ACSSA-100

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

ISASecure inspection and certification schemes

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	2026.01.12	Initial version available at https://ISASecure.org

Contents

1 Scope 6
2 Normative references 8
2.1 General 8
2.2 Accreditation 8
2.3 ISASecure symbol and certificates 8
2.4 Technical specifications 8
2.5 External references 9
3 Definitions and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 15
4 ISASecure ACSSA inspection and certification schemes 15
4.1 Eligibility for ACSSA 15
4.2 Comparison of ACSSA inspection and certification schemes 16
4.3 Use cases: inspection and certification 17
4.4 Overview of process for ACSSA inspection 17
4.5 Overview of process for ACSSA certification 17
4.6 ACSSA certified IACS 18
4.7 ACSSA and other 62443 certifications 18
4.8 Organizational roles 20
4.9 Inspection and certification scheme documentation 21

Table of Figures

Figure 1. Reference standards for ACSSA requirements 6
Figure 2. Certification vs. inspection program 16
Figure 3. ISASecure ACSSA documents 22

Bibliography 26

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 is the highest-level document that describes two ISASecure schemes referred to under the name ACSSA (Automation and Control System Security Assurance). The ACSSA inspection scheme and the ACSSA certification scheme both evaluate an IACS as deployed for an accountable asset owner. This document enumerates all documents that define these schemes, and describes the scope of each of these defining documents. ISCI also offers programs that evaluate 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.

1 Scope

This document provides an overview of the operation of the ISASecure ACSSA (Automation and Control System Security Assurance) inspection and certification programs, the roles of all organizations that participate in carrying out these two programs, and the documents that define participant roles as well as the technical aspects of the programs. This document also provides an overview of the ACSSA evaluation process used in the programs, and requirements for ACSSA certification of an IACS (Industrial Automation and Control System) which has been deployed for an accountable asset owner. ACSSA applies to an IACS either in operation, or near the transition to that lifecycle phase (see Section 4.1).

ACSSA evaluation requires a partition of the IACS into security zones. An IACS is eligible for ACSSA programs, if the asset owner seeking ACSSA evaluation is fully accountable for managing, operating, and maintaining all hardware and software within these zones, and for all ingress/egress points for external communication and communication between zones. In the case that cyber elements that do not meet these criteria have an interface to an IACS (which may include but are not limited to public cloud applications and infrastructure components), the IACS with scope defined to exclude those elements is eligible for ACSSA. For such an evaluation, the evaluator will verify that the asset owner's risk assessment has examined threats due to this interface, as specified in ACSSA-300 [ACSSA-300].

Future versions of ACSSA will evolve along with the ISA/IEC 62443 standards to address the unique risks of cloud implementations of IACS functions, so that such systems inclusive of their cloud-based functionality will become eligible for ACSSA under future releases of the programs.

NOTE 1 Another common example IACS is a SCADA system (supervisory control and data acquisition) where all supervisory elements and distributed elements are fully managed, operated and maintained by the asset owner, but connections between central and distributed elements use an infrastructure not dedicated to the SCADA system. This system could be eligible for ACSSA if the ingress/egress points for this communication are also fully managed, operated, and maintained by the asset owner.

The same evaluation method for an IACS is used under the ACSSA inspection scheme and the ACSSA certification scheme. An ACSSA evaluation references four parts of the ANSI/ISA/IEC 62443 series of standards shown in Figure 1. The leftmost arrows indicate that a security risk assessment is an aspect of an asset owner's security program such that its results drive other aspects of that program. The other arrows in the figure indicate that the security program both influences and is influenced by, the asset owner's use of service providers and technical system capabilities to meet security requirements.

