ACSSA-101

ISA Security Compliance Institute – Automation and Control System Security Assurance –

Evaluation planning for the asset owner

Version 1.1

January 2026

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the SPECIFICATION.

Without limiting the foregoing, ASCI disclaims all liability for harm to persons or property, and users of this SPECIFICATION assume all risks of such harm.

In issuing and making the SPECIFICATION available, ASCI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASCI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this SPECIFICATION should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

To the maximum extent permitted by applicable law, in no event shall ASCI or its suppliers be liable for any special, incidental, punitive, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the SPECIFICATION, the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION, or otherwise under or in connection with any provision of this SPECIFICATION, even in the event of the fault, tort (including negligence), misrepresentation, strict liability, breach of contract of ASCI or any supplier, and even if ASCI or any supplier has been advised of the possibility of such damages.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

Revision history

version	date	changes
1.1	26.01.12	Initial version available at https://ISASecure.org

Contents

Figures

Tables

FOREWORD

This is one of a series of documents that defines ISASecure® programs that evaluate the conformity of industrial automation and control systems (IACS) to the ANSI/ISA/IEC 62443 standard. These programs are developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This document is intended to assist the asset owner in understanding the ACSSA conformity assessment scheme and preparing for an ACSSA evaluation (inspection or certification).The ACSSA conformity assessment scheme is based on ISA/IEC 62443 standards that are relevant to the asset owner and an installed and operating IACS. ISCI also offers programs that evaluate ISA/IEC 62443 conformity for control system products and product suppliers. Further information for all ISASecure® conformity assessment programs can be found on the web site https://ISASecure.org.

Executive Summary

The ISASecure® Automation and Control System Security Assurance (ACSSA) program is a conformity assessment scheme for asset owners that is based on relevant parts of *ISA/IEC 62443 Security for Industrial Automation and Control Systems (IACS)*. The ACSSA program has two options: an inspection, or a certification.

The scope of an ACSSA evaluation includes the following:

- An IACS that is in-operation or operations-ready
- A Security Program (SP) that documents the security policies and procedures for the IACS
- The roles, responsibilities and training for the personnel that interact with the IACS
- The service providers that are responsible for IACS maintenance, integration or other services

The primary audience for this document is the asset owner. The intent is to assist the asset owner in understanding the ACSSA conformity assessment program, determining the scope of an ACSSA evaluation (inspection or certification), and preparing for an ACSSA evaluation. By following the guidance in this document, the asset owner will be prepared to engage with an Inspection Body (IB) or a Certification Body (CB).

This document answers the following questions about the ACSSA conformity assessment program:

- What is the scope of an ACSSA evaluation (Section 2)
- Which ISA/IEC 62443 standards are used in an ACSSA evaluation, and what are the basic concepts included in these standards? (Section 4)
- Is there an overview of the ACSSA conformity assessment program (Section 5)
- What are the key policies, procedures and artifacts that are needed for a successful inspection or certification outcome? (Section 6)
- What are the typical expectations and activities of an ACSSA evaluation? (Section 7)
- How does an asset owner apply for an ACSSA evaluation? (Section 8 and Annex A)

In order to obtain useful results from an ACSSA evaluation, an asset owner should have in place the basic elements required under the ISA/IEC 62443 standards which are:

- An SP which documents the security policies and procedures for the IACS
- Documentation of the partitioning of the IACS into individual security zones and conduits
- Security risk assessments that document the risk, target security level, and security measures for each security zone and conduit
- An up-to-date asset inventory of the systems and components that are included in the IACS
- The proper configuration and utilization of the IACS technical security capabilities
- A list of the service providers that have a documented agreement to perform maintenance, integration, or other services for the asset owner
- An incident management program for the IACS

For a complete list of ACSSA requirements, refer to *ACSSA-300 Inspection and certification* requirements, and *ACSSA-311 Evaluation methods*

1 Introduction

The ISASecure® Automation and Control System Security Assurance (ACSSA) program is a conformity assessment scheme for the asset owner that is based on relevant parts of ISA/IEC 62443 Security for Industrial Automation and Control Systems (IACS).

A recent report[1] by the Control System Cyber Security Association International (CS2AI.org) showed that ISA/IEC 62443 was the most frequently used standard for OT compliance activities. Furthermore, the report goes on to say “The prominence of ISA/IEC 62443 underscores its role as a cornerstone in the cybersecurity strategy for industrial control systems (ICS) and OT networks. Its comprehensive coverage of cybersecurity principles, from system design to operations and maintenance, makes it a critical framework for organizations looking to safeguard their operational technologies against cyber threats.” [B.4.1.3]

The ACSSA program has two options: an inspection, or a certification. An inspection is performed by an Inspection Body (IB), and a certification is performed by a Certification Body (CB). The same evaluation methodology for an IACS is used for an inspection or a certification. The requirements for this evaluation methodology are documented in *ACSSA-311 Evaluation Methods* and *ACSSA-300 Inspection and certification requirements*.

The primary objective of this document is to help the asset owner understand the key concepts in the ISA/IEC 62443 standards and the ISASecure® ACSSA conformity assessment program in order to prepare for engagement with an Inspection Body or a Certification Body.

This document has the following sections:

- Section 2 – describes the scope of the ISASecure® ACSSA conformity assessment program
- Section 3 – reproduces some key terms and definitions from the ISA/IEC 62443 standards and ACSSA-300
- Section 4 – describes some key concepts from the ISA/IEC 62443 standards needed to understand ACSSA
- Section 5 – provides an overview of the ACSSA conformity assessment program
- Section 6 – lists some key policies, procedures and artifacts that are needed to achieve a successful outcome
- Section 7 – discusses the expectations and activities associated with an ACSSA evaluation
- Section 8 – describes how to apply for an ACSSA evaluation
- Annex A – provides a template that can be used to define the scope of an ACSSA evaluation
- Annex B – provides a list of references used in this document

[1] CS2AI *2024 OT Technology Cyber Security Report*, page 22. https://www.cs2ai.org/annual-reports [B.4.1.3]

2 Scope

The scope of an ACSSA conformity assessment is defined by the following [ACSSA-300 4.1]:

- a named organization that fills the role of *asset owner* for the IACS
- specified hardware and software for the IACS, defined in an asset inventory under change control
- IACS *security zones* that are in-operation or operations-ready, where the latter is defined as commissioning is complete, security program documentation is complete and training of personnel that interact with the IACS is complete
- specified *equipment under control* (EUC) that is being controlled by IACS, identified individually by type and location of this equipment, in a named list under change control
- a list of *service providers* internal or external to the asset owner organization that perform integration or maintenance tasks for the IACS
- a named *Security Program (SP)* for the IACS that documents the security policies and procedures and is under change control
- The roles, responsibilities and training for the personnel that interact with the IACS

The following ISA/IEC 62443 standards are in the scope of the ACSSA conformity assessment program:

- ISA/IEC 62443-2-1 Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners [B.2.1.3, B.2.1.4]
- IEC 62443-2-4 Security for industrial automation and control systems Part 2-4: Security Program requirements for IACS service providers [B.2.1.5]
- ISA/IEC 62443-3-2 Security for industrial automation and control systems Part 3-2: Security risk assessment for system design [B.2.1.6, B.2.1.7]
- ISA/IEC 62443-3-3 Security for industrial automation and control systems Part 3-3: System security requirements and security levels [B.2.1.8, B.2.1.9]

There are two options available for the ACSSA conformity assessment program [ACSSA-100 4.0]:

- An *Inspection* is performed by an *Inspection Body* and determines conformity to the individual requirements in the ISA/IEC 62443 standards listed above. The deliverable from an Inspection is an Inspection Report. [ACSSA-100 4.2, 4.4]
- A *Certification* is performed by a *Certification Body* and attests conformity to the ISA/IEC 62443 standards listed above. The deliverables from a Certification are an Inspection Report and a Certificate [ACSSA-100 4.2, 4.5]

3 Terms and definitions

Terms and definitions are documented in ACSSA-300 and ISA/IEC 62443 standards. Some terms and definitions are duplicated here for the convenience of the reader.

3.1 ISA/IEC 62443 definitions

3.1.1
asset owner
organizational role ultimately accountable for one or more IACS

NOTE 1 Used in place of the generic word end user to provide differentiation.

