Security for the Industrial Internet of Things (IIoT)

Class 2: Safety Considerations

September 18, 2018

Louis W. Giokas

Presented by:

DesignNews

CEC CONTINUING EDUCATION CENTER

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

- Introduction
- Definitions
- Architecture
- Component Implications
- Conclusion/Next Class

Introduction

- We need to consider security and safety together, they can affect one another
- Note that safety does not ensure security and security does not ensure safety
- This comes about because of the integration of physical and computing elements
- Systems under computer control interacting with humans or other physical objects are often safety critical

Introduction

- Approaches to safety in systems has generally evolved as a separate discipline concerned with mechanical and electrical systems that were not connected
- Safety considers events that are typically not intentional
  - Natural forces: fire, storms
  - Equipment failures

Introduction

- Security breaches are typically planned and often executed over a period of time
- They are intentional, where safety issues are traditionally the result of "accidents"
- In connected systems, we have a new source of problem, namely the intentional causing of a safety issue

Definitions

- Cyber Physical Systems (CPS)
  - Systems made up of both computational (cyber) and physical elements
- Safety-critical
  - A system which may cause harm if a failure occurs
- Safety (according to N. G. Leveson in *Safeware – System Safety and Computers*, 1995)
  - "freedom from accidents or losses"

Definitions

- Security is concerned with information
- Privacy is a correlate to security
  - Security is a prerequisite
- Coupling
  - A change in one system causes an effect (change) in another
- Threat surface
  - The computing and digital communications of a system

