Frequently Asked Questions

The ISA99 committee and 62443 standards

Introduction

This document answers many of the most commonly posed questions about the ISA99 committee ("the committee") and its work in developing the ISA-62443 (IEC 62443) series of standards on the subject of Industrial Automation and Control Systems (IACS) cybersecurity. As additional questions are posed by stakeholders and other interested parties, they will be addressed here.

The committee provides this document to all interested parties as a means of improving our communications and outreach. All are encouraged to share this information widely and to suggest improvements or additions to its content. Feedback may be directed to the committee co-chairs at ISA99chair@gmail.com.

The questions are arranged into the following topics and sub-topics:

General

ISA

Q1: Who is ISA?

The International Society of Automation (ISA) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world.

ISA is accredited by The American National Standards Institute (ANSI) as a developer of U.S. National standards, many of which are also adopted internationally. These standards help automation professionals streamline processes and improve industry safety, efficiency, and profitability. Over 150 standards reflect the expertise of more than 4,000 industry experts around the world. Since 1949, ISA has been recognized as the expert source for automation and control systems consensus industry standards.[1]

More detailed information about ISA is available on the website.

Terminology and Nomenclature

Q2: The terminology associated with these standards can be confusing. Please explain the difference between ISA99 and ISA-62443.

ISA99 refers to the committee, which simply means that this is the ninety-ninth committee chartered by the ISA Standards and Practices Board. The ISA-62443 term refers to the standards produced or adopted by this committee. The number 62443 was adopted for the sake of harmonization with the nomenclature used by IEC (see Q3).

Q3: Please explain the conventions for naming and numbering the various 62443 standards.

The committee understands that some may find the nomenclature associated with the 62443 standards difficult to follow. Reducing this confusion starts with the understanding that for each of the documents in the series there will be both an ISA and an IEC edition. The former is given several the form “ISA-62443-x-y” and the latter are numbered “IEC 62443-x-y.” Once approved by ANSI the ISA designation becomes “ANSI/ISA-62443-x-y.”

The first few documents developed by the committee were released as ISA-99.xx.yy. After agreeing with IEC TC65 WG10 to co-develop the full range of IACS Security Standards, the numerical designation for the series of standards and technical reports was changed to 62443.

Each of these has a document number or designation of the form [ANSI/ISA-|IEC][TR] 62443-x-y, where:

- TR is an optional designation for technical reports only.
- “x” is a number from 1 to 4, indicating the categories.
- “y” is the number within a specific series.

[1] https://www.isa.org/standards-and-publications/isa-standards/

Q4: On the ISA website I see ISA-99.00.01, ISA-99.02.01, and other ISA99 documents for sale. Are these the same as ISA 62443-1-1, ISA 62443-2-1, etc. ?

In short, yes. The changes to the numbers of some of the earliest standards in the series (e.g., from ISA-99.00.01 to ISA-62443-1-1) were a consequence of the change in nomenclature adopted as part of the collaboration between ISA and IEC.

Q5: How were the 62443 standards developed, and by whom?

Most of the ISA/IEC 62443 series of standards are developed primarily by the ISA99 committee of the International Society of Automation, with contribution, review, and adoption by IEC TC65, a technical committee of the Geneva-based International Electrotechnical Commission. The 62443-2-4 standard was developed by IEC TC65 WG10 and ISA industry professionals and adopted by ISA as ANSI/ISA-62443-2-4. ISA99 draws on the input of cybersecurity experts across the globe in developing consensus standards that apply to all industry sectors and critical infrastructure, providing a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems.

The ISA99 Committee

Committee Management

Q6: How is the ISA99 committee managed?

The operating procedures of the ISA Standards and Practices Department require that each standards committee have a managing director and one or more chairs responsible for directing committee activities and reporting progress. Common practice is to have two co-chairs for each committee to allow for continuity if a single chairperson is not available.

