Course Outline (September 2023)

I. Introduction to Cybersecurity for Smart Manufacturing Professionals

- 1.1 Cybersecurity and its importance in Smart Manufacturing
  - 1.1.1 Cybersecurity and its role in protecting businesses and individuals
  - 1.1.2 Basic definitions - Confidentiality, Integrity, Availability, Vulnerability, Threat, Risk
  - 1.1.3 Motivations behind cyber-attacks
  - 1.1.4 Industry 4.0 and the importance of cybersecurity in smart manufacturing
- 1.2 Common Cyber Attacks and How They Work
  - 1.2.1 Common types of cyber-attacks – malware, phishing, ransomware, password attacks, Wi-Fi attacks
  - 1.2.2 Real-world examples (2018—2022)
  - 1.2.3 Understanding the impact of cyber-attacks on businesses, financial markets, critical infrastructure, national security, and individuals
  - 1.2.4 Examples of sensitive information that need to be protected (e.g., personal data, financial information)
  - 1.2.5 How cyber-attacks are evolving and why they are becoming more frequent
  - 1.2.6 Understanding the motivations behind cyber-attacks (e.g., financial gain, espionage, sabotage)
- 1.3 Cloud Security and Its Importance in Smart Manufacturing
  - 1.3.1 Overview of cloud computing
  - 1.3.2 Role of cloud computing in smart manufacturing
  - 1.3.3 Risks, threats, and challenges associated with cloud computing
- 1.4 Standards

II. Identification, Authorization, and Access Control

- 2.1 Understanding Access Control Principles
  - 2.1.1 Overview of access control and its importance in manufacturing
  - 2.1.2 Authentication mechanisms and their importance (e.g., passwords, biometrics, two-factor authentication)
- 2.2 Potential attacks on Access Control mechanisms
  - 2.2.1 Internal and external threats
  - 2.2.2 Risks to the company
  - 2.2.3 The principle of least privilege and why it's important to limit access
- 2.3 Best Practices for Managing User Accounts and Permissions
  - 2.3.1 The impact of unauthorized access on identification and authorization with examples
  - 2.3.2 Best practices for access control automation
- 2.4 Cloud-Based IAM Solutions and Their Importance in Smart Manufacturing
  - 2.4.1 Overview of cloud-based IAM solutions and their use in smart manufacturing
  - 2.4.2 Importance of cloud-based IAM solutions for securing access to cloud systems and data
  - 2.4.3 Best practices for implementing and managing cloud-based IAM solutions

III. Configuration Management and Maintenance

- 4.1 What is Configuration Management and Maintenance?
  - 4.1.1 Understanding the concept of configuration management and how it helps keep smart

manufacturing systems secure
- 4.1.2 The role of configuration management in reducing risk and improving security
- 4.1.3 MTConnect overview, operation and secure configuration

4.2 Overview of Industrial IoT and the wireless networks in manufacturing
- 4.2.1 Basics and applications of Industrial Internet-of-Things (IIoT)
- 4.2.2 Bluetooth, ZigBee, RFID and NFC and how to configure them
- 4.2.3 Example scenario of an IIoT network in a CNC machining shop floor

4.3 Why You Need to Update Regularly
- 4.3.1 Understanding the importance of regularly updating configurations and software
- 4.3.2 Why it's important to keep configuration information accurate and up to date
- 4.3.3 How configuration management helps you meet industry standards and regulations
- 4.3.4 How patch management helps maintain security
- 4.3.5 The importance of having a comprehensive maintenance plan in place.

4.4 Importance of Monitoring and Protecting Systems
- 4.4.1 The importance of monitoring systems for potential security issues
- 4.4.2 How poor maintenance can affect the performance and security of your smart manufacturing systems
- 4.4.3 The role of regular security assessments in maintaining security
- 4.4.4 Best practices for securing and protecting equipment and sensitive information

4.5 Cloud-Based Backup and Recovery Solutions and Their Importance in Smart Manufacturing
- 4.5.1 Overview of cloud-based backup and recovery solutions and how they are used in smart manufacturing
- 4.5.2 The importance of cloud-based backup and recovery solutions for protecting against data loss in the event of a disaster or a system failure

4.6 Best practices for keeping system and software secure
- 4.6.1 Best practices for configuring systems and software to ensure optimal security
- 4.6.2 Best practices for maintaining and updating software, hardware and other components to minimize vulnerabilities
- 4.6.3 Best practices for implementing and managing cloud-based backup and recovery solutions in smart manufacturing

IV. Awareness, Training, and Non-technical Elements

3.1 Importance of Ongoing Cybersecurity Education and Training for Workers
- 3.1.1 Why ongoing awareness and training is important in cybersecurity
- 3.1.2 The impact of lack of awareness and training on cybersecurity risk
- 3.1.3 The importance of making cybersecurity training a priority for all employees

3.2 Common Security Risks and Best Practices
- 3.2.1 Understanding the latest threats and best practices for protecting against them
- 3.2.2 Understanding the importance of awareness and training in identifying potential cyber threats
- 3.2.3 Developing, implementing, and reviewing security policies and procedures: best practices and importance
- 3.2.4 The importance of regular security policy review and update

3.3 Non-Technical Elements Impacting Security
- 3.3.1 The role of management and organizational culture in promoting a secure environment
- 3.3.2 The impact of human error on security
- 3.3.3 The role of physical security in protecting sensitive information
- 3.3.4 The importance of security policies and procedures in reducing risk