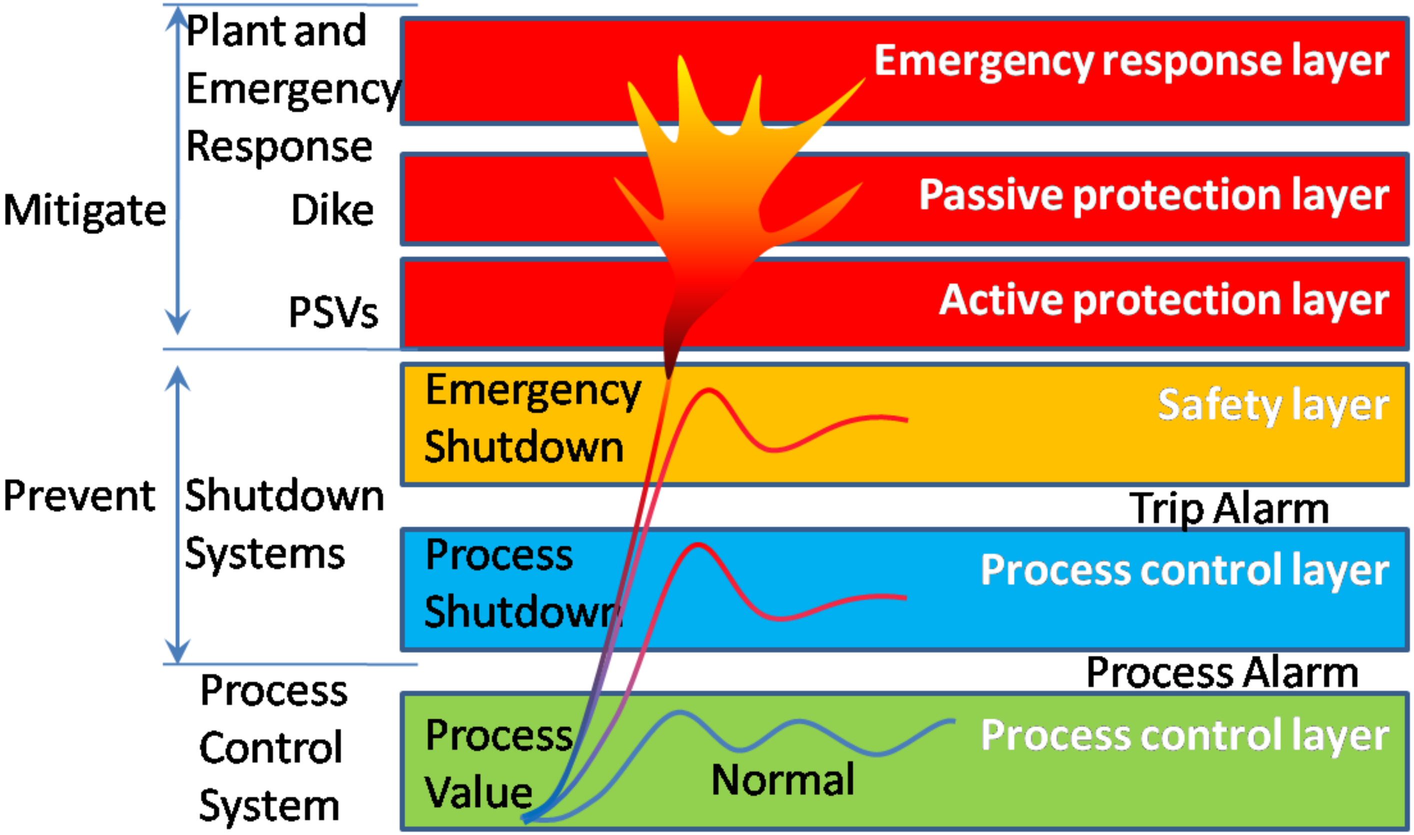
Architecture

- We talk about architecture for safety (and security) in terms of an approach for designing systems
- Generally all of the types of systems in the industrial landscape we consider will evolve in time
  - New machines and components
  - New products output

