Future Challenges and Changes in Industrial Cybersecurity

Sid Snitkin
VP Cybersecurity Services
ARC Advisory Group
Srsnitkin@ARCweb.com
Agenda

♦ Industrial Cybersecurity Today
  ♦ Scope, Assumptions and Strategies
  ♦ Current State and Major Gaps

♦ Changes that will Impact Current Practices
  ♦ Changes in ICS Technology
  ♦ More Dependence on IT and Cloud Systems
  ♦ Broad-based Adoption of IIoT
  ♦ New “Industrial” Use Cases like Smart Cities

♦ The Future Industrial Cybersecurity Landscape
  ♦ No More Cybersecurity Silos
  ♦ Expanded Industrial Cybersecurity Strategies

♦ Conclusions and Recommendations
About ARC Advisory Group

Who are we?  What do we do?  Who are our Clients?

♦ Industry Analyst Firm Focused on Industrial Automation and Operational Technology
♦ Established in 1986
♦ Global Presence:  US, Germany, France, Japan, China, Korea, India, Brazil, Argentina, Singapore
♦ Advisory Services for Users & Suppliers
♦ Global Events and Publications
♦ Market and Industry Research
  ◇ Automation Products
  ◇ Manufacturing IT
  ◇ ALM, PLM, SCM
  ◇ Industrial Cybersecurity
  ◇ Industrial Internet of Things (IIoT)
  ◇ Big Data & Analytics
  ◇ Industry, Infrastructure, Smart Cities

Partial List of Energy and Manufacturing Clients

Partial List of ARC’s Enterprise Software and Services Clients

Partial List of Automation Companies
Industrial Facilities are Complex, Costly and Dangerous
Preventing Problems is Essential to Safety and Profitability
Industrial Cybersecurity Today
Separate, Relatively Siloed Strategies for ICS and IT Cybersecurity

Well-Defined Use Cases, Perimeters and Architectures

IT Cyber Security

ICS Cyber Security
ARC ICS Cybersecurity Maturity Model
Mitigation Costs and Resources Rise with Risk Reduction

ICS Supplier or Cyber Service Provider
Part-time Plant ICS Staff
Full-time Plant ICS Staff
Full-time ICS Cyber Operations Group

Cybersecurity Management Solutions

Physical Security, Security Practices, Access Control, Asset Inventory, Device Hardening, Vulnerability Mgmt
DMZ’s, Firewalls, Unidirectional Gateways, Anti-Malware
App Whitelisting, Zone Firewalls, Device Firewalls
SIEM, Anomaly & Breach Detection, Threat Intelligence, Incident Mgmt

Level of Protection

Secure
Defend
Contain
Monitor
Manage

Program Maturity
Mitigation Costs and Resources Rise with Risk Reduction

**ARC ICS Cybersecurity Maturity Model**

- **Actual Resources**
  - ICS Supplier or Cyber Service Provider
  - Part-time Plant ICS Staff
  - Full-time Plant ICS Staff
  - Full-time ICS Cyber Operations Group

- **Actual Technology**

- **Resource Gap**

- **Technology Gap**

**Cybersecurity Management Solutions**

**Level of Protection**
- Physical Security, Security Practices, Access Control, Asset Inventory, Device Hardening, Vulnerability Mgmt
- DMZ’s, Firewalls, Unidirectional Gateways, Anti-Malware
- App Whitelisting, Zone Firewalls, Device Firewalls
- SIEM, Anomaly & Breach Detection
- Threat Intelligence, Incident Mgmt

**Manage**

**Program Maturity**
- Secure
- Defend
- Contain
- Monitor

---

**VISION, EXPERIENCE, ANSWERS FOR INDUSTRY**

© ARC Advisory Group • 7
Addressing Today’s Security Gap
Enabling the Benefits of Cyber Technology Investments

♦ Triage Security Management Tasks (Lower to Higher ARC Security Rungs)

♦ Allocate Security Responsibilities to the “Right” Resources (Plant/Corporate/External)
  ♦ ICS/Operational Knowledge Requirements
  ♦ Cybersecurity Knowledge Requirements

