Preface

In 2007, the US National Science Foundation (NSF) recognized Cyber Physical Systems as a key area of research. A Cyber Physical System (CPS) is a system that combines and coordinates the Internet and physical elements. These systems are distributed networks executing in unpredictable environments and built from control systems and embedded systems to monitor and regulate the physical world in real time. Cyber Physical Systems can be found in aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, consumer appliances, and transportation. Unlike embedded systems, Cyber Physical Systems are designed as a structure of interacting elements with physical input and output. In embedded systems, the importance is more on the computational elements and less on the connection between the computational and physical elements. Enhancements in science and engineering will significantly increase the flexibility, independence, competency, functionality, consistency, and security of Cyber Physical Systems. They also widen the prospective of Cyber Physical Systems in several dimensions like collision avoidance, nano-level manufacturing, search and rescue in inaccessible environments, air traffic control, and healthcare monitoring.

This is not about adding computing and communication techniques to conservative inventions where both sides maintain distinct individualities. This is about the integration of computing and networking with physical systems to generate novel innovations in science, technical skills, and creations. CPS will have an amazing impact on the future of industry. Lagging behind in the fundamentals of CPS may render our scientific and technological arrangement antiquated. Whether we recognize it or not, we are in the center of a pervasive, thoughtful change in the way humans arrange physical systems and design their physical environment.

The main objectives of this book are to shed light on the significance of CPS for the future and to explain the fundamental wireless communication architectures with the computing systems to understand the design methodologies of CPS, which addresses the design and security challenges while communicating between systems in CPS. The book also includes open research issues in CPS. It consists of the following 15 chapters, each of which contains multiple sections focusing on various aspects in that section. Each chapter ends with a conclusion specifying future research challenges related to it. In the following paragraphs, we present a brief overview for each of the chapters and the sections therein.

Chapter 1 defines Cyber Physical Systems with its features. Cyber is an integration of computation, communication, and control systems. Physical means natural and human-made systems that are managed and governed by the physics regulations and functioning in constant time. In Cyber Physical Systems, the cyber and physical systems are those firmly incorporated at all stages and dimensions. Starting in late 2006, the US National Science Foundation (NSF) and other United State federal agencies sponsored several workshops on CPSs. In 2007, the NSF identified CPSs as a key area of research. CPS uses em-
bedded computers and networks to compute, communicate, and organize physical actions. Simultaneously, a CPS receives feedback on how physical events impact computations and vice versa. Just as the Internet transforms how humans interact with one another, CPSs will transform how we interact with the physical world around us. In the latter part of this chapter, the challenges and opportunities in CPS are discussed. It also focuses on research trends in CPS. A summary of Wireless Cyber Physical Systems is explicated at the end of this chapter.

Chapter 2 focuses on prototype architecture for CPS and explains the approach to design open data service architecture for CPS. This chapter deals with the CPS architectural style, which can be used to provide support to the plan and assessment of other structural designs for cyber physical systems. It also shows the interconnections between physical and cyber components. In this prototype architecture, the important attributes of this architecture for CPS, which helps to identify many research challenges, are described and explained. We also discuss the open information service structural design to deal with the issues related to management of data in CPS. Along with the single-layer and multi-layer survivability of architecture, a portable CPS structure, which is known as multi-layer widespread structure, is discussed. This system uses unlicensed and licensed networks with various spectrums to connect CPS through different gateways. A research-related wireless access network project is described. In multilayer wireless networking, it describes the functionality of heterogeneous CPS networking. The last section focuses on mobile networking between various reachable networks and mobile devices.

Chapter 3 provides an overview on CPS design and discusses various CPS design components to create a network control for CPS. A large set of CPS physical processes are referred to as Cyber Physical System community. This CPS community deals with the modelling and design optimization of CPS. The network elements that are model-based emphasize control over system with various temporal semantics. Model-based design is a great technique for CPSs and are mainly used for developing mathematical modelling to plan, examine, prove, and certify dynamic systems. This is described in ten fundamental steps. This design methodology helps in assessing the development of CPS. Due to difficulty and nonexistence of accurate and technical tools, the three necessary elements in the strategy and study of existing and forthcoming cyber-physical systems are also explained in the chapter. The latter section of this chapter deals with the network latency in CPSs. At the end of this chapter, CPS design challenges are addressed.

Chapter 4 lists a variety of issues and challenges in connecting wireless and ad hoc networks. This chapter shows the interconnection issues in different wireless networks such as ad hoc networks and sensor networks. It also specifies the need for multicast routing protocols in mobile networks, because these wireless networks are suitable for multicast communication due to its inherent transmission ability. Based on the area to be covered, mechanism used for sensor deployment, and various properties of sensor network properties, different coverage formulations have been suggested. In addition, several constructions reachable areas and their expectations along with an outline of the explanations are described. Though IEEE 802.11 planned for organization-based systems, the Distributed Coordination Function (DCF) offered in IEEE 802.11 permits mobile networks to communicate with the channel exclusive of the base location. Several performance issues related to IEEE 802.11 are revealed. This chapter identifies the main reasons for performance losses and provides solutions for the scenarios in which issues were raised. The chapter discusses the issues arising during transmission in different wireless networks, such as Wi-Fi, 802.11-based wireless networks, etc. It also addresses the issues related to mobile IP and location tracking.

