Preface

The physical infrastructure, equipment, and facilities are gradually instrumented, controlled, automated, and administered through computerization and possibly internetworking. Such an arrangement is known in the literature as a Cyber-Physical System (CPS). The emerging CPS may range from small-scale industries to large-scale connected systems of diverse areas such as transportation, avionics, defense, entertainment, industrial control system, safety-critical systems, healthcare, *etc.* The cyber components monitor and control the real-world physical devices and infrastructures to improve the quality of services, including reliability and resource utilization.

However, the automation and connectivity of all the networked computing devices increase the security risks and leverage the opportunity to perform successful attacks to compromise system safety with catastrophic effects on human lives and the environment. The attackers compromise the system by exploiting existing vulnerabilities that arise due to inappropriate policies, facilitation to external entities, inefficient and inaccurate protection mechanisms and procedures. Several powerful attacks have been launched on critical infrastructures in recent years, resulting in substantial financial losses, productivity losses, and physical injuries. Protecting Industrial control systems (ICS) from cyber attacks is critical to a country's economic development and social stability. This is an emergent need that security is also considered in the modeling of CPS in general and safety-critical systems in particular. Through a detailed literature survey of existing modeling, analysis, and system organization methods, we find some significant issues and challenges. During development, functionality often takes priority over security. Security measures were implemented late as an add-on resulting in brittle designs that lack proper integration. Further, several techniques are proposed to perform the security analysis in

early phases of the system development life cycle. However, most of these present the qualitative assessment rather than quantitative assessment.

This thesis presents the security modeling and arrangement approaches to overcome these research gaps in the early phases. The first chapter proposes a design-time methodology to map and analyze the system security using Stochastic Petri Nets (SPN) and their fundamental properties. The presented theoretical framework exploits the power of SPN to model the stochastic nature of the system in the presence of external threats. It provides the mathematical support for structural and behavioral analysis to validate the effect of responsive mitigations against security vulnerabilities qualitatively and quantitatively. The effectiveness of the proposed methodology is shown through a case study of Nuclear Power Plant (NPP).

Deploying preventive or responsive measures alone may not be enough to detect, prevent and respond to intrusion attempts and subsequent sophisticated attacks. In the second chapter, we have extended the earlier work, where multiple intrusion prevention and response techniques are applied in place of responsive measures only, and their combined effect on system security and availability are analyzed quantitatively using Generalized Stochastic Petri Nets (GSPN). As SPN suffers from a state explosion problem, GSPN is used to deal with the problem. Moreover, the proposed model helps to prioritize the available security measures.

As CPSs are mostly distributed systems, it is interesting to consider a possible approach for the separation of functionality and security concerns for CPS that are usually organized and created in a distributed manner. In the third chapter, we propose a distributed multi-tier architectural model of CPS and its management as per aspect orientation and leader election as observable in distributed computing systems to improve the CPS performance, security, and functionality management.