Intelligent Monitoring and Control: Essential Guidance for Critical Infrastructure Security

Ultra Electronics, 3eTI
April 2016
About the Presenter

- 25+ years experience aligning technology to the needs of business and in transforming concepts into sustained customer programs.
- Led development and deployment of US Navy’s first cyber-secure perimeter security surveillance and industrial controls systems.
- MBA, University of Maryland; B.S., Electrical Engineering, Howard University; B.S., Mathematics, Bowie State University.
Session Overview

- ICS cyber attacks & risks associated
- Overlooked protocol-based vulnerabilities
- An intelligent approach to a secure-system design
- Systems-based methods to leave operations uninterrupted
- US Navy, Enterprise Industrial Control System Case Study
- Summary and conclusions
Catastrophic Impacts of Critical Infrastructure Failure

Video demonstration

Project Aurora: INL cyber attack on a generator caused damaging vibration

Sayano-Shushenskaya power station: Turbine vibration caused violent damage
ICS Attacks - Growing & Getting More Intense

DHS reported a seven-fold increase between 2010-2015

- **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?

- **Israeli Electric Authority**
  - Ransomware delivered via phishing emails to the office network

98% of incidents ICS-CERT responded to in FY 2014 and FY 2015 could have been prevented
Critical Infrastructure Cyber Security is about Risk Mgmt.

What are the risks?

• Risk Management is Protection
  – Know what you want to protect (asset)
  – Know why you want to protect them (impact)
  – Know what you are willing to protect them against (threat)

• What are the Impacts?
  – Denial of view
  – Denial of control
  – Manipulation of view
  – Manipulation of control

• What are the Threats?
  – Non-targeted, non-ICS specific (e.g. Conficker/Slammer)
  – Targeted but non-ICS specific (e.g. Duqu, Shamoon)
  – Targeted and ICS specific (e.g. Stuxnet)

• Risk = Vulnerability & Threat & Impact
  – You can’t always do much about the threats or impacts
  – Therefore risk management is often vulnerability management (not attack-vector management)
Typical ICS Architecture
Enterprise to Control

- Enterprise Networks
- External Networks
- Support Network
- Process Control Network
- Control Network
- Facility Network
- Office Network
ICS Cyber Security Gap
The IT/OT gap is a divide that must be bridged

**Boundary Protections**
- Firewalls
- Network Intrusion Detection
- DMZ/Proxy Servers

**Endpoint Protections**
- Host intrusion prevention (anti-virus/firewall/application whitelisting)
- Policy enforcement
- Configuration management
- Device connection management
- Data transfer management
- External alerting & reporting

**Pre-Stuxnet Protection**
- Firewalls
- DMZ/Proxy Servers
- Air Gaps

**Post-Stuxnet Protections**
- Anti-virus on PCs & Servers
- Firewalls/data-diodes
- Configuration/patch management

**Overlooked Security Gaps**
- PLCs
- RTUs
Industrial Protocols
The backbone of critical infrastructure operations

• Common Industrial Protocols
  – DNP3, BACnet, OPC, Modbus

• What They Control
  – Industrial Control Systems - SCADA, BA, DCS
  – Supports machine-to-machine (M2M) interactions
  – Human intentions but machine interactions
    ▪ Send & receive data from machines
    ▪ Send commands to machines
    ▪ Store information generated by machines

• Security Vulnerabilities
  – Security relies on error free implementation
  – Built into application layer - Does not provide independent security (single point of failure)
  – Relies on good key management - No assurance that it has been done correctly
  – Assumes that the attacker is external
  – No mitigation in case of malicious user or software
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
Fragility vs Robustness

**FRAGILE**
- Plugging something into my system could bring the whole thing down
- A user could unintentionally impact my system
- Having malware on a PC could damage my system

**ROBUST**
- Go ahead and plug it in if you want, it can’t do anything
- Our system can withstand accidental knocks
- Malware will only be disruptive, not damaging
Fragility Causes Issues
Examples: DNP3, Havex/OPC

