COURSE TITLE	**CYBER PHYSICAL SYSTEM**
COURSE CODE	**01CC0604**
COURSE CREDITS	**3**

Objective:

1 Students will be able to apply modeling and control techniques to represent and simulate cyber-physical systems using tools such as Simulink and Stateflow, analyze the interaction between sensing, computation, communication, and actuation in real-time systems to understand system behavior and dependencies, and evaluate design choices including communication protocols, timing constraints, and reliability trade-offs to develop efficient and robust cyber-physical system solutions.

Course Outcomes: After completion of this course, student will be able to:

1 Apply modeling techniques and computational tools to represent and simulate the behavior of cyber-physical systems.

2 Implement control strategies and real-time system concepts to manage interactions between physical and computational components.

3 Analyze system interactions, communication dependencies, and vulnerabilities in CPS environments to identify potential risks.

4 Evaluate CPS design choices, including safety, reliability, and security measures, based on application requirements.

5 Design and develop secure, efficient, and reliable cyber-physical system solutions for real-world applications.

Pre-requisite of course: Solid foundation in programming (e.g., C, C++, Python). Basic understanding of data structures and algorithms. Familiarity with fundamental concepts of control systems or dynamical systems (basic calculus and differential equations). Basic knowledge of computer networks.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Cyber Physical Systems** Definition and Characteristics of CPS, Distinction from Embedded Systems, IoT, and Sensor Networks, Key Concepts: Physical dynamics, sensing, actuation, computation, communication, feedback loops, Societal Impact and Challenges of CPS (Safety, Security, Privacy, Reliability, Usability), Examples of CPS across domains: Smart Grid, Autonomous Vehicles, Medical Devices, Industrial Control Systems (SCADA), Smart Buildings	6

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
2	**Modeling Physical Dynamics for CPS** Introduction to Modeling Physical Processes: State-space models, differential equations (brief review), Hybrid Systems: Modeling systems with interacting continuous and discrete dynamics, Modeling Techniques: Bond graphs, Simulink/Stateflow (introduction), Modeling Tools and Simulation Environments for CPS, Abstraction and Hybridization of Physical Systems	6
3	**Control and Real-Time Aspects in CPS** Introduction to Control Theory for CPS: Feedback control, stability, performance, Digital Control: Sampling, quantization, real-time constraints, Digital Control: Sampling, quantization, real-time constraints, CPS Control Design Considerations: Handling delays, uncertainties, and packet loss in networked control systems, and Validation of CPS Control Logic	6
4	**CPS Networking and Communication** Networking Requirements for CPS: Timeliness, reliability, safety-critical communication, Wireless Communication in CPS: Challenges (interference, range), protocols (e.g., Zigbee, Bluetooth Low Energy, WirelessHART), Wired Communication in CPS: Industrial Ethernet, Fieldbuses (e.g., Modbus, Profibus - concepts), Networked Control Systems (NCS): Architectures, challenges of communication constraints on control performance, Time Synchronization in Distributed CPS	8
5	**CPS Security, Safety, and Applications** CPS Security Threats: Attacks on sensors, actuators, control logic, communication networks (e.g., Stuxnet overview), Vulnerabilities at the Cyber-Physical Interface: Exploiting physical properties via cyber means, cyber effects on physical systems, CPS Security Mechanisms: Secure boot, secure communication protocols (adapted for CPS constraints), intrusion detection for CPS, CPS Safety: Hazard analysis, safety standards (overview), achieving safety in the presence of cyber threats, Case Studies of CPS Applications: Detailed look at the architecture, challenges, and security of selected real-world CPS	8
Total Hours		**34**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Simulating a Simple Physical System: Using a simulation tool (e.g., Python with SciPy, MATLAB/Simulink, OpenModelica) to model and simulate the dynamics of a basic physical system (e.g., a simple pendulum, a mass-spring-damper system).	2

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
2	**Practical 2** Implementing a Basic Digital Control Loop: Writing code on a microcontroller or in a simulation environment to implement a simple feedback control system (e.g., controlling an LED brightness based on a sensor input).	2
3	**Practical 3** Interfacing Sensors and Actuators: Connecting a sensor (e.g., temperature, light) and an actuator (e.g., LED, motor) to a microcontroller or single-board computer and writing code to read sensor data and control the actuator.	2
4	**Practical 4** Analyzing Network Traffic in a Simulated CPS: Using a network simulator (e.g., NS-3, Mininet) to set up a simple CPS network and analyze the characteristics of control or sensor data packets.	2
5	**Practical 5** Simulating a Denial-of-Service (DoS) Attack on a CPS Network: Introducing network congestion or delay in a simulated CPS environment and observing the impact on control performance (in a safe, simulated environment).	2
6	**Practical 6** Implementing Basic Authentication for a CPS Device: Adding a simple authentication mechanism (e.g., password or key-based) for accessing or sending commands to a simulated or real CPS component.	2
7	**Practical 7** Exploring a CPS Testbed (Virtual or Physical): Working with a pre-built virtual lab environment or a physical testbed to interact with and observe the behavior of a more complex CPS example (e.g., a simulated smart grid component, a robotic arm).	2
8	**Practical 8** Analyzing Data from a CPS: Processing and analyzing sensor data collected from a simulated or real CPS to identify anomalies or patterns.	2
9	**Practical 9** Investigating Security Vulnerabilities in a Simple CPS Model: Using a provided vulnerable CPS model (in a safe environment) to explore how cyber inputs can affect physical outputs or vice versa.	2
10	**Practical 10** Mini-Project: Designing a Basic Secure CPS Component: Designing and potentially implementing (in simulation or on hardware) a small CPS component that incorporates basic security considerations (e.g.,authenticated sensor data transmission, input validation for actuator commands).	2
Total Hours		**20**

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Textbook :

1 "Introduction to Embedded Systems: A Cyber-Physical Systems Approach, Edward A. Lee and Sanjit A. Seshia, LeeSeshia.org, 2011

References:

1 Cyber-Physical Systems: From Theory to Practice, Cyber-Physical Systems: From Theory to Practice, Raj Rajkumar, Insup Lee, Lui Sha, John Stankovic, CRC Press, 2016

2 Principles of Cyber-Physical Systems, Principles of Cyber-Physical Systems, Rajeev Alur, MIT Press, 2015

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	0.00	30.00	30.00	20.00	20.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 NPTEL Course: Foundations of Cyber Physical Systems

2 Coursera: Cyber-Physical Systems: Modeling and Simulation

3 Udacity: Cyber-Physical Systems Design & Analysis