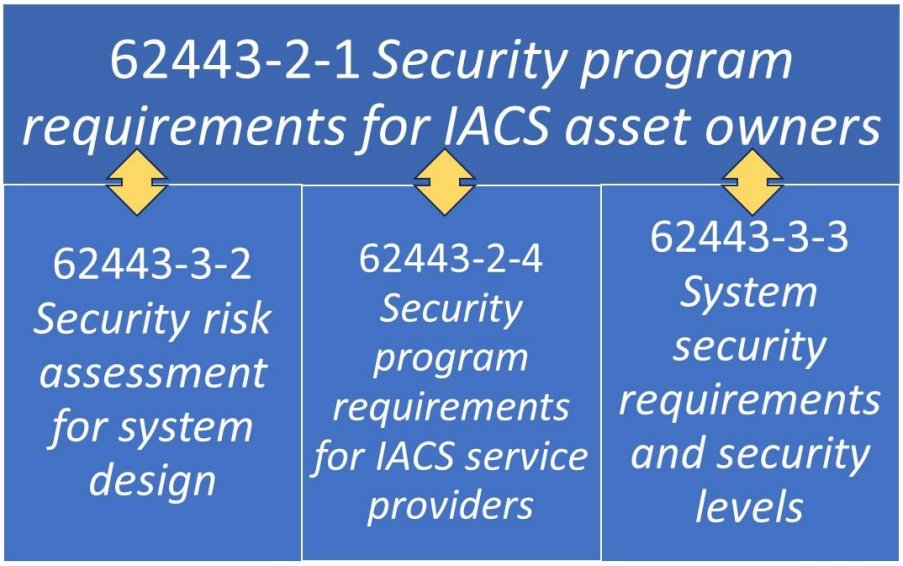

Figure 1. Reference standards for ACSSA requirements

The description in this document of requirements for the ACSSA programs is at a summary level, providing an overview of the programs. All ACSSA program requirements are formally detailed as numbered requirements in other ACSSA scheme documents. All scheme documents are described in Section 4.9.

Conformity to the standards in Figure 1 is evaluated as follows:

- **62443-2-1 [IEC 62443-2-1] conformant policies and procedures:** The evaluator will verify that the asset owner has policies and procedures in place for their security program for the IACS, that meet the requirements for asset owners in 62443-2-1.

- **62443-3-2 [IEC 62443-3-2] conformant risk assessment policies and procedures:** The evaluator will verify that a risk assessment has been carried out for the IACS in accordance with documented policies and procedures that conform to 62443-3-2.

- **62443-2-4 [IEC 62443-2-4] conformant support from service providers:** The evaluator will identify cases where a service provider is responsible for processes that deliver capabilities described in this standard, for the IACS under evaluation. In these cases, the evaluator will verify that these processes, as applied for this IACS, conform to this standard. This is distinct from a conformity assessment using this standard that provides a general review of the capabilities of a service provider organization to serve its clients in accordance with the standard. A service provider can be an external organization under contract to the asset owner. A service provider can also be an organization internal to the asset owner, for which a description of IACS responsibilities exists, and which the asset owner has elected for evaluation to 62443-2-4 as a service provider under ACSSA. ACSSA will also review subcontractors under these external or internal organizations.

  NOTE 2 If a service for the IACS is performed by the asset owner themselves, the internal organization performing the service will not be evaluated under 62443-2-4 unless requested of the ACSSA conformity assessment body by the asset owner. If this is not requested, the asset owner organization performing the service will be evaluated to all 62443-2-1 requirements, which include those that are impacted by the performance of that service.

- **62443-3-3 [IEC 62443-3-3] conformant control system:** The evaluator will verify that the asset owner has configured and is utilizing technical capabilities described in 62443-3-3 provided by the hardware and software control system for the IACS. The evaluator will verify alignment with the results of the asset owner's risk assessment, and with the policies and procedures of their security program. This is distinct from a conformity assessment of a product using this standard, that evaluates whether the product has the capabilities described in the standard. Such an assessment is not intended to examine the utilization of these capabilities in the context of a specific IACS deployment; whereas this is the intent for ACSSA.

The detailed specifications that describe an ACSSA evaluation are the documents ACSSA-300, ACSSA-304 [ACSSA-304], and ACSSA-311 [ACSSA-311], listed in Section 2. The differences between the ACSSA inspection and certification schemes are described in Section 4.2.

The ISASecure conformity assessment programs have been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cyber security for IACS. The ISASecure ACSSA conformity assessment programs achieve this goal by offering a common industry-recognized method for evaluating conformity to 62443 for an IACS. An asset owner that achieves ACSSA certification for an IACS, can display the ISASecure ACSSA symbol in association with that IACS.

ISCI also offers product and product development process certification programs for:

- IACS components, the ISASecure CSA program (Component Security Assurance), which evaluates conformity of component products with 62443-4-2 [3] [4], including a requirement for conformity of development process with 62443-4-1 [1] [2]

- IIoT devices and gateways, the ICSA program (IIoT Component Security Assurance), which evaluates conformity with 62443-4-2 including 62443-4-1, with exceptions and extensions for the IIoT environment

- Control systems, the ISASecure SSA program (System Security Assurance), which evaluates conformity of system products with 62443-3-3, including a requirement for conformity with 62443-4-1

- Secure product development lifecycle, the SDLA program (Security Development Lifecycle Assurance), which evaluates product supplier conformity with 62443-4-1.