NOTE 2 In the context of this document [62443-2-1], asset owner also includes the operator of the IACS.

[SOURCE: 62443-2-1:2024]

3.1.2
industrial automation and control system (IACS)
collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation

[SOURCE: 62443-2-4:2023]

3.1.3
maturity level (ML)
qualitative method of characterizing the capability of an organization to implement security requirements according to documented policies and procedures and their historical performance in doing so

[SOURCE: 62443-2-1:2024]

3.1.4
product supplier
organizational role responsible for the manufacture and support of IACS hardware and/or software products

NOTE This term is used in place of the generic word “vendor” to provide differentiation.

[SOURCE: 62443-2-1: 2024]

3.1.5
security level (SL)
measure of confidence that the system under consideration, security zone or conduit is free from vulnerabilities and functions in the intended manner

NOTE The ISA/IEC 62443 standards define four security levels which represent characteristics of threat actors against whom a system is to defend, and are assigned to security capabilities that can be selected to defend against attackers with those characteristics.

[SOURCE: 62443-3-2:2020]

3.1.6
security program (SP)
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures and products that are applicable to the IACS

NOTE 1 The SP [security program] for IACS asset owners refers to the policies and procedures defined by them to address cybersecurity concerns of the IACS. This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.

NOTE 2 For ACSSA, an asset owner typically has one security program for an IACS. However, they can have more than one, where different security programs address different parts of the IACS.

[SOURCE: 62443-2-1:2024, NOTE 2 added]

3.1.7
security zone

grouping of logical or physical assets that share common security requirements

NOTE 1 A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

NOTE 2 This definition and NOTE 1 are from 62443-3-3. A security zone configuration is part of the evidence submitted by applicants for ISASecure® ACSSA certification, as required by the ACSSA specifications.

[SOURCE: 62443-3-3:2013]

3.1.8
service provider

role of an organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner

NOTE This term is used in place of the generic word "vendor" to provide differentiation.

[SOURCE: 62443-2-4:2023]

3.2 Conformity assessment definitions

3.2.1
accreditation
third party attestation related to a conformity assessment body, conveying formal demonstration of its competence, impartiality, and consistent operation in performing specific conformity assessment activities

[SOURCE: ISO/IEC 17000:2020]

3.2.2
accreditation body (AB)
authoritative body that performs accreditation

[SOURCE: ISO/IEC 17000:2020]

3.2.3
certificate
document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program

NOTE For ISASecure® ACSSA, there are certificates for certified IACS, inspection bodies, and certification bodies.

3.2.4
certification
third party attestation related to an object of conformity assessment, with the exception of accreditation

NOTE Here, this refers to either a successful authorized evaluation of a product or a process to ISASecure® criteria. This outcome permits the product supplier or organization performing the process to advertise this achievement in accordance with certification program guidelines. In the context of ACSSA, the operation of an IACS is viewed as a process that the asset owner performs.

[SOURCE: ISO/IEC 17000:2020]

3.2.5
certification body (CB)
third-party conformity assessment body operating certification schemes

NOTE 1 A certification body can be non-governmental or governmental (with or without regulatory authority).

NOTE 2 For ACSSA, this term is used to refer to organizations accredited for the ACSSA certification scheme.

[SOURCE: ISO/IEC 17065:2012]

3.2.6
certification scheme
overall definition of and process for operating a certification program

3.2.7
conformity assessment
demonstration that specified requirements are fulfilled

[SOURCE: ISO/IEC 17000:2020]

3.2.8
conformity assessment body (CAB)
body that performs conformity assessment activities, excluding accreditation

NOTE For ACSSA certification programs, a conformity assessment body may be an inspection body, a certification body, or both.

[SOURCE: ISO/IEC 17000:2020]

3.2.9
conformity assessment scheme
conformity assessment program

set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment

[SOURCE: ISO/IEC 17000:2020]

3.2.10
inspection
examination of a product (3.2), process (3.3), service (3.4) [section references from ISO/IEC 17020], or installation or their design and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements

NOTE 1 Inspection of processes can include personnel, facilities, technology or methodology.

NOTE 2 Inspection procedures or schemes can restrict inspection to examination only.

NOTE 3 Adapted from ISO/IEC 17000:2004, definition 4.3.

NOTE 4 The term “item” is used in this International Standard to encompass product, process, service, or installation, as appropriate.

[SOURCE: ISO/IEC 17020:2012]

3.2.11
inspection body (IB)
body that performs inspection

NOTE 1 An inspection body can be an organization, or part of an organization.

NOTE 2 For ACSSA, this term is used to refer to organizations accredited for the ACSSA inspection scheme.

[SOURCE: ISO/IEC 17020:2012]

4 Basic 62443 Concepts

This section describes several basic concepts from the ISA/IEC 62443 standards that are needed to understand the ACSSA program. For a full overview of the ISA/IEC 62443 standards you can read *ISAGCA Quick Start Guide: An Overview of ISA/IEC 62443 Standards.* [B.4.1.1]

4.1 ISA/IEC 62443 Standards

The ISA/IEC 62443 standards was developed by two standards development organizations: the International Society of Automation (ISA) Standards Committee 99, and the International Electrotechnical Commission (IEC) Technical Committee 65 Working Group 10. These standards development organizations worked together to ensure that the content in the ISA labeled document is the same as the IEC labeled document.

The scope of an ACSSA conformity assessment program is an IACS that has been installed and is in-operation or operations-ready. Therefore, the following ISA/IEC 62443 standards form the basis for the ACSSA conformity assessment program:

- *ISA/IEC 62443-2-1 Security program requirements for IACS asset owners* specifies the requirements for policies and procedures to secure an IACS. The intended audience includes asset owners who have responsibility for the design and implementation of such a program. [B.2.1.3, B.2.1.4]
- *IEC 62443-2-4 Security Program requirements for IACS service providers* specifies requirements for IACS services such as system integration or system maintenance that has been delegated by the asset owner to a service provider. [B.2.1.5]
- *ISA/IEC 62443-3-2 Security risk assessment for system design* addresses cybersecurity risk assessment and system design for an IACS. The output of processes that follow this standard are a security risk assessment, a security zone and conduit model, and Target Security Levels for each security zone and conduit. These are documented in the Cybersecurity Requirements Specification. [B.2.1.6, B.2.1.7]
- *ISA/IEC 62443-3-3 System security requirements and security levels* specifies the technical requirements for an IACS system based on security level. The principal audience includes suppliers of control systems, system integrators and asset owners. [B.2.1.8, B.2.1.9]

4.2 Industrial Automation and Control System (IACS)

An Industrial Automation and Control System (IACS) is defined as the collection of personnel, hardware, software, policies and procedures involved in the operation of Equipment Under Control and that can influence safe, secure and reliable operation. Examples of IACS include Distributed Control Systems, Industrial Control Systems, Supervisory Control and Data Acquisition Systems, and Safety Instrumented Systems.

The term “Industrial” should be interpreted in its broadest sense; many sectors such as buildings, food and beverage, manufacturing, pharmaceuticals, process industries, transportation, and water and wastewater have all used the ISA/IEC 62443 standards to reduce the cybersecurity risk of their automation and control systems.