The ISA99 committee has expanded this leadership model by creating a leaders' working group (Working Group 5) consisting of the co-chairs of each of the other working groups. This group meets regularly to report on and discuss the status of the committee, raise and address any issues, and direct committee activities. The notes from all meetings of this group are available on the committee portal. This group has also documented several common governance-related processes and guidelines for use by the committee.

As with other committees, ISA99 has several work and task groups, each with specific responsibilities and assigned work products.

Participation and Contributions

Q7: How can my company support the work of the committee?

As with membership in ISA, committee membership rests with an individual and not with the employer or a company. Employer support typically takes the form of allowing employee contribution. While it is possible for several people from the same company to be members of the committee, only one voting member per company is permitted.

Companies can also support the work products of the committee through a corporate membership in the ISA Global Cybersecurity Alliance (ISA GCA).

Q8: Do I have to be an ISA member to join the committee?

No. Anyone is welcome to join the committee and may contribute at any level that is most appropriate for their situation.

Q9: How can I join the committee?

Information about how to join the committee is available on the ISA website (https://www.isa.org/forms/join-a-standards-committee). Your email address will be added to the general committee mailing list and you will be given access to the committee collaboration portal. There is no commitment required and you are free to participate in committee activities at any level you feel is appropriate for your situation.

Q10: What are the requirements for contributing to the development of the 62443 standards?

There are no specific or formal requirements for assisting in the development of ISA standards. Committee members and contributors are assumed to have an interest in the work of the committee in question, as well as relevant expertise and experience. Contributions range from reviewing and commenting on draft documents to supplying content on specific topics.

Q11: Are there different classes or types of committee members?

The majority of those on the committee are information members who receive committee mailings may attend committee meetings, and may submit comments on drafts or other information when requested by the committee. Information membership is open to anyone with an interest in the work of the committee, without any specific obligations beyond the completion of a member information summary.

Voting members are nominated by the committee co-chairs in recognition of material contributions to the work of the committee and confirmed by existing voting members. Voting members are expected to participate at least three times during each calendar year or to contribute significantly to the work of the committee in some other way as recognized by the (co) Chairs, such as providing technical content to draft documents, Participation is defined as attending a significant portion of a meeting (or teleconference) of the committee. Voting members are also expected to return votes on all letter ballots submitted to the committee. They may still be an active voting member, even if they are unable to attend meetings, by contacting the Committee Chair and by consistently corresponding with the committee.

If a committee has multiple members from the same company, only one member may be voting; the others are information members. Of the information members, the committee must approve when one of the information members requests to be an alternate voting member. An alternate's vote is counted only if the principal representative fails to vote.

Q12: How does one become a voting member of the committee?

Any member may apply to become a voting member, subject to the restriction that there may be only one voting member from a given company. Such applications are first reviewed by the committee co-chairs and, if requirements are met, they are submitted as a ballot to the current voting members for approval. In general, voting privileges are granted based on the nature and level of the contributions from the applicant.

Relationships with external groups and organizations

Q13: Does ISA99 work with external groups or organizations and if so, how are these relationships managed?

The ISA99 committee has formal and informal liaison relationships with several other groups and organizations that have an interest or stake in industrial cybersecurity. Examples include:

- Various IEC committees (e.g., IEC TC65 WG10, IEC TC45)
- ISO JTC1 SC27
- ISA Global Cybersecurity Alliance (ISA GCA)
- The Industrial Internet Consortium (IIC)
- ISA84 committee on process safety
- ISA Security Compliance Institute (ISCI)
- National organizations, such as the National Institute of Standards and Technology (NIST) in the United States

Additional relationships may be formed as required by circumstances, where mutual benefits have been identified. Most of these relationships are described in the form of an informal relationship description maintained by the committee. All formal liaisons must be proposed to and approved by the Standards and Practices Board.

Relationship with IEC

Q14: Please describe the relationship between the ISA99 committee and IEC, and how this impacts the standards.

