ICS Cybersecurity Programs for Multi-national Corporations

Kaspersky Industrial Control Systems Cybersecurity International Summit: Safeguarding Progress

Melissa Crawford | Plant Security Services | September 28-30, 2017
Introduction: Siemens Plant Security Services

- Siemens Plant Security Services business provides industrial companies with comprehensive expertise as well as the specialist skills and knowledge of a global network of experts for automation and cyber security.

- The scalable offer includes comprehensive consulting, technical implementation and continuous service (Manage Security). The portfolio is available for existing Siemens plants as well as for technical plants from third-party providers.

Melissa Crawford
Global Cyber Security Consultant for Industrial Control Systems
- 8 years experience global ICS/SCADA projects
- Responsible for development of cyber security strategies for multinational corporations, IEC62443 Assessments and remote incident handling

Vladimir Vylkov
Principal Cyber Security Consultant
- >20 Years Experience ICS
- Responsible for global technical consulting, risk and vulnerability assessments, business development activities for global sales
Overview

- Introduction to MultiNational Corporations
- Principles of the ICS cybersecurity Program for MultiNational Corporations
- Program Rollout and Division of Tasks
- Maintenance and Monitoring Phase
- Reference MNC Examples: Linde and Siemens
- Closing, Contact & Security Information
Multinational Corporations

Common Characteristics

Production Facilities in multiple countries and continents
- Numerous facilities: 15 to 1000
- Country specific risks and regulations
- Cultural and Language barriers
- Country-specific security level requirements

Global Headquarters and regional organizations
Localized operating procedures

Source: Shutterstock
Pillars of Effective ICS Security Program

People
- Formation of ICS cybersecurity competence team
- Establishing cybersecurity awareness training program for all plant personnel

Processes
- Establishment of effective operational processes and security guidelines

Technology
- Identification and validation of effective technical security controls
- Continuous monitoring of the plant security and compliance status
Top-Down Approach:
ICS Security Strategy Begins with an Initiative at the Board Level

Security Strategy
- Board/CEO

Organization for ICS Security
- CIO/CISO

Security Program Development
- Global

Implementation and Management
- Regional
Cybersecurity Program Principals: Basic Phases of the Program

Phase Order

1. Asset Identification and Risk Assessment
2. Guideline / Policy Development
3. Awareness Training and Rollout
4. Governance and Follow-up Auditing
5. Monitoring Center
6. Built-in Lifecycle Protection Measures
ICS Cybersecurity Program: 
Major Elements to be Considered

<table>
<thead>
<tr>
<th>Training</th>
<th>Policies &amp; Procedures</th>
<th>Host Based Controls</th>
<th>Network Based Controls</th>
<th>Risk Management</th>
<th>Project Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness training</td>
<td>DR + IR</td>
<td>Hardening</td>
<td>Security Monitoring &amp; Analysis</td>
<td>Inventory and Asset DB</td>
<td>PM from MNC and Partner</td>
</tr>
<tr>
<td>Technical Security Training</td>
<td>Procurement Guidelines</td>
<td>Whitelisting</td>
<td>NGFW</td>
<td>Risk analysis</td>
<td>Contractor Management</td>
</tr>
<tr>
<td>Training on the Job (Rollout)</td>
<td>Removable Media policy</td>
<td>Antivirus</td>
<td>Network Segregation</td>
<td>Incident Response</td>
<td>Roll-Out Management</td>
</tr>
<tr>
<td></td>
<td>User Management</td>
<td>Patch Management</td>
<td>IDS/ IPS</td>
<td>KPI Monitoring</td>
<td>Overall Security Concept</td>
</tr>
<tr>
<td></td>
<td>RAS Concept</td>
<td></td>
<td>Network Hardening</td>
<td>Security Testing</td>
<td>Organizational Concept</td>
</tr>
<tr>
<td></td>
<td>Change Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Standards for Local Network Design</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Technical Controls**

- Standards for Local Network Design
- Technical Controls
- Removable Media policy
- Patch Management
- Physical measures
- User Management
- DR + IR
- Procurement Guidelines
Security Rollout – Team Distribution: Take into account Geographical Location, Cultural Variations and Timezones

Central Coordination HQ / Project Management

- Americas
- EMEA
- Asia
- Pacific

Core Team 1
Core Team 2
Core Team 3
Core Team 4
Security Rollout:
Ensure Appropriate Skill-set in Forming the Core Teams

Competence Profile of Core Team (each of the 4 Groups with 4-5 people):