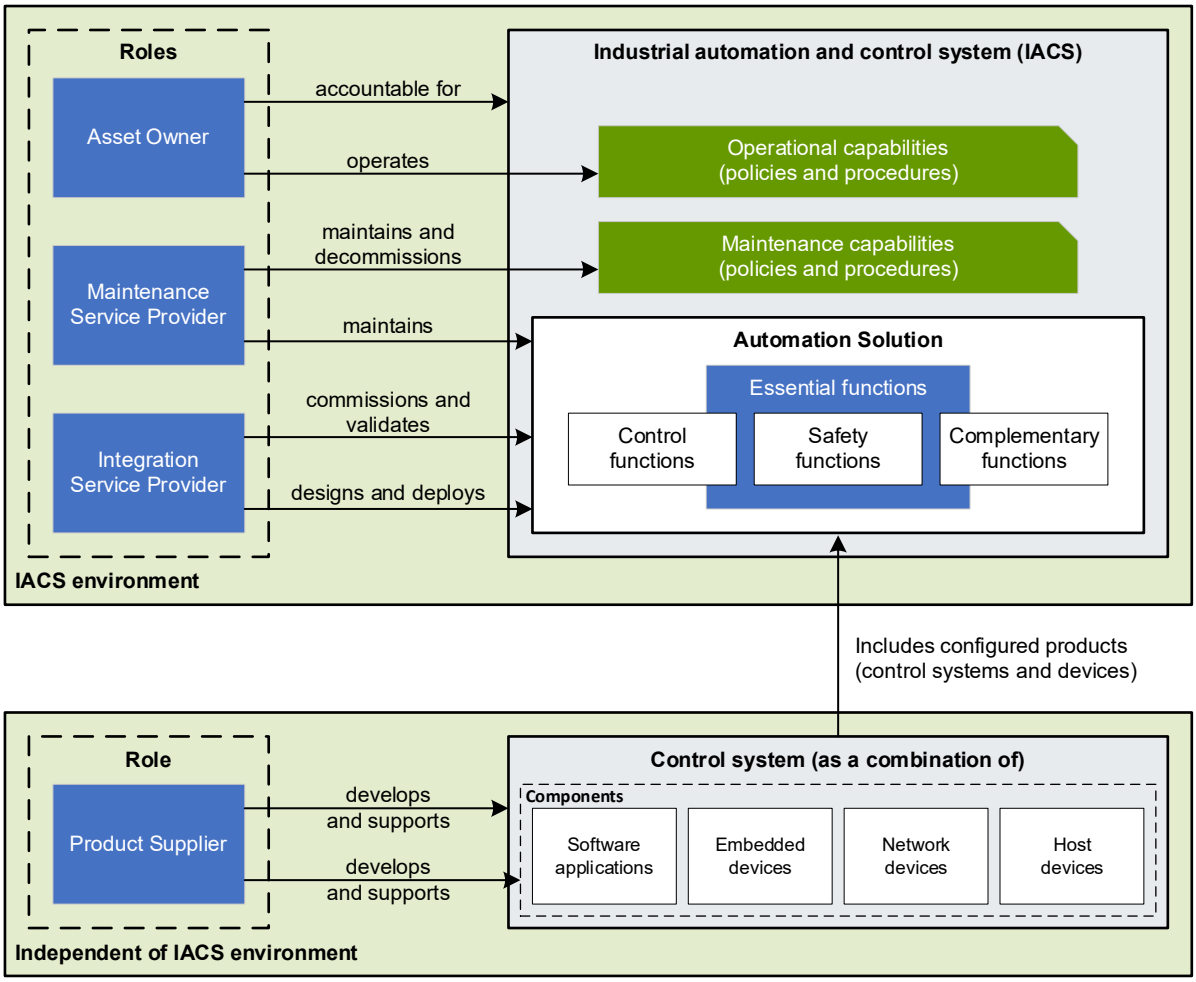

Figure 1 - Roles, Products, Automation Solution and IACS

The right-hand side of Figure 1 shows the types of systems and components that are identified in the ISA/IEC 62443 standards:

- *components* are provided by a product supplier and include the following types:
  - *embedded device* – special purpose device designed to directly monitor or control the equipment under control
  - *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 suppliers
  - *network device* – device that facilitates data flow between devices, or restricts the data flow, but does not directly interact with the Equipment Under Control
  - *software application* – one or more software programs and their dependencies that are used to interface with the process or the control system itself
- A *control system* consists of an integrated set of *components* (*embedded devices*, *host devices*, *network devices* and *software applications*) that is provided by a product supplier.
- An *Automation Solution* is the realization of one or more *control systems* at a particular facility. It includes essential functions such as safety functions and control functions and other supporting functions such as historization and engineering.

- The *Industrial Automation and Control System (IACS)* includes the Automation Solution and the operational capabilities and maintenance capabilities (policies and procedures) necessary to support it.

4.3 Principal roles

The ISA/IEC 62443 standards are organized by the Security Programs for principal roles and technical requirements. The left-hand side of Figure 1 shows the relationship between principal roles and the IACS that are identified in the ISA/IEC 62443 standards:

- *Asset Owner* is an organization that 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* is an organization that provides maintenance and support activities for an Automation Solution.
- *Integration Service Provider* is an organization that provides system 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 security zones and conduits and participate in the security risk assessment.
- *Product Supplier* is the organization that manufactures and supports a hardware and/or software product. Products may include control systems, embedded devices, host devices, network devices and/or software applications.

4.4 Security Program

There are three types of security measures that are defined in ISA/IEC 62443 standards to meet one or more security requirements:

- *Process security measures* are policies and procedures that are documented and implemented by trained personnel. Process security measures are measured by *Maturity Levels*.
- *Technical security measures* are implemented in the hardware and software of systems and components. Technical security measures are measured by *Security Levels*.
- *Compensating security measures* are alternate security measures that are implemented when a technical or process security measure is not available to meet a security requirement.

ISA/IEC 62443-2-1 specifies the SP requirements for the IACS asset owner. ISA/IEC 62443-2-4 specifies the SP requirements for the IACS service provider for those activities and tasks that are delegated from the asset owner to a service provider.

The SP covers the entire lifecycle of the IACS. Because the lifetime of an IACS can be longer than the product supplier support timeframe, the standard recognizes that not all requirements can be met by legacy systems, so compensating security measures may be needed to secure the IACS.

Although the asset owner is ultimately accountable for the secure operation of the IACS, implementation of security measures requires the support of product suppliers and service providers. The asset owner must include requirements for security throughout the supply chain to meet the overall SP requirements.

The SP for the IACS must be coordinated with the overall Information Security Management System (ISMS) of the organization. The ISMS sets the overall security governance and policies for the enterprise. However, the IACS is significantly different from IT systems, so there are additional requirements and considerations for its SP.

4.5 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.

ISA/IEC 62443-3-3 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 systems (ISA/IEC 62443-3-3) and components (ISA/IEC 62443-4-2).

Table 1 - Security Level definitions

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*

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

- *Target Security Levels (SL-T)* are the desired level of security for a particular security zone or conduit. They are determined as the result of the security risk assessment process (ISA/IEC 62443-3-2) and are documented in the Cybersecurity Requirements Specification. SL-T are used to select and configure products and design additional security measures during the integration phase of the IACS lifecycle.

- *Capability Security Levels (SL-C)* are the security levels that systems (ISA/IEC 62443-3-3) or components (ISA/IEC 62443-4-2) can provide when properly integrated and configured. These levels state that a particular system or component is capable of meeting the Target Security Level natively without additional compensating security measures.

- *Achieved Security Levels (SL-A)* are the actual levels of security for a particular security zone or conduit. These are measured after the security zone or conduit is commissioned and in operation.

4.6 Maturity Level

While Security Levels are a measure of the strength of technical requirements, Maturity Levels are a measure of the effectiveness of processes (people, policies and procedures). The ACSSA conformity assessment program uses Maturity Levels to measure how thoroughly policy and procedural requirements are met. Table 2 shows the definition of Maturity Levels from ISA/IEC 62443-2-1 (modified).

Table 2 - Maturity Level definition

Level	This document	Description
1	Initial	At this level, processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency over time can be difficult to show. NOTE: “Documented” in this context refers to the procedure followed in performing this process, not to the results of performing the process.
2	Managed	At this level, documentation exists that describes how to manage the delivery and performance of the process. This documentation can be in the form of written procedures or written training programs for performing the process. The discipline reflected by ML 2 helps to ensure that processes are repeatable, even during times of stress. When these processes are in place, their execution will be performed and managed according to their documented procedures.
3	Defined / Practiced	At this level, there is evidence that the processes documented in Level 2 are consistently practiced on the IACS. The performance of a Level 3 process can be shown to be repeatable over time.
4	Improving	At this level, the effectiveness or performance improvements of the process can be demonstrated using suitable metrics. This results in a SP that improves the process through technological/procedural/management changes over time.