The principal formal point of contact with IEC is through a liaison in ANSI called the United States National Committee Advisory Group or USNC TAG. This is a group of liaisons representing the US interests by sitting on individual IEC standards committees (SC) or Working Groups (WG) or Technical Committees (TC). (Source, ANSI IEC USNC TAG Procedures USNC Technical Advisory Groups (ansi.org)

There is a working liaison relationship between the ISA99 committee and IEC Technical Committee 65 Working Group 10. Within the context of this relationship, there is an agreement that the majority of the standards and technical reports in the 62443 series are developed by the ISA99 committee and offered for consideration and approval by TC65 WG10 as IEC issued documents. To date, the only exception to this is the 62443-2-4 standard which was developed by IEC TC65 WG10 and adopted and approved by ISA as ANSI/ISA-62443-2-4.

Q15: How is the relationship managed?

ISA and IEC each have their respective processes for committee and group operation. ISA99 and IEC TC65 WG10 leaders hold regular meetings to coordinate plans and activities. Each group of leaders is then responsible for reporting developments to their respective committee members and other constituents.

The ISA99 committee leaders are preparing governance documents that describe in more detail how such relationships are monitored and managed.

Relationship with ISO

Q16: Please describe the relationship between the ISA99 committee and ISO, and how this impacts the standards.

The principal formal point of contact with ISO is through a liaison in ANSI called the United States Technical Advisory Group or USTAG. This is a group of liaisons representing the US interests by sitting on individual ISO standards committees (SC) or Working Groups (WG) or Technical Committees (TC). (source, ANSI ISO USTAG Procedures U.S. TAGs to ISO Committees (ansi.org)

Our principal point of contact with ISO is via the Joint Technical Committee 1 (ISO/IEC JTC1 SC27), which is the group responsible for the ISO-2700x standards. Our liaison relationship with that group provides the context in which we share draft documents and collect comments and feedback.

Q17: What is the relationship between the ISA99 committee and the ISA Security Compliance Institute (ISCI)?

The ISCI board includes a liaison representative from the ISA99 committee who is proposed to ISCI by the ISA99 committee co-chairs. Any nominee from the committee must be approved by the ISCI board. The ISA99 representative has voting rights on all matters brought before the ISCI governing board except on voting for the ISCI board chair and ISCI board vice-chair, and, on voting for approval of the ISCI annual budget.

Q18: What is the relationship between the ISA99 committee and the ISA Global Cybersecurity Alliance (ISA GCA)?

The objectives of the ISA Global Cybersecurity Alliance include the acceleration of adoption of standards, certification, education programs, advocacy efforts, and thought leadership related to industrial cybersecurity. The ISA GCA can provide funding for some of the activities related to, but not part of, the development of our standards. This could include promotion of the standards, or outreach to various stakeholders on adoption, application, etc. ISA GCA activities are coordinated with those of the ISA99 committee to ensure that our messages are consistent.

Standards Approval Processes

Q19: How are the 62443 standards approved for publication and release?

There are separate processes for the ISA and IEC versions of standards and other work products in the 62443 series. In the case of ISA, each standard is first submitted for review and approval by the voting members of the ISA99 committee. Once the standard has been approved by the committee voting members it is then submitted for review and approval by the ISA Standards and Practices Board of Directors. The details of the ISA voting procedures are available on the ISA website.

ANSI requires all Accredited Standard Developers ASD's to submit their drafted standards in a compatible IEC approved format to comply with a global standardization initiative. This allows an easier process for international adoption of standards developed by ANSI accredited developers such as ISA.

IEC has separate policies and procedures for approval of their standards. These are available on the IEC website.

Current Focus Areas

Q20: What are the current areas of focus for the committee?

The standards and technical reports that make up the series have been developed over more than fifteen years. With most of the major topics addressed, our focus has shifted to ensuring that the series is comprehensive and consistent across the various parts. Application of the standards across a broad set of industry sectors and suitability for IIoT are also significant considerations.

