

# National Forensic Sciences University

## School of Cyber Security and Digital Forensics

Course Name: M. Sc. CS & M.Sc. DFIS (Batch: 2023-25)

Sem - III

Exam: MSE

Subject Code: CTMSDFIS III P4

Time: 3:30 pm to 05.00 pm

Subject Name: Critical Infrastructure Security

Date: 02-11-2023

Total Marks: 50

Student Name: \_\_\_\_\_

Enroll. No.: \_\_\_\_\_

(40 Marks)

Q1) Answer the following (Any 8)

Full form of the following: i) SCADA ii) ICS iii) DCS iv) HMI v) IACS

State the use of SCADA in Petroleum Industry.

You are training a team of Intern, where one Intern asks about SCADA and what Local Control Systems means. Give a brief idea on the asked questions.

What is DNP3? Discuss about common input and output data being transferred.

Answer:

- The data rate between RTU & Controlled Devices is High. (Select from High or Low)
- In DNP3 addressing 12 no of addresses are reserved for special needs in future.
- Higher the data rate, loop operates in close control mode. (Select from Open or Close)
- DNP3 is a Non protocol (proprietary / non-proprietary)
- According to the PURDUE Model, which levels fall under Process Control Zone? (Just write Level No & Names)

Differentiate IT vs OT.

Explain the task of Link Layer, Transport Layer & Application Layer in DNP3 (TCP/IP Layering)

Explain DNP3 Frame. Source (RTU) Destination (PLC)

- Explain the security features and measures provided by DNP3 through the concept of layering to mitigate cyber threats and ensure data integrity. - CRC
- The organization needs SCADA to be implemented, kindly discuss its use cases along with its advantages and challenges to the organization as an expert in the field of SCADA.

Q2) Explain SCADA Referential Architecture with all suitable layers.

(10 Marks)

