

# **GUJARAT TECHNOLOGICAL UNIVERSITY**

# Master of Engineering Semester – III Subject Code: 4735901 Subject Name: Industrial Control Systems (ICS) Cyber Security

## Type of 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 Scheme:**

Teaching Scheme			Total Credits	Assessment Pattern and Marks			Total	
L	Т	PR	С	Theory		Practical		Marks
				ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

### **Course Content:**

Sr No	Course Content		of	%
51 110			rs	
1	Unit-I: ICS Overview	04		10
	Overview of ICS-Processes & Roles, Industries.			
	Purdue Levels 0 and 1-Controllers and Field Devices, Programming Controllers. Purdue 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.			
2	Unit-II: ICS Security Architecture	04		10



# **GUJARAT TECHNOLOGICAL UNIVERSITY**

#### Master of Engineering Semester – III Subject Code: 4735901

Subject Name: Industrial Control Systems (ICS) Cyber Security

	Network Segmentation and Segregation, Boundary Protection,		
	Logically Separated Control Network.		
3	Unit-III: SCADA Networks Protocols	06	15
	Ethernet and TCP/IP Concents 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.		
4	Unit-IV: Enforcement Zone Devices and Cryptography	06	15
	Firewalls and NextGen Firewalls in ICS. Modern Data Diodes. NIDS/NIPS and		
	NetFlow, USB Scanning and Honeypots		
	, , , , , , , , , , , , , , , , , , , ,		
5	Unit-V: Standards and Regulations for Cybersecurity	08	20
	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, ICS Security Policy Review		
6	Unit W. Applying Compile Controls to ICC for Naturals	00	20
0	onit-iv: Applying Security condities to ics for Network	00	20
	Unidirectional Gateways, Single Points of Failure, Redundancy and Fault		
	Tolerance, Preventing Man-in-the-Middle Attacks, Authentication and		
	Authorization, Monitoring, Logging, and Auditing.		
7	Unit-VII : Current Trends	04	10
ĺ ′			10
	The latest technology attacks in ICS with AI and its countermeasures.		

#### Textbook:

Cyber-security of SCADA and Other Industrial Control Systems, Edward J. M. Colbert, Alexander Kott, Springer Cham



# **GUJARAT TECHNOLOGICAL UNIVERSITY**

#### Master of Engineering Semester – III Subject Code: 4735901 Subject Name: Industrial Control Systems (ICS) Cyber Security

#### **Reference Book:**

- 1. Cybersecurity for Industrial Control Systems, by Tyson Macaulay, Bryan L. Singer, Auerbach Publications
- 2. Industrial Network Security by Eric Knapp, Joel Langill, Elsevier

#### **Course Outcome:**

After completion of the Course, Students will be 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 ICS.	АР
03	To implement incident response and handling methodologies.	АР
04	To analyse different models & techniques for securing the ICS systems.	AN
05	To evaluate different Standards and Regulations for Cybersecurity related to ICS.	EL

\*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

#### Suggested Course Practical List:

• The practical work will be carried out based on the content covered during the academic sessions.

## List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM platform.
- Recently Published papers/articles in reputed journals.