Securing the Supply Chain

for Commercial off the Shelf (COTS)
Industrial Automation and Control Devices and Systems
Using IEC 62443 Standards

www.isasecure.org

July 13, 2016

Andre Ristaino
Managing Director,
ISA Automation Standards Compliance Institute
Agenda

• About ISA Security Compliance Institute
• IEC 62443 Standards and structure
• Structure of ISASecure scheme
• Description of ISASecure Certifications
• ISASecure Roadmap
ISCI Organization

501 c 6 Not for profit
Conformity Assess Subsidiary of ISA

CHAIRMAN
Ed Crawford, Chevron

ISA99 COMMITTEE LIAISON
Eric Cosman-Dow

EXECUTIVE DIRECTOR (NON-VOTING)
Andre Ristaino

MARKETING CHAIRMAN
Kevin Staggs, Honeywell

VICE CHAIRMAN
Johan Nye, ExxonMobil

TECHNICAL CHAIRMAN
Paul Forney, Schneider Electric
Supporters-ISCI Member Companies

ISCI membership is open to all organizations

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

Member organizations

- Chevron
- Bedrock Automation
- Aramco Services
- CSSC
- Codenomicon
- exida
- ExxonMobil
- Honeywell
- IT Promotion Agency, Japan
- KPMG Consulting Ltd. Japan
- Schneider Electric
- TSC Advantage
- WisePlant HQ
- Yokogawa
- ISA99 Committee Liaison
Why Certify COTS Products?

1. Security capabilities are **independently assessed** and certified by experts at accredited ISASecure labs.

2. **Reduces effort** for end user to validate and verify security capabilities.

3. **Objective metrics** for security capabilities based on industry standards. (Hundreds of years of SME and knowledge codified into IEC 62443-x-x from hundreds of committee participants.)
IACS Security Lifecycle

Asset Owners
Operate and Maintain
Site Specific Systems

Integrators/Asset Owners
Engineer and Integrate
COTS into Site Specific Systems

Suppliers
Design and Manufacture
COTS Control Systems
IEC 62443 Standards Family

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

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

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

Status Key
- Published
- In development
- Planned
- Published (under review)
- Out for comment/vote
IEC 62443 Standards Family - Roles

Industrial Automation and Control System (IACS) (from ISA 62443-2-4)

Asset Owner
- Operates site-specific solution
  - ISA/IEC 62443-2-1
  - ISA/IEC 62443-2-3
  - ISA/IEC 62443-1-3

System Integrator
- Integrates PRODUCTS into a solution (design and deployment)
  - ISA/IEC 62443-2-4

Operational and maintenance capabilities (policies and Procedures)

Automation Solution
- [Technical Security Requirements – ISA/IEC 62443-3-3]
  - Subsystem 1
  - Subsystem 2
  - Complementary hardware and software

Product Supplier
- Develops using security lifecycle
  - ISA/IEC 62443-4-1

Includes a configured instance of the PRODUCT(S)

Off-the-shelf product DESIGNED for intended use-case

System, subsystem, and components: examples
Owner Operator Risk Reduction

Technology-Security Capabilities

Process-Maturity

Personnel-Competency
Internationally Accredited ISO/IEC 17065 Conformance Scheme

ISASecure certification programs are supported by labs accredited to ISO/IEC 17065 and ISO/IEC 17025 lab operations by international ISO/IEC 17011 accreditation bodies (AB).

- Provides global recognition and acceptance of ISASecure certifications
- ISASecure can scale on a global basis using independent CB’s
- Independent ISO/IEC 17011 accreditation by global accreditation bodies ensures certification process is open, fair, credible, and robust.
- ISCI is expanding MOU’s with Accreditation Bodies and Labs

DaKKS
(Germany accreditation authority)
IEC 62443 Standards Family - Roles

Industrial Automation and Control System (IACS) (from ISA 62443-2-4)

- **Asset Owner**
  - Operates site-specific solution
    - ISA/IEC 62443-2-1
    - ISA/IEC 62443-2-3
    - ISA/IEC 62443-1-3

- **System Integrator**
  - Integrates PRODUCTS into a solution (design and deployment)
    - ISA/IEC 62443-2-4

  **CONFIGURED** for intended environment (project/site specific)

- **Product Supplier**
  - Develops using security lifecycle
    - ISA/IEC 62443-4-1

