Cyber Security for Process Control Systems

ABB’s view

Tomas Lindström, Cyber Security Manager, ABB Control Technologies
Cyber security for process control systems for vendors and system owners

- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services
## ABB: the pioneering technology leader

### What (Offering)

<table>
<thead>
<tr>
<th>Pioneering technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products 58%</td>
</tr>
<tr>
<td>Systems 24%</td>
</tr>
<tr>
<td>Services &amp; software 18%</td>
</tr>
</tbody>
</table>

### For whom (Customers)

<table>
<thead>
<tr>
<th>Utilities</th>
<th>Industry</th>
<th>Transport &amp; Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>~35% of revenue</td>
<td>~40% of revenue</td>
<td>~25% of revenue</td>
</tr>
</tbody>
</table>

### Where (Geographies)

<table>
<thead>
<tr>
<th>Globally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia, Middle East, Africa 38%</td>
</tr>
<tr>
<td>Americas 29%</td>
</tr>
<tr>
<td>Europe 33%</td>
</tr>
</tbody>
</table>

| ~$35 bn revenue | ~100 countries | ~132,000 employees |
## ABB Ability™ System 800xA, the #1 DCS in process control

The process information core

### Plant-wide consolidation, collaboration and optimization

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One system solution for process-, power automation and safety</td>
<td>Plant centric view – operational excellence</td>
</tr>
<tr>
<td>Seamless connectivity to value added systems and applications</td>
<td>Lower cost of ownership</td>
</tr>
<tr>
<td>Full scope asset monitoring</td>
<td>Streamline procedures and become more predictive</td>
</tr>
<tr>
<td>Integrated operations with embedded functionality</td>
<td>Operator effectiveness reducing downtime</td>
</tr>
</tbody>
</table>

### Proven track record

- **10,000** systems
- **100** countries
- **45,000** controllers
- **40,000** workstations
- **30,000,000** I/Os
Agenda

Cyber security for process control systems for vendors and system owners

- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services
Cyber Security @ ABB

Three guiding principles

**Reality**
There is no such thing as 100% or absolute security

**Process**
Cyber security is not destination but an evolving target – it is not a product but a process

**Balance**
Cyber security is about finding the right balance – it impacts usability and increases cost

Cyber security is all about risk management
ABB Cyber Security Approach

Full lifecycle coverage

Product
Design
Implementation
Verification
Release
Support

Project
Design
Engineering
FAT
Commissioning
SAT

Plant
Operation
Maintenance
Review
Upgrade

ABB requires the same of our suppliers
Cyber Security Best Practices
International standards and guidelines

Details of Operations
Design Details
Completeness

IT Energy Industrial Autom.

NIST 800-53
ICE 62351
ICE 62443
ISO 27K
IEEE P 1686
NIST Cyber Security Framework

Details of Operations
Design Details
Completeness

Lots of similar support available

Source: ESCoRTS Project (European network for the Security of Control and Real-Time Systems), with ABB additions.
Cyber Security Best Practices

The IEC 62443 standard

Focus for Integrators and Operators

Focus for system/product Vendors
Agenda

Cyber security for process control systems for vendors and system owners
- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services
## Cyber security for the Product Lifecycle

The SD³ + C Security Framework

|------------------|--------------------------------------------------------------------------------------------------|
| Secure by Default | Default installation and usage with minimal attack surface  
                  Built in functions for Defense in Depth                                                   |
| Secure in Deployment | Support for Secure Project and Plant Lifecycle  
                        Validation of 3rd party software and solutions                                           |
| Communication     | Correct information to those who need to know                                                   |
Security in the Product Development Process

Security verification and validation

Overview

Product- / System Type Testing of security requirements

Robustness testing:
– by product R&D
– and product independent test center: DSAC

Testing by ABB’s Device Security Assurance Center (DSAC)

Device Profiling

Vulnerability scanning
(checking for known vulnerabilities)

Network flooding

Fuzzing
("checking for unknown vulnerabilities")

Thorough vendor testing more effective than 3rd party certification
Communication

Inform those who need to know in case of problems

Reporting a suspected problem:
- ABB Customer: The regular ABB contact
- Others: www.abb.com/cybersecurity or cybersecurity@ch.abb.com

