Security for the Industrial Internet of Things (IIoT)

Class 1: IIoT Landscape

September 17, 2018

Louis W. Giokas

DesignNews

CEC CONTINUING EDUCATION CENTER

Presented by: Digi-Key ELECTRONICS

This Week's Agenda

Monday	IIoT Landscape
Tuesday	Safety Considerations
Wednesday	Security Concerns
Thursday	Data Theft and Attacks
Friday	Solutions and Future Directions

Course Description

As the Industrial Internet of Things (IIoT) expands into ever more areas, issues with security become critical. Some of the greatest benefits to be gained come from connecting systems and sensors on the factory floor to corporate systems and multiple sites. The downside is that this leaves these systems, which are critical to the business, open to intrusions, potentially negating the benefits. There are two areas of vulnerability. The first is disruption of operations. The second is the theft of data. In this course, we will look at some of the issues involved and potential solutions to both problems. These include some standard solutions to protect infrastructure as well as solutions that can be embedded in the protocol stack of the devices themselves.

Today's Agenda

- Overview
- Components
- Communications
- Applications
- Conclusion/Next Class

Overview

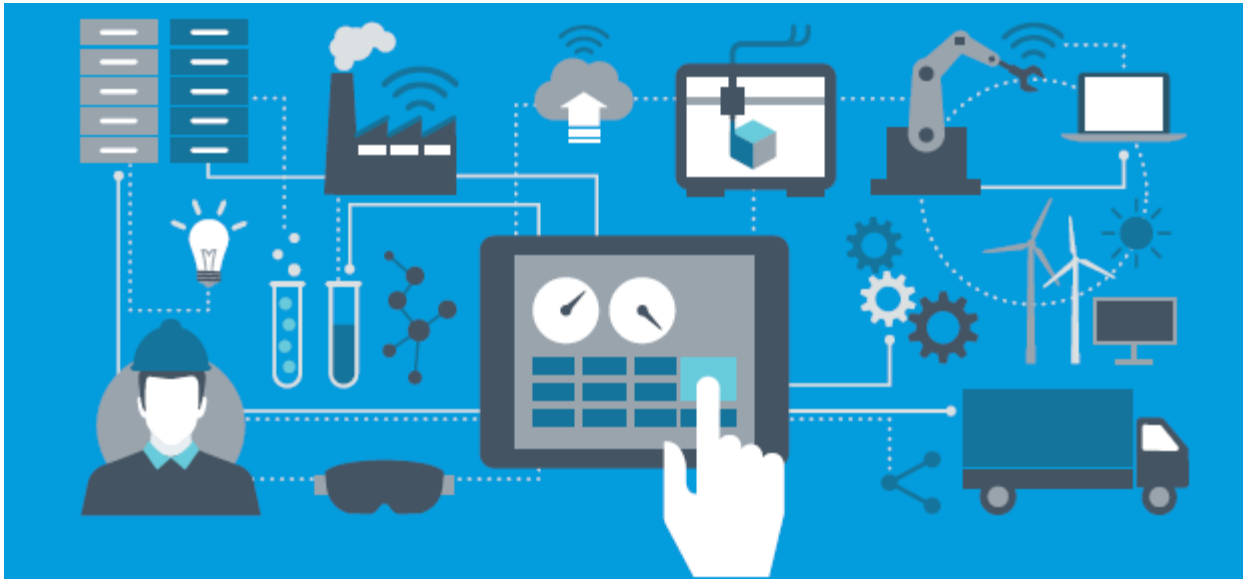
- We will look at the Industrial Internet of Things (IIoT) which is a subset of the Internet of Things (IoT)
- These are “things” or devices which are used in industrial settings and typically have different requirements and characteristics from other IoT devices.

Overview

- By Industrial we mean not only devices in factories, but generally will include:
  - Factories (of course)
  - Warehouse and distribution centers
  - Industrial equipment in remote locations
  - Mines, roadbuilding and other “outdoor” locations
  - Utilities
    - Water and wastewater treatment plants
    - Power generation plants

Overview

- A typical manufacturing environment



Overview

- We will look at security AND safety in these systems
  - The two go hand-in-hand
  - This is driven by the inclusion of computing elements at the “thing” level and at all levels in the system
    - This opens up the “attack surface” considerably
  - Safety concerns are much more important in IIoT than the rest of IoT

Overview

- Another term used for these systems is Cyber-Physical Systems (CPSs), which is a superset of the IIoT and IoT
  - Couple the IIoT elements (the plant) to computational resources (computing subsystem) used to manage and control the system
  - Failures, or attacks, can change the state of the computing subsystem which can then change the physical state of the plant

