ISASecure®

Quick Start Guide:

An Overview of ISASecure® Certification

International Society of Automation
Setting the Standard for Automation™

www.ISASecure.org

Quick Start Guide:
An Overview of ISASecure® Certification

A certification scheme based on ISA/IEC 62443 Security for Industrial Automation and Control Systems

Executive Summary

ISASecure® is a third-party conformity assessment scheme based on the ISA/IEC 62443 series of standards. A third-party conformity assessment scheme is also known as a certification scheme. ISASecure® currently certifies Industrial Automation and Control System (IACS) products and the security development lifecycle used by Product Suppliers. Products include IACS Systems such as DCS and SCADA, and IACS Components such as embedded devices, host devices, network devices, and software applications.

The ISA Security Compliance Institute (ISCI) is the owner and developer of the ISASecure® Certification Scheme, which is the set of rules and procedures that identifies the types of products and processes being assessed, identifies the specified requirements, and provides the methodology to perform a certification. ISCI is a non-profit subsidiary of the International Society of Automation (ISA), and includes Asset Owners, Product Suppliers, certification bodies, and other interested organizations as members.

While ISCI develops and maintains the ISASecure® Certification Scheme, it does not perform the certification itself. This is done by an ISASecure® Certification Body, which is an organization that specializes in third-party conformity assessments. Certification bodies are accredited by an accreditation body based on the ISO/IEC 17065 standard [43], which addresses topics such as confidentiality and impartiality in the certification process. Through the accreditation and certification process, an ISASecure® Certificate issued by an ISASecure® Certification Body is recognized globally and demonstrates that the applicable ISA/IEC 62443 requirements have been met.

Currently available ISASecure® Certification Schemes are:

- **Security Development Lifecycle Assurance (SDLA)** – a certification that the Product Supplier's security development lifecycle meets the requirements of ISA/IEC-62443-4-1 – Product security development lifecycle requirements. [36]

Certified System ISASecure®

Certified Component ISASecure®

Figure 1 - ISASecure® Product Certification Schemes

- **System Security Assurance (SSA)** – a certification that the IACS System meets the requirements of ISA/IEC-62443-3-3 – System security requirements and security levels [35] and has been developed using SDLA certified processes.
- **Component Security Assurance (CSA)** – a certification that the IACS Component meets the requirements of ISA/IEC-62443-4-2 – Technical security requirements for IACS components [37] and has been developed using SDLA certified processes. IACS Components include embedded devices, host devices, network devices and software applications.

The primary benefit of third-party conformity assessment, or certification, is that it establishes trust between IACS stakeholders (Asset Owners, Product Suppliers, and Service Providers) that the applicable requirements of ISA/IEC 62443 have been met. While conformity assessments can be performed by a first-party (e.g. Product Supplier) or a second-party (e.g. Asset Owner), the independence and capabilities of an accredited third-party assessor provides a higher level of trust that the product or process meets the specified requirements.

ISASecure® benefits for the Asset Owner and Integration Service Provider (or system integrator) include the procurement of IACS products that have been designed and developed using the ISA/IEC 62443 security development lifecycle, and that have the capability to meet the technical requirements of ISA/IEC-62443 standards. ISASecure® benefits for the Product Supplier include improved product security through independent assessment of their products and security development lifecycle, and improved product sales via the use of ISASecure® Certifications in product marketing.

Table of Contents

Introduction

This document provides an overview of the ISASecure® Certification Scheme for the Security of Industrial Automation and Control Systems (IACS), which is based on the ISA/IEC 62443 series of standards. The goal of the ISA/IEC 62443 Series is to improve the safety, integrity, availability and confidentiality of Industrial Automation and Control System (IACS) using a risk-based, methodical and complete process throughout the entire lifecycle. The ISA/IEC 62443 Series describes a set of common terms and requirements that can be used by Asset Owners, Product Suppliers and Service Providers to secure their control systems and the equipment they control. The ISASecure® Certification Scheme independently demonstrates that the specified requirements of ISA/IEC 62443 standards have been met.

Understanding ISA/IEC 62443

In order to understand the ISASecure® Certification Scheme, we must first understand the ISA/IEC 62443 standards upon which they are based. The following topics are excerpts from Quick Start Guide: An Overview of ISA/IEC 62443 Standards [44] that provides a user-friendly high-level description of the ISA/IEC 62443 Series of Standards. The Quick Start Guide can be found at: https://gca.isa.org/isagca-quick-start-guide-62443-standards

Scope and Purpose

The scope of the ISA/IEC 62443 Series is the Security of Industrial Automation and Control Systems (IACS). An IACS is defined as a collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation.

Note that an IACS includes more than the technology that comprises a control system; it also includes the people and work processes needed to ensure the safety, integrity, availability and confidentiality of the control system. Without people that are sufficiently trained, risk appropriate technologies and security measures, and work processes throughout the security lifecycle, an IACS could be more vulnerable to cyberattack.

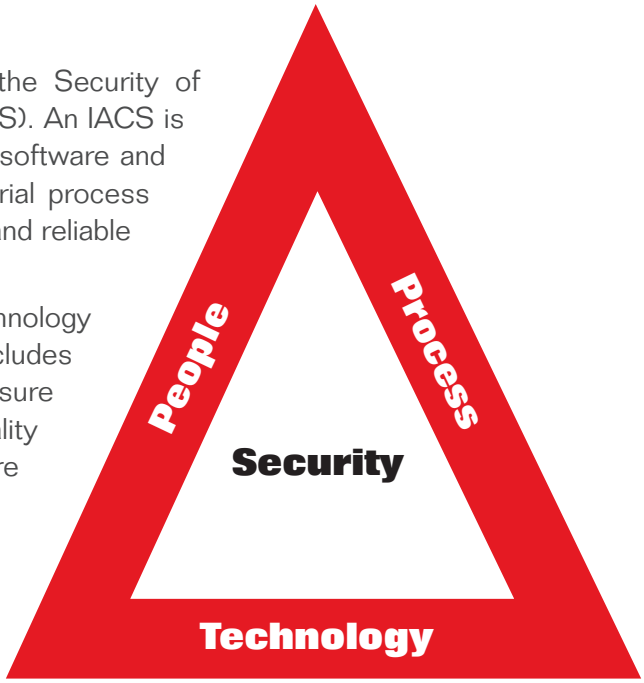


Figure 2 - The Security Triad

Relevant ISA/IEC 62443 Standards

The following ISA/IEC 62443 standards are needed to understand the ISASecure® Certification Scheme: [4]

