IIOT Application in Cyber Security (Manufacturing)

Unit Code: ASC/N6462

Version: 1.0

NSQF Level: 5.5

Automotive Skills Development Council || 153, GF, Okhla Industrial Area, Phase 3
New Delhi 110020 || email:garima@asdc.org.in

Description

An Individual at this job will be Ensuring Cybersecurity by Develop and enforce cybersecurity policies, protocols, and standards for IIoT applications in manufacturing environments

Scope

The scope covers the following :

- Deploy IIOT Sensors into Manufacturing Entities Via Secured Communication Networks.
- Collect & Monitor the Status of Manufacturing Entities as per network security design.
- Installation of application layer & Perform threat assessment

Elements and Performance Criteria

Deploy IIOT Sensors into Manufacturing Entities Via Secured Communication Networks

To be competent, the user/individual on the job must be able to:

PC1. select appropriate industrial software (networking window) as per the project requirements.

PC2. Perform appropriate core and auxiliary support process as per the project document

PC3. Integrate security parameters for data present in edge computing devices, cloud platforms, open-source databases

PC4. define the manufacturing entities based on criticality and security threat levels in network security architecture

Collect & Monitor the Status of Manufacturing Entities as per network security design

To be competent, the user/individual on the job must be able to:

PC5. monitor the communication status & behavior of edge & cloud computing devices present in the IIOT network by using monitoring applications.

PC6. monitor the status of field and control device in the IIOT network.

PC7. interpret the field & control device status with edge computing device data on the dashboard

Installation of application layer & Perform threat assessment

To be competent, the user/individual on the job must be able to:

PC8. evaluate criticality and security of threat levels of manufacturing entities.

PC9. analyze data security performance metrics to highlight the threats in comparison with network security parameters

PC10. maintain and update the communication status of physical systems in the manufacturing process.

PC11. implement regular threat assessment across devices to strengthen resistance against attack.

PC12. Maintain the threat Assessment Record & Recovery Plan

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. Organization procedures for health, safety and security, individual role and responsibilities in this context.

KU2. Organization's emergency procedures for different emergency situations and the importance of following the same.

KU3. Understanding the fundamentals of IIoT, including sensor technologies, data communication protocols, edge computing, and cloud integration

KU4. Familiarity with different types of sensors used for monitoring manufacturing assets and the principles of data acquisition.

KU5. Understanding of data transmission protocols, edge computing concepts, and their applications in IIoT.

KU6. Knowledge of cyber security principles, encryption methods, and access controls for securing IIoT data.

KU7. Understanding of SCADA, ERP, and other manufacturing systems and their integration with IIoT applications.

KU8. Awareness of data privacy regulations, industry standards, and compliance requirements

KU9. Data Transmission Protocols like MODBUS, Ethernet.

KU10. Understanding of factors influencing scalability in IIoT applications

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. read safety instructions/guidelines

GS2. modify work practices to improve them

GS3. work with supervisors/team members to carry out work related tasks

GS4. Complete tasks efficiently and accurately within stipulated time

GS5. inform/report to concerned person in case of any problem

GS6. make timely decisions for efficient utilization of recourses

GS7. write reports such as accident report, in at least English/regional language

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Deploy IIOT Sensors into Manufacturing Entities Via Secured Communication Networks	**15**	**15**	**-**	**6**
PC1. select appropriate industrial software (networking window) as per the project requirements.	5	5	-	2
PC2. Perform appropriate core and auxiliary support process as per the project document	5	5	-	2
PC3. Integrate security parameters for data present in edge computing devices, cloud platforms, open-source databases	2	2	-	1
PC4. define the manufacturing entities based on criticality and security threat levels in network security architecture	3	3	-	1
Collect & Monitor the Status of Manufacturing Entities as per network security design	**14**	**14**	**-**	**8**
PC5. monitor the communication status & behavior of edge & cloud computing devices present in the IIOT network by using monitoring applications.	5	5	-	3
PC6. monitor the status of field and control device in the IIOT network.	4	4	-	2
PC7. interpret the field & control device status with edge computing device data on the dashboard	5	5	-	3
Installation of application layer & Perform threat assessment	**11**	**11**	**-**	**6**
PC8. evaluate criticality and security of threat levels of manufacturing entities.	3	2	-	2
PC9. analyze data security performance metrics to highlight the threats in comparison with network security parameters	2	3	-	1
PC10. maintain and update the communication status of physical systems in the manufacturing process.	2	2	-	1

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC11. implement regular threat assessment across devices to strengthen resistance against attack.	2	2	-	1
PC12. Maintain the threat Assessment Record & Recovery Plan	2	2	-	1
NOS Total	**40**	**40**	**-**	**20**

National Occupational Standards (NOS) Parameters

NOS Code	ASC/N6462
NOS Name	IIOT Application in Cyber Security (Manufacturing)
Sector	Automotive
Sub-Sector	Manufacturing
Occupation	Production Engineering
NSQF Level	5.5
Credits	2
Minimum Educational Qualification & Experience	Completed 3 year UG degree (In trades: Manufacturing/Mechanical/Automobile/Electrical/Electronic or relevant) OR Pursuing 3rd year of UG (In trades: Manufacturing/Mechanical/Automobile/Electrical/Electronic or relevant) and continuous education)
Version	1.0
Last Reviewed Date	NA
Next Review Date	NA
CCN Category	1