Based upon ISA/IEC 62443-2-1:2024 Table 1

4.7 Security Risk Assessment

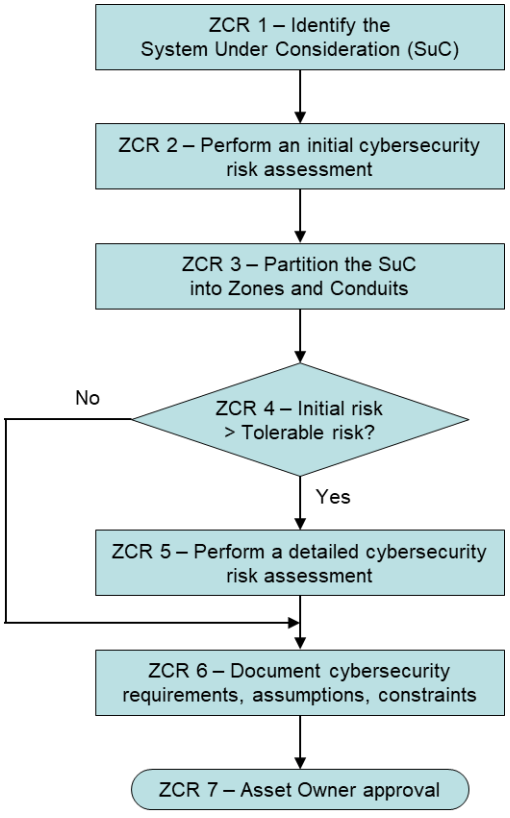

Figure 2 – Security risk assessment process

Figure 2 shows the security risk assessment process in ISA/IEC 62443-3-2, which describes the requirements for addressing the cybersecurity risks in an IACS, including the partitioning into security zones and conduits with associated Target Security Levels. While ISA/IEC 62443-3-2 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 in ISA/IEC 62443-3-2.

The security risk assessment process includes the following concepts:

- System Under Consideration – defines the scope of the risk assessment
- Equipment Under Control – determines the types of consequences and severity that could occur
- Security zone and conduit partitioning – is a method to segregate physical access (e.g. doors and locks) and logical access (e.g. network segmentation) for a group of IACS assets
- Target Security Level – determines the set of technical security measures that apply to a particular security zone or conduit

4.8 Essential Functions

Essential functions are defined as functions or capabilities that are required to maintain health, safety, the environment and the availability of the Equipment Under Control. Essential functions include:

- the Safety Instrumented Function (SIF)
- the control function for Equipment Under Control that requires high availability
- the ability of the operator to view and manipulate the Equipment Under Control

The loss of essential functions is commonly termed: loss of protection, loss of control, and loss of view respectively. In some use cases additional functions such as history may be considered essential.

ISA/IEC 62443-3-3 requires that security measures shall not adversely affect essential functions of a high-availability IACS unless it is supported by a security risk assessment. The concept of essential functions places some design constraints on the design of IACS security measures:

- Access control shall not prevent the operation of essential functions
- Essential functions shall be maintained if the zone boundary protection (firewall) goes into a fail close/island mode
- A denial-of-service event on the control system or safety instrumented system (SIS) network shall not prevent safety instrumented functions (SIF) from acting

4.9 Security Zones and Conduits

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

A key step in the security risk assessment process is to partition the System Under Consideration into separate security 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.

Partitioning the System Under Consideration into security zones and conduits can also reduce overall risk by limiting the scope of a successful cyber-attack. ISA/IEC 62443-3-2 requires or recommends that some assets are partitioned as follows:

- separate business and control system assets (required)
- separate safety related assets (required)
- separate temporarily connected devices (recommended)
- separate wireless devices (recommended)
- separate devices connected via external networks (recommended)

4.10 Cybersecurity Requirements Specification

ISA/IEC 62443-3-2 also requires that security measures from the security risk assessment as well as security requirements based on company or facility-specific policies, standards and relevant regulations are documented in a Cybersecurity Requirements Specification (CRS). The CRS does not have to be a standalone document; it can be included as a section in other relevant IACS documents. The CRS includes information such as a description of the System Under Control, security zones and conduits, threat environment, and security measures from security risk assessments.

5 ACSSA Overview

The Automation and Control System Security Assurance (ACSSA) program is a conformity assessment program that describes the inspection or certification of an Industrial Automation and Control System (IACS) installed and in-operation, or operations-ready, in an asset owner's facility. This section provides an overview of the ISASecure® ACSSA program.

5.1 ACSSA roles and responsibilities

The following describes the roles and responsibilities of the organizations that are involved in the development, accreditation, planning and execution of the ACSSA program:

- The Conformity Assessment Scheme Owner is responsible for the creation and maintenance of the ACSSA conformity assessment scheme. The Conformity Assessment Scheme Owner for ACSSA is the ISA Automation Standards Compliance Institute (ASCI) – ISA Security Compliance Institute (ISCI) which creates and maintains conformity assessment schemes under the ISASecure® brand.

- Accreditation Bodies (AB) are responsible for the accreditation of Conformity Assessment Bodies (CAB). Accreditation is a third-party attestation that the conformity assessment body is able to perform the evaluation consistently and with competence and impartiality. Accreditation Bodies are accredited to ISO/IEC 17011.

- Conformity Assessment Bodies (CAB) are responsible for performing the conformity assessment activities for an inspection or certification. There are two types of CAB:
    - *Inspection Bodies (IB)* are responsible for performing inspections and are accredited to ISO/IEC 17020
    - *Certification Bodies (CB)* are responsible for performing certifications and are accredited to ISO/IEC 17065

5.2 ACSSA documents

Figure 3 shows the documents that describe the ACSSA program. On the left-hand side are the ACSSA documents. On the right-hand side are the standards that form the basis for the ACSSA conformity assessment program.

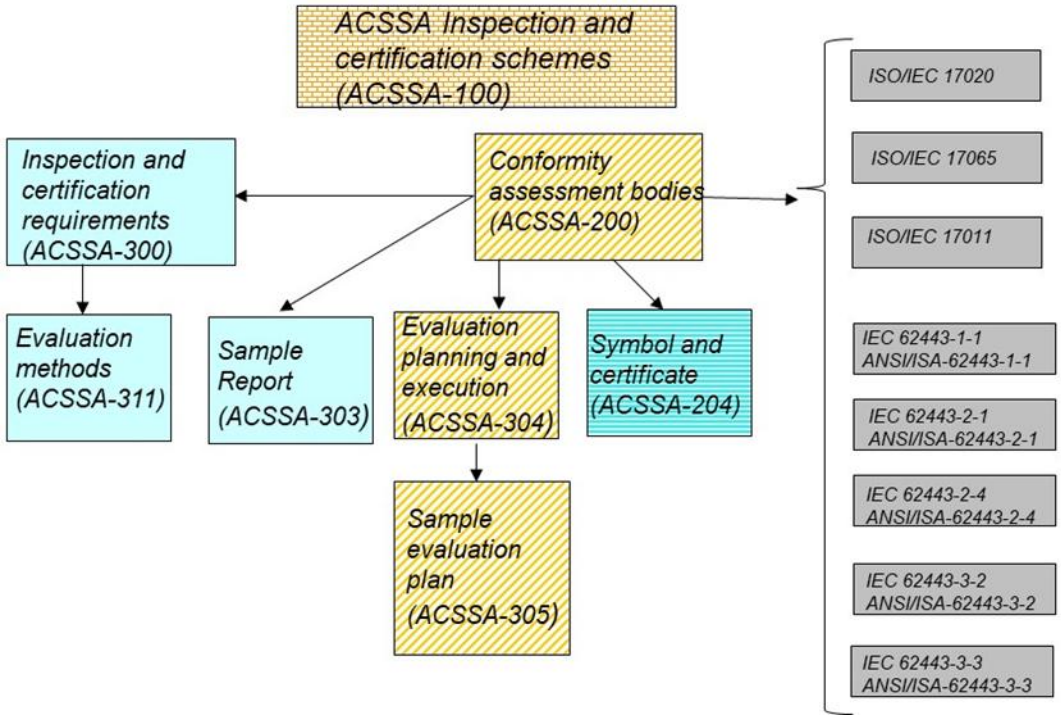

Figure 3 - ISASecure® ACSSA documents

Here is a summary description of each of the main ACSSA documents:

- *ACSSA-100 ACSSA Inspection and certification schemes* provides an overview of the ISASecure® ACSSA program including both the inspection and certification programs
- *ACSSA-101 ACSSA Evaluation planning for the asset owner (this document)* describes the information needed by an asset owner to prepare for and engage with a conformity assessment body (CAB) to initiate an inspection or certification.
- *ACSSA-200 Operations and accreditation for conformity assessment bodies* describes the requirements for the accreditation and operations of a CAB for inspection or certification
- *ACSSA-204 Instructions and Policies for Use of the ISASecure® Symbol and Certificates* describes the proper usage of the ISASecure® symbol and certificate
- *ACSSA-300 Inspection and certification requirements* describes the scope of an IACS evaluation and the requirements of an ACSSA inspection or certification
- *ACSSA-303 Sample Inspection Report* provides a sample inspection report for an inspection or certification
- *ACSSA-304 Evaluation planning and execution* provides guidance to the CAB for the planning and execution of an ACSSA inspection or certification
- *ACSSA-305 Sample evaluation plan* provides a sample evaluation plan
- *ACSSA-311 Evaluation methods* describes the technical criteria that are used in an inspection or certification evaluation based on ISA/IEC 62443 requirements

5.3 ACSSA Inspection

An asset owner organization might use an ACSSA inspection for internal purposes, to gauge the current security posture of an IACS in-operation, or the security-readiness of an IACS that is deemed operations-ready.