- Part 1-1: Terminology, concepts and models introduces the concepts and models used throughout the series. The intended audience includes anyone wishing to become familiar with the fundamental concepts that form the basis for the series. [29]
- Part 2-1: Establishing an IACS security program describes what is required to define and implement an effective IACS cyber security management system. The intended audience includes Asset Owners who have responsibility for the design and implementation of such a program. [30]
- Part 3-2: Security risk assessment for system design addresses cybersecurity risk assessment and system design for IACS. The outputs of this process are a Zone and Conduit model, associated Risk Assessments and Target Security Levels. These are documented in the Cybersecurity Requirements Specification. This standard is primarily directed at Asset Owners and Integration Service Providers. [34]
- Part 3-3: System security requirements and security levels describes the requirements for an IACS System based on Security Level. The principal audience includes Product Suppliers of IACS System products, Integration Service Providers and Asset Owners. [35]
- Part 4-1: Product security development life-cycle requirements describes the requirements for a Product Supplier's security development lifecycle. The principal audience include Product Suppliers of IACS System and IACS Component products. [36]
- Part 4-2: Technical security requirement for IACS Components describes the requirements for IACS Components based on Security Level. IACS Components include embedded devices, host devices, network devices and software applications. The principal audience includes Product Suppliers of IACS Component products. [37]

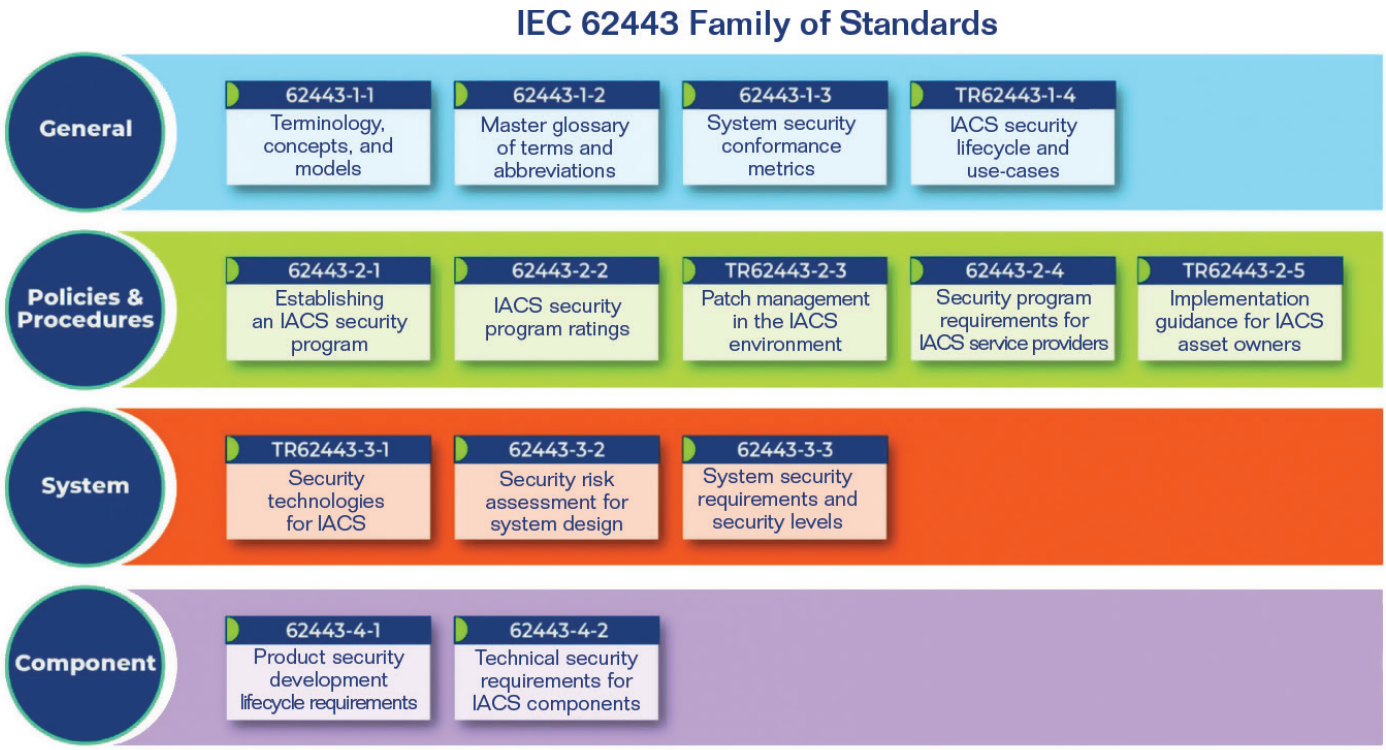


Figure 3 - The ISA/IEC 62443 Series

Principal Roles

To understand how to use the ISA/IEC 62443 Series it is first necessary to understand the relationship between roles, control system, Automation Solution and IACS. Figure 4 visualizes this relationship.

The left-hand side of the drawing shows the roles that are identified in the ISA/IEC 62443 Series:

- Asset Owner is accountable and responsible for the IACS. The Asset Owner is also the operator of the IACS and the Equipment Under Control.
- Maintenance Service Provider provides support activities for an Automation Solution.
- Integration Service Provider provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning and handover to the Asset Owner. The Integration Service Provider may also facilitate and assist in the activity to partition the System Under Consideration into Zones and Conduits and perform the Risk Assessment.
- Product Supplier is the organization that manufactures and supports a hardware and/or software product. Products may include IACS Systems and IACS Components such as embedded devices, host devices, network devices and/or software applications.

It is important to understand that a role is not necessarily an organization. An organization can have multiple roles, and the responsibilities for a particular role can be split among multiple organizations. For example, an Asset Owner organization can have the Operations role and all or part of the Maintenance Service Provider role. It is also not uncommon that a Product Supplier organization has the Product Supplier role, the Integration Service Provider role, and portions of the Maintenance Service Provider role. Finally, while all or part of the responsibilities in a role can be delegated to other organizations, the accountability for the IACS must remain with the Asset Owner organization.

