IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 2, Ver. I (Mar-Apr. 2016), PP 104-110
www.iosrjournals.org

Challenges and Current Solutions of Cyber Physical Systems

Lokesh. M. R[1], Y.S. Kumaraswamy [2] Tejaswini K.N[3]
[1](*Senior Assistant Professor, Information Science and Engineering New Horizon College of Engineering Bangalore and Research Scholar, Department of Computer Science and Engineering Sathyabama University, Chennai, India)*
[2](*Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, Devanahalli, Bangalore, India*)
[3](*PG Scholar (Software Engineering), Information Science and Engineering New Horizon College of Engineering Bangalore. India)*

Abstract: *The interaction among people has been increased rapidly due to advances in internet and increased use of smart phones that are now available at all price ranges. The next step is to improve communication among machines by connecting the machines and giving intelligence to them to communicate among machines by connecting the machines and giving intelligence to them to communicate with other machines and also to interact with people. Cyber Physical Systems (CPS) are a natural consequence of an increasingly connected physical world. CPS have wide range of applications at the same time there are several challenges to implement these systems. In order to identify the challenges and current solutions and propose research possibilities in different areas of CPS we survey the literature of this area. Our approach is to identify the challenges in different areas of CPS including monitoring and actuator infrastructure, communication network, computation and control operation. We identify different elements in each area and explain the nominal and abnormal behaviour of all the elements. Finally we will explain the current solutions to deal with the abnormal behaviour of the elements.*

Keywords: *Cyber-Physical system, Architecture, monitoring and actuator, Communication Network, Computation and Control Operations*

I. Introduction

The advent of internet erased the boundaries of the world. Communication among the people has been increased rapidly and data rates going faster and faster day by day. Internet has transformed the people's lifestyles, businesses, studies, entertainment. Going further is the communication between people and machines which is a current ongoing research area. But, still there is a small gap between the cyber world where the information is processed, altered and exchanged and the physical world where we live.

Cyber Physical Systems (CPS) is a dominant research topic with wide range of applications in many areas. The word (CPS) refers to a new cohort of systems with integrated computational and physical capabilities that can collaborate with humans through many new techniques. CPS are the outcome of amalgamation of cyber world and the physical world. Conventional cyber systems were commonly contemplated as passive, "dumb" part in the physical world, but with CPS, now we have to consider what is being displace or varied in the physical world. The power to collaborate with, and expand the capacity of, the physical world through computation, communication, and control is a crucial facilitator for upcoming technological advances.

A considerable distinction between CPS and regular control system or an embedded system is the ability to use communications, which adds scalability and reconfigurability as well as potential instability and complexity. Moreover, CPS has apparently more intelligence in sensors and actuators as well as considerably stringent performance limitations. Progression in the cyber world such as communications, sensing, networking, storage, computing and control, along with the advances in physical world such as hardware, materials, and renewable "green" fuels, are all rapidly merging to realize the class of highly interactive computational systems that are reckoning on actuators and sensors to monitor and trigger the changes.

CPS have multitudinous applications in many fields like consumer, health care, military, transportation, energy, manufacturing, robotics and infrastructure. CPS applications are coming up across multiple sectors, such as adaptive cruise control and antitheft devices in cars and ATM's, flight control and electrochromic cabin windows in airplanes, location services in cell phones, entertainment, gaming, flight control and electrochromic cabin windows in airplanes, pacemakers in humans, haptic systems and robotic vacuum devices at homes.

The applications of CPS make human life more comfortable. Advances in CPS can make applications faster, perform distributed integration of large scale systems (e.g., automated road and airspace traffic control), temporally more and spatially precise (e.g., telerobotic surgery), demonstrate high efficiency (e.g., zero-net

energy buildings) , robust to hostile or not reachable environments (e.g., autonomous search and rescue, disaster recovery), and enhance quality of life (e.g., ubiquitous healthcare), augment human capabilities (e.g., body sensor nets, brain–computer interfaces). Cyber–physical coupling itself has enormous impact. CPS promises to hence streamline paradigm shifts in our society.

