Automation Standards Compliance Institute

501 c 6 Not for profit
Conformity Assessment Subsidiary of ISA

ASCI Board

ISA Security Compliance Institute

ISA100 Wireless Compliance Institute

ISCI Board

WCI Board

Technical Director
Periodic Contractors

ASCI Staff
Andre Ristaino-Managing Director
Mike Brazda-Marketing & Ops Support

Accreditation Bodies
ANSI/ANAB
JAB
DAkkS

Certification Bodies
TUV Rheinland
Exida
CSSC-CL
CSA Group

Test Tool Suppliers
GE Digital-Achilles
Synopsis-Defensics
Hitachi-Raven
See Beyond-Beyond Secure
CNCERT-Acheron

Certification In-house via training; shared revenue

In-house developed test tools
Securing the Supply Chain

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

www.isasecure.org

Andre Ristaino
Managing Director,
ISA Automation Standards Compliance Institute
Agenda

- About ISA Security Compliance Institute
- Structure of ISASecure scheme
- IEC 62443 Standards and structure
- Description of ISASecure Certifications
- ISASecure Roadmap
- Website www.isasecure.org
ISASecure® Founding Companies

- Siemens
- ExxonMobil
- Chevron
- bp
- Schneider Electric
- Yokogawa
- Honeywell
- Rockwell Automation

ISA99 Committee Liaison
ISASecure® Supporter Companies

IPA

Saudi Aramco

KPMG

CSSC

WisePlant®

CODENOMICON

YPF
Supporters-ISCI Member Companies

ISCI membership is open to all organizations

- Strategic membership
- Technical membership (includes CB’s)
- Government/Associate membership
- Adopter/Supporter

Member organizations
- Chevron
- Bedrock Automation
- Aramco Services
- CSA Group
- CSSC
- exida
- ExxonMobil
- Honeywell
- IT Promotion Agency, Japan
- KPMG Consulting Ltd. Japan
- Schneider Electric
- Synopsis
- TUV Rheinland
- WisePlant HQ
- Yokogawa
- YPF
- ISA99 Committee Liaison
No Membership Required

Asset owners specify ISASecure in procurement specifications and/or choose from list of certified products on ISASecure website.

Suppliers submit products to an ISASecure certification body of choice.

Certified products are listed on ISASecure website and certification body website.
ISCI Organization

501 c 6 Not for profit
Conformity Assessment Subsidiary of ISA

ISCI Governing Board

Chairman – Kenny Mesker, Chevron
Vice-chairman – Johan Nye, ExxonMobil
Technical Chairman – Kevin Staggs, Honeywell
Marketing Chairman – Dan Desruisseaux, Schneider Electric
ISA99 Committee Liaison – Eric Cosman
Staff Managing Director – Andre Ristaino (non-voting)
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.
• AB and CB agreements continue to expand.
### ISO/IEC 17065 / ISO/IEC 17025 Accredited Certification Bodies

<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>
<tr>
<td>TUV Rheinland</td>
<td>DAIkkS</td>
<td>Global operations – HQ Cologne, Germany</td>
</tr>
</tbody>
</table>

*Additional Certification Bodies are in Accreditation Process.*
exida.com, LLC
HQ Sellersville, PA/global locations

The first ISASecure chartered lab, accredited in 2011
CSSC-CL

Control Systems Security Corporation
Tokyo & Tagajo City Japan
TUV Rheinland

TUV Rheinland Headquarters
Cologne Germany
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. (scarcity of talented cybersecurity expertise)

3. Objective metric 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.)

One specification, one service mark, one assessment
End-user Benefits and Value

- Simplifies procurement specification process
- End users understand standards-based product cybersecurity capabilities
- Capabilities independently validated by external entity
- Confidence that security features will evolve over time
- ISCI provides a forum where end-users can ensure that ISA/IEC 62443 standards are implemented as intended
- Forum where an end-user can include their company specific requirements in certification specifications
Supplier Benefits and Value

• Differentiate solutions to marketplace
• Assurance products meet standards-based cybersecurity requirements that are maintained over the product lifecycle
• Cybersecurity is a dimension of product quality
• Suppliers will soon face product liability accountabilities
IACS Security Lifecycle

Suppliers
Design and Manufacture COTS Control Systems

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

Asset Owners
Operate and Maintain Site Specific Systems
IEC 62443 Standards Family

General
- ISA-62443-1-1: Terminology, concepts and models
- ISA-62443-1-2: 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

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

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

**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

Includes a configured instance of the PRODUCT(S)

CONFIGURED for intended environment (project / site specific)