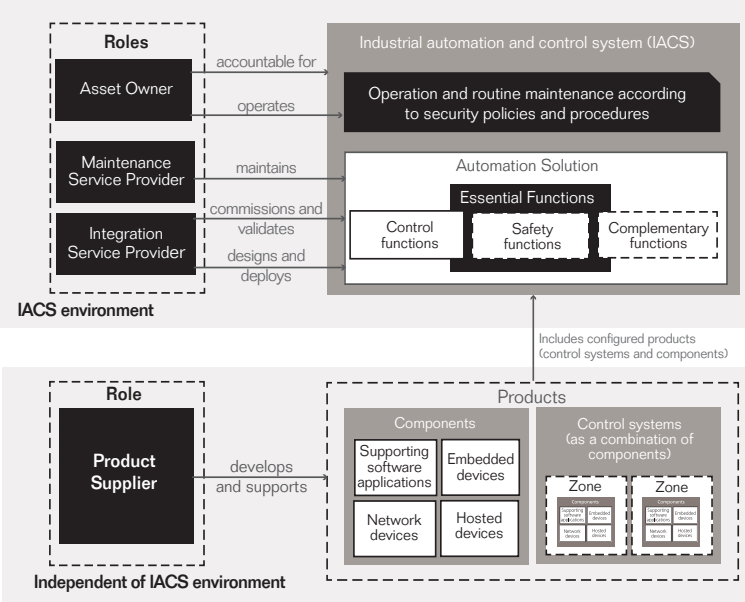


Figure 4 - Roles, Products, Automation Solution and IACS

Component, System, Automation Solution and IACS

The right-hand side of the drawing shows the types of IACS Systems and IACS Components that are identified in the ISA/IEC 62443 Series:

- IACS Components are provided by a Product Supplier and include the following types:
  - Embedded device – special purpose device designed to directly monitor or control an industrial process
  - Host device – general purpose device running an operating system capable of hosting one or more software applications, data stores or functions from one or more Product Suppliers
  - Network device – device that facilitates data flow between devices, or restricts the data flow, but may not directly interact with a control process
  - Software application – one or more software programs and their dependencies that are used to interface with the control system or the Equipment Under Control.
- IACS System (or Control System) consists of an integrated set of IACS Components which is provided by a Product Supplier.

- Automation Solution is the realization of IACS Systems and Components at a particular facility. It includes essential functions such as safety functions and control functions and other supporting functions such as historization and engineering. It is specified by the Asset Owner and provided by the Integration Service Provider.
- The Industrial Automation and Control System (IACS) includes the Automation Solution and the operational and maintenance policies and procedures necessary to support it. It is operated by the Asset Owner and maintained by the Asset Owner and/or Maintenance Service Provider.

Risk Assessment

Part 3-2 describes the requirements for addressing the cybersecurity risks in an IACS, including the use of Zones and Conduits, and Security Levels. While Part 3-2 includes the requirements for the risk assessment process, it does not specify the exact methodology to be used. The methodology used must be established by the Asset Owner and should be consistent with the overall risk assessment methodology of the organization. Examples using the risk matrix methodology are included as informative content. Figure 5 shows the risk assessment process. [34]

Zone and Conduit

A key step in the Risk Assessment process is to partition the System Under Consideration into separate Zones and Conduits. The intent is to identify those assets which share common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk. [34]

A Zone is defined as a grouping of logical or physical assets based upon risk or other criteria such as criticality of assets, operational function, physical or logical location, required access or responsible organization.

A Conduit is defined as a logical grouping of communication channels that share common security requirements connecting two or more zones.

Partitioning the System Under Consideration into Zones and Conduits can also reduce overall risk by limiting the scope of a successful cyber-attack. Part 3-2 requires or recommends that some assets are partitioned as follows:

- Shall separate business and control system assets
- Shall separate safety related assets
- Should separate temporarily connected devices
- Should separate wireless devices
- Should separate devices connected via external networks

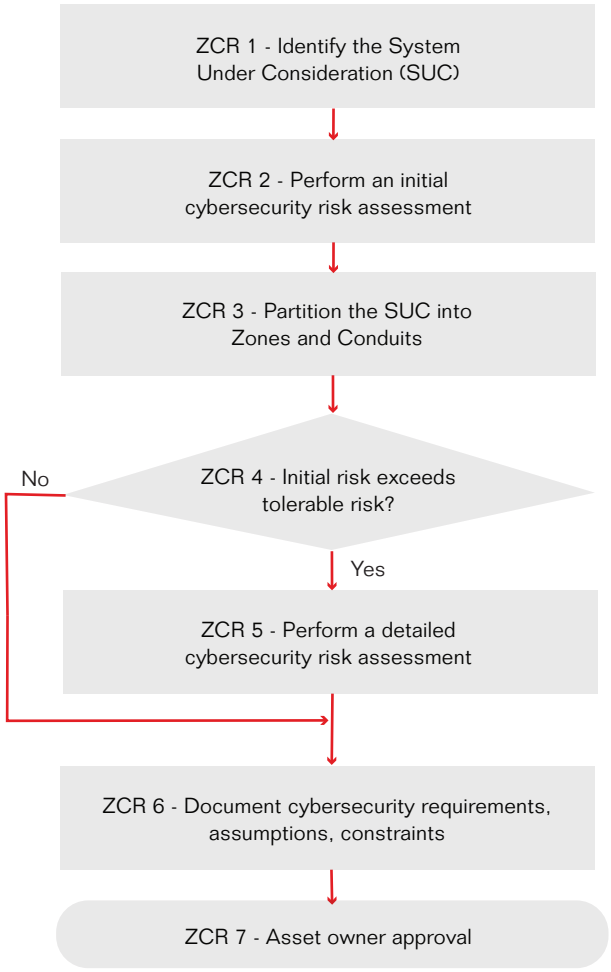


Figure 5 - Risk Assessment Process

Security Level

Security Level is defined as the measure of confidence that the *system under consideration*, security zone or conduit is free from vulnerabilities and functions in the intended manner. [34]

Part 3-3 further defines the Security Level in terms of the means, resources, skills and motivation of the threat actor, as shown in Table 1. It is used as a means to discriminate between requirement enhancements for IACS Systems [35] and IACS Components. [37]

There are three types of Security Levels that are used throughout the ISA/IEC 62443 Series:

- Capability Security Levels (SL-C) are the level of security that IACS Systems [35] or IACS Components [37] can provide when properly integrated and configured. These levels state that a particular IACS System or Component is capable of meeting the SL-T natively without additional compensating security measures.

