in integration of embedded system analytics and medical devices that there's a rapid progression in this area. In current, Pace maker, medical ventilator, infusion pump, etc., are some of the modern research and design fields in Medical Cyber physical System (MCPS). Most of the systems incorporate a large number of physical devices including sensors, gyros, etc., to generate, sense, analyse and share large quantities of medical data for processing. However, there are a large number of hindrances and obstacles one faces while designing the structure and chassis of such kind of devices and machines. These include positioning of patients, large scale communication and computation along with scalability.This section discusses about scope and importance of cyber physical system and medical cyber physical system in various sectors/ applications. Now, next section will discussseveral (mitigated) popular attacks on CPS and MCPS in detail.

5. POPULAR ATTACKS ON CYBER PHYSICAL SYSTEMS AND MEDICALCYBER PHYSICAL SYSTEMS

A cyber-attack is defined as an attack on computer systems/architecture, or information systems with malicious and disastrous intentions and to exploit these resources. The attack is usually in the form of an individual or group acting against other civilian groups in the society with the mind set of acquiring unsecured and valuable personal data from the victim.Cyber-attacks on Cyber Physical Systems (CPSs) are on the rise as physical systems become more interconnected and are higher in number. Now, some types of attackers for CPS and MCPS.

5.1 Types of Attackers in Cyber Physical Systems

External Threats: An external threat is any vulnerability which can be exploited to gain access to an environment from outside that environment [8]. Some of the eternal threats re listed here in CPS as:

- Cyber Criminals: They include an individual/a group of people who use the advent of technology to commit cyber-crimes to retrieve personal data and information from organizations or companies to generate profits.
- Hacktivists: They are the group of people who take on to malicious activities for political or religious agenda, through which they feel that they are fighting political injustice.
- State-Sponsored Attackers: They have specific objectives in coordination with either the political, commercial or military interests of their nation.

- The government has a number of skilled hackers in detecting vulnerabilities and exploiting them before the holes are patched.

Insider Threats: It involves threats to an organization's security or data that comes from within and mainly includes former/current employees working in the particular organization. These types of attacks are critical to detect, because they are being done from inside the infrastructure (and depends on trust-component) [8].

Types of Attackers in Medical Cyber Physical Systems

- Data Breaches: They are malware-based attackers who retrieve highly confidential medical data from the healthcare industries and sell it for personal gains.
- Ransomware Attackers: These types of attackers critically disable the server or the computer system until a ransom amount of money is not handed over to them. In critical applications like e-healthcare, it tends to be life threatening for the patients if the attackers meddle with the healthcare devices.
- Social Engineers: They look forward to exploiting the healthcare network's security system by targeting the hospital staff.This is easily executed by sending emails and tricking them into clicking some link which helps in retrieving the passwords and other data.
- Insider Attackers: Even the most secure MCPS is easily handled by these attackers as they consist of the disgruntled and criminally motivated employees who have intentions of turning up against their own organization due to some past records [9].

Now, some popular attacks on cyber physical systems are listed as:

Stuxnet: It is an extremely complicated computer worm that exploits many of the previously unknown Windows zero-day vulnerabilities to infect computers and PC's and spread. The main aim of this Stuxnet was to cause real-world physical effects. By targeting centrifuges, it used to produce the enriched uranium that powers nuclear devices, weapons and reactors.When infecting a computer, it checks if the computer is connected to specific models of Programmable Logic Controllers (PLCs) manufactured by Siemens [10]. PLCs are used to identify how computers interact with and control industrial machinery like uranium centrifuges. The malicious worm then alters the PLCs' programming and algorithm, resulting in the centrifuges being spun too fast and for too long.Thisdamage or destroy the delicate equipment in the process.While this happens, the PLCs convey a fake message to the computer controller that everything is working fine, masking and hiding what is running in the background.We can say that Stuxnet was created by the intelligence agencies of the United States and Israel. This program was used to develop the worm was given the code name "Operation Olympic Games" initiated by President George W. Bush and continued by President Obama. The U.S. and Israeli governments created Stuxnet as a tool to derail and delay the Iranian program to develop nuclear weapons.

Distributed Denial of Services (DDoS): It is a malicious attempt to destruct normal traffic of a particular server, service or network by overwhelming the goal or surrounding infrastructure with bogus data or a flood of internet traffic. They mainly achieve effectiveness by making use of many computer systems as sources of attack traffic [11].It is compared to a traffic jam which clogs up the highway, preventing the regular traffic from reaching its desired location.Some recent DDoS attacks are those of GitHub (2018- through memcaching rather than botnets which took down GitHub for around 20 mins only because they had an efficient DDOS mitigation service that detected it and minimized the effect immediately), DYN (2016- with the help of a malware called 'Mirai', they executed the then largest DDoS attack using botnet involving massive trickle down effects), etc.