DHS reported a seven-fold increase in ICS incidents between 2010-2015

“98% of incidents ICS-CERT responded to in FY 2014 and FY 2015 would have been prevented”
Building a Predictable & Resilient System
Five essential guidelines to intelligently monitoring and control

1. Control which machines can speak
2. Restrict who machines listen to
3. Prevent message manipulation
4. Only allow well-formed & appropriate messages
5. Monitor for changes
US Navy Case Study
Establishing a secure critical infrastructure environment for efficient shore operations

Requirements
- Compliance with DoD and Federal mandates
- Efficiency savings through automation
- Optimization of plant operations
- Safe & Reliable operations
- Share information between stakeholders
- Connect equipment over an IP network
- Utilize open & common protocols
- Effective Force protection and public safety
- Utility critical infrastructure protection

Concerns
- Unauthorized access to networks/systems
- Loss of command & control or data integrity
- Loss or degradation of system availability
- Malware infection manipulating operations
- Cyber-attack causing physical impact
- Reputation loss due to publicized vulnerabilities or attacks
- Intentional misuse of systems or control
- Cyber attacks impacting normal operations

Project Scope
- Six Military Installations
  - 25,652 acres
  - 3,129 buildings
  - 2,822 non-bldg structures
  - 1,029 utilities locations
  - 10 runways
  - 6 hangers
  - 44 piers-wharfs
  - 3 small arms training
  - 21 small boats
- Total Plant Replacement Value (PRV): $14B
- Operations & Maintenance Budget: $500M/yr
- Reimbursable Budget: $15M/yr

*Courtesy of NDW - CNIC G2 Fact and Figures
Solution: A Defense-in-Depth Architecture

Facility/Base Operations

- Management Consoles
  - Surveillance
  - SCADA/DDC
  - Advanced Metering

- Installation Operations Center
  - SCADA
  - DDC
  - Advanced Metering
  - Remote Meters
  - Remote Cameras
  - ICS Servers
  - Video Server

- Wide Area Network
  - Data Acquisition Server (DAS)
  - Region ICS Server
  - Region Video Server

- Regional Operations Center
  - Management Consoles
    - Surveillance
    - SCADA/DDC
    - Advanced Metering

- Enterprise Systems
Solution: A Defense-in-Depth Architecture
With accredited cyber hardened approach addressing internal and external threats
Summary: Building & Operating Robust ICS
Implementing DDoS security & complying with DHS's ICS
Security Strategies will significantly reduce operational risks

<table>
<thead>
<tr>
<th></th>
<th>Application Whitelisting</th>
<th>Native application parsing and deep packet inspection (DPI), devices extend whitelisting to the data and commands sent between devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Ensure Proper Configuration Management</td>
<td>Prevents unauthorized connections over the network. Identify and prevent updates or configuration changes – allowing only to those with permission.</td>
</tr>
<tr>
<td>3</td>
<td>Reducing Your Attack Surface Area</td>
<td>Uses end-to-end encryption to prevent unauthorized devices that access the network from attacking or interfering with critical controls.</td>
</tr>
<tr>
<td>4</td>
<td>Build A Defendable Environment</td>
<td>Validated cryptographic protections to ensure that critical control traffic is isolated from other traffic even if transported over the same network.</td>
</tr>
<tr>
<td>5</td>
<td>Manage Authentication</td>
<td>Supports out-of-band management and cryptographically isolated in-band management and partitions those authorized to configure/manage security controls from those authorized to configure/manage industrial controllers.</td>
</tr>
<tr>
<td>6</td>
<td>Secure Remote Access</td>
<td>Employs FIPS 140-2 Validated and Common Criteria certified for assured protection and can be trusted to provide secure remote access over its encrypted connections.</td>
</tr>
<tr>
<td>7</td>
<td>Monitor and Respond</td>
<td>Device-level monitoring capability to detect any unauthorized activity, silently drop it, and/or send immediate alerts to authorized personnel.</td>
</tr>
</tbody>
</table>
Questions & Contacts

Benga Erinle
President
Ultra Electronics, 3eTI

301.944.1369
benga.erinle@ultra-3eti.com

www.ultra-3eti.com
info@ultra-3eti.com