To deploy the CPS applications we need some elements which will fall under three categories sensors and actuators, communication network and computing nodes. The sensors and actuators collect the data from physical world. The collected data will be transmitted over the network to the computing nodes where the data will be processed and result will be generated and displayed in a format that is required by the end users. Each area has several challenges that need to be addressed when actual deployment is done in the real world.

In this paper we discuss about different concerns about CPS. First explains how CPS is show as layered Architecture. Second we explain the challenges in different areas of CPS with examples then we explain about different existing solutions to overcome such challenges. We end the paper by outlining some research directions that helps to vanquish the challenges and deploy the CPS in real world.

II. Layered Cyber-Physical system Architecture

This architecture describes the formation of cyber-physical system .The architecture is represented in modular fashion, consisting of physical world integrated with cyber world with Monitoring and Actuation Infrastructure, Network Communication Infrastructure, and Distributed Centralized or Decentralized Control and Computation Infrastructure.

A. Physical Process system

The Physical entity refers to the mechanical, chemical, electronic elements of a system which are interconnected to perform a particular operation. Examples of this system are energy systems, power systems, nuclear power plants etc. Here resilience of such systems is achieved through improving features such as robustness and reliability.

Part of each layer of cyber feedback control loop

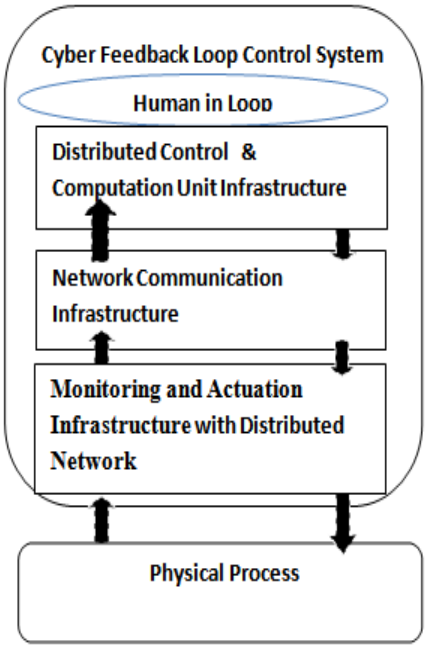

Figure 1: Cyber-Physical System in generic Layered Architecture

B. Cyber feedback loop control system

The cyber world has various elements to monitor and control the physical process of the system. Depending on the functionality of the element, we propose, layered approach to distinguish the elements as follows with wide applications from health care to smart grid; each application uses it's know sensing types and its network.

Monitoring and Actuation Infrastructure layer: This layer observes the physical entity status and acts as an interface between the physical and cyber world. This is done by various types of sensors, actuators device and it

is networked to each other. As we know that cyber physical system having ECG, EMG, EEG, SpO2, accelerometer, & tilt sensors, ECG & PPG ,Video camera, audio, RFID, & smart, door lock Light, smoke, & temperature sensors, heat flux, gas(O2, CO,&CO2), GPS, accelerometer, magnetometer, Camera WiFi, and compass are some of the different types of sensors used in various application like medical application, electronics application, transport application, smart grids application , and game applications.

Network Communication Infrastructure layer: This layer forwards the status information to Distributed Control and Computation Unit infrastructure. Based on the type of the application, Network communication infrastructure uses various technologies like switch, router and gateway with corresponding protocols. Body Sensor Network, GPRS, GSM, Wireless sensor Network, 3G, Bluetooth, WiFi Cellular and Internet are the different types of communication network are used between "Monitoring and Actuation" and "Control and Computation Unit" for different application.

Distributed control and computation Unit infrastructure layer: This layer is also called as Supervisory layer that offers human-machine interactions and capability of centralized decision-making. Doctors and nurses, data acquisition and storage component, agent-based command-control component, query manager agent and a set of Command, Control, Communication and Intelligence (C3I) user-interface agents to interact with users, an intelligent traffic signal control protocol to speed up car-crossing at intersections and smart user's phone are used as a control and computation unit in various applications.