♦ Fill Internal Capability Gaps through Training and Hiring

♦ Invest in an Appropriate Cybersecurity Management Solution
  ♦ Single View of all Cyber Assets (all vendors, all kinds of assets)
  ♦ Asset Inventory, Configuration and Backup Management
  ♦ Vulnerability and Patch Management Support
  ♦ Support for Anomaly & Breach Detection and Incident Management

♦ Invest in an Appropriate Secure Remote Access Platform
  ♦ Single Access Point for Multiple Remote Users
  ♦ Controlled Access for Different Vendors/Support Groups
  ♦ Session Monitoring, Recording and Compliance Support
Future Challenges Require a Broader Industrial Cybersecurity
New Technologies, New Practices and New Use Cases

ICS-centric Developments

- Cloud-based ICS applications
- End-to-end ICS-IT Business Processes (ERP, PLM, SCM, ALM)
- Emerging ICS Technology Changes (OPA, SDN, etc.)
- Plant IIoT deployments to collect data for cloud analytics
- ICS Technology Changes (Virtualization, Edge Gateways, etc.)
- External deployments of IIoT as a platform for distributed control

IT-centric Developments

Enhancements

Major Extensions
ICS and IT Developments Will Require New Strategies & Competencies

Integrated IT-OT Strategies are Essential to Ensure End-to-End Security

♦ ICS-centric developments will require new strategies for
  ♦ Shifts in Purdue Model functionality (Virtualization, Edge Gateways, OPA)
  ♦ Flatter control system architectures (Virtualization, OPA)
  ♦ New options for containing intrusions (SDN)

♦ IT-centric developments will require new strategies for
  ♦ Recognition that operational continuity is a shared ICS/IT responsibility
  ♦ Development of end-to-end business process security
  ♦ Integration of ICS and IT security management practices and people
  ♦ Cloud Apps that require service contracts incorporate ICS requirements
IIoT Will be the Most Significant Disrupter
The Use Case Explosion Will Undermine Basic ICS Assumptions

♦ IIoT is a vision for the future of Industrial Control
  ♦ IIoT includes an open “environment” for connectivity and a multitude of Industrial “Things”
  ♦ Things may be individual devices or collections of devices with a single connection to the IIoT environment
  ♦ Things will include everything from sensors to control systems – they will include new and legacy devices
  ♦ Today companies are considering IIoT as data collection and analytics ... Tomorrow companies will leverage IIoT as their new distributed control system platform
  ♦ Use cases will explode as companies find innovative ways to leverage connectivity
Plant IIoT Deployments Require Enhanced Cybersecurity Programs
Companies are Already Launching Predictive Maintenance Programs

Cybersecurity Challenges

- New devices in plants using wi-fi and cellular, new protocols like MQTT, etc.
- Cloud interfaces to collect sensor data
- Device-level remote access for vendors to update software
- Service people accessing devices directly via bluetooth, wifi, etc.
- etc.

Cloud Apps
Analytics
Pred Maint, Optimization

Device Suppliers

Data Collector
IIoT Devices

© ARC Advisory Group • 12
IIoT is Designed to Enable Innovation
Tomorrow’s Use Cases Have Yet to Be Defined

No Clear Use Cases for Strategy Development ...
No Natural Boundaries for Segregating ICS and IT Cybersecurity Responsibilities!
A Future View of Industrial Control Systems – Power
Future Distribution Networks Require IIoT, Autonomous Control and Broad Connectivity

Ubiquitous Connectivity

Suppliers & Service Providers
Enterprise Systems
Smart Consumer Devices
Cloud Services
Mobile Devices
DER & Micro Grids
Power Plants
Remote Intelligent Assets
In-Plant Intelligent Assets
IoT Smart Module
A Future View of Industrial Control Systems – Smart Cities
Smart Cities are Hotbeds of New, Innovative IIoT and ICS Connectivity Use Cases

- Suppliers & Service Providers
- Enterprise Systems
- Smart Consumer Devices
- Building Management
- Traffic Management
- Remote Intelligent Assets
- Public Safety
- DER & Micro Grids
- Water Systems
- Smart Lighting

