Reg. No.															

Question Paper Code	13400

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Eighth Semester

Electronics and Instrumentation Engineering

20EIEL801 - CYBER SECURITY FOR INDUSTRIAL AUTOMATION

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Which of the following is not a component of physical security? (a) Access Controls (b) Surveillance Systems (c) Data Encryption (d) Security Personnel	1	K1	CO1
2.	What is the final step in a successful cyberattack? (a) Reconnaissance (b) Exploitation (c) Command and Control (d) Actions on Objectives	1	K1	CO1
3.	How are risks typically classified in cybersecurity? (a) Operational and Strategic (b) High, Medium, and Low (c) Internal and External (d) All of the above	1	K1	CO2
4.	Which of the following is NOT a method of risk treatment? (a) Risk Avoidance (b) Risk Transfer (c) Risk Acceptance (d) Risk Aggravation	1	K1	CO2
5.	Which of the following is crucial for generating cybersecurity information for IACS? (a) Network Traffic Analysis (b) Financial Audits (c) Employee Training Programs (d) Customer Feedback Surveys	1	K1	CO3
6.	What is the purpose of a risk assessment in the context of IACS cybersecurity? (a) To evaluate the potential impact of identified risks on the system (b) To increase network speed (c) To streamline production processes (d) To train employees	1	K1	CO3
7.	What is the primary goal of the cybersecurity lifecycle? (a) To develop new software (b) To protect information systems from cyber threats (c) To increase network speed (d) To reduce operational costs	1	K1	CO4
8.	During the detailed design process, which document is typically created to guide implementation? (a) Security Policy (b) Incident Response Plan (c) Design Specification Document (d) Risk Assessment Report	1	K1	CO4
9.	During which phase of incident response is the root cause of the incident analyzed? (a) Containment (b) Eradication (c) Recovery (d) Post-incident analysis	1	K1	CO5
10.	Which document outlines the steps to be taken during an incident response? (a) Incident Response Plan (b) Disaster Recovery Plan (c) Business Continuity Plan (d) Security Policy	1	K1	CO5

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	Differentiate between IACS culture and IT paradigms.	2	K2	CO1
12.	Explain the concept of external threat sources.	2	K2	CO1
13.	What is the significance of the final step in a cyberattack?	2	K1	CO1
14.	Describe network segmentation and its benefits in cybersecurity.	2	K2	CO2
15.	How are risks classified in cybersecurity?	2	K1	CO2
16.	What is the purpose of having security policies in an organization?	2	K1	CO2

17.	Identify the importance of evaluating realistic threat scenarios in IACS to determine vulnerabilities and potential risks.	*2*	*K2*	*CO3*
18.	Why is network traffic analysis crucial for generating cybersecurity information for IACS?	*2*	*K1*	*CO3*
19.	What is the primary goal of the cybersecurity lifecycle?	*2*	*K1*	*CO4*
20.	Describe the purpose of the Yokogawa Virus Check Service.	*2*	*K2*	*CO4*
21.	Name a common activity performed during Cybersecurity FAT.	*2*	*K1*	*CO5*
22.	What is the primary goal of the recovery phase in incident response?	*2*	*K1*	*CO5*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Explain the significance of the Industrial Security Environment in modern industrial operations.	*11*	*K2*	*CO1*
		OR			
	b)	Discuss the impact of the installation step in a cyberattack on industrial systems.	*11*	*K2*	*CO1*
24.	a)	Examine the impact of environmental security controls on the reliability of industrial automation systems. Identify potential challenges and solutions.	*11*	*K4*	*CO2*
		OR			
	b)	Analyze the impact of various network segmentation strategies on mitigating cyber threats in industrial automation. Construct a comparative model to interpret their effectiveness	*11*	*K4*	*CO2*
25.	a)	Explain the process of identifying the scope of Industrial Automation and Control Systems (IACS) and why it is critical for cybersecurity assessment.	*11*	*K2*	*CO3*
		OR			
	b)	Summarize the process of conducting a gap assessment in IACS cybersecurity. What are the key areas typically assessed during this process?	*11*	*K2*	*CO3*
26.	a)	Describe the key components of a firewall design. What are the main considerations when implementing a firewall in an industrial automation network?	*11*	*K2*	*CO4*
		OR			
	b)	Illustrate how a detailed design process is developed for a cybersecurity project. Provide an example of how detailed technical specifications are created and implemented.	*11*	*K2*	*CO4*
27.	a)	Describe the process and significance of Cybersecurity Factory Acceptance Testing (FAT). How does it differ from Site Acceptance Testing (SAT)?	*11*	*K2*	*CO5*
		OR			
	b)	Explain the importance of developing a cybersecurity test plan. Discuss its key components and how they contribute to the overall security testing process.	*11*	*K2*	*CO5*
28.	a) (i)	Compare and analyze the effectiveness of different intrusion detection methods (e.g., anomaly-based, signature-based) in detecting and mitigating cyber threats.	*6*	*K4*	*CO4*
	(ii)	What are the common network diagnostic tools used in cybersecurity?	*5*	*K2*	*CO5*
		OR			
	b) (i)	Analyze the effectiveness of Yokogawa's integrated security solutions in managing cybersecurity risks for industrial automation.	*6*	*K4*	*CO4*
	(ii)	Discuss the role of cybersecurity audits in an organization's security strategy.	*5*	*K2*	*CO5*