Q21: Can you please provide additional information about the "consistency group" in the ISA99 committee?

The consistency task group (WG5TG3) is responsible for reviewing the technical content of the series and making recommendations for improvement to quality, completeness, or consistency. Those recommendations are being used to guide the development of second editions of several parts of the series.

The 62443 Series of Standards

General

Q22: Can you please explain the categories in the 62443 series?

There are several categories of documents within the series, each with a specific focus and intended audience. These are shown in the following figure.

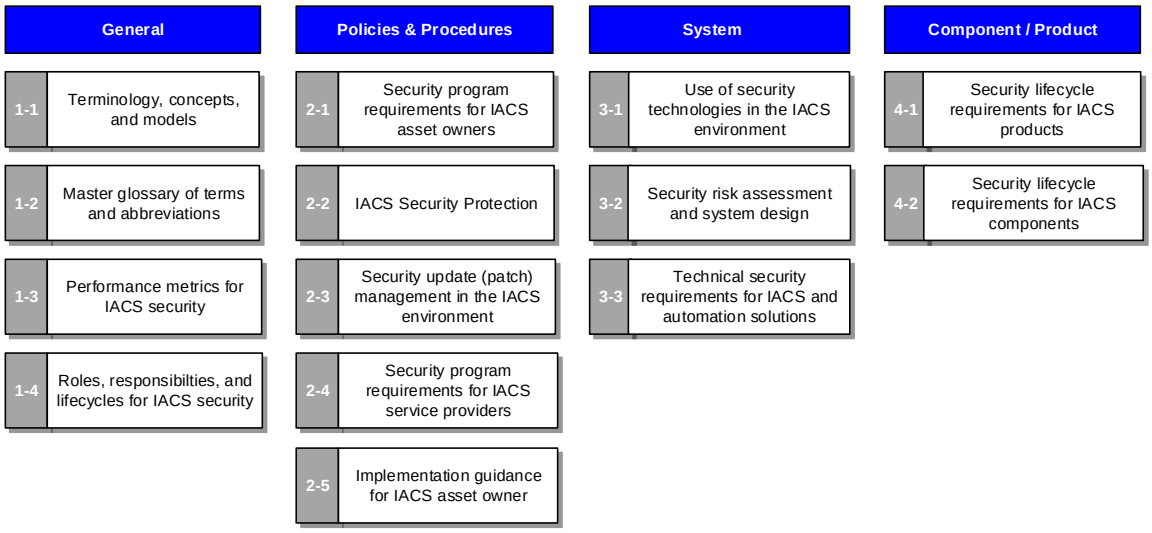

Figure 1 – 62443 Document Categories

- The first category (General) offers standards and technical reports containing general information about the subject. This includes an introduction to concepts and models and the master glossary.
- Documents in the second category (Policies and Procedures) are directed primarily at the asset owner or end-user and address what is required for an effective cybersecurity program
- The third category (System) includes documents that provide technical requirements for systems. The intended audience includes systems integrators, asset owners, and service providers.

- The fourth category (Component/Product) includes documents that provide technical requirements for individual products or components. The primary intended audience is product suppliers.

Q23: Please describe the purpose and intended use of each of the standards in the 62443 series.

The organization of the documents in the 62443 series is shown in Figure 1 (above).