Chapter 5 describes the Cyber Physical Internet (CPI). The first section provides an overview of Large-Scale CPSs components, which describes protocol architecture of CPI. This chapter also focuses on CPS Interconnection Protocol (CPS-IP) and specifies a detailed design of CPS-IP. This chapter explores
the concept of the Cyber Physical Internet (CPI) and discusses the design necessities of it. In addition, it provides the restrictions of the present networking concepts to satisfy these necessities. The structural design of protocol stack for CPI has an extra layer Cyber-Physical Layer (CY-PHY Layer) to offer a conceptual description of the properties and type of cyber physical information. To enable standard communication between heterogeneous systems, Cyber Physical System-Interconnection Protocol is used. This protocol is mainly designed for special CPSs, which require overall instruction and performance guarantee for cyber physical interaction. The main objective of this protocol is to offer CPSs heterogeneity at three different levels: function interoperability, policy regulation, and performance assurance. Later, the transport protocol services used in the design of CPS-IP are explained.

Chapter 6 deals with the network QoS management and discusses the network characteristics and QoS requirements for CPS. An overview of aspect-oriented QoS modeling is dealt along with its specification for CPS. Wireless Sensor Actuator Networks (WSANs) perform a vital role in CPS. This chapter describes the key features of WSANs and the necessities of QoS provisioning in the perception of cyber physical computing. Network Quality of Service (QoS) is one of the research issues that is focused on in wide way. To address the challenges identified, a feedback scheduling framework is explained in the latter part of this chapter. It is a difficult task to satisfy end-to-end QoS requirements in CPSs. To overcome this, a model-driven middleware called NetQoPE is used to protect the application designers from the complications of programming at lower level CPU and by streamlining network QoS mechanisms. The chapter shows how NetQoPE provides QoS assurance for CPS applications. The chapter concludes with the possible challenges in Internet QoS.

Chapter 7 elucidates the security issues and challenges for CPS. This chapter gives a brief view on security control for CPS, which analyzes threats and uncertainties in cyber physical networks. It also describes a robust context-aware security framework for CPS. IT and CPS have a well-built organization of information and a set of skilled professionals for providing information security, but providing security to CPS is a new challenge as systems are interconnected. This chapter gives a brief study of CPS security by identifying and defining the problem of secure control systems and also observes the protections that information security and control theory provide to the system. Later, a set of challenges are described, which are required to enhance the security of CPSs. As today’s cyber physical systems are part of critical structure, an open and interconnected situation strengthens the effect of malicious actions. Even though in distributed systems delay is bearable, CPSs should follow certain timing requirements to perform regular process.

Chapter 8 addresses the security issues with respect to cyber physical systems. As cyber physical system security is not satisfactory, the security of a particular infrastructure depends on both internal and other related vulnerabilities. Communications between components in the cyber and physical realms lead to unintentional information flow. This chapter describes the difficult communications that occurs between the cyber and physical domains and their impact on security. Assailants may be competent to initiate exclusive attacks to cyber physical systems. There are several types of attacks that affect the interactions between the cyber and physical devices, which might be in a passive way or in an active method. Even though the communication provides authenticity and confidentiality, a few attacks form some threats against ad hoc routing protocols as well as location-based security systems. It has been said that many attacks modify the activities of the targeted control system. At the end of the chapter, we describe how control systems are affected by malicious attacks and also how to resolve these issues.

Chapter 9 describes the interoperability and communication issues in cyber physical systems. Cyber physical systems involve multi-domain models during the development process of the design. This chapter focuses on integrated design methodology that provides reliable relationships between various system
models of heterogeneous types. Each model is linked with the base architecture over the abstraction of an architectural view framework. From quadrotor perspective, this framework compares system models from different domains. Present methods lack in modeling, analysis, and design of CPSs due to nonexistent of an integrated framework. To overcome these difficulties, an architectural level system model is defined to capture the structural interdependencies. A base architecture for the complete system is described in this chapter to confirm the structural reliability the model elements and components present in it. The usefulness of this process is exemplified in the quadrotor air vehicle.

