REVISED SYLLABUS

Academic Year 2020-2021

Department of Electronics & Communication Engineering

School of Engineering and Technology

Central University of Rajasthan

NH-8 Jaipur- Ajmer Highway, Bandarsindri

Kishangarh -305802

District-Ajmer, Rajasthan

Website: www.curaj.ac.in

List of programs offered by the department

M.Tech in Cyber Physical System (CPS)
B.Tech in Electronics & Communication Engineering (ECE)

M.Tech CPS program:

(a) Program Objectives:

PO1. The main objective of this program is to train manpower who can understand both cyber system and physical system collectively and able to handle the challenges towards system security against possible system attacks.
PO2. To train students who are capable to design cyber components to meet the overall specifications of a unified system.
PO3. The program will develop ability among the students to design logical software-hardware architecture so that the overall objective from the system can be achieved.
PO4. To motivate students towards research in emerging areas and prepare them to solve realistic problems in Cyber Physical Systems.
PO5. To train young generations of the nation on emerging technologies and produce professionals, who can contribute in the growth of society and nation.
PO6. To produce professionals with high technical skills, research attitude and moral values for ever growing needs of Industry, academics and research organizations.
PO7. Develop ability among the students to understand the practical problems and contribute towards the implementations of the technical projects.

Course Learning Outcomes:

1. At the end of the program, the ability will be developed among the graduates so that they can understand the specific requirements of the CPS and utilize it into the different sub-systems design.
2. The program will develop capability among the graduates to co-design hardware-software architecture in distributed environment.
3. Graduates will be able to model overall CPS using hybrid system and other approaches and validate the model.
4. During the course, students will develop skills such as critical thinking and problem-solving approaches. They can utilize such skills to solve scientific problems and communicate technical ideas in a professional way.
5. With a focused one-year research leading to a thesis, students should be able to understand the "art" and "science" of research and should be capable enough to apply this training to newer/other fields and problems.

Scheme and Detail Syllabus

M.Tech in Cyber Physical System (w.e.f. 2020-21 and onward batches)

					Contact hours/ week		
Sem I					**L**	**T**	**P**
	Code	**Title of the course**	**Type of course**	**Credit**			
1	MTC511	Probability Theory and Distributions	Core 1	4	3	1	0
2	MTC512	Advance Computer Network	Core 2	4	3	1	0
3	MTC513	Internet of Things	Core 3	4	3	0	2
4	MTC514	Foundation of Embedded Systems	Core 4	4	3	0	2
5	--	Elective 1	Prog. Elective 1	4	3	1	0
6		AECC	Mandatory	2	2	0	0
7		*Fitness (Mandatory)*	*Fitness*	--	*0*	*0*	*0*
8		*Societal (Mandatory)*	*Societal*	--	*0*	*0*	*0*
		Total program credits		**22**			
Sem II							
1	MTC521	Cryptography and Network Security	Core 5	4	3	0	2
2	MTC522	Cyber Physical System	Core 6	4	3	0	2
3	MTC523	Cyber and Digital Forensic	Core 7	4	3	1	0
4	--	Elective 2	Prog. Elective 2	4	3	1	0
5	--	Elective 3	Open Elective 1	4	3	1	0
6		AECC	Mandatory	2	2	0	0
7		*Fitness (Mandatory)*	*Fitness*	--	*0*	*0*	*0*
8		*Societal (Mandatory)*	*Societal*	--	*0*	*0*	*0*
		Total program credits		**22**			
Sem III							
1	--	Elective 4 (Online mode NPTL/COURSERA)	Open Elective 2	4	4	0	0
2	MTC611	Dissertation – I	Core 9	24	0	0	24
		Total program credits		**28**			
Sem IV							
1	MTC621	Dissertation – II	Core 10	24	0	24	0
		Total program credits		**24**			

Student have to select elective from the department elective list (attached). Further, any elective subject offered by other departments of the University like Dept. of CSE, Dept. of CS and Dept. of DAS can be considered as elective for this programme subject to approval of Dean of the School.

Mapping Table showing relationship between core courses and POs

Sr. No.	Title of the course	Course Code	PO1	PO2	PO3	PO4	PO5	PO6	PO7
1	Probability Theory and Distributions	MTC511	●	●	✓	✓	✓	✓	●
2	Advance Computer Network	MTC512	●	●	●	✓	✓	✓	✓
3	Internet of Things	MTC513	●	●	●	●	●	✓	✓
4	Foundation of Embedded Systems	MTC514	●	●	●	●	✓	✓	✓
5	Cryptography and Network Security	MTC521	●	●	✓	●	✓	●	✓
6	Cyber Physical System	MTC522	●	●	●	●	✓	✓	✓
7	Cyber and Digital Forensic	MTC523	✓	✓	✓	●	●	●	✓
8	Dissertation – I	MTC611	✓	✓	✓	✓	✓	●	●
9	Dissertation – II	MTC621	✓	✓	✓	✓	✓	●	●

Detailed Structure of the Program

SEMESTER I: M.Tech in Cyber Physical System

MTC511: Probability Theory and Distributions

Course Outlines: This course focused on modern probability theory concepts and its applications for decision-making to solve daily life problems. The course is heavily oriented towards the formulation of mathematical concepts on probability and probability distributions and densities with practical applications.

Course Objectives:

1. To provide students with a formal treatment of probability theory.
2. To equip students with essential tools for statistical analyses.
3. To foster understanding through real-world statistical applications.

Course Outcomes:

At the end of the course students should be able to:

1. Develop problem-solving techniques needed to accurately calculate probabilities.
2. Apply problem-solving techniques to solving real-world events.
3. Apply selected probability distributions to solve problems.
4. Present the analysis of derived statistics to all audiences.

List of PO that the course covers: PO1, PO2, PO7.

Level: Mastery

Prerequisites: An undergraduate level course on mathematics and basic knowledge of probability theory.

Course Description:

Probability Theorem: Properties of probability, Conditional probability, Independence, Bayes theorem.

Discrete Distributions: Probability distribution functions and cumulative distribution functions.

Continuous Distributions: Probability density functions and cumulative distribution functions, joint and marginal probability density functions.

Mean and variance; moment -generating functions, Marginal and conditional probability distributions, Some specific discrete distributions.

Functions of Random Variables: Distribution function technique, Transformation technique,

Moment-generating function techniques.

Text/References:

1. DeGroot, Morris H., and Mark J. Schervish. Probability and Statistics. Addison-Wesley.
2. Feller, William. An Introduction to Probability Theory and Its Applications, Wiley.
3. Freund, W.J., Mathematical Statistics, Prentice-Hall.
4. Hoel, P.G., Mathematical Statistics, John Wiley & Sons.
5. Hogg, R.V., & Craig, A.T., Introduction to Mathematical Statistics, Prentice-Hall, Inc.
6. Mood, A.M., Graybill, F.A., Boes, D.C., Introduction to the Theory of Statistics, McGraw Hill.
7. Papoulis: Probability, Random Variables and Stochastic Processes, McGraw Hill.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTC512: Advanced Computer Networks

Course Outline: This is an advanced course which focuses on advance topics such as network design, performance issues and implementation issues in modern enterprises. In addition, this course also targets to give an overview of various modern forms of networks such as sensor networks, vehicular networks, under-water and body area networks.

Course objectives:

1. This course aims at delivering concepts related to introduction to networking components, their hardware, software stack and their implementation.
2. In addition, this course targets at discussing concepts related to network performance, evaluation, simulation at length with limitations of various techniques.
3. This course also focus on providing an overview of newer forms of computer networks such as sensor networks, vehicular networks, underwater and body area networks and their related protocols, performance issues and suitable usage with case-studies.
4. This course also aims at taking cases of enterprises for possible network design with respect to scale, applications, performance and capacity planning.

Course Outcomes:

1. At the end of this course students should be able to understand the TCP/IP software stack and its relation with layered architecture in the code.
2. In addition, students should be able to understand various network protocols, their open-source implementations, performance issues, and simulations.
3. Understanding various newer forms of networks with their features, limitations and related protocols.

4. Participants of this course should be able to understand cases of enterprises/organizations and should be able to design network diagram, capacity planning and addressing and devices needs.

List of PO that the course covers: PO1, PO2, PO3.

Level: Mastery

Prerequisites: An undergraduate level course on computer networks.
.

Course Description:

Introduction: Introduction to Layered architecture, Networking hardware and software stacks.

Network Performance: Network Simulation and Modelling, Performance issues in networks, Protocol case studies (e.g. HTTP, HTTPS, SSL, DHCP, DNS, Transport protocols and Routing protocols in wired and wireless networks and their performance).

Modern Networks: Mobile Networks, Sensor Networks, Vehicular Networks, Underwater Networks and Body Area networks and related performance issues. **Enterprise networks:** Enterprise network infrastructure planning and design. Capacity planning of servers and data centres.

Text/ References

1. Selected research papers for most of the topics.
2. Top-Down Network Design- Networking Technology, Author Priscilla Oppenheimer, Publisher- Pearson Education, 2010.
3. Computer Networking: A Top-Down Approach (6th Edition), J Kurose and KW Ross, Pearson, 2012.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTC513: Internet of Things (IoTs)

Course Outlines: Internet of Things (IoT) is presently a hot technology over the globe. Government, academia, and industry are involved in different aspects of research, implementation, and business with IoT. The Internet of Things (IoT) is a course about the new paradigm of objects interacting with

people, with information systems, and with other objects. The course will focus on creative thinking and hands-on project development.