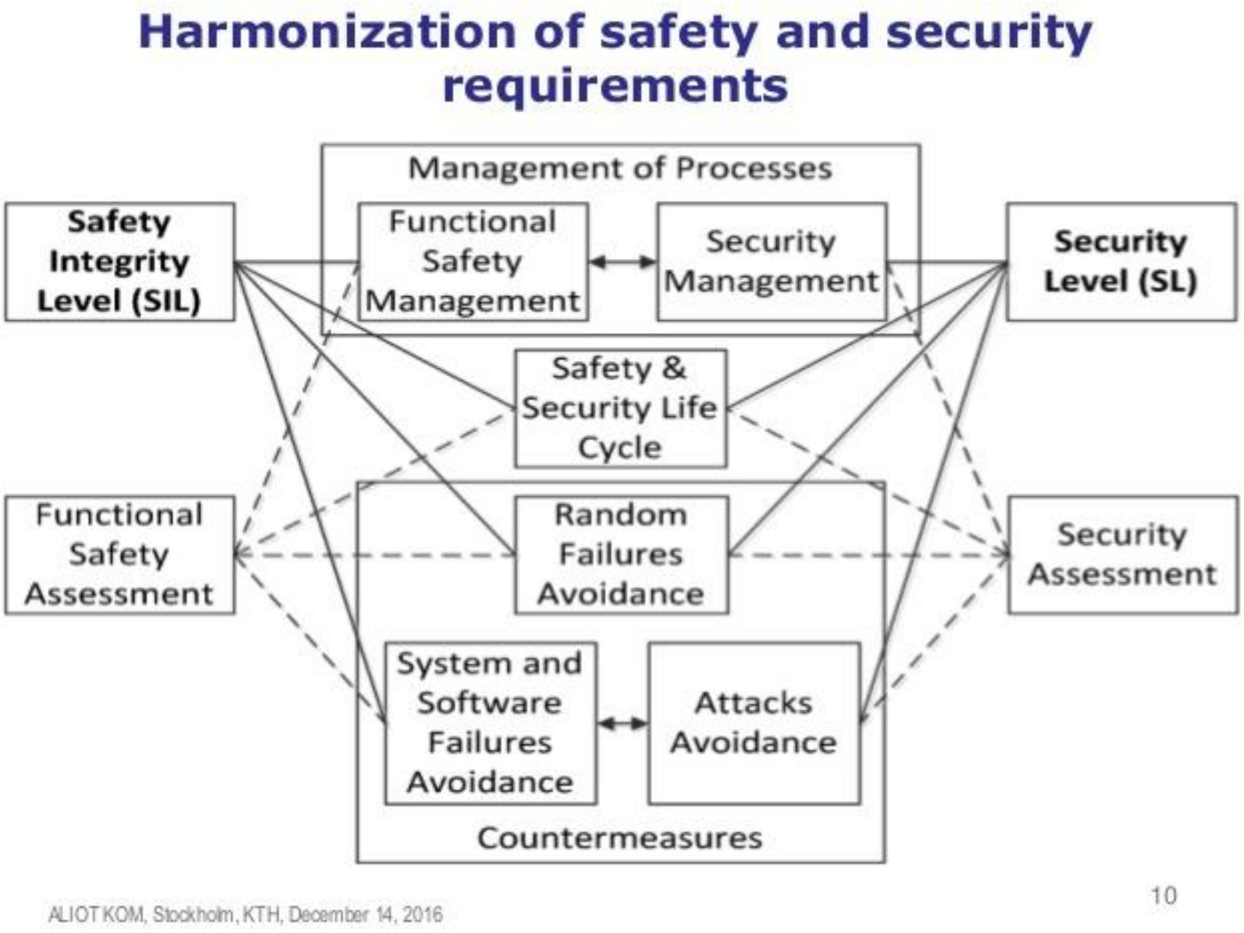
Architecture

- One of the issues we deal with are that safety has typically been handled by one group and security by another
  - Different analytic techniques
  - Different design standards
  - Different certification regimes
- Pulling these together does not diminish the work done by each independently

Architecture



Architecture



Harmonization of safety and security requirements

Management of Processes

Safety Integrity Level (SIL)

Functional Safety Management

Security Management

Security Level (SL)

