



ISA **Security Compliance Institute**

Providing Industrial Control Systems
Security Standards Compliance





Program Overview

Industry leaders from a number of major control system users and manufacturers have formed an organization to establish a set of well-engineered specifications and processes for the testing and certification of critical control systems products.

"The organization's mission is to 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 to:

- *Facilitate the independent testing and certification of control system products to a defined set of control system security standards;*
- *Use existing control system security industry standards where available, develop or facilitate development of interim standards where they don't already exist, and adopt new standards when they become available; and*
- *Accelerate the development of industry standards that can be used to certify that control systems products meet a common set of security requirements.*

The standards, tests, and conformance processes for control systems products will allow the products to be securely integrated. An ultimate goal is to push the conformance testing into the product development lifecycle so that the products are intrinsically secure."

For more details on the ISA Security Compliance Institute (ISCI), including history, operations, scope, budget, membership terms, and how to join, visit www.ISASecure.org.

ISASecure Program Benefits

The ISASecure program has been developed by the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry-wide improvement of cyber security for Industrial Automation and Control Systems (IACS). It achieves this goal by offering a common industry-recognized set of device and process requirements that drive device security, simplifying procurement for asset owners and device assurance for equipment vendors.

The rewards to the automation controls industry and to your company are significant.

For **asset owners**, a well designed and managed product security certification process results in reduced cost and time commitments for product selection and deployment. Key benefits:

- Reduced costs for and time spent on validation and verification of security capabilities
- Assurances that ISASecure products are more secure “out of the box,” leading to improved process reliability and safety
- Mitigation of government security compliance regulation through full industry participation
- Creation of an assurance “stamp” for security, like the assurance “stamp” that exists for safety, through ISASecure security certification
- Instant recognition of product security characteristics and capabilities via the ISASecure security certification stamp
- Ability for asset owners to specify and successfully procure ISASecure compliant products with known security levels
- Favorable positioning for organizations with regards to insurance requirements that may emerge for security compliance levels
- Reduced overall cost of delivery from the ISASecure program’s leveraging of industry capabilities



For **suppliers and integrators**, the certification process provides a single compliance framework and an ISASecure industry stamp of approval, resulting in faster time to market and lower development and integration costs. Key benefits:

- Suppliers are able to make and substantiate clear claims of compliance to a consensus, open industry standard via the ISASecure designation
- Certification responds to a common need for a shared security vision to be executed by suppliers, asset owners, and consultants: ISASecure profiles help suppliers build what users want
- The program provides security requirements guidance from industry to suppliers based on ISASecure testing standards
- The ISASecure program addresses the security characteristics of the product that allow it to be integrated into a larger system

For **standards bodies** and **government agencies** developing industrial security specifications, ISASecure promotes better, field-tested standards that are clearly being followed by industry.



Program Description

The ISA Security Compliance Institute (ISCI) developed specifications for ISASecure certifications using the framework of the **ISA99 Standards Roadmap** and based them on a security lifecycle approach to establish the scope and direction of the program.

The program is based on automation controls lifecycle phases including:

- **Devices and Systems**—Conform to ISASecure Requirements (Products constructed to secure characteristics and behaviors)
- **Supplier Practices**—Product Development Lifecycle (Design for Security)
- **User Practices**—Integration/Deployment, Operations, Lifecycle Management (Manage for Security)

The first ISASecure certification focuses on security of embedded devices and addresses device characteristics and supplier development practices for those devices. This certification is the ISASecure Embedded Device Security Assurance Certification, or ISASecure EDSA certification. An embedded device that meets the requirements of the ISASecure specifications receives the ISASecure EDSA certification—a trademarked designation that provides instant recognition of product security characteristics and capabilities and provides an independent industry stamp of approval similar to a “Safety Integrity Level” Certification (ISO/IEC 61508).

The ISASecure EDSA certification offers three levels of certification for a device, reflecting increasing levels of device security assurance. The three certification levels are ISASecure Level 1 for Devices, ISASecure Level 2 for Devices, and ISASecure Level 3 for Devices. All three levels of certification