Course Objectives:
The objective of this course is to impart necessary and practical knowledge of components of Internet of Things and develop skills required to build real-life IoT based projects.

Course Outcomes:
On successful completion of the course, the student will:

1. Understand the concepts of Internet of Things and its hardware and software components.
2. Interface I/O devices, sensors & communication modules.
3. Design IoT applications in different domain and be able to analyze their performance.
4. Implement basic IoT applications on real life IoT based projects

List of PO that the course covers: PO1, PO2, PO3, PO4, PO5.

Level: Mastery

Prerequisites: An undergraduate level course on Digital Electronics, C programming Language and Embedded Systems.

Course Description:

Unit I: Introduction to IoT
Brief History and evolution of IoT, Definition of IoT, Characteristics of IoT, Physical design of IoT, Logical design of IoT, Functional blocks of IoT. Communication models and APIs.

Unit II: IoT & Machine to Machine
Machine to Machine, Difference between IoT and M2M, Software define Network, SDN and NFV for IoTs.

Unit III: Challenges in IoT
IoT Services Platform: Functions and Requirements, Design challenges, Development challenges, Internet of Things Security and Privacy, Other challenges.

Unit IV: Developing IoTs
Introduction to Python and IoT tools, Developing applications through IoT tools, Developing sensor based application through IoT platform.

Unit V: Specific applications of IoT

IOT for Home automation, Smart Cities, Environment monitoring, IOT for financial inclusion, Logistics monitoring, IOT for rural empowerment, Industry applications, Health monitoring, Other IoT applications.

Text/References Books:

1. Vijay Madisetti, Arshdeep Bahga, Ïnternet of Things, "A Hands-on Approach", University Press.
2. Ammar Rayes and Samer Salam, "Internet of Things From Hype to Reality" (2nd Edition) Springer.
3. Dr. SRN Reddy, Rachit Thukral and Manasi Mishra, "Introduction to Internet of Things: A practical Approach", ETI Labs.
4. Pethuru Raj and Anupama C. Raman, "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", CRC Press.
5. Jeeva Jose, "Internet of Things", Khanna Publishing House, Delhi.
6. Adrian McEwen, "Designing the Internet of Things", Wiley.
7. Raj Kamal, "Internet of Things: Architecture and Design", McGraw Hill 7. Cuno Pfister, "Getting Started with the Internet of Things", O Reilly Media.
8. Jean-Philippe Vasseur, Adam Dunkels, Morgan Kuffmann, "Interconnecting Smart Objects with IP: The Next Internet" Elsevier.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

Lab 1: Internet of Things (IoTs) Lab

Course Outlines: This laboratory introduces practical aspects of internet of things (IoT) to the students which focused on the experimental implementation of ubiquitous IoT applications such as weather station, home automation, switching over internet, sensor networks etc. This Lab also introduces the concepts of single board computers, different sensors and cloud storage in order to address the applicability, and challenges associated with IoT.

Course Objectives:

1. To provide introduction to practical aspects of Internet of Things.
2. To equip students with essential tools to implement IoT for different application domain.
3. To foster understanding through real-world applications related to internet of things.

Course Outcomes:

At the end of the course students should be able to:

1. Implement different IoT application
2. Apply internet of Things concepts to solve real word problems and industrial problems.

List of PO that the course covers: PO1, PO2, PO3, PO4, PO5.
Level: Mastery

Prerequisites: An undergraduate level course on Digital Electronics, C programming Language and Embedded Systems.

List of Experiments

1. Familiarization with Raspberry Pi 4, operating system and input/output ports.
2. Introduction to programming for IoT application and input/output interfacing.
3. Write a program to interface LED and Buzzer interfacing. Extend this program to blink LED and tone generation.
4. Write a program to interface Push button and Digital sensor (IR/LDR). Extend this program to securely shutdown raspberry pi with a sound.
5. Write a program to read temperature and humidity using available sensors. Extend this program to continuously read the data for 5 minutes.
6. Write a program to communicate raspberry pi with cloud storage.
7. Write a program to interface relay and control the switching using internet.
8. Write a program to interface LCD to Raspberry Pi and display temperature and humidity readings on it.
9. Write a program to interface sensor to Raspberry Pi and log the data to online spreadsheet and plot the data.
10. Make a weather station using available sensor modules.
11. Write a program for home automation and control using available sensor modules.

Assessment Method: Viva and Experimental exam.

Any need for revision of existing rules: No

MTC514: Foundation of Embedded Systems

Course Outlines: This course introduces microcontroller and embedded systems to the students which focused on in-depth study of different microcontroller architecture, ARM and interfacing to different components covering daily life problems to industrial problems. The course is heavily oriented towards the programming and interfacing of different input/output devices to ARM microcontroller and their practical applications.

Prerequisites: An undergraduate level course on Digital Electronics and C programming Language.

Course Objectives:

1. To provide introduction to Microcontroller and Embedded Systems.
2. To equip students with essential tools for Embedded systems.
3. To foster understanding through real-world applications related to embedded systems.

Course Outcomes:

At the end of the course students should be able to:

1. Apply Embedded system concepts to solve real word problems.
2. Present solution to automated systems to make life easier.
3. Apply concepts of embedded systems and microcontroller to enhance existing systems.
4. Ability to develop concepts, logics towards solving a unknown problem in research and industry.

List of PO that the course covers: PO1, PO2, PO3, PO4.

Level: Mastery

Prerequisites: An undergraduate level course on Digital Electronics and C programming Language.

Course Contents:

Introduction to Embedded Systems: Embedded System, Microprocessor and Microcontroller, Microcontroller family, CISC, RISC and ARM, 8-bit and 32-bit microcontrollers.

The ARM Architecture: ARM Technology, Cortex Core, ARM Programming**,** ARM Architecture Set Architecture**,** Code optimization, Cortex-M3 Microcontroller, general pin configurations, I/O ports and pin, counters, timers, serial I/O, interrupts, physical systems.

ARM programming: C/C++ programming Language, Compiling and Programming, Data types, timer in C/C++, I/O programming in C/C++, logical operations, arithmetic operations, data conversion in C/C++, interrupts and serial communication in C.

ARM I/O Interfacing: LED, Switch, 7segment display, LED array, keyboard, buzzer interfacing, serial and USB communication, LCD, Graphical LCD, Touch LCD.

ARM Interfacing and Processing: Digital and Analog input-output, ADC and DAC interfacing, Different sensor interfacing such as temperature sensor, light sensor, ultrasound sensor, gas sensor, introduction to I2C, external memory interface, real time clock interfacing, introduction to digital calender (using RTC), Wireless communication: Bluetooth, WiFi, and Zigbee.

Mechanical system interfacing: Interfacing to relay, DC motor, Stepper Motor, servo motor, flex sensors, flexible skin, Application: Humanoid, Robotics and Art.

Embedded system for cyber physical systems: Cyber physical system and Embedded system, concept of SoC, single board computer, application of Embedded systems in cyber physical systems, Introduction to wireless sensor network and IoT.

Text/References Books:

1. Steve Furber, "ARM System-on-Chip Architecture" Addison-Wesley, 2000.
2. Yifeng Zhu, "Embedded Systems with ARM Cortex-M Microcontrollers in Assembly Language and C", 3rd Ed, E-Man Press LLC, 2017.
3. J.W. Valvano, "Embedded Microcomputer System: Real Time Interfacing", Brooks/Cole, 2000.
4. Jack Ganssle, "The Art of Designing Embedded Systems", Newness, 1999.
5. V.K. Madisetti, "VLSI Digital Signal Processing", IEEE Press (NY, USA), 1995.
6. David Simon, "An Embedded Software Primer", Addison Wesley, 2000.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

Lab 2: Embedded System Lab

Course Outlines: This course introduces microcontroller and embedded systems to the students which focused on in-depth study of different microcontroller architecture, ARM and interfacing to different components covering daily life problems to industrial problems. The course is heavily oriented towards the programming and interfacing of different input/output devices to ARM microcontroller and their practical applications.

Course Objectives:

1. To provide practical experience to use embedded systems.
2. To equip students with essential tools for embedded systems and microcontrollers.
3. To foster understanding through real-world applications related to embedded systems.

Course Outcomes: At the end of the course students should be able to:

1. Solve real-world problems by applying embedded system concepts.
2. Practically implement embedded systems using microcontrollers and interfacing with the IO modules.
3. Ability to develop concepts, logics towards solving problem in industry and research.

List of PO that the course covers: PO1, PO2, PO3, PO4.

Level: Mastery

Prerequisites: An undergraduate level course on Digital Electronics and C programming Language.

List of Experiments:

1. Familiarity to ARM Cortex and trainer kit.
2. ARM Cortex C programming, hex generation and programming.
3. ARM Cortex timer and LED blinking and input port.
4. ARM Cortex interfacing to LED, LED array and 7 segment display.
5. ARM Cortex interfacing to 16 X 2 LCD and graphic LCD.
6. ARM Cortex interfacing to 4 X 4 keypad and keyboard.
7. ARM Cortex Serial and USB Communication and interrupts.
8. Interfacing to ADC and DAC.
9. Interfacing to LDR and Temperature Sensor.
10. Interfacing to External Memory and Real time clock (RTC).
11. Interfacing to DC motor and Stepper Motor.