Target Security Levels (SL-T) are the desired level of security for zones and conduits in a particular Automation Solution. They are determined as the result of the Risk Assessment process [34] and are documented in the Cybersecurity Requirements Specification. [34] SL-T are used to select products and design additional security measures during the integration phase of the Automation Solution security lifecycle.

- Achieved Security Levels (SL-A) are the actual levels of security for zones and conduits in a particular Automation Solution. These are measured after the Automation Solution is commissioned and in operation. Part 2-2 combines SL-A with operational and maintenance policies and processes to form the Security Program Rating for a particular Automation Solution.

It is important to note that the ISASecure® SSA and CSA Certifications only demonstrate that the IACS Systems or Components offered by a Product Supplier have achieved a Capability Security Level (SL-C) in accordance with ISA/IEC 62443-3-3 [35] and ISA/IEC 62443-4-2 [37] respectively. The Asset Owner must add the appropriate policies, processes and skilled personnel to meet the Achieved Security Level (SL-A).

Security Level	Definition	Means	Resources	Skills	Motivation
1	Protection against casual or coincidental violation				
2	Protection against intentional violation using simple means with low resources, generic skills and low motivation	simple	low	generic	low
3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation	sophisticated	moderate	IACS specific	moderate
4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation	sophisticated	extended	IACS specific	high

Table 1 - Security Level Definition

Lifecycle View

Another view of the ISA/IEC 62443 Series is the lifecycle view. There are two independent lifecycles described in the series: the Product Security Lifecycle, and the Automation Solution Security Lifecycle. The Automation Solution Security Lifecycle is further divided into an Integration Phase and an Operation and Maintenance Phase. Table 2 shows the relationship between the Parts of the ISA/IEC 62443 Series and the various lifecycles and phases.

Note that Part 3-3 spans the Product Security Lifecycle and the Integration Phase of the Automation Solution Security Lifecycle. This is because while the Product Supplier is the main audience for Part 3-3, the Integration Service Provider may also combine IACS Components to create IACS Systems. An example would be a SCADA system, where the Integration Service Provider combines the SCADA system with embedded devices (e.g. PLC) to create an Automation Solution. The ISASecure® Certification Scheme currently includes certification of products and the security development lifecycle in the Product Development Lifecycle.

<table>
<tr><th rowspan="2">Product Development Lifecycle</th><th colspan="2">Automation Solution Lifecycle</th></tr>
<tr><th>Integration</th><th>Operation and Maintenance</th></tr>
<tr><td colspan="3">Part 1-1: Terminology, Concepts, and Models</td></tr>
<tr><td rowspan="5"></td><td colspan="2">Part 2-1: Establishing an IACS Security Program</td></tr>
<tr><td colspan="2">Part 2-2: IACS Security Program Rating</td></tr>
<tr><td colspan="2">Part 2-3: Patch Management in the IACS Environment</td></tr>
<tr><td colspan="2">Part 2-4: Security Program Requirements for IACS Service Providers</td></tr>
<tr><td colspan="2">Part 3-2: Security Risk Assessment for System Design</td></tr>
<tr><td colspan="3">Part 3-3: System Security Requirements and Security Levels</td></tr>
<tr><td>Part 4-1: Product Security Development Lifecycle Requirements</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Part 4-2: Technical Security Requirements for IACs Components</td></tr>
</table>

Table 2 - ISA/IEC 62443 Standards - Lifecycle View

ISASecure® Certification

ISA Security Compliance Institute

The ISA Security Compliance Institute (ISCI) is the owner and developer of the ISASecure® Certification Scheme. ISCI is one of several operational groups within the Automation Standards Compliance Institute (ASCI), which is a 501c non-profit corporation owned by the International Society of Automation (ISA).

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, Product Suppliers, Service Providers 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;
- 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. The ultimate goal is to push the conformance testing into the product development life cycle so that the products are intrinsically secure.

Information about the ISA Security Compliance Institute and the ISASecure® Certification Scheme is publicly available and can be found at www.isasecure.org

- ISCI Membership - https://www.isasecure.org/en-US/About-Us/Current-Members
- ISASecure® Certification Scheme - https://www.isasecure.org/en-US/Certification
- ISASecure® Certification Bodies - https://www.isasecure.org/en-US/Certification-Bodies
- ISASecure® Certified IACS Components - https://www.isasecure.org/en-US/End-Users/Certified-Components
- ISASecure® Certified IACS Systems – https://www.isasecure.org/en-US/End-Users/Certified-Systems
- ISASecure® Certified SDL - https://www.isasecure.org/en-US/End-Users/Certified-Development-Organizations
- Types of products - https://www.isasecure.org/en-US/Documents/06-0519-What-Products-are-Certifiable-revise-27Jun

ISASecure® Certification Scheme

Table 3 describes the ISASecure® Certification Scheme using the terms and definitions found in ISO/IEC 17000 – Conformity assessment – Vocabulary and general principles [12].

- ISASecure® is a third-party conformity assessment scheme, also known as a certification scheme. The ISASecure® Certification Scheme currently includes SDLA, SSA and CSA.
- The ISASecure® Certification Scheme is based on the specified requirements in the ISA/IEC 62443 series of standards.
- ISASecure® third-party conformity assessment bodies, also known as ISASecure® Certification Bodies, perform the assessment and issue ISASecure® Certificates for IACS Systems, Components and product security development lifecycles. The Product Suppliers' proprietary information is held in confidence by the ISASecure® Certification Body.
- ISASecure® Accreditation Bodies assess the capability of ISASecure® Certification Bodies to perform ISASecure® Certifications by assessing their competence, consistent operation and impartiality.
- The ISA Security Compliance Institute is the certification scheme owner and is responsible for the development and maintenance of the ISASecure® Certification Scheme.

