ISA Security Compliance Institute

ISASecure

NIST Cybersecurity Framework
ISCI Response to Request for Information

Date:	April 5, 2013
Organization:	Automation Standards Compliance Institute / The Automation Federation
Committee:	ISA Security Compliance Institute (ISCI)
Type:	International standards compliance certification programs
Sector Scope:	Cross-sector
Technical Scope:	Industrial Automation and Control Systems

On behalf of the ISA Security Compliance Institute (ISCI), we are pleased to submit this response to the Request for Information on the subject of Framework for Reducing Cyber Risks to Critical Infrastructure. In providing the requested information, we have focused on the ISASecure certification programs for Industrial Automation and Control Systems, which is a set of conformance programs for the ISA-62443 series of standards.

Respectfully,

Andre Ristaino
Managing Director, Automation Standards and Compliance Institute

Johan Nye
Chairman, Governing Board of the ISA Security Compliance Institute

67 Alexander Drive P.O. Box 12277 RTP, NC 27709
Phone 919-990-9222 Fax 919-549-8288

Table of Contents

Useful Links

ISASecure - http://www.isasecure.org/

ANSI/ISASecure – http://www.ansi.org/isasecure/

ISA 99 – http://isa99.isa.org/

67 Alexander Drive P.O. Box 12277 RTP, NC 27709
Phone 919-990-9222 Fax 919-549-8288

1 About the Automation Standards Compliance Institute (ASCI)

ISA is a professional engineering society and an ANSI accredited standards development organization (SDO) that manages standards committees comprised of volunteer subject matter experts in the field of industrial automation and process controls. During its 65 year history, ISA published over 144 industry standards, many of which have been adopted as international standards.

In 2006, ISA established the Automation Standards Compliance Institute (ASCI) as a separately incorporated non-profit organizational entity to support programs that assess automation-related standards compliance. The institute's charter addresses a wide range of standards compliance assessments including software or hardware products, implementation methods, solutions, companies and individuals. ASCI provides the organization and staff necessary to support on-going conformance operations; and ensures a level of independence between ISA's standards committee processes and the conformance certification programs.

ASCI conformance certification programs provide a vital link between the standards ISA develops and the implementation of those standards. ASCI also offers a platform to partner with other organizations and assess conformity of their standards. A feasibility study, market study, and legal assessment performed in 2005 and 2006 indicated that a standards conformity program was needed to provide a useful link between automation standards and the products, services, processes and systems that use them. The studies revealed that automation users are increasingly recognizing the value of adopting true industry standards and that the next step in this evolution was to ensure that the solutions selected in fact adhere to these standards. ASCI is chartered to educate users and help suppliers transform standards into real interoperable products.

ASCI is governed by a Board of Directors comprised of ISA leaders, legal counsel, and an industry consultant. Within ASCI, groups called *Institutes* are formed to address specific interest areas for standards conformance. Each Institute operates as an industry consortium, establishing its own membership structure and governance policies based on stakeholder needs and industry requirements. Institute memberships are fair and open, and conformance certifications are available to Institute members and non-members. ASCI bylaws share the open constructs of ISA, while accounting for compliance organization requirements. ASCI Articles of Incorporation and Bylaws are available online at the following links:

Articles of Incorporation

Bylaws

ASCI currently operates two Institutes:

- ISA Security Compliance Institute (ISCI) www.isasecure.org
- ISA100 Wireless Compliance Institute (WCI) www.isa100wci.org

The ISA Security Compliance Institute is the organization responding to this RFI.

67 Alexander Drive P.O. Box 12277 RTP, NC 27709
Phone 919-990-9222 Fax 919-549-8288

2 About the ISA Security Compliance Institute (ISCI)

The ISA Security Compliance Institute manages the ISASecure® program which recognizes and promotes cyber-secure products and practices for industrial automation suppliers and operational sites.

The ISASecure® designation is earned by industrial control suppliers for products that demonstrate adherence to ISCI cyber security specifications derived from open, consensus industry standards. ISASecure® certifications evaluate product/system cyber security characteristics, laboratory test products/systems and, assess supplier's adherence to cyber security lifecycle development best practices.

2.1 Mission

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;
- 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.

