Model Curriculum

NOS Name: IIOT Application in Cyber Security (Manufacturing)

NOS Code: ASC/N6462

NOS Version: 1.0

NSQF Level: 5.5

Model Curriculum Version: 1.0

Automotive Skills Development Council | E 113, Okhla Industrial Area, Phase – III,
New Delhi – 110020

Table of Contents

Training Parameters

Sector	Automotive
Sub-Sector	Manufacturing
Occupation	Production Engineering
Country	India
NSQF Level	5.5
Aligned to NCO/ISCO/ISIC Code	NCO-2015/2144.0801
Minimum Educational Qualification and Experience	UG Diploma in relevant field with 1.5 Years of Relevant experience OR 3rd year of UG Degree in relevant field OR Diploma after 10th in relevant field with 3 Years of Relevant experience
Pre-Requisite License or Training	NA
Minimum Job Entry Age	20 Years
Next Review Date	15/03/2027
NSQC Approval Date	15/03/2024
QP Version	1.0
Model Curriculum Creation Date	15/03/2024
Model Curriculum Valid Up to Date	15/03/2027
Model Curriculum Version	1.0
Minimum Duration of the Course	60 Hours
Maximum Duration of the Course	60 Hours

Program Overview

This section summarizes the end objectives of the program along with its duration.

Training Outcomes:

At the end of the program, the learner should have acquired the listed knowledge and skills.

- Enhanced Operational Efficiency:
  - IIoT applications enable real-time monitoring of manufacturing processes, equipment performance, and supply chain logistics. By leveraging data analytics and machine learning algorithms, manufacturers can optimize production processes, minimize downtime, and reduce waste.
- Improved Quality Control:
  - IIoT sensors embedded in manufacturing equipment can collect vast amounts of data regarding product quality and consistency. Analyzing this data in real-time allows manufacturers to identify and address quality issues early in the production process, thereby reducing defects and improving overall product quality.
- Predictive Maintenance:
  - IIoT-enabled predictive maintenance systems continuously monitor the condition of machinery and equipment on the factory floor. By analyzing data such as temperature, vibration, and energy consumption, these systems can predict potential failures before they occur, allowing for proactive maintenance activities and minimizing unplanned downtime.
- Enhanced Cybersecurity Measures:
  - Implementing IIoT applications in automotive manufacturing requires robust cybersecurity measures to protect sensitive data and prevent cyber-attacks. Training programs focusing on cybersecurity best practices, threat detection, incident response, and secure network architecture are essential to ensure the integrity and security of IIoT systems.

Sub-NOS Details	Theory Duration	Practical Duration	On-the-Job Training Duration	Total Duration
ASC/N6462- - IIOT Application in Cyber Security (Manufacturing) NSQF Level- 5.5	**15:00**	**45:00**	**00:00**	**60:00**
Module: 1 - Introduction to IIOT Application in Cyber Security (Manufacturing) Mapped to ASC/N6462	05:00			05:00
Module: 2- IIOT Application in Cyber Security (Manufacturing) Mapped to ASC/N6462	10:00	45:00		55:00
Total Duration	**15:00**	**45:00**	**00:00**	**60:00**

Module Details

Bridge Module-1 Introduction to IIOT Application in Cyber Security (Manufacturing)
Mapped to ASC/N6462

Terminal Outcomes:

- Interpret the concept of Industrial Internet of Things (IIoT) and its role in manufacturing
- Design and implement IIoT solutions for Cyber Secured manufacturing
- Integrate different types of IIoT sensors and devices used in IIOT Networks.

Duration: *<5:00>*	**Duration**: *<00:00>*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Concept of Industrial Internet of Things (IIoT) and its role in asset monitoring in manufacturing. • Various types of sensors and devices used in IIoT asset monitoring, such as temperature, pressure, vibration, and acoustic sensors. • Importance of data collection, storage, and analysis in IIoT asset monitoring, and how it can help identify potential equipment failures before they occur. • Different types of IIoT platforms used for asset monitoring, such as cloud-based platforms and edge computing devices.	
Classroom Aids:	
Whiteboard, marker pen, projector	
Tools, Equipment and Other Requirements	
IIOT Sensors, I/O Link, Communication Protocol Device, Edge Computing Device	

Module: 2 IIOT Application in Cyber Security (Manufacturing)

Mapped to ASC/N6462

Terminal Outcomes:

- Understanding of Manufacturing System and IIoT Communication Networks:

Participants will gain a comprehensive understanding of manufacturing systems, including the various components, processes, and communication networks involved in industrial operations. They will also learn about IIoT communication networks, which enable machines, sensors, and other devices to communicate and exchange data in real-time.

