CYBER PHYSICAL SYSTEM SECURITY

Code: CS31222CS	Course Type: Elective	Semester: II
Evolution Scheme (TA-MSE-ESE): 20-30-100	Total Marks: 150	L-T-P (Credits): 3-0-0 (3)

Pre-Requisites: Computer Networks, Operating Systems, Control Systems, Cryptography, Embedded Systems, Programming (C/Python), Basic Knowledge of Distributed Systems.

Course Objective: To develop understanding of cyber-physical system security, threat models, defense mechanisms, and secure embedded system design for building resilient and trustworthy intelligent interconnected systems.

Course Outcomes: At the end of the course, the student will be able to

CO-1	Analyze the architecture, components, and threat landscape of cyber-physical systems
CO-2	Identify vulnerabilities and design secure CPS architectures with formal guarantees
CO-3	Implement security mechanisms for embedded, networked, and control-based systems
CO-4	Evaluate resilience, safety, and trustworthiness of CPS under adversarial conditions

Course Articulation Matrix:

PO	PEO-1	PEO-2	PEO-3	PEO-4	PEO-5
CO-1	3	2	2	-	-
CO-2	3	3	2	1	1
CO-3	3	3	3	2	2
CO-4	3	3	2	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Foundations of Cyber-Physical Systems

Introduction to CPS: architecture, components (sensors, actuators, controllers, communication networks), Modeling of CPS: hybrid systems, discrete-continuous interactions, Applications: smart grids, autonomous vehicles, industrial control systems (ICS), healthcare systems, Threat landscape: attack surfaces, adversary models, safety vs security interplay, Fundamental principles of CPS security and resilience.

Unit-2: Vulnerabilities and Attack Mechanisms in CPS

Attacks on sensing and actuation: spoofing, false data injection, replay attacks, Network-level attacks: DoS, man-in-the-middle, routing attacks in CPS networks, Control-layer attacks: stealthy attacks on control loops, zero-dynamics attacks, Hardware and embedded vulnerabilities: side-channel attacks, firmware attacks, Case studies: Stuxnet, Ukraine power grid attack, attacks on autonomous systems.

Unit-3: Security Mechanisms for CPS

Secure communication protocols for CPS and IoT systems, Cryptographic techniques: lightweight cryptography, key management in constrained devices, Authentication and access control in CPS environments, Intrusion detection and anomaly detection using machine learning, Secure state estimation and resilient control techniques, Blockchain integration for CPS security and trust management.

Unit-4: Resilience, Safety, and Emerging Trends

Fault tolerance and resilience in CPS under adversarial conditions, Formal methods for CPS security verification (model checking, theorem proving), Safety-critical system design and standards (IEC 62443, NIST CPS framework), Risk assessment and threat modeling methodologies, Privacy in CPS (data protection in smart environments), Emerging areas: digital twins, AI-driven CPS security, Edge/IoT security, Autonomous Systems Security.

Learning Resources:

Text Books:

1. Rajeev Alur, Principles of Cyber-Physical Systems, MIT Press
2. Al-Sakib Khan Pathan, Securing Cyber-Physical Systems, CRC Press

Reference Books:

1. Kim Zetter, Countdown to Zero Day (Stuxnet)
2. S. Sridhar, A. Hahn, M. Govindarasu, Cyber-Physical System Security for the Smart Grid
3. Dieter Gollmann, Computer Security, Wiley
4. Cardenas, Amin, Sastry – Research papers on CPS security