2.2 Accreditation

Accreditation assures users of the competence and impartiality of the certification body (CB) being accredited. ISASecure® is an ISO/IEC Guide 65 conformance scheme. As such, all ISASecure® certification bodies (test labs) are independently accredited to ISASecure® requirements, ISO/IEC Guide 65 and ISO/IEC 17025 by an ISO/IEC 17011 accreditation body such as ANSI/ACLASS, the Japan Accreditation Bureau (JAB) and other country-specific ISO/IEC 17011 accreditation bodies. The link to the ANSI/ACLASS website for ISASecure® is www.ansi.org/isasecure.

ISO/IEC 17011 accreditation bodies participate in Multilateral Recognition Arrangements (MRA) via global forums such as the International Accreditation Forum (IAF) and Asia Pacific Accreditation and Certification Commission (APAC). The purpose of the MRA is to establish a globally efficient approach for ensuring that certificates of conformance issued by a lab in any global region are fully recognized by other participating regions. The MRA agreements reduce supplier conformance certification costs and, reduce barriers to trade and, support global scalability of the ISASecure® conformance scheme.

2.3 ISCI Relationship to ISA99 Standards Committee and ISA-62443 standards

ISCI develops industrial automation control systems certifications which assess conformance to the ISA-62443 standards. To ensure that the ISASecure® certifications remain harmonized with the ISA-62443 standards, ISCI has committed to update ISASecure® certification specifications when the referenced standards are changed by the ISA-62443 committees during planned review/maintenance activities. A formal liaison position has been established on the ISCI Governing board to facilitate correspondence between the ISA99 standards committee and ISCI. The liaison role facilitates a formal feedback loop from implementers (ISCI stakeholder groups) of the standards to the standards committees drafting and maintaining the standards. Stakeholder groups include automation suppliers, asset owner/operators, system integrators, accredited test labs and, test tool suppliers.

The ISA-62443 standards are developed by the ISA 99 committee, which maintains a formal liaison with IEC TC65/WG10 and ISO/IEC JTC1/SC27. ISA-62443 standards are simultaneously submitted to the ISA committee and international bodies for approval. Please refer to the ISA 99 Cybersecurity Framework RFI submittal, section 5, for additional information.

ISCI conformance schemes also reference other relevant international standards, such as IEC 61508 and IEC 61511 for Safety Instrumented Systems, as appropriate to the particular certification program.

2.4 Membership

Membership is open to commercial organizations such as suppliers and owner/operators, trade associations and government organizations for a fee. The following membership categories were established to represent all stakeholder groups:

- Strategic membership – voting members of the Governing Board and Technical Committee
- Technical membership – voting members of the Technical Committee
- Association membership – non-voting members of the Technical Committee
- Government membership – non-voting members of the Technical Committee
- Informational membership – non-participating organization desiring to stay current regarding ISCI affairs

Current ISCI members include the following organizations:

- Chevron
- exida
- ExxonMobil
- Honeywell
- Information-technology Promotion Agency, Japan (IPA)
- Invensys
- ISA99 Standards Committee Liaison
- RTP Corporation
- Siemens
- Yokogawa

67 Alexander Drive P.O. Box 12277 RTP, NC 27709
Phone 919-990-9222 Fax 919-549-8288

3 ISASecure Certification Programs

One of the challenges in the Industrial Automation and Control System (IACS) marketplace is that many products are shipped with vulnerabilities that with the proper design, development and test processes in place, could be prevented. Because many IACS products ship with vulnerabilities, it is difficult for asset owners to secure them.

ISASecure® addresses this challenge by establishing accredited product certification programs that verify that the supplier has followed a Security Development Lifecycle, and that the product is shipped without known vulnerabilities.

The ISASecure® program facilitates the reduction of an asset owners' risk by certifying suppliers' products to a specific Security Level. Asset Owners are then able to specify, through their procurement process, the Security Level that is needed for their application, based on a risk assessment process. In addition, ISASecure® certification reports ensure that mitigations and processes necessary to be addressed by the asset owner are clearly identified in user documentation.

The ISASecure® program also addresses risk for the supplier's organization by certifying their products do not include known vulnerabilities and incorporating a security development lifecycle that includes the response to the discovery of new vulnerabilities after the initial certification is complete.