ACSSA evaluates a deployed control system and related asset owner policies and procedures. Other 62443 conformity assessment programs offered by ISASecure and others, evaluate off-the-shelf products based on 62443-3-3 and 62443-4-2, and development lifecycle process based on 62443-4-1. Achievement of these certifications for components and systems that are part of an asset's owner's IACS is not a prerequisite for meeting ACSSA requirements. However, use of products certified to ANSI/ISA/IEC 62443 will be beneficial for attaining ACSSA certification, as described below in 4.7.

Information for these product and process certification schemes can be found at https://ISASecure.org.

2 Normative references

NOTE Section 4.9 provides a diagrammatic and expository overview of the ISASecure ACSSA documents and their relationships. All ACSSA documents include information relevant to both the ACSSA inspection scheme and the ACSSA certification scheme, with the exception of [ACSSA-205] which provides an editable ACSSA certificate format, applicable to the certification scheme only.

2.1 General

NOTE The following document lists all document titles and versions that define ACSSA 1.0.0. It is reissued to list any errata or updated versions subsequently issued for the baseline documents.

[ACSSA-102] *ISA Security Compliance Institute Automation and Control System Security Assurance – Baseline document versions and errata for ACSSA 1.0.0 specifications,* available at https://ISASecure.org

2.2 Conformity assessment body operations and accreditation

NOTE The following documents describe how to achieve conformity assessment body status and operate as an ISASecure ACSSA inspection body and/or certification body, referred to jointly as conformity assessment bodies.

[ACSSA-200] *ISA Security Compliance Institute Automation and Control System Security Assurance – Operations and accreditation for conformity assessment bodies*, available at https://ISASecure.org

[ACSSA-304] *ISA Security Compliance Institute Automation and Control System Security Assurance – Evaluation planning and execution*, available at https://ISASecure.org

[ACSSA-305] *ISA Security Compliance Institute Automation and Control System Security Assurance – Sample evaluation plan*, available at https://ISASecure.org

2.3 ISASecure symbols and certificates

NOTE The following document describes the ISASecure symbols and certificates and how they are used for the ISASecure ACSSA programs.

[ACSSA-204] *ISA Security Compliance Institute Automation and Control System Security Assurance – Instructions and policies for use of ISASecure symbols and certificates*, available at https://ISASecure.org

[ACSSA-205] *ISA Security Compliance Institute Automation and Control System Security Assurance – Certificate Document Format,* available at https://ISASecure.org

2.4 Technical specifications

NOTE 1 This section includes the specifications that define technical criteria for evaluating an IACS under the ACSSA inspection or certification program.

[ACSSA-300] *ISA Security Compliance Institute Automation and Control System Security Assurance – Inspection and certification requirements,* available at https://ISASecure.org

[ACSSA-303] *ISA Security Compliance Institute Automation and Control System Security Assurance – Sample inspection and certification reports*, available at https://ISASecure.org

NOTE 2 The following document provides the detailed technical evaluation criteria for an ACSSA inspection or certification of an IACS.

[ACSSA-311] *ISA Security Compliance Institute Automation and Control System Security Assurance – Evaluation methods,* available at https://ISASecure.org

2.5 External references

External references are documents that are used by the ISASecure ACSSA program but maintained outside of the ISASecure program.

2.5.1 ANSI/ISA/IEC 62443 security standards

NOTE The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC. In this document, the designation "62443-m-n" is used to reference the technical content of one of these standards.

[ANSI/ISA-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*

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

[ANSI/ISA-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*

[IEC 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*

[IEC 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*

[ANSI/ISA-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*

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

[ANSI/ISA-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*

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

2.5.2 International standards for certification programs

NOTE The following international standards apply to the ISASecure ACSSA inspection and certification processes.

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

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

2.5.3 International standards for accreditation programs

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies,*" November 2017

3 Definitions and abbreviations

3.1 Definitions

3.1.1
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]

3.1.2
accreditation body
authoritative body that performs accreditation

[SOURCE: ISO/IEC 17000:2020]

3.1.3
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]

3.1.4
attestation
issue of a statement, based upon a decision, that fulfillment of specified requirements has been demonstrated

NOTE The resulting statement, referred to in ISO/IEC 17000 as a "statement of conformity", is intended to convey the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, provide contractual or other legal guarantees.

[SOURCE: ISO/IEC 17000:2020]

3.1.5
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.

3.1.6
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]

3.1.7
certification body
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]

3.1.8
certification scheme
overall definition of and process for operating a certification program

3.1.9
cloud
collection of networked remote servers

NOTE In this document, “remote” is relative to a reference point. A “remote” server is a server such that the communication path to that server from the reference point is not fully under the control of the organization using the communication path.