<table>
<thead>
<tr>
<th>Industry Expertise</th>
<th>Project Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Competencies</td>
<td>Site Commissioning Experience</td>
</tr>
<tr>
<td>Network Security Competencies</td>
<td>Integration Know-How</td>
</tr>
</tbody>
</table>
Implementation: Global and Regional Team Distribution of Tasks

Global Tasks HQ
- Quality Assurance
  - Single point of contact
  - Ensure quality and check the proper implementation per concept during the global implementation
- Advanced Technical Support
  - Provide specific configuration details
  - Provide support in case of lack of regional resources
  - Coordinate and assess the implementation of measures applying to configuration changes
- Organizational Structure
  - Change Management Consulting
  - Security Integration into Lifecycle Management
- Training
  - Security Awareness Training
  - ICS Security Feature Training for administrators

Regional Team Tasks
- Quality Assurance
  - Single point of contact
  - Ensure quality and check the proper implementation according to HQ concept
- Technical Support
  - Implement specific configuration details from HQ
  - Get support in case of lack of regional resources from HQ
  - Coordinate and assess the implementation of measures applying Engineering Change Requests
- Organizational Structure from the HQ
  - Change Management Consulting
  - Security Integration into Lifecycle Management
- Training
  - Security Awareness Training
  - ICS Security Feature Training for administrators
  - Training Plant Personnel on the Job during Installation
ICS Security Measures Implementation:
Security Partner Synchronization

- MNC Global HQ
  - Information on Start of Implementation
  - Assignment of Implementation
  - Own capabilities?
    - Yes: Execute implementation
    - No: Notify HQ of finish (Quality assurance)

- MNC Regional Organization
  - Request for quotation
  - Ordering support

- Security Partner HQ
  - Inform the region
  - Support of HQ
    - No: Starting Preparation
    - Yes: Offer generation

- Security Partner RC
  - Starting Preparation
  - Own capabilities?
    - No: Support by HQ Seniors
    - Yes: Executing implementation
Maintenance and Monitoring: Continuously Monitor and Adapt the Security Program to the Changing Threat Scenario

Focus: Ensure risks are appropriately mitigated with effective measures and according with the current threat landscape
Plant Security Reference
Linde Gas – Industrial Security Program

Profile
• The Linde Group is a world leading supplier of industrial, process and specialty gases.
• Linde products and services can be found in nearly every industry, in more than 100 countries.

Challenge
• Different maturity level for industrial security at Linde Gas
• Need for holistic implementation concept

Solution
• Development of a comprehensive program for industrial security for >600 production sites and all remote operation centers
• Support of pilot implementation in Region Germany and Asia Pacific

Customer benefit
• Unified approach for a global roll out to achieve a higher maturity level for Industrial Security
• Cost effective and optimal strategy to deploy on all platforms globally (non-vendor specific)
Plant Security Reference
Air Separation Company Examples

Security Measures for HMI Security Zone:
- Asset management
- User and Password management
- Hardening
- Monitoring
- Backup/Restore
- VM Backup/Restore
- VM Management
- Patch Management
- AV/Whitelisting
- VM Out-of-band Management
- Site Firewall with port filtering

Security Measures for Control Security Zone:
- Firmware update management
- Asset management
- Hardening
- Password management
- FS/SIS Password management
- Site firewall
Holistic Security Concept Takes Security on the Next Level - A Holistic Approach for IT and OT

HSC answers key questions for security in business

“What in my business do I need to protect?”

Identification of the critical business assets is a core component of the concept.

“Which level of security do I need?”

Security level drives requirements, in alignment with IEC 62443, to protect against attacks.

“How do I protect the specific assets?”

Standards based security solutions are applied to protect and monitor the critical assets.

HSC addresses 5 levers including the IT:

- IT Infrastructure
- Handle Incidents
- Improve process
- Enhance Awareness
- Security features

Unrestricted © Siemens AG 2017. All rights reserved.
Page 16 April 2017
Protection Levels are the Key Criteria and Cover Security Functionalities and Processes

Security functions:
- Based on IEC 62443-3-3
- Security Level 1-4

Security process:
- Based on IEC 62443-2-4 and ISO27001
- Maturity Level 1 - 4

Protection Level (PL)

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Protection Levels:
- PL 1
- PL 2
- PL 3
- PL 4
Security in Siemens Production

- Siemens has defined a Holistic Security Concept (HSC) based upon IEC 62443 & ISO 27000

- HSC protects integrity and safeguards confidentiality of the development and manufacturing environment

- HSC measures are defined and monitored in development and production departments
## Selected HSC Security Measures from PL 1 to PL 4

