INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

CYBER PHYICAL SYSTEMS								
II Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
BCSE30	**Elective**	3	-	-	3	40	60	100
Contact Classes:48	**Total Tutorials: Nil**	**Total Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: Computer organization and Architecture, Advanced algorithms, Cryptography								

I. COURSE OVERVIEW:

Cyber-physical systems, which consist of physical systems tightly integrated and/or controlled by software, are ubiquitous in many safety critical domains, including automotive, avionics, railways, healthcare, atomic energy, power, and industrial automation. The principles of design and implementation of cyber-physical systems are remarkably different from that of other embedded systems because of the tight integration of real valued and dense time real time systems with software based discrete automated control. The course aims to expose the student to real world problems in this domain and provide a walk through the design and validation problems for such systems. Applications for CPS research are far reaching and span medical devices, smart buildings, vehicle systems, and mobile computing. The application domain for this course will be cyber-physical vehicle systems though techniques are more broadly applicable. Current literature, techniques, theories, and methodologies will be reviewed and discussed.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The basic design, architecture and design principles of cyber physical systems.
II. The fundamental concepts of cryptography for ensuring security of cyber- physical systems
III. The sources of vulnerability in a cyber physical system systematically via attack surfaces.
IV. The various modeling formalisms for CPS, such as hybrid automata, state-space methods, etc.

III. COURSE OUTCOMES;

CO1 Analyze overall specifications of CPS and translate it to the different sub-systems design requirements.
CO2 Define embedded systems and cyber-physical systems (CPS) and give examples
CO3 Understand various modeling formalisms for CPS, such as hybrid automata, state-space methods, etc.
CO4 Apply modeling and associated tools for Hybrid system.
CO5 Analyze CPS by with holistic models of cyber and physical components.

IV. COURSE SYLLABUS:

MODULE – I: INTRODUCTION TO CYBER PHYCIAL SYSTEM (9)

Motivation and examples of CPS e.g. Energy, Medical and Transportation cyber physical systems; Key design drivers and quality attributes of CPS. Attributes of high confidence CPS.

MODULE – II: CYBER PHYSICAL SYSTEM DESIGN (9)

Continuous systems modeling; Discrete time system modeling; Finite state machine; Extended state machines; Hybrid system modeling; Classes of Hybrid Systems.

MODULE – III: ANALYSIS AND VERIFICATION (9)

Basic concepts of embedded systems; Embedded Processors; Input-outputs; Invariants and Temporal Logic; Linear Temporal Logic;

Equivalence and Refinement; Development of models from specifications; Reachability analysis and Model Checking.

MODULE - IV: CYBER PHYSICAL SYSTEM MODELLING (9)

Modeling experiments in continuous, discrete and hybrid system; Verification of model using different techniques; Sensitivity analysis of Models; Sensitivity analysis of Hybrid Models; Scheduling in embedded system.

MODULE – V: SECURITY IN CYBER PHYSICAL SYSTEMS (9)

Security issues of Industrial Control Systems; Integrity attacks on SCADA systems; Model based technique to detect integrity attacks on sensors; threat model and its effect on control scheme; countermeasure for detecting such attacks; watermarking scheme; Design of observers under sensor and actuator attacks; design of observer for distributed environment under different attacks; applications of swarms of UAVs; Control design with denial service attack; case studies

V. TEXT BOOKS:

1. R. Rajkumar, D. de. Niz and M. Klein, “Cyber Physical Systems”, Addision-Wesely, 2017.
2. E.A.Lee and S AShesia, (2018), “Embedded System Design: A Cyber-Physical Approach”, Second Edition, MIT Press.
3. A.Platzer, “Logical Foundations of Cyber Physical Systems”, Springer, 2017.

VI. REFERENCE BOOKS:

1. F. Pasqualetti, F. Dörfler and F. Bullo, “Attack Detection and Identification in Cyber-Physical Systems”, in IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, Nov. 2013.
2. H. Fawzi, P. Tabuada and S. Diggavi, “Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks”, in IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454-1467, June 2014.
3. Yilin Mo, RohanChabukswar and Bruno Sinopoli, “Detecting Integrity Attacks on SCADA Systems” in IEEE Transactions on Control System Technology, Vol. 22, No. 4, 2014.
4. F. Pasqualetti, F. Dörfler and F. Bullo, “Control Theoretic methods for Cyber Physical Security”, in IEEE Control System Magazine, pp. 110-127, Feb. 2015.

VII. WEB REFERENCES:

1. https://www.nist.gov/el/cyber-physical-systems
2. https://www.cs.cmu.edu/~aplatzer/course/fcps14/fcps14.pdf
3. https://www.eecs.umich.edu/courses/eecs571/lectures/lecture2-intro-of-CPS.pdf