[SOURCE: ISO 20294:2018, 3.5.8, note added]

3.1.10
commission
bring (something newly produced, such as a factory or machine) into working condition

[SOURCE: Oxford Languages]

3.1.11
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

NOTE Definitions for these component types are found in 62443-4-2 [3] [4].

[SOURCE: 62443-4-2:2018]

3.1.12
conformity assessment
demonstration that specified requirements are fulfilled

[SOURCE: ISO/IEC 17000:2020]

3.1.13
conformity assessment body
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]

3.1.14
conformity assessment scheme
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]

3.1.15
control system
hardware and software components of an IACS

[SOURCE: 62443-3-3:2013]

3.1.16
gap analysis
review to provide information about requirement areas that may need attention in order to support a desired statement of conformity

3.1.17
equipment under control
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

[SOURCE: 62443-1-1:2007]

3.1.18
impartiality
objectivity with regard to the outcome of a conformity assessment activity

NOTE Objectivity can be understood as freedom from bias or freedom from conflicts of interest.

[SOURCE: ISO/IEC 17000:2020]]

3.1.19
industrial automation and control system
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]

3.1.20
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]

3.1.21
inspection body
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]

3.1.22
integration service provider
service provider that provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover

NOTE Integration service providers are often referred to as integrators or Main Automation Contractors (MAC).

[SOURCE: 62443-2-4:2023]

3.1.23
maturity level
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]

3.1.24
pass/passing
meet/meeting the criteria for passing an ISASecure evaluation as defined within the technical ISASecure specifications

3.1.25
product
system, subsystem or component that is manufactured, developed or refined for use by other products and/or users

NOTE Adds “and/or users” to definition from source.

[SOURCE : 62443-4-1:2018]

3.1.26
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]

3.1.27
provisional conformity assessment body status
interim, temporary recognition status granted by ISCI during which a conformity assessment body is authorized to perform evaluations and grant ISASecure certifications per program procedures

NOTE ISCI grants provisional CAB recognition status for an ISASecure ACSSA inspection body or certification body when an ACSSA accreditation body has assessed all requirements as passing, but has not yet formalized the accreditation of the inspection or certification body.

3.1.28
security level
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 associated to security capabilities that can be selected to defend against attackers with those characteristics.

[SOURCE: 62443-3-2:2020]

3.1.29
security program
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures and products that are applicable to the IACS

NOTE The security program for IACS asset owners refers to the policies and procedures defined by them to address cyber security concerns of the IACS. This can include physical security measures used to reduce the cyber security attack surface.

[SOURCE: 62443-2-1:2024]

3.1.30
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]

3.1.31
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]

3.1.32
statement of conformity
See NOTE to definition for **attestation**.

3.1.33
surveillance
systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity

[SOURCE: ISO/IEC 17000:2020]

3.1.34
symbol
graphic or text affixed or displayed in accordance with program rules to designate conformity assessment body participation or client achievements under an ISASecure conformity assessment program

NOTE An earlier term for symbol is “mark.”

3.1.35
version of ISASecure inspection or certification
ISASecure conformity assessment criteria in force at a particular point in time, defined by the set of specification versions that define the conformity assessment program, and identified by a three-place number, such as ISASecure ACSSA 1.0.0

3.1.36
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document.

ACSSA	Automation and Control System Security Assurance
ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CAB	conformity assessment body
CB	certification body
CSA	Component Security Assurance
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
IB	inspection body
ICSA	IIoT Component Security Assurance
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
ILAC	International Laboratory Accreditation Cooperation
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
ML	maturity level
SCADA	supervisory control and data acquisition
MRA	Multilateral Recognition Arrangement, Mutual Recognition Arrangement
SDLA	Security Development Lifecycle Assurance
SSA	System Security Assurance

4 ISASecure ACSSA inspection and certification schemes

4.1 Eligibility for ACSSA

Asset owners responsible for an IACS can apply for ACSSA inspection or certification, if the IACS is either in operation, or near transition to operation. “Near transition to operation” means that the asset owner can supply information submissions and meet other preparedness criteria defined in the ACSSA specifications. Examples of required submissions are a system asset inventory under change control and a risk assessment for the IACS performed in accordance with 62443-3-2. Examples of other required preparedness criteria are completion of commissioning and availability of policies and procedures for conformity with 62443-2-1. Detailed ACSSA eligibility criteria for an IACS are specified in ACSSA-300.

The scope of the IACS itself that is the subject for evaluation, is determined by the asset owner. The required submission of documentation to define this scope is also found in ACSSA-300. Examples are asset inventory for the system under evaluation, list of equipment under control, policies and procedures, and list of service providers.

