Cyber Physical System

Navin Dhinnesh ADC
Assistant Professor (Sr. Gr)
Department of Computer Applications
Mepco Schlenk Engineering College, Sivakasi

Abstract

In 2006, Cyber Physical Systems (CPS), the new word was invented in the United States [1]. The combination of devices like sensors with embedded systems is quickly receiving its place in cyber world. These devices jointly with the information filed are becoming the main focal point, called as Cyber Physical Systems. This word was found keeping in mind the escaling significance of relations among the mutually related computing systems with the physical world [2]. The author of this paper gives an overview of CPS architecture, its functions and its security threat.

Keywords- Internet of Things, Sensor, Cyber-Physical Systems, Real Time Systems, Embedded Systems

I. INTRODUCTION

Combining the applications that are very much beneficial in the aspect of computing both in space and time are said to be cyber physical systems [3]. The combined effect of two systems, cyber and physical, has changed our work style [4]. The Cyber Physical System (CPS) is considered as a smart system, which is extremely interconnected. CPS and Internet of Things (IoT) have closely related concepts. The CPS impact is very much obvious in the field of autonomous vehicles, Robots, etc., CPS have assisted in the development of smart devices [5. These smart devices are connected by means of IoT and allowed to work together. The combination of both CPS and IoT are capable of capturing and processing data so that the user gets constructive information from it. CPS is considered to be networked as well as distributed among Real Times Systems (RTS) [6]. CPS has few distinguished properties like: Self-adaptation, Self-organization, Self-optimization, etc.

Some of the examples of CPS are: medical devices, aerospace systems, defense systems, etc. CPS should function dependably, at the same time in a safe and secure manner. CPS is measured as convergence of embedded systems. Now a day the field of aerospace, factory automation is very much in need of CPS. These lead to finding of new research horizons. CPS is also for non-technical users too. CPS is now a day becoming ubiquitous. As internet brought change in transformation in human life, CPS change the way in working together with the physical world. CPS will work with the systems that react more swiftly and also with the systems that are so accurate [7]. In coming years, all the smart systems will be using CPS. Cross layer design plays a vital role here since a system is believed to be CPS if and only if there exists a stiff interaction among physical and cyber parts.

II. ARCHITECTURE OF CPS

The CPS architecture shown in Figure 1 comprises of Controller, Sensor and Actuator to interact with the physical world. Physical world include: physical entities, humans, and physical sensors. The CPS architecture will be suitable mainly for many applications and also for services.

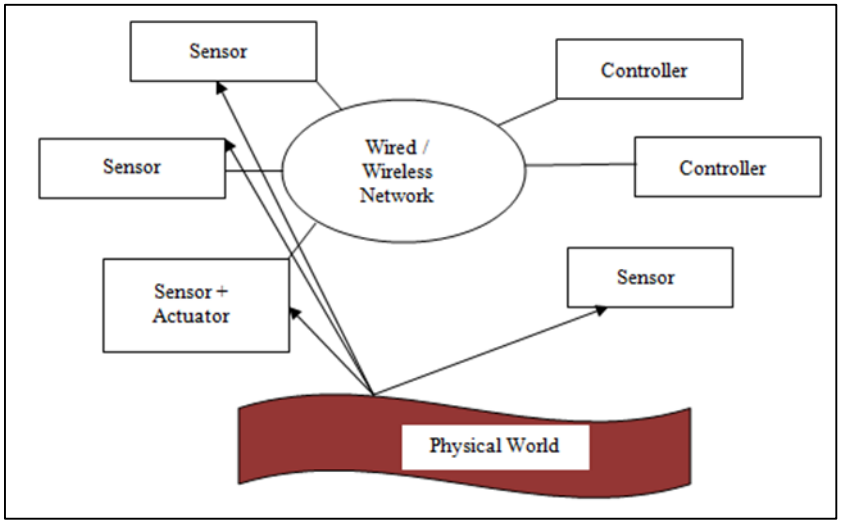

Fig. 1: CPS Architecture

A. Functions of Cyber Physical System

CPS functions are classified into five levels. They are: i) Configuration Level, ii) Cognition Level, iii) Cyber Level, iv) Data to Information Conversion Level, and v) Smart Connection Level. The five levels [4] are shown in Figure 2