- Identification of Security Risks:

Participants will learn to identify potential security risks and vulnerabilities within manufacturing systems and IIoT communication networks. This includes understanding common attack vectors such as unauthorized access, data breaches, malware, and denial of service attacks.

- Knowledge of Security Protocols and Technologies:

Participants will become familiar with various security protocols and technologies used to secure manufacturing systems and IIoT communication networks. This includes encryption, authentication mechanisms, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

- Designing Security Layers:

Participants will learn how to design robust security layers to protect manufacturing systems and IIoT communication networks from cyber threats. This involves implementing defense-in-depth strategies that incorporate multiple layers of security controls at different points within the system architecture.

- Implementing Security Measures:

Participants will gain practical experience in implementing security measures across manufacturing systems and IIoT communication networks. This may include configuring firewalls, setting up access controls, encrypting data transmissions, and deploying security software and hardware solutions.

- Monitoring and Incident Response:

Participants will learn how to monitor manufacturing systems and IIoT communication networks for suspicious activities and security incidents. They will also gain skills in incident response and mitigation, including how to investigate security breaches, contain the damage, and recover from attacks.

Duration: *<10:00>*	**Duration**: *<45:00>*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**

Foundational Understanding: IIoT Principles: • Principles of IIoT principles, including connectivity, interoperability, and the role of sensors in enabling the Internet of Things in an industrial context. Understanding Threat Landscape: • Identify potential threats and vulnerabilities within the manufacturing system and IIoT networks. • Recognize the diverse attack vectors and methods used by malicious actors to exploit weaknesses. Risk Assessment: • Evaluate the risks associated with different components, processes, and interactions within the manufacturing system and IIoT networks. • Prioritize security measures based on the level of risk and potential impact on operations and assets. Security Architecture Design: • Develop a comprehensive security architecture that encompasses both physical and digital aspects of the manufacturing environment. • Define security zones and segmentation strategies to isolate critical assets and sensitive data from unauthorized access. Access Control and Authentication: • Implement robust access control mechanisms to restrict unauthorized access to systems, devices, and data. • Utilize multi-factor authentication (MFA) and strong authentication protocols to verify the identity of users and devices. Encryption and Data Protection: • Apply encryption techniques to protect data both in transit and at rest within the manufacturing system and IIoT networks. • Implement encryption standards such as AES (Advanced Encryption Standard) for	• Understanding Threat Landscape: Gain a comprehensive understanding of the various cybersecurity threats and vulnerabilities specific to manufacturing systems and IIoT networks. Learn about common attack vectors, such as malware, ransomware, insider threats, and supply chain attacks. • Risk Assessment and Management: Learn how to conduct risk assessments to identify potential security risks and prioritize them based on their potential impact on manufacturing operations and critical assets. Develop strategies for mitigating these risks through the implementation of security controls and countermeasures. • Secure Network Design: Acquire knowledge and skills in designing secure network architectures for manufacturing systems and IIoT communication networks. Understand the principles of network segmentation, access control, encryption, and intrusion detection/prevention to protect sensitive data and critical infrastructure. • Authentication and Authorization: Learn about the importance of strong authentication and authorization mechanisms to control access to manufacturing systems and IIoT devices. Explore technologies such as multi-factor authentication, role-based access control, and certificate-based authentication to enforce least privilege and ensure only authorized users and devices can access resources. • Data Protection and Privacy: Understand the importance of data protection and privacy in manufacturing environments, especially considering the sensitive nature of production data and intellectual property. Learn about data encryption, data masking, and data anonymization techniques to safeguard data at rest, in transit, and during processing.

securing communication channels and data storage.	• Monitoring and Incident Response: Develop skills in monitoring manufacturing systems and IIoT networks for suspicious activities and security incidents. Learn how to deploy security monitoring tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) solutions, to detect and respond to security breaches in real-time.
Classroom Aids:	
Whiteboard, marker pen, projector	
Tools, Equipment and Other Requirements	
• IIOT Sensors, I/O Link, Communication Protocol Device, Edge Computing Device	

Annexure

Trainer Requirements

Trainer Prerequisites						
Minimum Educational Qualification	**Specialization**	**Relevant Industry Experience**		**Training Experience**		**Remarks**
		Years	***Specialization***	***Years***	***Specialization***	
B.E/B.Tech	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	3	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	1	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA
B.E/B.Tech	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	4	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	0	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA
Diploma	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	5	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	1	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA
Diploma	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	6	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	0	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA

Trainer Certification	
Domain Certification	**Platform Certification**
"IIOT Application in Cyber Security (Manufacturing) ", ASC/N6462, minimum accepted score is 80%	"Recommended that the trainer is certified for the job role "Trainer (VET and Skills)", Mapped to Qualification Pack: MEP/Q2601, V2.0" Minimum accepted score is 80%."

