GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Automation and Robotics / Instrumentation & Control

Subject Code : DI05000271

Subject Name: Industrial Network Security

w. e. f. Academic Year:	2026-27
Semester:	5th
Category of the Course:	MOPEC

Prerequisite:	Students should have basic knowledge of industrial instrumentation and measurement systems, including sensors, transducers, and signal conditioning. They should also be familiar with process control fundamentals, PLC basics, industrial communication protocols, and basic computer networking concepts such as LAN, IP addressing, and network devices. Understanding of SCADA/DCS systems and industrial automation environments will help students understand security challenges in industrial networks.
Rationale:	The aim of this subject is to provide Instrumentation & Control diploma engineering students with the knowledge and skills necessary to protect industrial networks from cybersecurity threats. As more and more industrial systems become connected to the internet, the risk of cyber-attacks increases. By studying Industrial Network Security, students will be better prepared to design, implement, and maintain secure industrial networks. This will help them ensure the reliability and availability of industrial systems, which is critical for the manufacturing, energy, and transportation industries.

COURSE OUTCOME:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
1	Identify the Industrial Control Systems (ICS) and detail its operation.	U
2	Clarify the different types of ICS networks.	U A
3	Explain Industrial Network Protocols.	U A
4	Understand and establish security zones and conduits.	U A
5	Explain and implement Network security and access controls.	R U

**Revised Bloom's Taxonomy (RBT)*

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Automation and Robotics / Instrumentation & Control

Subject Code : DI05000271

Subject Name: Industrial Network Security

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(M)	PA(I)	ESE (V)	
3	0	0	3	70	30	00	00	100

COURSE CONTENT:

Unit	Topics and Sub-topics	No. Of Hrs.	% Weightage
Unit-I Introduction to ICS and Operations	1.1 Industrial control system (ICS), common industrial security recommendations. 1.2 APTs and weaponized malware 1.3 System assets: Programmable Logic Controller, Remote Terminal Unit, Intelligent Electronic Device, Human–Machine Interface, Supervisory Workstations, Data Historian, and other assets 1.3.1 System operations: Control loops, control processes, feedback loops, production information management, business information management1.5 Process management	12	25 %
Unit-II ICS Network Design and Architecture	2.1 Introduction to Industrial Networking. 2.2 Differences in Industrial Network Architectures by Function 2.3 Common Topologies 2.4 Network Segmentation, Types of Segmentation, Characteristics of Segmentation, Physical vs. Logical Segmentation 2.5 Network Services 2.6 Wireless Networks 2.7 Remote Access o Performance Considerations: Latency, Jitter, Bandwidth, Throughput, Type of Service, Class of Service, Quality of Service, Network Hops	12	25 %
Unit-III Industrial	3.1 Overview of Industrial Network Protocols.	9	20 %

Network Protocols	3.2 Fieldbus Protocols: Modbus, Distributed Network Protocol (DNP), PROFIBUS, Industrial Ethernet, PROFINET, EtherCAT 3.3 Backend Protocols: Open Process Communications (OPC), Inter-Control Center Communications Protocol (ICCP) 3.4 AMI and the Smart Grid 3.4.1 Industrial Protocol Simulators		
Unit-IV Establishing Zones and Conduits	4.1 Security Zones and Conduits 4.2 Identifying and Classifying Security Zones and Conduits 4.3 Recommended Security Zone Separation 4.3.1 Establishing Security Zones and Conduits	6	15 %
Unit-V Implementing Security and Access Controls	5.1 Implementing Network Security Controls 5.2 Implementing Host Security and Access Controls 5.2.1 How Much Security is Enough?	6	15 %
	Total	**45 Hrs**	**100%**

AFFECTIVE DOMAIN OUTCOMES:

The following sample Affective Domain Outcomes (ADOs) are embedded in many of the above-mentioned COs and PrOs. More could be added to fulfil the development of this competency.

a) Work as a leader/a team member for assigned student activity.
b) Follow safety practices and procedure in Lab.
c) Realize the importance of engineering for societal development.
d) Develop gradually the engineering mindset in day-to-day observation

SUGGESTED STUDENT ACTIVITIES:

Other than the classroom and laboratory learning, following are the suggested student-related co-curricular activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

a) Teachers-guided self-learning activities; Course/ library/ internet/lab-based mini projects.
b) Students' activities like course/topic-based seminars; Internet-based assignments, and a presentation on the Industrial Control Systems and various Network Protocols.

SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any):

Following Sample strategies teacher can use to accelerate the attainment of the various outcomes in this course:

1. Massive open online courses (MOOCs) may be used to teach various topics/ subtopics.
2. Guide student(s) in undertaking micro-projects.
3. 'L' in section No. 4 means different types of teaching methods that are to be employed by teachers to develop the outcomes.
4. About 20% of the topics/sub-topics which are relatively simpler or descriptive in nature is to be given to the students for self-learning, but to be assessed using different assessment methods.
5. With respect to section No.10, teachers need to ensure to create opportunities and provisions for co-curricular activities.
6. Introduce Industrial cyber security laws and Network protocols among the students.
7. Helping the students to understand the concepts of the world wide web (WWW) and the Internet

SUGGESTED MICRO-PROJECTS:

1. Arrange a seminar regarding Industrial Network Security, different types of Protocols, and security zones in the classroom.
2. Arrange an appropriate industrial visit for students, where they can relate the classroom teaching/ learning.

SUGGESTED LEARNING RESOURCES:

Sr. No	Title of book	Author	Publication with place, year and ISBN
1	Industrial Network Security	Eric D. Knapp And Joel Thomas Langill	ELSEVIER Publications. ISBN: 978-0-12-420114-9
2	Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS	Tyson Macaulay and Bryan L. Singer	Auerbach Publications ISBN: 1439801967
3	Industrial Automation and Control System Security Principles	Ronald L. Krutz and Russell Dean Vines	International Society of Automation ISBN-13: 978-1937560638
4	Cybersecurity and Cyberwar: What Everyone Needs to Know	P.W. Singer and Allan Friedman	Oxford University Press India ISBN: 9780199918119

SUGGESTED LEARNING WEBSITES:

1 **National Institute of Standards and Technology (NIST)** – Industrial Control System security guidelines and standards.
https://www.nist.gov

2 **SANS Institute – Industrial Control System Security** – Training materials, articles, and security resources related to ICS and SCADA systems.
https://www.sans.org

3 **ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)** – Information about vulnerabilities, threats, and cybersecurity advisories for industrial systems.
https://www.cisa.gov/ics

4 **Wireshark Official Website** – Resources and tutorials for network packet analysis.
https://www.wireshark.org

5 **Cisco Networking Academy** – Free courses and resources related to networking and cybersecurity.
https://www.netacad.com

6 **OWASP (Open Web Application Security Project)** – Information about security vulnerabilities, threats, and best practices.
https://owasp.org

7 **Kali Linux Official Website** – Tools and documentation for penetration testing and security assessment.
https://www.kali.org

8 **PROFIBUS & PROFINET International (PI)** – Resources and technical information about industrial communication networks.
https://www.profibus.com

9 **FieldComm Group** – Information about FOUNDATION Fieldbus and industrial communication standards.
https://www.fieldcommgroup.org

10 **Cybersecurity and Infrastructure Security Agency (CISA)** – Security guidelines and alerts for industrial networks.
https://www.cisa.gov

* * * * * *