Safety & Security Life Cycle

Functional Safety Assessment

Random Failures Avoidance

Security Assessment

System and Software Failures Avoidance

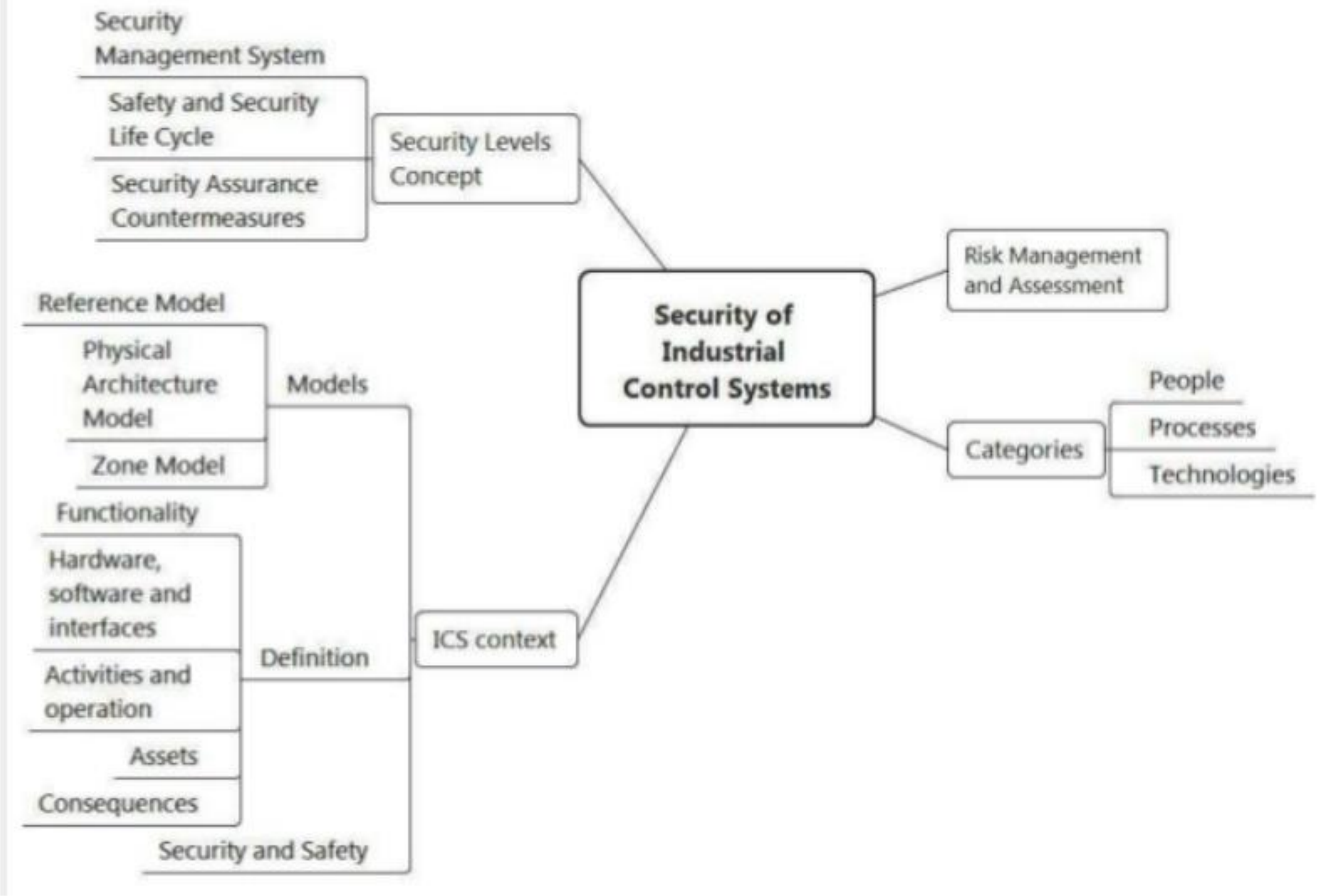
Attacks Avoidance

Countermeasures

ALIOT KOM, Stockholm, KTH, December 14, 2016

10

Architecture


Security Management System
Safety and Security Life Cycle
Security Assurance Countermeasures
Security Levels Concept
Reference Model
Physical Architecture Model
Zone Model
Models
Functionality
Hardware, software and interfaces
Activities and operation
Assets
Consequences
Definition
Security and Safety
ICS context
Security of Industrial Control Systems
Risk Management and Assessment
Categories
People
Processes
Technologies