Human in Loop: This layer embedded with Distributed computation and control layer were higher level policy and decision taken to appropriate query. In some situation other than intelligence decision support system or knowledge database human intervention is also required for support.

III. Challenges in Cyber-Physical System

Challenges with Monitoring And Actuator Infrastructure:

The sensors and actuators exists in the physical space. They collect the information from the surrounding and give it to the cyberspace for processing using the networking elements. The practical deployment of the sensors and actuator poses several challenges that needs to be addressed properly to achieve the desired functionality. Some of the challenges are

Dependability which is the characteristic of a system to carry out desired functionalities during its operation without evidential degradation in its outcome and performance. Dependability indicates the degree of reliability put in the entire system. A system which is highly dependable should operate correctly without intrusion, perform the needed functionalities as desired and it should not break down during its processing. It is a very difficult task to assure dependability before actual system operation. For example, timing uncertainties regarding sensor readings and immediate actuation may deteriorate dependability and lead to unexpected results. There is a visible interdependency between Cyber and physical components of the system and during system operation those underlying components might be dynamically interconnected, which, makes dependability analysis very problematic. The solution to this is to introduce a common language that clearly explains dependability related information across constituent systems/underlying components in the design stage.

Accuracy means the degree of match between a system's measured/observed values to its actual/calculated one. A system which is highly accurate should give actual outcome as close as possible. Maximum accuracy comes into play especially for the applications of CPS where even small imprecision lead to system break downs. For example, an object tracking system which is motion based if uses imperfect sensor conditions then based on incorrect object position estimation it may take untimely control action, which causes the system failure.

Efficiency means the amount of usage of resources (such as energy, cost, time etc.) that are required by the system to perform required functionalities. A system which is highly efficient should operate correctly and use optimum amount of system resources. Usually the sensors and actuators use more power to perform their operations. In CPS applications Efficiency is mainly needed for energy management. So, CPS applications can be developed in such a way that it consumes minimal energy by keeping the sensors in a sleep mode based on the criticality of the application.

Robustness is the ability to with stand different environmental conditions. Usually the sensors will be place in the physical world which leads to challenge of facing different environmental conditions. So the sensors and actuators should be manufactured in a way that they can work under any kind of environmental conditions without any inaccuracy in the expected out comes and also with minimal energy consumption. Since, these sensors and actuators are placed in the outside world it is profitable if they can use renewable energy resources

like solar energy. So, the applications of CPS must be developed in such a way thinking about all the possible environmental conditions.

Availability gives the ratio of total time that a system or a component is functional during a specified period and the length of the period. The availability of the sensors and actuators is very important. In case of any failure these should be a mechanism to notify the occurrence of failure and also to with stand at least till the notification is sent to the concerned. In any situation the system should be designed in such a way that in case of critical applications the Availability should be made as hundred percent by keeping redundant systems.

Cost of the sensors and actuators is an important concern to develop an application of CPS. Even though the networking hardware is available at affordable prices the cost of sensors and actuators is still high. Advances in research of developing affordable hardware with accurate sensibility should be done to make CPS applications more available to all classes of people.

Challenges with Communication Network:

The Deployment of CPS applications involve communication network that acts as intermediate connection between the physical world and the cyber world. The cyber and physical worlds can be integrated using wireless or wired networks each of which has its own challenges. Some of the challenges related to the communication network are

Wiring: It is difficult to implement CPS applications using wired network. Most of the applications uses wireless networks. If wiring is used the cost of wiring is an important factor which effects the deployment of application. Maintenance of wiring is also a tedious task. But using wired network loss of data will be less and reliability and security will be high.

Power and Energy: The network elements used for CPS applications consume power and energy to transmit the data to cyber space. A mobile device is small in size, generally handy and dedicated to provide desired set of functionalities; the ability to deliver the power by its power source may not be as much as the one installed in a fixed device. When a device is allowed to move freely, it would generally be hard to receive a continuous supply of power. A mobile device should be able to operate in an efficient and effective manner to conserve energy. To make it more specific, it should be able to transmit and receive in an intelligent manner so as to minimize the number of transmissions and receptions for certain communication operations.

