Industrial Networking Basics

Summary

Industrial network protocols are designed to allow communication between sensors, motors, intelligent electronic devices, and programmable logic controllers found in a manufacturing/industrial environment. These protocols were historically developed to reduce the amount and complexity of physically wired connections needed to implement a typical industrial system's control loop. Industrial networking has since evolved allowing industrial devices to communicate over TCP/IP and the Internet. Since these protocols are designed to be simple and reliable security is often minimal or nonexistent. This scenario teaches students the basics of three industrial networking protocols and some security vulnerabilities found in each. The scenario includes lab work in which the student will use common security tools to observe how industrial networking protocol's function.

Learning Outcomes

- Summarize the history and purpose of industrial network protocols.
- Discuss the basics and security concerns associated with Modbus TCP/IP.
- Discuss the basics and security concerns associated with PROFINET.
- Discuss the basics and security concerns associated with Ethernet/IP.
- Utilize common security tools to examine industrial protocols in action.

Systems

- Kali Linux – Hacker
    - Username: student; Password: Password01
- Industrial Control System
    - Windows XP – OPC Server
        - Username: student; Password: Password01
    - Windows XP – HMI
        - Username: student; Password: Password01
    - PLC/Pump/Sensors
        - Username: root; Password: Password01
- pfSense – Router/Firewall
    - Username: admin; Password: Password01

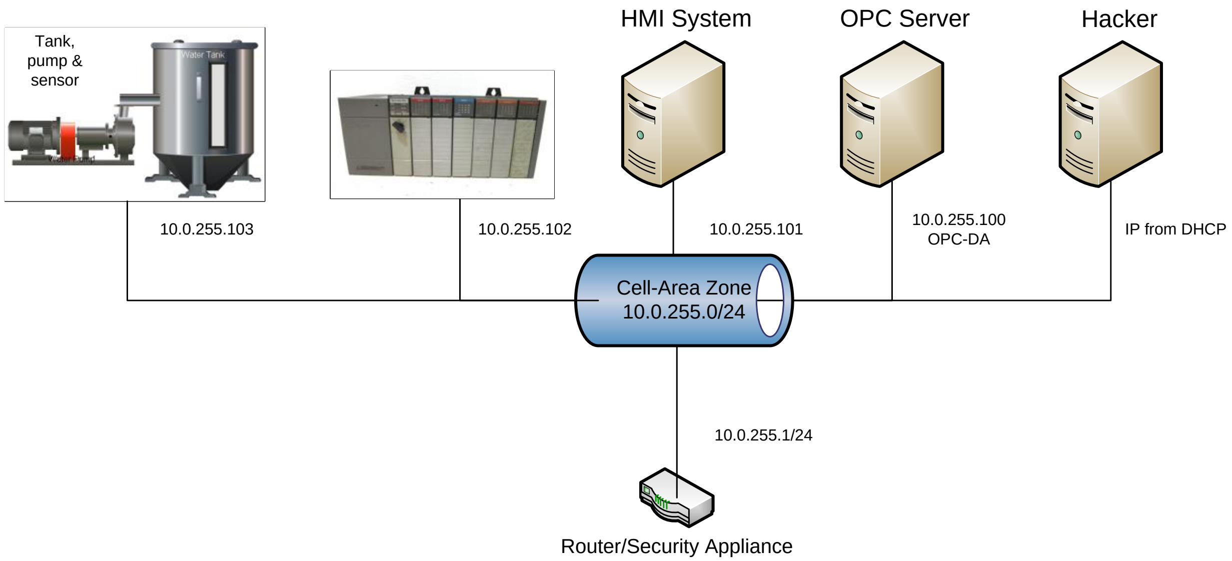
General Lab

Approximate time to complete – 1 Hour 30 Minutes

Students will examine the basic functionality provided by common ICS components such as HMI systems and OPC servers. Students will transfer data to and from a virtual industrial device using Modbus TCP/IP, PROFINET and Ethernet/IP protocols. While doing this they will use common security tools to capture and/or manipulate the data while in transit.

Setup and Deploy

Basic System and Network Diagram



For Further Information

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (April 2017). *ICS Advisory (ICSA-17-101-01) Schneider Electric Modicon Modbus Protocol*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-17-101-01.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (February 2019). *ICS Advisory (ICSA-13-011-03) Rockwell Automation ControlLogix PLC Vulnerabilities*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-13-011-03.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (April 2020). *ICS Advisory (ICSA-19-283-02) Siemens PROFINET Devices (Update E)*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-13-011-03.

National Institute of Standards and Technology (NIST) (May 2015). *Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.