Term	Definition	ISASecure equivalent
Conformity Assessment	demonstration that specified requirements are met. Conformity assessments can be first-party, second-party or third-party.	
Specified Requirements	need or expectation that is stated	ISA/IEC 62443 standards
Certification	third-party conformity assessment, excluding accreditation	ISASecure® certification
Conformity Assessment Scheme	set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements, and provides the methodology of performing conformity assessment	
Certification Scheme	third-party conformity assessment scheme	ISASecure® certification scheme
Conformity assessment body	body that performs conformity assessment activities, excluding accreditation	
Certification body	third-party body that performs conformity assessment activities, excluding accreditation	ISASecure® certification body
Accreditation	third-party attestation related to conformity assessment body conveying formal demonstration of its competence, consistent operation and impartiality in performing specific conformance assessment activities	ISASecure® accreditation
Accreditation body	body that performs accreditation	ISASecure® accreditation body
Certification Scheme Owner	Person or organization responsible for development and maintenance of a conformity assessment scheme	ISA Security Compliance Institute

Table 3- ISO/IEC 17000 conformity assessment terms

Figure 6 shows the roles and responsibilities for the ISASecure® Certification Scheme:

- The ISA Security Compliance Institute develops and maintains the ISASecure® Certification Scheme based on applicable ISA/IEC 62443 standards and selects accreditation bodies that meet the requirements of ISO/IEC 17011 [13].
- ISASecure® Accreditation Bodies assess the capabilities of ISASecure® Certification Bodies and accredit them in accordance with the ISASecure® Certification Scheme, ISO/IEC 17025 [14], and ISO/IEC 17065 [15].
- IACS Asset Owners and IACS Integration Service Providers specify that the products used for their Automation Solutions are certified in accordance with the ISASecure® Certification Scheme at a specified Capability Security Level (SL-C).
- IACS Product Suppliers request certifications for their security development lifecycle and their IACS products from an ISASecure® Certification Body in accordance with the ISASecure® Certification Scheme.
- If the conformity assessment of the security development lifecycle and the product demonstrates that the applicable requirements of ISA/IEC 62443 are met, then the IACS Product Supplier receives an ISASecure® Certificate, which is available to the Integration Service Provider and Asset Owner on the ISASecure.org website.

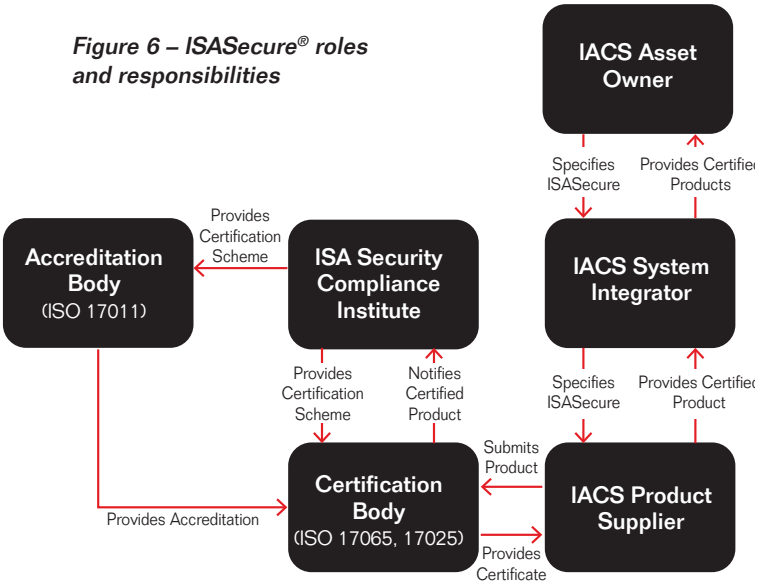
ISASecure® Security Development Lifecycle Assurance (SDLA)

The ISASecure® Security Development Lifecycle Assurance (SDLA) certification scheme is based on ISA/IEC-62443-4-1:2018 – Security for industrial automation and control systems, Part 4-1: Product security development life-cycle requirements. [36]

The ISASecure® SDLA certification scheme [1] includes a Software Development Lifecycle Process Assessment (SDPLA), which includes the following eight practices from ISA/IEC-62443-4-1:

- Security Management (SM)

Figure 6 – ISASecure® roles and responsibilities



- Specification of security requirements (SR)
- Secure by design (SD)
- Secure implementation (SI)
- Security verification and validation testing (SVV)
- Management of security-related issues (DM)
- Security update management (SUM)
- Security guidelines (SG)

For initial SDLA certification, the certification body will verify that the Product Supplier has a documented security development lifecycle under change control that complies with SDLA requirements. The certification body will also review selected artifacts showing the Product Supplier has executed the documented processes. If some required artifacts are not yet available, but the Product Supplier demonstrates readiness to execute related aspects of the security development lifecycle, an initial certificate may be granted with a 12 month duration. During this time, if the remaining artifacts are presented, a final SDLA certificate is granted.

Figure 7 - ISASecure® SDLA

An ISASecure® SDLA certification expires in three years and may be extended once the Product Supplier passes a recertification audit. The recertification audit verifies that changes to the previously certified security development lifecycle are recorded and comply with the current version of SDLA, and that the current security development lifecycle is being followed for all products within its defined scope.

Since both the ISASecure® System Security Assurance (SSA) and ISASecure® Component Security Assurance (CSA) certification schemes require an assessment of the Product Suppliers' security development lifecycle, the SDLA certification allows the Product Supplier to complete this certification once and apply it to multiple product certifications.

ISASecure® System Security Assurance (SSA)

The ISASecure® System Security Assurance (SSA) certification scheme [8] is based on ISA/IEC-62443-3-3:2013 – Security for industrial automation and control systems, Part 3-3: System security requirements and security levels. [35]

The ISASecure® SSA certification scheme assesses the Capability Security Level (SL-C) of the IACS System in accordance with ISA/IEC-62443-3-3. IACS Systems that can be certified consist of an integrated set of IACS Components, are under configuration control and version management, and are provided by a single Product Supplier.