Assessment Method: Viva and Experimental exam.

Any need for revision of existing rules: No

Programme Elective – I (Elective 1)	Any course from the list of department electives. Further, any elective subject offered by other departments of the University like Dept. of CSE, Dept. of CS and Dept. of DSA can be considered as elective for this programme subject to approval of Dean of the School.

SEMESTER II: M.Tech in Cyber Physical System

MTC521: Cryptography and Network Security

Course Outlines: This course deals with the underlying principles of cryptography and network security, and discusses both their theoretical foundations and practical applications.

Course objectives:

The course is designed to train the graduates in:

1. In depth understanding of network security.

2. In depth understanding of the Cryptographic Techniques.
3. To apply cryptographic techniques in computer systems.
4. To design new or modify existing cryptographic techniques.
5. To work in research institutions / Industry in the field of Security.

Course Outcomes:

Graduates after completing the course shall gain:

1. Ability to understand concepts of network security and cryptographic techniques.
2. Ability to design and analyze cryptographic techniques.
3. Ability to solve network security issues in real time applications.
4. Ability to take up doctoral level research work in security.

List of PO that the course covers: PO1, PO2, PO4.

Level: Mastery

Prerequisites: Basic knowledge of Discrete Structures and Algorithms.

Course Description:

Cryptography: Introduction, steganography, Public versus private key cryptography.
Stream Ciphers: Conventional Ciphers, playfair, Hill, mono-alphabetic and poly-alphabetic.
Private-key cryptography: Feistel structure, DES, design of S-boxes, AES, Triple DES, Differential and linear cryptanalysis.
Public key cryptography: Key management, Diffie-Hellman, ElGamal, RSA. Random Number Generation, Primality testing, Elliptic Curves and ECC.
Digital Signature: DSA and its variants, discrete logarithm based digital signatures.
Network Security: Authentication and signature protocols; Kerberos, real-time communication security, IPSec: AH, ESP, IKE; SSL/TLS, e-mail security, PEM and S/MIME, PGP, web security, network management security, wireless security. Threats in networks, firewalls, intrusion detection, Honeypots, password management.

Text/References:

1. D.R. Stinson, Cryptography - Theory and practice, CRC Press.
2. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Applied Cryptography, CRC Press.
3. Stallings, Cryptography and Network Security, Pearson Education.
4. B Schneier, Applied Cryptography, Wiley. ISBN 0-471-11709-9
5. C. Kaufman, R. Perlman, Network Security, Prentice Hall.
6. https://nptel.ac.in/courses/106105162/
7. https://nptel.ac.in/courses/106105031/13

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

Lab 3: Cryptographic Lab

Course Outlines: This is a lab course in cryptography. This course will provide practical knowledge about cryptography and network security to the students.

Course Objectives:

1. In depth understanding of network security.
2. In depth understanding of the Cryptographic Techniques.
3. To apply cryptographic techniques in computer systems.
4. To implement existing mechanisms and study their behavior, functioning and performance.
5. To design new or modify existing cryptographic techniques.

Course Outcomes: At the end of the course students should be able to:

1. Ability to understand concepts of network security and cryptographic techniques.
2. Apply security principles to system design.

List of PO that the course covers: PO1, PO2, PO4.

Level: Mastery

Prerequisites: Basic knowledge of Discrete Structures and Algorithms.

List of Experiments

Implementation of following mechanism in C/C++/Java.

1. Write a program to implement Caesar Cipher.
2. Write a program to implement Monoalphabetic Cipher.
3. Write a program to implement Polyalphabetic Cipher.
4. Write a program to implement Hill Cipher.
5. Write a program to implement Rail Fence Technique.
6. Write a program to implement Rotor Machines.
7. Write a program to implement S-DES.
8. Write a program to implement DES.
9. Write a program to implement AES-128.
10. Write a program to implement Diffie Hellman Key exchange.

11. Write a program to implement RSA public key algorithm.
12. Write a program to implement ECC (Elliptic Curve Crypto) Diffie Hellman.
13. Write a program to implement RSA Digital Signature.
14. Write a program to implement DSS Digital Signature.
15. Write a program to implement Hash and MAC Algorithm.

Assessment Method: Viva and Experimental exam.
Any need for revision of existing rules: No

MTC522: Cyber Physical System

Course Outlines: This course introduces cyber physical system to the students which focused on different ubiquitous applications we interact in our day to day life ranging from simple system to mission critical applications. Such ubiquitous physical systems are controlled or integrated with the software to provide crucial functionality to various applications such as railway, avionics, automobile, healthcare, industrial, power or nuclear automation. Due to complicated interaction/integration with the real time systems and critical data processing makes cyber physical systems different from the embedded systems. This course aims to expose the student to cyber physical systems and provide a walk through the fundamentals, design and validation using real world examples.

Course Objectives:

1. To provide introduction to Microcontroller and Embedded Systems.
2. To equip students with essential tools for Embedded systems.
3. To foster understanding through real-world applications related to embedded systems.

Course Outcomes:

At the end of the course students should be able to:

1. Apply Embedded system concepts to solve real word problems.
2. Present solution to automated systems to make life easier.
3. Apply concepts of embedded systems and microcontroller to enhance existing systems.
4. Ability to develop concepts, logics towards solving a unknown problem in research and industry.

List of PO that the course covers: PO1, PO2, PO3, PO4.

Level: Mastery

Prerequisites: An undergraduate level course on Digital Electronics, C programming Language and Embedded Systems.

Course Description:

Introduction: Cyber-Physical System, Key Features of CPS, Application Domains of CPS, Basic principles of design and validation of CPS, Challenges in CPS.

CPS Platform components: CPS HW platforms, Processors, Sensors and Actuators, CPS Network - Wireless, CAN, Automotive Ethernet, Scheduling Real Time CPS tasks, Synchronous Model and Asynchronous Model.

Synchronous and Asynchronous Model: Reactive Components, Components Properties, Components Composing, Synchronous Designs and Circuits, Asynchronous Processes and operations, Design Primitives in Asynchronous Process, Coordination Protocols in Asynchronous Process, Leader Election, Reliable Transmission.

Security of Cyber-Physical Systems: Introduction to CPS Securities, Basic Techniques in CPS Securities, Cyber Security Requirements, Attack Model and Countermeasures, Ddvanced Techniques in CPS Securities.

CPS Application: Health care and Medical Cyber-Physical Systems, Smart grid and Energy Cyber-Physical Systems, WSN based Cyber-Physical Systems, Smart Cities.

Text/References Books:

1. E. A. Lee and S. A. Seshia, "Introduction to Embedded Systems: A Cyber-Physical Systems Approach", 2011.
2. R. Alur, "Principles of Cyber-Physical Systems," MIT Press, 2015.
3. Raj Rajkumar, Dionisio de Niz and Mark Klein, "Cyber-Physical Systems", Addison-Wesley, 2017
4. Rajeev Alur, "Principles of Cyber-Physical Systems", MIT Press, 2015
5. Fei Hu, "Cyber-Physical Systems", CRC Press 2013

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

Lab 4: Cyber Physical System Lab

Course Outlines: This laboratory introduces practical aspects of cyber physical system to the students which focused on the experimental implementation of ubiquitous applications such as traffic light in smart cities, robotics, drones and industries. Due to complicated interaction/integration with the real time systems and critical data processing in the CPS, different algorithms are implemented in this lab to address the challenges associated with CPS.

Course Objectives:

1. To provide introduction to practical aspects of cyber physical systems.
2. To equip students with essential tools to implement CPS for different application domain.
3. To foster understanding through real-world applications related to cyber physical systems.

Course Outcomes: At the end of the course students should be able to:

1. Apply CPS to implement different CPS application models.
2. Apply cyber physical system concepts to solve real word problems.

List of PO that the course covers: PO1, PO2, PO3, PO4.

Level: Mastery

Prerequisites: An undergraduate level course on Digital Electronics, C programming Language and Embedded Systems.

List of Experiments

1. Familiarity to Embedded and robot platform.
2. Familiarity to Embedded C and hardware interfacing.
3. Implementation of Moore Machine using Traffic Light Controller.
4. Implementation of Mealy Machine using rocket controller.
5. Implementation of line robot.
6. Write a program in MATLAB to implement open loop system stability.
7. Write a program in MATLAB to implement timed automation.
8. Write a program in MATLAB to implement conveyor belt automation.
9. Write a program in MATLAB to implement PID controllers for drones.
10. Implement a machine learning algorithm for an autonomous robotics (CPS).
11. Study the machine learning in smart grids and monitoring.

Assessment Method: Viva and Experimental exam.

Any need for revision of existing rules: No

MTC523: Cyber and Digital Forensic

Course Outline: This course will cover the fundamentals of computer forensics and investigations. Topics will include historical and current digital forensic and investigative security issues; a systematic

approach to computer investigations; digital forensics, email and image file analysis, and guidelines for investigation reporting.

Course Objectives: This course aims to

1) Understand the principles of criminal laws related to computer related crimes, elements of cyber-terrorism and process of computer forensics.
2) Understand various aspects of cyber-crime such as motivation, investigation, cyber-crime and defense mechanisms.
3) Understand the various stages of forensics investigation with a focus on evidence identification and collection.