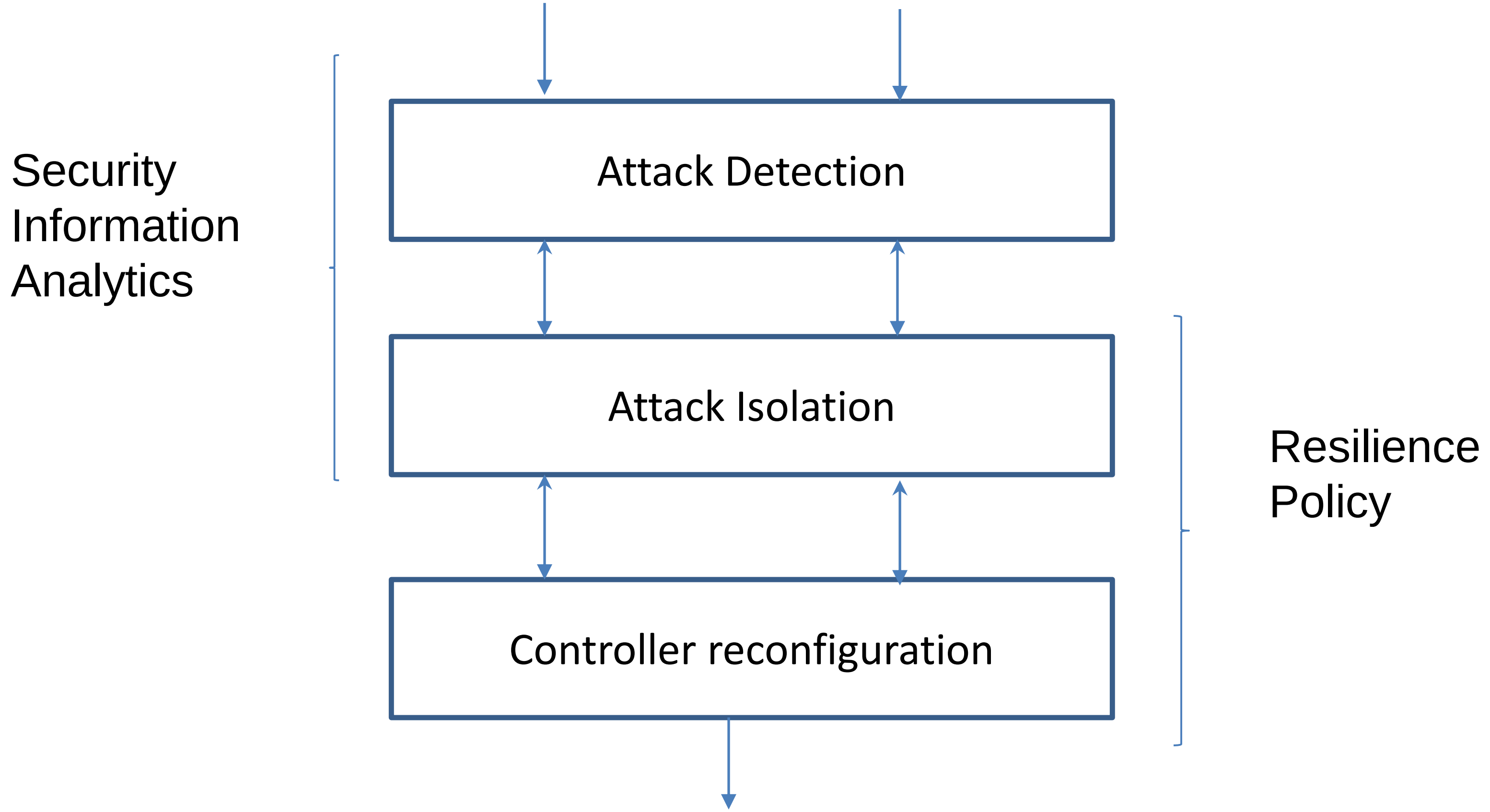
Architecture

- Models, architectures and standards are key to designing, deploying and operating systems that are safe and secure
  - The level of complexity in this interaction is a driver
  - Liabilities and potential business disruption are also key factors
  - The issue is too complex to be dealt with on an ad-hoc basis

Component Implications

- Components in an IIoT setting should be robust and reconfigurable
  - Safety critical components can be designed to detect and isolate attacks
  - Safety information evolves over time
    - Collection and analysis of safety data
  - While smart components open the “threat surface” they also potentially improve our ability to respond to safety issues