Components

- There are many types of components in an IIoT system we will consider
  - Sensors
  - Actuators
  - Communications equipment
  - Computing equipment
- Each has unique safety and security implications

Components

- Sensors
  - In some sense these are a core component
  - Make possible all the other functions of an integrated industrial system
  - Can be simple or complex
    - Simple: IR sensor, shaft encoder, presence
    - Complex: vision systems
  - State of the sensor is an important consideration
  - Security of the data is getting more important

Components

- Actuators
  - In actively controlled processes actuators have a key role in the industrial setting
  - Systems controlled can be simple (e.g., a gate) or complex (e.g., a robot)
  - Safety is a primary consideration
    - Human interaction considerations
  - Spoofing of signals to an actuator can cause havoc

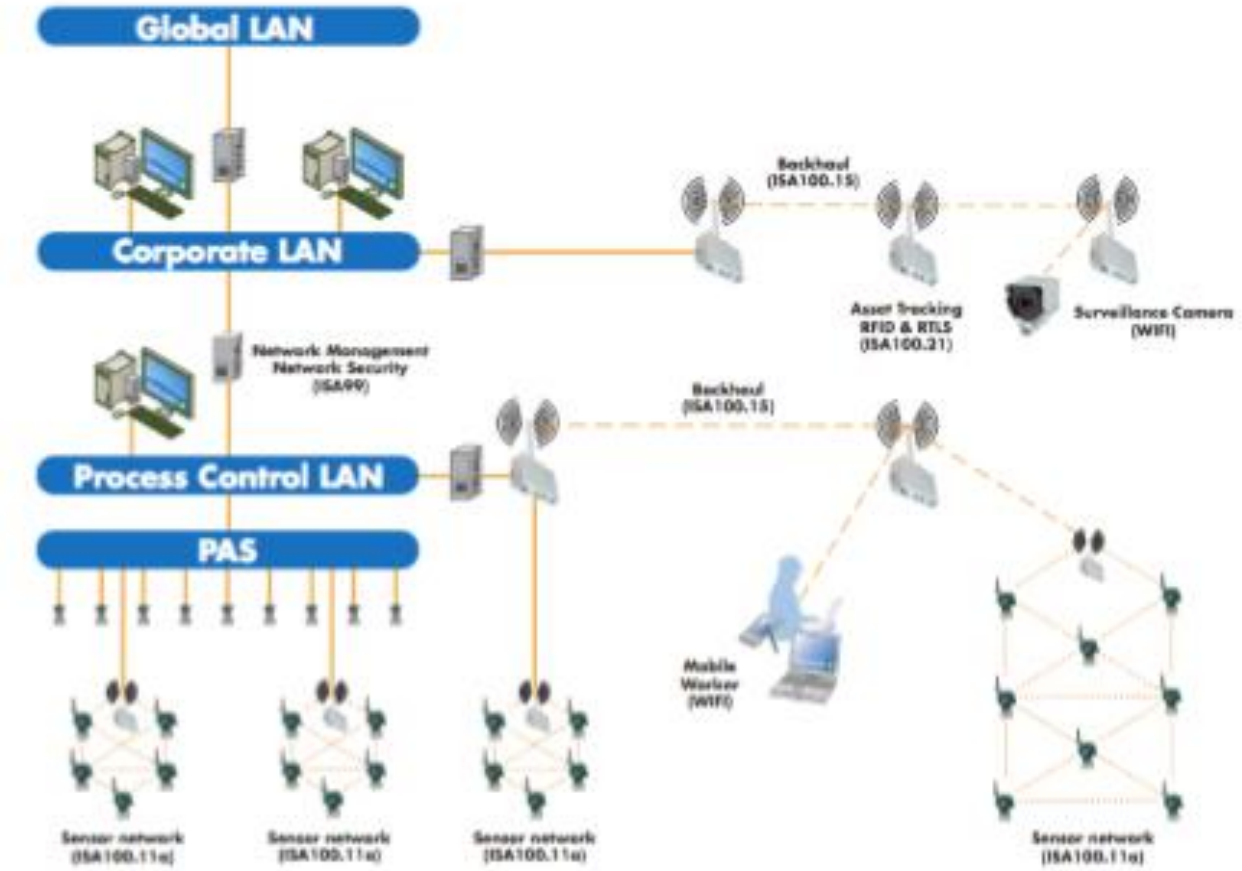
Components

- Computing Equipment
  - Increasingly, computational elements are be pushed further and further from the central processing facility
  - Smart devices, even down to the individual sensor, allow for more complex measurement
  - Systems such as vision systems often require extensive computing
  - Edge computing resources efficiently distribute processing
  - Opens up more opportunities for beaches

