Chapter 1

Introduction

Traditional electro-mechanical system, infrastructure, equipment, and facilities are gradually instrumented, controlled, automated, and administered through computerization and possibly internetworking and such arrangements are referred in the literature as Cyber-Physical Systems (CPSs) [78]. A CPS intertwines the computation and communication capabilities into physical systems to monitor and control the system functionalities and states to achieve a high degree of automation [25]. Most of the modern CPSs are distributed and asynchronous systems. These are the network-ready extensions of multi-level heterogeneous embedded systems with a large number of distributed sensors, actuators, and computing devices and can be shown as FIGURE 1.1.

These nodes execute different software modules or processes to perform real-time and non-real-time jobs to achieve a common goal. Thus, the weaving of cyber components with the physical system improves resource utilization, autonomy, scalability, performance, reliability, availability *etc.* A generalized cyber-physical system architecture [78] is presented in FIGURE 1.2. There are five levels: connection, conversion, cyber, cognitive, and configuration to design and support a CPS. The emerging CPS may range from small-scale industries to large-scale connected systems of diverse areas. They are becoming the backbone for managing critical infrastructures and systems such as civil, safety-critical, and defense. Some of the

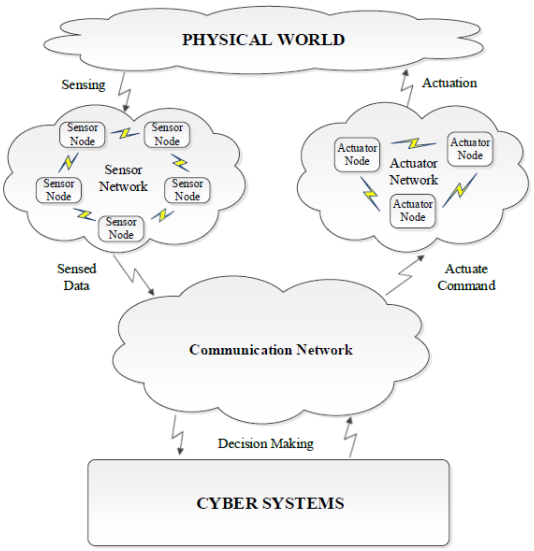

FIGURE 1.1: Holistic view of a CPS

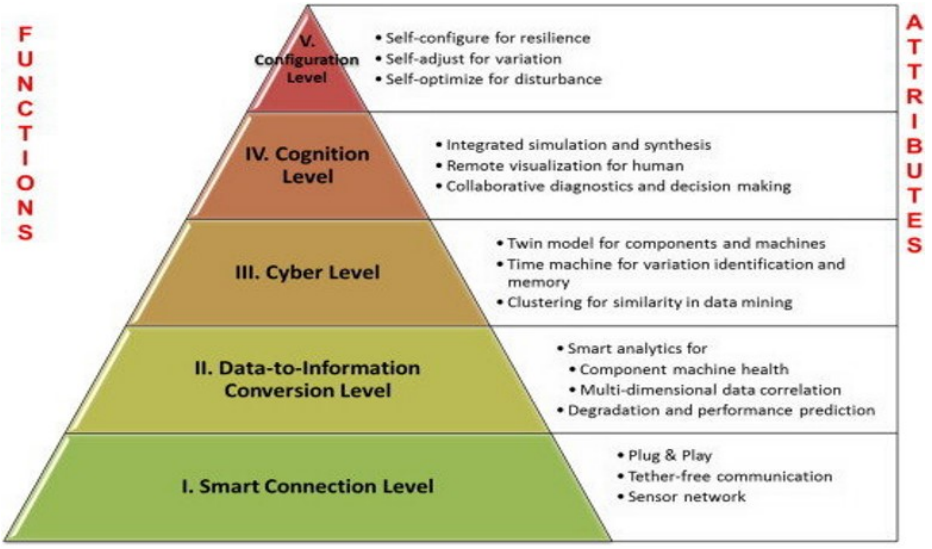

FIGURE 1.2: Major responsibilities of CPS architecture layers [78]

major application areas include medical and health care, intelligent transportation, Homes and buildings automation, agriculture, defense systems, power and thermal management, manufacturing, smart grid, social robotics, and data centers [95] [53] [24] [53][44] [78] [132] [135].