Mobility: CPS applications such as smart cities may require the networking elements to be mobile**.** Unlike wired networks, all devices are free to move in a wireless network. To support mobility, as a user moves around an ongoing connection should be kept alive. In any network, when a mobile host moves from the coverage of a base station or access point to that of another one a handoff occurs. Therefore we need a protocol to ensure seamless transition during a handoff. This involves many issues like deciding how data is routed during the handoff process and when a handoff should occur. Sometimes, packets are lost during a handoff. In an ad hoc network, when a mobile host moves the topology changes. So to cater for the topological changes of an ongoing data communication, the transmission route may need to be recomputed. As an ad hoc network may consist of many mobile hosts, the design of an effective and efficient routing protocol is challenging.

Data Rate: A CPS application requires increasing the current data rates to support future high speed applications. If application requires large amount of data transfer like live video streaming then high data rates is required. Data rate is a function of various factors such as the data compression algorithm, power control, and the data transfer protocol, interference mitigation through error-resilient coding,. Therefore, the design should be well thought out by the manufacturer that considers these factors in order to achieve higher data rates. When multimedia applications such as video conferencing or traffic surveillance are to be supported by a wireless network data, compression plays a vital role. Currently, compression standards such as MPEG-4 produce compression ratios of the order of 75 to 100. Improving the existing data compression algorithms to produce high quality audio and video even at these compression rates is a challenge. Unfortunately, highly compressed multimedia data is more sensitive to interference and network errors and it is necessary to use the algorithms to protect sensitive data from being spoiled. We should explore efficient error control algorithms with low overhead. Other solution to improve the data rates would be to employ intelligent data transfer protocols that adapt to the traffic characteristics and time-varying network.

Security: CPS applications require more security which is a big concern in wireless networking. Mobility of devices increases the security concerns in a wireless network. To provide security to its users current wireless networks employ authentication and data encryption techniques on the air interface. An application like smart work places in large enterprises deploys IP network level security solution to ensure that the corporate network and proprietary data are safe. To make access to fixed access networks reliable Virtual private network (VPN) is an option. It is imperative that wireless security features must be updated constantly, since hackers are getting smarter.

Signal Fading: When compared with wired media, wireless transmission of may lead to distortion of signal or weakened signal since they are transmitted over an unprotected, open, and ever changing medium

with unclear boundary. Up on that, before it arrives at the receiver the same signal may disperse and travel on different paths due to diffraction, reflection, and scattering due to the obstacles. So, to reach the destination the dispersed signals on different paths may take different times. Thus, the resultant signal after summing up all dispersed signals may have been significantly attenuated and distorted when compared with the actual transmitted signal. The receiver may not recognize the signal and hence the transmitted data cannot be received. Thus the unreliability of the wireless networks causes a substantial number of packet losses.

Challenges with Computation and Control Operations:

Different applications of CPS require different type of computations and control operations. If application is just to trigger an action if some event occurs then the computing system does not require high storage but response time should be low. If application is in such a way that it store data and perform some analytics and deliver such information to the users then the system requires huge storage and processing capabilities. Usually the computations and control operations are done by the servers. So based on application there are different challenges in this area also, some of them are

Processing Speed: CPS applications not only have to find and analyze the relevant data they need, they must find it quickly. Visualization helps applications perform analyses and make decisions much faster, but the challenge is at high speed the application has to go through the large volumes of data and access the level of detail needed. As the degree of granularity increases the challenge grows. One possible solution is hardware. Some vendors are using powerful parallel processing and increased memory to crunch large volumes of data extremely quickly. Another method is putting data in-memory but using a grid computing approach, which involves many machines to solve a problem. Both approaches allow the applications to explore huge data.