Commuinications

- Many communications media are in use
  - Wired
    - Traditional for in plant systems
  - Wireless
    - Becoming more common and reliable
    - Replacing wired systems in some contexts
    - More flexible
  - Cellular
    - Services provided by carriers for just this purpose
  - Satellite
    - Very remote locations

Communications



Communications

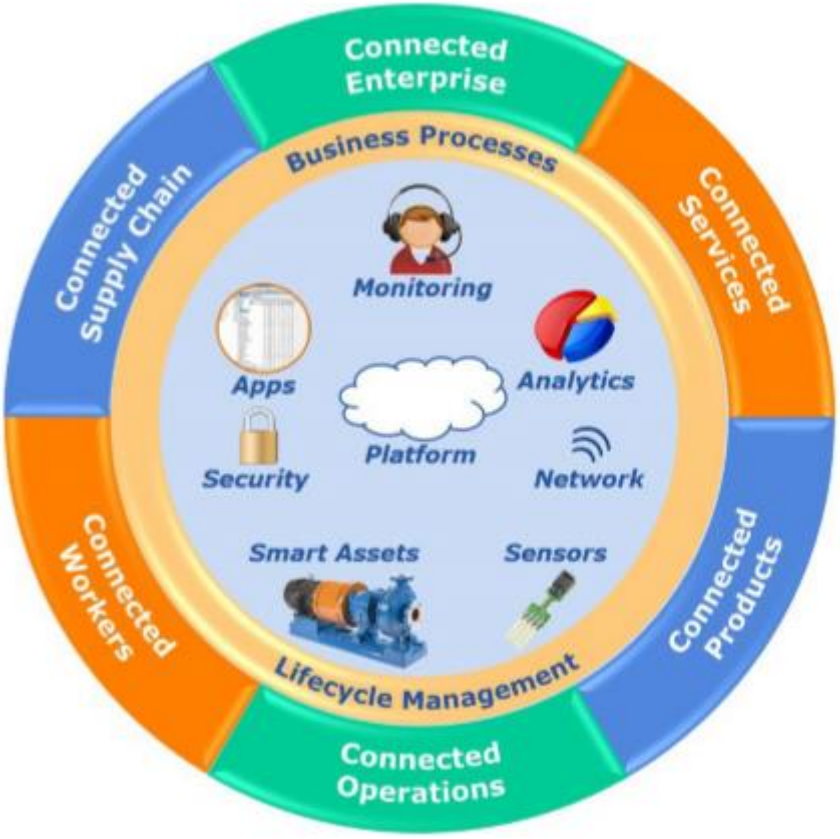


Image courtesy - Automation Research Corp

Communications

- Wired Networks
  - Most expensive to install
  - Highest capacity
  - Susceptible to physical disruption
  - Most secure
    - Network can be monitored for data intercept
  - Many types of protocols in use
    - E.g., Ethercat, Interbus, Profibus, Modbus

Communications

- Wireless networks
  - Wi-Fi
  - Mesh networks
    - IEEE 802.15.4 (ZigBee)
  - Bluetooth
    - For shorter distance applications/monitoring
  - Easy and inexpensive to set up
  - Self organizing
  - Adaptive
    - Handles failures and movement of equipment

Applications

- Plant Control
  - "Traditionally" what we think about
  - Control machines, robots and conveyors
  - Devices may include PLCs, as well as more complex devices
  - Tied back to plant management systems in many cases
  - SCADA (Supervisory Control and Data Acquisition)

Applications

- Logistics Monitoring
  - Monitoring functions transportations and logistics functions
  - May have control functions as well
    - Many monitoring only functions
  - An extension to the plant system
  - Deep interaction with ERP systems

Applications

- Remote Equipment monitoring
  - Often equipment installed in remote locations will be monitored to collect analytics data and to detect failures in advance in order to facilitate servicing
    - E.g., large diesel engine attached to a generator or pump installed in a remote location which send back a data packet on a set schedule (5 min.)

Applications

- Analytics
  - A major goal for collecting data, either in an industrial plant or on remote equipment is the analysis of the data for a number of reasons:
    - Predictive analytics
      - Predict failures
      - Project efficiency
      - Verify design data/assumptions
  - These functions are generally done at centralized, or cloud, facilities
  - Can be real-time or background

Conclusion/Next Class

- Today we laid out the landscape we are going to consider in the rest of the class
- We looked at the field in general and some aspects of components, communications and applications
- Tomorrow we will consider safety