# Cyber Securing ICS: Architecture-Based Approaches that Preserve Operational Integrity

Jun 5, 2019

National Cyber Summit

Ultra ELECTRONICS

# Agenda

- Overview of ICS Cybersecurity
- Defense-in-Depth
- New Zero Trust Architecture
- Technologies for Digital Trust
- Q & A


About Presenter:
**Chris Guo Ph.D**
**Ultra Electronics**
**Principal Architect**

- More than 20 years of experience
- Software/hardware security
- Wireless and encryption
- Responsible for certifications including FIPS 140-2 and Common Criteria
- Ph.D. in Electrical Engineering from the University of Virginia

# ICS Attacks Getting More Intense

## Targeting critical physical and informational infrastructure

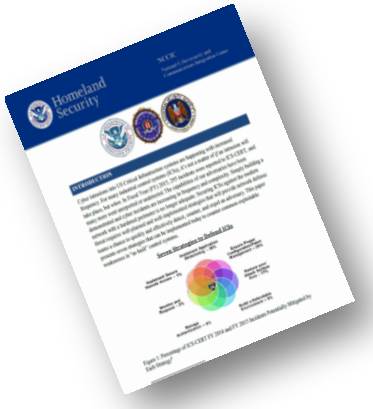
- **Hatman Malicious Firmware**
  - Firmware loaded into a Triconix safety instrumented system (SIS)
  - Allowed for potentially hazardous situations to go unchecked
- **Kemuri Water Company**
  - Hackers accessed hundreds of PLCs
  - Manipulate control applications altering chemicals
- **Ukraine Utilities**
  - Left 700,000 homes and 225,000 customers in the dark
  - 1st successful cyber intrusion to knock a power grid offline
- **New York Dam**
  - Recently confirmed Iranian hackers opened the flood gates
  - Questions raised – was this a dress rehearsal for something larger?
- **Mirai IOT botnet**
  - 100's of thousands of IOT compromised IOT devices unknown to owners

Ultra ELECTRONICS | 3eTI

# DHS's Seven ICS Security Strategies

## Recommend to go beyond the firewall

In 2017, 2700+ incidents were reported to ICS-CERT… many more went unreported or undetected