4.2 Comparison of ACSSA inspection and certification schemes

The present document contains information that applies to both the ACSSA inspection and certification schemes. Figure 2 shows the relationship between these schemes. The term “conformity assessment body” (CAB) is used, as in the figure below, when referring to either an inspection body (IB) or certification body (CB) for ACSSA.

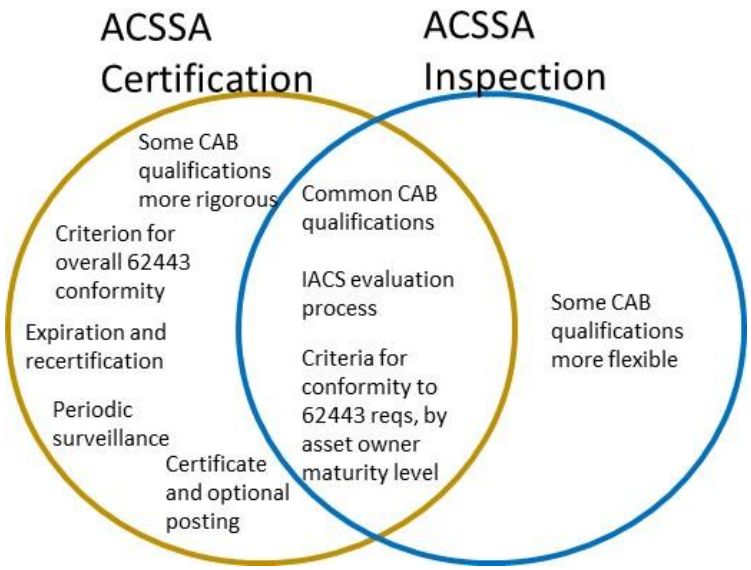

Figure 2. Certification vs. inspection program

Evaluation process and criteria for conformity with individual 62443 requirements are identical for ACSSA inspection and for an initial ACSSA certification. Key differences between the two programs address the following other program aspects:

- **Conformity statements:** Under the ACSSA inspection and certification programs, requirements in 62443-2-1 are evaluated according to the same specified criteria, and evaluated either as practiced at maturity level 3 (ML 3), at maturity level 2 (ML 2), or as not meeting ML 2. 62443-2-4, 62443-3-2, and 62443-3-3 requirements associated with each 62443-2-1 requirement must also be met based on specified criteria that support the maturity level that the evaluator determines is met for that 62443-2-1 requirement. Conformity to 62443-3-3 requirements must also be aligned with the security level assigned per the asset owner’s risk assessment to each security zone of the system under evaluation.

  NOTE 1 An ACSSA inspection body may also offer evaluation to ML 1 as an option. This can provide useful information to the asset owner; it does not support a statement of conformity or certification. At this time ACSSA does not specify criteria for evaluating ML 4. Such an IACS would be evaluated as meeting ML 3.

  NOTE 2 Scheme specification ACSSA-311 enumerates “associated requirements” for each requirement in 62443-2-1.

  Based upon such an evaluation, an ACSSA inspection program result attests to conformity of an IACS to individual requirements in the 62443 standards. There is no formal designation for passing an ACSSA inspection overall. An inspection attests to conformity of an IACS with requirements in the standards 62443-2-1, 62443-2-4, 62443-3-2, and 62443-3-3. The titles for these standards are shown in Figure 1.

  An ACSSA certification attests to overall conformity of an IACS with 62443. In particular, it attests to conformity of an IACS with the standards 62443-2-1, 62443-2-4, 62443-3-2, and 62443-3-3. The certification program defines criteria for granting certification to an IACS based upon the results of the ACSSA evaluation. Specifically, 62443-2-1 and 62443-3-2 requirements must be met at ML 3. 62443-2-4 and 62443-3-3 requirements associated with each 62443-2-1 requirement must also be met, based

on criteria that support asset owner ML 3 for the 62443-2-1 requirement. ACSSA does not offer certification for ML 1 or ML 2.

NOTE 3 Although 62443-3-2 does not discuss a concept of maturity level, for ACSSA all requirements in that part of the standard are viewed as sub requirements under the 62443-2-1 requirement ORG 2.1 *Security risk mitigation.* From the 62443-2-1 rationale for ORG 2.1: "See ISA-62443-3-2 for more information about risk assessments and risk tolerance." Therefore the 62443-2-1 concept of maturity level is applied when defining criteria for ML 2 and ML 3 for 62443-3-2 requirements.

