International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 12 | Dec 2018 www.irjet.net p-ISSN: 2395-0072

Architectural Modeling and Cybersecurity Analysis of Cyber-Physical Systems - A Technical Review

Sachin Sen[1], Paul Pang[2]

[1]*Lecturer (Part-Time), Dept. of Computer Science, Unitec Institute of technology, Auckland, New Zealand*
[2] *Professor, Dept. of Computer Science, Unitec Institute of technology, Auckland, New Zealand*

Abstract:- *Cyber-Physical Systems (CPS) are heterogeneous systems in which computing and communication systems are interacting and controlling physical dynamics. By the best use of computing devices, communication technologies and being integrated with physical systems, CPS have been leveraging the economy. But as the CPS research is still in its early stages, lacks sufficient standards, and efficient system architectures; as a result, CPS research is progressing slowly. On the other hand, due to its integration with the public internet, security has become a critical concern. This technical review has focused on architectural modeling by splitting the CPS in different categories, as well as analyzes foreseeable cybersecurity concerns. The review also has identified some challenges and issues of this emerging systems and has explored future research directions.*

Key Words: Technical review, cyber-physical systems, Internet of Things, cyber domain, physical domain, CPS, IoT.

1. INTRODUCTION

THIS technical review has produced a comprehensive report on Cyber-Physical Systems (CPS) and the Internet of Things (IoT) by addressing architectural modeling and analyzing cybersecurity aspects of these technologies. A CPS is a mechanism tightly integrated with the internet and its users, which is controlled by computer-based algorithms. Physical and software components are deeply interconnected in CPS, each operating on different spatial and temporal scales, exhibiting distinct and multiple behavioral modalities, and interacting with each other in many ways which change with context [1]. The Internet of Things can be defined as the network of home appliances, physical devices, vehicles and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to exchange and connect data [2]–[4]. IoT has created more opportunities for more direct integration of the physical world into computer based systems, resulting in reduced human exertion, economic benefits, and efficiency improvements [5]–[7]. CPS are being leveraged by the IoT and/or IoE due to their similarity of application areas. CPS and the IoT are similar in their functions and share the same basic architecture. Nevertheless, CPS presents a higher level of coordination and more potential combinations between physical and computational elements [8]. An integration between the cyber and physical worlds, along with the interaction with the IoT, has been reflected in Figure 1.

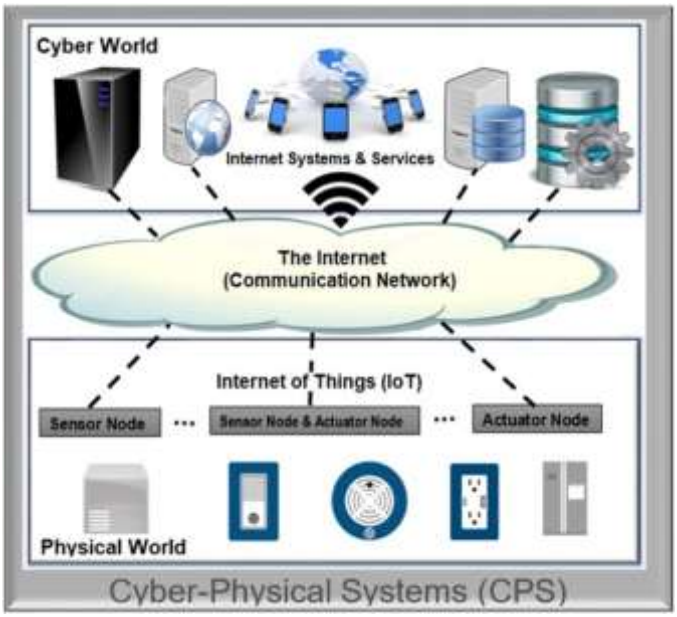

Fig. 1. Cyber-Physical Systems (CPS) Integrated with the Internet of Things (IoT).

CPS are an emerging technology and have attracted the attention of a large amount of researchers, business communities, and industries. The ”cyber system” typically consists of computing, control, and networking, while the ”physical dynamics” include the mechanical, electrical, thermal, biological, and chemical behaviors of the physical entities. The National Science Foundation (NSF) of the USA identified CPS as a key research area in 2008, and was listed as the number one research priority by the President’s Council of advisors of the US on science and technology [9]. The modern grand vision of real-world CPS have been enabled by the heterogeneous composition of computing, sensing, actuation, and network communication [10]. In CPS, computing, networked communication, and control are closely tied with the physical dynamics [11]. The CPS is the computer controlled Physical System and communicated through Computing Networks; it requires a certain layered approach, which may not be similar to the traditional Computing Networks, due to the different nature of CPS.

The way in which we conduct business, entertainment, studies, research, etc. has been influenced by the internet over the last few years, however, there are still some gaps in information exchanging in the physical world; CPS is intended to fill out those gaps by providing a broader view of how the computing domain interacts with the physical domain [12]. CPS possess multi-dimensional system features which integrate and coordinate between physical control and computing processes, combined with the network of distributed elements with the capability of computation, communication, and control, and highly rely on tight collaboration of those capabilities [13]. Due to their heterogeneity and sophistication, CPS require radical changes in the way sense and control platforms are designed to regulate the whole collaborative system [11].

CPS are used for communication, control, and computation of data from physical entities by using sensors. CPS can be used in social behavior optimization, as the world we live in consists of many varieties of societal elements such as animals, birds, insects, and humans, and their complex social behaviors can have effects on the world around them. CPS can be used to monitor and optimize the social behavior of these social elements [14]. The major application of CPS are in the area of intelligent transport systems, smart national infrastructure, national healthcare systems, robotic control systems, and/or any national disaster situations or emergencies. The common feature of those systems/applications is that those require a large number of sensors to be deployed over a wider area in order to implement complex control and monitoring functions [15]. Therefore, in order to transport real-time information from a wide number of sensors, the main challenge is to develop a scalable communication architecture [15].

CPS could form and interact through wired, wireless, or mobile network media, therefore, CPS can be operated through the combination of these three categories of network media. The system's physical dynamics will be sensed through IP-based sensors; the sensors will form a Wireless Based Access Networks (WBAN) in a heterogeneous environment. Therefore, the communication within the WBAN will occur through a multi-layered communication model or platform, as per requirements of the specific application area or scenario.

The communication architecture which suits Wireless Sensor and Actuator Networks (WSAN), and specifically, is suitable for IP-based Sensor Networks (IPSN), are more appropriate in this environment. A number of papers have been written, published, and presented in the internationally reputable communities, journals and symposiums regarding the architecture of the CPS and communication platform within the CPS environment.

CPS are systems of collaborating computational elements controlling physical entities, and thus can be found in areas as diverse as the aerospace and automotive industries, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances. This system is often referred to as embedded systems; in embedded systems the emphasis tends to be more on the computational elements, and less on an intense link between the computational and physical elements.

This review will produce a comprehensive report about the technical aspects of CPS, focusing on the architectural modeling, cybersecurity, issues, and applications of the whole CPS infrastructure. The rest of the document is organized as follows: Section II will provide an overview of Cyber-Physical Systems, which will include a brief history of CPS, why CPS are required, notations and definitions used in the report, and categorization of the CPS architecture. Section III through to Section V will discuss different categories of CPS, category-wise CPS architectures, their modeling, system stabilization, etc. Section VI will outline the design challenges considering application aspects and issues. Section VII will analyze cybersecurity, security issues, and challenges. Finally, section VIII will conclude the report with some future research directions.

2. OVERVIEW OF CYBER-PHYSICAL SYSTEMS

Technical advances in computing and information technology have reached such an era that computers and computing technology have made dramatic changes to the people of the world and their lives. People used to think of the computer as a PC and computing as browsing the network and the internet, whereas now most computers and computing devices in the world have become components of CPS.

In the cyber-physical context, different domains such as electronic system design, control theory, real-time systems, and software engineering are involved; the communication in which links among sensors, computational systems, and actuators, is another important aspect of the cyber physical systems [16]. A cyber-physical network is designed to access different types of networks such as Wireless Local Area Networks (WLAN) and Wide Area Wireless Access Networks (WWLAN) ubiquitously; Jia Shen et al. in [17], have proposed such a CPS multilayer heterogeneous framework. The networked computing systems with the integration of physical systems/processes have evolved the new generation CPS with the combination of science, technology and engineering. The CPS use network communication and computation that embeds and interacts with physical dynamics to add newer capabilities to the physical processes. In CPS, a physical layer

transports data from the physical dynamics to the cyber layer through the communication network, and the cyber layer transmits instructions using man-machine interface or actuators to the physical layer [18]. The interconnection between the physical world and the virtual world is reflected by these cyber-physical interactions; a graphical representation of such cyber and physical interaction has been given in [18] as Figure 2.