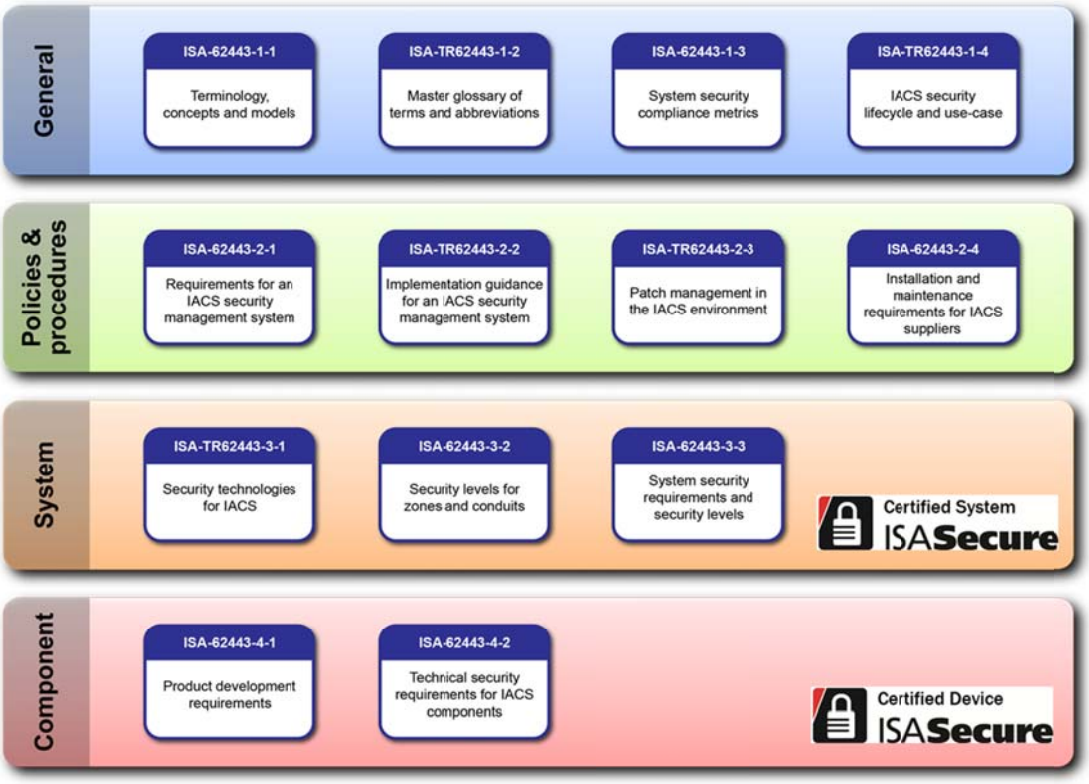

Figure 1 – Relationship between ISA99 Standards and ISASecure® Certification

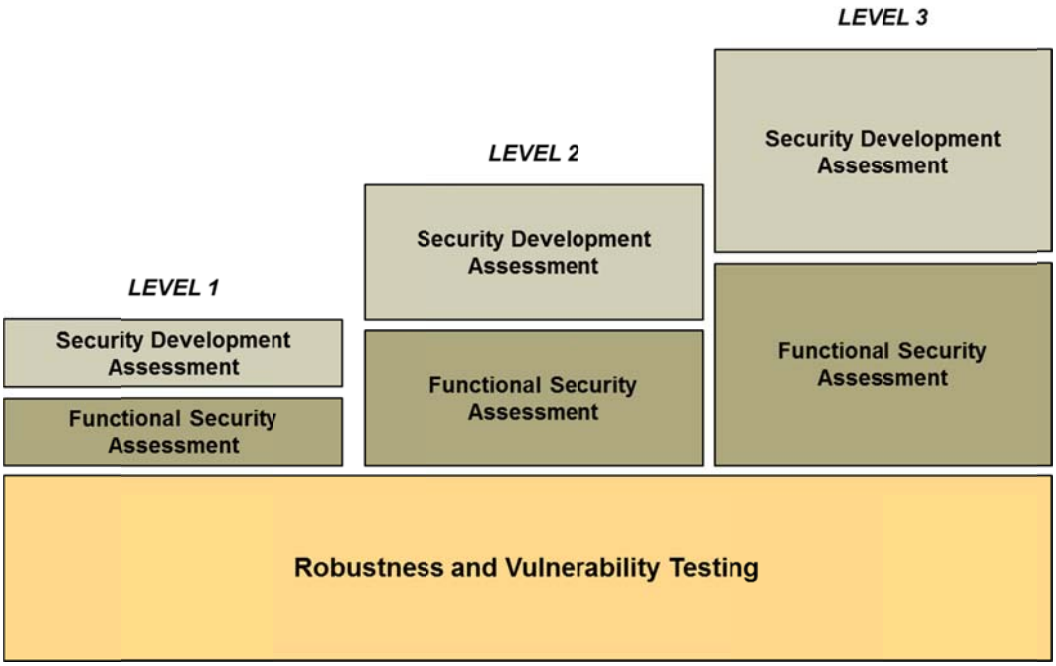

Figure 2 – Elements of an ISASecure Certification Program

3.1 Security Development Lifecycle Assurance (SDLA)

ISASecure® SDLA is a certification program to assess the supplier's product development process to determine if it incorporates a Security Development Lifecycle. The ISASecure® SDLA certification program is currently under development and is expected to be released in the second half of 2013.

The Security Development Lifecycle (SDL) is intended to reduce the susceptibility of software products to cyber vulnerabilities by providing a framework for training, process, and tools resulting in security value to customers. The SDL is tasked with institutionalizing cyber-security within the culture of R&D and across the organization and has been successful in many companies at reducing the susceptibility of products to security vulnerabilities. The SDL seeks to infuse security into all phases of the product lifecycle starting with requirements and proceeding through the end of life for a product. It brings security into the early stages of design and development and ensures that implementation and validation follow the best practice guidelines for creating secure code running in the suite of Industrial Control System applications and products. It is important to note that SDL is a continuous improvement process as the security landscape is ever evolving.

ISCI seeks to certify vendors with development organizations that follow an auditable and well managed SDL process by awarding the ISASecure® logo for SDLA. The certification process looks at each of the following phases to ensure that each show demonstrable compliance to the SDLA specification.

SDLA Phases:

1. Security Management Process – This is the versioned process for planning and managing the security development activities.
2. Security Requirements Specification – Customer driven security requirements must be documented along with security features and mitigations to potential threats that drive the need for these features.
3. Security Architecture Design – The SAD encompasses the high level design and ensures that security is included in the design
4. Security Risk Assessment (Threat Model) – Threat Modeling is the fundamental concept in SDL that determines which components can affect security and which components need threat analysis, security code reviews and security testing.
5. Detailed Software Design – DSD goes to the module level and ensures that each follow security design best practices.