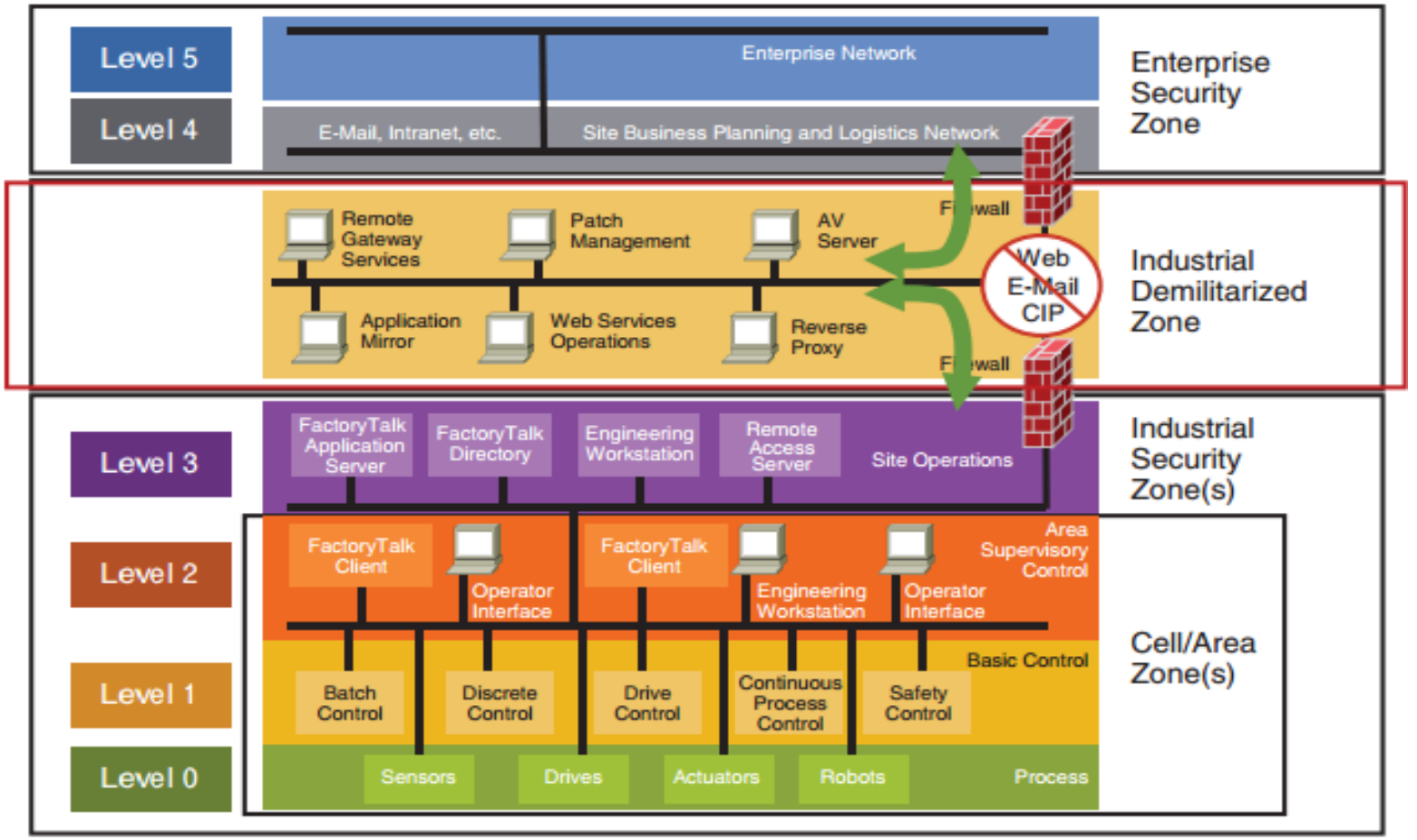



**98%** of incidents reported **would have been prevented** if they follow strategies outlined in this report

| | |
|---|---|
| **1** | Application Whitelisting (AWL) |
| **2** | Ensure Proper Configuration Mgt |
| **3** | Reducing Your Attack Surface Area |
| **4** | Build A Defendable Environment |
| **5** | Manage Authentication |
| **6** | Secure Remote Access |
| **7** | Monitor and Respond |

Ultra ELECTRONICS | 3eTI

# Typical ICS Purdue Model



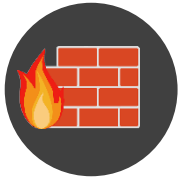
# ICS Design Assumptions

- Everyone is who they say they are
- What is said, is what is heard
- Errors can be detected and recovered
- Events are accidental not intentional
- Availability is paramount
- Reliability is success
- System will be operating for many years

# ICS Cybersecurity Best Practice

## Defense-in-Depth (DID) Architecture

# DID Cybersecurity Methods



— **'Traditional Firewall' Rules:** Control Data Flows

— **DPI Rules & Alerts:** Control Commands, Addresses & Values

— **Remote Logging:** Record significant events/changes (L1-L7)

— **End-to-End Encryption:** Securing the 'insecure by design'

— **Analytical Engine:** Network traffic and operational logs

Ultra ELECTRONICS | 3eTI

# DID Architecture Is Not Enough

## Putting operational integrity at risk

- Current DID practices are not sufficient
- Many concerns are not addressed
  - Application Server software/configuration integrity
  - PLC firmware/configuration integrity
  - Sensor/Actuator Data Integrity

# Challenges of ICS Cybersecurity

## #1 issue is security is not built-in

- Current DID methods defend against an ecosystem that had no security built-in
  - Lost of authentication of origin - ICS moved from analog to digital network
  - Can't enforce integrity among ICS components - Thus there is no default trust
- Firewalls, network traffic analysis and pattern matching technologies are band -aids solutions

