Chapter 3

Safety–Critical, Dependable, and Fault–Tolerant Cyber–Physical Systems

Guru Prasad Bhandari
Banaras Hindu University, India

Ratneshwer Gupta
Jawaharlal Nehru University, India

ABSTRACT

Cyber-physical systems (CPSs) are co-engineered integrating with physical and computational components networks. Additionally, a CPS is a mechanism controlled or monitored by computer-based algorithms, tightly interacting with the internet and its users. This chapter presents the definitions relating to dependability, safety-critical and fault-tolerance of CPSs. These definitions are supplemented by other definitions like reliability, availability, safety, maintainability, integrity. Threats to dependability and security like faults, errors, failures are also discussed. Taxonomy of different faults and attacks in CPSs are also presented in this chapter. The main objective of this chapter is to give the general information about secure CPS to the learners for the further enhancement in the field of CPSs.

1. INTRODUCTION

Cyber-Physical System (CPS) is computer-enabled mechanism interacting networks of physical and computational components with feedback loops where physical processes affect computations and vice versa. CPS will provide the basics of our critical infrastructure, in terms of emerging and future smart services, and improve our quality of life in many aspects (Wolf, 2009; Alho, 2017). Basically, CPS is a mechanism controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users functioning on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a numerously that change with context (Foundation, 2008).

DOI: 10.4018/978-1-5225-5510-0.ch003
CPS is also known as a special class of embedded systems that use embedded computers and networking infrastructure to control physical workflow processes. CPS uses multiple sensing and actuation units that gather, process, exchange and use information as a team is the next generation of co-engineered systems. Such collection of units that bridge the cyber-world of computing and communications with the physical and biological worlds are called Cyber-Physical Systems (Antsaklis, 2014). CPS has been applied in many areas specially in automotive robotics, aerospace, defense, medical devices (pacemakers, insulin pumps), in critical infrastructure (supervision and direct control of power plants, oil and gas distribution networks, refineries), transportation (airplanes and air-traffic control, rail), in consumer products (camcorders, cameras, mobile phones), in chemical process industries, manufacturing and automobiles (anti-lock braking system (ABS), electronic stability control, fuel injection, emission control) etc.

The major problem of achieving dependable operations for CPS’s open and networked control systems is approached using a systems engineering process to gain an understanding of the problem domain, since fault tolerance cannot be solved only as a software problem due to the nature of CPSs, which includes close coordination among hardware, software and physical objects (Alho, 2017). Challenges for software architecture of CPSs includes - sharing of huge amounts of data to optimize processes, utilization and predictive maintenance levels while having predictable timing for end-to-end latencies, V&V, especially security and safety, of evolving systems, scale increase from closed network to integrated system of systems, flexible allocation of resources needed for scalability, stakeholders want systems to be easy to use, build, maintain and repurpose, wide range of timing requirements, stakeholders want to use whatever communication network best meets application specific requirements, support for evolvability, including modifiability and maintainability, product variation for mass-produced systems etc.

In this chapter, we will give a brief introduction about CPSs with its background information. Safety-critical CPSs, dependable CPSs and fault-tolerant CPS will be introduced and their composite explanation will also be emphasized in this chapter. Current challenges in CPSs to make the system safety, dependable and fault-tolerant will be explained with their associated issues. State-of-the-art of the proposed solution to make CPS reliable will also be provided through the chapter. Finally, future direction and conclusion will be provided. Figure 1 presents a Cyber-Physical Systems - a concept map (as in (Asare et al., 2017)).

The structure of this chapter is as follows. Introduction section briefly overviews the chapter, its theme, and purpose. Background of the cyber-physical systems is given in the second section followed by the literature review section. Safety-critical, dependable cyber-physical systems are briefly explained in third section. After that, some current challenges of cyber-physical systems are also presented. State-of-the-art on the solutions for current challenges is also discussed followed. The final section concludes the chapter.

2. BACKGROUND

CPS (Cyber-Physical System) integrates with computing and communication capabilities, monitoring and control of entities in the physical world through a network system that works so dependability, safely, securely, efficiently and in real-time (NSF, 2006). Based on such a broad definition, CPSs are almost synonymous with networked digital control systems and embedded systems. Moreover, CPS means large, complex physical systems that are interacting with a considerable number of distributed computing
Related Content

Conceptual Modeling Method for Separation of Concerns and Integration of Structure and Behavior
[www.igi-global.com/article/conceptual-modeling-method-separation-concerns/61395?camid=4v1a](www.igi-global.com/article/conceptual-modeling-method-separation-concerns/61395?camid=4v1a)

Hardware Virtualization on Dynamically Reconfigurable Processors
[www.igi-global.com/chapter/hardware-virtualization-dynamically-reconfigurable-processors/50426?camid=4v1a](www.igi-global.com/chapter/hardware-virtualization-dynamically-reconfigurable-processors/50426?camid=4v1a)

HMM-Based Vietnamese Speech Synthesis
[www.igi-global.com/article/hmm-based-vietnamese-speech-synthesis/133113?camid=4v1a](www.igi-global.com/article/hmm-based-vietnamese-speech-synthesis/133113?camid=4v1a)

A Survey on Using Nature Inspired Computing for Fatal Disease Diagnosis
[www.igi-global.com/article/a-survey-on-using-nature-inspired-computing-for-fatal-disease-diagnosis/199004?camid=4v1a](www.igi-global.com/article/a-survey-on-using-nature-inspired-computing-for-fatal-disease-diagnosis/199004?camid=4v1a)