  **Off-the-shelf product DESIGNED** for intended use-case

**Operational and maintenance capabilities**
(policies and Procedures)

**Automation Solution**
[Technical Security Requirements – ISA/IEC 62443-3-3]

- Subsystem 1
- Subsystem 2
- Complementary hardware and software

**PRODUCT**
[Technical Security Requirements –
ISA/IEC 62443-3-3, ISA/IEC 62443-4-2]

- Applications
- Embedded Devices
- Network Components
- Host Devices

System, subsystem, and components: examples
Three ISASecure® certifications available

1. **Embedded Device Security Assurance (EDSA)**
   - product certification
     - IEC 62443-4-2
     - IEC 62443-4-1

2. **System Security Assurance (SSA)**
   - product certification
     - IEC-62443-3-3, IEC 62443-4-1, IEC 62443-4-2

3. **Security Development Lifecycle Assurance (SDLA)**
   - process certification
     - IEC-62443-4-1

(Schneider Electric is worlds first vendor to achieve SDLA; at 3 different sites)
ISASecure®
Embedded Device Security Assurance (EDSA)

IEC 62443-4-1
IEC 62443-4-2
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
EDSA

- Certification that the supplier’s product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of IEC 62443-4-1 and IEC 62443-4-2 for embedded devices (will be revised when IEC 62443-4-1 and IEC 6443-4-2 are updated by IEC)
- Independent certification of the product’s security capabilities and security level (SL) as defined by the IEC 62443 standards
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

Security Development Lifecycle Assurance (SDLA)

- 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)

Communications Robustness Testing (CRT)

Vulnerability Identification Testing (VIT)

- 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.
  - Structured penetration testing at all entry points
  - Scan for known vulnerabilities (VIT)
ISASecure®
System Security Assurance (SSA)

IEC 62443-3-3
IEC 62443-4-1
IEC 62443-4-2
SSA Overview

- Certification that the supplier’s product is robust against network attacks and is free from known security vulnerabilities

- Meets requirements of IEC 62443-3-3, IEC 62443-4-1 and IEC 62443-4-2 (SSA was revised in 2013 to align with IEC 62443-3-3 requirements after IEC approval)

- Independent certification of the product’s security capabilities and security level (SL) as defined by the IEC 62443 standards
What is a “System”?

- Industrial Control System (ICS) or SCADA system
- Available from a single supplier
- Supported by a single supplier (could be a system integrator)
- 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
ISASecure SSA Certification Program

**System Security Assessment (SSA)**

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

**Security Development Lifecycle Assessment (SDLA)**

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

**Functional Security Assessment (FSA)**

Identifies Vulnerabilities in Actual Implementation
- Structured penetration testing at all entry points
- Scan for known vulnerabilities (VIT)
- Combination of CRT and other techniques

**System Robustness Testing (SRT) and Vulnerability Identification Testing (VIT)**
IEC 62443-4-1

ISASecure®
Security Development Lifecycle Assurance
(SDLA)
SDLA Overview

- Certification that the supplier’s product development sites have work process include security considerations throughout the lifecycle.
  (Development organization process certification-site specific)

- Meets requirements of IEC 62443-4-1
  (will be revised when IEC 62443-4-1 is maintained by IEC)

- Based on several industry-recognized security development lifecycle processes
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
Security Levels in ISASecure Certifications

- **Security Level 1**
  - Secure Development Lifecycle Assessment
  - Functional Security Assessment
  - Vulnerability Identification Testing
  - Communication Robustness Testing

- **Security Level 2**
  - Secure Development Lifecycle Assessment
  - Functional Security Assessment
  - Vulnerability Identification Testing

- **Security Level 3**
  - Secure Development Lifecycle Assessment
  - Functional Security Assessment
  - Vulnerability Identification Testing

- **Security Level 4**
  - Secure Development Lifecycle Assessment
  - Functional Security Assessment
  - Vulnerability Identification Testing
  - Robustness Testing
How to Use ISASecure in Procurement

1. Asset Owner assesses risk and determines required security levels (similar to SIL requirements analysis) for COTS application categories / systems.

