Security for the Industrial Internet of Things (IIoT)

Class 5: Solutions and Future Directions

September 21, 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

DesignNews
CEC CONTINUING EDUCATION CENTER
Presented by: Digi-Key ELECTRONICS

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
- Networks
- Components
- Systems
- Future Directions
- Conclusion
- References

Overview

- The IIoT is a complex environment and a high value environment
  - Disruption can be extremely costly
- Their highly networked nature creates a large attack surface which must be protected
- Well architected and designed systems can help mitigate threats and other failures
  - The same mitigation and recovery techniques applied to threats can also help recover from failures

Overview

- Standardization provides a way to deal with IIoT threats
  - Enforce proven methods for security and safety
  - Enhance interoperability
- Modeling and design provide a way to develop systems with threats in mind
  - Anticipate threats
  - Put mitigation strategies in place to handle those that get through

Overview

- We will look at three “aspects” of the IIoT and how they can best be addressed from a security point of view
  - Networks
  - Components
  - Systems
- The systems approach brings together all the aspects of a CPS in the industrial context

Networks

- Network standards that promote operation in adverse conditions can be a key component in a secure and safe system
  - Adaptive networking approaches essential
- For in plant wireless networks we consider
  - Wi-Fi: IEEE 802.11a/b/g/n
  - Ultra short range Wi-Fi: IEEE 802.11ad WiGig
  - Short range low rate: IEEE 802.15.3a
  - Bluetooth and BluetoothLE

Networks

- Adaptability
  - Mesh network approaches are best for mitigation
  - Mesh networking approaches can be applied to more that just those devices originally designed for them (e.g., mesh or adaptive Wi-Fi)
  - Monitoring is essential for detecting and mitigating situations
    - Reconfiguration can be automatic, manual or both

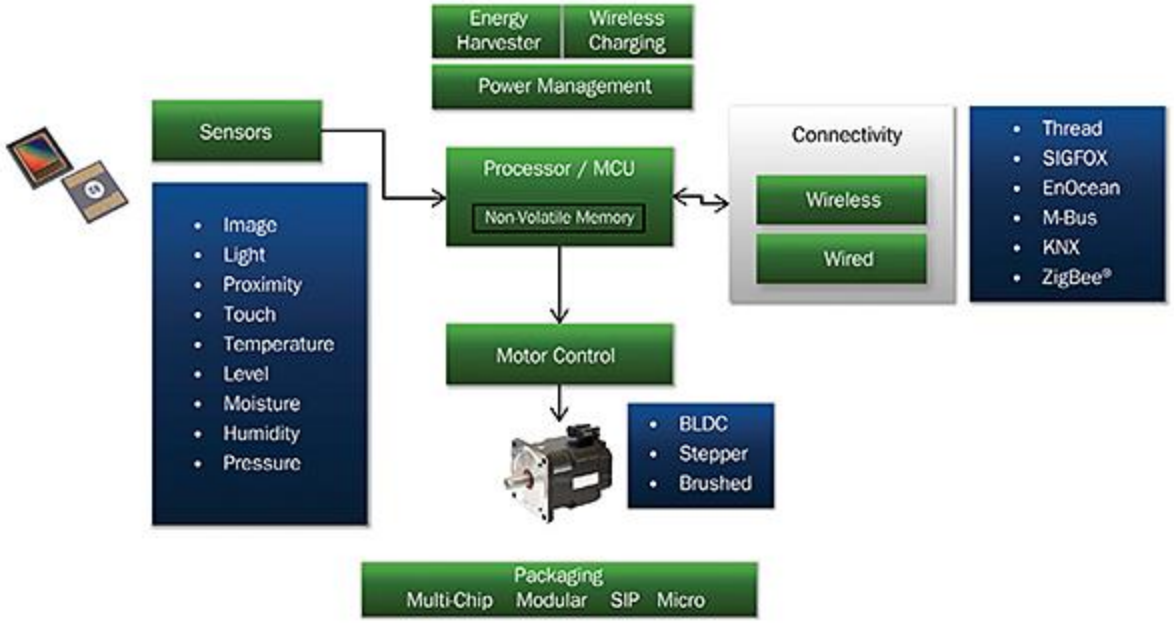
Networks

- Approach for design
  - Security policy: ensure confidentiality-integrity-availability (CIA)
  - Secure network: protocol level security, access restrictions, overhead of security features
  - Secure components: select devices based on their security features
  - Security auditing: during operations and in the design phase

