GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Master of Engineering

Level: PG

Branch: Cyber Security

Course / Subject Code : ME02059091

Course / Subject Name: Industrial Control Systems and Cyber Security

w. e. f. Academic Year:	2024-25
Semester:	2
Category of the Course:	Professional Elective Course

Prerequisite:	Computer Network, Internetworking concepts, TCP/IP, Networking Design/architecture, Vulnerability Assessment Risk Management.
Rationale:	• The course will explore the understanding of industrial control system components, purposes, deployments, significant drivers, and constraints. • The course will focus on Control system approaches to system and network defense architectures and techniques • The course will also cover the Incident-response skills in a control system environment.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	To understand the infrastructure and protocols for the Industrial Control Systems.	UN
02	To develop the attack plan which covers hacking processes, vulnerabilities assessment for Industrial Control Systems.	AP
03	To implement incident response and handling methodologies.	AP
04	To analyse different models & techniques for securing the Industrial Control Systems.	AN
05	To evaluate different Standards and Regulations for Cybersecurity related to Industrial Control Systems.	EL

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
03	00	02	04	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**Unit-I: Industrial Control Systems Overview** Overview of Industrial Control Systems - Processes & Roles, Industries. Purdue Model Levels 0 and 1-Controllers and Field Devices, Programming Controllers. Purdue Model Levels 2 and 3- HMIs, Historians, Alarm Servers, Specialized Applications and Master Servers, Control Rooms and Plants, SCADA. IT & ICS Differences-ICS Life Cycle Challenges, Physical and Cyber Security, OT &ICS security challenges.	04	10
2.	**Unit-II: Industrial Control Systems Security Architecture** Network Segmentation and Segregation, Boundary Protection, Logically Separated Control Network.	04	10
3.	**Unit-III: SCADA Networks Protocols** Ethernet and TCP/IP Concepts in ICS, ICS Protocols over TCP/IP, Enumerating Modbus TCP, How ICS Are Targeted, Study of Attacks, ICS as a High–Value Target, Attack Methodologies In ICS, Challenges of Vulnerability Management Within ICS.	06	15
4.	**Unit-IV: Enforcement Zone Devices and Cryptography** Firewalls and NextGen Firewalls in ICS, Modern Data Diodes, NIDS/NIPS and Netflow, USB Scanning and Honeypots	06	15
5.	**Unit-V: Standards and Regulations for Cybersecurity** ISO 27001, ICS/SCADA, NERC CIP, CFATS, ISA99, IEC 62443, NIST SP 800-82 Creating ICS Cyber Security Policy: Policies, Standards, Guidance, and Procedures Culture and Enforcement, Examples and Sources, Industrial Control Systems Security Policy Review	09	20
6	**Unit-IV: Applying Security Controls to Industrial Control Systems for Network** Unidirectional Gateways, Single Points of Failure, Redundancy and Fault Tolerance, Preventing Man-in-the-Middle Attacks, Authentication and Authorization, Monitoring, Logging, and Auditing.	10	20
7	**Unit-VII: Current Trends** The latest technology attacks in Industrial Control Systems with Artificial Intelligence and its countermeasures.	06	10
	TOTAL	**45**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
10	**20**	**20**	**20**	**20**	**10**

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Cyber-security of SCADA and Other Industrial Control Systems, Edward J. M. Colbert, Alexander Kott, Springer Cham
2. Cybersecurity for Industrial Control Systems, by Tyson Macaulay, Bryan L. Singer, Auerbach Publications
3. Industrial Network Security by Eric Knapp, Joel Langill, Elsevier

(b) Open-source software and website:

1. Course-related online MOOC on SWAYAM NPTEL/Coursera Platform.
2. Recently published papers/articles of reputed journals/conferences.

Suggested Course Practical List:

- List of Laboratory/Learning Resources Required: The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required: IBM, ISA, CISA, SANS websites etc.

Suggested Project List: Buffer overflow attacks and Industrial Control System Network, Incident Response Plan for Industrial Control Systems and Cyber Security, etc.

* * * * * * *