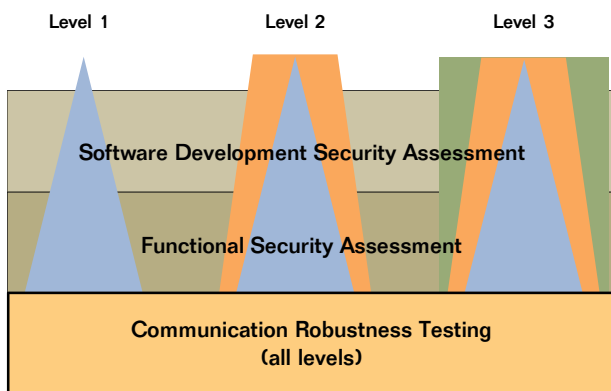
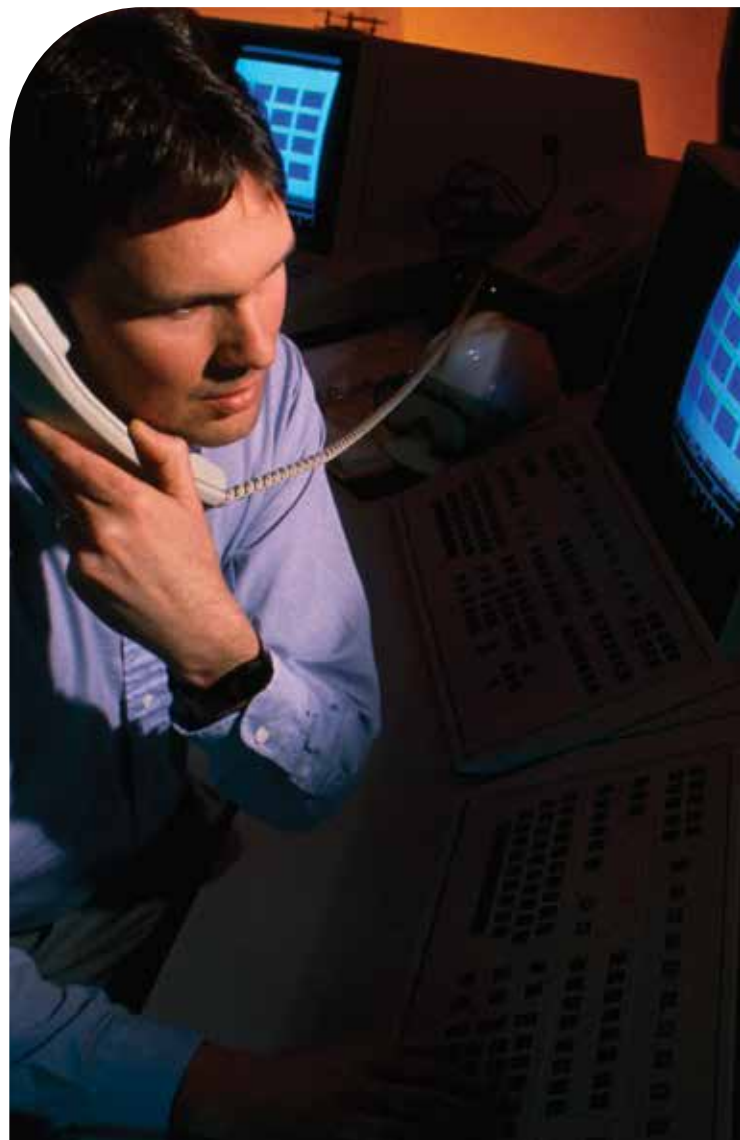


Figure 1 - Structure of ISASecure EDSA Certifications

granted under this program require the following technical elements:

- Software Development Security Assessment (SDSA)
- Functional Security Assessment (FSA)
- Communication Robustness Testing (CRT)

SDSA and FSA requirements increase in rigor for levels 2 and 3, while CRT criteria are the same regardless of the certification level (see Figure 1). The ISASecure Embedded Device Security Assurance Certification brochure, available for download from **www.ISASecure.org**, provides more details about the three technical certification elements, the certification levels, and the certification program.



Technical Scope of ISA Security Compliance Institute Compliance Testing

Strategically, the technical scope of the ISASecure program extends from the device level to the gateways (Level 0 to Level 3 plus the gateway interface between Level 3 and Level 4) as reflected by this ISA99 reference model.

ISA99 Reference Model



ISCI compliance requirements development and testing will be initiated in phases starting with the following devices in priority sequence:

1. Wired IP network devices
2. Wireless IP network devices
3. Windows-based devices

ISASecure compliance profiles will be expanded based on tactical (near-term) and strategic (long-term) compliance topics based on marketplace feedback.

Membership Categories

Organizations may join the ISA Security Compliance Institute at any level. ISCI strives to represent a fair cross-section of the automation controls community, using policies and guidelines to ensure that the organization maintains a balance of asset owners, suppliers, and other significant stakeholders. Annual membership dues are based on corporate revenues and listed on the membership application.

Strategic Membership (Voting)

Recommended for companies who wish to set the strategic objectives of the consortium.

