EET-3100: MANUFACTURING NETWORK DEVICES

Cuyahoga Community College

Viewing: EET-3100 : Manufacturing Network Devices

Board of Trustees:
May 2024

Academic Term:
Fall 2024

Subject Code
EET - Electrical/Electronic Engineer

Course Number:
3100

Title:
Manufacturing Network Devices

Catalog Description:
Introduction to architectures, models, protocols, and networking elements that connect users, devices, applications and data through the Internet and across modern manufacturing networks. Covers how to verify communications between devices and recognize data transmission types. Also includes how to design, deploy, and maintain a logical and physical network infrastructure for their manufacturing operation. The student will gain a sufficient level of knowledge to build a converged multi-service, plant-wide network and operate as a credible domain expert in a multi-function team.

Credit Hour(s):
3

Lecture Hour(s):
1

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):
Use the different types of software and servers that are required in a networked manufacturing environment.

Objective(s):
1. Compare the strengths and weaknesses of each Network Switching Topology (Bus, Star, Mesh, Tree, etc.).
2. Practice using robust network protocols through hands-on lab.
3. Demonstrate the use of TCP (Transmission Control Protocol) and IP (Internet Protocol) and their applications in hands-on lab activities.
4. Utilize the components of Network Virtualization.
5. Explain the role of a hypervisor.
6. Construct a LAN (Local Area Network) and VXLAN (Virtual eXtensible Local Area Network) to simulate how they work.
7. Make use of the concept of virtual switching and routing.

Course Outcome(s):
Apply the basic concepts of networking while implementing a high availability network.

Objective(s):

1. Demonstrate through hands-on labs how routers use private IP addresses to communicate with other LAN devices connected to the same router.
2. Show how two devices communicate in a Half-Duplex ethernet network through the use of hands-on labs.
3. Demonstrate the concept of CSMA/CD (Carrier Sense for Multi-Access with Collision Detection) on an industrial network.
4. Utilize a MAC (Media Access Control address) through a hands-on lab.
5. Make use of the different types of ethernet transmissions.
6. Design and develop a network architecture using ethernet protocol.
7. Explain the concept of STP (Spanning Tree Protocol) and what it is used for.
8. Show how STP adds additional protection against OSI (Open System Interconnect) Layer 2 forwarding loops.

Course Outcome(s):

Develop a Smart Manufacturing Network Security policy to better protect against threats to data security.

Objective(s):

1. Experiment with how wireless network devices are made secure on the manufacturing floor.
2. Distinguish the difference between Smart Manufacturing Network Security and cybersecurity.
3. Examine differences in security levels between Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access2 (WPA2) and Wi-Fi Protected Access3 (WPA3) and discuss reasons for selecting one or the other for manufacturing networks.

Course Outcome(s):

Examine the various methods used in setting up and implementing network security for Smart Manufacturing facilities.

Objective(s):

1. Discuss the benefits of segmentation for network security.
2. Compare and contrast the two methods of network segmentation.
3. Create a diagram using VLAN (Virtual Local Area Network) segmentation for network security.
4. Demonstrate how network segmentation is implemented in a manufacturing network.
5. Examine how remote manufacturing devices are protected using segmentation techniques.

Course Outcome(s):

Design, implement, and support security for Smart Manufacturing devices and data.

Objective(s):

1. Demonstrate how wireless networking devices on the manufacturing floor are made secure.
2. Make use of an IACS (Industrial Automation and Control System) through hands-on lab.
3. Compare and contrast the concepts of SCADA (Supervisory Control and Data Acquisition), PLCs (Programming Logic Control) and HMI (Human Machine Interface).
4. Utilize the three main components of Network Virtualization.
5. Experiment with IT/OT (Information Technology/Operational Technology) through the use of hands-on labs.
6. Apply the concept of Internet of Things (IoT).
7. Apply the concept of Network Convergence and how it combines data, video and audio into a single network through hands-on labs.
8. Experiment with the components of a manufacturing data center.

Course Outcome(s):

Use critical thinking and problem-solving skills while using real-world equipment in a classroom setting.

Objective(s):

1. Demonstrate how to use a Command Line Interface (CLI).
2. Demonstrate the EXEC command via the CLI.
3. Demonstrate the CONFIGURE command via the CLI.

4. Demonstrate the VLAN command via the CLI.
5. Demonstrate the INTERFACE command on the CLI.
6. Demonstrate the LINE CONSOLE command on the CLI.
7. Compare the advantages and disadvantages of a Managed Switch versus an Un-Managed Switch.
8. Apply the concept of a DMZ (Demilitarized Zone).

Course Outcome(s):

Configure both Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) on manufacturing network devices.

Objective(s):

1. Make use of the concept of an Intrusion Detection System (IDS).
2. Compare an IDS to a Firewall.
3. Compare and contrast the different kinds of IDSs.
4. Apply the concept of an Intrusion Protection System (IPS)
5. Demonstrate the capability of an IDS.
6. Demonstrate the capability of an IPS.