To obtain an ACSSA inspection, the asset owner applies to an accredited Inspection Body (IB) for a specified IACS. The IB determines eligibility of the IACS in accordance with ACSSA-300. Once eligibility is established, the IB and asset owner will jointly plan the evaluation. Once the evaluation plan is approved by the asset owner, the evaluation commences. Once completed, the asset owner will receive a formal ACSSA inspection report. The report provides statements of conformity to individual 62443 requirements.

An inspection is a one-time evaluation of a specific IACS at a specific time. The asset owner may schedule future inspections as they see fit, to measure progress.

In some cases, an ACSSA report developed under the ACSSA inspection program by an IB, may be used as evidence toward an ACSSA certification. Detailed program procedures on this topic are found in ACSSA-200.

5.4 ACSSA Certification

An asset owner organization might use an ACSSA certification as part of a long-term public commitment to maintain their SP, or because an external entity offers benefits for maintaining a certification, or the asset owner requires a certification to meet regulatory requirements.

To obtain an ACSSA certification, an asset owner applies to an accredited Certification Body (CB) for certification of a specified IACS. The CB determines eligibility of the IACS in accordance with requirements of ACSSA-300. Once eligibility is established, typically the CB performs a gap analysis to assist the asset owner in preparing for the formal evaluation. Once the formal evaluation of the IACS is complete, if the IACS meets the ACSSA certification criteria, it is granted certified status until an expiration date as specified in ACSSA-300. The asset owner receives a certificate and an inspection report. The inspection report is the same as described in Section 5.3.

A certificate is valid for three years. An annual surveillance process is required to maintain the certification until its expiration date. A recertification process is required to extend the certification for another three years. At this time a new certificate and certification report are issued. The maintenance of certification process is described in ACSSA-300 Section 5.

An asset owner with an IACS that has been certified under the ACSSA certification program may display the ISASecure® symbol and a certificate granting certification, in accordance with program procedures found in ACSSA-204.

At the request of an asset owner organization, ISCI will post on its web site (isasecure.org) the name of the asset owner organization and the information on their ACSSA certificate(s). An asset owner that does not elect that ISCI post this information, may request that ISCI provide the information directly to a specified third party.

5.5 Information disclosure

All asset owner information submitted to the CAB, and any inspection or certification documents generated during the evaluation must be protected from public disclosure by the CAB. The CAB must demonstrate their ability to protect information as part of the accreditation process [ISO/IEC 17020 4.2, ISO/IEC 17065 4.5]. Any public release of this information must be approved by the asset owner [ACSSA-200 ACSSA.R2].

ASCI and ISCI shall not have access to information generated during ISASecure® evaluations, except by permission of the asset owner, or as required to fulfill ISCI's oversight role as the conformity assessment scheme owner. [ACSSA-200 ACSSA.R1]

5.6 ACSSA evaluation method

ACSSA-311 Evaluation methods documents the evaluation criteria for an inspection or certification. The evaluation criteria are based on requirements from the following ISA/IEC 62443 standards:

- 62443-2-1 includes requirements for the policies and procedures of the asset owner's SP

- 62443-3-2 includes requirements for the asset owner's security risk assessment process
- 62443-2-4 includes requirements for the policies and procedures of the service provider's SP that have been delegated by the asset owner through contractual agreements
- 62443-3-3 includes technical requirements that utilize the technical capabilities of the IACS as required to support the policies and procedures specified in 62443-2-1

ACSSA-311 Evaluation methods includes the following information for each requirement:

- Maturity Level 2 Activity – documentation of policies and procedures (not applicable for 62443-3-3)
- Maturity Level 3 Activity – demonstration that policies and procedures are being followed
- Security Level – selection of requirements based on security risk assessment
- Artifact Type (D-Document, O-Observe, T-Test)
- Document Type
- Cross references between 62443-2-1, 62443-2-4, 62443-3-2 and 62443-3-3

The evaluation result types vary depending on the 62443 standard, and the Maturity Level and Security Level of the requirement being assessed. The evaluation result types are shown in Table 3 below.

Table 3 - ACSSA-311 Evaluation result types

Evaluation result type	Description	Applies to 62443 Part			
		2-1	2-4	3-2	3-3
Met	The requirement is met	Yes	Yes	Yes	Yes
Not met	The requirement is not met	Yes	Yes	Yes	Yes
Not required - documented risk justification	The requirement is not required because there is a documented risk justification for not meeting this requirement	Yes			Yes
Not required - for target security level of zone	The requirement is not required because the Security Level of the requirement is greater than the Target Security Level for the Security Zone being assessed	Yes			Yes
Not required - technology not used in IACS or Security Zone	The requirement is not required because the technology is not in use in the Security Zone being assessed	Yes			Yes
Not feasible or allowed by law	The requirement is not feasible or not allowed by law	Yes	Yes		
Not required by asset owner	For Part 2-4 requirements, the requirement is not in the scope of the service providers contractual responsibilities		Yes		

Evaluation result type	Description	Applies to 62443 Part			
		2-1	2-4	3-2	3-3
Verified by independent certification	For Part 2-4 requirements, the requirement has been verified by an independent third party certification		Yes		
Documented compensating security measure in place	The requirement is not met, but there is compensating security measure that is documented and being executed				Yes

Certification pass criteria are that there are no applicable requirements that have a “Not met” evaluation result for Maturity Level 2 and Maturity Level 3, based on the Target Security Level for each security zone.

5.7 Maintenance of Certification

After attaining an ACSSA certification, there is a process to maintain the certification. To maintain an ACSSA certification, the CB performs an annual surveillance activity in the first and second years after certification is achieved. Surveillance activity covers any IACS changes, continued conformity to basic requirements, and a sampling of other requirements both based on risk and by random selection. A full recertification is required every third year, followed by annual surveillance. ACSSA-300 Section 5 and ISASecure_ACS.R21 through R28 describes the requirements for surveillance and recertification activities, and the handling of any nonconformities found. The process for addressing nonconformities depends upon their classification as major or minor.

6 Key Policies, Procedures and Artifacts needed for success

The intent of this section is to describe the documents and artifacts that are needed to have a successful ACSSA certification. In other words, the asset owner is unlikely to pass a certification if these documents and artifacts are not available. It is not intended to be a complete list or guarantee of success.

An inspection may be done for an organization regardless of their level of organizational maturity, to evaluate the degree to which the IACS meets 62443 requirements.

6.1 Security Program

The SP includes the security policies, processes and procedures that are needed to secure an IACS. There are two types of security programs evaluated as part of the ACSSA program: the asset owner SP, and the service provider SP. The requirements for each type of security program are described in ACSSA-311 and are based on the following ISA/IEC 62443 standards:

- ISA/IEC 62443-2-1 Security program requirements for IACS asset owners
- ISA/IEC 62443-2-4 Security program requirements for IACS service providers

In most cases, an IACS will be governed by a single asset owner SP. However, ACSSA does allow for the evaluation of multiple asset owner SPs. Since there are typically multiple service providers interacting with an IACS, ACSSA will typically evaluate the SP for each service provider.

