PART - II (SEMESTER – III)

MCSC301: MINOR PROJECT [0-0-4]

MCSE301: CYBER PHYSICAL SYSTEMS [3-0-1]

Course Objectives:

Cyber-physical systems (CPS) have a utility in many safety-critical areas such as automotive, avionics, trains, healthcare, atomic energy, power, and industrial automation. CPS are composed of integrated physical systems that are either controlled by software or are strongly integrated. The objectives of this course are to introduce students to the modelling of CPS, and to develop the ability to analyze and simulate different CPS systems. The student will also learn to develop skills to help them plan, implement, and monitor cyber security mechanisms to protect information technology assets.

Course Learning Outcomes (CO):

At the end of this course, a student will be able to:

CO1: use the modeling software and related tools for the hybrid system.

CO2: to use comprehensive models of physical and cyber components to examine CPS.

CO3: to take up research work in multi-disciplinary areas keeping in mind the environment safety concerns

CO4: state the need and scope for cyber laws.

CO5: enumerate various network attacks, and describe their sources and mechanisms of prevention

Syllabus:

Unit I: Introduction and examples of cyber physical systems (CPS) in different domains, Important design aspects and quality attributes of CPS, Finite state machine, Characteristics of high confidence CPS, Discrete System Modelling, Continuous systems modelling, Extended state machines, Modelling of Hybrid systems, Various classes of Hybrid Systems, Analysis and Verification, Concepts of embedded systems, Input-outputs, Invariants and Temporal Logic, Linear Temporal Logic, Refinement and Equivalence, Model Development, Rechability Analysis and Model Checking

UNIT II: Cyberspace, Internet of things, Cyber Crimes, Cyber Security, Cyber Security Threats, Cyber laws and legislation, Law Enforcement Roles and Responses. Network Threat Vectors, MITM, OWAPS, ARP Spoofing, IP & MAC Spoofing, DNS Attacks, SYN Flooding attacks, UDP ping-pong and Fraggle attacks, TCP port scanning and reflection attacks, DoS, DDOS. Network Penetration Testing Threat assessment, Penetration testing tools, Penetration