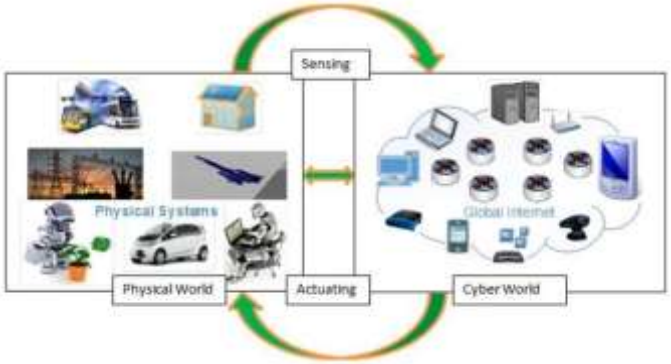

Fig. 2. CPS Architecture of Interaction between Physical and Cyber World.

CPS have been leveraging the economy by the best use of computers, computing devices, network computing/communication technology, integrated with physical systems. CPS range from small scale physical systems such as pacemakers to huge scale national infrastructures. As CPS have been interacting among physical systems and computing and networked communications, they have evolved from the combination of computer science and engineering, rather than from just one or the other. Therefore, this is a completely newly evolved technology which utilizes both computer science and engineering methodologies. The cyber world has explored this new era of technology where the existing technologies such as computing, computer science, engineering, and engineering science contribute hugely. The complete Cyber-Physical System is specifically designed as a network of elements interacting with physical input and output instead of the devices running standalone, which ties closely with sensor networks and the robotics concept.

2.1 Background and Context

CPS are critical to real-time awareness of the environment or situation, are used to control a broad growing range of applications, which include medical devices, advanced robotic devices, autopilot systems, smart energy-efficient buildings, modern agricultural systems, and advanced manufacturing systems [19]. Due to integrated solution methods and their usefulness for monitoring and optimizing growing critical physical environments, CPS have attracted industries, universities, the world's major vendors, and motivated researchers to put significant attention towards the research of the capability and effectiveness of CPS.

The National Science Foundation (NSF) of the USA was attracted by the growing technology of CPS since 1995 and started finding more about this growing technology; they have funded a significant amount for CPS research since then [18]. In addition to funding, NSF has been organizing regular technology events and conferences on CPS, and especially since 2008, CPS week has been held by the NSF on a regular basis [18].

Today, Cyber-Physical Systems are one of the central attractions of international research and business communities, and appear in the world's top platforms like ACM and IEEE. Both ACM and IEEE have been organizing the "International Conference on Cyber-Physical Systems (ICCPS)" regularly every year since 2010 at different world venues. Cyber-Physical Systems are a new generation's engineered systems, and have integrated computational and physical capabilities, and embedded computing interacts with humans through many new modalities. This allows for quick detection and reporting of necessary physical dynamics, due to the capability of CPS and their integration of computational and physical processes [20]. CPS provide real-time, secure, dependable, and efficient operations for quality data communications.

Embedded computing systems add capabilities to the physical systems, which in turn make the computer controlled physical systems increasingly efficient. Networked communication and computation integrating with physical systems evolve a new era of opportunities, which is more efficient, reduces building and operating costs, and also adds new capabilities in managing complex physical system dynamics. CPS are an application-specific technology, and its decreased cost of sensing, computation, and networking are technological and economic drivers for a new era of computing. More efficient technology and lower operation costs are the main economical drivers which push CPS to the technological forefront as new and modern engineering systems.

It is generally acknowledged that the embedded computing system allows people to add capabilities to physical processes or systems, and that there seems to be no other alternate technology which allows for performing and gaining such computing advantages. Integrated computing and mechanical systems can produce smart automobile systems, computing system integrated with electrical power systems can make national infrastructure Smart Grid systems, and computing and communication systems, when integrated with robotics systems, evolve to form efficient cyber-physical robotic systems, the applications of which include smart health systems, disaster management, and emergency situation management.

Therefore, by merging communication and computing with physical dynamics, we can see that CPS bring tremendous benefits to the way the physical world is being interacted. In CPS, individual computing devices, when working together, can form complex systems, resulting in new capabilities which are safer, more efficient, and effectively allow for a reduction in terms of cost. Though CPS has been identified as one of the major evolving technologies, it's research still in the early stage. The CPS communication, therefore, do not have established architectures and standards; this necessitates architectural modeling of this huge technology. The CPS technology can support from small scale pace maker to large scale smart grid as well as smart transport systems, which can result in a very complex management and operation procedures. Therefore, the CPS needs to split into different categories as proposed in the next section and model accordingly, in order to make it's management and operation easier.

2.2 Categorization of Cyber-Physical Systems

In Cyber-Physical Systems, when we consider monitoring or optimizing physical dynamics, often questions arise, such as (1) "what to perform", (2) "how to perform" and (3) "when to perform". These questions also depend on the types of environments or situations that are to be handled.

"What to perform" refers to the physical dynamics of the system, such as properties, status, and other necessary parameters of the physical systems or entities. These physical dynamics are varied in nature for different physical entities or applications. "When to perform" asks for perfect timing of the physical dynamics of the systems to be monitored and optimized. CPS are used to deal with real-time data, and therefore the dynamics are to be sensed in real-time.

Though data, properties, or parameters are different for different physical systems, "what to perform" and "when to perform" are common to most systems, i.e. how real-time data or dynamics should be sensed for all physical entities in CPS.

The other question, "how to perform", depends on the environment. CPS expect to perform in any situation or environment. This could be sensing data for a single physical entity like health monitoring of a single patient, a robotic surgery system, or traffic monitoring for certain parts of a city, etc. CPS can be applied for bulk sensor networks in a distributed system, such as a massive disaster situation, city wide traffic monitoring, i.e. for vast area-wide systems. We can also apply Cyber-Physical Robotic Systems (CPRS), where we can use a single robot or robot teams for interacting with certain situations such as remote human unreachable disaster situations, smart manufacturing plants, smart gardens, etc. We can use wireless sensors for all of those situations, like integrated smaller systems or distributed systems. Due to the major development of mobile handheld equipment, we can collect real-time information or data through mobile or handheld devices. This could include the robotics technology as well. For example, we can collect security information like intruder or burglar alarm data through smart mobile phones, we can collect real-time information about traffic incidents through mobile devices, and we can even manage smart construction systems using network connections from smart tablets. Mobile robot teams can be very useful for a search and rescue situations in a disaster event. Nowadays, a number of handheld devices, such as PDAs, smart 4G phones, Windows phones, tablets and iPads are available, which are very useful in communicating real-time information as and when required.

Based on the nature of the cyber-physical environments and different situations discussed above, the CPS are categorized as, (1) Integrated Cyber-Physical Systems (ICPS), (2) Distributed Cyber-Physical Systems (DCPS), and (3) Mobile Cyber-Physical Systems (MCPS).

In CPS, it is obvious that communication needs to be real-time, faster, secure, and lossless. The communication domains interact with the physical domains using real-time computing and control in order to meet the environment of the physical domains, where services are required to collect real-time parameters of the physical dynamics. In CPS, the communication domain uses Wireless Sensor Networks (WSN) to collect real-time dynamics sensed from the physical entities. Data communication can also occur through hand-held mobile devices as well.

The Cyber-Physical Architectures are formed according to the category of the CPS and obviously, according to the requirements of specific applications. Table I shows the characteristics of Different Cyber-Physical Systems. The categorized CPS and their architectures are discussed in details in the following three sections.

TABLE I CHARACTERISTICS OF DIFFERENT CYBER-PHYSICAL SYSTEMS

Types of CPS	Categorywise Characteristics of Cyber-Physical Systems		
	Definitions of Different Category CPS	*Architectural Approach*	*Communication and Control*
Integrated CPS	Traditional, localized control	Top-down	Locally
Distributed CPS	Physical devices are widely distributed, sensors arbitrarily distributed and sensed data contain external environmental input	Both Top-down and Bottom-up	Globally
Mobile CPS	System controlled with mobile/handheld devices, therefore mobility and motion controls are taken into account	Both Top-down and Bottom-up	Locally and Globally

3. INTEGRATED CYBER-PHYSICAL SYSTEMS

The traditional Cyber-Physical Systems are referred to as integrated, contained in a local area, are real-time, and are securely communicated between the communication domain and physical domain using sensors, actuators, and the computational units. Examples of such systems are control of nuclear power plants, robot controlled remote surgery, flight control for fighter jets, security systems for buildings, etc. [21].

3.1 Architecture of Integrated CPS

The cyber-physical architectures of integrated CPS are application-specific and the control area is localized. The research base of CPS depends on an accurate architecture, whereas there aren't any generalized architectures or frameworks to be used in most of the applications [22]. The architecture of this category of CPS are vertically integrated [21]. The architectures of integrated CPSs vary from application to application; for example, the CPS architecture of monitoring city traffic is different to that of health monitoring systems. Following figure 3 is a sample architecture of such systems.