Assessor Requirements

Trainer Prerequisites						
Minimum Educational Qualification	**Specialization**	**Relevant Industry Experience**		**Training Experience**		**Remarks**
		Years	***Specialization***	***Years***	***Specialization***	
B.E/B.Tech	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	3	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	1	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA
B.E/B.Tech	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	4	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	0	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA
Diploma	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	5	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	1	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA
Diploma	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	6	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	0	Mechanical/Automobile /Mechatronics/Electronics/Electrical/ Manufacturing	NA

Assessor Certification	
Domain Certification	**Platform Certification**
"IIOT Application in Cyber Security (Manufacturing): "ASC/N6462", minimum accepted score is 80%	Recommended that the Accessor is certified for the job role "Assessor (VET and Skills)", Mapped to Qualification Pack: MEP/Q2701, V2.0" Minimum accepted score is 80%.

Assessment Strategy

1. Assessment System Overview:

- Batches assigned to the assessment agencies for conducting the assessment on SDMS/SIP or email
- Assessment agencies send the assessment confirmation to VTP/TC looping SSC
- Assessment agency deploys the ToA certified Assessor for executing the assessment
- SSC monitors the assessment process & records

2. Testing Environment:

- Confirm that the centre is available at the same address as mentioned on SDMS or SIP
- Check the duration of the training.
- Check the Assessment Start and End time to be as 10 a.m. and 5 p.m.
- If the batch size is more than 30, then there should be 2 Assessors.
- Check that the allotted time to the candidates to complete Theory & Practical Assessment is correct.
- Check the mode of assessment—Online (TAB/Computer) or Offline (OMR/PP).
- Confirm the number of TABs on the ground is correct to execute the Assessment smoothly.
- Check the availability of the Lab Equipment for the particular Job Role.

3. Assessment Quality Assurance levels / Framework:

- Question papers created by the Subject Matter Experts (SME)
- Question papers created by the SME verified by the other subject Matter Experts
- Questions are mapped with Semester-wise Curriculum.
- Question papers are prepared considering that level 1 to 3 are for the unskilled & semi-skilled individuals, and level 4 and above are for the skilled, supervisor & higher management
- Assessor must be ToA certified & trainer must be ToT Certified
- Assessment agency must follow the assessment guidelines to conduct the assessment

4. Types of evidence or evidence-gathering protocol:

- Time-stamped & geotagged reporting of the assessor from assessment location
- Centre photographs with signboards and scheme specific branding
- Biometric or manual attendance sheet (stamped by TP) of the trainees during the training period
- Time-stamped & geotagged assessment (Theory + Viva + Practical) photographs & videos

5. Method of verification or validation:

- Surprise visit to the assessment location
- Random audit of the batch
- Random audit of any candidate

6. Method for assessment documentation, archiving, and access

- Hard copies of the documents are stored
- Soft copies of the documents & photographs of the assessment are uploaded / accessed from Cloud Storage
- Soft copies of the documents & photographs of the assessment are stored in the Hard Drives

References

Glossary

Term	Description

Declarative Knowledge	Declarative knowledge refers to facts, concepts and principles that need to be known and/or understood in order to accomplish a task or to solve a problem.
Key Learning Outcome	Key learning outcome is the statement of what a learner needs to know, understand and be able to do in order to achieve the terminal outcomes. A set of key learning outcomes will make up the training outcomes. Training outcome is specified in terms of knowledge, understanding (theory) and skills (practical application).
OJT	On-the-job training (Mandatory); trainees are mandated to complete specified hours of training on site
Procedural Knowledge	Procedural knowledge addresses how to do something, or how to perform a task. It is the ability to work, or produce a tangible work output by applying cognitive, affective or psychomotor skills.
Training Outcome	Training outcome is a statement of what a learner will know, understand and be able to do upon the completion of the training.
Terminal Outcome	Terminal outcome is a statement of what a learner will know, understand and be able to do upon the completion of a module. A set of terminal outcomes help to achieve the training outcome.

Acronyms and Abbreviations

NOS	National Occupational Standard(s)
NSQF	National Skills Qualifications Framework
QP	Qualifications Pack
TVET	Technical and Vocational Education and Training
AMC	Annual Maintenance Contract
PPE	Personal Protective Equipment
IIOT	Industrial Internet of things
KPI	Key Performance Indicators