Off-the-shelf product DESIGNED for intended use-case
Three ISASecure® certifications available

1. Embedded Device Security Assurance (EDSA) product certification
   IEC 62443-4-2
   IEC 62443-4-1
   Vulnerability Identification Test
   + Communication Robustness Test

2. System Security Assurance (SSA) product certification
   IEC-62443-3-3
   IEC 62443-4-1
   IEC 62443-4-2
   Vulnerability Identification Test
   + Communication Robustness Test

3. Security Development Lifecycle Assurance (SDLA) process certification
   IEC-62443-4-1
360 Degree Product Evaluation

More than just testing!
ISASecure®
Embedded Device Security Assurance (EDSA)

IEC 62443-4-1
IEC 62443-4-2
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 6443-4-2 is published)

• Independent certification of the product’s security capabilities and security capability level (SL) as defined by the IEC 62443 standards
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

**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)**
- 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)

**Communications Robustness Testing (CRT)**

**Vulnerability Identification Testing (VIT)**

ISA Security Compliance Institute
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

• Independent certification of the product’s security capabilities and security capability 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)
An ISASecure Certified Development Organization

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

- Based on several industry-recognized security development lifecycle processes
# SDLA Practice Areas - ISA/IEC 64443-4-1

<table>
<thead>
<tr>
<th>Practice Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security Management (SM)</td>
<td>The purpose of the security management practice is to ensure that the security-related activities are adequately planned, documented and executed throughout the product’s lifecycle.</td>
</tr>
<tr>
<td>2. Specification of Security Requirements (SR)</td>
<td>The processes specified by this practice are used to document the security capabilities that are required for a product along with the expected product security context.</td>
</tr>
<tr>
<td>3. Secure by Design (SD)</td>
<td>The processes specified by this practice are used to ensure that the product is secure by design including defense in depth.</td>
</tr>
<tr>
<td>4. Secure Implementation (SI)</td>
<td>The processes specified by this practice are used to ensure that the product features are implemented securely.</td>
</tr>
<tr>
<td>5. Security Verification and Validation Testing (SVV)</td>
<td>The processes specified by this practice are used to document the security testing required to ensure that all of the security requirements have been met for the product and that the security of the product is maintained when it is used in its product security context.</td>
</tr>
<tr>
<td>6. Security Defect Management (DM)</td>
<td>The processes specified by this practice are used for handling security-related issues of a product that has been configured to employ its defense in depth strategy (Practice 3) within the product security context (Practice 2).</td>
</tr>
<tr>
<td>7. Security Update Management (SUM)</td>
<td>The processes specified by this practice are used to ensure security updates associated with the product are tested for regressions and made available to product users in a timely manner.</td>
</tr>
<tr>
<td>8. Security Guidelines (SG)</td>
<td>The processes specified by this practice are used to provide documentation that describes how to integrate, configure, and maintain the defense in depth strategy of the product in accordance with its product security context.</td>
</tr>
</tbody>
</table>
ISASecure Product Certification Levels

Security Level 4
- 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 2
- Secure Development Lifecycle Assessment
- Functional Security Assessment
- Vulnerability Identification Testing

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

Communication Robustness Testing

Vulnerability Identification Testing
<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</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</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</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</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>Haronomas / Industrial-DEO / Haronomas-DEO</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>
<tr>
<td>Beijing Consen Technologies</td>
<td>Safety Related PES</td>
<td>TSxPlus V1.0</td>
<td>CM01-A-V001</td>
<td>EDSA v20 Level1</td>
<td>TUV Rheinland</td>
</tr>
<tr>
<td>HIMA Paul Hildebrandt GmbH</td>
<td>Safety Related PES</td>
<td>HIMAX X</td>
<td>CPU 01 FW Version 8.8 &amp; COM 01 FW Version 9.2</td>
<td>EDSA v2.0 Level T1</td>
<td>TUV Rheinland</td>
</tr>
<tr>
<td>TOSHIBA CORPORATION</td>
<td>DCS Controller</td>
<td>CIEMAC-DS/nv (TOSDIC-CIE DS/nv)</td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
<td></td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>Safety Related Programmable Electronic System</td>
<td>TRICONEX Communication Module TCM</td>
<td>4355X, Firmware Revision Build 290 (TCM2) 288</td>
<td>EDSA 2.0.0 Level</td>
<td>TUV Rheinland</td>
</tr>
<tr>
<td>ABB</td>
<td>Controller</td>
<td>HPC800 Controller</td>
<td>HCA800B1</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Tri-Sen Systems Corporation</td>
<td>Safety Related Programmable Electronic System</td>
<td>TSxPlus V1.0</td>
<td>CM01-A-V001</td>
<td>EDSA 2.0.0 Level 1</td>
<td>TUV Rheinland</td>
</tr>
</tbody>
</table>