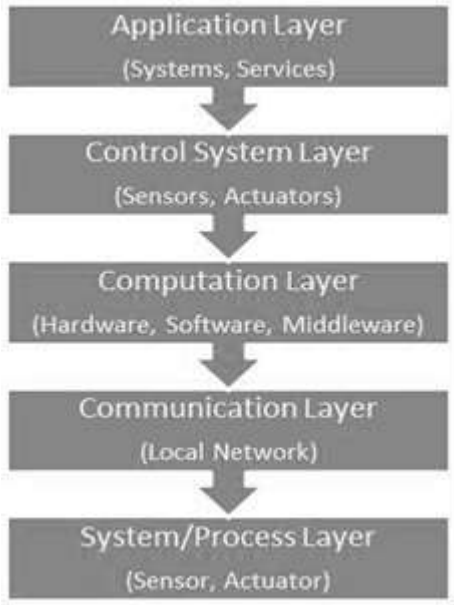

Fig. 3. A sample Integrated CPS Architecture.

3.2 Modeling and Stability Analysis of Integrated CPS

In any complex system design, mathematical modelling is very important, especially for physical systems, as no physical system is deterministic. In [23], Ghorbani et al. have provided a mathematical model to capture characteristics of the dynamics of blood glucose. Stability of the system also is a major concern. When CPS is applied to manage and monitor a critical situation, the instability would cause due to delay in communication, which also could cause packet loss during data transfer. Therefore, system stabilization would have to be considered seriously in such system design considerations. This report has reviewed modelling and stability of CPS using a Passivity Model proposed in [24].

A system is passive or stable when a storage function exists and the stored system energy is bounded by the supplied energy to the system [24]. The powerful tool for system analysis and control system design, is the raditional passive

systems theory [24]. Here, a system $\sum$ has been considered with the following definition:

$$\dot{\psi}(t) = f(\psi, u) \quad (1)$$

$$y = g(\psi, u) \quad (2)$$

where $\psi \in \Psi \subset \Re^n$ is state of the process, $u \in U \subset \Re^m$ is the input to the control system and $y \in Y \subset \Re^p$ is the control system output. The system $\sum$ becomes passive or stable if a storage function $W(\psi) \geq 0$ exists, therefore, $\forall t_1 \geq t_0 \geq 0, \psi(t_0) \in \Psi$ and $u \in U$:

$$W(\psi(t_1)) - W(\psi(t_0)) \leq \int_{t_0}^{t_1} u^T(\tau) d(\tau) \quad (3)$$

Alternatively, if $W(\psi)$ is differentiable, the above equation (3.3) can be written as,

$$\dot{W}(\psi) \leq u^T(t) y(t), \quad \forall t \geq 0 \quad (4)$$

Here, $W(\psi)$ is the initial energy or the energy content of the system and $w = u^T(t)y(t)$ is the power fed to the system.

Definition 3.1, If a storage function exists and the initial or storage energy in the system is bounded above by the energy fed or supplied to the system, the system can be defined as passive. Therefore, in the passive system, the storage function W satisfies $W(0) = 0$, if the system is dissipative with supply rate $w(u, y)$ [25] [26]. This means, in passive system, $u^T(t)y(t) \geq \dot{W}(\psi)$.

A passive system provides the fundamental and inherent safety in building system infrastructures that are insensitive to implementation uncertainties [10].

Definition 3.2, The passive system can be defined as lossless i.e., stable, if $u^T(t)y(t) = \dot{W}(\psi)$. Therefore, the system is stable when $u^T(t)y(t) = \dot{W}(\psi)$.

4. DISTRIBUTED CYBER-PHYSICAL SYSTEMS

In distributed CPS, the physical entities are widely distributed and wireless sensors are arbitrarily distributed, so that they can sense the complete system jointly; there would be a network infrastructure which will communicate through the whole sensor system [27], [28]. Examples of distributed Cyber-Physical Systems include city-wide Transport Network management, Power Distribution Smart Grid, Irrigation Hydro-Power Network, etc. [27]–[29].

4.1 Architecture of Distributed Cyber-Physical Systems

Distributed CPS is a heterogeneous system, where a huge physical system infrastructure, with large-scale computation and communication systems, becomes a complex hybrid system. It would really be a difficult environmental aspect to deal with. Goswami et al. in [30] have shown that, in the case of distributed control applications, hybrid protocols (time-triggered and event-triggered) do not perform well, therefore by re-engineering the control applications, has found better results that the communication occurs in two modes instead of the hybrid modes.

In distributed CPS architecture, the system architecture required to handle huge number of nodes, therefore, in order to proof the concept, a large test-bed requires testing and validation of the concept. Tennina et al. in [31] have introduced a large-scale system architecture, named EMMON, which was tested in dense and real-time embedded monitoring, that included 300+ wireless sensor nodes and according to them, this was the largest test-bed introduced so far in Europe for such system testing.

In order to support safety critical real-time control of distributed systems, CPS require an appropriate architecture suitable for widely distributed systems. Benveniste in his paper [32], has proposed a Loosely Time-Triggered architecture, which is comprehensive, but computation and communication units are triggered by autonomous, non-synchronized clocks. Yong et al. in [26] has proposed an architecture for DCPS with an application for Smart Transport systems. Figure 4 shows a sample architecture applicable to distributed CPS.

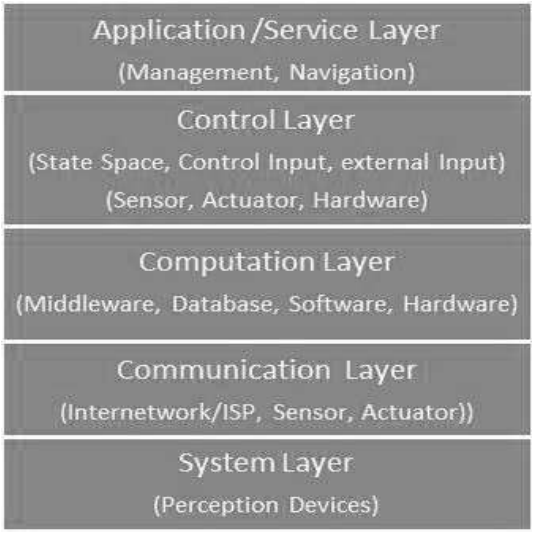

Fig. 4. A Sample Architecture for Distributed CPS.

4.2 Modeling and Stability Analysis of Distributed CPS

In [33], Woochul Kang et al. have introduced a Real-Time Data Distributed Service (RDDS) for CPS, where, they considered a fire-fighting team involved in a search and rescue task; each fire-fighter is equipped with a PDA collecting dynamic statuses through nearby sensors, then

collaborating and sending information back to the cyber systems. They used a test bed with fixed network that didn't consider environmental impacts on the information processed. Therefore, they have shortcomings of providing accurate information; this situation needs to consider the external inputs for data accuracy due to the distributed open system. As physical systems are not deterministic, in CPS, physical systems are modelled using the control theory with the use of differential equations, that are strongly dependent on time variation; the cyber systems, i.e. the computational part uses a discrete-event model of mathematics, therefore, the whole cyber and physical systems, together, become a hybrid model. In distributed CPS, a large number of agents or systems are connected; in order to model and stabilize such huge heterogeneous systems, it needs to use a multi-node approach with the passivity model. In handling faults and stabilizing such heterogeneous complex systems, a number of the state variable of remote nodes need to be estimated with the best possible accuracy [34]. The challenging aspects of stabilizing a heterogeneous distributed complex system are crucial; an approach to compositionality involves using passivity theory, and with some assumptions, the system can be made stable [35].

A study in [35], Antsaklis et al. have considered an interconnected nonlinear distributed systems $(\chi_0, \chi_1, ..., \chi_p = \chi_i)$, which is defined by,

$$\dot{\psi}_i = f_i(\psi_i, u_i) \tag{5}$$

$$y_i = g_i(\psi_i, u_i) \tag{6}$$

$$u_i = u_{ei} - \sum_{j=0}^{q} \mathbb{H}_{ij} y_i \tag{7}$$

where, u_i is the input of the subsystem i, u_{ei} is an external input, y_i is the output of the respective subsystem and $\mathbb{H}_{ij}$ are constant matrices.

Let us define $y = [y_1^T, ..., y_p^T]$, $\bar{\mathbb{H}} = [\mathbb{H}_{ij}]$, $u = [u_1^T, ..., u_p^T]$ and $u_{ei} = [u_{e1}^T, ..., u_{ep}^T]$. Then the inputs of interconnected distributed systems would be represented by:

$$u_e - \bar{H} y$$

Now, by manipulating the abovementioned state space system, using the similar concept of section 3, the distributed system can be stabilized. Detailed calculation has been found in [35].

Theorem 4.1, By categorizing the distributed agents into symmetrical groups and with the application of local control laws, the stability conditions for large-scale systems can be derived [36].

Theorem 4.2, In the interconnected heterogeneous and distributed systems, symmetries are obtained through identical dynamics of subsystems and by characterizing the structure of collected information [35], [37].

5. MOBILE CYBER-PHYSICAL SYSTEMS

Nowadays, there are plenty of handheld devices available, which utilize mobile networks to communicate with each other, as well as with the internet. The increasing popularity of these handheld or mobile devices has increased the idea and interest of the mobile CPS concept.