- **Time aspect of statement of conformity:** Both inspections and certifications provide a report that documents evaluation results at a point in time. However, a certification is valid over a specified time period, requires periodic review during that time period (known as surveillance), and offers a recertification process to further maintain the certification beyond that time period, as specified in ACSSA-300 [ACSSA-300].

- **Qualifications for IB vs. CB**: Impartiality requirements are more rigorous for an ACSSA CB than for an ACSSA IB. An IB may work sequentially on both consulting and inspection for the same subject IACS, as long as the work is done by different individuals and impartiality is maintained. A CB (as a legal entity) cannot offer or perform both related consulting and certifications.

  NOTE 4 In specific terms, ACSSA inspection bodies are qualified and operate under the standard [ISO/IEC 17020], in accordance with the requirements for a Type A or Type C inspection body as defined in that document. Certification bodies are qualified and operate in accordance with the standard [ISO/IEC 17065]. See also 4.9.3. An organization may qualify as both an IB and a CB under ACSSA program rules. These topics are fully covered in the ACSSA specification [ACSSA-200].

4.3 Use cases: inspection and certification

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 ready for operation. They may schedule future inspections as they see fit, to measure progress. An ACSSA inspection could be used to extend or confirm efforts by internal audit resources of the asset owner organization.

An asset owner organization might use a *certification* as part of a long-term public commitment to maintain their security program, or because an external entity offers benefits for maintaining a certification, or an external entity requires a certification under some circumstances. Examples of such external entities could be customers, insurance providers, or regulators that work with the asset owner organization.

4.4 Overview of process for ACSSA inspection

To obtain an ACSSA inspection, an asset owner applies to an accredited IB for inspection of a specified IACS. The IB determines eligibility of the IACS in accordance with requirements of ACSSA-300. Once eligibility is established, the asset owner and CAB create an evaluation plan. After execution of the agreed plan and evaluation of the IACS is complete, the asset owner will receive a cover letter from the IB that attests to completion of the evaluation, which references the resulting report. The asset owner will receive a formal ACSSA inspection report conforming to the ACSSA-specified format and content defined in ACSSA-303 [ACSSA-303]. The report provides statements of conformity to individual 62443 requirements as described in Section 4.2, and descriptions of any nonconformities found.

ISCI will not publish information about IACS and identities of asset owners that have undergone ACSSA evaluation under the ACSSA inspection program. With asset owner permission, this can be done by the IB. 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 [ACSSA-200]. In this case, an asset owner may request ISCI publication of an ACSSA certificate granted as discussed in Section 4.5.

4.5 Overview of process for ACSSA certification

To obtain an ACSSA certification, an asset owner applies to an accredited 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 planned and completed, then 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 a formal certification report. The certification report includes the contents that comprise a formal inspection report, as described in Section 4.4. A periodic surveillance process specified in ACSSA-300, is required to maintain the certification until its expiration date. A recertification process is required to extend the certification beyond the expiration date. At this time a new certificate and certification report are issued.

Note that an IACS is evaluated to the same criteria whether or not it is in operation. However, for some requirements, evidence available to demonstrate conformity may differ. In these cases, the ACSSA specifications allow for several types of evidence.

4.6 ACSSA certified IACS

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 [ACSSA-204]. A certification references a 3-digit certification version that identifies the set of ISASecure specifications used for the certification. For example, the ABC Company IACS at City Y, might be certified to ISASecure ACSSA 1.0.0.

At the request of an asset owner organization, ISCI will post on its web site https://ISASecure.org, the name of the asset owner organization and the information on their certificate(s) that are in valid status. 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.

4.7 ACSSA and other 62443 certifications

This section discusses the relationship of ACSSA to other 62443 certifications. An asset owner will gain significant leverage for conformity to ACSSA criteria, by employing system products that conform to 62443-3-3, component products that conform to 62443-4-2, and service providers that conform to 62443-2-4. They gain further leverage for demonstrating this conformity in an ACSSA evaluation, if these products and service providers are certified for conformity to these standards. Examples are products certified under ISASecure CSA or ISASecure SSA, and a maintenance service provider that holds a 62443-2-4 certification for their vulnerability scanning services. The use of vendors with these achievements, though not required by ACSSA, may fulfill in part the requirements for the 62443-3-3 and 62443-2-4 elements of an ACSSA evaluation. The following discussion outlines those aspects of the ACSSA requirements that are fulfilled by conformity and certification to these individual parts of the 62443 standard, and the aspects that remain to be met, to pass the 62443-3-3 and 62443-2-4 elements of an ACSSA evaluation.