- **62443-1-1** introduces the terminology, 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.
- **62443-1-3** helps asset owner organizations improve their risk posture by providing a methodology for the development of quantitative metrics that can be implemented for a wide range of IACS.
- **62443-1-4** provides a more detailed description of the underlying life cycle for IACS security.
- **62443-2-1** describes what is required to define and implement an IACS cybersecurity management system. The intended audience includes end-users and asset owners who have responsibility for the design and implementation of such a program.
- **62443-2-2** provides guidance on the development and validation of security measures to protect an IACS against cyber-security threats.
- **62443-2-3** provides guidance on developing a patch management program for IACS. The intended audience includes anyone who has responsibility for the design and implementation of patch management processes and procedures.
- **62443-2-4** specifies requirements for suppliers of IACS systems and related components. The principal audience includes suppliers of control systems solutions. This standard was developed by IEC TC65 WG10.
- **62443-2-5** (planned) will provide guidance on what is required to operate an effective IACS cybersecurity management system. The intended audience includes end-users and asset owners who have responsibility for the operation of such a program.
- **62443-3-1** describes the application of various security technologies to an IACS environment. The intended audience includes anyone who wishes to learn more about the applicability of specific technologies in a control systems environment.
- **62443-3-2** addresses security risk assessment and system design for IACS. This standard is primarily directed at asset owners or end-users.
- **62443-3-3** provides the foundations for assessing the security levels provided by an automation system. The principal audience includes suppliers of control systems, system integrators, and asset owners.
- **62443-4-1** describes the derived requirements that apply to the development of products. The principal audience include suppliers of control systems products and components included in control systems solutions.
- **62443-4-2** contains sets of derived requirements that provide a detailed mapping of the system requirements to subsystems and components of the system under consideration. The principal audience include suppliers of components embedded in control systems solutions.

Q24: What is the status of each of the standards in the 62443 series? Which ones are available?

Most of the standards in the series have been completed, with several being revised to prepare second or subsequent editions. In some cases, there may be small differences in the state of the corresponding IEC version.

Since this information can change rapidly and without notice, please direct inquiries about the status of standards to the committee co-chairs at ISA99Chair@gmail.com.

Q25: Are the IEC and ISA editions of 62443 standards identical?

For a given standard in the series, the technical content of the ISA and IEC is identical. Differences between the two versions are limited to front matter and other supporting information.

Q26: Have the 62443 standards been translated to other languages?

The IEC versions of the standards are translated to French as part of the formal release process. IEC national committees may translate the IEC version into local language with permission from IEC. In the case of the ANSI/ISA versions, ISA does not have the resources to provide translations. However, there have been past initiatives to translate selected standards into local languages.

Q27: Is it permissible for me to translate a standard on my own and offer it to my colleagues?

Published standards are protected by copyright and should not be copied or distributed to others without permission. Those wishing to translate them into other languages should contact the copyright holder (i.e., ISA or IEC) for more information about appropriate use.

Q28: IEC and others (e.g., WIB) is writing all of the 62443 series parts, why are they labeled ISA-62443?

The premise for this question is incorrect. As explained above, only the 62443-2-4 standard was developed outside of the ISA99 committee. In that specific case, the standard was created using report M 2784 X10 from the process automation users' association in the Netherlands (WIB)[2] as the primary source. All other standards and reports in the 62443 series have been developed by the ISA99 committee and submitted simultaneously for approval to both ISA and IEC.

Q29: How do I obtain copies of the standards?

ISA versions can be purchased from ISA or IHS, while IEC versions can be purchased from IEC and affiliate national organizations. A benefit of ISA membership is the ability to view society's standards for free.

Q30: How do the 62443 standards compare to other standards in this area?

Many of the other available standards focus on specific sectors, regions, or constituencies. For example, the NERC CIP standards were developed by and for the bulk electrical sector in North America. Although commonly referred to as standards, the NIST SP800-53 and SP800-82 documents are special publications, primarily developed as guidance for U.S. federal systems. The 62443 series is the most comprehensive set of standards, developed using an open, consensus-based process, that applies across sectors and addresses the entire security life cycle.

The NERC, NIST, and other documents all contain information that is useful beyond their intended application. Perhaps most important, the guidance in all these documents is largely consistent.

[2] https://www.wib.nl/

Application

Q31: How do I apply the 62443 standards?

A detailed answer to this question is beyond the scope of this document.