As portable computing machines, mobile devices are widely accepted; their accelerated processing power, pervasive cellular connections and range of sensors, have become the ideal platform for building Cyber-Physical Systems [38]. Mobile devices such as WiFi and Bluetooth-enabled smart phones and tablets are becoming more and more intelligent from day-by-day communication through mobile networks. High level programming languages are also being developed and are readily available for their intelligent communications. Also, mobile robotics systems can be applied in controlling intensive production in agricultural and industrial sectors, and help in search and rescue events. In situations like an intensive greenhouse horticultural system, where the environment is optimal for plants but unhealthy for humans, using mobile robots can be very useful alternatives [39]. Robot-controlled medical systems are also a potential cyber-physical area. Minimally invasive surgical processes, which are robot-assisted and image-guided, are evolving fast due to their potential effectiveness and improved patient management [40].

5.1 Architecture of Mobile Cyber-Physical Systems

As stipulated in [41], real-time video of rush hour traffic can be shared through internet, or real-time video of house surveillance cameras can be received through mobile phones if an abnormal situation is detected. Real-time video monitoring with cyber-physical surveillance systems is becoming a popular cyber-physical application [42]. AnySence, a Communication Architecture for ubiquitous Video-Based Cyber-Physical Systems, has been proposed in [41].

Mobile CPS applications have a huge potential for the new century's computing and IT revolution, which includes: high confidence medical systems, traffic control and managing traffic situations, advanced automotive systems, and more manageable disaster recovery systems, etc. [38]. Robots or robot teams are also examples of mobile physical entities and the communication domain interacting with these mobile teams form effective Cyber-Physical Robotic Systems (CPRS). CPRS are very effective if

engaged in the management of disasters, search and rescue situations, in the manufacturing industries, and in the management of healthcare systems. Therefore, the CPRS could become a very useful CPS sub-category.

Mobile CPS are used for the purpose of tracking and controlling mobile systems comprising of mobile devices. Like ICPS and DCPS, MCPS architectures control the sensor-rich real-time embedded systems, which closely interact with the physical world; such systems collect data from the physical domain, using sensors and feed the collected sensor data to the computing resources for making real-time decisions. Hanz and Guirguis in [43], has proposed a layered architecture, which is capable of controlling the motion of cyber-physical mobile devices. Figure 5 shows a sample architecture for Mobile CPS.

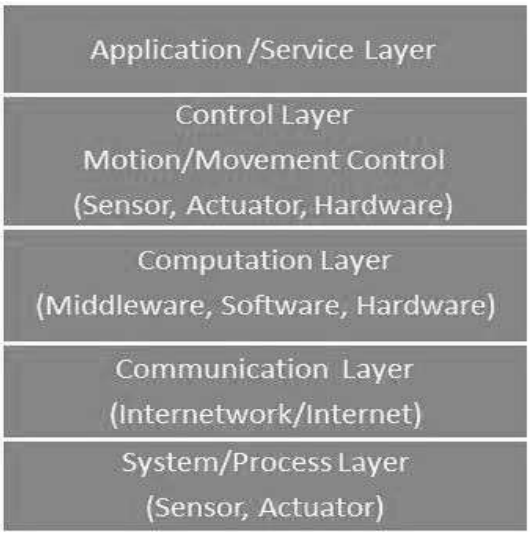

Fig. 5. A sample Layered Mobile CPS Architecture.

5.2 Modeling and Stability Analysis of Cyber-Physical Robotic System

In mobile CPS, a cyber-physical robotic system is very useful as discussed above. In this chapter, we shall review a system for modelling and stabilizing a mobile robotic system applied to robotic motion control. In mobile CPS such as the mobile motion control of robots, where the system is a distributed parameter system, the system state will evolve along both time and space; in this situation, instead of traditional finitely dimensioned input-output relationships, partial differential equations would be more suitable for modeling the system [44]. Assuming a robotic system for analysis of its motion control and stabilization, let us consider a dynamic equation for the robot control systems; dynamic equations are derived for any mechanical systems using the Euler-Lagrange equation below [45]:

$$\frac{d}{dt}\left(\frac{\partial \mathbb{L}}{\partial \dot{\Phi}}\right) - \frac{\partial \mathbb{L}}{\partial \Phi} = \tau \tag{8}$$

where $\Phi = (\Phi_1, ..., \Phi_n)^T$ is a set of generalized co-ordinates of the system, $\mathbb{L}$ is the Lagrangian, which is the difference between kinetic energy ($\mathbb{K}$) and potential energy ($\mathbb{P}$) i.e., $\mathbb{L} = \mathbb{K} - \mathbb{P}$ and τ is the force vector and represented as $\tau = (\tau_1, ..., \tau_n)^T$. The potential energy $\mathbb{P} \mapsto \mathbb{P}(\Phi)$ which is independent of $\dot{\Phi}$, whereas kinetic energy is quadratic function of $\dot{\Phi}$ in the form [45]:

$$\mathbb{K}(\Phi, \dot{\Phi}) = \frac{1}{2}\dot{\Phi}^T \mathbb{D}(\Phi)\dot{\Phi} \tag{9}$$

where $\mathbb{D}(\Phi)$ is $n \times n$ is the symmetric inertia matrix and positive definite for each $\Phi \in \Re^n$ on $\mathbb{Q}$. Therefore, the Euler-Lagrange equation becomes:

$$\mathbb{L} = \mathbb{K} - \mathbb{P} = \mathbb{K}(\Phi, \dot{\Phi}) = \frac{1}{2}\dot{\Phi}^T \mathbb{D}(\Phi)\dot{\Phi} - \mathbb{P}(\Phi) \tag{10}$$

Now, by manipulating the above equations using the Euler-Lagrange method, the following dynamic model has been obtained (for detail manipulation, please refer to [45]).

$$\mathbb{D}(\Phi)\ddot{\Phi} + \mathbb{C}(\Phi, \dot{\Phi})\dot{\Phi} + \mathbb{G}(\Phi) = \mathbb{B}(\Phi)u \tag{11}$$

where, $u = (u_1, ..., u_{N-1}) \in \Re^{N-1}$. The dynamic model in (5.4) can be re-written in the stable state space form as follows [46]:

$$\dot{\Psi} = \begin{bmatrix} \dot{\Phi} \\ \mathbb{D}^{-1}(\Phi)[-\mathbb{C}(\Phi, \dot{\Phi})\dot{\Phi} - \mathbb{G}(\Phi) + \mathbb{B}(\Phi)u] \end{bmatrix} \tag{12}$$

which is equivalent to:

$$\dot{\Psi} =: f(\Psi) + g(\Psi)u \tag{13}$$

where, $\Psi := (\Phi, \dot{\Phi})$. The state space model $\chi = \mathbb{T} \times \mathbb{Q}$, for each $\Psi \in \chi$, $g(\Psi)$ is a $2N \times (N-1)$ matrix and its i^{th} column is g_i, $(\Psi, \dot{\Psi})$ for $\mathbb{T} \times \mathbb{Q}$, g is independent of $\dot{\Psi}$ in natural co-ordinates.

Now using the processes of section 3 and 4, the above robotic state space model can be stabilized.

6. DESIGN CHALLENGES OF CYBER-PHYSICAL SYSTEMS

This section will explain the challenges in designing the CPS of the heterogeneous, hybrid, and complex physical domain. This chapter will also discuss the security issues and security design concepts in this evolutionary technology space. Subsection A will discuss the application

aspects in the design of Cyber-Physical Systems. Subsection B will discuss about issues and challenges in the design of Cyber-Physical Systems.

6.1 Application aspects of the Cyber-Physical Systems Design

Cyber-Physical Systems deal with complex and critical application areas, therefore it is vital to consider the aspects and natures of different applications which will be benefited by CPS technology. With the advancement of CPS technology comes huge applications such as e-health systems, traffic control and safety, advanced automotive systems, process control, energy conservation, environmental control, avionics, instrumentation, and defence systems, all of which will be benefited by adapting modern systems [47].

Cyber-Physical applications are growing fast, and the application areas are widening to include vast ranges of complex systems which are heterogeneous in nature. CPS applications range from small-scale, safety-critical pacemaker controllers to largescale distributed Smart Grids [48]. While these systems have great potential, they require fundamental reassessments of the prevailing paradigms in communication and computation abstractions [48].

CPS are including more and more applications; this in future might expand to be applied to each and every computing capable application to improve their extreme capability. Jason et al. in [49] has proposed a cyber physical approach to be used for Graphical Processing Units (GPU), and their experiment has shown that the GPU tasks can be completed 34 percent faster than with the existing methods.

Common applications of CPS typically fall under sensor-based communication-enabled autonomous systems. For example, many wireless sensor networks monitor some aspect of the environment and relay the processed information to a central node. Other types of CPS include smart grids, autonomous auto-mobile systems, medical systems monitoring, process control systems, distributed robotics, and space aircrafts.