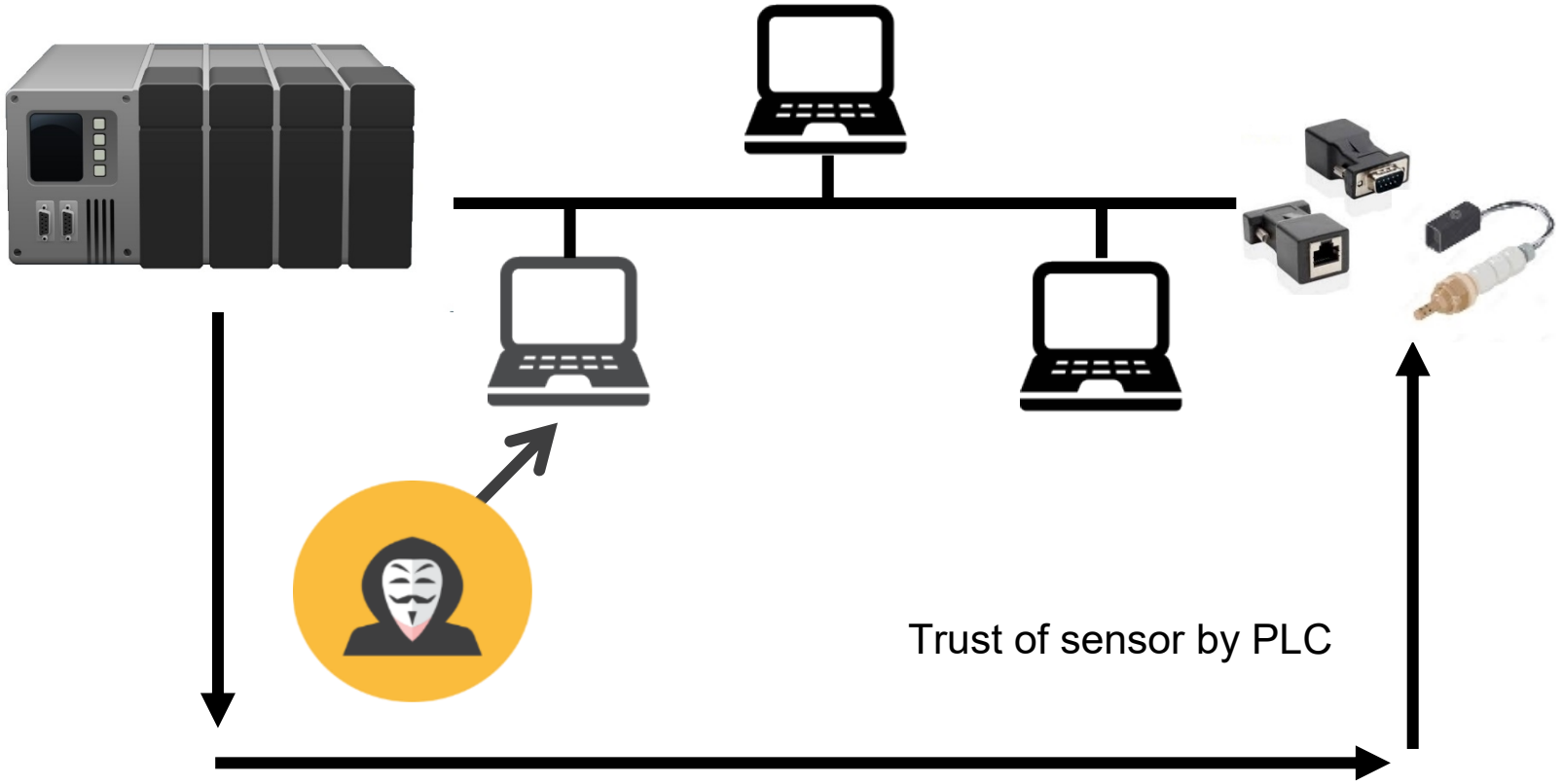
# Move Towards a Zero Trust Architecture

Zero Trust means **do not automatically trust** anything inside or outside your perimeters. **You also must verify** anything and everything trying to connect to its systems before granting access.