Components

- Smart components can be designed for secure operation
  - Build in secure and resilient features
    - Built-in Security Policy Controller (SPC)
  - Tamper proof components
    - Prevent physical and electronic attacks
  - Validation
    - Test components for resilience to expected attack vectors

Components


Energy Harvester
Wireless Charging
Power Management
Sensors
Image
Light
Proximity
Touch
Temperature
Level
Moisture
Humidity
Pressure
Processor / MCU
Non-Volatile Memory
Connectivity
Wireless
Wired
Thread
SIGFOX
EnOcean
M-Bus
KNX
ZigBee®
Motor Control
BLDC
Stepper
Brushed
Packaging
Multi-Chip
Modular
SIP
Micro

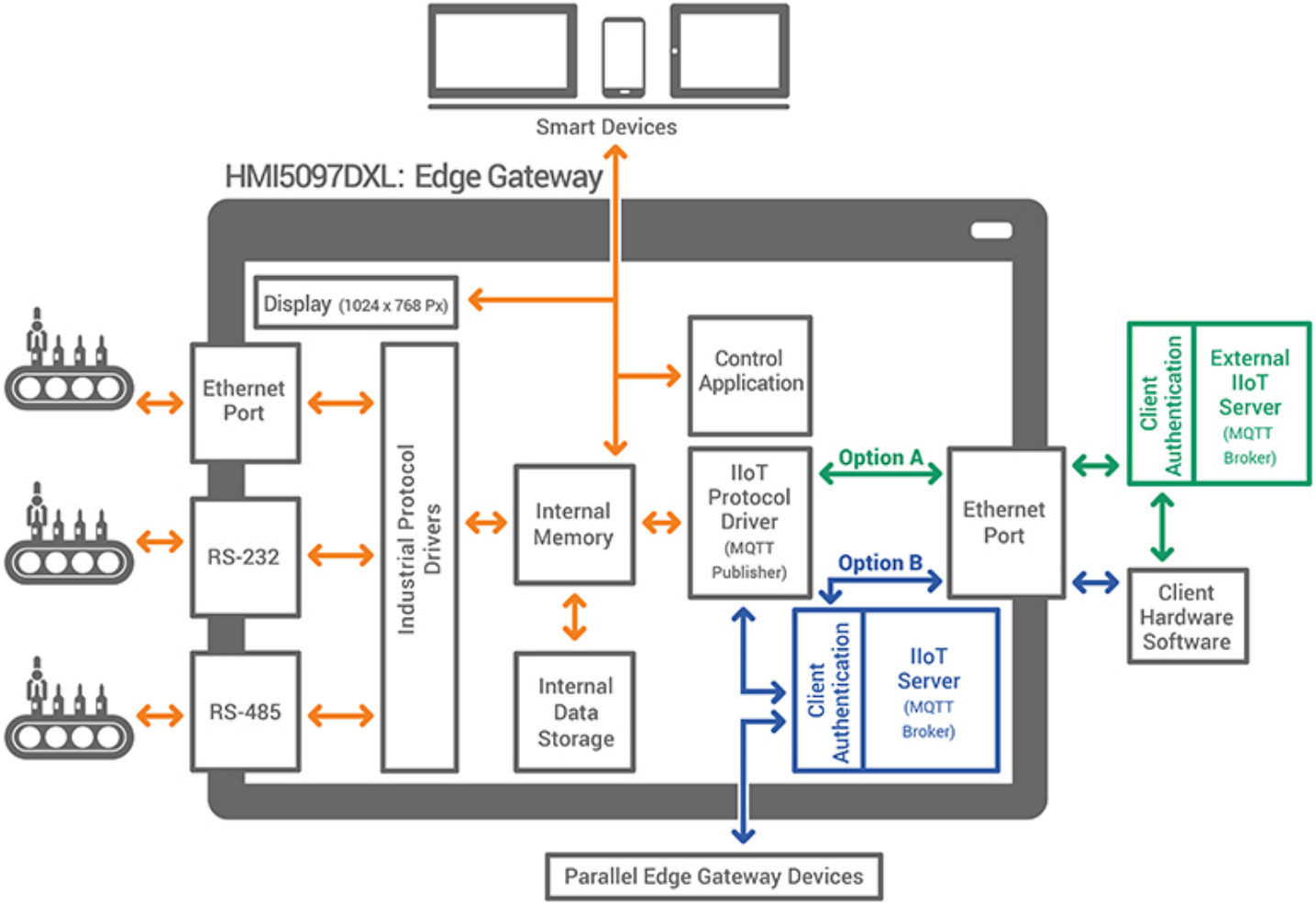
Systems

- As we have seen, the best way to address security and safety in the IIoT is take a systems approach
  - Modeling
    - Systems operations
    - Threat scenarios
    - Mitigation strategies and procedures
    - Evolution strategies
      - Ensure that security is not compromised as system evolves

