Developing an Industrial Controls Security Framework

Ernie Hayden CISSP CEH GICSP
Executive Consultant
www.securicon.com
Agenda

- Agenda*
- The Opportunity
- The Approach
- Current Framework
- Future Plans/Changes
- Q&A
Part 2 of the Presentation...

- Introduction to **AcuSec™ Securicon’s Critical Infrastructure Risk Assessment Methodology**
- Introduced by...
  
  Mr. Harry Regan CISM CISSP PSP
  VP, Commercial Services
  Securicon, LLC

*The AcuSec Methodology provides organizations with:*

- A Repeatable Process
- Consistent Terminology
- Measureable Results
The Opportunity…

- Major Global Consumer Products Company Hired Securicon to Help with ICS Security…

- Key Needs
  - Kick-start ICS Security for 20+ global factories
  - Begin assessing ICS Security program from organizational perspective as well as at plants
  - Assist in hiring ICS Security Lead
  - Develop framework for implementing ICS Security across the corporation

CAVEAT
Allowed to Discuss Framework but Company Wishes to Remain Anonymous
The Framework Began

Key Questions to Be Answered…
  ◦ Purpose?
  ◦ Functions of Framework?
  ◦ Scope?
Purpose of the Framework

- **Philosophy:**
  - ICS systems are the foundation of the production systems and factories
  - Without their safe, secure and reliable operations production and shipments negatively impacted...
    - Customer Satisfaction ↘
    - Corporate Revenue ↘

- **The Framework establishes the key elements of ICS security for the plants and factory operations**
  - For: ICS architecture, design, procurement, operation, maintenance, repair and decommissioning...

- **Overall Intent:**
  - Compliment and integrate with overall cyber and physical security controls for corporation and associated regional/national laws affecting the company
Functions of a Conceptual Framework

- **Criteria:**
  - Does it help analyst/policymaker understand and provide structure to a complex phenomena (i.e., ICS Security)?
  - Does it help focus on important dimensions of policy design?
  - Does it help generate additional hypotheses for possible future action?
  - Does it offer guidance for prioritizing actions?

- **Reference:**
  - *Border Security: The Complexity of the Challenge*
Scope of Framework

- **Key Reference:** ISA Security of Industrial Automation and Control Systems Master Glossary (March 2013) – ISA–TR62443–1–2

- **ICS Defined As:**
  - Personnel, hardware and software –
    - that can affect or influence the safe, secure, and reliable operation of an industrial process
    - Involved in the operation of the industrial processes and that can affect or influence its safe, secure and reliable operation
Scope (Continued)

- **Systems Include** –
  - ICS including distributed control systems (DCS)
  - Programmable Logic Controllers (PLCs)
  - Remote Terminal Units (RTUs)
  - Intelligent Electronic Devices (IED)
  - SCADA
  - Networked Electronic Sensing and Control, Monitoring and Diagnostic Systems – Includes Safety Instrumented Systems (SIS)
  - Associated Information Systems
    - Advanced/Multivariable Control, Online Optimizers, Dedicated Equipment Monitors, Process Historians, Manufacturing Execution Systems (MES)
  - Associated Human, Network or Machine Interfaces for Control, Safety and Mfg Ops
Primary ICS Security Philosophy

- Specifically Expressed in Framework
- Needed to Aid in IT/OT “Communications”

A – Availability

I – Integrity

C – Confidentiality
“REFERENCE MODEL:” is a framework for understanding significant relationships among entities in select environments – and for development of consistent standards and specifications supporting that environment.

- **Basis:** Purdue Model
Now – What Standards to Follow?
First, an Inventory...

