Security for the Industrial Internet of Things (IIoT)

Class 3: Security Concerns

September 19, 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
- Dimensions of Security
- Threats
- Risk Assessment
- Resilience
- Conclusion/Next Class

Overview

- Our consideration of security is concerned with the cyber part of Cyber Physical System (CPS)
- Attempts to tamper with the system are referred to as cyber attacks
- These take many different forms ranging from loss of sensitive information to destruction of systems

Overview

- Our goal is three fold:
  - Prevention of cyber attacks
  - Intrusion detection
  - Resilience
- While prevention is the goal, full protection is very expensive and generally impossible, especially in the face of determined adversary
  - Thus intrusion detection and resilience must be planned for as well

Dimensions of Security

- Threats and their mitigation can occur during design or during operations
- Model-based design techniques, architectures and system synthesis tools can all help ensure that security (and safety) can be improved
- During operations there are techniques that can help identify attacks (and bugs)
  - Monitors
  - Diagnosis (aids in resilience)
  - Secure protocols

Dimensions of Security

Phase	Threats	Countermeasures
Design-time	Design-time attacks	Threat analysis and hardening
	Architectural flaws	Safety-critical networked control
	Component flaws	QoS-aware service-oriented architectures
	Supplier flaws	Synthesis of control software
Run-time	Run-time attacks	Monitors
	Bugs	Fingerprinting
		Repair

Dimensions of Security

- Standards
  - Basic Information Security
    - ISO/IEC 27002
  - Industrial Automation and Control
    - ISA/IEC-62443
- Communication networks open up vulnerabilities
  - Especially critical at the IIoT level
  - Connection to the Internet the most common entry

Threats

- As we have seen, threats and vulnerabilities can be introduced at many points in the design and operation of an industrial IIoT based system
- Threats have different purposes and outcomes
- Both external and internal actors must be considered
- The confluence of wireless networks and IIoT devices increases the points of vulnerability

Threats

Application	Attack Origin	Attack Type
Manufacturing Control	USB devices, phishing	Eavesdropping, Side channel attacks, Resonance attacks
Additive Manufacturing	Acoustic sensors, microphones	IP theft
Manufacturing Control	Phishing	Privilege escalation
Energy	Computer system	Forced update
Energy	Smart meter	Eavesdropping, DoS, Integrity