6. Document Security Guidelines – Updated periodically, secure coding guidelines must be accessible to all developers and be instrumental in guiding the security code reviews for enforcement.
7. Module Implementation & Verification – The implementation must follow the secure coding guidelines and thorough security code reviews, static code analysis and module testing ensure that the modules are implemented as securely as possible.
8. Security Integration Testing – Once to the integration phase, the modules are subjected to fuzz testing for interfaces and parsers and also subjected to penetration testing where appropriate.
9. Security Process Verification – An independent assessment is made to ensure the process has been followed as specified.
10. Security Response Planning – It is imperative that a process be put in place so that a development organization can respond quickly to security issues found in the field.
11. Security Validation Testing - Verification must follow from the threat model that each threat is correctly and efficiently mitigated and that all security requirements have been satisfied.
12. Security Response Execution – This takes into consideration documented preventative and corrective actions to security problems in the field. As well, an organization must have a process to validate security patches from other vendors that are used within its products (e.g. COTS OS)

67 Alexander Drive P.O. Box 12277 RTP, NC 27709
Phone 919-990-9222 Fax 919-549-8288

3.2 Embedded Device Security Assurance (EDSA)

ISASecure® EDSA is a certification program for embedded devices, which are special purpose devices running embedded software designed to directly monitor, control or actuate an industrial process. The ISASecure® EDSA certification program is currently available and several suppliers' devices have been certified to ISASecure® Security Level 1 or 2.

ISASecure® certification of embedded devices has three elements:

1. Communication robustness testing (CRT)
2. Functional Security Assessment (FSA)
3. Software Development Security Assessment (SDSA)

CRT examines the capability of the device to adequately maintain essential services while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). These tests include specific tests for susceptibility to known network attacks.

FSA examines the security capabilities of the device, while recognizing that in some cases security functionality may be allocated to other components of the device's overall system environment.

Finally, SDSA examines the process under which the device was developed.

The program offers three certification levels for a device, offering increasing levels of device security assurance. These certifications are called ISASecure® EDSA Level 1, ISASecure® EDSA Level 2, and ISASecure® EDSA Level 3.