2. Asset owner downloads and reviews ISASecure certification requirements, noting Security Levels (SL).

3. Specify matching ISASecure SL level in COTS procurement document plus any company or project specific additions.

<table>
<thead>
<tr>
<th>Asset Owner Control System Requirements</th>
<th>ISASecure SSA Requirements from website</th>
<th>Additional Corporate standards or project specific requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# ISASecure EDSA Certified Devices

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Type</th>
<th>Model</th>
<th>Version</th>
<th>Level</th>
<th>Test Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honeywell Process Solutions</td>
<td>Safety Manager</td>
<td>HPS 1009077 C001</td>
<td>R145.1</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>RTP Corporation</td>
<td>Safety manager</td>
<td>RTP 3000</td>
<td>A4.36</td>
<td>EDSA 2010.1 Level 2</td>
<td>exida</td>
</tr>
<tr>
<td>Honeywell Process Solutions</td>
<td>DCS Controller</td>
<td>Experion C300</td>
<td>R400</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Honeywell Process Solutions</td>
<td>Fieldbus Controller</td>
<td>Experion FIM</td>
<td>R400</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Yokogawa Electric Corporation</td>
<td>Safety Control System</td>
<td>ProSafe-RS</td>
<td>R3.02.10</td>
<td>EDSA2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Yokogawa Electric Corporation</td>
<td>DCS Controller</td>
<td>CENTUM VP</td>
<td>R5.03.00</td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
</tr>
<tr>
<td>Hitachi, Ltd.</td>
<td>DCS Controller</td>
<td>HISEC 04/R900E</td>
<td>01-08-A1</td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
</tr>
<tr>
<td>AZBIL (formerly Yamatake)</td>
<td>DCS Controller</td>
<td>Harmonas / Industrial-DEO / Harmonas-DEO system Process Controller DOPC IV (Redundant type)</td>
<td>R 4.1</td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>Field Process Controller</td>
<td>FCP280</td>
<td>S91061</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>Tricon CX</td>
<td></td>
<td></td>
<td>EDSA 2020.1 Level 1</td>
<td>TUV Rheinland</td>
</tr>
</tbody>
</table>
## ISASecure Certified Development Organizations

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Locations</th>
<th>SDLA Version</th>
<th>Security Level (1-4)</th>
<th>Certification Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schneider-Electric</td>
<td>Foxboro, MA, USA</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider-Electric</td>
<td>Worthing, UK</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider-Electric</td>
<td>Hyderabad, India</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
</tbody>
</table>

*Additional supplier development organizations being assessed for compliance to SDLA.*
# ISASecure Recognized Test Tools

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Product Name</th>
<th>Test Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable</td>
<td>Nessus</td>
<td>Vulnerability Identification Testing against US-CERT NVDB</td>
</tr>
<tr>
<td>Beyond Security</td>
<td>beSTORM EDSA</td>
<td>CRT, SRT and network robustness testing</td>
</tr>
<tr>
<td>Hitachi</td>
<td>Raven</td>
<td>CRT, SRT and network robustness testing</td>
</tr>
<tr>
<td>Synopsys</td>
<td>Defensics X</td>
<td>CRT, SRT and network robustness testing</td>
</tr>
<tr>
<td>Wurldtech</td>
<td>Achilles Satellite</td>
<td>CRT, SRT and network robustness testing</td>
</tr>
</tbody>
</table>

Additional CRT test tools under evaluation for recognition for use in ISASecure conformity assessment scheme.
### ISASecure Certification Bodies (CB)

<table>
<thead>
<tr>
<th>ISASecure Certification Body</th>
<th>Accrediting Authority</th>
<th>Location(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exida, LLC</td>
<td>ANSI ANAB</td>
<td>Global operations – HQ Sellersville, PA USA</td>
</tr>
<tr>
<td>CSSC-CL</td>
<td>Japan Accreditation Board (JAB)</td>
<td>Japan and AP region - HQ Tokyo, Japan</td>
</tr>
</tbody>
</table>

*Additional CB accreditation in progress in Germany (DAkkS)*
ISASecure Roadmap-new work

1. Developing an application software only certification (*Application Security Assurance-ASA*)

2. **Collaborating** with Building Automation Systems (BAS) stakeholders to expand IEC 62443 certification to BAS control systems.

3. **Collaborating** with European Union – ERNCIP CA program

4. Reaching out to other stakeholders including UL, industry groups such as LOGIIC, CABA, NAMUR, WIB; seek to **harmonize certifications globally**-EU, Japan, USA

5. **Expanding industrial protocol coverage** for inclusion in CRT certification testing.
Why Certify COTS Products?

1. Security capabilities are **independently assessed** and certified by experts at accredited ISASecure labs.

2. **Reduces effort** for end user to validate and verify security capabilities.

3. **Objective metrics** for security capabilities based on industry standards. (hundreds of years of SME and knowledge codified into IEC 62443-x-x from hundreds of committee participants.)
Thank You!

Q&A

Andre Ristaino
67 Alexander Drive
Research Triangle Park, NC 27709 USA
Phone: +1 919-990-9222  Mobile: +1 919-323-7660
Email: aristaino@isa.org
Web Site: www.isasecure.org