The systems that require measuring and monitor large amounts of information are equipped with a large network of wireless sensors; CPS are increasingly being used for such huge systems. Examples include health care systems, medical devices, smart grid, intelligent transportation systems, and advanced auto-mobile systems [50], [51]. The aircraft or the space vehicles, due to its autonomous movement and functionality, can be considered as the prime examples of cyber-physical systems [52].

CPS are spreading to the smart transport sectors, advanced and modern agricultural systems and many more areas. Transport systems like Railway Cyber-Physical Systems (RCPS) require interaction between train controllers, communication networks, and the physical world [53]. In RCPS, behaviour of the physical world such as velocity, flow and density are all dynamic and changing continuously, therefore the control and communication architecture is totally different, and will integrate all varied natures of those parameters [53]. An integrated CPS which is designed to include all of those optimizations would deliver a very smart and advanced RCPS.

Air-Transport is another highly prospective transport system; Cyber-Physical Aerospace Systems (CPAS) involve communication, sensing, and actuation of widely distributed physical devices and computational components through the heterogeneous computing environment of physical processes [54]. Therefore, CPAS require close interaction between cyber and physical worlds, both in time and space, and needs new methods of characterizing and controlling dynamic processes across a heterogeneous network of sensors and computational devices [54].

Another typical CPS example of the Smart Grid system is the Advanced Metering Infrastructure (AMI), in which a large amount of data from thousands of meters are collected and processed through an AMI [15]. A Smart Grid is defined as the integration of digital computing and communication technologies with power-delivery infrastructure; the smart grid is an example of critical cyber-physical system in the modern world [55]. Georg et al. has introduced INSPIRE, a Hybrid Simulator Architecture which is capable of evaluating both Power Systems and ICT Networks [56].

Kinsy et al in [48] has shown how to build a heterogeneous architecture for power electronics which is an emerging field of CPS; they designed the architecture which enables high fidelity with 1 microsecond latency and emulation time-step.

Cyber-Physical Energy Systems (CPES) is another potential CPS area which operates with the integration of IT and physical processing, with Local and Wide Area Communication Networks [56]. An interesting architecture for Cyber-Physical Energy Systems (CPES) has been proposed in [57] which could be useful for intelligent charging systems for electric vehicles. Figure 6 shows the proposed architecture of such a CPES as stipulated in [57].

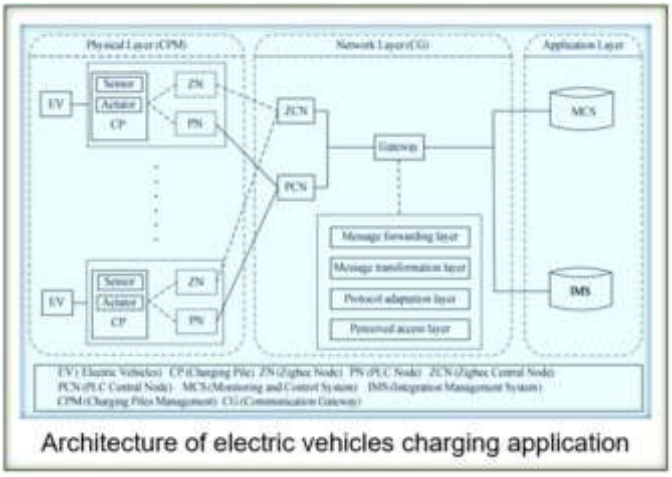

Fig. 6. An Architecture of a Cyber-Physical Systems (CPS) application [57].

6.2 Issues and Challenges of the Design of Cyber-Physical Systems

Due to a hybrid nature and heterogeneous characteristics, the operation and maintenance, as well as the designs of cyber-physical components, are a very complex task. One of the most complex systems is CPRS, where the software and hardware structures are very complex; these are becoming more and more complex over the recent years. These systems often consist of a few subsystems which need to be arranged and operated in a decentralized situation, and therefore those complexities can lead to serious problems maintaining and operating the system, even during the design phase [60]. The cyber domain is controlled by discrete mathematical logic, whereas the physical domain is controlled by state feedback control laws. Physical properties or the dynamics of a system are modelled to a state space system, using mathematical relations, normally by forming differential equations in order to determine physical dynamics for monitoring and optimization. Due to the heterogeneous nature and differences in dynamics of different physical systems, the design task of CPS leads to a great challenge. It is easy to write the requirements of the physical domain in languages, but while designing, significant issues arise due to the difficulty of deriving mathematical relations such as state space systems. There would be a great research opportunity stemming from designing a robotic CPS architecture, although this can lead to a big challenge due to the mobile nature of robots. In order to determine the state of the environment, advanced robotic hardware systems are equipped with sensors and effectors. Therefore, building a cyber-physical infrastructure controlling a robot is a huge challenge [61].

CPS in real-life such as building automation systems and unmanned automotive vehicles are controlled by network control systems, and the system dynamics emerged through the interactions between computing, communication, and physical dynamics [10], [25]. Monitoring and optimizing the physical dynamics of building automation systems are not similar in nature, and can be compared to that of unmanned automotive vehicles. Similarly, the variation in the requirements will be found in other systems, such as controlling and tracking mobile robot teams, smart power grids, smart gardens, national health care systems, etc. When designing a complex system, system failure has to be an important consideration during the design; a failure of the cyber system may not necessarily stop the operation or change the behavior of the networked elements, but will impact the performance of those elements when a potential or major failure occurs [62], [63]. Another issue is, CPS contain a huge number of wireless sensors, but due to the limited bandwidth and heavy interference in the wireless sensor networks, the efficient allocation of network resources is a major design concern [64]. The Wireless Sensor Network (WSN) adopted in the CPS are facing more stringent design challenges in comparison to the conventional WSNs, because the WSN in CPS must have good scalability, perform with low latency, and be energy efficient [65], [66]. For some of the systems, where environmental factors such as temperature, weather, and water conditions change frequently, it is difficult to estimate accurate data; CPS design of such physical domains thus presents itself to inherent issues [67].

Another major issue that has been noticed during this study is the delay in delivery of packets through the network. Cyber-Physical networks are designed to carry mainly delay-sensitive real-time information. Today's internet does not guarantee bandwidth for real-time delivery; current internet architectures are working on the best effort basis.

7. CYBERSECURITY OF IOT AND CYBER-PHYSICAL SYSTEMS

Due to the innovative discovery of Cyber-Physical Systems and their diversification of human benefits, interconnected Internet of Things-based devices are increasing exponentially, which leads to privacy issues and security challenges being introduced [83]. IoT-based devices would become more pervasive than even mobile phones, and would have access to peoples sensitive personal credentials such as usernames, passwords, etc., which could be an easy cyberattack target of hackers; a variety of cyberattacks could be caused due to the vulnerabilities of smart IoT devices, which the hackers will consider the weakest link in order to break the sensitive and secure infrastructures [84].

7.1 Cybersecurity Issues and System Vulnerabilities

Security in the CPS spaces is getting another major concern. While managing CPS locally at a smaller scale, security may not be a major concern; when the system actuation is extended through to the internet, the system may exhibit security vulnerability. According to Borg [59], company executives and key researchers are moving into the crosshairs of the cyberhackers worse than ever before (this has never happened in the past), as hackers are increasingly targeting industrial equipment, particularly focusing on hardware, i.e. process control, including programmable logic controllers and local networks; this could hurt the affected company by resulting drop in the stock price due to possible failure of quality control. The cyberhackers could earn more money than from a credit card fraud, and could even advantage them further by taking position in the stock market [51]. With the Internet of Things in place, these security risks are increasing; systems will be more vulnerable when more physical infrastructures are connected to the internet. Figure 7 is showing such a vulnerability in CPS.

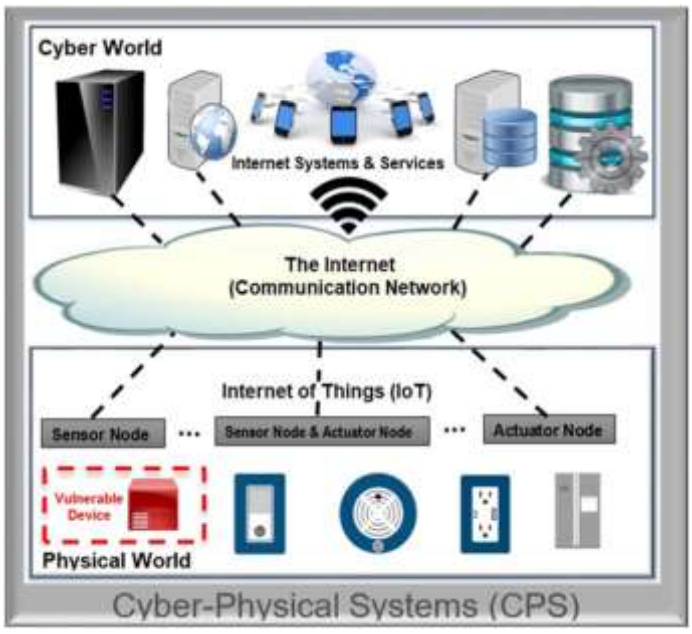

Fig. 7. Cyber-Physical Systems (CPS) and the Internet of Things (IoT) with a Vulnerable Physical Device.