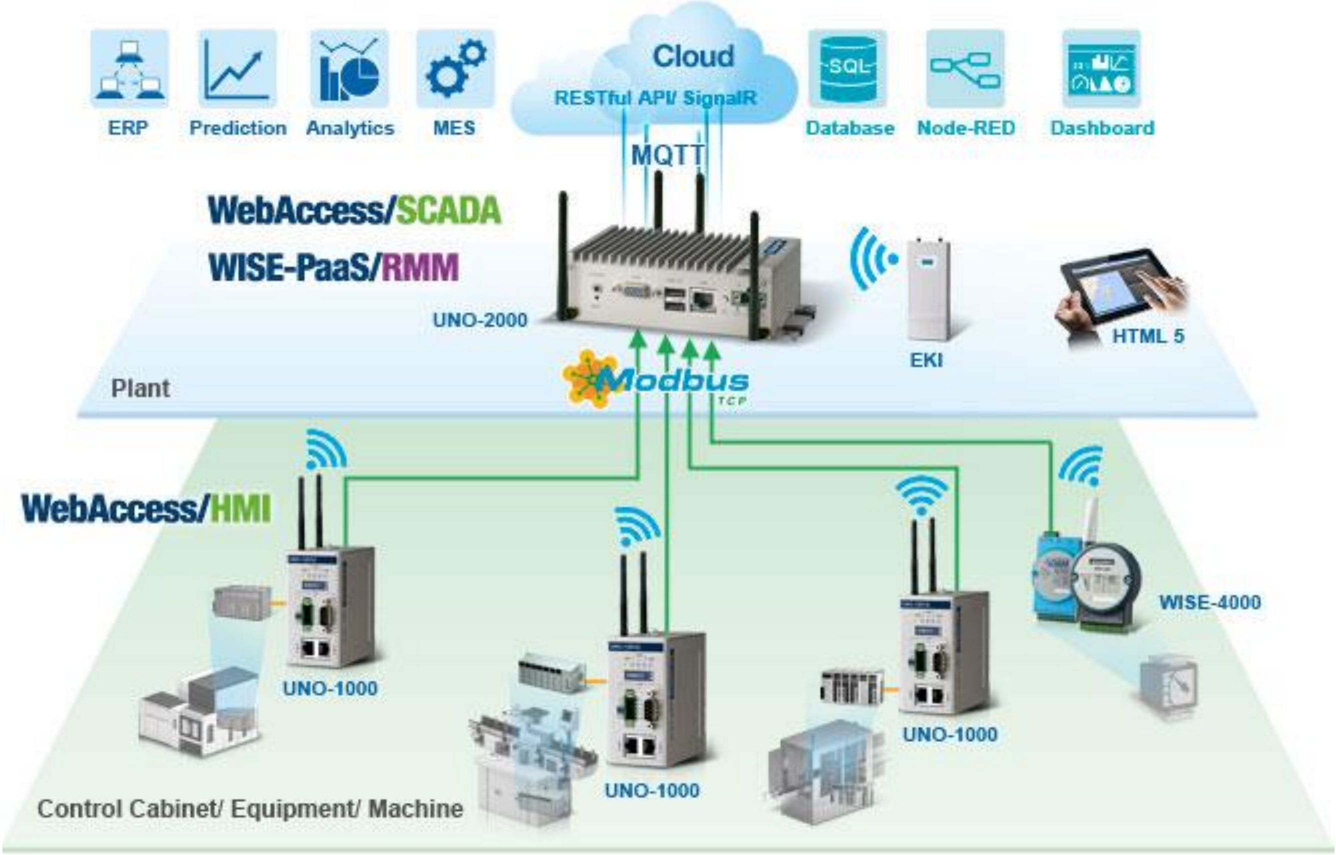
Component Implications



Component Implications

- Commercial of the Shelf (COTS) products which are certified are easier to use
  - Many are configurable and programmable
  - Lots of options in industrial controllers and communications nodes
  - May restrict design choices
  - Typically will be mixed with custom components
  - May front-end custom components

Component Implications



Component Implications

- Custom components
  - Require more analysis
  - Must be certified to standards
    - Increased testing
  - Will certainly be used
    - Flexibility
  - Take a systems engineering approach to ensure safety requirements are met

Conclusion/Next Class

- Today we talked about Safety in IIoT systems
  - This is a necessary corollary to security
- We looked at architectures and components
- Tomorrow we will turn to Security concerns