Course Outcomes: After completing students will be able to:

1) Realize the cyber-crimes, their nature, possible places of forensic artifacts, their secure collection, reporting and presentation in the court of law, and detection of fabrication and distortion of information.
2) Understand the various computer forensics practices involved at various practical stages of forensic investigation.
3) Understand the concepts related to attacks, their countermeasures, ethical issues and policies.

List of PO that the course covers: PO4, PO5, PO6.

Level: Mastery

Prerequisites: There are no specified course prerequisites, prospective students are advised that this is a technology-based course that focused on collecting security data and digital evidence.

Course Description:

Module 1: Introduction and overview

Introduction to Cyber and digital Forensics, Understanding the need for digital forensics; Defining digital forensics, number systems in forensic: binary, decimal and HEX, ASCII and unicode; computer hardware, Understanding computer components, Digital Media, hard disk basics, GREP.

Module 2: Forensic tools

Brief overview of forensic toolkit (FTK), various forensic tools: General, specialist and case management purpose tool, Forensic Software and Hardware: Disk Imaging, Forensic Software and hardware tools, hardware write/blocker, hard drive acquisition, Processing the scene, Forensic based operating systems, Debian-based, Ubuntu-based and Gentoo-based.

Module 3: Files and File Systems

Windows file systems, File system analysis, various file system categories, Application level search techniques, specific file systems, FAT concept and analysis, The big pictures, FAT data structure, Boot structure, Directory entries, FAT32, NTFS concepts, MFT, Forensic file images.

Module 4: Cybercrime and forensic report
Cyber-terrorism, principles of criminal law, computer forensic investigation, elements of personnel security and investigations, principles of risk and security management, conspiracy in computer crime, and computer fraud investigation; Cybercrime in defence, Forensic report: creating forensic report, proper report writing; Email analysis, POP and MAP; File signature analysis, File signature and extension; Hash analysis: Hashing of files and libraries.

Text/References:

1. Albert J. Marcella, Fred Guillossou, Cyber Forensics (From Data to Digital Evidence)
2. Dorothy E. Denning: Information Warfare and Security, Addison Wesley.
3. Daniel Ventre: Information Warfare, Wiley.
4. Winn Schwartau: Information Warfare: Second Edition, Thunder's Mouth Press, NY.
5. Edward Waltz: Information Warfare Principles and Operations, Artech House.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

Programme Elective – II (Elective 2)	Any course from the list of department electives. Further, any elective subject offered by other departments of the University like Dept. of CSE, Dept. of CS and Dept. of DSA can be considered as elective for this programme subject to approval of Dean of the School.
Open Elective – I (Elective 3)	

SEMESTER III: M.Tech in Cyber Physical System

Open Elective – II (Elective 4)	The student is required to take course outside the department or any course offered by SWAYAM/COURSERA/NPTEL can be considered as a course on the same discipline as replacement or as elective, subject to permission of Dean of the School.

MTC611: Dissertation – I	

This is the first part of the major dissertation wherein every student shall be expected to contribute to domain knowledge incrementally. It is expected that the work should be focused in a particular area for concept, design, implementation and analysis.

SEMESTER IV: M.Tech in Cyber Physical System

MTC621: Dissertation – II	

This will be culmination of dissertation – I of semester – III. In this (Stage-II), the evaluation shall be done through an Open seminar with an external examiner. Thesis shall be submitted with abstract. The school should work to standardize the thesis template for uniform submissions.

Assessment of dissertation I and II:

In 3rd and 4th semester each, there will be two types of evaluation internal evaluation and external evaluation with equal weightage. Internal evaluation will be done by the concerned supervisor every month and marks have to be submitted to the Dean.

External evaluation will be done by the two examiners (one external and one internal, other than supervisor). This evaluation will be done at the end of every semester.

List of Departmental Electives

Following list has to be used for offering department Elective. Additional Elective can be added as and when required after taking departmental approval.

Course Code	Programme / Open Elective (s)
MTE601	Wireless Sensor Networks
MTE602	Cloud Computing
MTE603	Information Retrieval
MTE604	Ad-Hoc Networks
MTE605	Biometric Security
MTE606	Data Mining
MTE607	Computational Number Theory
MTE608	Machine Learning
MTE609	Design of Electromechanical Systems
MTE610	Computer Vision
MTE611	Formal Methods in CPC & Automation
MTE612	Cryptanalysis
MTE613	Ethical Hacking
MTE614	Internet Security & Privacy
MTE615	Advanced Real-Time Systems

Detailed Syllabus of Electives (Program / Open Elective)

MTE601 Wireless Sensor Networks

Course Outlines: This course deals with the comprehensive knowledge about wireless sensor networks. The course will cover different layers used in WSN and their design considerations. Topics will include sensor network architectures, hardware platforms, physical layer techniques, medium access control, routing, topology control, WSN applications and other advanced topics.

Course Objectives:

1. To teach state of art of wireless sensor networks and its application to real time scenario.
2. To discuss importance of communication protocols and study various protocols at different layers.
3. To teach challenges in routing protocol and overview of transport layer protocols.
4. Give introduction to the operating protocols used in the WSNs.

Course Outcomes:
After complete this course, students should be able to list various applications of wireless sensor networks, describe the concepts, protocols, and differences underlying the design, implementation, and use of wireless sensor networks. Also implement and evaluate new ideas for solving wireless sensor network design issues.

List of PO that the course covers: PO1, PO2, PO3, PO5, PO6.

Level: Mastery

Prerequisites: An undergraduate level course on wireless communication.

Course Description:

Unit I: Introduction
Overview of Wireless Sensor Networks – Characteristics, Applications, Design objectives, challenges. Technological Background – MEMS Technology, Hardware and Software Platforms, Wireless Sensor Network Standards. Sensor network architectures and protocol stack.

Unit II: Medium Access Control
Fundamental MAC protocols, Objectives of MAC design, Energy efficiency in MAC design, MAC protocols for wireless sensor networks – Contention based protocols, Contention free protocols, Hybrid protocols.

Unit III: Network and Transport Layer
Fundamentals and Challenges of Routing protocol, Overview of Routing protocols: Location-aided protocols, Layered and In-network processing-based protocols, Data centric and multipath Protocols. Data aggregation mechanisms. Traditional transport protocols, Transport protocols for sensor

networks.

Unit IV: Operating Systems for WSN
Operating System Design Issues, Examples of Operating Systems- TinyOS, Mate, MagnetOS, MANTIS, OSPM, EYES OS, SenOS, EMERALDS, PicOS.

Unit V: Applications of WSN
WSN Applications - Home Control - Building Automation - Industrial Automation - Medical Applications - Reconfigurable Sensor Networks - Highway Monitoring - Military Applications - Civil and Environmental Engineering Applications - Wildfire Instrumentation - Habitat Monitoring - Nanoscopic Sensor Applications WSN Applications: Structural Health Monitoring, Traffic Control, Health Care.

Text/References Books:

1. Jun Zheng and Abbas Jamalipour, "Wireless sensor networks - A networking perspective", WILEY, 2009.
2. Kazem Sohraby, Daniel Minoli, & Taieb Znati, "Wireless Sensor Networks-Technology, Protocols, And Applications", John Wiley, 2007.
3. Holger Karl and Andreas Willig, "Protocols and Architectures for Wireless Sensor Networks", John Wiley & Sons, Ltd, 2005.
4. Waltenegus Dargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks-Theory and Practice", WILEY, 2010.
5. Thomas Haenselmann, "Wireless Sensor Networks: Design Principles for Scattered Systems", Oldenbourg Verlag, 2011.
6. E. H. Callaway, Jr. E. H. Callaway, "Wireless Sensor Networks Architecture and Protocols", CRC Press.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE602: Cloud Computing

Course Outline: The course on Cloud Computing will enable the students to understand the aspects of this emerging and growing computing paradigm with various ingredients such as cloud computing service models, virtualization technology, and practical aspects such as security and implementation issues.

Objectives:

1. To learn the fundamentals of cloud computing, its architecture, and various service levels.

2. To understand the formal model of virtualization and various virtualization techniques.
3. To equip students with cloud application frameworks, auto-scaling and resource allocation strategies and related open issues.
4. To understand the state-of-the-art cloud security issues and solutions in cloud computing.

Outcomes:

1. At the end of this course, students should be able to understand, design and configure various cloud services at the level of infrastructure, software, and platform.
2. With the help of a strong lab component, students should be able to setup cloud infrastructures using software such as OpenStack or Eucalyptus.
3. Understanding of cloud security and dependencies on CSP and possible solutions.
4. Cloud adoption decision making for different case studies and understanding of SLAs.

List of PO that the course covers: PO1, PO2, PO5.

Level: Mastery

Prerequisites: An undergraduate level course on Computer Networks and Operating System.

Course Description:

Introduction: Introduction to various computing paradigms, cluster computing, grid computing, autonomic computing, introduction to cloud Computing, various layers of cloud computing services (Software, Infrastructure, and Platform), cloud architecture, challenges and risks.

Virtualization: Formal model of virtualization, virtual machine monitors (Xen, VirtualBox, VMware etc.), virtual appliances, VM provisioning, Cloning and Snapshots, VM Backup and Recovery, VM migration, and Inter-operability Issues.