There are four elements included in the ISASecure® SSA certification scheme:

- Security Development Lifecycle Process Assessment for Systems (SDLPA-S) – the Product Supplier must hold a current ISASecure® SDLA certification, and the system being certified is included in the scope of that SDLA certification. [15]
- Security Development Artifacts for Systems (SDA-S) – an examination of the artifacts required by the SDLA certification for the system that is being certified. [13]
- Functional Security Assessment for Systems (FSA-S) – an assessment that each security zone in the system meets the requirements of ISA/IEC-62443-3-3 for the specified Security Level. The ISASecure® Certificate will list the Capability Security Level (SL-C) for each security zone in the system. [12]
- Vulnerability Identification Testing for Systems (VIT-S) – a scan of all network interfaces of all IACS Components in each security zone from inside the security zone using the Tenable Network Security Nessus vulnerability assessment tool with an ISASecure-specific policy. [14]

ISASecure® Component Security Assurance (CSA)

The ISASecure® Component Security Assurance (CSA) certification scheme [18] is based on ISA/IEC-62443-4-2:2019 – Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS Components. [37]

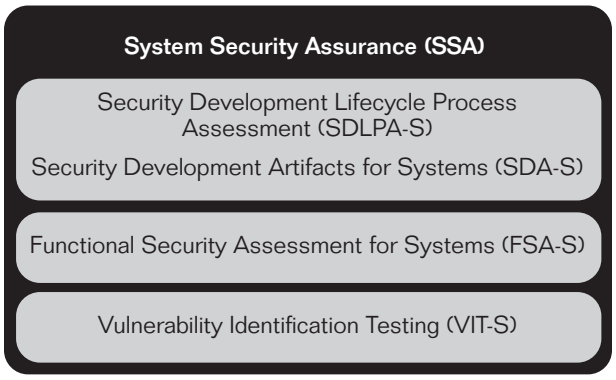


Figure 8 - ISASecure® SSA

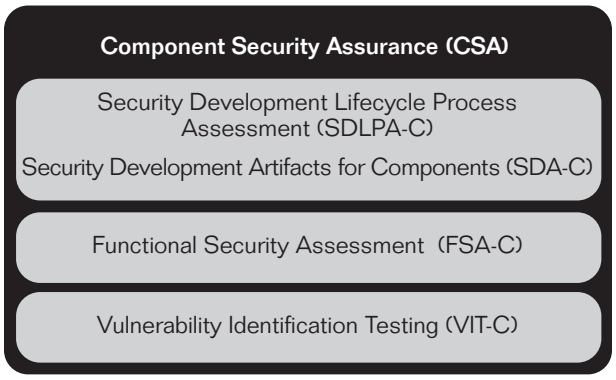


Figure 9 - ISASecure® CSA

There are four types of IACS Components that can be assessed using the ISASecure® CSA certification scheme:

- Embedded devices such as controllers, programmable logic controllers, and safety instrumented systems
- Host devices such as industrial computers, embedded PCs, HMI panels and industrial tablets
- Network devices such as routers, switches, firewalls, wireless access points and security appliances
- Software applications such as control application software, data historians and HMI software

The ISASecure® CSA certification scheme assesses the Capability Security Level (SL-C) of the IACS Component in accordance with ISA/IEC-62443-4-2. Composite devices, which may include more than one type of component, are evaluated against all of the requirements for each component type.

There are four elements included in the ISASecure® CSA certification scheme:

- Security Development Lifecycle Process Assessment for Components (SDLPA-C) – the Product Supplier must hold a current ISASecure® SDLA certification, and the component being certified is included in the scope of that SDLA certification. [26]
- Security Development Artifacts for Components (SDA-C) – an examination of the artifacts required by the SDLA certification for the IACS Component that is being certified. [24]
- Functional Security Assessment for Components (FSA-C) – an assessment that the IACS Component meets the requirements of ISA/IEC-62443-4-2 for the specified Security Level. [23]
- Vulnerability Identification Testing for Components (VIT-C) – a scan of all network interfaces of the IACS Component being certified using the Tenable Network Security Nessus vulnerability assessment tool with an ISASecure-specific policy. [25]

Using the ISASecure® Certification Scheme

Benefits of using ISASecure® Certification

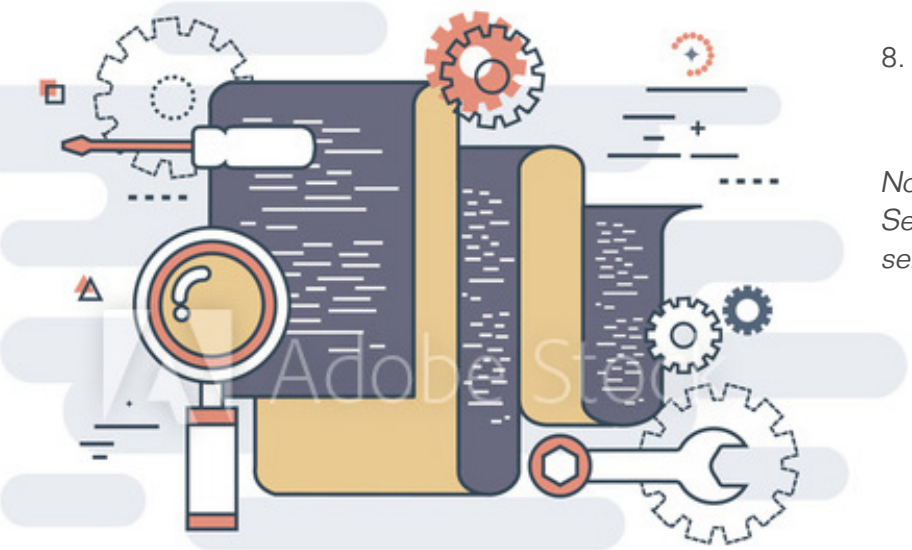
- The ISASecure® SDLA certification independently demonstrates that the Product Supplier has used a product security development lifecycle that complies with ISA/IEC 62443-4-1 – Product security development lifecycle requirements, which includes:
  - A security development lifecycle integrated with the product development lifecycle
  - Secure design including defense in depth and threat modelling
  - Secure implementation and security verification and validation testing
  - Management of security related issues and security update management
  - Security hardening guidelines that are available to Asset Owners and Integration Service Providers
- The ISASecure® SSA certification independently demonstrates that IACS System products comply with the requirements of ISA/IEC-62443-3-3 – System security requirements and security levels at a specified Capability Security Level (SL-C).
- The ISASecure® CSA certification independently demonstrates that IACS Components comply with the requirements of ISA/IEC-62443-4-2 – Technical security requirements for IACS components at a specified Capability Security Level (SL-C).
- Products procured using the ISASecure® Certification Scheme have the capability to support the requirements of ISA/IEC-62443-2-1 – Security program requirements for IACS asset owners because the technical requirements for IACS Systems and IACS Components are derived from ISA/IEC-62443-2-1
- ISASecure® specifications are publicly available, so all stakeholders can review the certification criteria and how they are used to certify a security development lifecycle or an IACS product