Chapter 10 discusses different networking issues in heterogeneous networking. To make a network survivable it must be heterogeneous. The functionality of this network is defined by a set of protocols and its operations. In heterogeneous networks, if a protocol is weakened by any attack, it will not affect the entire network. Applying this heterogeneity concept, a new survivability paradigm is described in this chapter. This network architecture improves the network’s heterogeneity without losing its interoperability. Several issues discovered in security and survivability applications can be converted into scheduling problems. To overcome this, a new model is described to support design and analysis with security and survivability concerns. A five-step model is introduced to transmute applications into model abstractions and representations with solutions resulting from scheduling algorithms. A reverse transformation converts the solutions back to the application domain.

Chapter 11 focuses on mobile computing issues in the heterogeneous environment. The fast development of mobile computing has produced a wide variety of technologies that affect systems in the mobile computing realm. Even though mobile computing focuses the importance of interrelated systems, the qualifying of interoperability remains an important constraint. In this chapter, several techniques are explained to manage various heterogeneity characteristics along with the key concepts related to these systems. A general approach is described to manage the heterogeneity. It has been seen that to have a better performance in overlapping networks, it is necessary to switch between the networks due to mobility and congestion. This problem is overcome by overlay networks that identify the existing network and then select the best network and allow transmission from one node to another node in the same network or create a novel network. In this way, this architecture provides a way to transmit packets to the mobile host using the available network.

Chapter 12 describes the cluster-based architecture for the heterogeneous environment. Along with the heterogeneous devices, Web-based content increases the necessity for computational services. However, recent trends make it difficult to execute such computations at the terminal side, whereas service providers often allow computations during different load operations. Many computational services are using conventional distributed systems, which provide successful packet transmission in IP networks. In this chapter, proxy architecture and its related tasks are discussed. Some of the necessary requirements, such as incremental scalability, 24x7 availability, and cost-effectiveness, are recognized for scalable network services. To administrate a large cluster and to construct a cluster-based scalable network services, a layered architecture is recommended. This architecture captures the scalable network service requirements and utilizes service-programming models to perform Transformation, Aggregation, Caching, and Customization (TACC) of Internet substance. For better performance, the architecture with the TACC programming model uses data semantics to create novel network services.

Chapter 13 discusses different network services required for cyber physical systems. A novel framework formed from a collection of independent agents that interact with each other is determined to provide a network service. Agents in this structure have the capability to perform independent activities such as duplication, migration, etc. A new method is developed in this chapter by means of genetic algorithms
to change the behavior of agents over peers and also to improve the network service performance in a
distributed and well planned way. Architecture with a remote control device, Personal Universal Control-
ler (PUC), is described. The PUC provides two-way communication with the applications for copying
specification for its functionality and constructing an interface for monitoring that electrical device. The
requirements of every application hold the information about its dependency information and availability
of appliance conditions. The network protocols, such as Service Discovery Protocols, are explained with
their types and functionality.

Chapter 14 shows the different cyber physical control systems with respect to intelligent and real
time systems. The focus of algorithmic design is to solve composite problems. Intelligent systems use
intellectual concepts like evolutionary computation, artificial neural networks, fuzzy systems, and swarm
intelligence to process natural intelligence models. Artificial intelligence is used as a part of intelligent
systems to perform logic- and case-based reasoning. Systems like mechanical and electrical support
systems are operated by utilizing Supervisory Control and Data Acquisition (SCADA) systems. These
systems cannot accomplish their purpose, provided the control system deals with the reliability of it.
In CPSs, dimensions of physical processes are taken by sensors and are processed in cyber subsystems
to drive the actuators that affect the physical processors. CPSs are closed-loop systems. The adaptation
and the prediction are the properties to be followed by the control strategies that are implemented in
cyber subsystems.

Finally, Chapter 15 discusses various cyber physical systems management techniques. Most of
the systems are unsuccessful during integration due to insignificant consequences occurring in them.
This is due to lack of system scalability that fails to provide an improved workload of the system. This
chapter describes the parameters to be measured while evaluating the scalability of the structure. The
parameters to be measured are described in a scalability review that represents the problems in it. The
primary requirement of CPSs is system reliability because an unreliable system yields service interrup-
tion and financial cost. A CPS cannot be set up in critical applications in which system reliability and
predictability are inefficient. To provide safety critical systems, a high volume of data is dealt, containing
operator-in-loop and operating online constantly. The combined characteristics of physical and computa-
tional components allow CPSs to use hybrid dynamical models to integrate discrete and continuous
state variables that use computational tools to resolve composite problems.

As an intellectual challenge, CPS is about the intersection, not the union, of the physical and the
cyber. It is not adequate to individually understand the physical components and the computational
components. We must instead understand their interaction. The design of such systems, therefore,
requires understanding the joint dynamics of computers, software, networks, and physical processes. It is
this study of changing aspects that sets this discipline apart. This book will be of considerable interest
to researchers, professionals, and students with the backgrounds of computer science and electrical and
electronics communication.

P. Venkata Krishna
VIT University, India

V. Saritha
VIT University, India

H. P. Sultana
VIT University, India