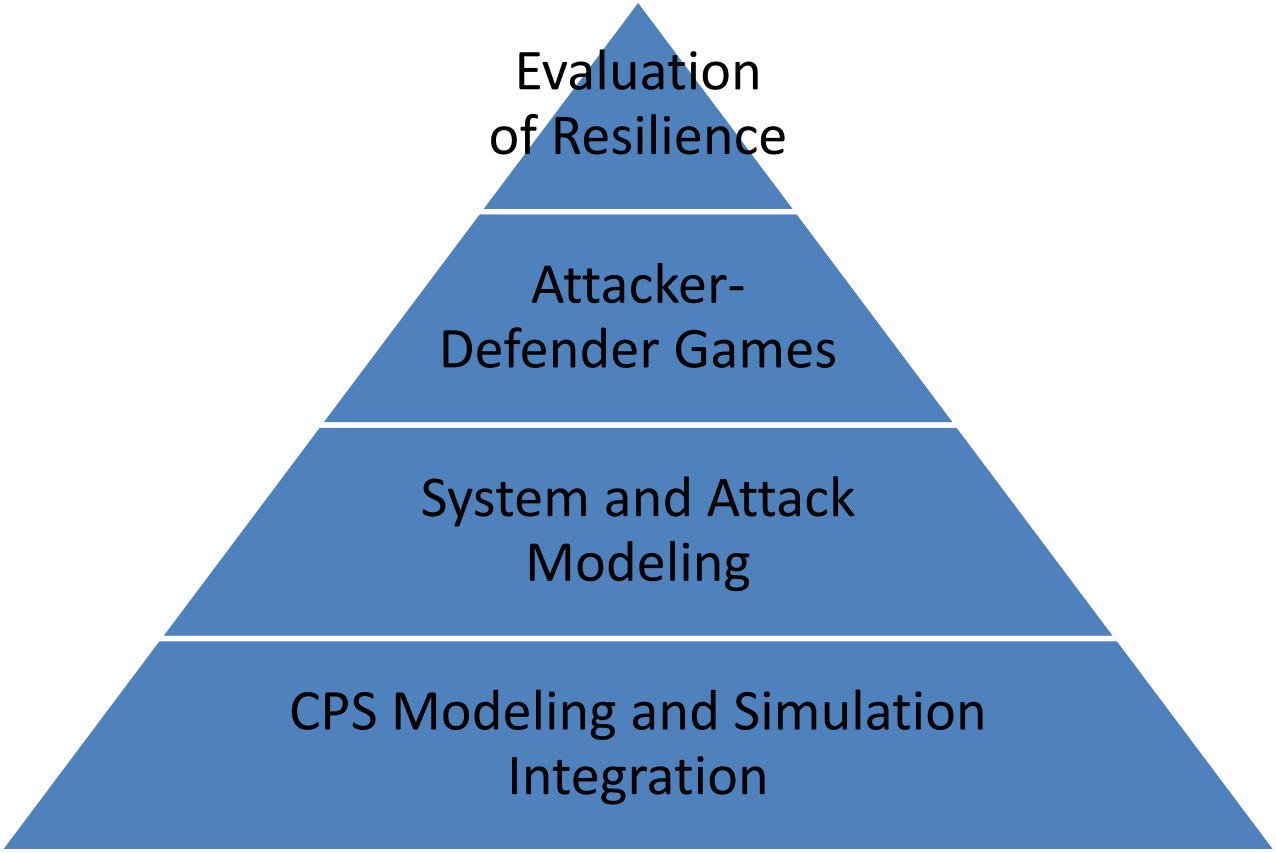
Risk Assessment

- Risk assessment of a CPS is essential to understanding the issues and vulnerabilities associated with the system
- Modeling and simulation are key to performing a risk assessment
- These tasks help to analyze the architecture as designed and to determine any modification to the overall architecture or to individual components

Risk Assessment

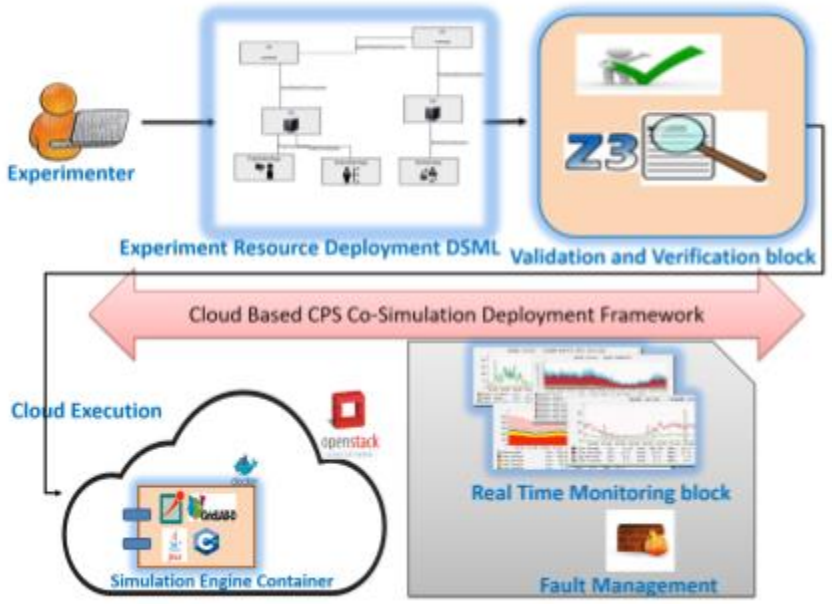
- Modeling and simulation also enable the use of game-theory as well as analytic methods of detecting vulnerability
- As threats happen, these models may also help recover from an attack
- Several environments are available to implement these functions

Risk Assessment



Risk Assessment

This is an example of a system designed to model and deploy IIoT based CPS systems.
In addition to running scenarios and providing validation and verification, run-time monitoring is included.
Using such systems also eases the inevitable changes to systems that happen over time.



Resilience

- Our goal is to detect anomalous behavior that can be attributed to cyber attacks, and then to respond appropriately
- Two main areas of attack that can be made resilient are:
  - Network
  - Control systems

Resilience

- Network
  - In an attack on the network, there are a number of standard responses to various types of attack
  - Monitoring is critical
  - In wireless networks reconfiguration may be possible
    - Mesh networks, adaptive Wi-Fi (incorporating mesh type protocols
  - Rerouting of traffic in LANs and WANs
  - At design time ensure redundant connections

Resilience

- Control system
  - Sensors
    - Adaptive sensors with intelligence
      - This may be in an edge device
    - Sensor monitoring
  - Actuators
    - Built-in safeguards
    - Integration with sensors
    - Manual override

Resilience

- Control system – continued
  - Supervisory controller
    - Built-in/designed-in attack detection
    - Attack isolation
    - Circumvention
  - Parameters/Variables
    - Develop a database of values and ranges
      - Knowledge-based
      - Data-driven
    - Facilitate detection and reset operations

Conclusion/Next Class

- We covered security considerations for the IIoT and CPSs
- Some major aspects include:
  - Threats
  - Risk assessment
  - Resilience
- Tomorrow we will cover Data Thefts and Attacks