Understanding Data: If the application of CPS requires data analysis then it takes a lot of understanding to get data in the right shape so that we can use visualization. For example, if an application involves identifying a user by the data taken from social media content, we need to understand who the user is in a general sense such as a customer using a chosen set of products and understand what it is you're trying to visualize out of the data. Visualization tools are likely to be of less value to the user, without some sort of context. The solution to this challenge is to have the proper domain expertise in place. The people analyzing the data have a deep understanding of what audience will be consuming the data, where the data comes from how that audience will interpret the information.

Accuracy and Timeliness: These two are very important factors in CPS applications. Even if an application can find and analyze data quickly and keep it in the proper context for the audience that will be consuming the information, the value of data for decision-making purposes will be reduced if the data is not accurate or timely. This challenge is there in any data analysis, but when considering the volumes of information involved in CPS applications with big data, it becomes further more pronounced. To solve this problem, applications need to have an information management process or data governance in place to ensure the data is clean. It's good to have a pro-active method to address data quality issues so that we can avoid problems which may arise later.

Storage: Some applications of CPS that involves data analytics may need to store large volumes of data. Conventional WAN-based transport methods cannot move terabytes of data at the speed required for applications. It uses a portion of available bandwidth and do transfer at speeds that are unsuitable for such huge volumes, introducing unacceptable delays in storing retrieving and processing data.

Control: CPS applications involve lot many devices that capture the data from the physical world and also the devices that transfer the data from physical to cyber world. So this poses a challenge for the node that control all these devices. Identifying the exact device and controlling it is a difficult task. There should be a way of creating the device Id that is generic so that application should be available to all kind of devices that can be benefitted.

Challenges with Overall Deployment of CPS:

Maintainability is the ability of a system to be repaired in case any failure occurs. A system which is highly maintainable should be repaired in a simple and quick manner with minimum expenses of supporting resources, and it should not cause additional problems during the maintenance process. If there is a close interaction among the system components like sensors, actuators, networking components, and physical components constituting CPS infrastructure, we can propose autonomous predictive /corrective diagnostic mechanisms. Using such mechanisms continuous monitoring and testing of the infrastructure can be performed. The result of monitoring and testing facilities help finding which units need to be repaired. Some elements, which causes frequent failures, can be designed again or disposed and replaced with better quality elements.

Availability is the characteristic of a system to be available for accessing even when errors occur. A system is said to be highly available if it isolates malfunctioning portion from itself and resume the operation even in the absence of it. Harmful cyber-attacks questions the availability of the system services significantly.

For example, in Medical applications of Cyber-Physical Systems, necessary actions will be taken in a timely manner to save a patient's life based on medical data. Cyber-attacks or failure of systems/components may lead to the loss of medical data causing risk to the patient's life.

Safety is the quality of a system not to cause any danger, harm or risk anywhere around it while it is in operation. A system which provides high safety should be in accordance with all kinds of safety regulations to a maximum extent and should implement guaranteed safety mechanisms if anything goes wrong. For Example, Safety of manufacturing industries can be guaranteed using embedded control systems with an automated process control and sensors and actuators that collect the data across the manufacturing industry. Sensors connected to a smart network could detect operational failures and help in prevention of dangerous incidents due to those failures.

Resilience is the property of a system to continue in its operation and provision of services in an acceptable quality even though the system is exposed to any kind of errors. A system with high resiliency should be able to detect any kind of failures as early as possible and should be able to self-heal and also should be able to recover faster to continue to meet the demands for services. If an application is critical then high resilience comes into play (e.g. automated brake control in vehicular Cyber-physical systems). While designing a highly resilient CPS we need to have a complete understanding of important failures and errors, the resilience properties of the required application, and evolution of system due to the dynamically varying nature of the operational environment.

Adaptability is the ability of a system to survive by adjusting its own configuration in accordance with different circumstances in the environment. A system with high adaptability should be quickly adjust to changing needs. Adaptability is one of the important features in the next generation air transportation systems. The capability of the next generation should enhance performance of air space using its computerized air transportation network which allows air vehicles immediately to accommodate themselves to changing environment such as weather conditions, routing of air vehicle, air traffic congestion, and other issues related to security.