Man in the Middle Attack: This is a type of attack that occurs when the hacker himself intercedes the communication between the server and the client to extract useful and valuable data [12]. It executes the hack by substituting the IP address of the hackers' computer with that of the client's and hence deludes the server as the server continues to communicate with the hacker assuming that it is the true client. In 2014, Lenovo installed MITM (SSL Hijacking) adware called Super fish on their Windows PCs as a modern solution to prevent MITM. In 2015, a British couple (the Lupton's) lost £340,000 in an email eavesdropping/ email hijacking MITM attack which was indeed a fatal loss for them.

Phishing Attack: It involves the practice of sending emails which appear to be from trusted sources but actually intends to load some malicious malware into the target system without the knowledge of the client in the form of a mail attachment or any other plausible source.This can be minimized with the help of sandboxing-a technique used for testing the email content before its put into use.

Insider Attack: It is considered as an attack executed by a professional who has authorized system access and hence, he or she can be tagged as a traitor.They intend to attack all computer security elements and range from stealing sensitive data to inducing Trojan viruses in the network.

Similarly, now some popular attacks in Medical Cyber Physical Systems are included as:

- When it comes to cyber physical system attacks in the medical field, the main motive behind doing so is to either breach the privacy and medical details of the patients or personal information of patients, directly influencing the patient by injecting false commands and information with the help of wireless tools, etc.
- DOS attacks are the most common type of CPS attacks in the medical field which retrieves the patient's details and passes it onto hands which misuse it.
- Another common type of attack is UDP (User Datagram Protocol) Flood which aims at sending large number of data packets to the targeted server with the motto of freezing it to any further responses, replies, processes and feedbacks such that the firewall in charge of it may also get exhausted.
- The next popular type is the ICMP (Internet Control of Message Protocol) Flood attack wherein the attacker takes down the system by sending overwhelming number of ICMP requests, hence exploiting all the available bandwidth and denying legitimate access to the authorized users.

Hence, this section discusses several mitigated attacks (including types of attacks) like Stuxnet, Phishing, Man in Middle, etc., attacks on CPS and MCPS. Now, next section will discuss several issues and challenges in CPS and MCPS.

6. ISSUES AND CHALLENGES IN CYBER PHYSICAL SYSTEMS AND MEDICALCYBER PHYSICAL SYSTEMS

Nowadays cyber-physical systems are widely used in many applications, the security considerations of these systems should be of very high importance. Compromise of these systems (via many security vulnerabilities, attacks) in critical infrastructure will cause serious consequences [13]. We require efficient security countermeasures into cyber-physical systems to overcome such attacks. Also, patching and frequent updates are not implemented or updated correctly in cyber physical systems/ control systems.Some new research Challenges in MCPS are High assurance software, Interoperability, Context awareness, Security and privacy, and Certifiability[14].

In summary, MCPS open doors to many researchers, sectors, etc., with respect to overcome security and privacy concerns.Note that designing of an efficient CPS architecture with good styles, and designs is a big issue. We require a multi-view, multi-stakeholder, extensible framework for designing and validating early design decisions taken when architecting CPS. Hence, many issues like security, privacy, trust in many cyber physical systems have been discussed in table 1 (refer appendix - A). Some challenges towards CPS (in general) are in terms of Modifiability, Performance, Dependability, Portability, Flexibility, Heterogeneity, Reliability, Maintainability, Verifiability and Compatibility. Hence, this section discusses several critical issues and challenges in CPS and MCPS. Now, next section will discuss several suggestions/ solutions towards MCPS in the last decade.

7. SOLUTIONS, TOOLS TOWARDS MEDICALCYBER PHYSICAL SYSTEMSIN THE PREVIOUS DECADE

In the past few decades, people have been trying to make use of body sensor networks or wireless body area networks to reduce the amounts of wire connections and physical inputs required. Intrusion Detection Systems (IDS) are used to identify the hacker patterns and the algorithms used to destroy the CPS in medical field. However, the installation of IDS is a difficult task as it is hard to connect to MCPS actuator systems. Earlier even homomorphic encryption was put into implementation. It is a basic form of encryption which mainly allows computation and processing on cipher-texts and data and generates an encrypted result, which on decryption would match the result of the operations as if they were performed on the plaintext [15].