**ISASecure EDSA Certified Devices-March 2018**
ISASecure® EDSA Certified Products
ISASecure® EDSA Certified Products

Schneider Electric

YOKOGAWA

TOSHIBA
Leading Innovation

ABB
### ISASecure SDLA Process 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>Lake Forest, CA USA</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider-Electric</td>
<td>Calgary AB, Canada</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>
<tr>
<td>Honeywell Process</td>
<td>Phoenix, AZ</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
</tbody>
</table>
ISASecure® EDSA Product Certificates

Certificate / Zertifikat / 合格証
RTP 1103060 C001

Certificate issued by:
Exida

Certificate holder:
RTP Corporation
Pompano Beach, FL USA

Has been assessed per the relevant requirements of:
IEC 61508: 2010 Parts 1-7
and meets requirements providing a level of integrity to:
IEC 61508: Systematic Integrity-SIL 3 Capable Random Integrity: Type B Element

Safety Function:
The RTP-3000 reads inputs, performs its programmed safety function, and generates outputs.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements. The unit must be operated in a network and operational environment per the Security Manual requirements.

Michael Regoff
Evaluating Assessor

Page 1 of 2

Certificate

968/EDSA 1000.00/17

Product tested:
Safety-Related Programmable Electronic System

Certificate holder:
Schneider Electric Systems USA, Inc.
20601 Rancho Parkway
South Lake Forest, CA 92630
USA

Type designation:
TRICON System V11.2

Tricon Communication Module TCM 4381 A/B/A

Firmware Revision 6415 Build 275

Tricon Communication Module TCM 4382 A/B/A

Firmware Revision 6415 Build 275

Scope and result:
ISASecure Embedded Device Security Assurance (EDSA) 2010.1 - Level 2

Specific requirements:

The system complies with the requirements of ISASecure EDSA 2010.1 - Level 1.

For the use of the system the safety and security considerations as documented in the product and user guides must be considered.

Mark Gull
Dipl.-Ing. Hannu Gull

TÜV Rheinland Industrie Service GmbH
Siemensstrasse 1
D-53757 Bonn
Germany
ISASecure® SDLA Process Certificates

Certificate / Zertifikat / 合格証

SCH 1608125 C001
exida hereby confirms that the Security Development Lifecycle Process
Practiced by Schneider Electric Software
Calgary, AB Canada

Has been assessed per the relevant requirements of:
ISASecure® Security Development Lifecycle Assurance (SDLA) Program
Version 1.3
And meets the requirements for:
LEVEL 2

Certificate / Zertifikat / 合格証

HPS 1505160 C001
exida hereby confirms that the Standard HPS Iterative Process (HIP)
Practiced by Honeywell Process Solutions
Phoenix, AZ
USA

Has been assessed per the relevant requirements of:
ISASecure® Security Development Lifecycle Assurance (SDLA) Program
Version 1.3
And meets the requirements for:
LEVEL 1
ISASecure Recognized Test Tools

ISASecure test tool specifications and recognition process ensures that all test tools meet ISASecure requirements and provide consistent test outcomes.

<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</td>
</tr>
<tr>
<td>Hitachi</td>
<td>Raven</td>
<td>CRT, SRT and network robustness</td>
</tr>
<tr>
<td>Synopsys</td>
<td>Defensics X</td>
<td>CRT, SRT and network robustness</td>
</tr>
<tr>
<td>Wurldtech</td>
<td>Achilles Satellite</td>
<td>CRT, SRT and network robustness</td>
</tr>
<tr>
<td>CNCERT/CC &amp; Beijing Xinlian Kehui Technology Co., LTD</td>
<td>Acheron 2.2</td>
<td>CRT, SRT, and network robustness</td>
</tr>
</tbody>
</table>
ISASecure Roadmap-new work

1. Collaborating with Building Control Systems (BCS) stakeholders to ensure ISASecure certifications properly address BCS.

2. Align EDSA with ISA/IEC 62443-4-2 Component requirements
   a) Include network components, applications, and host systems

3. Collaborating with European Union – ERNCIP CA program

4. Reaching out to other stakeholders including UL, industry groups such as ASHRAE, LOGIIC, CABA, NAMUR, DoD;

5. Seek to harmonize certifications globally-EU, Japan, USA, AP

6. Expanding protocols to include in CRT test requirements
Participating Organizations

Download Working Group Final Report at
ISASecure Certification Growth
Thank You

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