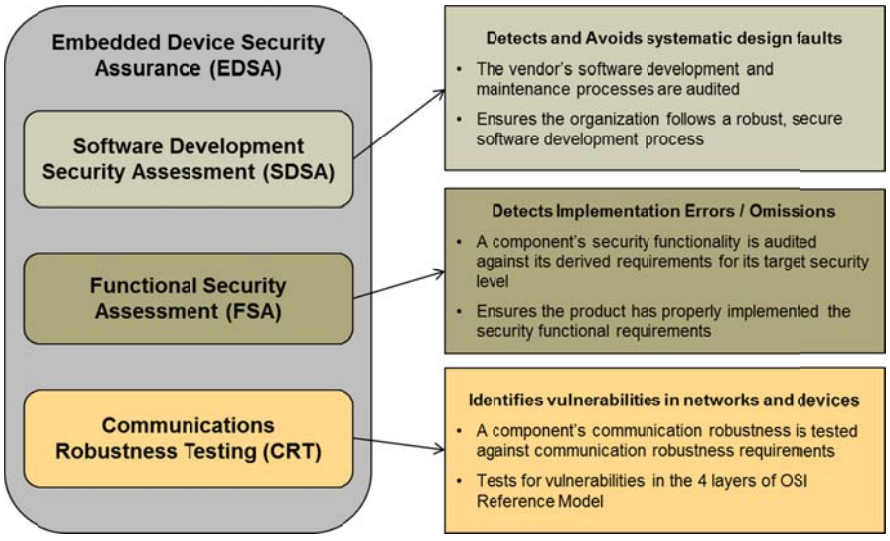

Figure 3 – EDSA Certification Program Elements

3.3 Systems Security Assurance (SSA)

The ISASecure® SSA is a certification program for Industrial Automation and Control Systems. The certification is to test and assess for compliance to the ISA-62443 standards. The primary focus of the SSA program is compliance to ISA-62443-3-3. The ISASecure® SSA certification program is currently under development and is expected to be released in the middle of 2013.

There are three elements to the ISASecure® SSA certification program

1. System Robustness Testing (SRT)
2. Functional Security Assessment (FSA)
3. Security Development Assessment (SDA)

SRT contains two elements. The first element of SRT is a scan of the system for known vulnerabilities. This scanning is done using commercial tools such as Nessus. The second element of SRT is to subject the devices in the system as well as the overall system to different forms of malicious network traffic. The malicious network traffic will consist of malformed network packets as defined in the ISASecure® Communications Robustness Test specification as well has abnormally high traffic rates of all forms of traffic. The system is expected to maintain essential functionality while being subjected to the SRT.

The FSA examines the security capabilities of the system and compliance to the ISA-62443-3-3 standard. The 62443-3-3 standard defines security controls and an associated security level for an implementation in a specific security zone as defined in ISA-62443-3-2. A security level is assessed for each zone in the system being assessed.

Finally, the SDA examines the process artifacts from the development process used in designing/creating the system. These artifacts are produced as the result of the development organization following the processes outlined in ISA-62443-4-1.

The program offers four certification levels for a zone of a system, offering increasing levels of system security assurance. The four levels are based on the Security Levels defined in ISA-62443-3-3.