The Chief Security Officr of PTC, a Massachusetts-based software firm, Corman, Josh, raised his concern about the vulnerability of IoT due to there being more physical systems and facilities connected to wireless networks, which will be difficult to tackle with the traditional IT security methods [58].

According to Corman in [58], the following are six burning issues due to vulnerabilities in the IoT and Cyber-Physical Communication networks:

- Consequences of security failure would be more serious and no doubt would be very urgent, when digital cars or infusion pumps are attacked; this will result in destroying peoples lives.
- The nationwide hacking system is an all-out cyber war; today's adversaries are no longer hackers trying to make money, or cause mischief, but rather bring IoT security to face special challenges.
- Some software vendors and chip makers recently offered 10-years and 7-years of support for IoT products, whereas others either limit their support to 2 or 3 years, or don't even provide any specified support contract yet, which could turn into vulnerability in security.
- Economics is another issue, as in some cases, a connected product that generates small profits might require patches, updates, and security evaluations; those must cause added costs to the product and will impact the profit, or if the updates are not done, might cause security vulnerabilities.
- Corman's fifth reason is to do with the scary reality of the weak link being the vulnerability, when connected devices are built with firmware, software, and hardware by different companies; the company that creates telematics of a not updating the software could cause the entire car to be vulnerable.
- The sixth reason is about connected devices in live environments unlike any IT system; for example, in smart homes, there is no software expert/manager to apply patches to connected fridges, which may turn into facing a vulnerability risk.

Therefore, maintaining the above as well as securing big plants, networks, and establishments, cybersecurity is of paramount importance and addressing it is required for the success of IoT/CPS operations in the Cyber-Communication space.

7.2 Cyber-Attack System Modeling and Analysis

Increasingly, control system networks are being connected to enterprise networks; the control system networks that possess critical control systems may be vulnerable to cyberattacks [68]. Some specific examples of CPS are smart grids, pervasive healthcare systems, unmanned air vehicles, etc.; in the modern world, these

are becoming integrated, and as the integration deepens, securing these systems becomes more important [69].

When systems are being developed and combined to form the CPS, the total risk of the whole system would definitely be much greater than those of the component systems [70]. In recent years, attacks on software are spreading to the embedded systems and the incidents like the Stuxnet attack, which are attacks in the automation systems, are possible because the computational and physical dynamics are these days being connected to the internet [71], [72].

There haven't been many attacks yet on CPS, because most of the CPS models use their proprietary protocols, but in the future, more attacks can be expected in this area, because of the interaction between CPS and the internet [73]. The security would be more vulnerable with the interconnection to the public internet; this would have been a much bigger concern with the new internet concept, i.e. the Internet of Things or the Internet of Everything. IoT vulnerabilities are caused by there being more physical systems and facilities connected to Wireless Sensor Networks (WSN) [58]. CPS systems for national infrastructures, such as national power grids, smart energy systems, advanced metering infrastructures, etc. are becoming increasingly at risk, as the cyber security incidents have gained increasing credibility as viable risks to those huge infrastructures [74]. Now, these are being connected to the internet, and thus the risk of attack will increase [72].

As the CPSs are related to the physical systems, equipment, humans, national infrastructures, expensive establishments, and critical infrastructures, the damage would definitely be larger and may not be recoverable, therefore attacks on CPS should be taken very seriously [75]. The issues of security and safety are of greater importance for pervasive computing, although this is a great concern regardless [76]. Preschern et al [72], has built a security model one-out-of-two (1oo2) on the basis of the paper by Kai Hansen [77], which covers possible attacks and outcome and discussed the attack scenarios from an attacker's point of view.

This type of security measure may protect systems to some extent, but with the new internet concept, the risk of attacks will increase that may not be covered by this. Let us consider a CPS/IoT-based Wireless Sensor Network (WSN) under attack as shown in figure 8. In this figure, we can see two scenarios, (a) Scenario One (Star Network topology) and (b) Scenario Two (Closed Loop Ring network topology). In Scenario One, the target vulnerable device is behind three nodes from the attack point, where the attacker needs to travel two hops, and in Scenario Two, the target vulnerable device is behind four nodes from the attack point, where the attacker needs to travel three hops. Therefore, if the target vulnerable device is behind N nodes, the attacker needs to travel $N - 1$ hopes and the associated matrices of attack inputs would be in the form of an identity matrix.

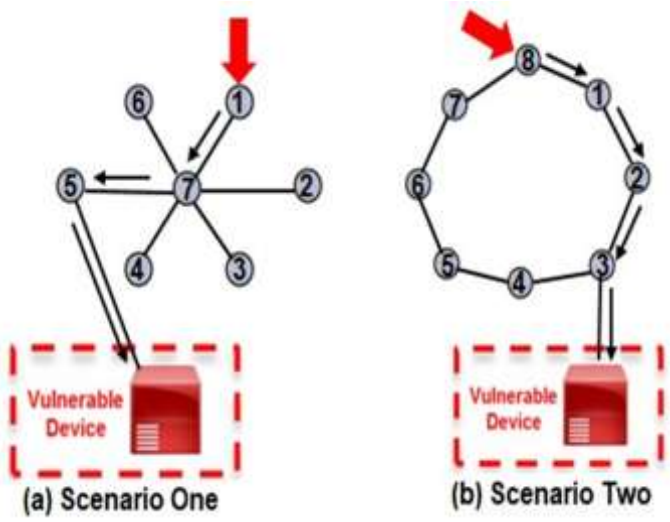

Fig. 8. CPS/IoT based Wireless Sensor Network (WSN) under Attack.

While designing the security of a critical infrastructure, it is mandatory to consider possible attacks to the system. When stepping in to investigate the security of a system, the first

thing to do is to define an attack model [78]. In this technical review, we have studied attack detection and identification approaches modelled in [79]–[81], where they have considered cyber-physical attacks on power networks and distributed malicious attacks on CPS. They analyzed a generalized model, $\mathbb{E}\dot{\psi}(t) = \mathbb{A}\psi(t) + \mathbb{B}u(t)$ and $y(t) = \mathbb{C}\psi(t) + \mathbb{D}u(t)$, where, $\psi(t) \in \Re^n$, $y(t) \in \Re^p$, $\mathbb{E} \in \Re^{n\times n}$, $\mathbb{A} \in \Re^{n\times n}$, $\mathbb{B} \in \Re^{n\times m}$, $\mathbb{C} \in \Re^{p\times n}$, $\mathbb{D} \in \Re^{p\times m}$. In this state space system, $\mathbb{E}$ has been assumed as singular matrix, the input terms $\mathbb{B}u(t)$ and $\mathbb{D}u(t)$ are supposed to be unknown inputs, and these are the disturbances affecting the above system. These disturbed input signals are the cause behind the attack to the CPS state system and it is assumed that the state variable and the output variable respectively can be compromised by the attacker [79].

They have considered, $\mathbb{B} = [\mathbb{I}, 0]$ and $\mathbb{D} = [0, \mathbb{I}]$ are appropriately dimensioned and partitioned into identity and zero matrices, i.e. $u(t) = [u_\psi(t)^T, u_y(t)^T]^T$. Therefore, $(\mathbb{B}u(t), \mathbb{D}u(t)) = (u_\psi(t), u_y(t))$ is the state attack affecting the system dynamics and output attack corrupting output measurement vectors [79]. But they did not consider environmental impact or external inputs, which is common in the distributed cyber-physical domain, and also did not analyze the convergence of distributed monitors and optimizers, because of which this model may be useful for locally integrated cyber-physical architectures, but not sufficient for widely distributed systems.

Most embedded systems or CPS systems are designed without security in mind, and these systems are normally protected by firewalls, which do not ensure the security for attacks from within the systems, therefore security has to be part of the design process of CPS in order to provide sufficient protection [82].

8. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this technical review, we have studied and analyzed currently available works, experiments, and research available for Cyber-Physical Systems (CPS); its' current architectures, models, and possible cybersecurity issues are also analyzed and discussed in detail. Along with other wide uses, the Internet of Things (IoT) is the most revolutionary application of CPS. Therefore, CPS have become paramount and are at the centre of attraction for researchers, major network vendors, university and institutional researchers, as well as industries and business communities. For easy management and operation, CPS are categorized in three different classes: Integrated CPS, Distributed CPS, and Mobile CPS. A comprehensive review has been made and discussed about the communication architectures and modeling of all three categories. While reviewed, due to the heterogeneous and hybrid complex nature of the physical dynamics of different systems, it has been found that concrete common architecture and standards have not yet been developed.