NIST Standards

Framework for Improving Critical Infrastructure Cybersecurity

Protesting Industrial Control Systems

ISO 27001/2

International & Industry Standards

ISA/IEC-62443 Products

RIPE Framework not available at this time
Decision: Basic/Foundational Requirements

- AC – Access Control
- AT – Awareness & Training**
- AU – Audit & Accountability
- BC – Business Continuity
- CM – Configuration Management**
- IR – Incident Response

- PM – Program Management**
- PS – Personnel & Security
- RA – Risk Analysis**
- SC – System & Communication Protection
- SA – System and Services Acquisition & Development**

** = Initial Areas of Focus

Similar to NIST 800–53 Security Control Classes, Families & Identifiers
Conclusion: Foundational Standards to Use


- NIST 800–82, *Guide to Industrial Controls Systems Security (R2)*


- ICS–CERT Recommended Practices
Next Step – The Control Matrix
<table>
<thead>
<tr>
<th>Functional Requirement</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>System and Communication Protection (SC)</td>
<td>SC-1 Network Segmentation</td>
<td>SC-1.1 Develop the Network Segmentation Architecture -- A network segmentation countermeasure strategy employing security zones shall be developed for ICS devices based upon the risk level of the ICS.</td>
<td>ANSI/ISA-99.02.01-2009, 4.3.3.4.1, NIST 800-53 R4 AC-4, SC-1, SC-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SC-1.2 Employ Isolation or Segmentation on High-Risk ICS - High-risk ICS shall be isolated from or employ a barrier device to separate it from other zones with different security levels or risks.</td>
<td>ANSI/ISA-99.02.01-2009, 4.3.3.4.2, NIST 800-53 R4 AC-4, SC-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SC-1.3 Block Non-Essential Communications with Barrier Devices -- Barrier devices shall block all non-essential communications in and out of the security zone containing critical control equipment.</td>
<td>ANSI/ISA-99.02.01-2009, 4.3.3.4.3, NIST 800-83, R4, SC-7</td>
</tr>
</tbody>
</table>

Many formatting ideas taken from NIST Cybersecurity Framework
Risk & Impact Analysis
Framework is intended to provide guidance and a semblance of criteria in order to ascertain ICS impact levels...to be ultimately used to categorize ICS components and systems for risk assessments...

Reference: 800–82, Revision 2, Page 88
Table 6-2. Possible Definitions for ICS Impact Levels Based on Product Produced, Industry and Security Concerns

<table>
<thead>
<tr>
<th>Category</th>
<th>Low-Impact</th>
<th>Moderate-Impact</th>
<th>High-Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Produced</td>
<td>• Non-hazardous materials or products</td>
<td>• Some hazardous products or steps during production</td>
<td>• Critical infrastructure (e.g., electricity)</td>
</tr>
<tr>
<td></td>
<td>• Non-ingested consumer products</td>
<td>• High amount of proprietary information</td>
<td>• Hazardous materials</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Ingested products</td>
</tr>
<tr>
<td>Industry Examples</td>
<td>• Plastic injection molding</td>
<td>• Automotive metal industries</td>
<td>• Utilities</td>
</tr>
<tr>
<td></td>
<td>• Warehouse applications</td>
<td>• Pulp and paper</td>
<td>• Petrochemical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Semiconductors</td>
<td>• Food and beverage</td>
</tr>
<tr>
<td>Security Concerns</td>
<td>• Protection against minor injuries</td>
<td>• Protection against moderate injuries</td>
<td>• Pharmaceutical</td>
</tr>
<tr>
<td></td>
<td>• Ensuring uptime</td>
<td>• Ensuring uptime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Capital investment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protection against major injuries/loss of life</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensuring uptime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Capital investment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trade secrets</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensuring basic social services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Regulatory compliance</td>
<td></td>
</tr>
</tbody>
</table>
ICS Cybersecurity Model/Grading
<table>
<thead>
<tr>
<th>Grade</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (GREEN)</td>
<td>Adaptive -- The organization adapts its ICS cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.</td>
</tr>
<tr>
<td>B (YELLOW)</td>
<td>Repeatable – Managed -- The organization’s ICS security practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly performed and updated</td>
</tr>
<tr>
<td>C (ORANGE)</td>
<td>Ad Hoc -- ICS Security practices are approved by local management, partially implemented but not broadly or effectively implemented.</td>
</tr>
<tr>
<td>D (RED)</td>
<td>Not Implemented or Marginal -- ICS security management practices are not formalized, and security is managed in an ad hoc and sometimes reactive manner.</td>
</tr>
</tbody>
</table>
Additional Security Guidance
1. Common Control System Constraints