Systems

- Security Metrics
  - Provide a continuous feedback loop to help identify areas of risk, improve effectiveness and demonstrate compliance with security standards
  - Identify problems early to assist in faster response
- Performance Indicators
  - Provide personnel with dashboards targeted at security metrics for the system
  - Changes in these indicators can highlight issues before the get out of control

Systems

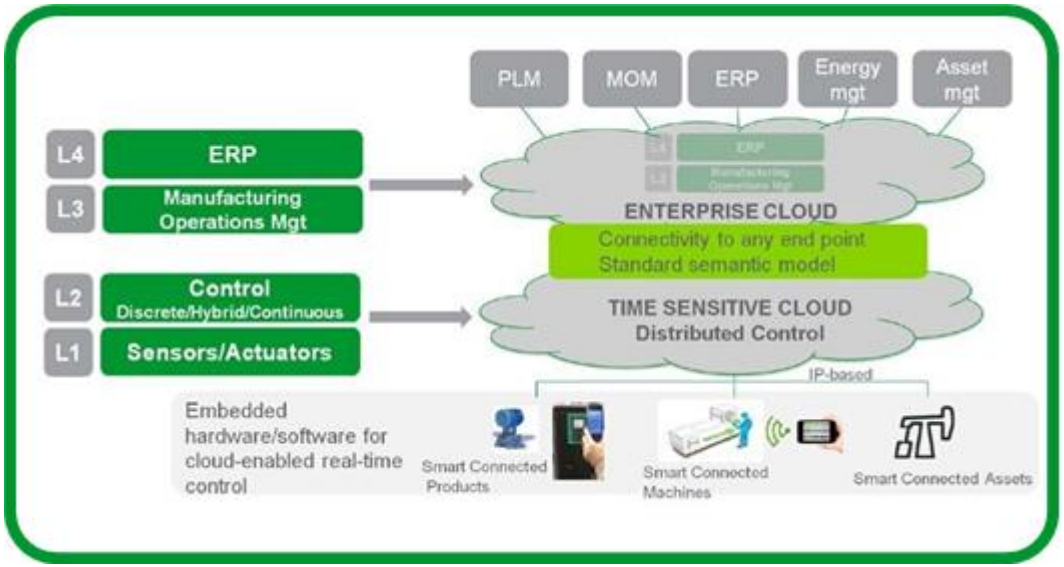

Smart Devices
HMI5097DXL: Edge Gateway
Display (1024 x 768 Px)
Ethernet Port
RS-232
RS-485
Industrial Protocol Drivers
Internal Memory
Internal Data Storage
Control Application
IIoT Protocol Driver (MQTT Publisher)
Option A
Option B
Ethernet Port
Client Authentication
External IIoT Server (MQTT Broker)
Client Hardware Software
Client Authentication
IIoT Server (MQTT Broker)
Parallel Edge Gateway Devices

Future Directions

- Key aspects:
  - Communication Components
    - Harden the protocol stack
    - Build-in encryption and security protocols to prevent loss of data
  - Systems
    - Build security into the design
    - Synthesize and integrate

Future Directions

- Cloud implementations becoming more common
  - Real-time features being provided
  - Can introduce more concerns



Conclusions

- In this session we have talked about some of the strategies and technologies which promote security in the IIoT
- In the course we have given an over of security and safety concerns for the IIoT
- Contact me:
  - E-mail: lgiokas@outlook.com
  - Twitter: @naperlou or #dncec
  - LinkedIn: search for Louis Giokas (the other one is my cousin)

References

- IEEE
  - Proceedings of the IEEE, January 2018
  - Standards for communications protocols
- ICS-CERT: https://ics-cert.us-cert.gov/
- World Economic forum has some good high-level documents in this area
- System modeling
  - SURE at Vanderbilt University
  - ARMET: http://www.mdpi.com/2079-9292/6/3/58/htm