The architectural modeling in this technical review includes mathematical modling, in order to stabilize the systems against disturbances; by considering those disturbances as attack inputs. In addition, a cybersecurity attack model has also been analyzed and discussed as part of this technical review. To explore further, in the future, we can consider some use cases of CPS and IoT infrastructures to investigate their current model including cybersecurity vulnerabilities; this will help instigate and propose architectural improvements along with cyber-safe security measures. In these future researches, we might consider different classes of CPS architectures as has been categorized in this technical review; this might narrow down the research works to facilitate detailed investigation.

REFERENCES

[1] "US National Science Foundation (NSF), Cyber-Physical Systems (CPS): https://www.nsf.gov/publications/

[2] Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". https://www.linux.com/NEWS/21-OPEN-SOURCE-PROJECTSIOT. Retrieved 23 October 2017.

[3] "Internet of Things Global Standards Initiative". https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspxITU. Retrieved 28 July 2016.

[4] Hendricks, Drew. "The Trouble with the Internet of Things". London Datastore. Greater London Authority. https://data.london.gov.uk/blog/the-trouble-with-the-internet-of-things/ Retrieved 06 August 2016.

[5] Vermesan, Ovidiu; Friess, Peter (2014). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems (PDF). Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4.

[6] Mattern, Friedemann; Floerkemeier, Christian. "From the Internet of Computers to the Internet of Things" (PDF). ETH Zurich. Retrieved 23 October 2016.

[7] Santucci, Grald. "The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects" (PDF). European Commission Community Research and Development Information Service. Retrieved 23 October 2016.

[8] Rad, Ciprian-Radu; Hancu, Olimpiu; Takacs, Ioana-Alexandra; Olteanu, Gheorghe (2015). "Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture". Conference Agriculture for Life, Life for Agriculture. 6: 7379.

[9] Jiankun Hu, H.R. Pota, and Song Guo. Taxonomy of attacks for agent based smart grids. Parallel and Distributed Systems, IEEE Transactions on, 25(7):18861895, July 2014.

[10] N. Kottenstette, J.F. Hall, X. Koutsoukos, J. Sztipanovits, and P. Antsaklis. Design of networked control systems using passivity. Control Systems Technology, IEEE Transactions on, 21(3):649665, May 2013.

[11] P. Nuzzo, J.B. Finn, A Iannopollo, and AL. Sangiovanni-Vincentelli. Contract-based design of control protocols for safety-critical cyberphysical systems. In Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014, pages 14, March 2014.

[12] J.R.B. Garay and S.T. Kofuji. Architecture for sensor networks in cyberphysical system. In Communications (LATINCOM), 2010 IEEE Latin American Conference on, pages 16, Sept 2010.

[13] Wei Meng, Quan Liu, Wenjun Xu, and Zude Zhou. A cyber-physical system for public environment perception and emergency handling. In High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on, pages 734738, Sept 2011.

[14] J. Nielsen, L. Rock, B. Rogers, A Dalia, J. Adams, and Yang-Quan Chen. Automated social coordination of cyber-physical systems with mobile actuator and

sensor networks. In Mechatronics and Embedded Systems and Applications (MESA), 2010 IEEE/ASME International Conference on, pages 554559, July 2010.

[15] Jiazhen Zhou, R.Q. Hu, and Yi Qian. Scalable distributed communication architectures to support advanced metering infrastructure in smart grid. Parallel and Distributed Systems, IEEE Transactions on, 23(9):16321642, Sept 2012.

[16] D. Quaglia. Cyber-physical systems: Modeling, simulation, design and validation. In Embedded Computing (MECO), 2013 2nd Mediterranean Conference on, pages 12, June 2013.

[17] Jia Shen, Fei Xu, Xiangyou Lu, and Huafei Li. Heterogeneous multilayer wireless networking for mobile cps. In Ubiquitous Intelligence Computing and 7th International Conference on Autonomic Trusted Computing (UIC/ATC), 2010 7th International Conference on, pages 223227, Oct 2010.

[18] Li Yongfu, Sun Dihua, Liu Weining, and Zhang Xuebo. A service oriented architecture for the transportation cyber-physical systems. In Control Conference (CCC), 2012 31st Chinese, pages 76747678, July 2012.

[19] R. Marculescu. Design of future integrated systems: A cyber-physical systems approach. In Power and Timing Modeling, Optimization and Simulation (PATMOS), 2013 23rd International Workshop on, pages 11, Sept 2013.

[20] B. Syed, A Pal, K. Srinivasarengan, and P. Balamuralidhar. A smart transport application of cyber-physical systems: Road surface monitoring with mobile devices. In Sensing Technology (ICST), 2012 Sixth International Conference on, pages 812, Dec 2012.

[21] T. Wolf, M. Zink, and A Nagurney. The cyber-physical marketplace: A framework for large-scale horizontal integration in distributed cyber physical systems. In Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on, pages 296302, July 2013.

[22] Liang Hu, Nannan Xie, Zhejun Kuang, and Kuo Zhao. Review of cyber physical system architecture. In Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2012 15th IEEE International Symposium on, pages 2530, April 2012.

[23] M. Ghorbani and P. Bogdan. A cyber-physical system approach to artificial pancreas design. In Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2013 International Conference on, pages 110, Sept 2013.

[24] J. Sztipanovits, X. Koutsoukos, G. Karsai, N. Kottenstette, P. Antsaklis, V. Gupta, B. Goodwine, J. Baras, and Shige Wang. Toward a science of cyber-physical system integration. Proceedings of the IEEE, 100(1):2944, Jan 2012.

[25] N. Kottenstette, X. Koutsoukos, J. Hall, J. Sztipanovits, and P. Antsaklis. Passivity-based design of wireless networked control systems for robustness to time-varying delays. In Real-Time Systems Symposium, 2008, pages 1524, Nov 2008.

[26] C.I Byrnes, A Isidori, and J.C. Willems. Passivity, feedback equivalence, and the global stabilization of minimum phase nonlinear systems.
Automatic Control, IEEE Transactions on, 36(11):12281240, Nov 1991.

[27] S. Deshmukh, B. Natarajan, and A Pahwa. State estimation over a lossy network in spatially distributed cyber-physical systems. Signal Processing, IEEE Transactions on, 62(15):39113923, Aug 2014.

[28] S. Deshmukh, B. Natarajan, and A Pahwa. State estimation in spatially distributed cyber-physical systems: Bounds on critical measurement drop rates. In Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on, pages 157164, May 2013.

[29] J. Taneja, R. Katz, and D. Culler. Defining cps challenges in a sustainable electricity grid. In Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on, pages 119128, April 2012.

[30] D. Goswami, R. Schneider, and S. Chakraborty. Re-engineering cyberphysical control applications for hybrid communication protocols. In Design, Automation Test in Europe Conference Exhibition (DATE), 2011, pages 16, March 2011.

[31] S. Tennina, M. Bouroche, P. Braga, R. Gomes, M. Alves, F. Mirza, V. Ciriello, G. Carrozza, P. Oliveira, and V. Cahill. Emmon: A wsn system architecture for large scale and dense real-time embedded monitoring. In Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on, pages 150157, Oct 2011.

[32] A. Benveniste. Loosely time-triggered architectures for cyber-physical systems. In Design, Automation Test in Europe Conference Exhibition (DATE), 2010, pages 38, March 2010.

[33] Woochul Kang, K. Kapitanova, and Sang Hyuk Son. Rdds: A real time data distribution service for cyber-physical systems. Industrial Informatics, IEEE Transactions on, 8(2):393405, May 2012.

[34] F.A.T. Abad, M. Caccamo, and B. Robbins. A fault resilient architecture for distributed cyber-physical systems. In Embedded and RealTime Computing Systems and Applications (RTCSA), 2012 IEEE 18th International Conference on, pages 222231, Aug 2012.

[35] P.J. Antsaklis, M.J. McCourt, Han Yu, Po Wu, and Feng Zhu. Cyberphysical systems design using dissipativity. In Control Conference (CCC), 2012 31st Chinese, pages 15, July 2012.

[36] Po Wu and P.J. Antsaklis. Symmetry in the design of large-scale complex control systems: Some initial

results using dissipativity and lyapunov stability. In Control Automation (MED), 2010 18th Mediterranean Conference on, pages 197202, June 2010.

[37] Po Wu and P.J. Antsaklis. Passivity indices for symmetrically interconnected distributed systems. In Control Automation (MED), 2011 19th Mediterranean Conference on, pages 16, June 2011.

[38] Jae Yoo Lee, Du Wan Cheun, and Soo Dong Kim. A comprehensive framework for mobile cyber-physical applications. In Service-Oriented Computing and Applications (SOCA), 2011 IEEE International Conference on, pages 16, Dec 2011.

[39] R. Garro, L. Ordinez, and O. Alimenti. Design patterns for cyber physical systems: The case of a robotic greenhouse. In Computing System Engineering (SBESC), 2011 Brazilian Symposium on, pages 1520, Nov 2011.

[40] E. Yeniaras, J. Lamaury, Zhigang Deng, and N.V. Tsekos. Towards a new cyber-physical system for mri-guided and robot-assisted cardiac procedures. In Information Technology and Applications in Biomedicine (ITAB), 2010 10th IEEE International Conference on, pages 15, Nov 2010.

