Reg. No															

Minor CERTIFICATION EXAMINATION, NOVEMBER 2023

Third Semester

18EIE010T - CYBER SECURITY FOR INDUSTRIAL AUTOMATION

(For the candidates admitted during the academic year (2018-2019 to 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.	Which of the following are versions of Profibus? (A) Profibus PA, Profibus CP, Profibus CIP (B) Profibus PA, Profibus DP, Profibus FMS (C) Profibus PA, Profibus CP, Profibus FMS (D) Profibus PA, Profibus CIP, Profibus FMS	1	1	1
2.	Which layer of the OSI model converts packets into electrical or optical signals for sending on the transmission media? (A) Application (B) Presentation (C) Physical (D) Session	1	1	1
3.	ANSI/ISA-84.00.01-2004 Part 1(IEC 61511-1 Mod) defines which of the following as an "instrumented system used to implement one or more safety instrumented functions (SIF)"? (A) Safety surety system (B) Failure proof system (C) Safety instrumented system (D) Safety function system	1	1	1
4.	ANSI/ISA-99.00.01-2007 defines which of the following as "a type of control system in which the system elements are dispersed but operated in a coupled manner?" (A) Distributed control system (B) Discrete control system (C) Dispersed control system (D) Coupled control system	1	1	1
5.	A VPN that provides secure communications over a public network between two trusted networks is known as which of the following? (A) Host-to-host (B) Gateway-to-gateway (C) Host-to-gateway (D) Host-to-demilitarized zone	1	1	2
6.	IPsec provides which of the following two modes of operation? (A) Symmetric key mode and transport mode (B) Authentication mode and tunnel mode (C) Transport mode and tunnel mode (D) Transport mode and transparent mode	1	1	2
7.	A private network that operates as an overlay on a public infrastructure is known as which of the following? (A) Virtual private network (B) Dual band network (C) 4G network (D) Demilitarized zone	1	1	2
8.	A cryptographic attack in which the attacker has access to multiple samples of encrypted messages that have been encrypted with the same algorithm and attempts to find the key is known as which of the following? (A) Chosen ciphertext (B) Ciphertext only (C) Adaptive chosen ciphertext (D) Known plaintext	1	1	2

9. Which of the following can lead to a single point of failure in an industrial automation and control system? 1 1 3
(A) Separation of duties
(B) Disk redundancy
(C) Combination of safety and security mechanisms
(D) Use of authentication with identification

10. What is a detective control that is more frequently applied in IT systems than in control and automation systems? 1 1 3
(A) Firewall
(B) Separation of duties
(C) Bio-metrics
(D) Auditing

11. In Smart Grid Terminology, DER stands for which of the following terms? 1 1 3
(A) Delayed energy reduction
(B) Determined energy requirements
(C) Distributed energy requirements
(D) Distributed energy resources

12. What subsystem of the Smart Grid comprises hardware and meter data management (MDM) software that provide the normal meter reading functions as well as supporting two-way communications that can exchange energy information and commands with customer's devices through a home area network? 1 1 3
(A) Advanced Metering Infrastructure (AMI)
(B) Energy Management System (EMS)
(C) Energy Services Interface (ESI)
(D) Smart Grid Interface (SGI)

13. Which of the following is NOT true regarding Stuxnet? 1 1 4
(A) Attacks both networked and non-networks PCs
(B) Installs device drivers using valid, digital certificates
(C) Infects Apple Macintosh computers
(D) Infection is accomplished through USB flash drives

14. Which of the following is NOT characteristic of an insider threat? 1 1 4
(A) Many insider attacks are conducted by disgruntled insiders
(B) Most insider attacks do not result in serious losses or harm
(C) Many insider attacks are conducted remotely
(D) Many inside attackers have privileged access to computer systems

15. Which of the following groups of elements is presented in NIST SP 800- 37 to manage risk? 1 1 4
(A) Categorize, Select, Implement, Authorize
(B) Categorize, Evaluate, Implement, Monitor
(C) Determine, Select, Implement, Authorize
(D) Determine, Evaluate, Implement, Monitor

16. According to NIST SP 8000-37, which of the following "provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle?" 1 1 4
(A) Risk Monitoring Framework (RMF)
(B) Risk Assessment Framework (RAF)
(C) Risk Management Framework (RMF)
(D) Risk Evaluation Framework (REF)

17. 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

18. 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

19. 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

20. In ANSI/ISA-TR99.00.01-2007, what are the three main categories of physical security elements? 1 1 5

(A) Active, identification and monitoring devices, and passive
(B) Active, real-time, and passive
(C) Active, identification and monitoring devices, and real-time
(D) Reactive, identification and monitoring devices, and passive

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 steps involved in automation installation 4 2 1
23. Describe the term authentication and authorization of information system security 4 2 2
24. Explain any two threat actions in IACS based on NIST standard 4 2 3
25. Show the structure of multi-tiered risk management approach in IACS 4 2 4
26. Explain the functions of technical control as defined by NIST standard. 4 2 5
27. Summarize high power electromagnetic threats in smart grid application 4 2 4

PART - C (5 × 12 = 60 Marks) — Marks BL CO

Answer **all** Questions

28. (a) (i) Describe the structure of Safety Instrumented Systems(SISs) of IACS with neat sketch. 12 2 1
(ii) Summarize the issues in IACS Security.

(OR)

(b) Explain the block diagram of SCADA and DCS with neat sketch.

29. (a) Outline the terminologies of Information System Security. 12 4 2

(OR)

(b) Illustrate the different types of firewalls used in information system security with neat sketch.

30. (a) (i) Summarize the factors to be considered in adapting IT security methods to IACS. 12 2 3
(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.

31.	(a) Explain any two types of harmful threats to IACS.	12	2	4
	(OR)			
	(b) Summarize the NIST 800-39 integrated enterprise risk management system with neat sketch.			
32.	(a) Describe the cybersecurity lifecycle of a IACS with neat sketch.	12	2	5
	(OR)			
	(b) Summarize the ANSI/ISA security technologies for IACS.			

* * * * *