Ubiquitous Connectivity
Industrial Cybersecurity Has to Embrace These Developments
IIoT Demands a Broad View of Industrial Cybersecurity

♦ Cybersecurity is “the” key concern for companies that want to (need to) begin their IIoT journey

♦ Companies need general guidelines to ensure that they can securely roll out new innovative business strategies

♦ While security is important, it’s naïve to think that companies will continue to delay deployments

♦ The time has come for the ICS Cybersecurity community to acknowledge and address these future ICS/IT/IIoT cybersecurity challenges!
Industrial Organizations Will Depend on Many Kinds of Cyber Assets
Operational Continuity Requires an Integrated Cybersecurity Strategy

**Today**

- Industrial Control Systems
- Enterprise Systems
- IoT
- IIoT

**Tomorrow**

- Industrial Control Systems
- Enterprise Systems
- Cloud
- IIoT
- IoT

ICS-IT-IIoT
# A Strategy for an Integrated ICS-IT-IIoT Cybersecurity Strategy

Changes are Needed in Every Strategy Dimension

<table>
<thead>
<tr>
<th></th>
<th>Today’s Industrial Cyber Security Includes</th>
<th>Future Industrial Cyber Security Requires</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mission</strong></td>
<td>Protect Plants &amp; Infrastructure</td>
<td>Protect Plants, Infrastructure, Smart Cities</td>
</tr>
<tr>
<td></td>
<td>AIC</td>
<td>AIC and CIA</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Systems</td>
<td>Systems, IIoT Things, Mobile Devices, Cloud</td>
</tr>
<tr>
<td></td>
<td>Private Networks</td>
<td>Private &amp; Public Networks</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td>Internal ICS Groups</td>
<td>Internal ICS &amp; IT Groups</td>
</tr>
<tr>
<td></td>
<td>ICS Supplier Service Groups</td>
<td>ICS &amp; IIoT Supplier Service Groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Networking Services Partners</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloud App &amp; Data Services Partners</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
<td>Defense-in-Depth</td>
<td>Defense-in-Depth</td>
</tr>
<tr>
<td></td>
<td>Manage Security at Perimeter</td>
<td>Manage Security at Device</td>
</tr>
<tr>
<td></td>
<td>Secure Networks</td>
<td>Secure Networks and Messages</td>
</tr>
<tr>
<td></td>
<td>Secure Zones</td>
<td>Secure Zones, Devices, Messages, Data</td>
</tr>
<tr>
<td></td>
<td>Authorize People</td>
<td>Authorize People &amp; Devices</td>
</tr>
<tr>
<td></td>
<td>Manage Software Vulnerabilities</td>
<td>Manage Software &amp; Device Vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>Secure Servers</td>
<td>Secure Servers and Data</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td>Endpoint Security Wrappers</td>
<td>Secure-by-Design Endpoint Devices</td>
</tr>
<tr>
<td></td>
<td>Network Firewalls</td>
<td>Network and Device Firewalls</td>
</tr>
<tr>
<td></td>
<td>Data Encryption</td>
<td>Data &amp; Message Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy Monitoring &amp; Enforcement</td>
</tr>
</tbody>
</table>
Conclusions and Recommendations

♦ Today’s unmaintained/unused security products are providing a false sense of security. Address your security gaps and really reduce your cyber risks:
  ♦ Hire, train and develop relationships with external support groups
  ♦ Implement an appropriate Cybersecurity Management Solution
  ♦ Implement an appropriate remote access solution

♦ Integrating IT and ICS cybersecurity efforts is essential to achieve operational continuity:
  ♦ Loss of IT systems can shut down operations as quickly as loss of ICS
  ♦ Many ICS attacks originate in corporate IT systems
  ♦ IT expertise is needed for incident management and recovery

♦ Recognize that cybersecurity is a key enabler of IIoT improvement efforts:
  ♦ Learn about IIoT and support IIoT Cybersecurity standards efforts
  ♦ Develop a cybersecurity program that enables safe, timely deployment of your corporate improvement efforts
Thank You.

For more information:
Contact the author at srsnitkin@arcweb.com
Visit our web pages at www.arcweb.com
Attend ARC’s 2018 Forum in Orlando, Feb 12-15