

Seat No.: _____

Enrolment No. _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Tech. Cyber Security - Semester - II - August-2022

Subject Code: CTMTCS SII P5 EL5

Subject Name: Critical Infrastructure Security

Time: 11:00 AM to 02:00 PM

Date: 05-08-2022

Total Marks: 100

Instructions:

1. Write down each question on separate page.
2. Attempt all questions.
3. Make suitable assumptions wherever necessary.
4. Figures to the right indicate full marks.

- | | Marks |
|--|-------|
| Q.1 (a) Explain the third generation of SCADA. | 04 |
| (b) Draw and Explain two firewall DMZ architecture. | 04 |
| (c) Write a detailed note on Control Theory. | 08 |
| OR | |
| Write a detailed note on PLC. | |
| (d) Illustrate the detailed difference between normal IT Security and OT security on some of the parameters. | 09 |
| | |
| Q.2 (a) Draw the typical SCADA / ICS Architecture | 04 |
| (b) Discuss the Cross Site Scripting and how it can affect ICS environment. | 04 |
| (c) Discuss the history of ICS from ancient time to modern time. | 08 |
| (d) Draw the ladder diagram for follow: | 09 |
| 1) Two motors are controlled with one button | |
| 2) After 25 minutes of both the motors turned on, the third motor should start. | |
| 3) After starting of third motor for 15 minutes every thing shall be shutdown. | |
| 4) May use kill switch. | |
| OR | |
| Write a detailed note on DNP3. | |
| | |
| Q.3 (a) State the difference between Modbus and DNP3. | 04 |
| OR | |
| Discuss the tables of modbus protocol. | 04 |
| (b) Write the full form of the following: | |
| - ICS | |
| - CSIRT | |
| - DLL | |
| - CVE | |
| (c) Explain the message passing in modbus protocol with diagram. | 08 |
| (d) Write a detailed and real world ICS malware case study. | 09 |
| | |
| Q.4 (a) What is CIA triad in ICS and why? | 04 |
| OR | |
| What is Risk Management in ICS. | 04 |
| (b) Explain four functions of control system. | 08 |
| (c) Discuss penetration testing strategies in detail. | |