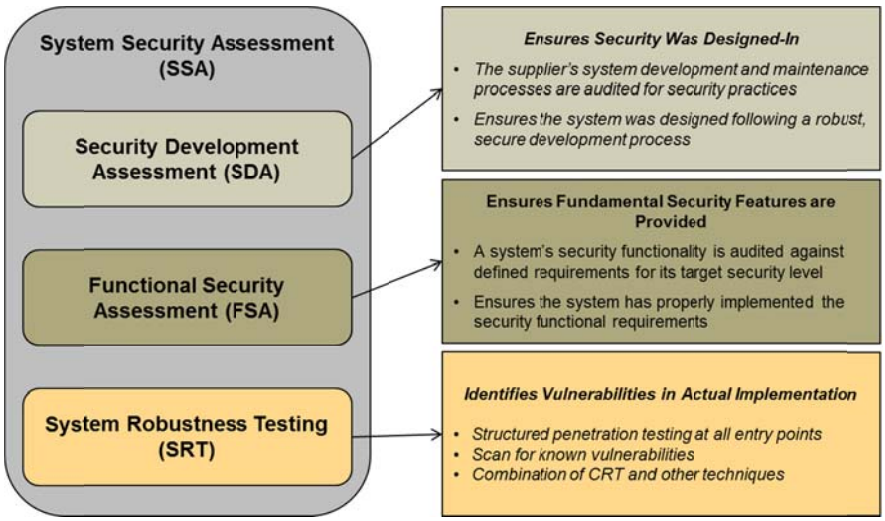

Figure 4 – SSA Certification Program Elements

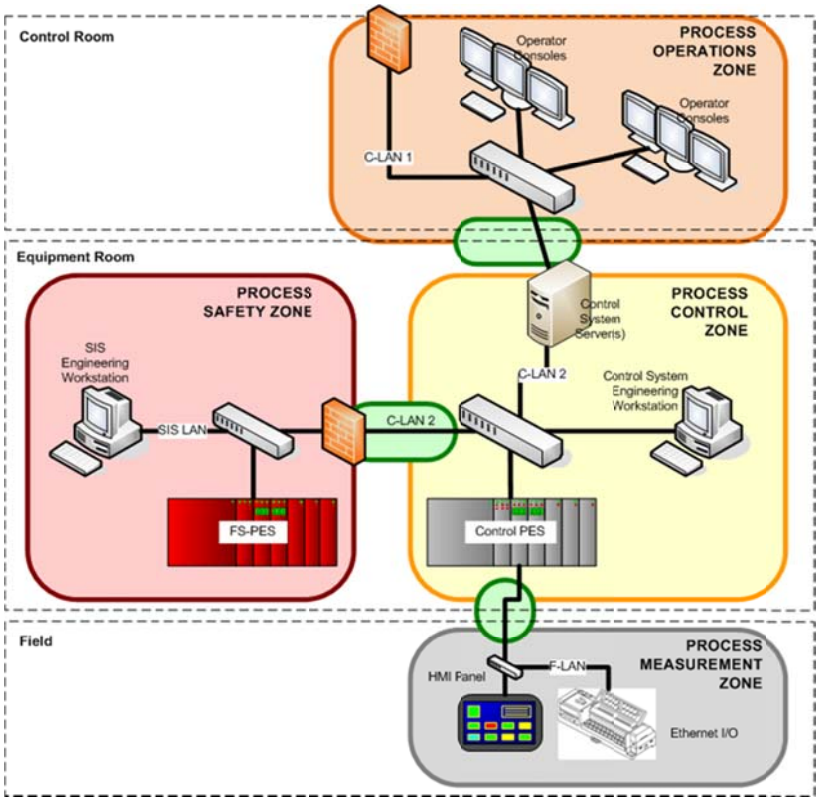

Figure 5 – Example of an Industrial Control System

4 Response to RFI Questions

ISASecure® certification programs are conformance schemes based on the ISA-62443 series of cross-sector industry standards for the Security of Industrial Automation and Control Systems. The ISA-62443 standards are developed by the ISA 99 committee. Please refer to the *ISA 99 Response to the NIST Cybersecurity Framework RFI* for comprehensive replies to the RFI questions. Please see below for responses to the Cybersecurity Framework RFI questions that are particularly relevant to the ISASecure® certification program.

4.1.1 What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

ISASecure certification programs are accredited as an ISO/IEC Guide 65 conformance scheme and ISO/IEC 17025 lab operations by ANSI/ACLASS.

ISASecure certification programs reference the ISA-62443 series of Industrial Automation and Control Systems security standards as the primary source for compliance requirements. For industrial safety systems, the ISASecure program references the IEC 61511 and IEC 61508 industry standards.

A full list of the industry standards referenced by ISASecure can be found at www.ISASecure.org.

4.1.2 What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Wherever possible the ISASecure certification program references international standards such as those from ISO and IEC.

The ISA-62443 standards are developed by the ISA 99 committee, which maintains a formal liaison with IEC TC65/WG10 and ISO/IEC JTC1/SC27. ISA-62443 standards are simultaneously submitted to the ISA committee and international bodies for approval. Please refer to the ISA 99 Cybersecurity Framework RFI submittal, section 5, for additional information.

ISASecure certification programs are also ANSI/ACLASS accredited, which provides international recognition for the products that are certified according to these programs.

67 Alexander Drive P.O. Box 12277 RTP, NC 27709
Phone 919-990-9222 Fax 919-549-8288