It is observed that the integration of cyber components with physical devices and infrastructures enhances the capabilities of traditional infrastructures, however, several issues and challenges are associated with these systems [95] [53] [78] [135]. Before we

come to the security modeling issues in this thesis, other pertinent issues are given as:

- Security
- Autonomy
- Reliability and availability
- Safety
- Coordination and consistency
- Heterogeneity and interoperability
- Modularity
- Flexibility and scalability

Security: Security is a property to protect the system from unauthorized access and disturbance. Interconnectivity of devices, systems & infrastructures and their possibilities of being network-ready, possibly including internet communication, has resulted in many considerations of security threats. The successful attacks may be a matter of security and safety concerns by disrupting the critical system's functionality or exfiltrating the sensitivity information. These security failures may result in severe damages ranging from affecting critical infrastructures to the loss of human lives. Hence, it is challenging to identify security requirements and assess the security policies while designing CPSs.

Autonomy: It refers to the system being self-aware and capable of making its own choices to deliver satisfactory performance while dealing with significant uncertainties. However, it is challenging to design the real-time system components that are aware of their own and other components states because of unreliable communication medium and heterogeneity.

Reliability: It is defined as probability of failure free operation during specified time under given conditions [15]. It is calculated as an exponentially decaying probability function that depends on failure rate $F(t)$.

$$R(t) = 1 - F(t) \tag{1.1}$$

Availability: It refers to the probability that the system is ready to deliver functionality when required.

$$Availability = \frac{MTBF}{MTBF + MDT} \tag{1.2}$$

where, $MTBF$ is mean time between failure or uptime, MDT is mean down time, $MTBF + MDT$ is total time.

Safety: It is the conditional probability that the system has survived the period during an exposure time interval without an accident, provided that it was functioning without catastrophic failure at start time [15] [76]. It ensures the absence of catastrophic consequences on users and the environment. Safety is related to reliability and can be derived using equation

$$unsafety = (1 - R(t)) * HL \tag{1.3}$$

where, HL is hazard level.

Coordination and consistency: CPS is generally organized as a distributed system. One of the main goals of distributed computing is to complete a task in a faster manner by combining the power of multiple machines. Here, multiple independent nodes work together, so coordination and consistency maintenance is inevitable to complete a task successfully. In a distributed system, nodes are independent and connected through links that may be unreliable. The nodes and links may fail and recover independently, and there is no shared memory concept. Hence, the nodes communicate and coordinate through messages passing, and the concept

of semaphore does not work to maintain consistency. The coordination and consistency maintenance is not straightforward in a distributed system. On the other hand, unpredictable communication delay also makes coordination and consistency maintenance more challenging.

Heterogeneity and interoperability: Heterogeneity and interoperability are crucial issues of CPS. CPS is a collection of heterogeneous components, where different kinds of hardware and software work together cooperatively to solve problems. There may be many different representations of data and different instructions sets in the system. Different nodes may follow different architecture and have different operating systems, programming languages, and communication media and protocols. Attempts to provide a universal canonical form of information to communicate and share the knowledge among them are challenging. So, interoperability among nodes is also difficult and challenging.

Modularity: As CPSs are generally large-scale systems; hence, to conquer the system design and management complexity, the system must be modular. Low coupling and high cohesive modules help in building software quickly and to localize the fault and to prevent the fault propagation. However, with increasing CPS size and complexity, there exist a lot of interdependencies among CPS components to perform different tasks, modularity preservation becomes quite challenging.

Scalability and Flexibility: Scalability refers to the ability to add or remove resources in the system on demand. Flexibility relates to the ease with which a component or system can be modified for specific situations or applications. As CPSs are expected to serve large users and respond smartly in emergencies, flexibility and reconfigurability are mandate qualities. However, it is challenging to monitor the state of the current group of subsystems and reason about potential changes to track down an optimal configuration with available resources. These challenges become more difficult to be handle in the presence of real-time constraints. Moreover, these configurations must be consistent in these distributed architectures.

As there is more and more dependence on computerized control of industry for *eg.* Industry 4.0, where vulnerability exploitation may compromise the CPS with severe impacts, this thesis is concerned with dealing with some of the challenges related to CPS security.

OUTLINE: The rest of this chapter is organized as follows. Section 1.1 defines the research goals and the problem statement of this thesis. In Section 1.2, we present the motivation of the thesis. The significant contributions of this work are presented in Section 1.3. Section 1.4 describes scope of research. Finally, Section 1.4 finishes the chapter by detailing the structure of this thesis.