Cloud Computing Services: IaaS, PaaS and SaaS services and case studies (OpenStack, GFS, MapReduce, BigTable etc.). Application Migration to Cloud, Auto-scaling and on-demand resource allocation schemes, Cloud Service Level Agreement (SLA), SLA monitoring, accounting and verification, data center automation and containers.

Cloud Security: Cloud Security Challenges and Risks, Data Security, Application Security, Virtual Machine Security, Cross-VM attacks, Identity Management and Access Control, Establishing Trusted Cloud computing, Cloud Storage security, deduplication and Disaster Recovery in Clouds.

Text/ References

1. Hwang, Kai, Jack Dongarra, and Geoffrey C. Fox. Distributed and cloud computing: from parallel processing to the internet of things. Morgan Kaufmann, 2013.
2. Cloud Computing Bible, Barrie Sosinsky, Wiley-India, 2010.
3. Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds. Cloud computing:

Principles and paradigms. Vol. 87. John Wiley & Sons, 2010.
4. Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.
5. Various survey and research papers.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE603: Information Retrieval System

Course Outline:

Information retrieval is the process through which a computer system can respond to a user's query for text-based information on a specific topic. IR was one of the first and remains one of the most important problems in the domain of natural language processing. Web search is the application of information retrieval techniques to the largest corpus of text anywhere. The course focuses on IR methods for the processing, indexing, querying, organization, and classification of textual documents, including hypertext documents available on the world-wide-web.

Objectives:

1. To provide the foundation knowledge in information retrieval.
2. To present scientific support in the field of information search and retrieval.
3. Demonstrate the usage of different data/file structures in building computational search engines.
4. Students will be able to learn different indexing techniques to apply database systems.

Learning Outcomes:

After the completion of the course, the students will be able to

1. Understand basic concepts and techniques in Information Retrieval.
2. Understand how statistical models of text can be used for other IR applications, for example, clustering.
3. Use data structures and indexing methods in information retrieval systems.
4. Understand the measures to evaluate the performance of algorithms.

List of PO that the course covers: PO1, PO2, PO6.

Level: Mastery

Prerequisites:

1. Students must know Data Base Management Systems.

2. They must also have the concept of different types of algorithms used for searching data.
3. They must also have minimal knowledge of natural language such as thesaurus, synonyms, etc.

Course Description:

Unit I: Introduction

Definition, Objectives, Functional Overview, Relationship to DBMS, Digital libraries and Data Warehouses, Information Retrieval System Capabilities - Search, Browse.

Unit II: Cataloging and Indexing

Objectives, Indexing Process, Automatic Indexing, Information Extraction, Data Structures: Introduction, Stemming Algorithms, Inverted file structures, N-gram data structure, PAT data structure, Signature file structure, Hypertext data structure, Automatic Indexing: Classes of automatic indexing, Statistical indexing, Natural language, Concept indexing, Hypertext linkages.

Unit III: Document and Term Clustering

Introduction, Thesaurus generation, Item clustering, Hierarchy of clusters – User Search Techniques: Search statements and binding, Similarity measures and ranking, Relevance feedback, Selective dissemination of information search, weighted searches of Boolean systems, Searching the Internet and hypertext -Information Visualization: Introduction, Cognition and perception, Information visualization technologies.

Unit IV: Text Search Algorithms

Introduction, Software text search algorithms, Hardware text search systems. Information System Evaluation: Introduction, Measures used in system evaluation, Measurement example-TREC results. Multimedia Information Retrieval, Models and Languages, Data Modeling, Query Languages, Indexing and Searching, Libraries and Bibliographical Systems.

Text/References:

1. Information Storage and Retrieval Systems: Theory and Implementation By Kowalski, Gerald, Mark T Maybury Kluwer Academic Press, 2000.
2. Modern Information Retrieval by Ricardo Baeza-Yates, Pearson Education, 2007.
3. Information Retrieval: Algorithms and Heuristics by David A Grossman and Ophir Frieder, 2nd Edition, Springer International Edition, 2004.
4. Information Retrieval Data Structures and Algorithms By William B Frakes, Ricardo Baeza- Yates, Pearson Education, 1992.
5. Information Storage & Retrieval by Robert Korfhage – John Wiley & Sons.
6. Introduction to Information Retrieval by Christopher D. Manning and Prabhakar Raghavan, Cambridge University Press, 2008

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE604: Ad-Hoc Networks

Course Outline:

The proposed course covers a special class of Wireless Networks which are Ad-Hoc Networks in which structure of networks varying with respect to time. In real life these networks play vital role in advanced communication system. The best practical examples of Ad-Hoc Networks is VANETs, it is practical implementation of Ad-Hoc networks to serve various on-demand application of internet users. Now-a-Days most of the applications require ad-hoc networks because of on-demand day-to-day needs. The proposed course covers research issues in various layers. One of the major concerns is energy management in Wireless Ad-Hoc Networks to design adaptive protocols.

Objectives:

1. Demonstration of available spectrum for Wireless Communication for various operations.
2. Allocation details of spectrum to various applications.
3. The need of Ad-Hoc Networks for various applications.
4. Channel allocation mechanism for various on-demand applications using Ad-Hoc Networks.
5. Various Network Layer protocol operations for routing the packets.
6. Energy Management scheme while transmitting the data.

Outcomes:

1. The proposed course improves the connectivity to share information for various applications.
2. Basic understand of signals and physical layer medium for transmitting the data in the form of analog signal.
3. Channel allocation strategy to improve the connectivity in Ad-Hoc Networks.
4. Design and Develop new routing protocol for MANETs.
5. Detail study of various kind routing protocol such as proactive, reactive and hybrid kind to improve the performance of Ad-Hoc Networks.
6. Able to introduce various energy efficient routing protocol schemes for ad-hoc networks.

List of PO that the course covers: PO3, PO5, PO6.

Level: Mastery

Prerequisites: Undergraduate level course in mobile and wireless communication.

Course Description:

Unit I: Introduction
Fundamentals of Wireless Communication Technology – The Electromagnetic Spectrum, Radio propagation Mechanisms, Characteristics of the Wireless Channel, Mobile ad hoc networks (MANETs) and Vehicular ad hoc networks (VANETs): concepts and architectures. Applications and Design Challenges of MANETs and VANETs.

Unit II: Mac Protocols
Issues in designing a MAC Protocol, Classification of MAC Protocols: Contention based protocols-Contention based protocols with Reservation Mechanisms- Contention based protocols with Scheduling Mechanisms – Multi channel MAC-IEEE 802.11. IEEE Standards: 802.11a, 802.11b etc,. 802.15, HIPERLAN

Unit III: Routing Protocols
Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks, Classifications of Routing Protocols, Power Aware Routing Protocols. Multi cast routing in Ad Hoc Wireless Networks: Issues in Designing a Multicast Routing Protocol, Classifications of Multicast Routing Protocols. Energy Efficient Multicasting, Multicasting with Quality of Service Guarantees, Application Dependent Multicast Routing.

Unit IV: Energy Management
Energy Management in AdHoc Wireless Networks: Classification of Energy Management Schemes, Transmission Power Management Schemes, System Power Management Schemes. Special topics in Ad Hoc and wireless networks.

Text/ References

1. C S. Ram Murthy, B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall of India, 2nd ed. 2005.
2. R. Hekmat, Ad hoc Networks: Fundamental Properties and Network Topologies, Springer, 1st ed. 2006.
3. B. Tavli and W. Heinzelman, Mobile Ad Hoc Networks: Energy Efficient Real Time Data Communications, Springer, 1st ed. 2006.
4. Carlos De MoraisCordeiro, Dharma Prakash Agrawal "Ad Hoc & Sensor Networks: Theory and Applications", World Scientific Publishing Company, 2006.
5. G. Anastasi, E. Ancillotti, R. Bernasconi, and E. S.Biagioni, Multi Hop Ad Hoc Networks from Theory to Reality, Nova Science Publishers, 2008.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE605: Biometric Security

Course Outlines: Biometrics is about how we can recognize people automatically, by personal characteristic like fingerprints and faces etc. Information needs to sense it and then deliver an assessment of the identity associated with that data. This course covers the uses and applications of biometrics and how to undertake basic research in biometrics using case studies including biometric recognition system like Face, Signature, Fingerprint, Iris, Tongue recognition etc.

Course Objective: The course aims to:

1. Assess ways of how we identify people, identify different environments for biometric use, define biometrics.
2. To understand various kinds of biometric systems, securities and Recognition systems.
3. The newest approaches to biometrics and how they fit in its technological landscape.

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

1. Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems.
2. Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications.
3. Be able to work effectively in teams and express their work and ideas orally and in writing.
4. Identify the sociological and acceptance issues associated with the design and implementation of biometric systems.
5. Understand various Biometric security issues.

List of PO that the course covers: PO1, PO2, PO4.

Level: Mastery

Prerequisites: Fundamental knowledge in Biometrics.

Course Description:

UNIT-I: Introduction and overview

Biometrics-Introduction-history, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems-selecting a biometric for a system; Applications, Key biometric terms and processes, biometric matching methods-Accuracy in biometric systems, performance evaluation, basic image operations, edge detection in digital images, filtering,

sharpening etc.