A *policy* is a high-level statement that describes guidelines and principles that govern actions and decisions that align with an organization's goals. The asset owner SP includes one or more policy documents that meets the requirements of ISA/IEC 62443-2-1. Each service provider's SP includes one or more policy documents that meets the requirements of ISA/IEC 62443-2-4 applicable to their responsibilities. For example, the asset owner may establish a policy that users of the IACS must be uniquely identified (USER 1.1 SL 2). If a service provider has been delegated responsibility to manage accounts, then the service provider must also meet this policy (SP.09.02)

A *process* is a series of related tasks or activities that are performed to achieve a specific goal. It describes what needs to be done and in what order. For example, to meet the above policy, the asset owner would establish an account management process that governs the creation, modification, and deletion activities for user accounts. This process may group together related ISA/IEC 62443 requirements, for example USER 1.1 to 1.5.

Note: the term *process* is not to be confused with the term *industrial process*.

A *procedure* is a detailed, step-by-step set of instructions on how to perform a specific task or activity. For example, there may be a procedure document that covers the deletion of user accounts upon termination of an employee.

The asset owner has flexibility in how to organize the policy, process, and procedure documents for an IACS, provided this set of documents collectively meet the requirements of ISA/IEC 62443-2-1. Similarly, the service provider has flexibility in how to organize the policy, process, and procedure documents for those requirements that have been delegated to them by the asset owner.

6.2 Security Risk Assessments

Security risk assessments are central to the implementation of the ISA/IEC 62443 standards. The requirements for the security risk assessment process are specified in ISA/IEC 62443-3-2 and include:

- Defining a System Under Consideration (SUC) for an IACS
- Assessing the initial risk for the SUC
- Partitioning the SUC into security zones and security conduits
- Assessing risk for each security zone and security conduit
- Establishing the Target Security Level (SL-T) for each security zone and security conduit
- Documenting the security requirements for each security zone and conduit
- Asset owner approval of the security risk assessment

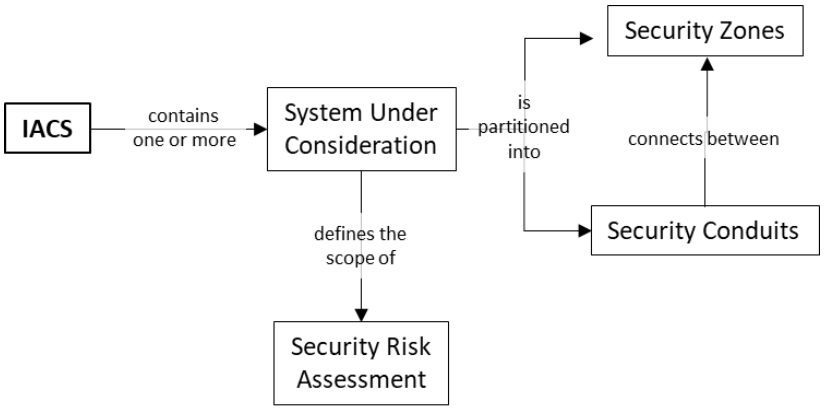

Figure 4 - Security risk assessment ontology

The asset owner has considerable flexibility in organizing the set of security risk assessments for an IACS. However, it is important that the set of security risk assessments covers the scope of the IACS under evaluation. The relationships between IACS, System Under Consideration, and Security Zone and Conduit is shown in Figure 4 and are described as:

- the scope of an ACSSA evaluation is one IACS
- an IACS can have one or more Systems Under Consideration
- a System Under Consideration can have one or more Security Zones
- each Security Zone has a Target Security Level and a set of security requirements
- a System Under Consideration can have one or more Security Conduits
- each Security Conduit has a Target Security Level and a set of security requirements

In a large asset owner facility, there may be many Systems Under Consideration and many security zones and conduits. The ACSSA evaluation method allows the CAB to select a sample of SUCs and Zones for evaluation, provided the sample set is representative of the entire IACS. Sampling requirements for SUCs and Zones are described in ACSSA-300 Section 4.4.3 and ISASecure_ACSSZS.R1 through R5.

ISA/IEC 62443-3-2 specifies requirements that the asset owner's security risk assessment must meet. However , it does not prescribe the exact methodology to be used; this must be established by the asset owner and documented in the policies and procedures documentation of the SP. Specific policies and procedures for security risk assessments that must be established and documented by the asset owner are:

- A process to assess threats and vulnerabilities

- A process to assess the impact of consequences, including the consequences for information risk and operational risk [ISA/IEC 62443-1-1:2007, 4.4]
- A process to assess the risk, including the establishment of tolerable risk
- A process to partition the SUC into security zones and conduits
- A process to establish the SL-T and security requirements for each security zone and conduit

The Target Security Level (SL-T) is used to select the Capability Security Level (SL-C) of the systems and components in the security zone or conduit from ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2 respectively. It is important to note that simply selecting a system or component with the required SL-C is not enough; the capabilities must be *utilized* by correctly implementing and configuring the system or component to meet the SL-T. The methodology for determining an SL-T from the unmitigated risk of the security zone is not prescribed by ISA/IEC 62443-3-2 and must be determined by the asset owner when defining the policies and procedures for security risk assessment. [ISA/IEC 62443-3-2 ZCR 5.6, Annex A]

If technical security measures are not available, then the process allows for the design and implementation of compensating security measures. These are typically process security measures that compensate for the lack of a technical security measures. A key consideration for compensating security measures is their effectiveness compared to the technical security measure they are replacing.

6.3 Security Zone and Conduit Partitioning

The security risk assessment process partitions the SUC into security zones and conduits for each SUC in the IACS. There are two aspects to the partitioning: physical partitioning and logical partitioning.

For the physical security zone model, access to IACS systems and components is controlled by separating assets into physical security zones with access control restrictions. For example, the outer perimeter of a facility would be a security zone, with building and room security zones that have physical access controls nested within it. [62443-2-1 ORG 3.1]

Partitioning SUC (and IACS) assets into logical security zones, is typically achieved by network segmentation with data flow restrictions implemented as security conduits between security zones. There are several requirements and recommendations specified in 62443:

- Separate business and IACS assets (required) [62443-2-1 NET 1.1, 62443-3-2 ZCR 3.2]
- Separate safety-related assets (required) [62443-2-1 NET 1.3, 62443-3-2 ZCR 3.3]
- Separate temporarily-connected devices (recommended) [62443-3-2 ZCR 3.4]
- Separate wireless devices (recommended) [62443-3-2 ZCR 3.5]
- Separate devices connected via external networks (recommended) [62443-3-2 ZCR 3.6]

Requirements are included in inspections and certifications and are required to be met to achieve a certification. Recommendations are included in inspections and certifications but are not required to achieve a certification.

6.4 IACS Asset Inventory

ISA/IEC 62443-2-1 CM 1.1 requires that the asset owner maintain an updated list of the IACS assets, including devices, hardware components, software components, communications protocols and open communications ports used in the IACS, including, but not limited to:

- organizational responsibilities
- manufacturer
- model

- version numbers
- serial numbers
- network interfaces
- communications addresses
- revision/patch levels
- history

In addition to the above list for IACS devices, hardware and software, ISA/IEC 62443-3-2 ZCR 6.4 requires that the following information is documented for each security zone and conduit:

- name and/or unique identifier
- accountable organization
- definition of logical boundary
- definition of physical boundary, if applicable
- safety designation
- list of all logical access points
- list of all physical access points
- list of data flows associated with each access point
- connected zones or conduits
- list of assets and their classification, criticality and business value
- SL-T
- applicable security requirements
- applicable security policies
- assumptions and external dependencies

The asset owner has some flexibility in how to meet these requirements. There can be one or more inventories that are manually created and maintained or automatically created and maintained. If the inventory is automatically created and maintained, however, the risks to the IACS of network scanning of IACS components should be considered. Network scanning has been known to cause some IACS components to fail.

6.5 IACS Service Providers agreement and responsibilities

Service providers that provide integration or maintenance services for the IACS must meet the requirements of ISA/IEC 62443-2-4 for those responsibilities that have been delegated to them by the asset owner. The responsibilities that have been delegated must be documented in a services agreement or other contractual agreement.

For example, if the asset owner has delegated software update (patch) management to a service provider (ISA/IEC 62443-2-1 COMP 3.1-3.5) then the service provider must meet the associated requirements in ISA/IEC 62443-2-4 (SP.11.01 – SP.11.06)

As part of the ACSSA evaluation, the asset owner will be asked to provide a list of all service providers that interact with the IACS, their roles and responsibilities, the documented agreements that govern the relationship, and the documented policies and procedures that the service provider must follow.