Entitlements

Strategic Members enjoy all privileges of lower categories of membership, and:

- Establish and direct the Institute's market strategy, overall objectives, and operating policies and procedures
- Have voting rights and a guaranteed seat on the Governing Board

Technical Membership (Voting)

Recommended for companies who wish to influence compliance specifications and processes. Technical Members determine and manage the detailed tasks necessary to develop specifications for compliance profiles, develop procedures and software tools needed for compliance testing, establish technical support programs for suppliers and asset owners, and complete other outreach activities necessary to operate the ISASecure compliance program.

Entitlements

Technical Committee Members receive full, voting participation in all technical processes and enjoy all privileges of all categories of membership other than those specific to Strategic Membership.



Associate Membership (Non-voting)

Recommended for consortiums, quasi-governmental organizations such as NERC, industry groups, academia, and test labs who wish to participate in Institute activities and/or demonstrate support for the Institute's mission.

Entitlements

Associate members have the right to participate in Institute Activities such as technical forums and outreach. They may also review technical specifications but cannot vote on them.

Government Membership

Recommended for government organizations of any nation (except those excluded by United States of America Federal Government Policies) who wish to participate in Institute activities and/or demonstrate support for the Institute's mission.

Entitlements

Government members have the right to participate in Institute activities such as technical forums and outreach. They may also review technical specifications but cannot vote on them.

Supporter Membership (Non-Voting)

Recommended for academics, consultants, analysts, and individuals.

Entitlements

Supporter Members receive periodic information regarding technical specifications and other ISASecure program updates, but may not actively engage in formal technical meetings of ISCI.

Membership Entitlements

In addition to the overall benefits realized by the automation controls community at large, all ISCI Members are entitled to the following benefits:

- 1. ISASecure Logo Usage**—Members are entitled to use the ISASecure logo on products and systems that meet the ISASecure compliance specifications. Logo usage guidelines will be available to Members for guidance in using the ISASecure logo on products and displays and in literature and other customer facing communications.
- 2. Membership Directory**—Member organizations will be listed in the Member directory and on the ISCI website, www.ISASecure.org. The listing will include descriptions of their products and services and identify ISASecure offerings. Member organization will be recognized for their contributions to ISASecure programs and objectives.
- 3. Boards and Committees**—Depending upon your membership level, both asset owners and suppliers have the opportunity to provide leadership and direction to ISCI by participating on the Governing Board, Technical Committees, and Marketing Committees. Asset owners and suppliers will be able to receive advance notification of changes and enhancements to ISASecure profiles.
- 4. Intellectual Property Rights**—Voting members may use the Intellectual Property Rights (IPR) of ISCI for design, deployment, manufacturing, and integration engineering of products using ISASecure technology. Members will receive continuous updates of ISASecure technical specifications.
- 5. Voting**—Strategic Members and Technical Members are the voting membership levels, and are encouraged to participate in elections of Governing Board positions and periodic elections of Technical Steering Committee leaders.
- 6. Member Discounts**—Members are entitled to discounts for products and services offered by ISCI including technical support, training, development tools, and consulting services.
- 7. Member Outreach Programs**—ISCI facilitates ISASecure community programs including online forums to exchange ideas on best practices, technical issues, and other topics. ISCI also facilitates regional technical exchanges and technology demonstrations for educational purposes and to promote the use of ISASecure technology.
- 8. Promotional Activities**—In addition to ISASecure logo usage, Members are offered opportunities to promote their companies and products through sponsorships, joint marketing and advertising efforts, seminars, publishing opportunities, technology expositions, and an email newsletter.



About ASCI and the ISA Security Compliance Institute

The Automation Standards Compliance Institute (ASCI) is a non-profit organization incorporated by the International Society of Automation (ISA) in 2006 to provide a home for certification, conformance, and compliance assessment activities in the automation arena. ASCI extends the work that ISA has conducted for over 50 years in standards development by facilitating the effective implementation of automation industry standards. ISA provides professional management services to ASCI, drawing on an experienced staffing, financial, and administrative infrastructure.

The ISA Security Compliance Institute (ISCI) functions as an operational group within ASCI. ASCI bylaws share the open constructs of ISA while accounting for compliance organization requirements. Operating the ISCI within ASCI allows the organization to efficiently leverage the organizational infrastructure of ASCI.

For more information about the ISA Security Compliance Institute, visit www.ISASecure.org.

How to Join the ISA Security Compliance Institute

Interested organizations may join at any time. Please feel free to contact us for more details using the contact information below.

Membership application forms, including member fees and mailing instructions, are available for download at www.ISASecure.org.

Contact Information

Andre Ristaino
Managing Director, Automation Standards Compliance Institute

Direct 919-990-9222

Fax 919-549-8288

Email aristaino@isa.org
www.ISASecure.org