- It is a contrast to defending perimeters of castles
- There may not be any castle—think cloud computing
- Protect edge is as important as protect the core

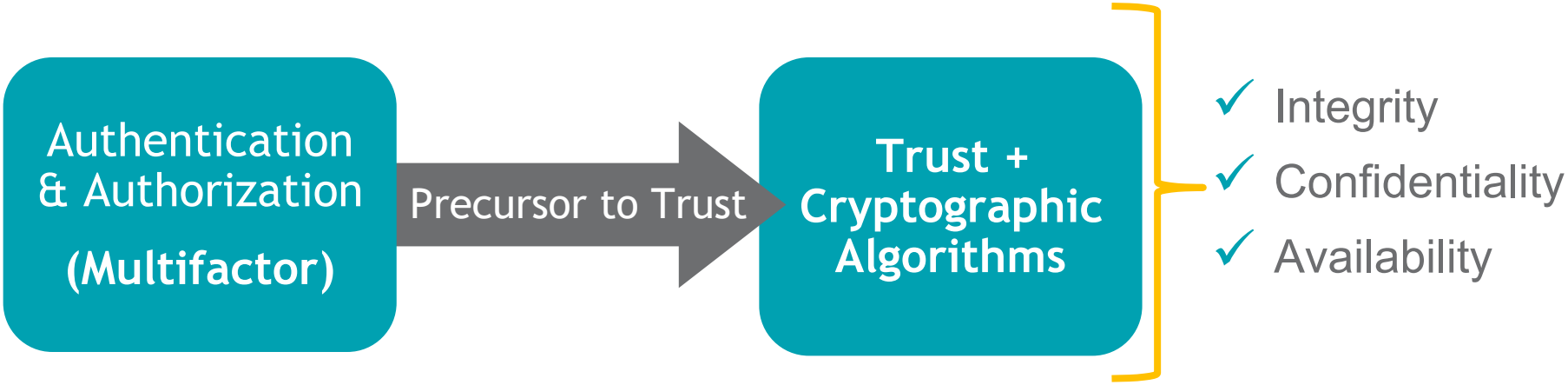
# Zero Trust Architecture in ICS

## Setup trust between the PLC and sensor



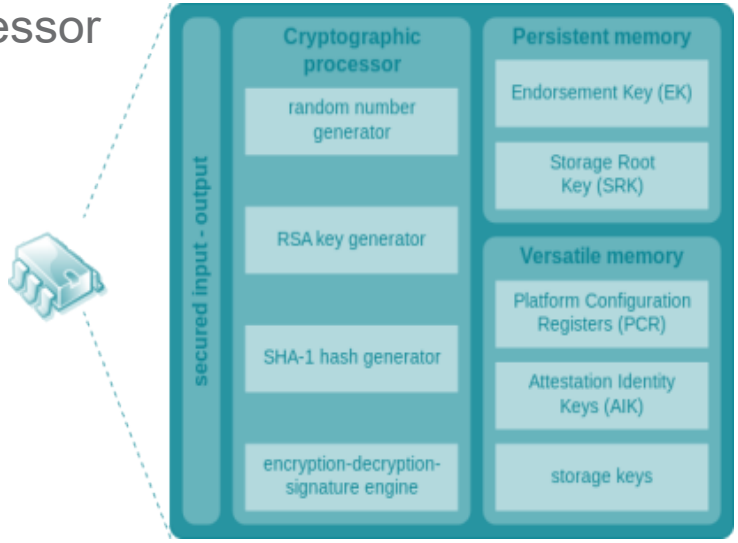
# Zero Trust Architecture

## Build on Security



# Hardware Security
## TPM (Trusted Platform Module)

- TPM is the corner stone for trusted computing
  - International standard for secure cryptoprocessor
  - Integrate keys into hardware
  - Secure key storage, generation
  - Enable trust anchor