Tools and Mechanisms for Detecting These (Mitigated or Listed in Section V) Attacks

- Hyper Network Model of Statistical Analysis System (SAS): It has a simple structure with a protection scheme and other functions usually in use for other types of transmission substations.

- Each function consists of multiple Logical Nodes (LNs). A Logical Node (LN) is a sub-function located in a physical node, which exchanges data with other separate logical entities [16].
- It acquires data from current transformers and voltage transformers, and calculates the measurands.
- In the hyper-network model of SAS, a function which consists of a set of logical nodes, a hyper-edge participates in multiple functions and is more generic and helps in identifying the critical data retrievers.

Hence, this section discusses several existed solution, tools and mechanisms to overcome/ detect these attacks (in the previous decade). Now, next section will discuss several modern solutions towards MCPS (including many opportunities) for the next decade.

8. MODERN SOLUTIONS AND OPPORTUNITIES TOWARDS MEDICAL CYBER PHYSICAL SYSTEMS

One of the modern solutions to tackling attacks on MCPS is nothing but to implement Virtual Private Network (VPN). VPN basically virtualizes the private network and makes use of strong security solutions for providing private communications over the public physical network. A VPN is an alternative to a private network or a private leased connection. To overcome the problem of Intrusion Detection System (IDS), a new methodologies likeEDADT algorithm, hybrid IDS model, semi-supervised approach and varying HOPERAA Algorithm [17].Also, one method is introduced recently [18], which is based on behavioural rule details and intricacies for defining normal behavioural patterns for any given medical device or machine. They are capable of testing medical sensor measurements and actuator settings to detect the malfunctioning of physical properties visible because of attacks.

Opportunities in Medical Cyber Physical System: The fact that CPS in the medical field is only in its gradually developing stage itself can be considered as one of the main platforms for developing and innovating ideas in this field. The ideology of interdisciplinary approach integrating robotics, Artificial Intelligence (AI) and medical knowledge together increases the precision and accuracy rates and help in increasing the efficiency of the CPS[19]. Opportunities for future research in CPS can be as: achieving reliability via a dedicated middleware, component-based reasoning for performance improvement and flexibility by adopting the aspect-oriented programming model, portable agents. Further, we find that most of the research challenges (listed in section VI) are mostly unsolved and we believe that future research in these areas can provide an additional level of security to respective CPS/ MCPS.Hence, this section discusses several modern solutions, opportunities for near future towards MCPS. Now, next section will conclude this work in brief.

9. CONCLUSION WITH FUTURE REMARKS

Medical Cyber-Physical Systems (MCPS) is an application of cyber physical system in a sector, like that a CPS can be in many applications like smart grids, smart cars, industrial control systems (ICS), etc. Several mitigated issues have been included in table 1 (refer appendix - A). MCPS are healthcare critical integration of a network of medical devices. MCPS systems are progressively used in hospitals/e-healthcare application to get quality and efficient (cheaper), i.e., high-quality healthcare services. But, as we have seen and discussed that MCPS design faces several challenges like inoperability, security/privacy, and high assurance (in system software). We see that MCPS faces unique set of challenges, different from any other CPS domain.

Hence, in this article infrastructure, importance/scope of CPS, etc., have been discussed in detail (to enrich the knowledge of researches, related to networked Medical Device (MD)). Our main aim is to improvethe efficiency and safety in e-healthcare applications. Through that, we can assist doctors/specialists of hospitals/medical device to solve many crucial issues (related to medical machines/ devices) or challenges facedin the design of the medical device's network. Hence, researchers who are willing to or are interested in working in/towards raised issues are kindly welcome to continue their research work (in near future).

References

[1] Amit Kumar Tyagi and Shamila.M. (2019).Spy in the Crowd: How User's Privacy is getting affected with the Integration of Internet of Thing's Devices.Elsevier.