NOTE Conformity of components in a zone to 62443-4-2 contributes to conformity of the zone to 62443-3-3 due to the relationship between those standards. In most cases, a security capability required under 62443-4-2 is a component capability that has been derived from a parallel system capability found in 62443-3-3.

4.7.1 Product certifications

ACSSA ML 3 criteria for a 62443-3-3 requirement examine the utilization of required technical capabilities in a zone based upon its target security level and upon any additional requirements resulting from the asset owner's risk assessment. The existence of a required capability in a zone and the verification that it is appropriately utilized are both examined in an ACSSA evaluation. Certification of system products to 62443-3-3 and component products to 62443-4-2 contribute evidence that required technical capabilities exist in a product, and therefore are present in a zone containing the product. Such certifications review a product as it is offered for sale, and therefore do not examine whether or how a specific user utilizes product capabilities.

It is logical for an evaluator to examine first whether a product has a security capability, and then to examine how the capability is configured and utilized in the IACS under evaluation. For the first step, a zone that supports a security capability may be shown to support it either using evidence from prior product certifications, or by direct evaluation by the ACSSA evaluator. The former method is expected to make the ACSSA evaluation process more efficient.

If an IACS zone is comprised of products that do not have a capability required by 62443-3-3 for the target security level of that zone, then in order to pass the ACSSA evaluation, the asset owner will need to either provide a risk-based rationale, or identify, deploy, and provide rationale for compensating security measures to compensate for the risk which that capability would have mitigated if present. An asset owner will not need to perform these actions if they deploy products that support security capabilities required under 62443-3-3 or 62443-4-2 for the security level of the zone. This does not necessarily mean that all products in the zone need these capabilities, or need a related certification. In some cases, a subset of products in a zone may support a capability for the entire zone. For example, several devices in the zone may not have sufficient audit storage, but forward their logs to another storage device in the zone when their storage space is exceeded. Likewise, only one device in a zone may have the capability to identify and report unauthorized wireless devices, but it is configured to have visibility to all zone communication.

In summary, in order to evaluate a zone for a specific 62443-3-3 requirement, the ACSSA evaluator would first verify that either (1) the capability described by that requirement is present and supports the entire zone (2) compensating security measures are present, or (3) a risk-based rationale has been provided that the capability is not required in the zone. Assurance of the support of the security capability for the zone for (1) can most easily be based upon certifications for products in the zone. The evaluator may then commence verification that the capability is configured and utilized in accordance with asset owner policies and procedures, which will complete the ACSSA evaluation of the 62443-3-3 requirement for the zone.

NOTE It is often the case that if all components or systems that comprise a zone conform to 62443-4-2 or 62443-3-3, then the overall zone conforms to 62443-3-3. However, this is not universally true, so verification of conformity for the zone is still required by the evaluator in this case. For example, different components in the zone may have incompatible implementations for the same requirement, so that the overall zone cannot be supported by using all of those features together.

Conversely, an IACS passing an ACSSA evaluation does not imply that systems or components used by that asset owner should receive a 62443-4-2 or 62443-3-3 certification, although they will be well positioned to apply. All security capabilities required under these standards may not be necessary for a particular IACS, so their presence may not be examined under ACSSA. Further, product certifications such as ISASecure CSA or ISASecure SSA examine not only the presence of security capabilities, but additional details of their implementation and artifacts from the application of a secure product development process for that product. These certification programs also incorporate independent tests by the evaluator for selected product security capabilities, and perform an aggressive form of vulnerability scanning. ACSSA evaluation for deployed systems does not incorporate such independent tests by the evaluator.

4.7.2 Service provider certifications

An asset owner can pass ACSSA ML 2 criteria for a 62443-2-4 requirement, if they employ a service provider for a task to which that requirement applies, that is certified to 62443-2-4 at ML 3 for that 62443-2-4 requirement.

NOTE Specific conditions to be met by the 62443-2-4 certification program are detailed in ACSSA-300.

If a service provider does not have an ML 3 certification for a 62443-2-4 requirement, but has a documented process intended to fulfill the requirement, this process may be presented as evidence to the ACSSA evaluator. However, ACSSA does not accept an ML 2 62443-2-4 certification to meet ML 2 ACSSA requirements.

In order to pass ACSSA ML 3 criteria, in addition to ML 2 evidence as just described, there must be evidence that the task to which a 62443-2-4 requirement applies was carried out by the service provider, specifically for the IACS under evaluation. Although the service provider's ML 3 certification would have required evidence of service provider execution of their process, that evidence may have been for other IACS and not for the IACS under ACSSA evaluation.

