Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - III - January-2023

Subject Code: CTMSCS SIII P4 EL3 **Date: 12-01-2023**

Subject Name: Critical Infrastructure Security

Time: 11:00 AM to 02:00 PM **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)	How does PLC Scan process works?	04
	(b)	Draw any typical Industrial Control System with proper labels.	04
	(c)	Write a detailed note on Firewall and put emphasis on Demilitarize Zone to protect ICS.	08
		OR	
	(c)	Illustrate the importance of Cyber Security in Critical Infrastructure Security.	08
	(d)	Discuss detailed real world case-study related to Critical Infrastructure Hacks.	09
Q.2	(a)	Explain Black-Box Testing strategies.	04
	(b)	What are the characteristics of RTU?	04
	(c)	Draw and Explain Purdue Model of ICS in detail.	08
	(d)	Reliance has oil refinery at Jamnagar, They are able to process 10k barrel crude oil in a day with three plants. They want to increase the strength by putting the fourth plant in the refinery. Now you are appointed as PLC Programmer to program the processes step by step. The process is as below: 1) Start the button 2) Crude will go to the container by motor 3) Temperature should be maintained on 2000 degree Celsius. 4) After 30 minutes in first container the crude should go to another container for 20 minutes and then to third container for final procedure, but the condition is the crude should be processed with first two container in order to go in the third one. Once third container processed the crude into oil within 60 minutes, it should go to the storage area for cool down.	09
		OR	
	(d)	Write a detailed note on DNP3.	
Q.3	(a)	Explain buffer overflow briefly.	09
		OR	
	(a)	Explain four functions of control system.	04
	(b)	Write the full form of the following: - DCS - ENISA	04 04

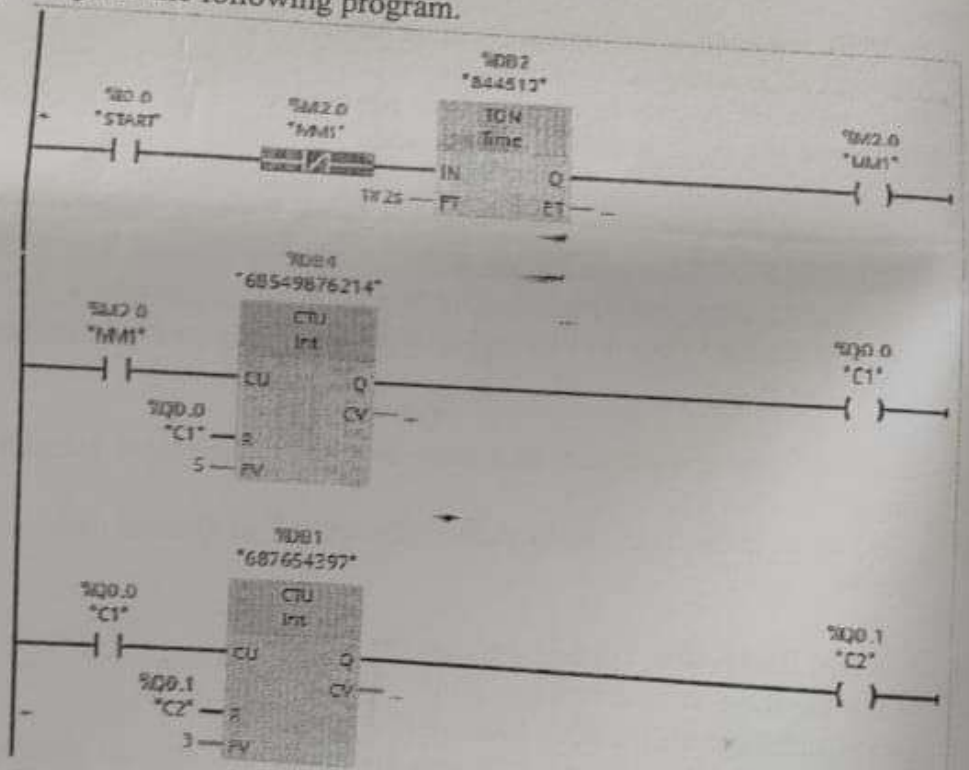
- SCADA
- NIST

(c) Write a detailed note on Control Theory. 08
(d) Write a detailed note on Modbus Protocol. 09

Q.4 (a) What are various attack vectors for ICS/SCADA. 09

OR

(a) What is CIA triad in ICS and why? 04
(b) Explain any four syntax of ladder logic with description. 04
(c) Discuss the importance of Security Standards for ICS and also explain one of the standard briefly. 04
(d) Explain the following program. 08



*****

Q.3

Q.4

Q.5

Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics & Information Security - Semester - 3 - Jan-2023

Subject Code: CTMSDFIS SIII P4 EL1 **Date:** 12/01/2023

Subject Name: Critical Infrastructure Security & forensics

Time: 11:00 AM to 02:00 PM **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)	Discuss the concept of Local Control System with appropriate diagram.	05
	(b)	Discuss the associated risk of SCADA systems.	06
	(c)	Differentiate between IT and OT Systems.	07
Q.2		Answer any three (03)	18
	(a)	What is Modbus Protocol? Explain the Architecture with a suitable diagram and discuss the data storage in standard Modbus.	
	(b)	Discuss the difference between Black Box, White Box and Gray Box Penetration Testing.	
	(c)	Discuss any one Incident of SCADA Attack & the mitigation techniques.	
	(d)	Discuss NERC CIP ICS Cyber Security Standard.	
Q.3		Answer any two (02)	14
	(a)	Explain ICS Cyber Kill Chain.	
	(b)	Discuss the Asset Identification & Characterization Stage of ICS Risk Assessment Process.	
	(c)	Discuss SP 800 – 82 ICS Cyber Security Standard.	
Q.4	(a)	State the full form of below stated key terms: i) SCADA ii) ICS iii) DCS iv) IACS v) CIS	05
	(b)	What are the major categories of ICS from functional point of view?	06
	(c)	Discuss the applications of SCADA Systems with examples.	07
Q.5		Answer any three (03)	18
	(a)	What is DNP3? Explain the request – response model with accepted inputs & outputs.	
	(b)	Discuss the function code stack in Modbus.	
	(c)	Discuss Packet Filtering Firewall.	
	(d)	Discuss Stateful Inspection & Proxy Firewall.	

Q.6 Answer any two (02) 14

(a) Explain SCADA System Architecture – PURDUE Model.

(b) Discuss various components of ICS.

(c) Discuss the Vulnerability Identification & Threat Modelling Stage of ICS Risk Assessment Process.