1.1 Research Goal and Problem Statement

Identifying the CPS security needs and analyzing their impact on system in the early phases of the system development life cycle is one of the major concerns. Though many CPS security modeling methods have been introduced so far, there are still some research questions regarding security modeling.

RQ-1: How to model and analyze a CPS behavior in the presence of different threats, particularly for a safety-critical system?

RQ-2: How to model intrusion-disruption for assessing the impact of integration of preventive and responsive security measures? How to deal with uncertainty in model parameter estimation?

RQ-3: A CPS is generally a form of a distributed system. How to deal with logical separation between functionality and security arrangements in a distributed CPS infrastructures possibly through leaders for the two aspects?

In this thesis, we are interested in answering all these research questions regarding the modeling and organizing the distributed CPSs. The main objectives of this thesis are as follows.

- To study the strength and weakness of existing modeling techniques for CPS security modeling.
- To identify security requirements as specifications and apply security in the form of various constraints.
- Modeling and analysis of CPS security to assess the system behaviour in presence of threats, their mitigation and handling of uncertainty in model parameter estimation.
- To present an architectural arrangement to integrate functionality and security.

The problem statement in this thesis includes two parts-

(i) To consider and explore qualitative and quantitative modeling of a CPS, particularly a for a safety-critical system, considering security aspect and assessing the possible impact of security on availability.

(ii) To consider a moderately large distributed CPS, which may have arrangement similar to distributed systems, for the integration of security arrangements along with modules/components/subsystems responsible for delivery of functionality.

1.2 Motivation

The inclusion of cyber components makes the CPS sufficiently vulnerable to cyber threats generated in-house or launched by malicious external entities or actors [133]. For interoperability and remit operation by multiple processes and stakeholders, the system needs to facilitate external entities (hardware and software) to obtain extreme privileges to operate on resources and execute functionality. Moreover, the interconnectivity of devices, systems & infrastructures, and their possibilities of being network ready, possibly including internet communication, has resulted in very many considerations of security threats. These factors increase the security risks by

opening the doors for attackers by increasing the attack surfaces to compromise and attack the system by exploiting existing vulnerabilities that may arise due to inappropriate policy, inefficient and inaccurate protection mechanisms, and procedures.

Using different attack surfaces and attack vectors, the attacker may install and execute malicious payloads on any attack surfaces, including sensors and communication networks locally or remotely, to attack and compromise high-value targets. Nodes in the control center are usually less susceptible as they are deployed in a physically confined environment to prevent tampering. The network-level vulnerabilities (insecure communication channel, remote access to the enterprise network, or node spoofing) are comparatively easier to exploit by launching cyber attacks. In a system, cyber-attacks are the condition of misuse or abuse that violate the security goals and hinder the intended system functionalities or intentional system failure.

TABLE 1.1: Cyber Attacks on cyber physical systems

Year	**Attack Name**	**Description**
2000	Insider attack [95]	Maroochy water control system hacked and flooded the grounds of a hotel and a nearby river with a million litres of sewage in Australia
2003	SQL Slammer [81]	Intrusion into the private control network of Davis-Besse Nuclear power plant in Ohio by exploiting the zero-day vulnerability in Microsoft SQL Server. The malware generated massive traffic, which clogged the communication between corporate and control networks.
2010	Stuxnet [107]	Thousands of nuclear centrifuges were infected and damaged in Iranian Nuclear power plant.
2011	Night Dragon [95]	Unable to directly attack SCADA systems. However, the corporate network segments belonging to companies that operate SCADA infrastructures were attacked to exfiltrated data such as operational blueprints.
2011	Duqu [10]	Doqu is an information stealer rootkit targeting MS Windows based PCs in Europe.
2012	Flame [153]	Flame targeted the Iranian and middle east computer and control systems to infect and steal the information.
2012	Wiper [155]	Wiper targeted the Iranian oil companies, which overwrite or delete the hard drive contents.
2015	BlackEnergy3 malware	Coordinated attack on Ukrainian power grid results in blackout
2016	W32.Ramnit and Conficker malware [73]	Virus infected computer system and USB drives but unable to pose a direct threat on Gundremmingen nuclear power plant's operating system in Germany
2019	DTrack RAT [97]	Virus Intruded the administrative network on Kudankulam Nuclear power plant in India, although unable to pose any threat to control network

These may be active or passive. The active attacks are comparatively more dreadful for a CPS and disrupt critical assets' physical processes and operations.