Methods of Evaluation:

1. Tests
2. Quizzes
3. Laboratory Reports
4. Homework
5. Projects

Course Content Outline:

1. Evolution of the Internet of Things (IoT)
   a. Defining IoT
   b. Making Technology and Architecture Decisions
   c. IoT Vulnerability
2. Planning for IoT Security
   a. Attack Continuum
   b. IoT System and Security Development Lifecycle
   c. Segmentation
3. IoT Security Fundamentals
   a. IoT Building Blocks
   b. IoT Hierarchy
   c. Layered Security Tiers
4. IoT Security Standards and Best Practices
   a. Defining Standards
   b. Standards for NFV, SDN, and Modeling for Services
   c. Communication Protocols
   d. Security Standards and Guidelines
5. Current IoT Architecture Design and Challenges
   a. Approaches to Architecture Design
   b. ITU-T Y.2060
   c. IEEE P2413 IoT Architecture
   d. AIOTI
   e. NFV-and SDN Based Architectures
   f. IoT Platform Design
6. Evolution and Benefits of SDX and NFV Technologies and Their Impact on IoT
   a. SDX and NFV History
   b. Software-Defined Networking
   c. Network Function Virtualization
   d. Impact of SDX and NFV in IoT and Fog Computing

7. Securing SDN and NFV Environments
    a. Securing Controller Southbound
    b. Securing Infrastructure Planes
    c. Securing Controller Northbound
    d. NFV Security Considerations
    e. Request and Response Headers, Response Codes
    f. REST Constraints
    g. REST API Versioning
8. Advanced IoT Platform and MANO
    a. Next-Generation IoT Platforms
9. Identity, Authentication, Authorization, and Accounting
    a. Introduction to Identity and Access Management for the IoT
    b. Access Control
    c. Authentication Privileges
    d. Authentication Methods
    e. Dynamic Authentication Privileges
    f. Access Control Lists
    g. TrustSec and Security Group Tags
    h. TrustSec Enablement SGACL
    i. Dynamic Authentication Privileges
    j. AWS Policy-based Authorization with IAM
    k. IoT Scaling
10. Threat Defense
    a. Centralized and Distributed Deployment Options for Security Services
    b. Fundamental Network Firewall Technologies
    c. Industrial Protocols
    d. Deep Packet Inspection
    e. Application Visibility and Control
    f. IDS and IPS
    g. Advanced Persistent Threats and Behavior Analysis
    h. Encrypted Traffic Analytics
    i. Malware Protection
    j. DNS-based Security
    k. Centralized Security Services Deployment Example
    l. Distributed Security Services Deployment Example
11. Data Protection in IoT
    a. IoT Data Lifecycle
    b. Data at Rest
    c. Data on the Move
    d. Protecting Data in IoT
    e. MQTT (MQ Telemetry Transport)
    f. Authentication in MQTT
    g. Authorization in MQTT
    h. Confidentiality in MQTT
    i. Integrity in MQTT
    j. Availability in MQTT
    k. RabbitMQ
    l. Authentication, Authorization, Confidentiality, and Integrity in RabbitMQ
12. Remote Access and Virtual Private Networks (VPN)
    a. Virtual Private Network Primer
    b. Site-to-Site IPsec VPN
    c. Software Defined Networking Based IPsec Flow
    d. Applying SDN-Based IPsec to IoT
    e. Software-based Extranet using Orchestration and Traditional Approach
    f. Remote Access VPN
    g. VPN, Network Access Manager, Endpoint Compliance, Roaming Protection, Network Visibility, and Threat Protection Modules.
13. Securing the Platform Itself

a. Visualization Dashboards and Multitenancy
b. Back End Platform
c. Communication and Networking
d. Fog Nodes
e. End Devices or “Things”

14. Smart Cities
    a. Evolving Technology Landscape for IoT
    b. Next-Generation IoT Platform
    c. IoT and Secure Orchestration Opportunity
    d. Case Examples
15. Industrial Environments: Oil and Gas
    a. Industry Overview
    b. IoT and Secure Automation Opportunity in Oil and Gas
    c. Upstream Environment
    d. Midstream Environment
    e. Downstream and Processing Environments
    f. Oil and Gas Industry Case Studies
    g. Power of SGT as a CoA
    h. Auto Quarantine Versus Manual Quarantine
16. The Connected Car
    a. Overview
    b. Secure Automation Opportunity
    c. Security for Connected Cars
    d. Power of SGT as a CoA
    e. MAC and VLAN
    f. Routing Concepts
    g. IPv4 and IPv6 Addresses

Resources

Sabella, Anthony, Rik Irons-Mclean, and Marcelo Yannuzzi. *Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT*. Cisco Press, 2018. https://www.ciscopress.com/store/orchestrating-and-automating-security-for-the-internet-9781587145032

Kaeo, Merike. *Designing Network Security*. 2nd edition. Cisco Press, 2003. https://www.ciscopress.com/store/designing-network-security-9781587051173

Anderson, Gary D. *Industrial Network Basics: Practical Guides for the Industrial Technician (Book 3)*. 14th ed. Createspace Receiving, 2021. https://www.textbooks.com/Industrial-Network-Basics-Volume-3-14-Edition/9781500930936/Gary-D-Anderson.php?kpid=9781500930936N&kenshu=_k_Cj0KCQjw2v-gBhC1ARIsAOQdKY3aUE38eAk0f3CmxVNuDc49DBUNxB7VwSsL2oA72gFZBoaKS4BHwj0aAqE2EALw_wcB_k_&mcid=XKS-7564-41-13289-GoogleShopping-PRIDREPLACE-291&gclid=Cj0KCQjw2v-gBhC1ARIsAOQdKY3aUE38eAk0f3CmxVNuDc49DBUNxB7VwSsL2oA72gFZBoaKS4BHwj0aAqE2EALw_wcB

Shin, Bongsik . *A Practical Introduction to Enterprise Network and Security Management 2nd Edition* . 2nd ed. Routledge, 2021.

Top of page
Key: 5134