- “Essential Function”
  - A function or capability that is required to maintain health, safety, the environment and availability of equipment under control.
Therefore – Selected “Constraints” Must be Followed:

- Security measures shall not adversely affect essential functions of a high availability ICS unless supported by a risk assessment.
- Security measures should not cause loss of protection, loss of control, loss of view or loss of other essential functions.
- Access controls shall not prevent operation of the essential functions.
- Essential functions of the ICS shall be maintained if zone boundary protection goes into fail–close and/or island mode.
- A denial of service (DoS) event on the ICS or SIS network shall not prevent the SIS and its associated functions from acting.

Reference: ANSI/ISA–62443–3–3 (99.03.03)–2013 – Page 24
2. Exceptions

- This section focuses on the need to allow for exceptions to the Framework and associated Matrix.
- Exceptions need to be reviewed for business risk and approved by plant management and the security organization.
- Exceptions are intended to be reviewed at least annually.
3. Enforcement

- Systems out of compliance are subject to disconnection from company network
- Employees – disciplinary action
- Vendors and 3rd Parties – termination of contract and/or loss of business with the company
Summary of Framework

- Purpose
- Functions of a Conceptual Framework
- Scope
- Framework Statement
- Primary ICS Security Philosophy
- Primary Network Reference Model
- Primary ICS Security Standards
- Risk and Impact Analysis for ICS
- ICS Cybersecurity Maturity Model/Grading
- Common Control System Constraints
- Exceptions
- Enforcement
- Appendix A: ICS Security Controls Matrix
Future Plans & Changes for the Framework
The Future...

- Framework being used globally
- Plant ICS security assessments in progress using Framework for reference
- Matrix continues to be augmented and updated
  - Challenges with rate of change to ISA/IEC–62443 Documents
- More work required to ensure it is viable
Thank You!!
Questions?

Ernie Hayden CISSP CEH GICSP
Executive Consultant
(C) 425-765-1400
ernie.hayden@securicon.com
Introduction to...

*AcuSec – Securicon’s Critical Infrastructure Risk Assessment Methodology*

Harry Regan CISM CISSP PSP
VP, Commercial Services
Today’s Concerns…

- Security compliance standards and guidelines continue to evolve and COST of security investments continue to rise

- Complications:
  - Inconsistent methods for defining risks, assessing risks and applying Risk Assessment formulas – even within the same organization
  - Inconsistent risk reporting → complicating corporate decisions and prioritization
  - Incomplete risk assessment reports
Offered Solution

**AcuSec**
- Provides accurate representation of risk across an organization
- Offers clients a phased, cost-effective and sustainable cybersecurity risk assessment process
- Includes scalable and repeatable risk assessment process while providing metrics, transparency and traceability
- Provides customization to accommodate and Organization’s:
  - Specific standards reporting
  - Unique risk impact definitions
  - In-place security controls
  - “Language,” terminology, and internal processes
Measurable Results

**AcuSec – Securicon’s Critical Infrastructure Risk Assessment Methodology**

[Heat Maps Categorizing Risk Exposure]

[Systems vs Implemented Security Controls]

34
Please visit our table in the Vendor Showplace to learn more about Securicon and AcuSec.

For More Details About AcuSec

Harry Regan CISM CISSP PSP
VP Commercial Services
(O) 703-914-2780 x104
harry.regan@securicon.com

Pat Differ
Director of Sales
(O) 410-848-6644
pat.differ@securicon.com