ISA Security Compliance Institute

ISASecure™ from an Asset Owner’s perspective

ISA Automation Week 2013
Presentation objectives

• Introduction to ISA/IEC 62443 Standards (ISA99)
• Introduction to ISA Security Compliance Institute (ISCI)
• Description of ISASecure Certification Programs

• How can you help improve ICS security?
  – Certify your products using ISASecure
  – Specify ISASecure in your procurement specifications
  – Become involved in ISA99 standards development
  – Become a member of ISA Security Compliance Institute
Rewind to the 1980’s

• Industry-wide focus on Safety due to some significant events

• Safety Instrumented Systems (SIS) technology changing from electrical relays to programmable electronic systems (PES)

• Limited skillset in asset owner organizations to assess SIS safety integrity

• Solution:
  – IEC 61508/61511 international standards
  – Independent 3rd party safety integrity assessment
Fast Forward to Today

- Industry-wide focus on Security due to many significant events
- Industrial Automation and Control Systems (IACS) technology changing from vendor proprietary to IP networking and COTS hardware/OS
- Limited skillset in asset owner organizations to assess IACS cybersecurity capabilities
- Solution:
  - ISA/IEC 62443 international standards
  - Independent 3rd party security assessment - ISASecure™
ISA / IEC-62443
International Standards
ISA/IEC 62443

- Scope is Industrial Automation and Control Systems (IACS)
- Scope is industry cross-sector
- Mostly developed by the ISA99 Committee and simultaneously submitted to IEC for international approval
- ISA99 Committee has a large volunteer membership from around the world
  - asset owners, suppliers, cybersecurity experts, IACS experts, and many others
About ISA99 Standards

- **General**
  - ISA-82443-1-1: Terminology, concepts and models
  - ISA-TR82443-1-2: Master glossary of terms and abbreviations
  - ISA-62443-1-3: System security compliance metrics
  - ISA-TR82443-1-4: IACS security lifecycle and use-case

- **Policies & procedures**
  - ISA-82443-2-1: Requirements for an IACS security management system
  - ISA-TR82443-2-2: Implementation guidance for an IACS security management system
  - ISA-TR82443-2-3: Patch management in the IACS environment
  - ISA-62443-2-4: Requirements for IACS solution suppliers

- **System**
  - ISA-TR62443-3-1: Security technologies for IACS
  - ISA-62443-3-2: Security levels for zones and conduits
  - ISA-62443-3-3: System security requirements and security levels

- **Component**
  - ISA-62443-4-1: Product development requirements
  - ISA-62443-4-2: Technical security requirements for IACS components

*Published as ISA-99.00.01-2007 and ISA-99.02.01-2009.*
ISA Security Compliance Institute (ISCI)
About ISCI

**Organization**

Consortium of Asset Owners, Suppliers, and Industry Organizations formed in 2007 under the ISA Automation Standards Compliance Institute (ASCI):

**Mission**

Establish a set of well-engineered specifications and processes for the testing and certification of industrial automation and control systems products

Decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders
Internationally Accredited Conformance Scheme

ISASecure certification programs are accredited as an ISO/IEC Guide 65 conformance scheme and ISO/IEC 17025 lab operations by ANSI/AClass.

- Provides global recognition for ISASecure certification
- Independent CB accreditation by ANSI/AClass and other global Accreditation Bodies such as JAB or UKAS
- ISASecure can scale on a global basis
- Ensures certification process is open, fair, credible, and robust.
Global Adoption

Japan Information-technology Promotion Agency

- Translating ISASecure specifications to Japanese
- Setting up a test lab in Sendai Japan - Control Systems Security Center (CSSC)
- JAB is undertaking the CSSC lab accreditation process
- Promoting ISASecure as part of the Japanese critical infrastructure security scheme.
ISCI Member Companies

ISCI membership is open to all organizations

- Strategic membership
- Technical membership
- Government membership
- Associate membership
- Informational membership

Member organizations

- Chevron
- CSSC
- exida
- ExxonMobil
- Honeywell
- IT Promotion Agency, Japan
- Invensys
- RTP Corp.
- Yokogawa
- ISA99 Committee Liaison
ISASecure™
Security Development Lifecycle Assurance (SDLA)
SDLA Overview

• Certification that the supplier’s product development work process includes security considerations throughout the lifecycle

• Meets requirements of ISA/IEC-62443-4-1 (future)

• Based on several industry-recognized security development lifecycle processes

• Expected to be available by end of 2013
SDLA Phases

1. Security Management Process
2. Security Requirements Specification
3. Security Architecture Design
4. Security Risk Assessment (Threat Model)
5. Detailed Software Design
7. Module Implementation & Verification
8. Security Integration Testing
10. Security Response Planning
11. Security Validation Testing
12. Security Response Execution
Multiple Product Certification

An organization’s product development process is certified once per the SDLA requirements.

Individual products are certified which includes an assessment to verify the certified SDLA process was followed.
ISASecure™
Embedded Device Security Assurance (EDSA)
EDSA Overview

• Certification that the supplier’s product is robust against network attacks and is free from known security vulnerabilities
• Meets requirements of ISA/IEC-62443-4-2 for embedded devices (future)
• Currently available
What is an Embedded Device?

Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process, examples:

- Programmable Logic Controller (PLC)
- Distributed Control System (DCS) controller
- Safety Logic Solver
- Programmable Automation Controller (PAC)
- Intelligent Electronic Device (IED)
- Digital Protective Relay
- Smart Motor Starter/Controller
- SCADA Controller
- Remote Terminal Unit (RTU)
- Turbine controller
- Vibration monitoring controller
- Compressor controller
ISASecure EDSA Certification Program

**Embedded Device Security Assurance (EDSA)**
- Detects and Avoids systematic design faults
  - The vendor’s software development and maintenance processes are audited
  - Ensures the organization follows a robust, secure software development process

**Software Development Security Assessment (SDSA)**
- Detects Implementation Errors / Omissions
  - A component’s security functionality is audited against its derived requirements for its target security level
  - Ensures the product has properly implemented the security functional requirements

**Functional Security Assessment (FSA)**
- Identifies vulnerabilities in networks and devices
  - A component’s communication robustness is tested against communication robustness requirements
  - Tests for vulnerabilities in the 4 lower layers of OSI Reference Model

**Communications Robustness Testing (CRT)**
ISASecure™
System Security Assurance (SSA)
SSA Overview

- Certification that the supplier’s product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of ISA/IEC-62443-3-3 (approved)
- Expected to be available by end of 2013
ISASecure SSA Certification Program

System Security Assessment (SSA)  
Security Development Lifecycle Assessment (SDL&A)

Functional Security Assessment (FSA)

System Robustness Testing (SRT) and Vulnerability Identification Testing (VIT)

Ensures Security Was Designed-In
- The supplier’s system development and maintenance processes are audited for security practices
- Ensures the system was designed following a robust, secure development process

Ensures Fundamental Security Features are Provided
- A system’s security functionality is audited against defined requirements for its target security level
- Ensures the system has properly implemented the security functional requirements

Identifies Vulnerabilities in Actual Implementation
- Structured penetration testing at all entry points
- Scan for known vulnerabilities (VIT)
- Combination of CRT and other techniques
What is a “System”?

- Industrial Control System (ICS) or SCADA system
- Available from a single supplier
- Supported by a single supplier
- Components are integrated into a single system
- May consist of multiple Security Zones
- Can be identified by a product name and version
- Off the shelf; not site or project engineered yet
SSA System Robustness Test

- **Asset Discovery Scan**
  - scan to discover the components on the network

- **Communications Robustness Test**
  - verify that essential functions continue to operate under high network load and malformed packets

- **Network Stress Test**
  - verify that essential functions continue to operate under high network load

- **Vulnerability Identification Test**
  - scan all components for the presence of known vulnerabilities
  - based on National Vulnerability Database
SSA System Robustness Test
In Summary

- ISA/IEC-62443 standards set the requirements for Industrial Automation and Control Systems
- ISASecure certifies that suppliers and products meet the ISA/IEC-62443 standards
- Asset Owners have confidence that the IACS products they purchase are robust against network attacks and are free from known security vulnerabilities
Who to contact for ISA99 committee

Eric Cosman
Co-Chairman ISA99 Committee
eric.cosman@gmail.com

Jim Gilsinn
Co-Chairman ISA99 Committee
jimgilsinn@gmail.com
Who to Contact to Certify Products

ISASecure EDSA Chartered Lab: exida
John Cusimano
Director of Security Services
Phone:  (215) 453-1720
Fax:    (215) 257-1657
Email:  jcusimano@exida.com
Website: http://www.exida.com
Who to contact for ISCI Membership

Andre Ristaino
Managing Director, ASCI
Phone: 919-990-9222
Fax: 919-549-8288
Email: aristaino@isa.org
Website: http://www.isasecure.org
## Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLASS</td>
<td>One of three brands of the ANSI-ASQ National Accreditation Board</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>CSSC</td>
<td>Control Systems Security Center, Japan-R&amp;D and test lab in Sendai Japan</td>
</tr>
<tr>
<td>ISA</td>
<td>International Society of Automation</td>
</tr>
<tr>
<td>IACS</td>
<td>Industrial Automation and Control System</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IPA</td>
<td>Information-technology Promotion Agency, Japan</td>
</tr>
<tr>
<td>ISCI</td>
<td>ISA Security Compliance Institute</td>
</tr>
<tr>
<td>JAB</td>
<td>Japan Accreditation Bureau-Japan based IEC accreditation body (AB)</td>
</tr>
</tbody>
</table>
ISA 62443 Status (Oct, 2013)

1. **General**
   - ISA-62443-1-1: Terminology, concepts and models
   - ISA-TR62443-1-2: Master glossary of terms and abbreviations
   - ISA-62443-1-3: System security compliance metrics
   - ISA-TR62443-1-4: IACS security lifecycle and use-case

2. **Policies & Procedures**
   - ISA-62443-2-1: Requirements for an IACS security management system
   - ISA-TR62443-2-2: Implementation guidance for an IACS security management system
   - ISA-TR62443-2-3: Patch management in the IACS environment
   - ISA-62443-2-4: Requirements for IACS solution suppliers

3. **System**
   - ISA-TR62443-3-1: Security technologies for IACS
   - ISA-62443-3-2: Security levels for zones and conduits
   - ISA-62443-3-3: System security requirements and security levels

4. **Component**
   - ISA-62443-4-1: Product development requirements
   - ISA-62443-4-2: Technical security requirements for IACS components