The best approach depends to a great degree on the role of the organization, the nature of the targeted application, and the maturity level of the organization. The standards describe a methodically engineered approach to addressing the cybersecurity of automated systems. They provide requirements for all the principal roles across the system life cycle, from product definition and development through integration, installation, operation, and support.

The first step in applying the guidance contained in the standards is to achieve awareness of what it means to secure a control system through focused training. This allows for the selection of the most appropriate standards in the series for a given situation.

In all cases, begin with the concepts and models that form the basis of the series, as well as a description of the life cycle and guidance as to which standards apply at each stage as well as the intended audience.

There are several resources (e.g., whitepapers and training) to assist the asset owner in understanding the many issues and risks to be considered when starting the process of applying cybersecurity to any automation system.

Q32: Are the 62443 standards focused exclusively on, or limited to, application in the process industries?

Although the 62443 standards were originally conceived with process industries such as chemical processing and petroleum refining as the primary focus, this was simply a reflection of the initial makeup of the committee. Their application is not limited to this scope. This is due to the concepts applied within 62443 that are modified to address the specific differences in requirements between information security and control systems security which must be considered. They have also been referenced or applied in other industries, including but not limited to, building automation, transportation, and medical systems. The committee expects this trend to continue as people see that the principles, fundamental concepts, and foundational requirements at the base of the series apply equally well in other industries.

Q33: Can you provide examples of the application of the 62443 standards in the industry?

Product suppliers (system products or components) are adopting specific standards in the series such as 62443-3-3, 62443-4-1, and 62443-4-2 to improve their development processes and the security of their products.

The 62443 standards have been broadly accepted by major asset owners in the several industries (e.g., chemical, oil & gas, transportation, etc.). The committee expects this trend to continue as people see that the principles, fundamental concepts, and foundational requirements at the base of the series apply equally well in other industries.

The United Nations Economic Commission for Europe expressed interest in integrating the ISA/IEC 62443 series of standards into its forthcoming Common Regulatory Framework on Cybersecurity (CRF), which is to serve as an official UN policy position statement for Europe. At a meeting in Geneva, UNECE's Working Party on Regulatory Cooperation and Standardization Policies recognized the ISA99 committee for its leading role in conceiving and developing the standards, while formally accepting review input submitted by industry experts.

Q34: Please clarify the positioning of 62443 as a "horizontal standard?"

The term "horizontal" is used within IEC to describe a standard that can be applied across a range of industries, sectors, or application spaces. The IEC standards Management Board (SMB) has recently approved 62443 for this designation.

Within the ISA portfolio of standards, the 62443 series has been considered the equivalent of horizontal since the formation of the ISA99 committee.

Fundamental Concepts

Q35: What exactly are the "fundamental concepts" that we hear about concerning the 62443 standards?

Fundamental concepts are elements of accepted and proven industry good practices that have been carefully adapted to address the special and unique circumstances security in control systems must consider, such as risks of economic loss, environmental damage to personnel injury and death, and continuous compliance with the physics associated with distributed control of physical objects and processes such as causality of effects of cyber and physical events occurring in physical processes. Information security typically does not have those types of risks to the extent presented in IACS environments.

Foundational Requirements

Q36: Please describe the idea behind "foundational requirements."

Early in the process of developing the standards, the committee identified a short list of foundational requirements that addressed the main technical elements of an effective security response. These are:

1. Identification and authentication control (IAC)
2. Use control (UC)
3. System integrity (SI)
4. Data confidentiality (DC)
5. Restricted data flow (RDF)
6. Timely response to events (TRE)
7. Resource availability (RA)

They were introduced in the 62443-1-1 standard and then used as the starting point for developing the system-level technical requirements appearing in 62443-3-3. Subsequent standards in the series have also used this list to develop detailed requirements in areas ranging from patch management to system and component development. We intend to be able to demonstrate traceability from each of the more detailed requirements in the series back to one or more of the foundational requirements.