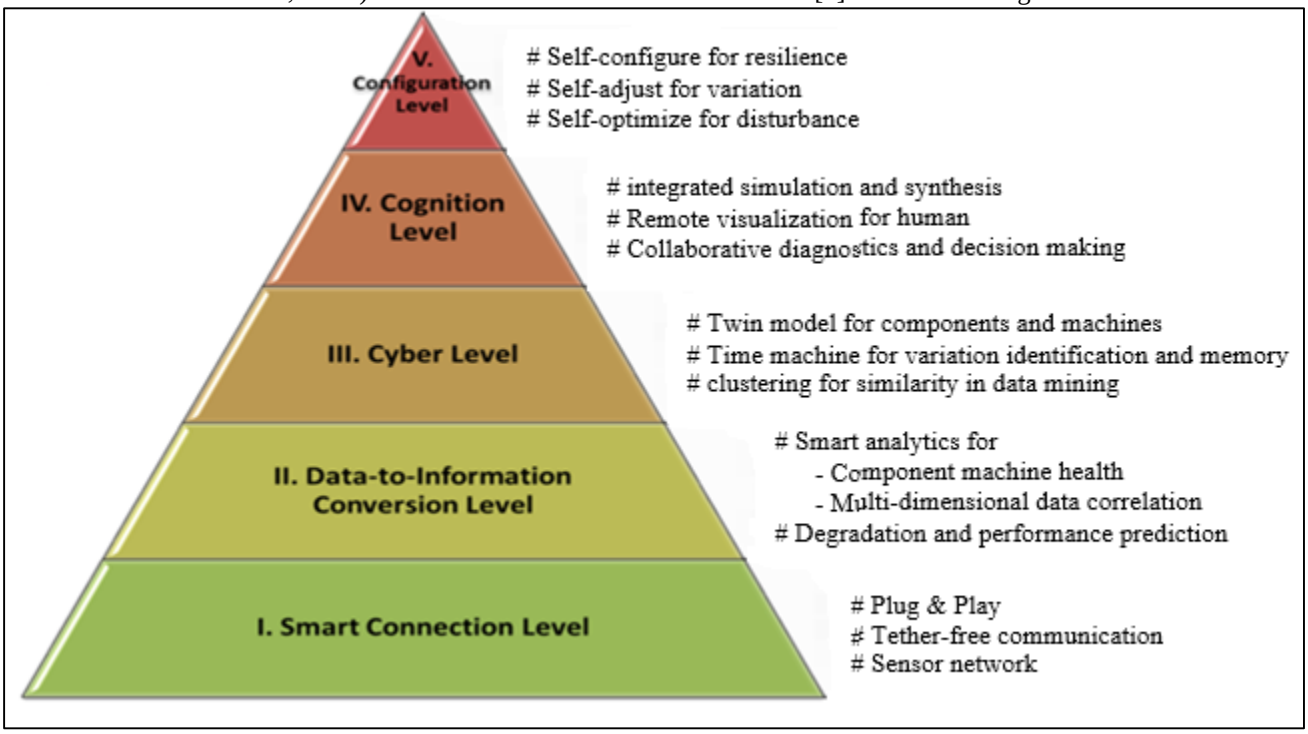

Fig. 2: Five levels of Cyber Physical System

Image Courtesy [8]

B. Security Threats in CPS

The most vulnerable threat in CPS are the potential threats, which must be handled from various angles. Conventionally if a system is said to be secure only when it suit the following three security necessities [9]: i) Confidentiality, ii) Availability, and iii) Integrity. A threat is nothing but a situation which is probable of making damage [10]. Potential threats are the one which will be possible but not thus far real. Every threat is classified into five critical factors as: source, target, motive, attack vector, and potential penalty. Table I shows the various critical factors and their outcomes.

