GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

Competency-focused Outcome-based Green Curriculum-2023 (COGC-2023)
Semester –V

Course Title: Industrial Network Security
(Course Code: 4351708)

Diploma programmer in which this course is offered	Semester in which offered
Instrumentation and Control Engineering	5th Semester

1. 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.

2. COMPETENCY

The fundamentals of industrial network security involve understanding the various cyber threats and vulnerabilities associated with industrial control systems (ICS). Potential cyber risks to ICS need to be identified and analyzed to mitigate their impact on industrial operations. To achieve this, a secure network architecture and security protocols, such as encryption and authentication methods, need to be designed and implemented to ensure the safety and security of industrial operations.

3. COURSE OUTCOMES (COs)

The course outcomes for the Industrial Network Security syllabus for Instrumentation and Control Diploma Engineering can include:

1. Identify the Industrial Control Systems (ICS) and detail its operation.
2. Clarify the different types of ICS networks.
3. Explain Industrial Network Protocols.
4. Understand and establish security zones and conduits.
5. Explain and implement Network security and access controls.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme (In Hours)			Total Credits (L+T+P/2)	Examination Scheme				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	CA	ESE	CA	ESE	
3	0	2	4	30*	70	25	25	150

(*): Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

Legends: ***L****-Lecture; T – Tutorial/Teacher Guided Theory Practice; P -Practical; C – Credit,* ***CA*** *- Continuous Assessment;* ***ESE*** *-End Semester Examination.*

5. SUGGESTED PRACTICAL EXERCISES

The following practical outcomes (PrOs) are the subcomponents of the Course Outcomes (Cos). Some of the **PrOs** marked **'*'** are compulsory, as they are crucial for that particular CO at the 'Precision Level' of Dave's Taxonomy related to 'Psychomotor Domain'.

Sr. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. Required
1	To identify network assets, vulnerabilities, and potential attack surfaces using network mapping tools.	I	2
2	Using password cracking tools, assess the strength of passwords and identify weak passwords that could be exploited by attackers.	I	2
3	configure firewalls to protect network assets and prevent unauthorized access to critical systems.	II	2
4	configure VPNs to provide secure remote access to industrial networks.	II	2
5	configure and test intrusion detection and prevention systems to detect and block potential attacks on industrial networks.	II	2
6	Students will configure and test encryption and decryption methods, such as SSL/TLS, to secure network communications.	II	2
7	Compare different antivirus software to protect against APTs and weaponized malware.	III	2
8	develop and test incident response plans, including procedures for identifying and responding to security breaches.	III	2
7	Develop a business information management plan that includes guidelines for collecting and storing data, as well as protocols for sharing information across the organization.	III	2
8	Implement different network topologies, including bus, star, and ring topologies to understand their advantages and disadvantages.	III	2
9	Study the Foundation fieldbus networks.	III	2
10	Study the PROFIBUS networks.	IV	2
11	Develop a plan to implement an industrial network for a specific application.	IV	2
12	Study different network segmentation techniques to enhance network security.	IV	2
13	Implement different network services, including DHCP and DNS to optimize network performance and security.	IV	2
14	Implement wireless networks for industrial applications and analyze the potential security vulnerabilities associated with wireless networks.	V	2

15	Implement remote access to an industrial network and analyze the potential security risks associated with remote access.	V	2
16	Study different Performance Considerations: Latency, Jitter, Bandwidth, Throughput.	V	2
	Minimum 14 Practical Exercises		**28**

Note

*i. More **Practical Exercises** can be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.*

ii. Care must be taken in assigning and assessing study reports as it is a first year study report. Study report, data collection and analysis report must be assigned in a group. Teacher has to discuss the type of data (which and why) before the group starts their market survey.

The following are some **sample** 'Process' and 'Product' related skills (more may be added/deleted depending on the course) that occur in the above listed **Practical Exercises** of this course required which are embedded in the COs and ultimately the competency.