ABB’s responses in case of product vulnerability:
- Responsible/Coordinated disclosure
- Field Communication: “Security Advisory” for customers via MyControlSystem
- If publically disclosed ➔ public response: ICS-CERT and www.abb.com/cybersecurity
Agenda

- Cyber security for process control systems for vendors and system owners
  - Guiding principles and concepts
  - Framework for Product Security
  - Implementing Defense in Depth for a process control system
  - Maintaining a secure system: Cyber Security Services
A Cyber Security Framework for system owners

Overview

1. Standards: Guidelines
   - Risk Assessment
   - Management Buy-in
   - Security Policy

2. Balance Security Measures:
   - Value for me ⇔ Value for X ⇔ Mitigation cost
   - Combine measures:
     - Defense in Depth
     - Work with system vendors
     - Request selected measures

3. Incident response
   - Disaster recovery

4. Training for all staff
   - Audit policy compliance

October 2, 2017
Slide 15
## Categories of Security Measures

The 7 Foundational Requirements of IEC 62443

| FR 1 Identification and authentication control | Who |
| User, software, & device authentication |
| Account management |

| FR 2 Use control | What |
| Authorization enforcement |
| Auditable events |

| FR 3 System integrity | Protect |
| Communication integrity |
| Malicious code protection |

| FR 4 Data confidentiality | Protect |
| Information confidentiality |

| FR 5 Restricted data flow | Protect |
| Network segmentation |

| FR 6 Timely response to events | Detect |
| Audit log accessibility |
| Continuous monitoring |

| FR 7 Resource availability | Protect |
| Denial of service protection |
| Control system backup |
Defense in Depth in 800xA

Who/What, Protect Hosts

- Secure Remote Access
- Malware protection: Antivirus and Application Whitelisting
- Windows User Authentication
- 800xA Role based Access Control
- Device Security Assurance Center (DSAC): Robustness tested products
- Device Security Assurance Center (DSAC): Robustness tested products
- DoS protection: Storm filter
- DoS protection: Loop filter
- Secure communication: IPSec
- Host Firewalls
- Automatic Hardening by System installer
- Validated Security Updates
- Secure Remote Access
- Malware protection: Antivirus and Application Whitelisting
- Windows User Authentication
- 800xA Role based Access Control
- Device Security Assurance Center (DSAC): Robustness tested products
- Device Security Assurance Center (DSAC): Robustness tested products
- DoS protection: Storm filter
- DoS protection: Loop filter
- Secure communication: IPSec
- Host Firewalls
- Automatic Hardening by System installer
- Validated Security Updates
System 800xA Networks

Protect Networks

RNRP:
System Network Redundancy
with Separate Networks

System Zoning
with full redundancy
(RNRP router/firewall)

DoS protection:
Rate limitation

Field Network
with ring redundancy
Audit logging with System 800xA
Detect 1, Create the information

Enable Logging/Audit Trail

- Operating system (Windows) events
- Control system events
- System User Actions
  800xA Audit Trail

System monitoring

- Control system built-in self-supervision
- Additional monitoring functions/log sources
  - Servers and Workstations
  - Network equipment
  - Add-on products (e.g. Malware protection)
- Collect via Windows Event Log, SNMP, SysLog
- More information from integrated equipment
  - ABB’s Network Equipment NE800
  - ABB’s PC Network Software Monitoring
Detect 2, Analyze the information

### Collection/Storage
- Collection in the control system
- Dedicated SIEM
  - Security
  - Information and Event
  - Management system

### Centralization
- Infrastructure by system owner
- Infrastructure by system vendor

### Monitoring/Analysis
- Performed by system owner
- Performed by system vendor
Cyber security for process control systems for vendors and system owners

- Guiding principles and concepts
- Framework for Product Security
- Implementing Defense in Depth for a process control system
- Maintaining a secure system: Cyber Security Services
Cyber Security Services

Cyber Security Fingerprint

- Interview
  Data collection

- Analysis

→ Report with
  - Cyber security status
    Identifies strengths and weaknesses
  - Recommendations on improvements

- Based on widely accepted industry standards*

*) Including, but not limited to: NERC-CIP, OLF-104, ISA-62443 (ISA99), ISO 27000
Security for a Process Control System: We can make it if we cooperate!