<table>
<thead>
<tr>
<th>Secure Physical Access</th>
<th>Organize Security</th>
<th>Secure Solution Design</th>
<th>Secure Operations</th>
<th>Secure Lifecycle management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revolving doors with card reader and PIN; Video Surveillance and/or IRIS Scanner at door</td>
<td>Revolving doors with card reader</td>
<td>Firewalls with Fail Close (e.g. Next Generation Firewall)</td>
<td>…</td>
<td>Online security functionality verification</td>
</tr>
<tr>
<td>Doors with card reader</td>
<td>No Email, No WWW, etc. in Secure Cell</td>
<td>2 PCs (Secure Cell/outside)</td>
<td>…</td>
<td>Automated backup / recovery</td>
</tr>
<tr>
<td>Locked building/doors with keys</td>
<td>Persons responsible for security within own organization</td>
<td>Physical network segmentation or equivalent (e.g. SCALANCE )</td>
<td>…</td>
<td>Remote access with cRSP or equivalent</td>
</tr>
<tr>
<td></td>
<td>Mandatory security education</td>
<td>Network segmentation Firewall protection (e.g. SCALANCE S)</td>
<td>…</td>
<td>Backup verification</td>
</tr>
<tr>
<td></td>
<td>Awareness training (e.g. Operator Awareness Training)</td>
<td></td>
<td>…</td>
<td>Remote access restriction (e.g. need to connect principle)</td>
</tr>
<tr>
<td></td>
<td>Mandatory rules on USB sticks (e.g. Whitelisting)</td>
<td></td>
<td>…</td>
<td>Backup / recovery system</td>
</tr>
</tbody>
</table>

- **PL 1:**
  - Locked building/doors with keys
  - Awareness training (e.g. Operator Awareness Training)
  - Mandatory rules on USB sticks (e.g. Whitelisting)

- **PL 2:**
  - Doors with card reader
  - Dual approval for critical actions

- **PL 3:**
  - Revolving doors with card reader
  - No Email, No WWW, etc. in Secure Cell

- **PL 4:**
  - Revolving doors with card reader and PIN; Video Surveillance and/or IRIS Scanner at door
  - Dual approval for critical actions
Elektronikwerk Amberg  
Implementation and operation of Industrial Security Monitoring

---

**Challenge**
- Highly sensitive IT-controlled processes
- Fully networked automation environment
- Comprehensive data flow and database
- Protection against industrial espionage, manipulation and hacker activities

**Solution**
- Implementation of Defense in Depth with S7-1500 and SCALANCE S using TIA Portal.
- Monitoring of security-relevant events
- Monthly status report on plant and system security
- Recommendations for optimizing the level of protection

---

**Profil**
Elektronikwerk Amberg is a prime example of a digital factory. The factory uses cutting-edge technologies to produce approximately fifteen million SIMATIC products each year.

---

**Customer benefit**
- Protection of networks and TIA components according to the defense-in-depth security concept
- Solid, in-depth security information thanks to Security Information and Event Management (SIEM)
- Continuous optimization of the security concept
<table>
<thead>
<tr>
<th><strong>Profile</strong></th>
<th><strong>Challenge</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Sinopec Qingdao Refinery is a super-large refining and petrochemical complex with a distillation capacity of 10 million tons per year</td>
<td>Operations without disturbances: Protect against all kind of disturbing viruses</td>
</tr>
<tr>
<td>It produces gasoline, kerosene, diesel, LPG, polypropylene and styrene</td>
<td>Smooth implementation</td>
</tr>
<tr>
<td></td>
<td>Largest standalone industrial security project worldwide</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Solution</strong></th>
<th><strong>Customer benefit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of a security solution for the PCS 7 environment including DMZ, Firewall, Anti-Virus, Patch Management, User Management and System hardening</td>
<td>Continuous protection of plant: reduce risk and maintain production availability</td>
</tr>
<tr>
<td>2 weeks implementation during downtime of the plant</td>
<td>Zero incidents or infections after the project: 18 months of safe operation</td>
</tr>
<tr>
<td></td>
<td>Blueprint for Chinese petrochemical customers</td>
</tr>
</tbody>
</table>
Closing Remarks, Questions, Contact

Siemens AG
Digital Factory
DF CS DS
Postbox 3240
91050 Erlangen
GERMANY

Melissa Crawford
Global cybersecurity Consultant for Industrial Control Systems
Digital Factory / DE / Plant Security Services
E-mail: melisssa.crawford@siemens.com

siemens.com/plant-security-services
Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.