ACSSA-311 includes cross-references between the asset owner requirements from 62443-2-1 and the associated service provider requirements from 62443-2-4.

6.6 IACS Product Supplier list and system security documentation

The asset inventory will contain a complete list of all IACS systems and components and their product suppliers. However, in order to meet ISA/IEC 62443-2-1 requirements for supply chain management (ORG 1.6), security development lifecycle (ORG 2.3), and security patch management (COMP 3.1-3.5) it is recommended to maintain a list of the key product suppliers of IACS systems and components.

ISA/IEC 62443-2-1 requires "policies and procedures addressing the use of a secure development lifecycle process for the development and support of systems and components used in the IACS." Such a lifecycle process typical requires the supplier make available security guideline documentation that describes how to integrate, configure and maintain a defense in depth strategy for their products. These documents are important to properly implement and configure the products to achieve the Target Security Level.

The use of products that have received ISASecure Certification will facilitate ACSSA Certification because the products have demonstrated that they have the capability to meet ISA/IEC 62443 requirements. Specific ISASecure Certifications that may be relevant for an ACCSA Certification are:

- Security Development Lifecycle Assurance (SDLA)
- System Security Assurance (SSA)
- Component Security Assurance (CSA)
- IIoT Component Security Assurance (ICSA)

6.7 Incident response and recovery

ISA/IEC 62443-2-1 has requirements for detection, storage, reporting, non-repudiation, time synchronization, and interfaces to security event logs [62443-2-1 EVENT 1.1-1.6]. There are also requirements for the analysis and response to security incidents. [62443-2-1 EVENT 1-7-1.8]. The SP will need documented policies and procedures for Incident Response and Recovery to meet these requirements. Since IACS security incidents can have physical consequences, the Incident Response procedures may need to include Emergency Response.

ISA/IEC 62443-2-1 also has requirements for Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) [62443-2-1 AVAIL 1.1]. To support these requirements, 62443-2-1 specifies requirements for backup and recovery. [62443-2-1 AVAIL 2.1-2.5].

7 ACSSA Evaluation planning and execution

The planning and execution of an ACSSA evaluation is a joint activity between the asset owner and the conformity assessment body for either an inspection or a certification. The planning and execution activities are described in *ACSSA-304 Evaluation planning and execution*.

7.1 Expectations

When entering into an agreement to perform an ACSSA inspection or certification it is important that the expectations of the asset owner and the conformity assessment body are clearly understood and communicated. These expectations should be documented in the ACSSA evaluation agreement. Here are some examples of asset owner and CAB expectations for an ACSSA evaluation [ACSSA-304 5.3.3]

Asset owner expectations of the CAB

- Designated CAB single point of contact
- CAB personnel are competent to perform the evaluation
- CAB personnel do not compromise the availability, safety or security of the IACS or EUC
- CAB personnel comply with asset owner safety and security policies and procedures
- Activities that may affect the IACS (e.g. scanning or testing) are risk justified and approved by the asset owner

Conformity Assessment Body (CAB) expectations of the asset owner

- Designated asset owner single point of contact
- Access to key stakeholders for review and approval of the plan and report
- Access to nominated resources for support and escalation of issues during the evaluation as needed
- Access to key personnel for meetings, interviews, and assessment of evidence
- Access to service provider and product supplier representatives as needed
- Access to inspect IACS systems, components and networks
- Access to physical facilities where IACS systems and components are located
- Gathering of application and submission information including SUC information, zone and conduit information, and system information (ACSSA-300 ISASecure_ACS.R6)

7.2 Define the scope of the ACSSA evaluation

The scope of an ACSSA evaluation is a single IACS with the following characteristics: [ACSSA-300 ISASecure _ACS.R1]

- A named organization that fulfills the role of asset owner for the IACS
- Specified hardware and software for the IACS, defined in an asset inventory under change control
- List of Equipment Under Control associated with the IACS and under change control
- Documented policies and procedures for an asset owner's named security program for the IACS, where this security program documentation is under change control
- List of service providers internal or external to the asset owner's organization that provide integration or maintenance services for the IACS
- List of asset owner and service provider personnel that have been assigned to interact with the IACS

The asset owner has considerable flexibility in defining the scope of the IACS. It can contain:

- One or more Security Programs

- One or more Systems Under Consideration (which define the scope of each security risk assessment)
- One or more Security Zones
- One or more Security Conduits
- One or more Systems
- One or more service providers

For an IACS to be eligible for ACSSA programs, the asset owner seeking ACSSA evaluation shall be fully accountable for managing, operating, and maintaining all hardware and software within all security zones of the IACS, and for all ingress/egress points for external communication and communication between security zones [ACSSA-300 ISASecure_ACS.R2]. Cyber elements that interface to the IACS (e.g. cloud-based functionality) must meet 62443 requirements for remote access and be included in security risk assessments. Cases where cloud-based functionality can directly or indirectly make changes to the equipment under control cannot be included in ACSSA evaluations.

7.3 Plan the ACSSA evaluation

The requirements for planning an ACSSA evaluation are described in ACSSA-304 Section 5 and ACSSA-200 ACSSA.R19. The planning phase of the evaluation includes the following activities:

- Project kick-off meeting
- Prepare and review ACSSA Evaluation scope [see Section 7.2 and Annex A]
- Prepare draft plan
- Review draft plan
- Approve and issue plan

7.4 Execute the ACSSA evaluation

The execution of an ACSSA evaluation is described in ACSSA-304 Section 6. A typical ACSSA evaluation workflow has three phases:

- ***Phase 1 – risk assessment evaluation.*** This phase evaluates that asset owner policies and procedures for security risk assessments comply with the requirements described in 62443-2-1 NET 1.1, 1.2, 1.3, and 62443-3-2 ZCR 1 through 7.
- ***Phase 2 – Maturity Level 2 evaluation.*** This phase evaluates the asset owner's policies and procedures to verify that their SP and service provider SPs, as applied to the IACS being evaluated, are *documented* in conformance with 62443-2-1 and 62443-2-4 at maturity level 2.
- ***Phase 3 – Maturity Level 3 evaluation.*** This phase evaluates the asset owner's policies and procedures to verify that their SP and the service provider's SP are *being practiced* in accordance with 62443-2-1, 62443-2-4, and 62443-3-3.

Evaluation criteria for each requirement are defined in ACSSA-311 Evaluation Methods.

The execution of an ACSSA evaluation will typically include the following activities:

- ***Gather documents and artifacts, such as***
    - Asset owner policy documents
    - Asset owner procedure documents
    - Asset owner technical documents (e.g. system configuration)
    - Asset owner risk assessment documents
    - Asset owner security zone partitioning documents (e.g. system architecture)
    - Service provider contracts or other agreements
    - Asset owner and service provider artifacts (evidence of policy/procedure execution)
    - Product supplier security documents
- ***Interview personnel, such as***
    - Asset owner administrators
    - Asset owner maintenance
    - Asset owner operations
    - Service provider representatives
    - Product supplier representatives
- ***Inspect Systems and Networks, such as***
    - Physical segmentation
    - Network segmentation and configuration
    - System configuration and settings
    - Compensating security measures
- ***Document the ACSSA evaluation***
    - Requirements [ACSSA-311]
    - Inspection or Certification report [ACSSA-303]
    - Certificate [ACSSA-204]

8 How to apply for an ACSSA evaluation

The asset owner application and submission requirements for an ACSSA evaluation is defined in ACSSA-300 ISASecure_ACS.R6.

An optional gap analysis to identify the submissions required can be requested by the asset owner and is described in ACSSA-300 ISASecure_ACS.R8.