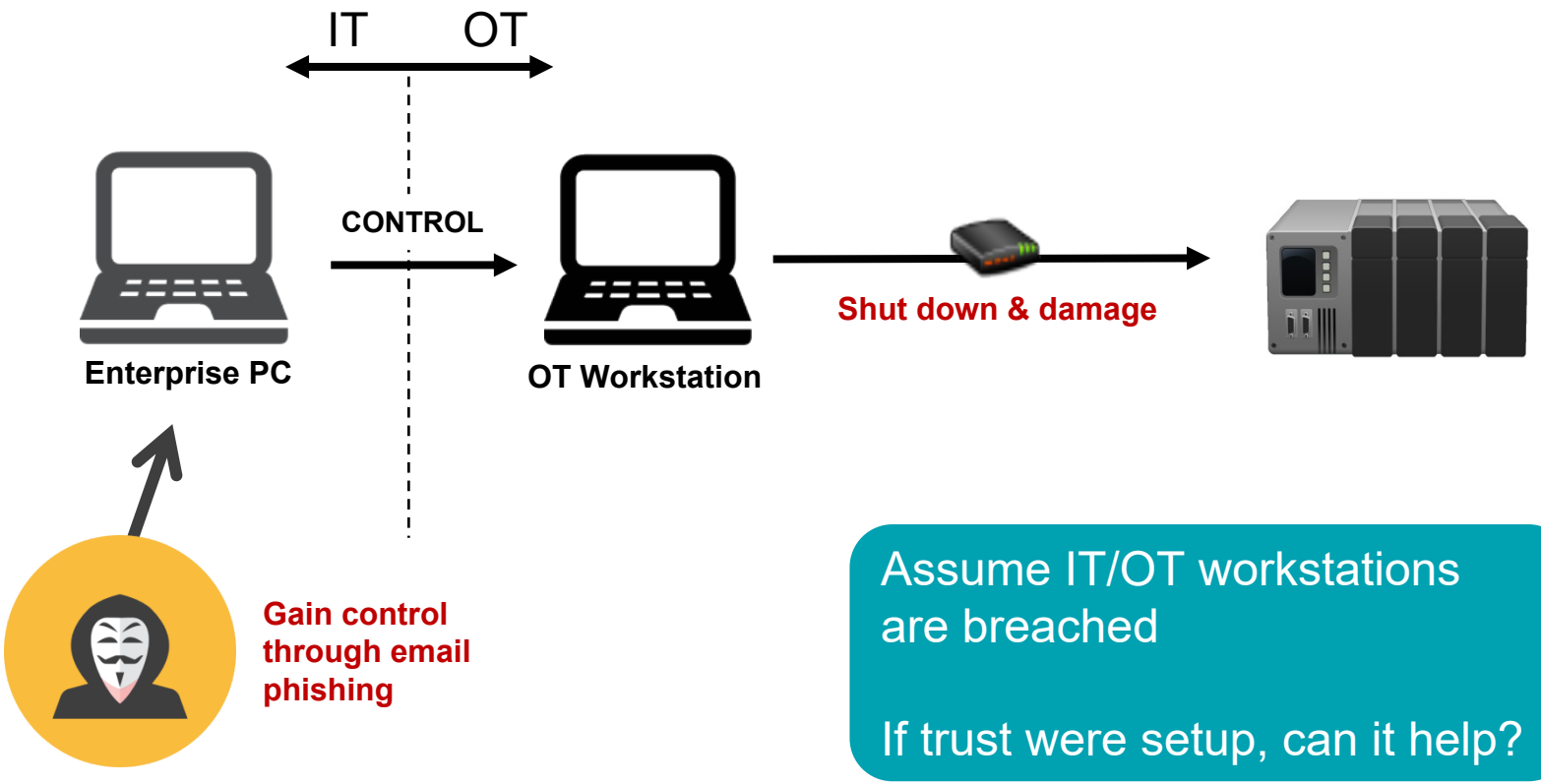



- Fit need of ICS - Setup a trust chain

PLC made by foreign Manufacture → PLC vendor → Certified solution provider → PLC owner → PLC owner onsite engineer