Table 1: Critical factors and their outcomes

S. No	*Critical Factor*	*Outcome*
1	*Source*	*is the origin of an attack* *Three types:* *i) Adversarial threat – from person, groups or nations* *ii) Accidental threat – accidentally caused* *iii) Environmental threat – natural disasters [11]*
2	*Target*	*main target will be CPS components as well as CPS applications*
3	*Motive*	*may be political or spying or criminal [12] [13]*
4	*Attack Vector*	*May execute any one among the following four methods.* *i) Interception* *ii) Interruption* *iii) Modification* *iv) Fabrication*
5	*Penalty*	*will negotiate the systems confidentiality, reliability, availability, privacy, or protection*

III. CHALLENGES IN CPS

There are numerous challenges in CPS. The author has taken into consideration Automotive and Medical CPS for our discussion.

A. Automotive Scenario [14]

People are now using lot of sensors in the field of automobile sector, mainly for protecting the passenger from any danger. The system will be assisting the drivers who are driving their vehicle in a monotonous manner. These are the basics of autonomous vehicles. A vehicle to be autonomous the sensors must be very much useful in assistance in fault findings, communication between vehicles, etc. The main communication among vehicles will permit exchange of data like speed, traffic, etc.

B. Medical Cyber-Physical Systems

This is mainly for monitoring the patients. These systems must also be monitored, since it should not mal function. Medical CPS is mainly for monitoring the patient`s body. The machines used to monitor patients are proton therapy, implantable devices, etc. The devices should work properly and must not malfunction. Safety and reliability are very important here.

IV. CONCLUSION

All the computing systems must be rethought. Although by using the CPS, a country may be protected from attacks coming from inside, but it cannot from the external world. Now a day the current trend is that everyone is practicing cyber physical system. Using this secured CPS, one can protect so many human lives.

ACKNOWLEDGEMENT

The author acknowledges the support and encouragement by the Management, Principal and Director of Computer Applications department, towards this work.

REFERENCE

[1] Lee, E. A. (2006). Cyber-physical systems—are computing foundations adequate? NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, Austin, Texas.
[2] L Wang, M Törngren, M Onori, "Current status and advancement of cyber-physical systems in manufacturing", Journal of Manufacturing Systems, 37, pp 517 -527, 2015
[3] Rajkumar R, et. al, "Cyber physical systems: The Next Computing Revolution", Design Automation Conference, 2010
[4] Wilbur L. Ross, Kent Rochford, "Framework for Cyber -Physical Systems: Overview, National Institute of Standards and Technology, U.S. Department of Commerce, Volume 1, Version 1.0, June 2017 Available : https://doi.org/10.6028/NIST.SP.1500-201.pdf
[5] Nishtha Kessawni, Sanjay Kumar, "Cyber Physical Systems and Smart Cities", CSI Communications, Vol 41, Issue 9, pp 29 – 30, December 2017
[6] Suseela, Kavitha, "Cyber Physical System (CPS) and its Implications", CSI Communications, Vol 41, Issue 9, pp 8 – 10, December 2017
[7] Antsaklis P, "Goals and Challenges in Cyber-Physical Systems Research Editorial of the Editor in Chief", IEEE Transactions on Automatic Control, Vol. 59, No. 12, Dec 2014
[8] https://en.wikipedia.org/wiki/Cyber-physical_system
[9] A Humayed, J Lin, F Li, B Luo, "Cyber-Physical Systems Security – A Survey", Cornell University Library, Jan 2017, Available: https://arxiv.org/pdf/1701.04525.pdf
[10] Charles P. Pfleeger and Shari Lawrence Pfleeger, "Security in Computing (4th Edition)", Prentice Hall PTR, Upper Saddle River, NJ, USA, 2006
[11] James L Cebula and Lisa R Young. A taxonomy of operational cyber security risks. Technical report, DTIC Document, 2010
[12] Roberto Setola. Cyber threats to scada systems, 2011.
[13] US-CERT. Cyber threat source descriptions, "https://ics- gov/content/cyber-threat-source-descriptions", 2009
[14] Bartocci E, "Cyber-Physical Systems: Theoretical and Practical Challenges", ERCIM news 2017. Available online: https://ercim-news.ercim.eu/en97/special/cyber-physical-systems-theoretical-and-practical-challenges