Once the cyber attack or cyber warfare is initiated, strategically specific targets are attacked to paralyse the opponent. Critical infrastructures such as telecommunications, water facilities, control systems, finance, energy resources, and transportation are targeted that can seriously ruin a nation. Few well-known attacks are mentioned in table 1.1. From where it is observable, the safety-critical CPS are targeted significantly. However, as safety-criticality has become a critical non-functional concern in such systems, the primary focus is still on safety assurance. Hence, security often does not get proper attention. Any mistake or ignorance in security analysis may greatly amplify the risk of significant damages in the presence of cyber threats. The security failure may result in severe consequences that may range from affecting critical infrastructures and the economy to even loss of human lives. Hence, this is an emergent requirement that security is considered in modeling CPSs in general and safety-critical systems in particular. As a cyber-physical infrastructure involves multiple stakeholders, there is a need for a clear definition, design, and architecture of secure CPS at this early CPS development phase. In these complex and capital-intensive systems, addressing the security features during the requirement analysis and design phase produces a more dependable system at low cost and less effort. If the concern is an afterthought and the system development process has progressed substantially, the design changes become costlier. Hence, it is better to identify and uncover the possible vulnerabilities from the early phases of the system development life cycle. This requires quantitative modeling and analysis of the intended system in the design phase to prevent security and subsequent system failures.

We have performed a literature survey in the second chapter of this thesis. This literature survey helps us to identify the issues and research gaps associated with CPSs security concerns. Researchers in the past years have proposed a good number of modeling and analysis methods for CPSs security. However, there are still some issues and research gaps that need to be addressed. These issues and research gaps form the motivation of this thesis. The identified research gaps are as follows.

- During development, functionality has often taken priority over security. Security measures were implemented late as an add-on resulting in brittle designs that lack proper integration. There is an absence of integrated functionality and security modeling framework that analyses the stochastic behavior of the system in the presence of attacks and mitigation Most of the existing works study the effect of security threats and mitigations separately from functionality.

- Need a formal approach to analyze the combined effect of applying preventive and responsive defense measures to reduce intrusion attempts and consequent attacks to secure the SC-CPS and ensure its availability.

- Emergent need to provide a possible approach for consideration of separation of functionality and security concerns for CPSs, that are normally organized in distributed manner.

1.3 Contribution

This thesis is committed to the modelling and organizing the CPSs with security to resolve various research gaps of the existing methods to address security issues in CPSs. This section provides important contributions to the thesis, including the modeling, analysis, organization, and comparative analysis of the proposed methods for addressing security integration in CPSs. The significant contributions are:

- A brief study on the strengths and weaknesses of existing modeling techniques for modeling CPS security.

- We propose a design-time methodology to map and analyze the system security qualitatively and quantitatively using Stochastic Petri nets and their fundamental properties.

- As the cyber threats target the cyber-physical systems functionalities and their availability, we present a Generalized Stochastic Petri Net (GSPN) based approach to analyze the effect of integrating the intrusion prevention and responsive measures on system availability.
- After considering the system model and understanding developed at the modeling level, to improve the CPS performance, security, and functionality management, we propose a distributed multi-tier architectural model of CPS and the management of such a distributed infrastructure through the concept of aspect-orientation and leader(s) as available in case of distributed computing systems.

1.4 Scope of Research

1. The proposed methodologies in this thesis work are applicable to any CPS, and case studies have been focused only on safety-critical systems, including Nuclear Power plants (NPP) and smart hospital management systems.
2. All the proposed models are available in the form of an analytical expression to quantify associated parameters.
3. In case of CPSs, the wear, and tear-out of the chip in which software resides has not been considered.

1.5 Thesis Outline

Various research issues regarding CPS security modeling are identified throughout this research work. To address these issues, modeling and organization methods are proposed. This thesis contains six chapters. Chapter 1 is an introductory chapter. Chapter 2 presents the literature survey. For better understanding and clear view, the core work of this thesis (derived from our research papers) is presented in Chapter

3, Chapter 4, and Chapter 5. Finally, Chapter 6 summarizes the thesis. Figure 1.3 depicts the organization of this thesis. A brief description of every chapter in this thesis is as follows.