Sr. No.	Sample Performance Indicators for the PrOs	Weightage in %
1	Lab Record	05
2	Answer one question about Industrial Networks	10
3	Writing steps on any two (one each from Section – II, III)	15
4	Executing of two exercises	40
5	Result /Printout	10
6	Viva Performance	20
Total		**100**

6. MAJOR EQUIPMENT/ INSTRUMENTS REQUIRED

This major equipment with broad specifications for the PrOs is a guide to procure them by the administrators to the user in uniformity of practical's in all institutions across the state.

I. Computer
II. Network security software
III. Firewall, Virtual private network (VPN)
IV. Router, Switch
V. Physical security equipment

7. 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 fulfill the development of this course competency.

a) Work as a leader/ team member.
b) Follow safety practices while using electrical, electronics, pneumatic instruments and tools.
c) Realize the importance of security zones in Industrial Networks.

The ADOs are best developed through laboratory/field-based exercises. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

i. Valuing Level in 1st year
ii. Organization Level in 2nd year.
iii. Characterization Level in 3rd year.

8. UNDERPINNING THEORY

The major underpinning theory is given below based on the higher level UOs of Revised Bloom's taxonomy that is formulated for the development of COs and competency. If required, more such UOs could be included by the course teacher to focus on the attainment of COs and competency.

Unit	Unit Outcomes (UOs) (4 to 6 UOs at different levels)	Topics and Sub-topics
Unit-I **INTRODUCTION TO ICS AND OPERATIONS**	1a. What is an industrial control system (ICS)? 1b. List common industrial security recommendations. 1c. Distinctions Between Common Advanced Persistent Threats (APT) and Weaponized Malware. 1d. What are the different types of assets? 1e. Explain different system operations to automate industrial operations. 1f. Explain how process management works.	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 1.4 System operations: Control loops, control processes, feedback loops, production information management, business information management1.5 Process management
Unit-II **ICS NETWORK DESIGN AND ARCHITECTURE**	2a. What is Industrial Networking? 2b. Write differences in Industrial Network Architectures by Function. 2c. Write and explain common topologies for Industrial Networking. 2d. Explain Network Segmentation. 2e. Explain Network Services. 2f. What are Wireless Networks?	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

	2g. Explain Wireless Network. 2h. Explain remote access. 2i. Explain different types of performance considerations. (Latency, Jitter, Bandwidth, Throughput, Type of Service, Class of Service, Quality of Service, Network Hops)	2.6 Wireless Networks 2.7 Remote Access 2.8 Performance Considerations: Latency, Jitter, Bandwidth, Throughput, Type of Service, Class of Service, Quality of Service, Network Hops
Unit-III **INDUSTRIAL NETWORK PROTOCOLS**	3a. Describe Industrial Network Protocols. 3b. Explain different fieldbus protocols in brief. 3c. Draw and explain the Modbus alignment with OSI 7-Layer model. 3d. Explain different backend protocols in brief. 3e. Describe OPC client–server communications.	3.1 Overview of Industrial 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 3.5 Industrial Protocol Simulators
Unit-IV **ESTABLISHING ZONES AND CONDUITS**	4a. Explain security zones and conduits in detail. 4b. How to identify various types of security zones and conduits? Also, classify them. 4c. Write about Recommended Security Zone Separation. 4d. Write the procedure for Establishing Security Zones and Conduits.	4.1 Security Zones and Conduits 4.2 Identifying and Classifying Security Zones and Conduits 4.3 Recommended Security Zone Separation 4.4 Establishing Security Zones and Conduits
Unit-V **IMPLEMENTING SECURITY AND ACCESS CONTROLS**	5a. Write the Implementation of Network Security Controls. 5b. Write about Implementing Host Security and Access Controls. 5c. How Much Security is Enough? Justify your answer.	5.1 Implementing Network Security Controls 5.2 Implementing Host Security and Access Controls 5.3 How Much Security is Enough?

9. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	INTRODUCTION TO ICS AND OPERATIONS	8	7	7	2	**14**
II	IICS NETWORK DESIGN AND ARCHITECTURE	8	4	7	3	**14**
III	INDUSTRIAL NETWORK PROTOCOLS	10	4	7	3	**16**
IV	ESTABLISHING ZONES AND CONDUITS	8	4	7	3	**14**
V	IMPLEMENTING SECURITY AND ACCESS CONTROLS	8	4	5	3	**12**
	Total	**42**	**23**	**33**	**14**	**70**

Legends: *R=Remember, U=Understand, A=Apply and above (Revised Bloom's taxonomy)*

10. 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 perform following activities in group and prepare reports of about 5 pages for each activity. They should also collect/record physical evidences for their (student's) portfolio which may 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.

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various outcomes in this course:

a) Massive open online courses (***MOOCs***) may be used to teach various topics/ subtopics.
b) Guide student(s) in undertaking micro-projects.
c) ***'L' in section No. 4*** means different types of teaching methods that are to be employed by teachers to develop the outcomes.
d) 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.
e) With respect to ***section No.10***, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.
f) Introduce Industrial cyber security laws and Network protocols among the students.
g) Helping the students to understand the concepts of the world wide web (WWW) and the Internet.

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her in the beginning of the semester. In the first four semesters, the micro-projects are group-based (group of 3 to 5). However, **in the fifth and sixth semesters**, the number of students in the group should ***not exceed three.***

The micro-project could be industry application based, internet-based, workshop-based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. Each student will have to maintain a dated work diary consisting of individual contributions in the project work and give a seminar presentation of it before submission. The duration of the micro project should be about **14-16** ***(fourteen to sixteen) student engagement hours*** during the course. The students ought to submit micro-project by the end of the semester to develop the industry-oriented COs.

A suggestive list of micro-projects is given here. This has to match the competency and the COs. Similar micro-projects could be added by the concerned course teacher:

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

13. 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

14. SOFTWARE/ LEARNING WEBSITES

- Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs)
- Human-Machine Interfaces (HMIs) and Supervisory Control and Data Acquisition (SCADA) systems
- Network switches, routers, and firewalls
- Network analyzers and protocol analyzers
- Vulnerability scanners and penetration testing tools
- Security information and event management (SIEM) software
- Industrial protocol simulators
- Wireless access points and network adapters
- Ethernet cables and connectors

15. PO-COMPETENCY-CO MAPPING

Semester V	Industrial Network Security (Course Code : 4351708)						
	POs						
Competency & Course Outcomes	**PO 1 Basic & Discipline specific knowledge**	**PO 2 Problem Analysis**	**PO 3 Design/ develop-ment of solutions**	**PO 4 Engineering Tools, Experimen-tation & Testing**	**PO 5 Engineering practices for society, sustainability & environment**	**PO 6 Project Manage-ment**	**PO 7 Life-long learning**
Competency	The fundamentals of industrial network security involve understanding the various cyber threats and vulnerabilities associated with industrial control systems (ICS). Potential cyber risks to ICS need to be identified and analyzed to mitigate their impact on industrial operations.						
Course Outcomes CO 1) Identify the Industrial Control Systems (ICS) and detail its operation.	2	-	-	1	2	-	1
CO 2) Clarify the different types of ICS networks.	2	-	-	1	-	-	1
CO 3) Explain Industrial Network Protocols.	2	-	-	1	-	-	1
CO 4) Understand and establish security zones and conduits.	2	-	-	1	1	-	1
CO 5) Explain and implement Network security and access controls.	2	-	-	1	1	-	1

*Legend: '**3**' for high, '**2**' for medium, '**1**' for low and '**-**' for no correlation of each CO with PO.*

16. COURSE CURRICULUM DEVELOPMENT COMMITTEE

Member – Board of Studies (GTU), Electrical and Allied branches

Prof. Suresh Z. Shyara, IC Engineering, AVPTI, Rajkot.

Prof. Mahesh J. Vadhavaniya, IC Engineering, Government Polytechnic, Palanpur.

GTU Resource Persons

Prof. M. S. Gohil, IC Engineering, Government Polytechnic, Gandhinagar.

Prof. D. J. Modi, IC Engineering, Government Polytechnic, Palanpur.