EET-3200: INDUSTRIAL IOT FUNDAMENTALS AND CYBERSECURITY

Cuyahoga Community College

Viewing: EET-3200 : Industrial IoT Fundamentals and Cybersecurity

Board of Trustees:
September 2023

Academic Term:
Fall 2024

Subject Code
EET - Electrical/Electronic Engineer

Course Number:
3200

Title:
Industrial IoT Fundamentals and Cybersecurity

Catalog Description:
Introduction to the Industrial Internet of Things (IIoT) and cybersecurity. Securing the connections, sensors, data, and safely adding new devices will be introduced. The basics of being safe online, securing sensors, and protecting collected data will be reviewed. Introduction to different types of malware and attacks and how manufacturing organizations protect themselves against these attacks. Corresponding CISCO badge may be awarded upon successful completion of the course.

Credit Hour(s):
4

Lecture Hour(s):
2

Lab Hour(s):
4

Requisites

Prerequisite and Corequisite
EET-1600 Industrial Routers, Switches, and Operating Systems for Smart Manufacturing, and EET-1620 Industrial Protocols and Machine Connectivity for Smart Manufacturing.

Outcomes

Course Outcome(s):
Explain what is cybersecurity and common approaches to staying safe online.

Essential Learning Outcome Mapping:
Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):
1. Explain the basics of being safe online, including what cybersecurity is and its potential impact.
2. Explain the most common cyber threats, attacks, and vulnerabilities.
3. Explain how to protect yourself while online.
4. Explain how organizations can protect their operations against these attacks.

Course Outcome(s):
Explain typical IIoT security risks and create a threat model.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Evaluate IIoT security risks in an industrial environment.
2. Evaluate physical device security vulnerabilities in IIoT systems.
3. Evaluate communication security vulnerabilities in IIoT systems.
4. Create an IIoT threat model.
5. Perform threat modelling activities to evaluate communication security vulnerabilities in IIoT systems.

Course Outcome(s):

Provide examples of solutions to reduce cybersecurity risks in an IIoT environment.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Use industry-standard models to explain security requirements in IIoT systems.
2. Evaluate application security vulnerabilities in IIoT systems.
3. Make recommendations to threat mitigation measures through the use of threat modeling and risk management frameworks.
4. Explain the impact of emerging technologies on IIoT security.
5. Evaluate IIoT security using a simple model.
6. Perform threat modeling activities to evaluate physical device security vulnerabilities in IIoT systems.

Course Outcome(s):

Perform vulnerability assessment activities with IIoT applications and protocols.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Recommend measures to mitigate threats to IIoT devices.
2. Determine vulnerabilities of the IIoT communication layer.
3. Utilize industry-standard models to explain security requirements in IIoT systems.
4. Use industry-standard models to explain IIoT systems.
5. Recommend measures to mitigate threats to IoT applications.
6. Explain innovations in IIoT security.
7. Apply skills learned to a challenging hands-on capstone activity.

Methods of Evaluation:

1. Homework
2. Laboratory experiments and reports
3. Midterm examination
4. Final examination
5. Portfolio

Course Content Outline:

1. What is the Industrial Internet of Things?
    a. An introduction to IIoT
    b. IIoT Architectures
2. Building an IIoT Network

   a. Sensors and Actuators
   b. Connecting to IIoT Devices over Wireless with IEEE 802.15.4
   c. Low Power Wide Area networks (LPWANs)
   d. IIoT Connectivity
   e. IPv6 Fundamentals for IIoT
   f. Management Protocols for IIoT
   g. IIoT Security
3. Harnessing the Data from IIoT Devices
   a. An Introduction to Analytics
   b. Fog and Edge Computing
   c. Data Analytics Architectures
4. IIoT Considerations for Industry
   a. Utilities and the Smart Grid
   b. Manufacturing
5. Connecting and Securing IIoT Devices
   a. Connecting IIoT Devices with Wireless Technologies
   b. Wireless Technologies
   c. Using Wi-Fi to Connect IIoT Devices
   d. Low Power Protocols and their Applications
   e. Long Range Communication Methods for IIoT
6. The World of Industrial IIoT and Operational Technology (OT))
   a. The Convergence of IT and OT
   b. An introduction to Supervisory Control and Data Acquisition (SCADA)
   c. The Purdue Model for Industrial Automation
   d. Synchronizing Timing of Industrial Devices
   e. Resiliency for Industrial Networks
7. Protecting IIoT Devices and Data from Cyberattack
   a. An introduction to the IIoT Cybersecurity
   b. Understanding Threat Vectors and Targets
   c. Anatomy of an IIoT Cyberattack
   d. Developing an IIoT Security Blueprint
8. Communicating with IIoT Devices
   a. How we Communicate with IIoT Devices
   b. An Introduction to Message Queuing Telemetry Transport (MQTT)
   c. IIoT Data Management Tools
9. IIot Cloud Platforms
   a. IIoT Cloud Platforms - Amazon Web Services (AWS) IIoT Suite
   b. AWS IIoT Suite Components and Architecture
   c. Working with AWS IIoT Core
   d. IIoT Cloud Platforms - Google Cloud IIoT
10. Evaluating the business drivers behind an IIoT project
   a. Scoping the project
   b. Selecting the right technology platforms
   c. The Future of IIoT

Resources

Barton, Robert & Jerome Henry. (2021) *Internet of Things (IoT) LiveLessons*, Pearson IT Certification. https://www.pearsonitcertification.com/store/internet-of-things-iot-livelessons-2nd-edition-video-9780137592241

Misra, Sudip. (2020) *Introduction to Industrial Internet of Things and Industry 4.0*, CRC Press.

Veneri, Giacomo & Antonio Capasso. (2018) *Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0* , Packt Publishing.

Resources Other

1. Krishnan, M.S. (2023) Industrial Internet of Things (IIoT) University of Michigan. https://www.coursera.org/learn/industrial-internet-of-things

Top of page

Key: 5117