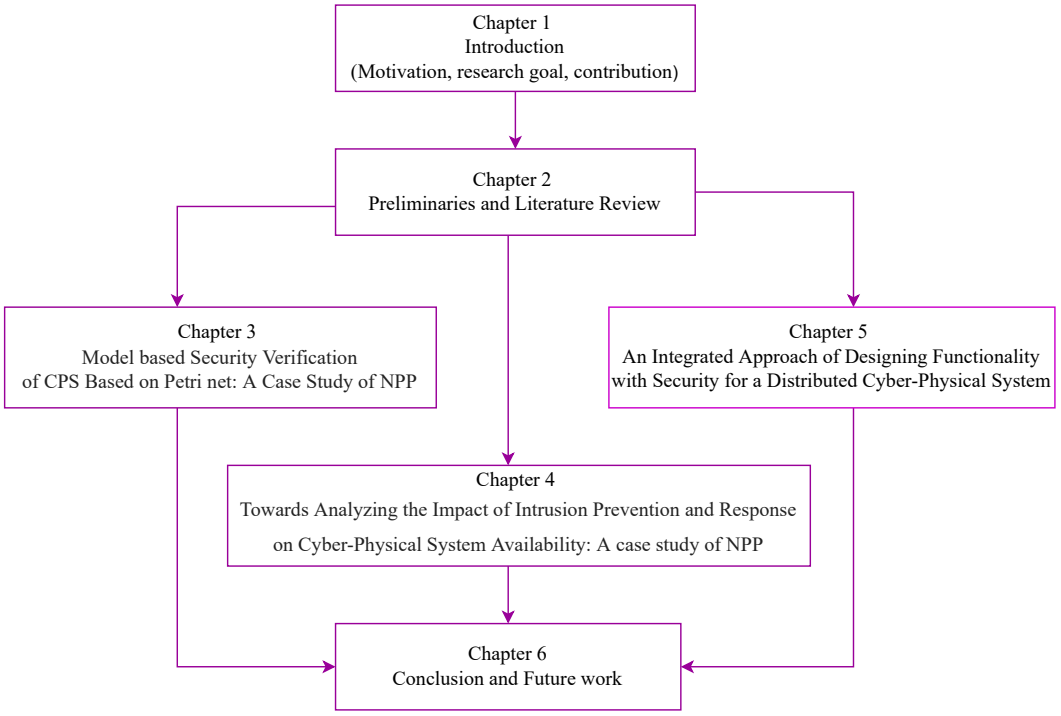

FIGURE 1.3: Thesis Structure

Chapter 1: This chapter briefly describes the CPSs and their importance. This chapter provides the motivations behind the thesis by explaining some research issues in the existing modeling and organization methods for CPS security. Further, it provides the research objectives and contributions. At the end of this chapter, we describe the thesis organization.

Chapter 2: This chapter first presents the preliminaries, including security concepts modeling approaches and the considered case study. Then it performs a literature survey related to the modeling and organization of distributed CPSs for security and identifies the issues and research gaps in the existing methods.

Chapter 3: The chapter provides a systematic approach to model and analyze the stochastic behavior of CPS in the presence of threats and possible mitigations in the early stages of system development. The approach qualitatively and quantitatively

analyses system security using SPN and its fundamental properties as standard evaluation metrics. The effectiveness of the proposed methodology is evaluated using a Nuclear power plant (NPP) case study [138].

Chapter 4: This chapter presents the intrusion-disruption model to show the attacker's behavior and its impact on the system's physical process and its availability. A GSPN based approach is presented to analyze the effect of combining the preventive and reactive measures against cyber-attacks and handling the state space explosion problem. By analyzing the model, system security is quantitatively estimated in terms of mean-time-to disrupt and system availability. We validate the combined effect of preventive and responsive measures on a case study of Nuclear power plant (NPP) [139].

Chapter 5: This chapter proposes a multi-tier architectural model of a cyber-physical system to improve the performance, maintainability, and security of a large-scale CPS. We introduce the concept of separately managing the functional and security concerns by electing the functional and security leaders to manage the CPS. Further, we propose a fault-tolerant leader election algorithm that can independently elect the functional and security leaders. For reducing the leader election overhead, the proposed election algorithm identifies a list of potential leader capable nodes and designates the highest potential node among them as the leader. After that, whenever the leader fails, another highest potential node in that list is instantly selected as the new leader. We also explain the proposed architecture and its management method through a case study. Further, we perform several experiments to evaluate the system performance [136].

Chapter 6: This chapter concludes the thesis by summarizing the main findings of the works done herein with possible future research directions.