CE4055 and CZ4055 – Cyber Physical System Security

Academic Year	AY1819	**Semester**	2				
Course Code	CE/CZ4055						
Course Title	Cyber Physical System Security						
Pre-requisites	CE/CZ1006 Computer Organisation And Architecture						
Pre-requisite for	NIL						
No of AUs	3						
Contact Hours	Lectures	26	TEL	-	Tutorials	12	Laboratories: 3

Course Aims

Cyber physical systems are typically designed as a network of interacting elements with physical input and output, and are characterized by the interaction between the physical world (sensors, user inputs, actuators) and the cyber world (processing, decision making). Cyber physical systems are the driving force behind modern civilization, being integral part of technologies, such as additive manufacturing, smartcard-based payment, power delivery systems, drone-based operations, and smart home automation. Cyber physical systems are characterized by stringent performance requirements, such as, extremely low energy budget, small area footprint and often hard real-time constraints. Due to the pervasive nature of the cyber physical systems in our everyday lives, it also runs the risk of huge security hazards.

In this course, we will learn about the basics of cyber physical systems, including the design principles and methodologies. Further, there will be a detailed treatment of the security challenges for cyber physical systems, which vary in practice due to the diverse nature of the application environment of cyber physical systems. These different forms of security breaches, observed across diverse cyber physical systems, will be put in a well-characterized taxonomy, to be systematically identified as attack surfaces. The techniques to handle these attacks will be described in a generic manner, including key management and wireless/RFID communication. The attack surfaces and protection/mitigation principles will then be elaborated with practical case studies, from the representative cyber physical systems such as automotive, smart card systems and smart grid.

Intended Learning Outcomes (ILO)

Upon the successful completion of this course, you shall be able to:

1. Describe the basic concepts of cryptography are used for ensuring security of cyber-physical systems
2. Describe the basic design, architecture and design principles of cyber physical systems
3. Identify the sources of vulnerability in a cyber physical system systematically via attack surfaces
4. Determine how security is incorporated at different abstractions and at different components of cyber physical systems

5. Articulate the principles behind the detection and mitigation of attacks for different attack surfaces of a cyber-physical system
6. Compare and contrast practical cyber physical system security such as for smart grid, smart vehicle, and smart card systems
7. Determine the performance overheads to consider for incorporating security in a cyber-physical system

CE4057 and CZ4057 – Time-Critical Computing

Academic Year	AY1819		**Semester**	1				
Course Code	CE/CZ4057							
Course Title	Time-Critical Computing							
Pre-requisites	CE/CZ1006 Computer Organisation And Architecture; CE/CZ2005 Operating Systems							
Pre-requisite for	NIL							
No of AUs	3							
Contact Hours	Lectures	26	TEL	-	Tutorials	13	Laboratories:	5

Course Aims

Cyber-Physical Systems (CPS) are a large-scale network of computing systems characterized by their interaction with the physical world (sensors and actuators). CPS are the driving force behind modern civilization, being an integral part of technologies such as avionics including drones, autonomous vehicles, etc. These systems generally have ***hard real-time constraints*** that require the cyber components to process physical inputs and generate appropriate physical outputs within pre-defined temporal requirements. For example, think about obstacle detection and avoidance in autonomous vehicles. Such systems, also called ***time-critical computing systems,*** are the primary focus of this course.

In this course, you will learn the fundamental concepts of a Real-Time Operating System (RTOS). RTOS is the core software platform used in time-critical computing, just like an OS in a general-purpose computing system. You will learn RTOS techniques for processor scheduling, process synchronization, etc. You will also learn how such time-critical computing platforms are networked together using protocols that support real-time communication. Building on this foundation, you will also learn how to implement a time-critical system using a drone-based platform.

Intended Learning Outcomes (ILO)

Upon successful completion, you should be able to:

1. Describe and analyze the three fundamental RTOs concepts: processor scheduling, process synchronization and process budgeting.
2. Describe and analyze the fundamental concepts of real-time communication: bounded latency, priority-based scheduling and Time-Division Multiple Access (TDMA).
3. Describe how these concepts are realized in practice, and discuss the associated implementation trade-offs.
4. Describe and analyze how these concepts affect the design of a CPS application in terms of satisfying its real-time requirements.
5. Design and implement a CPS application with real-time requirements, making efficient use of RTOS and real-time network features.