- The ISASecure® Certification Bodies are accredited based on the ISO/IEC 17000 series of standards which allows ISASecure® Certifications to be globally recognized.
- Product Suppliers can use ISASecure® Certificates in product marketing for their products.

ISASecure® for Asset Owners and Operators

How Asset Owners can use ISASecure® Certification:

1. Establish company policy for the use of ISA/IEC 62443
2. Establish company policy for minimum IACS Security Level using ISA/IEC-62443-3-3 – System security requirements and security levels
3. Perform/approve the IACS cybersecurity risk assessment, zone partitioning and selected Target Security Levels in accordance with ISA/IEC-62443-3-2 – Security risk assessment and system design
4. Document/approve the IACS Cybersecurity Requirements Specification (CRS) that includes ISASecure® Certification
5. Procure IACS System and IACS Component products based on IACS CRS with ISASecure® Certification



ISASecure® for Integration Service Providers

How Integration Service Providers can use ISASecure® Certification:

1. Establish company policy for the use of ISA/IEC 62443
2. Update Integration Service Provider processes to comply with ISA/IEC-62443-2-4 – Security program requirements for service providers
3. Independently certify that the Integration Service Provider processes comply with ISA/IEC-62443-2-4. As of this publication, a certification using the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE.org) is available. [9]
4. Determine Asset Owner policies regarding the use of ISA/IEC-62443 and ISASecure® for their projects, and minimum Security Levels for IACS Systems and Components.
5. Perform the IACS cybersecurity risk assessment, zone partitioning and Security Level selection with the Asset Owner
6. Complete the IACS Cybersecurity Requirements Specification that includes ISASecure® Certification
7. Procure IACS System and IACS Component products in accordance with IACS Cybersecurity Requirements Specification and ISASecure® Certification requirements
8. Complete the remaining integration phase lifecycle steps and handover the IACS to the Asset Owner.

Note: the steps to be completed by the Integration Service Provider will depend on the scope of the service agreement with the Asset Owner.

ISASecure® for Product Suppliers

For the Product Supplier certification supports a proactive approach to achieve competence in cybersecurity. It provides a recognized framework and path to understanding, establishing and continuing to improve best practices within the organization.

How Product Suppliers can use ISASecure® Certification:

1. Establish company policy for the use of ISA/IEC 62443
2. Update product development processes to comply with ISA/IEC-62443-4-1 – Product security development lifecycle requirements
3. Independently certify that the product development processes comply with ISA/IEC-62443-4-1 using the ISASecure® Security Development Lifecycle Assurance (SDLA) certification scheme
4. Design and develop IACS System products to comply with ISA/IEC-62443-3-3 – System security requirements and security level
5. Independently certify that the IACS System products comply with ISA/IEC-62443-3-3 using the ISASecure® System Security Assurance (SSA) certification scheme
6. Design and develop IACS Component products to comply with ISA/IEC-62443-4-2 – Technical requirements for IACS components
7. Independently certify that the IACS Component products comply with ISA/IEC-62443-3-3 using the ISASecure® System Security Assurance (SSA) certification scheme
8. Maintain the SDLA certification by re-certifying the product development processes every three years

Frequently Asked Questions

Is an ISASecure® Certification a point in time certification?

An ISASecure® product certificate is issued for a specific product and version. A significant upgrade to the product requires a re-certification. The product certification also requires that the Product Supplier has an ISASecure® SDLA certification, which requires that security vulnerabilities found after the product is released are analyzed and addressed, and threat models and security guidelines are updated as new threats emerge.

How much does an ISASecure® Certification cost?

For the Asset Owner and Integration Service Provider, there is no additional cost for an ISASecure® Certification. For the Product Supplier there are two parts of the total cost: the ISASecure® Certification fee which is published on the ISASecure.org website, and the cost associate with the conformity assessment itself which is negotiated with the ISASecure® Certification Body.

Are the security vulnerabilities of a certified product disclosed to the public?

If the ISASecure® Certification Body finds security vulnerabilities in the product during the certification process, they are reported to the Product Supplier for resolution in accordance with ISA/IEC-62443-4-1 and the SDLA certification.

Does the ISA Security Compliance Institute receive a Product Supplier's proprietary information?

ISASecure® Certification Bodies conduct assessments in accordance with ISO/IEC 17065 and maintain the confidentiality of the Product Supplier's assessment information. As the owner of the ISASecure® Certification Scheme, random work products related to a Product Supplier assessment may be examined by ISA Security Compliance Institute staff at infrequent intervals to ensure the quality of the ISASecure® Certification Scheme or to process a complaint to ISCI lodged by a Product Supplier.

Does the ISASecure SDLA certification support Maturity Levels?

The ISASecure® SDLA certification scheme currently does not assess the Maturity Level of the organization for the processes that are defined in ISA/IEC-62443-4-1.

Is the ISASecure® Certification Scheme aligned with ISA/IEC-62443 standards?

The first ISASecure® Certification Schemes were introduced before the relevant ISA/IEC-62443 standards were published and were based on committee drafts. Since then, the relevant ISA/IEC-62443 standards have been published, and all ISASecure® Certification Schemes have been updated to conform to the published standards.

The ISASecure® Certification Scheme previously included Communication Robustness Testing (CRT), has it been dropped in the most recent version?