Sustainability is the ability of a system to last long without compromising requirements of the system, while continuing to use the system's resources efficiently. A system that is highly sustainable must be durable, adaptable and resilient. The crucial part of energy provision and management policies is to achieve sustainability from energy perspective. For example, the Smart Grid allows energy distribution, management, and customization from the customer's perspective by utilizing green sources of energy extracted from the physical environment. However obstructions like irregular energy supply and unknown load characterization damages the efforts to maintain long-term operation of the Smart Grid. To maintain sustainability, the applications of CPS like Smart Grid requires use of real-time performance measurements, dynamic optimization techniques for usage of energy, environment-aware duty cycling of computing units, planning and operation under uncertainties, and devising self-contained energy distribution facilities

IV. Existing Solutions to Deploy a Cyber-Physical System

To actually deploy any application of CPS there are several challenges that needs to be addressed to ensure continuous operation. To achieve this development of applications should be done in a planned way from design to deployment. There are several challenges at each stage and there are numerous methodologies and tools that are proposed to overcome those challenges.

But still it is an evolving area because the requirements of CPS are not completely understood and are changing day by day and the complicated dynamic behaviour of CPS is difficult to capture in a simple understandable manner. Examples of such methodologies include capability of expressing timing constraints and spatial conditions and check if such constraints are satisfied, decomposing the life cycle into several stages based on the Model based development according to different views of systems.

To avoid security challenges there are different solutions like context-aware security framework for CPS that uses dynamic adaptability to the physical environment by the assistance of context coupling, use of distributed real-time software, use of competitive and co-operative resource management, using virtual test beds, use of highly confidential software to avoid security issues, integrating simulation and emulation platforms for security purposes, experimenting with different architectures to find the best suited architecture based on requirement of application, use of sandboxing controllers for cyber-physical systems.

To add resiliency to CPS there are several techniques proposes that uses artificial intelligence and danger theory based immune algorithms. These techniques uses the concepts of agents, self-awareness and self-healing approaches to achieve resiliency and make the system fault tolerant.

These are some of the examples of existing methodologies, still research is going on and lots of applications of CPS are under development.

V. Conclusion

The Cyber-Physical Systems (CPS) is an ongoing research area with huge popularity with wide variety of applications. It is mainly the result of integration of cyber and physical worlds. There are several challenges that come up while deploying such applications. In order to classify those challenges into three areas which are sensors and actuators that constitute the physical world, computation and processing elements that constitute the cyber world and networking elements that integrate the cyber and physical worlds we survey the literature of this area. We have also discussed some of the existing solutions and we conclude that existing solutions helps to face the current challenges to some extent as the applications of the CPS are growing day by day still there are lot more challenges yet to come we need to fore predict the upcoming challenges and should develop new technologies to safe guard the applications from those challenges.

References

[1]. Wang, Eric Ke, et al. "Security issues and challenges for cyber physical system." Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing. IEEE Computer Society, 2010.
[2]. Shi, Jianhua, et al. "A survey of cyber-physical systems." Wireless Communications and Signal Processing (WCSP), 2011 International Conference on. IEEE, 2011.
[3]. Gunes, Volkan, et al. "A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems." TIIS 8.12 (2014): 4242-4268.
[4]. Neuman, Clifford. "Challenges in security for cyber-physical systems." DHS: S&T workshop on future directions in cyber-physical systems security. Vol. 7. 2009.
[5]. Sun, Meng. "Challenges on Coordination for Cyber-Physical Systems."Applied Mechanics and Materials. Vol. 347. 2013.
[6]. Ali, Salman, et al. "Network Challenges for Cyber Physical Systems with Tiny Wireless Devices: A Case Study on Reliable Pipeline Condition Monitoring." Sensors 15.4 (2015): 7172-7205
[7]. Lokesh. M. R, Y.S. Kumaraswamy Nov 2014—On Autonomic Self Healing Architecture for Resiliency in Cyber Physical System International Journal of Multimedia and Ubiquitous Engineering ISSN No. 1975-0080 Volume 9, No. 11, Nov 2014