Security Standards Compliance

The proposed solution must have been developed using security development practices and have appropriate security features in place to mitigate potential risk. COMPANY NAME has selected IEC 62443 to define cybersecurity requirements. Vendors must certify products to the IEC 62443 standard using the ISA Secure Compliance scheme. For more details on ISA Secure, refer to the ISA Security Compliance Institute (ISCI) Certification Addendum.

Offer must provide proof of compliance with IEC 62443-4-1 through ISA Secure certification (for offer)

Offer must provide proof of compliance with IEC 62443-4-2 SCL- (define security level) through ISA Secure certification (for offer)

Offer must provide proof of compliance with IEC 62443-3-3 SL- (define security level) through ISA Secure certification (for system)

ISA Security Compliance Institute (ISCI) Certification Addendum

In accordance with IEC 62443, this addendum serves as the minimal requirements for any supplier providing network-connectable products and systems, as part of a contractual bid to COMPANY NAME, referred to as “The Procuring Organization” henceforth.

Background

The ISA Security Compliance Institute (ISCI), a not-for-profit automation controls industry consortium, manages the ISASecure conformance certification program. ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities.

The ISASecure designation is earned by industrial control suppliers for products that demonstrate adherence to industry consensus cybersecurity specifications for security characteristics and supplier development practices.

Certification Overview

ISCI offers three certifications with four security assurance levels (SAL) in alignment with ISA/IEC 62443. There is an expectation that any product and/or system meet the appropriate certification criteria summarized below. For more details and how to apply for certification, visit www.isasecure.org/en-US.

1. ISASecure Component Security Assurance (CSA) Certification

Component Security Assurance (CSA) focuses on the security of individual device characteristics and supplier development practices for those devices. The CSA certification is designed to certify to international standard IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development requirements and to the international standard IEC 62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components.

To obtain ISASecure CSA certification, a supplier must pass a security development lifecycle process assessment (SDLPA). Based upon this assessment, an ISASecure SDLA process certification is granted as described in SDLA-100 (see below). A supplier may already hold an SDLA process certification when they apply for an CSA certification or may apply for CSA and SDLA certification in parallel.

The program offers four certification levels for a device (Embedded, Host, Software, and Network), each offering increasing levels of device security assurance.

2. ISASecure System Security Assurance (SSA) Certification

The SSA requirements for certification include all control system requirements in IEC 62443-3-3 "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels” and all process requirements in IEC 62443-4-1 “Security for industrial automation and control systems – Secure product development requirements.” In addition, embedded devices and other components included in the control system under test must be CSA certified or meet the CSA requirements for certifier testing and functional assessment at the time of certification.

ISASecure SSA is a certification program for a particular subset of control systems. A control system product that meets all the following criteria may be certified under the SSA program:

- The control system consists of an integrated set of components and includes more than one device.
- The control system is available from and supported by a single supplier, although it may include hardware and software components from several manufacturers.
- The control system may have a fixed device and zone layout, or may be scalable, that is, may support replication of devices and of zones to scale for small and large installations.
- The system product is under configuration control and version management.

3. ISASecure Security Development Lifecycle Assurance (SDLA) Certification

ISASecure SDLA is a certification program that applies to the development lifecycle processes of suppliers for control system products. The ISASecure SDLA certification program certifies compliance to IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product lifecycle requirements (also published as ANSI/ISA-62443-4-1).

An SDLA certification is granted for:

- A named development organization or organizations
- A specific version of a named, documented development lifecycle process under version control that is used by that organization(s).

The documented process itself shall specify:

- Whether it applies to development of components, systems or both
- The scope of products to which the organization applies the process (which may be all products).