[2] Raghupathi, W. and Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health Information Science and Systems.
[3] Al Faruque, M., Regazzoni, F. and Pajic, M. (2015) Design Methodologies for Securing Cyber-Physical Systems. Proceedings of the 10th International Conference on Hardware/Software Codesign and System Synthesis, Amsterdam, 30-36.
[4] Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A. and Uhsadel, L. (2007) A Survey of Lightweight-Cryptography Implementations. IEEE Design & Test of Computers, 24, 522-533. https://doi.org/10.1109/MDT.2007.178
[5] T. Johnson. (2010).Fault-tolerant distributed cyber-physical systems: Two case studies, Masters Thesis, University of Illinois, Department of Electrical and Computer Engineering, Urbana, USA.
[6] B. Schneier. (1999)Attack trees, Dr. Dobbs journal, vol. 24(12), pp. 21–29.
[7] C. Ten, C. Liu, and G. Manimaran. (2008). Vulnerability assessment of cybersecurity for SCADA systems, IEEE Transactions on Power Systems, vol. 23(4), pp. 1836–1846.
[8] https://www.techopedia.com/definition/26217/insider-attack
[9] https://www.javatpoint.com/types-of-cyber-attackers
[10] https://www.csoonline.com/in/
[11] Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reiher (2004), Internet Denial of Services: attack and defense mechanisms
[12] Kyoung-Dae Kim and P. R. Kumar (2016), An Overview and Some Challenges in Cyber-Physical Systems, 5-6.
[13] Alvaro A. Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry, Department of Electrical Engineering and Computer Sciences. University of California, Berkeley, Department of Civil and Environmental Engineering. University of California, Berkeley, Department of Electrical and Computer Engineering. Carnegie Mellon University (2014), Challenges for Securing Cyber Physical Systems.
[14] Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat (2018), Cyber-physical systems and their security issues, 2013-2016.
[15] Jaime A. Camelio, Chair Lee J. Wells, Co-Chair Zhenyu (James) Kong William H. Woodall (2018), Quality Control Tools for Cyber-Physical Security of Production Systems, Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University, 51-56, https://ieeexplore.ieee.org/document/8514197
[16] Fabio Pasqualetti ,Florian Dörfler , Francesco Bullo (2013) Attack detection and identification in CPS, Volume: 58 , 200-220, Issue: 11.
[17] Z DeSmit, AE Elhabashy, LJ Wells, JA Camelio(2016), Elsevier, Cyber Physical Vulnerability Assessment in Manufacturing Systems, volume 5, 1063-1065.
[18] A J Cochenour. (2016). Behavioral model based malware protection system and method. US Patent 9,386,034.
[19] Ivano Malavolta, Henry Muccini, Mohammad Sharaf (2015), A Preliminary Study on Architecting CPS, proceedings of the 2015 European Conference on Software Architecture Workshops- ECSAW'15.
[20] Rafiullah Khan , Kieran McLaughlin, John Hastings David Laverty , Hastings David ,Sakir Sezer (2018) [16th Annual Conference on Privacy, Security and Trust (PST)] Demonstrating Cyber physical Attacks and defense for Synchrophasor Technology in Smart Grid, 20-21, https://ieeexplore.ieee.org/document/8514197.

Appendix – A

	Types	Security issues	Privacy	Trust	Advantages	Disadvantages
CPS	ICP	Loss of large economy benefits or social data.	They generate, process, and exchange vast amounts of security critical and privacy – sensitive data.	With an advent of Internet of Things (IoT), they promise a trustworthy working environment	They have made Machine to Machine interaction an easy task.	Managing and cooperation between the interconnected machines in the working environment.
	MCPS	Sensitive information of patients on being interrupted can lead to fatal consequences if data not in secure hands.	Privacy in the field of preserving health poses a challenge in MCPS.	The increasing complexity and efficiency of IC'S and microcontrollers in use, increase the trust factor.	Highly beneficial for the patients to receive a customized health care report and guidance.	Tackling the problem put forward by dealing with the context of uncertainty over the patient's life.
	SMART GRID[20]	They are susceptible to privacy and security issues.	There is an increasing concern over the privacy issues I n this system.	Fog computing paradigm proves to be trust attracting component in smart grid.	The possibility of processing real time critical data which are large in size.	Coping up with the construction of advanced smart grid with data analyzers in detail.
	DIST. ROBOTICS	Locks, priority inversions and interrupts usually break the formalisms.	It would depend mainly on the design and accuracy of construction.	Heavy use of legacy systems and large network platforms make trust issues vulnerable.	The bots can be exploited to full potential in a variety of fields.	Loose coupling of networks leads to huge data losses between the interconnected bots.

	AUTOMATED PILOT AVIONICS	Forecast traffic increase, capacity security, etc. are factors which reduce the security viabilities.		Considering the driver to be responsible for complete authority, trusting an automated machine in doing so poses a threat.	Its generic applicability across all transportation sectors for ease and convenience.	Weaknesses to gain unauthorized access over system control during flight time.