UNIT-II: Biometric Technologies
Physiological Biometric Technologies: Fingerprints, Technical description and characteristics, Competing technologies, strengths and weaknesses, deployment, Facial scan, Technical description, characteristics, weaknesses-deployment, Iris scan, Technical description, characteristics, strengths and weaknesses, deployment, Retina vascular pattern.

UNIT-III: DNA Biometrics
Technical description, characteristics, strengths and weaknesses, deployment, Hand scan, Technical description, characteristics, strengths and weaknesses deployment, DNA biometrics, Behavioral Biometric Technologies: Handprint Biometrics.

UNIT-IV: Various Biometrics
Signature and handwriting technology, Technical description-classification- keyboard / keystroke dynamics, Voice data acquisition, feature extraction, characteristics, strengths and weaknesses, deployment, Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

Text/References:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : "Biometrics -Identity verification in a network", 1st Edition, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul, "Implementing Biometric Security", 1st Edition, Wiley Eastern Publication, 2005.
3. John Berger, "Biometrics for Network Security", 1st Edition, Prentice Hall, 2004.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE606: Data Mining

Course Outlines: This course introduces basic fundamentals of Data Mining and its applications. In this course, different aspects of Data mining such as, pre-processing of data, pattern mining, clustering and classification are discussed. Different algorithms for the data mining is also included in this course.

Course Objectives:

1. To learn the fundamentals of Data Mining and challenges in Data mining.
2. To learn different components of data mining such as preprocessing, clustering, classification etc.
3. To explore different algorithms to implement data mining.
4. To explore applications and case studied related to data mining.

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

1. Process the data for the Data-Mining algorithms
2. Analyze the data mining algorithms for Association Rules, Classification and Clustering algorithms in Data mining
3. Implement concept of Data Mining for the general applications

List of PO that the course covers: PO1, PO2, PO4.

Level: Mastery

Prerequisites: An undergraduate level course on Digital Electronics and C programming Language.

Course Description:

Introduction to Data Mining: Data Matrix, Numeric Attributes and Analysis, Categorical Attributes and Analysis, Graph Data, Data Visualization Data Mining Techniques. Challenges in Data Mining

Data Preprocessing: Kernel Methods, High-dimensional Data, Data Cleaning, Data integration and Dimensionality Reduction Data Transformation, Data Discretization

Pattern Mining: Itemset Mining and Algorithms, Summarizing Itemsets, GenMax and Charm Algorithm, Sequence Mining, Graph Pattern Mining and gSpan Algorithm, Pattern and rule Assessment

Clustering: Introduction to Clustering, Types of Clustering, K-means Algorithm, Expectation-Maximization Clustering, Hierarchical Clustering, The DBSCAN Algorithm, Spectral and Graph Clustering, Validation of Clustering

Classification: Bayes Classifier, Naive Bayes Classifier, *K* Nearest Neighbors Classifier, Decision Tree Classifier and Algorithm, Linear and Kernel Discriminant Analysis, Support Vector Machines, Linear and Nonlinear SVM case, Classification Assessment

Text/References Books:

1. Mohammed J. Zaki and Wagner Meira, “Data Mining and Analysis: Fundamental Concepts and Algorithms”, Cambridge University Press, 2014
2. Jiawei Han, Micheline Kamber and Jian Pei, "Data mining: concepts and techniques", 3rd ed, Morgan Kaufmann publications, 2012
3. Vipin Kumar, Pang-Ning Tan, Michael Steinbach, Introduction to Data Mining, Addison Wesley, 2006.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE607: Number Theory

Course Outlines: This course introduces Number theory to the students which is the foundation of cryptology and the cyber physical systems security. This course is the focused on pure mathematics which is essential to develop the various computational techniques and skill sets for cyber physical system, cyber forensic and security.

Course objectives:
The course is designed to train the graduates:

1. To understand the use of pure mathematics in coding theory, cryptology, and computer science.
2. To be able to get logical thinking, and the ability for symbolic manipulation in order to understand the sophisticated mathematical tools.
3. To get knowledge of exercise sets containing thought-provoking true/false problems, numeric problems and various proof techniques to develop computational skills.

Course Outcomes:

Graduates after completing the course shall gain:

1. Ability to emphasis on problem-solving techniques such as doing experiments, collecting data, recognizing patterns, and numeric computations exercises.
2. Ability to understand the thought-provoking applications spread throughout, establishing a strong and meaningful bridge with geometry, computer science.
3. Enable to develop the problem-solving skills, hands-on experience with concepts and enhance the opportunity for computational exploration and experimentation.

List of PO that the course covers: PO1, PO3, PO6.

Level: Mastery

Prerequisites: An undergraduate level course on Mathematics.

Course Description:

Number Systems: Natural numbers, Mathematical induction, Recurrence relations, The Division Algorithm, Catalan Numbers, Prime and Composite Numbers, Fibonacci and Fermat Numbers Greatest Common Divisor, Euclidean algorithm, Fundamental theorem of Arithmetic.

Diophantine equations: Modulo arithmetic, Congruence classes, Modular Exponentiation, Towers of Powers Modulo m, Linear Congruences, Multiplicative inverse, Systems of Linear Congruences, Chinese remainder theorem, Wilson's Theorem, Euler's extended algorithm, Fermat's little theorem, Multiplicative Functions, Totient function, Euler's theorem.

Elementary number theory: Prime numbers, Number bases, Primality testing algorithm, Primitive Roots and Indices, The Order of a Positive Integer, discrete logarithm, primitive roots for Primes, Number sieves, The Algebra of Indices, Quadratic Residues, The Legendre Symbol.

Text/References:

1. Thomas Koshy, Elementary Number Theory with applications, Elsevier India, 2005.
2. Menezes, A, et.al. Handbook of Applied Cryptography, CRC Press, 1996
3. D.R. Stinson, Cryptography - Theory and practice, CRC Press.
4. Koblitz, N. Course on Number Theory and Cryptography, Springer Verlag, 1986
5. Martin Erickson and Anthony Vazzana: Introduction to Number Theory, Chapman & Hall/CRC.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE608: Machine learning

Course Outlines: This course introduces Machine learning to the students which focused on interdisciplinary techniques such as linear algebra, calculus, and programming that can be used to predict or decide the response without human intervention. The machine learning is the growing area in the field of cyber physical systems, security, industries and research. This course will familiarize the students with basic models and various algorithms to implement machine learning which is essential for the student to prepare them for research and industry application of machine learning techniques.

Course Objectives: By the end of the course, students should be able to:

1. Understand the basic of machine learning, supervised and unsupervised learning.
2. Identify different machine learning algorithms for supervised and unsupervised learning.
3. Understand cloud-based machine learning for mobile devices.

Course Outcomes: At the end of the course students should be able to:

1. Understand different machine learning algorithms and techniques.
2. Apply machine learning in the research and industry applications.

3. Apply the algorithms to a real-world problem, optimize the models learned and report on the expected accuracy that can be achieved by applying different machine learning models.

List of PO that the course covers: PO1, PO2, PO4.

Level: Mastery

Prerequisites: An undergraduate level course on linear algebra, calculus and a programming Language.

Course Description:

Introduction: Basics of Machine Learning, data and visualization, Varieties of Machine Learning, Types of learning, Boolean functions and classes (DNF, CNF) Machine learning applications, Regression, Supervised and Unsupervised Learning, Issues with machine learning.

Supervised Learning: VC Dimension, PAC Learning, Regression, Model Selection and Generalization, Basic methods: Distance-based methods, Nearest-Neighbors, Decision Trees, Na ve Bayes, Linear models: Linear Regression, Logistic Regression, Generalized Linear Models Support Vector Machines, Nonlinearity and Kernel Methods Beyond Binary Classification: Multi-class/Structured Outputs, Ranking

Unsupervised Learning: Clustering: K-means/Kernel K-means, Dimensionality Reduction: PCA and kernel PCA, Matrix Factorization and Matrix Completion, Generative Models (mixture models and latent factor models)

Scalable Machine Learning: Scalable Machine learning and cloud platform, Semi-supervised Learning, Active Learning, Inference in Graphical Models, Introduction to Bayesian Learning and Inference for scalable learning.

Text/References Books:

1. Tom Mitchell, “Machine Learning”, McGraw Hill, 2017.
2. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012
3. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.
4. Stephen Marsland, “Machine Learning: An Algorithmic Perspective”, 1st ed, Chapman & Hall, 2009

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE609: Design of Electromechanical system

Course Outlines: This course introduces electromechanical systems with emphasis on modelling, analysis and design techniques. A variety of electromechanical devices will be covered during course. The aim of the course is to develop understanding among the students about fundamental concepts of the electromechanical systems employed in real world.

