Reg. No															

B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Seventh Semester

18EIE401T - CYBER SECURITY FOR INDUSTRIAL AUTOMATION

(For the candidates admitted during the academic year 2020 - 2021 & 2021 - 2022)

Note:

i. **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

ii. **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours **Max. Marks: 100**

PART - A (20 × 1 = 20 Marks)

Answer **all** Questions

		Marks	BL	CO
1.	According to ANSI/ISA-99.00.01, "a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process" is an: (A) Industrial automation and control system (B) Distributed control system (C) Discrete control system (D) Programmable logic controller	1	1	1
2.	A "type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems" is defined by ANSI/ISA-99.00.01 as which of the following? (A) Distributed control system (B) SCADA system (C) Safety instrumented system (SIS) (D) Human-machine interface (HMI)	1	1	1
3.	Which one of the following items is NOT a component of a classical SCADA system model? (A) Human-machine interface (HMI) (B) Remote terminal unit (RTU) (C) Enterprise resource planning (ERP) (D) Programmable logic controller (PLC)	1	1	1
4.	Which of the following is NOT a characteristic of a SCADA master terminal unit (MTU)? (A) Has two-way communication with field devices (B) Usually located at the master control center (C) Has high-bandwidth communication requirements (D) Communicates through telephone, VHF/UHF radio, spread spectrum radio, satellite, and/or microwave	1	1	1
5.	Information system security is defined as comprising which of the following three basic elements? (A) Confidentiality, integrity, and authorization (B) Confidentiality, integrity, and availability (C) Audit, integrity, and availability (D) Security, integrity, and availability	1	1	2
6.	Protecting documents and messages from unauthorized disclosure refers to which of the following? (A) Confidentiality (B) Availability (C) Authorization (D) Integrity	1	1	2

7. An attack that overloads the resources of a computing system is an attack against which of the following? 1 1 2

(A) Integrity
(B) Availability
(C) Confidentiality
(D) Authentication

8. Which of the following items refers to the act of verifying a user's identity and confirming that a user is who he or she professes to be? 1 1 2

(A) Authentication
(B) Authorization
(C) Registration
(D) Accountability

9. Which of the following statements is generally TRUE regarding an industrial automation and control system? 1 1 3

(A) Installation of software patches can be performed routinely and frequently.
(B) Encryption of data can sometimes lead to problematic delays.
(C) Penetration testing can be conducted routinely and frequently.
(D) Confidentiality is a key concern in automation systems as opposed to integrity and availability.

10. In both IT and automation and control systems, which of the following is the primary concern in the event of an emergency or malicious event? 1 1 3

(A) Equipment safety
(B) Preservation of documentation
(C) Personnel safety
(D) Facility protection

11. Which of the following statements is FALSE? 1 1 3

(A) Flash drives and other portable memory devices can be sources of malware injections into control systems.
(B) Maintenance hooks and trap doors installed in automation and control systems for remote maintenance can be easy entry points to modify critical software and firmware with negative consequences.
(C) In many control system environments, control engineers, in general, do not have multiple responsibilities, such that the security principle of separation of duties is not normally violated.
(D) Many facilities house legacy systems with outdated technology, minimal memory and computing power, and little thought to security.

12. Which of the following actions is the most likely to result in blockages and lack of system availability in automation and control systems? 1 1 3

(A) Remote access
(B) Life cycle design
(C) Accountability
(D) Port scanning

13. In ANSI/ISA-99.00.01-2007, a "potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm," is which of the following? 1 1 4

(A) Threat
(B) Vulnerability
(C) Weakness
(D) Risk

14. The "expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence" is which of the following? 1 1 4

(A) Consequence
(B) Threat source
(C) Weakness
(D) Risk

15. The program and supporting processes to manage information security risk to organizational operations (i.e., mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation are defined as which of the following? 1 1 4

(A) Risk assessment (B) Risk management
(C) Risk mitigation (D) Risk association

16. The ANSI/ISA-99.02.01-2009 Cybersecurity Management System (CSMS) comprises which of the following three main categories? 1 1 4

(A) Risk analysis, addressing the risk, and monitoring and improving the CSMS
(B) Risk mitigation, addressing the risk, and monitoring and improving the CSMS
(C) Risk analysis, addressing the risk, and monitoring and improving the automation system
(D) Risk analysis, eliminating the risk, and monitoring and improving the CSMS

17. The controls of ANSI/ISA-TR99.00.01-2007 are organized into six categories. Which of the following is NOT one of those categories? 1 1 5

(A) Encryption Technologies and Data Validation
(B) Risk Mitigation Technologies
(C) Authentication and Authorization Technologies
(D) Filtering/Blocking/Access Control Technologies

18. ANSI/ISA-TR99.00.01-2007 describes which of the following as "the initial step in protecting an industrial automation and control system (IACS) and its critical assets from unwanted breaches. It is the process of determining who and what should be allowed into or out of a system"? 1 1 5

(A) Authorization (B) Authentication
(C) Identification (D) Confirmation

19. Which of the following are the major components of authentication and authorization technologies spelled out in ANSI/ISA-TR99.00.01-2007? 1 1 5

(A) Role-based, password, and challenge response
(B) Rule-based, user ID, and challenge response
(C) Role-based, password, and call-back
(D) Rule-based, password, and call-back

20. Which of the following does ANSI/ISA-TR99.00.01-2007 identify as the three main types of software that have to be considered in industrial automation and control system software? 1 1 5

(A) Mobile operating systems, real-time and embedded operating systems, and Web servers and Internet technologies
(B) Server and workstation operating systems, real-time and embedded operating systems, and wireless technologies
(C) Server and workstation operating systems, real-time and embedded operating systems, and Web servers and Internet technologies
(D) Server and workstation operating systems, real-time and embedded operating systems, and mobile technologies

PART - B (5 × 4 = 20 Marks) Marks BL CO

Answer **any 5** Questions

21. Explain the types of automation 4 2 1
22. Describe the term authentication and authorization of information system security 4 2 2
23. Explain any two threat actions in IACS based on NIST standard 4 2 3
24. Show the structure of multi-tiered risk management approach in IACS 4 2 4

25.	Explain the functions of technical control as defined by NIST standard	4	2	5
26.	Summarize high power electromagnetic threats in smart grid application	4	2	4
27.	Show the structure of IACS cybersecurity lifecycle	4	2	5

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

		Marks	BL	CO
28.	(a) (i) Describe the structure of Safety Instrumented Systems(SISs) of IACS with neat sketch. (ii) Summarize the issues in IACS Security. **(OR)** (b) Summarize the industrial automation and control system protocols.	12	2	1
29.	(a) Illustrate different types of cryptography technologies used in information system security with neat sketch. **(OR)** (b) Illustrate the concept of digital signature and Virtual Private Network (VPN) with neat sketch.	12	4	2
30.	(a) (i) Summarize the factors to be considered in adapting IT security methods to IACS. (ii) Differentiate IT and IACS from a standards perspective. **(OR)** (b) Summarize the emerging technological trends and associated concerns that directly and indirectly affect the IACS landscape.	12	2	3
31.	(a) Summarize the NIST 800-39 integrated enterprise risk management system with neat sketch. **(OR)** (b) Explain any two types of harmful threats to IACS.	12	2	4
32.	(a) Describe the cybersecurity lifecycle of a IACS with neat sketch. **(OR)** (b) Summarize the ANSI/ISA security technologies for IACS.	12	2	5

* * * * *