# Ukraine Power Grid Attack

## No trust setup

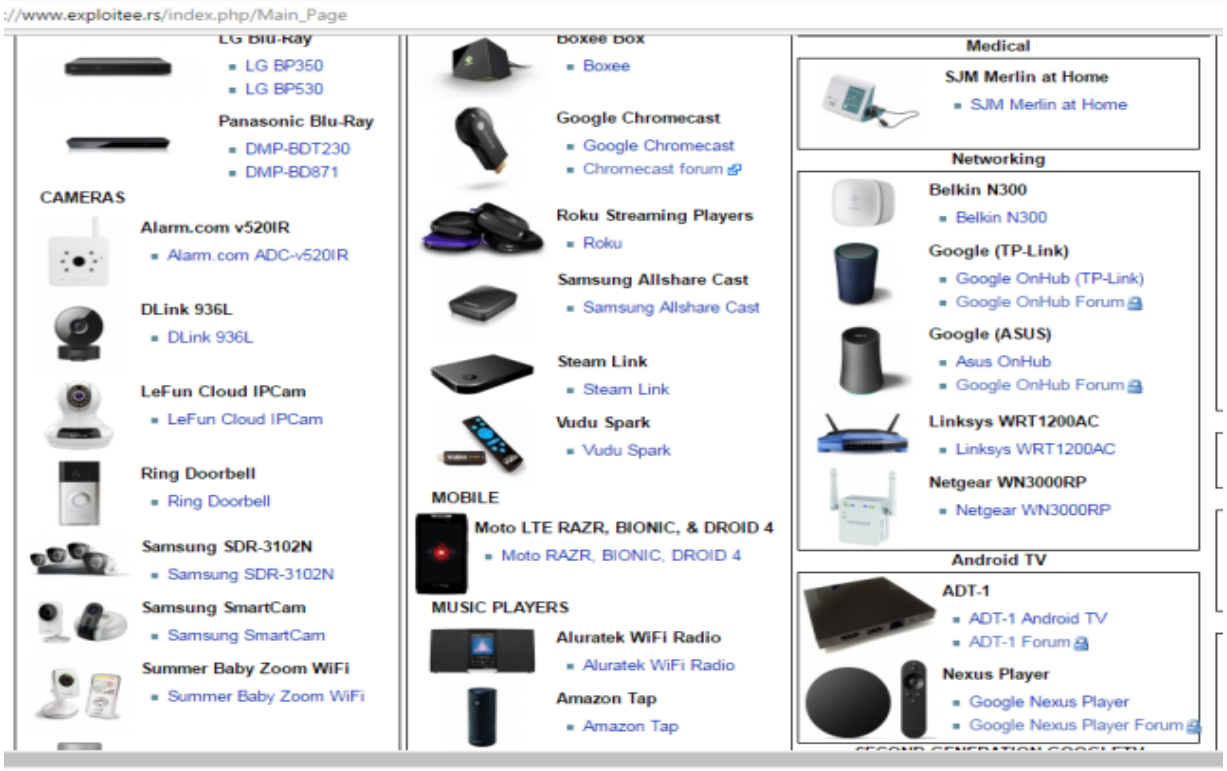



Assume IT/OT workstations are breached

If trust were setup, can it help?

# Security Design in ICS Protocol

- NO security built-in PLCs
  - Siemens S7 and S7Commplus were both hacked
- All IoTs are hackable
  - Industrial IoTs
  - Medical IoTs



# How to Enforce Zero Trust Architecture

- Manual trust setup
  - Application whitelist
  - Firewall whitelist
- Use Security Devices
  - Encryption devices have built-in trust & authentication
  - Bridge the trust between components in critical infrastructure (IP networks, LAN/VLAN and wireless)
- Protect the Edge
  - Setup security trust with encryption devices
  - Setup DPI to lock down the operation

Long term: Build-in security in critical components

# Summary

## It’s time to move to a Zero Trust Architecture for ICS

- Building a trust setup is essential
- Build security for both hardware and software
- Use cryptographic algorithms, TPM & security designed systems
- Use certified solutions (ex: FIPS 140-2, Common Criteria Validation)

# QUESTIONS

**Chris Guo**
Chris.guo@ultra-3eti.com

**Ultra Electronics, 3eTI**
www.ultra-3eti.com
info@ultra-3eti.com
linkedin.com/company/3eti
twitter.com/ultra_3eti
+1 800-449-3384
+1 301-670-6779

*Visit us at booth 519*