Course Objectives: The primary objectives of this course are described as follows:

1. To understand magnetic circuit analysis and use it to predict the electromagnetic characteristics of common devices
2. To understand finite element analysis for electromagnetic systems and use it to predict magnetic fluxes, forces, and torques in electric machine models
3. To understand the fundamentals of permanent magnetism and be able to specify permanent magnet materials for specific applications
4. To understand the principles of electromechanical energy conversion and use these principles to predict forces and torques in electric machine models
5. To develop nonlinear dynamic models of electric machines, simulate these systems using MATLAB and Simulink, and analyze their performance and response characteristics
6. To understand the fundamentals (machine topology, etc.) and basic operating characteristics (torque, speed, efficiency, etc.) of common electrical machines (induction motors, synchronous motors, DC motors, etc.)
7. To design, model, and simulate common (standard motors, etc.) and unique (railguns, active magnetic bearings, etc.) electric machines

Course Outcomes: After completing the course, students will be able to:

1. Select and apply a knowledge of mathematics, science, engineering, and technology to engineering technology problems that require the application of principles and applied procedures or methodologies.
2. Conduct standard tests and measurements; to analyze, and interpret experiments; and to apply experimental results to improve processes.
3. Design of electromechanical systems, components, or processes for broadly-defined engineering technology problems appropriate to program educational objectives.
4. Have a detail understanding upon the design, analysis and control of various types of electrical machines.
5. Have a knowledge of the impact of engineering technology solutions in a societal and global context.

List of PO that the course covers: PO2, PO3, PO4, PO6.

Level: Mastery

Prerequisites: An undergraduate level course on linear algebra, calculus and a programming Language.

Course Description:

Unit I: Introduction and overview
Introduction to electromechanical systems, Fundamentals of Electromagnetism: Maxwell's Equations-Static electric fields: Coulomb's law, Gauss's law, visualizing fields and potentials, capacitance, Electric currents: Ohm's law, continuity equation, Static magnetic fields: conservation of flux, Biot-Savart's law, Lorentz's force equation, Ampere's law, Biot-Savart's law, Lorentz's force equation, Faraday's law, inductance, Summary of Maxwell's equations.

Unit II: **Electromagnetic Circuits Analysis**
Introduction to Finite Element Analysis (FEA), Physical Problems, Mathematical Models, and the Finite Element Solution 2D using FEMM, 3D using ANSYS Maxwell.

Unit III: Electromechanical Energy Conversions
Conservation of energy, energy and coenergy, force and torque in EM machines, Generalized Machine theory (GMT): Analysis of standard rotating machine using GMT, Common electric Machines: Synchronous, reluctance, DC Motor speed control and PWM, H-bridge and DC Motor direction control, Sensors and sensing with Arduino.

Unit IV: Design of Electrical Machines
Modeling and Simulation of EM systems, Nonlinear analysis: linearization and Simulink Transient and steady-state dynamics; Design Considerations for Electric Machines: Iron Losses, Copper Losses, Flux Saturation; Design, analysis, and control - active magnetic bearings, railguns etc.

Texts/References

1) Buckner, G.D., Course Notes: MAE/ECE 535 Design of Electromechanical Systems.
2) Sadiku., Elements of Electromagnetics, Any Recent Edition, Oxford University Press.
3) Fitzgerald, A.E., C. Kingsley, and S.D. Ulmans. Electric Machinery, Any Recent Edition, McGraw-Hill.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE610: Computer Vision

Course Outlines: This course describes the Computer Vision to the students which focuses on development of algorithms and techniques to analyse and interpret the visible world around us through computer. This requires understanding of the fundamental concepts related to various aspects of multi-

dimensional data processing, pattern analysis/modelling, feature extraction etc. The fundamental knowledge of these concepts is necessary in order to implement computer vision in industries, commercial or research applications such as document processing, OCR, Biometrics, Medical diagnosis, surveillance etc.

Course Objectives:

1. To understand the fundamental of computer vision in both the theoretical and practical aspects.
2. Describe the foundation of image formation and processing for 2D and 3D Computer Vision.
3. To understand different technical approaches, algorithms, methods and advance concepts involved in computer vision.

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

1. Understand different methods and algorithms for the computer vision.
2. Implement different algorithms and techniques for the computer vision.
3. Develop applications using computer vision techniques.
4. Understand video processing, motion computation and 3D vision and geometry.

List of PO that the course covers: PO1, PO2, PO3, PO4.

Level: Mastery

Prerequisites: An undergraduate level course on data structure, linear algebra, calculus, and programming language (preferred Python).

Course Description:

Introduction: Image Processing, Computer Vision and Computer Graphics, Overview of Computer Vision Applications: Document Image Analysis, Biometrics, Object Recognition, Tracking, Medical Image Analysis, Content-Based Image Retrieval, Video Data Processing, Multimedia, Virtual Reality and Augmented Reality

Image Formation Models and Processing: Monocular imaging system, Radiance, Irradiance, BRDF, color etc, Projection, Camera and Camera calibration, Binocular imaging systems, geometry views, Structure determination, Photometric Stereo, Depth from Defocus, Image preprocessing, Image representations (continuous and discrete), Edge detection and feature extraction

Shape Representation and Segmentation: Contour based representation, Region based representation, Deformable curves and surfaces, Snakes and active contours, Level set representations, Fourier and wavelet descriptors, Medial representations, Multiresolution analysis

Object recognition and motion estimation: Hough transforms and other simple object recognition methods, Shape correspondence and shape matching, Principal component analysis, Shape priors for

recognition, Regularization theory, Optical computation, Stereo Vision, Motion estimation, Structure from motion

Applications: Applications of computer vision, Face detection and recognition, Surveillance, In-vehicle vision system, Medical application, industrial application

Text/References Books:

1. Richard Szeliski, "Computer Vision: Algorithms and Applications, 1st ed, Springer, 2010.
2. D. Forsyth and J. Ponce, "Computer Vision - A modern approach", 2nd Edition, Pearson Prentice Hall, 2012.
3. Richard Hartley and Andrew Zisserman, "Multiple View Geometry in Computer Vision", 2nd Edition, Cambridge University Press, 2004.
4. B. K. P. Horn, "Robot Vision", 1st Edition, McGraw-Hill, 1986.
5. E. R. Davies, "Computer and Machine Vision: Theory, Algorithms, Practicalities", 4th Edition, Elsevier Inc,2012.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE611: Formal methods in CPS and Automation

Course Outlines: This course introduces formal methods in cyber physical systems and automation to the students which focused on in-depth study of different methods in cyber physical systems. This course is mainly focused on the application of CPS in automation dealings with the hybrid automation, multi-agents systems and control strategies.

Course Objectives:

1. To provide introduction to CPS methods in automation with multi-agent systems and control strategies.
2. To equip students with various methods used in automation and CPS.
3. To foster understanding through real-world applications related to CPS and automation.

Course Outcomes: At the end of the course students should be able to:

1. Apply different methods in CPS for problems related with real word automation.
2. Present solution to automated systems by utilizing hybrid switching systems, multiagents systems and strategies for controlling.
3. Apply concepts and logic towards smart grids, smart cities, multi-agents robotics etc.

List of PO that the course covers: PO1, PO2, PO3, PO4, PO6.

Level: Mastery

Prerequisites: Postgraduate (Master) level course on Cyber Physical System, Embedded Systems, and programming Language (MATLAB/Python/Java/C++).

Course Description:

Mathematical Preliminaries for Hybrid Automata, Hybrid and Switching Systems: Foundations of Cyber Physical Systems - Computing, Control and Communication Modeling: Examples: bouncing ball, thermostat, transmission system, inverted pendulum swing-up, multi-tank system, manufacturing systems, supervisory control. Formal models for hybrid systems: continuous-time and discrete-event models Lyapunov stability of hybrid systems, Stability under arbitrary switching, Controller realization for stable switching, Computational methods to construct multiple Lyapunov functions - Linear Matrix Inequalities.

Multi-agent Systems Primer: Network Models (graphs, random graphs, random geometric graphs, state-dependent graphs, switching networks), Mobile Sensor Networks (coverage control, voronoi-based cooperation strategies)

Control Strategies: Distributed Control, Coordinated Control and decentralized control with delay effect and collision avoidance, Event Triggered Control, Game theory in coordination control

Applications: Multi-Agent Robotics (formation control, sensor and actuation models), Issues: Consensus, Collision avoidance, Connectivity Assurance, Smart Grid: Distributed Control, Sensor-controller coordination, Convex optimization

Text/References Books:

1. Broy M., "Cyber-Physical Systems - Innovation durch softwareintensive eingebettete Systeme.", Springer, 2010
2. R. Alur, "Principles of Cyber-Physical Systems," MIT Press, 2015.
3. Raj Rajkumar, Dionisio de Niz and Mark Klein, "Cyber-Physical Systems", Addison-Wesley, 2017.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE612: Cryptanalysis

Course Outlines: Cryptanalytics is the art and science of solving unknown codes and ciphers. Cryptanalysts try to break the codes and ciphers created and used by cryptographers. The course explains standard cryptanalysis techniques used for analyzing and attacking different types of cryptographic schemes.

Course Objectives:

1. Learn different cryptosystems and ciphers.
2. To discuss the basics of cryptanalysis and used it in breaking of different ciphers.
3. Develop understanding about different cryptanalysis methods used in cryptosystems.

Course Outcomes: At the end of the course students should be able to:

1. Understand modern concepts related to cryptanalysis and get insights of different cryptanalysis methods used in cryptosystems.
2. Analyze and use methods for cryptanalysis and reflect about limits and applicability of these methods.
3. Able to break the cryptosystems that are not secure.

List of PO that the course covers: PO1, PO2, PO5, PO6.

Level: Mastery

Prerequisites: Knowledge of Cryptography fundamentals.