Previous ISASecure® Certification Schemes included fuzz testing and network load testing (also known as CRT) as specific tests to be completed by the ISASecure® Certification Body as part of an SSA or EDSA certification. The ISA-62443-4-1 published standard includes a requirement that the Product Supplier has a process to perform fuzz testing and network traffic load testing as part of their security development lifecycle. The current version of ISASecure® SSA and CSA requires the ISASecure® Certification Body to inspect the artifacts that the Product Supplier has completed these tests for the product being assessed.

What happened to the ISASecure® Embedded Device Security Assurance (EDSA) certification scheme?

The ISASecure® EDSA certification scheme was introduced before the ISA/IEC 62443-4-2 Technical requirements for IACS components standard was published. This standard defines the requirements for embedded devices, host devices, network devices, and software applications. The ISASecure® Component Security Assurance (CSA) certification scheme was subsequently created to cover all IACS Component types specified in ISA/IEC-62443-4-2. So EDSA is now a part of the ISASecure® CSA certification.

Published ISASecure® Specifications

Security Development Lifecycle Assurance 3.0.0

1. SDLA-100 – ISASecure Certification Scheme
2. SDLA-102 – Baseline Document Versions and Errata
3. SDLA-204 – Instructions and Policies for The Use of The ISASecure® Symbol and Certificate
4. SDLA-205 – Certificate Document Format
5. SDLA-300 – ISASecure Certification and Maintenance of Certification Requirements
6. SDLA-312 – Security Development Lifecycle Assessment
7. ISASecure-118 – Policy for Transition to SDLA 3.0.0

System Security Assurance 4.0.0

8. SSA-100 – ISASecure Certification Scheme
9. SSA-102 – Baseline Document Versions and Errata
10. SSA-300 – ISASecure Certification Requirements
11. SSA-301 – Maintenance of ISASecure Certification
12. SSA-311 – Functional Security Assessment for Systems (FSA-S)
13. SSA-312 – Security Development Artifacts for Systems (SDA-S)
14. SSA-420 – Vulnerability Identification Test Specification
15. SDLA-100 – Isasecure Certification Scheme
16. SDLA-312 – Security Development Lifecycle Assessment
17. ISASecure-117 – Policy for Transition To CSA 1.0.0 And SSA 4.0.0

Component Security Assurance 1.0.0

18. CSA-100 – ISASecure Certification Scheme
19. CSA-102 – Baseline Document Versions and Errata
20. CSA-204 – Instructions and Policies for Use of The ISASecure® Symbol and Certificate
21. CSA-300 – ISASecure Certification Requirements
22. CSA-301 – Maintenance of ISASecure Certification
23. CSA-311 – Functional Security Assessment for Components
24. CSA-312 – Security Development Artifacts for Components
25. SSA-420 – Vulnerability Identification Test Specification
26. SDLA-100 – ISASecure Certification Scheme
27. SDLA-312 – Security Development Lifecycle Assessment
28. ISASecure-117 – Policy for Transition to CSA 1.0.0 And SSA 4.0.0

Published Standards and Technical Reports

29. ISA-62443-1-1-2007 / IEC TS 62443-1-1:2009 – Security for Industrial Automation and Control Systems, Part 1-1: Terminology, Concepts and Models
30. ISA-62443-2-1-2009 / IEC 62443-2-1:2010 – Security for Industrial Automation and Control Systems, Part 2-1: Establishing an Industrial Automation and Control Systems Security Program
31. ANSI/ISA-TR62443-2-3-2015 / IEC TR 62443-2-3:2015 – Security for Industrial Automation and Control Systems, Part 2-3: Patch Management in The IACS Environment

32. ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV – Security for Industrial Automation and Control Systems, Part 2-4: Security Program Requirements For IACS Service Providers
33. IEC Tr 62443-3-1:2009 - Security for Industrial Automation and Control Systems, Part 3-1: Security Technologies for Industrial Automation and Control Systems
34. ANSI/ISA-62443-3-2-2020 / IEC-62443-3-2-2020 – Security for Industrial Automation and Control Systems, Part 3-2: Security Risk Assessment and System Design
35. ANSI/ISA-62443-3-3-2013 / IEC 62443-4-2:2013 – Security for Industrial Automation and Control Systems, Part 3-3: System Security Requirements Aand Security Levels
36. ANSI/ISA-62443-4-1-2018 / IEC 62443-4-1:2018 – Security for Industrial Automation and Control Systems, Part 4-1: Product Security Development Life-Cycle Requirements
37. ANSI/ISA-62443-4-2-2018 / IEC 62443-4-2:2019 – Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components
38. IEC TR 63069:2019 – Industrial-Process Measurement, Control and Automation – Framework for Functional Safety and Security
39. IEC TR 63074:2019 – Safety of Machinery – Security Aspects Related to Functional Safety of Safety-Related Control Systems
40. ISO/IEC DIS 17000, Conformity Assessment – Vocabulary and General Principles
41. ISO/IEC 17011:2017, Conformity Assessment – Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies
42. ISO/IEC 17025:2017, General Requirements for The Competence of Testing and Calibration Laboratories
43. ISO/IEC 17065, Conformity Assessment – Requirements for Bodies Certifying Products, Processes and Services

References

44. Quick Start Guide: An Overview of ISA/IEC 62443 Standards, ISA Global Cybersecurity Alliance, https://gca.isa.org/blog/download-the-new-guide-to-the-ISA/IEC-62443-Cybersecurity-Standards
45. NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security
46. The 62443 Series of Standards: Industrial Automation and Control Security, ISA99 Committee
47. Frequently Asked Questions: The ISA99 Committee and 62443 Standards, ISA99 Committee
48. Instrumentation and Control Systems Security Explained: The What and The Why, ISA99 Committee
49. What's The Difference Series: Compliance vs Certification, Miriam Boudreax, Mireaux Management Solutions, https://www.mireauxms.com/blog/whats-the-difference-series-compliance-vs-certification/
50. Certification & Conformity, ISO.org, https://www.iso.org/conformity-assessment.html
51. Capability Maturity Model, wikipedia.org, https://en.wikipedia.org/wiki/capability_maturity_model
52. IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE.org)

View the ISASecure® Certifications at
www.isasecure.org/certification

ISASecure®

International Society of Automation
www.ISASecure.org
67 T.W. Alexander Drive
Research Triangle Park, NC 27709
+1 919 990 9222
aristaino@isa.org

06-0920