Annex A is a template that the asset owner can use to describe the scope of an ACSSA evaluation (inspection or certification) for initial contact with a CAB to develop the ACSSA evaluation plan. The template includes the following sections which together define the scope of an ACSSA evaluation:

- Asset owner information [A.1]
- Evaluation information [A.2]
- List of Security Programs [A.3]
- List of Equipment Under Control [A.4]
- List of Systems Under Consideration [A.5]
- List of Security Zones [A.6]
- List of main Automation and Control Systems [A.7]
- List of Service Providers [A.8]

8.1 Asset owner information

- Name of the Asset owner organization accountable for the IACS [ACSSA-300 ISASecure_ACS.R2]
- Location(s) of the IACS under evaluation
- Name, email, phone and address of the asset owner single point of contact for the evaluation

8.2 Asset Owner elections

- Type of evaluation: Inspection or certification [ACSSA-300 ISASecure_ACS.R3]
- Election and evaluation of Maturity Level 1 [ACSSA-300 ISASecure_ACS.R4]
- Publication of ACSSA inspection cover letter or certificate [ACSSA-200 ACS.R2]

8.3 List of Security Programs

An IACS is typically managed by one SP. However, ACSSA allows for the case where different parts of the IACS are managed by different SPs. Information for each Security Program includes:

- Security Program name
- Security Program version
- Last date the Security Program was revised
- Estimated number of documents (to allow the CAB to estimate evaluation effort)

8.4 List of Equipment Under Control

This is a list of the Equipment Under Control that the IACS under evaluation is connected to. It is not intended to be a detailed asset inventory of the EUC, but rather a high-level description of the equipment that the IACS is controlling. This list includes:

- Name of the Equipment Under Control
- Description of the Equipment Under Control

- Location of the Equipment Under Control

8.5 List of Systems Under Consideration

The IACS may include one or more Systems Under Consideration, where each SUC has an associated security risk assessment. This list includes:

- Name of the System Under Consideration
- Description of the System Under Consideration
- Name of the associated Security Risk Assessment

8.6 List of Security Zones

Each System Under Consideration is partitioned into one or more Security Zones. The list of Security Zones includes the following information:

- Name of the Security Zone
- Function or purpose of the Security Zone (e.g. safety function, control function)
- Target Security Level of the Security Zone
- Name of the associated System Under Consideration

8.7 List of Automation and Control Systems

Each Security Zone may have one or more automation and control systems. The list of automation and control systems includes the following information:

- Name of the system
- Function or purpose of the system
- System's product supplier
- Name of the associated Security Zone

8.8 List of Service Providers

Complete Service Provider details are described in ACSSA-300 ISASecure_ACS.R7. The list of Service Providers includes the following information:

- Name of the service provider
- Responsibilities of the service provider
- Role of the service provider (e.g. Integration, Maintenance, Other)
- Type of service provider (internal or external to the asset owner organization)

Annex A ACSSA Evaluation Scope Description Template

The purpose of this application is to allow the asset owner and the Inspection Body or Certification Body to come to agreement on the scope of an Automation and Control System Security Assurance (ACSSA) Inspection or Certification.

A.1 Asset Owner information

Name	{asset owner name}
Location	{Location(s) of the evaluation}
Contact name	{Name of the individual who is the single point of contact}
Contact email	{Address of the individual who is the single point of contact}
Contact phone	{Phone number of the individual who is the single point of contact}
Contact address	{Address of the individual who is the single point of contact}

A.2 Asset owner elections

Evaluation Type	{Inspection or Certification}
Election of optional evaluation to ML 1	{Yes, No}
Publication of ACSSA inspection cover letter or certificate	{Allowed, Not allowed} Note: the inspection or certification report is always confidential, this applies to the publication of the inspection cover letter or certificate.

A.3 List of Security Programs (SP)

List all Security Programs that are in the scope of the conformity assessment and their version and last update date. A Security Program is a group of one or more documents that describes the policies and procedures for the security of one or more IACS.

Security Program Name	**Security Program Version**	**Security Program last update date**	**Estimated number of documents**

A.4 List of Equipment Under Control (EUC)

List all Equipment Under Control that is in the scope of the conformity assessment and indicate their description and location.

EUC Name	EUC Description	EUC Location	

A.5 List of Systems Under Consideration (SUC)

List all Systems Under Consideration that are in the scope of the conformity assessment and indicate their description and location.

SUC Name	SUC Description	Security Risk Assessment

A.6 List of Security Zones

For each System Under Consideration, list all Security Zones that are in the scope of the conformity assessment and indicate the Security Zone Function, and Target Security Level.

Security Zone Name	Security Zone Function	Target Security Level	System Under Consideration

A.7 List of Automation and Control Systems

List the main automation and control systems that are in the scope of the conformity assessment and indicate which security zone(s) they are a member of.

Security Zone	Product Supplier	System Name	System Function

A.8 List of Service Providers

List the main service providers that are in the scope of the conformity assessment and indicate their responsibilities and type.

Service Provider Name	Service Provider Responsibilities	Service Provider Role	Service Provider Type
		{Integration, Maintenance, Other}	{Internal, External}

Annex B References

B.1 ACSSA program specifications

B.1.1.1 [ACSSA-100] ISA Security Compliance Institute Automation and Control System Security Assurance – ISASecure® inspection and certification schemes

B.1.1.2 [ACSSA-101] ISA Security Compliance Institute Automation and Control System Security Assurance – Evaluation planning for the asset owner

B.1.1.3 [ACSSA-102] ISA Security Compliance Institute Automation and Control System Security Assurance – Baseline document versions and errata for ACSSA 1.0.0 specifications

B.1.1.4 [ACSSA-200] ISA Security Compliance Institute Automation and Control System Security Assurance – Operations and accreditation for conformity assessment bodies

B.1.1.5 [ACSSA-204] ISA Security Compliance Institute Automation and Control System Security Assurance – Instructions and Policies for Use of the ISASecure® Symbol and Certificates

B.1.1.6 [ACSSA-205] ISA Security Compliance Institute Automation and Control System Security Assurance – Certificate Document Format

B.1.1.7 [ACSSA-300] ISA Security Compliance Institute Automation and Control System Security Assurance – Inspection and certification requirements

B.1.1.8 [ACSSA-303] ISA Security Compliance Institute Automation and Control System Security Assurance - Sample Inspection and Certification Reports

B.1.1.9 [ACSSA-304] ISA Security Compliance Institute Automation and Control System Security Assurance – Evaluation planning and execution

B.1.1.10 [ACSSA-305] ISA Security Compliance Institute Automation and Control System Security Assurance – Sample evaluation plan

B.1.1.11 [ACSSA-311] ISA Security Compliance Institute Automation and Control System Security Assurance – Evaluation methods

B.2 ANSI/ISA / IEC 62443 Series standards

The list below includes both ISA and IEC versions of the 62443 standard (except for IEC 62443-2-4). The technical content of each standard is identical.

B.2.1.1 [62443-1-1] ANSI/ISA-62443-1-1 (99.01.01) - 2007, Security for industrial automation and control systems Part 1-1: Terminology, concepts and models

B.2.1.2 [62443-1-1] IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security Part 1-1: Terminology, concepts and models

B.2.1.3 [62443-2-1] ANSI/ISA-62443-2-1-2024 Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners

B.2.1.4 [62443-2-1] IEC 62443-2-1:2024 Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners

B.2.1.5 [62443-2-4] IEC 62443-2-4:2023 Security for industrial automation and control systems Part 2-4: Security program requirements for IACS service providers

B.2.1.6 [62443-3-2] ANSI/ISA-62443-3-2-2020 Security for industrial automation and control systems Part 3-2: Security risk assessment for system design

B.2.1.7 [62443-3-2] IEC 62443-3-2: 2020 Security for industrial automation and control systems Part 3-2: Security risk assessment for system design

B.2.1.8 [62443-3-3] ANSI/ISA−62443−3−3 (99.03.03) - 2013, Security for industrial automation and control systems Part 3-3: System security requirements and security levels

B.2.1.9 [62443-3-3] IEC 62443−3−3:2013 Industrial communication networks - Network and system security Part 3-3: System security requirements and security levels

B.3 ISO/IEC 17000 Series standards

B.3.1.1 [17011] ISO/IEC 17011, Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies, November 2017

B.3.1.2 [17020] ISO/IEC 17020, Conformity assessment - Requirements for the operation of various types of bodies performing inspection, March 1, 2012

B.3.1.3 [17065] ISO/IEC 17065, Conformity assessment - Requirements for bodies certifying products, processes, and services, September 15, 2012

B.4 Other references

B.4.1.1 *Quick Start Guide: An Overview of ISA/IEC 62443 Standards*, ISAGCA Quick Start Guide FINAL.pdf

B.4.1.2 *Quick Start Guide: An Overview of ISASecure® Certification*, 0920-ISASecure-QuickStart-Guide-FINAL.pdf

B.4.1.3 Control System Cyber Security Association International (CS2AI.org) *2024 OT Technology Cyber Security Report*. https://www.cs2ai.org/annual-reports