Foundational requirements take accepted cybersecurity practices and interpret them to fit effectively into a control system design, applying a secure development life cycle process. Applying the foundational requirements as detailed in the various parts of 62443 guides the user through the complexities involved in mitigating risks inherent in control systems.

Compliance and Certification

Q37: What is the value of certification?

The perceived value of certification should take into consideration a variety of factors, beginning with the source of the requirements (i.e., the 62443 standards) as well as the specific interpretation (e.g., are all requirements cited or only an applicable subset) and the reputation of the certifying body.

Q38: What are the standards of ISA 62443 that can give rise to certification?

In general, any of the 62443 standards that contain testable normative requirements can form the basis for certification. Organizations (e.g., ISASecure™) that develop conformance specifications choose the standards of interest.

Q39: What are the routes that can be followed to obtain these certifications?

The first step is to identify the conformance testing organization. There are several choices, including those documented on the ISASecure™ web site. These organizations may use conformance specifications such as those developed by ISASecure, or they may "self-certify" using internally developed criteria based on their interpretation of the standards.

Q40: What are ISCI, ISASecure™, and their relationship?

The ISA Security Compliance Institute[3] (ISCI), a not-for-profit automation controls industry consortium, manages the ISASecure™ conformance certification program which is based upon the IAC security lifecycle as defined in the 62443 standards. The scope of the ISASecure certifications includes assessment of off-the-shelf industrial automation products and product development security lifecycle practices. 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 specifications are available for use by independent laboratories and certification bodies. The ISASecure™ designation is earned by industrial control suppliers for products or systems that demonstrate adherence to industry consensus cybersecurity specifications for security characteristics and supplier development practices.

More information–including details on what standards are addressed by certification–is available on the ISASecure website. Comments or questions may be submitted via this form.

Q41: What is the relationship between ISASecure and ISA99 committee?

Although both the ISA99 committee and ISCI are part of ISA, they have different purposes and operate independently. ISCI is managed by a Board consisting of representatives of sponsoring companies while the committee is an entirely volunteer effort. The ISCI Board also includes a single position for a leader from the committee to coordinate standards development and certification definition activities.

[3] https://www.isasecure.org/en-US/

Q42: Is ISASecure the only option for certification?

No, other organizations have also addressed the need for conformance to the 62443 standards.

The IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components[4] (IECEE) provides a framework for assessments in accordance with the IEC 62443 Security for industrial automation and control systems series of standards to result in an IECEE Certificate of Conformity–Industrial Cybersecurity Capability. The program specifies several different certifications related to 62443 as well as the related certificate structure and the applicable "test report forms." Complying certification bodies can publicly register at IECEE separately for parts of IEC 62443. Some companies are also providing independent certification based on their interpretation of specific standards in the 62443 series.

Technology Trends and Developments

Industrial Internet of Things (IIoT)

Q43: Do the 62443 standards address the security needs and issues related to the Industrial Internet of Things (IIoT)?

The requirements in the standards are not implementation-specific and for the most part, should apply in situations where internet-connected devices are used with the control system. The committee has chartered a working group (WG9) to identify security-related implications associated with the use of these technologies. The findings of this working group will be used to identify any additions or modifications that may be required in future editions of the standards.

More Information

The standards

Q44: Where can I get more information or training on the 62443 standards?

The primary focus of the ISA99 committee is on the development of the standards and technical reports in the 62443 series. However, during development, the committee has also developed a body of supporting information that introduces the standards and explains the basic concepts (including this FAQ). In addition, there is a growing collection of articles, whitepapers, etc. from other sources addressing the subject.

Professional training and associated certificates are available from ISA using materials developed by many of the original authors of the standards. Visit the website [https://www.isa.org/training-certifications/isa-training] for more information.

Other individuals and companies, including ISA local sections, have also developed training courses on related subjects, referencing many of the concepts contained in the 62443 series.

The committee

Q45: Where can I get more information about the committee and the status of the various standards?