[41] Guoliang Xing, Weijia Jia, Yufei Du, Posco Tso, Mo Sha, and Xue Liu. Toward ubiquitous video-based cyber-physical systems. In Systems, Man and Cybernetics, 2008. SMC 2008. IEEE International Conference on, pages 4853, Oct 2008.

[42] Pengbo Si, F.R. Yu, and Yanhua Zhang. Qos- and security-aware dynamic spectrum management for cyber-physical surveillance system. In Global Communications Conference (GLOBECOM), 2013 IEEE, pages 962967, Dec 2013.

[43] T. Hanz and M. Guirguis. An abstraction layer for controlling heterogeneous mobile cyber-physical systems. In Automation Science and Engineering (CASE), 2013 IEEE International Conference on, pages 117121, Aug 2013.

[44] C. Tricaud and YangQuan Chen. Optimal trajectories of mobile remote sensors for parameter estimation in distributed cyber-physical systems. In American Control Conference (ACC), 2010, pages 32113216, June 2010.

[45] R. Ortega and M.W. Spong. Adaptive motion control of rigid robots: a tutorial. In Decision and Control, 1988., Proceedings of the 27th IEEE Conference on, pages 15751584 vol.2, Dec 1988.

[46] E. R. Westervelt, J.W. Grizzle, and D.E. Koditschek. Hybrid zero dynamics of planar biped walkers. Automatic Control, IEEE Transactions on, 48(1):4256, Jan 2003.

[47] E.A Lee. Cyber physical systems: Design challenges. In Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on, pages 363369, May 2008.

[48] M. Kinsy, O. Khan, Ivan Celanovic, D. Majstorovic, N. Celanovic, and S Devadas. Time-predictable computer architecture for cyber-physical systems: Digital emulation of power electronics systems. In Real-Time Systems Symposium (RTSS), 2011 IEEE 32nd, pages 305316, Nov
2011.

[49] J. Aumiller, S. Brandt, S. Kato, and N. Rath. Supporting low-latency cps using gpus and direct i/o schemes. In Embedded and Real-Time Computing Systems and Applications (RTCSA), 2012 IEEE 18th International Conference on, pages 437442, Aug 2012.

[50] Min Ding, Haifeng Chen, A Sharma, K. Yoshihira, and Guofei Jiang. A data analytic engine towards self-management of cyber-physical systems. In Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on, pages 303308, July 2013.

[51] B. Stelte and G.D. Rodosek. Assuring trustworthiness of sensor data for cyber-physical systems. In Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on, pages 395402, May 2013.

[52] A.T. Klesh, J.W. Cutler, and E.M. Atkins. Cyber-physical challenges for space systems. In Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on, pages 4552, April 2012.

[53] Lichen Zhang. Aspect-oriented approach to modeling railway cyber physical systems. In Distributed Computing and Applications to Business, Engineering Science (DCABES), 2013 12th International Symposium on, pages 2933, Sept 2013.

[54] Lichen Zhang. Multi-view approach for modeling aerospace cyberphysical systems. In Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, pages 13191324, Aug 2013.

[55] A.P. Athreya and P. Tague. Survivable smart grid communication: Smartmeters meshes to the rescue. In Computing, Networking and Communications (ICNC), 2012 International Conference on, pages 104110, Jan 2012.

[56] H. Georg, S.C. Muller, N. Dorsch, C. Rehtanz, and C. Wietfeld. Inspire: Integrated co-simulation of power and ict systems for real-time evaluation. In Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on, pages 576581, Oct 2013.

[57] Yongqi Ge, Yunwei Dong, and Hongbing Zhao. A cyber-physical energy system architecture for electric vehicles charging application. In Quality Software (QSIC), 2012 12th International Conference on, pages 246250, Aug 2012.

[58] S. Higginsbotham. Internet of Everything: 6 Ways IoT is Vulnerable, IEEE Spectrum, Page 21, July 2018.

[59] S. Borg (Director, U.S., Cyber Consequences Unit), To Design Better Hardware, Think Like a Cyber-Criminal. At the MEMS and Sensors Technical Congress held at Stanford University, California, USA, to an audience of 130 Chief Technical Officers, Engineering Directors and Key Researchers, IEEE Spectrum, Page 22, July 2017.

[60] R. Maas, E. Maehle, and K.-E. Grosspietsch. Applying the organic robot control architecture orca to cyber-physical systems. In Software Engineering and Advanced Applications (SEAA), 2012 38th EUROMICRO Conference on, pages 250257, Sept 2012.

[61] S. Szominski, K. Gadek, M. Konarski, B. Blaszczyk, P. Anielski, and W. Turek. Development of a cyber-physical system for mobile robot control using erlang. In Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on, pages 14411448, Sept 2013.

[62] B. Falahati and Yong Fu. Reliability assessment of smart grids considering indirect cyber-power interdependencies. Smart Grid, IEEE Transactions on, 5(4):16771685, July 2014.

[63] S. Graham, G. Baliga, and P.R. Kumar. Abstractions, architecture, mechanisms, and a middleware for networked control. Automatic Control, IEEE Transactions on, 54(7):14901503, July 2009.

[64] Xufei Mao, Chi Zhou, Yuan He, Zheng Yang, Shaojie Tang, and Weichao Wang. Guest editorial: Special issue on wireless sensor networks, cyber-physical systems, and internet of things. Tsinghua Science and Technology, 16(6):559560, Dec 2011.

[65] Xi Deng and Yuanyuan Yang. Communication synchronization in cluster-based sensor networks for cyber-physical systems. Emerging Topics in Computing, IEEE Transactions on, 1(1):98110, June 2013.

[66] Sajal K. Das. Cyber-physical and networked sensor systems: Challenges and opportunities. In Advanced Intelligence and Awareness Internet (AIAI 2011), 2011 International Conference on, pages 11, Oct 2011.

[67] Dong Li, Ze Zhao, Li Cui, He Zhu, Le Zhang, Zhaoliang Zhang, and Yi Wang. A cyber physical networking system for monitoring and cleaning up blue-green algae blooms with agile sensor and actuator control mechanism on lake tai. In Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, pages 732737, April 2011.

[68] Seddik M. Djouadi, Alexander M. Melin, Erik M. Ferragut, Jason A Laska, and Jin Dong. Finite energy and bounded attacks on control system sensor signals. In American Control Conference (ACC), 2014, pages 17161722, June 2014.

[69] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv., 46(4):55:155:29, March 2014.

[70] C.W. Axelrod. Managing the risks of cyber-physical systems. In Systems, Applications and Technology Conference (LISAT), 2013 IEEE Long Island, pages 16, May 2013.

[71] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. Security Privacy, IEEE, 9(3):4951, May 2011.

[72] C. Preschern, N. Kajtazovic, and C. Kreiner. Built-in security enhancements for the 1oo2 safety architecture. In Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on, pages 103108, May 2012.

[73] L. Pietre-Cambacedes, M. Tritschler, and G.N. Ericsson. Cybersecurity myths on power control systems: 21 misconceptions and false beliefs. Power Delivery, IEEE Transactions on, 26(1):161172, Jan 2011.

[74] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. Smart Grid, IEEE Transactions on, 4(2):847855, June 2013.

[75] J. Wan. Advances in cyber-physical systems research. In KSII Transactions on Internet and Information Systems, vol. 5, no. 11, pp. 18911908, 2011, page 18911908, October 2011.

[76] Steven J. Templeton. Security aspects of cyber-physical device safety in assistive environments. In Proceedings of the 4th International Conference on Pervasive Technologies Related to Assistive Environments, PETRA 11, pages 53:153:8, New York, NY, USA, 2011. ACM.

[77] K. Hansen. Security attack analysis of safety systems. In Emerging Technologies Factory Automation, 2009. ETFA 2009. IEEE Conference on, pages 14, Sept 2009.

[78] R. Mitchell and Ing-Ray Chen. Survivability analysis of mobile cyber physical systems with voting-based intrusion detection. In Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, pages 22562261, July 2011.

[79] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. Automatic Control, IEEE Transactions on, 58(11):27152729, Nov 2013.

[80] F. Pasqualetti, F. Dorfler, and F. Bullo. Cyber-physical security via geometric control: Distributed monitoring and malicious attacks. In Decision and Control (CDC), 2012 IEEE 51st Annual Conference on, pages 34183425, Dec 2012.

[81] Fabio Pasqualetti, Florian Dorfler, and F. Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on, pages 21952201, Dec 2011.

[82] M. Naedele. Addressing it security for critical control systems. In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on, pages 115115, Jan 2007.

[83] K. Reeves and C. Maple, "IoT interoperability: Security considerations and challenges in implementation," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-7. doi: 10.1049/cp.2018.0007

[84] E. Anthi, L. Williams and P. Burnap, "Pulse: An adaptive intrusion detection for the Internet of Things," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-4. doi: 10.1049/cp.2018.0035