Course Description:

Unit I: Basics of Cryptosystem, Ciphers and Cryptanalysis
Cryptology, History of Cryptology, Principles of Good Cryptography, Fundamentals of cryptosystems, Basic model of the cryptosystem, Types of cryptosystem, Monoalphabetic Ciphers, Keying, Polyalphabetic Ciphers, Transposition Ciphers, Cryptanalysis, Steps in Cryptanalysis, Breaking Monoalphabetic Ciphers, Breaking Polyalphabetic Ciphers, Breaking Columnar Transposition Ciphers.

Unit II: General Cryptanalytic Methods
Brute force, Time-space tradeoffs, Rainbow tables, Slide attacks, Cryptanalysis of hash functions, Cryptanalysis of random number generators.

Unit III: Linear Cryptanalysis
Matsui's algorithms, Linear expressions for S-boxes, Matsui's piling up Lemma, Easy1 cipher, Linear expressions and key recovery, Linear cryptanalysis of DES, Multiple linear approximations, Finding linear expressions, linear cryptanalysis code.

Unit IV: Differential Cryptanalysis
S-box differentials, Combining S-box characteristics, key derivation, differential cryptanalysis code, differential cryptanalysis of Feistle ciphers, analysis, differential linear cryptanalysis, conditional characteristics, Higher order differentials, truncated differentials, impossible differentials, boomerang attack, interpolation attack, Related key attack.

Text/References Books:

1. Carl E. Vuono and Thomas F. Sikora, "Basic Cryptanalysis", Field Manual No 34-40-2, (1990).
2. Kevith M. Martin, "Everyday Cryptography: Fundamental principles and applications", Oxford University Press (2012).
3. Christopher Swenson, "Modern cryptanalysis techniques for advanced code breaking", Wiley (2008).
4. Mark Stamp and Richard M. Low, "Applied Cryptanalysis Breaking Ciphers in the Real World", Wiley-Interscience (2007).

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE613: Ethical hacking

Course Outline: This course focuses on the beginner's introduction to the ethical hacking process. This course also targets to provide that ethical hacking is a highly in-demand skill set, exciting profession, and key part of any organization's cybersecurity program.

Course objectives: This course aims to
1. Conduct online intelligence gathering for corporate/individual network security.
2. Scan & enumerate target systems in network.
3. Protect files/systems by open password-protected files.
4. Subvert vulnerable software applications from cyber-crimes.
5. Monitor keystrokes and user activity for network security
6. Aware of common phishing techniques.
7. Create backdoored programs & documents

Course Outcomes: On completion of the course, students will be able to

1. Understand the core concepts of Defensive and Offensive Security.
2. Understand the breaching of networks domains and systems.
3. Understand the ethics of Hacking.
4. Understand the limitations of Penetration Testing.
5. Understand the Cyber Crime Cases and IT act India and amendments.

List of PO that the course covers: PO4, PO6, PO7.

Level: Mastery

Prerequisites: Sound understanding of Operating System and Networking Concepts.

.

Course Description:

Unit I: Introduction

Introduction to ethical hacking, types of ethical hacking, hacking methodology and terminology, concept of networking, TCP/IP protocol stack, IP addressing and routing, TCP & UDP, IP subnetting, routing protocol, IP version, routing examples, Nessus installation: Process & operation details.

Unit II: Software exploitation

Metasploit Exploiting system software, Metasploit social engineering works, Metasploit social Engineering works, MITM attack, Basic concept of cryptography, private key cryptography, public key cryptography, cryptographic hash function.

Unit III: Hacking types and Daniel of service

Digital signature & certificate, applications, steganography, biometrics, network based attacks, DNS and Email security, side channel attacks, password cracking, phishing attack, maloeware, wifi hacking, Dos and DDos attack, DoS/DDos Attack Techniques, DoS/DDos Attack Tools, DoS/DDos Protection Tools.

Unit IV: Hardware hacking and SQL injection

Elements of hardware security, physical unclonable function, hardware Trojon, web application vulnerability scanning, SQL injection authentication bypass, SQL injection error based, QL injection error based from web application, SQLMAP, cross site scripting, file upload vulnerability, NMAP tool, network analysis using wireshark.

Text/ References

1. Cyber Crime and Law Enforcement- V. D. Dudeja, Commonwealth Publishers.
2. Introduction to Computer network and Cybersecurity- C. H Wu and J.D. Irwin.

3. Cryptography and Network Security: Principles and Practice- W. Stallings.
4. Hacking: The Art of Exploitation-Jon Erickson.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE614: Internet Security and Privacy

Course Outline: This course introduces the basics of internet security and privacy to the student that is the one of the important parameters to a cyber physical system and IoT systems. This course discusses the role of internet security and data privacy in the present modern systems that include different levels of data, their impact of the organization and assess control to such data. Different access control mechanism viz. physical, biometric, multilevel authentication is also covered in this course.

Course objectives: This course aims:

1. To introduce the fundamentals of internet security and privacy using the data classification, different authentication mechanism.
2. To introduce different types of information security threats, frauds and data thefts.
3. To introduce information security risk analysis and risk management using security assessment at different levels.

Course Outcomes: On completion of the course, students will be able to:

1. Understand different types of information security threats, fraud and thefts.
2. Understand the importance of information security and privacy needed in the modern systems.
3. Understand the different techniques for the information security risk assessment and management.
4. Understand and utilize different mode of information security mechanism.

List of PO that the course covers: PO1, PO2, PO4, PO6.

Level: Mastery

Prerequisites: Basic understanding of internet security.

Course Description:

Unit I:

Information Security and Threats: Introduction to Information Security, Threats, Frauds, Data Thefts, Malicious Codes and Hackers, Denial-of-Services (DoS) Attacks, Vulnerability, Security Policies and Procedures, Building Blocks of Information Security, Security related Terms, information Level Threats Vs Network Level Threats, information system security, Computer Viruses, Classifications of Threats.

Unit II:

Information Asset Classification and Privacy: Information Asset, Information Classification, Secret, Confidential, Private and Public Information, Declassification or Reclassification, privacy invasion, privacy challenges in test environment. Privacy Technological Impact.

Unit III:

Information security Risk Analysis and Management: Risk Analysis Process, Threat Identification, Probability of Threat Occurrence, Impact of the Threat and Controls, Risk Mitigation and Control Types, Cost Analysis, Risk Management, Approaches and Considerations, Security Models & Frameworks, Methodologies for Information System Security.

Unit IV:

Access Control: User Identity and Access Management, Authorization, Access and Privilege Management, System Level and Network Level Access Control, Intrusion Detection System and Event Logging, Cryptography.

Unit V:

Security Assessment and Techniques: Physical Security, physical entry controls, Biometric identification/Authentication techniques, User Identification & Authentication. Meaning, Biometric Techniques, Network security, Cryptography & Encryption, Databases Security.

Text/ References

1. D. Salomon, Data Privacy and Security. Springer New York, 2003.
2. Thomas J Shaw, “Information security and privacy: a practical guide for global executives, lawyers and technologists”, American Bar Association, Chicago, 2011.
3. S. Stalla-Bourdillon, J. Phillips, and M. D. Ryan, Privacy vs. Security. Springer London, 2014.
4. Houbing Song, Glenn A. Fink and Sabina Jeschke, "Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications", Wiley-IEEE Press, 2017

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No

MTE615: Advance Real-Time Systems

Course Outline: This course is focused on advance real time systems. This course introduces fundamental problems, concepts, and approaches in the design and analysis of real-time systems to the student. This course covers the issues related to the design and analysis of systems with real-time constraints, multi-tasking and scheduling problems associated with the real time systems.

Course objectives: This course aims:

1. Introduction to real time systems and real time operating systems.
2. To introduce the fundamental of Real-time scheduling and their analysis.
3. To introduce basic specifications and verification of timing constraints, multi-tasking and their properties.
4. To introduce the various design methods for real-time systems.

Course Outcomes: On completion of the course, students will be able to:

1. Understand advanced concepts in real time systems.
2. Understand and evaluate the performance of hard- and soft- real time systems.
3. Understand the use of multi-tasking techniques in real time systems and able to analyze multi task scheduling algorithms for various tasks.

List of PO that the course covers: PO2, PO4, PO5, PO6.

Level: Mastery

Prerequisites: Undergraduate level course on Operating Systems.

Course Description:

UNIT 1

Real-Time Systems: Introduction, Scope of Real Time systems, Hard Real Time systems, Soft Real-Time Systems, Real Time Application, Real-Time Systems Model, Application of Real Time Systems.

UNIT 2

Scheduling: Scheduling in Real Time Systems, Types of scheduling, Hard Real-Time Scheduling and approaches, Clock-Driven Scheduling, Priority-Driven Scheduling, Periodic Tasks, Scheduling Aperiodic and Sporadic Jobs in Priority- Driven Systems.

UNIT 3

Resources: Introduction, Resources in real time systems, Resource Access Control, Multiprocessor Scheduling and Access Control.

UNIT 4

Scheduling Flexible Computations and Tasks with Temporal Distance Constraints. Real-Time Communications, Real Time Operating Systems (RTOS), Application of real time operating systems, Limitations of RTOS, Embedded systems and RTOS.

Text/ References

1. Philip.A.Laplante, “Real Time System Design and Analysis”, 3rd Edition, PHI, 2004.
2. Jane Liu, “Real-Time Systems”, Prentice Hall, 2000.

Assessment Method: Written exam and Term Paper.

Any need for revision of existing rules: No