The easiest way to get information about current activities is to join the committee (ISA membership is not required). Committee members have access to an extensive body of information that is maintained on a collaboration portal. This includes historical information stretching back to the earliest days of the committee.

[4] https://www.iecee.org/

Other Standards

Q46: Are there other international standards that are related to 62443?

There are many other standards and practices that address aspects of operational cybersecurity. Some are industry-specific; some are national, and others are international. There are also standards in other areas of automation such as safety, communications, networking, and control systems design that have some level of dependency on effective cybersecurity. The number of available standards presents a challenge to those looking for appropriate guidance in this area.

The ISA99 committee and others developing the 62443 standards are committed to working closely with those responsible for other related standards to coordinate content and avoid duplication or inconsistency. For example, the 62443 standards build upon, rather than duplicate, the relevant guidance, and direction contained in the ISO/IEC 27000 series of standards on information security. The committee also has liaison relationships with organizations and committees such as the Industrial Internet Consortium (IIC) and the standards committee (ISO/IEC JTC 1/SC 27) responsible for the ISO/IEC 27000 standards.

Q47: Is the ISA99 committee aware of the UL 2900 series of standards? If so, how do they compare to the 62443 standards?

UL 2900 is a series of standards published by UL (formerly Underwriters Laboratories), a global safety consulting and certification company. The UL 2900 series of standards were developed as part of UL's Cybersecurity Assurance Program which provides manufacturers testable and measurable criteria to assess product weaknesses and to determine vulnerabilities and security risk controls. The first standard in this series is ANSI/UL 2900-1 which describes the general requirements for the cybersecurity of network connectable products. Other standards in the series provide more detailed requirements for specific applications. For example, ANSI/UL 2900-2-1 addresses healthcare systems.

Both UL and ISA are ANSI-accredited standards development organizations (SDO's).

NIST Framework

Q48: What is the relationship between the 62443 standards and the NIST cybersecurity framework (CSF)?

The National Institute of Standards and Technology (NIST) is a United States government agency that has been tasked by Congress to identify and develop cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators.

The NIST Cybersecurity Framework (CSF)[5] is voluntary guidance, based on existing standards, guidelines, and practices to assist organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

The framework core is a listing of functions, categories, subcategories, and informative references that describe specific cybersecurity activities that are common across all critical infrastructure sectors. This list includes several parts of the 62443 series.

[5] https://www.nist.gov/cyberframework

There has been a longstanding relationship between the ISA99 committee and NIST to ensure that the guidance and direction in the 62443 standards and the NIST special publications and framework remain consistent.

Standards and Regulations

Q49: I am regulated by NERC-CIP or some other regulatory agency (e.g., TSA, CFR, etc.) Am I required to follow ISA/IEC 62443?

Certain parts of NERC-CIP reference ANSI/ISA-62443 as good practice standards to be applied as guidance. If your organization is required to follow NERC-CIP for your control system cybersecurity, then ANSI/ISA-62443 is a good place to find the guidance to deploy the type of security NERC-CIP requires.

UPDATE 2021 TSA Pipeline Security Guideline of March 2018 reference ANSI/ISA-99.00.01 and ANSI/ISA-99.02.01 in section 7.4.

Always consider if a regulation (e.g., NERC, FERC, NRC, TSA) references standards as part of compliance with the regulation, as those may imply following the standard as part of the regulation. Another important side of the requirement question is customer specification. When the contract specifies compliance with the standard as part of the procurement language, it becomes a requirement whether it is regulatory or not.

Developing and promulgating technically sound consensus standards and recommended practices is one of ISA's primary goals. To achieve this goal the Standards and Practices Department relies on the technical expertise and efforts of volunteer committee members, chairmen, and reviewers. ISA is an American National Standards Institute (ANSI) accredited organization. ISA administers United States Technical Advisory Groups (USTAGs) and provides administrative support for International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) committees that develop process measurement and control standards. To obtain additional information on the Society's standards program, please write:

ISA
Attn: Standards Department
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