Conversely, documented processes of the service provider and evidence of their execution for the asset owner that have been presented under an ACSSA evaluation, may be submitted as evidence to support a 62443-2-4 certification for a service provider. However, an IACS passing an ACSSA evaluation does not imply that a service provider for that asset owner should receive a 62443-2-4 certification. The service provider's process used for an IACS asset owner and evidence of execution of that process would need to be evaluated by a

62443-2-4 certification body for sufficiency in a broader context than the specific IACS undergoing an ACSSA evaluation.

4.8 Organizational roles

The following organizations participate in the ISASecure ACSSA program.

- **Asset owners** are accountable for an IACS. They may define the boundaries of an IACS and apply for an ACSSA inspection or certification for the IACS. They may use passing an ACSSA certification as an internal goal, or to demonstrate the IACS security posture to external stakeholders. They may use information from a formal ACSSA inspection, or information derived from their internal use of the ACSSA specifications, to inform their security program.

- **Integration service providers** may be asked by an asset owner to serve as sources for existing or new system documentation, based upon work they performed previously during the integration phase for an IACS under evaluation.

- **Maintenance service providers** may be asked by an asset owner to serve as sources for maintenance process documentation and evidence of process execution for an ACSSA evaluation. If a maintenance service provider holds a suitable 62443-2-4 certification at ML 3, for requirements in that standard applicable to the tasks they will carry out for the IACS under evaluation, this certification contributes evidence for conformity to those requirements under ACSSA. Evidence in addition to this certification may be required to demonstrate conformity specifically for the IACS under evaluation. (See also 4.7 for further discussion of the relationship of ACSSA to other 62443 certifications.)

- **Product suppliers** may be asked by an asset owner to serve as sources for specific information about the capabilities of products used in the IACS, that is required as evidence for an ACSSA evaluation. ACSSA evaluation examines the asset owner's utilization of technical capabilities to meet the target security level of a zone. If a supplier of products for that zone holds a suitable 62443-4-2 or 62443-3-3 certification for such a product, that certification provides evidence that required capabilities for the zone are present for that product. The evaluator may then efficiently commence examination of the utilization of these capabilities by the asset owner. (See also 4.7.)

- **Conformity assessment bodies** (IBs and CBs) may accept an application from an asset owner for ACSSA evaluation of an IACS, and evaluate the IACS. IBs are authorized to issue formal ACSSA inspection reports. CBs are authorized to grant ACSSA certifications and issue ACSSA certification reports and certificates when certification criteria are met.

- **ISCI** defines, maintains and manages the overall ISASecure ACSSA inspection and certification programs, interprets the ISASecure specifications and maintains a web site to make program documentation available. The ISCI website also provides a list of conformity assessment bodies. When requested by an asset owner, an ACSSA certificate achieved by the asset owner is posted on the site or provided directly to specified third parties.

- **ASCI** (Automation Standards Compliance Institute)**,** as the legal entity representing ISCI, grants ACSSA IB and/or CB status to applicant organizations based on successful accreditation to criteria defined by ISCI.

- **ACSSA accreditation bodies** evaluate candidate organizations for ACSSA IB or CB status and determine if they meet program accreditation criteria.

- **External stakeholders for IACS security** such as insurance companies or closely connected business partners for an asset owner, may use results of a formal ACSSA inspection or achievement of a certification for a specific IACS, to assess the risk they themselves may encounter, that is influenced by the security posture of the IACS.

Note that an individual security consultant, or an organization selling consulting services or tools, performing research, or related activities, may use ACSSA specifications that have been licensed in accordance with ISCI terms, to assist their clients in attaining or promoting 62443 conformity. However, the privilege to issue authorized ACSSA inspection reports, certifications, or other conformity claims under the ACSSA name is limited to accredited ACSSA IBs and CBs. Licensing terms for the ACSSA specifications are found on the ISASecure website: https://ISASecure.org.

ISCI is organized as an interest area within ASCI, a not-for-profit 501 (c) (6) corporation owned by ISA (International Society of Automation). Descriptions of the governance and organizational structure for ASCI are found on the ISASecure website: https://ISASecure.org.

As described in ACSSA-200, in order to accredit ACSSA CBs, an accreditation body is required to be a signatory to the IAF Multilateral Recognition Arrangement (IAF MRA). In order to accredit ACSSA IBs, an accreditation body is required to be a signatory to the ILAC Mutual Recognition Arrangement (ILAC MRA).

Information related to ISASecure evaluations is private to conformity assessment bodies performing these evaluations, and is not disclosed to ASCI/ISCI, except as explicitly permitted by the asset owner for an IACS under evaluation, or for cause in ASCI/ISCI's role as manager of the ACSSA program.

4.9 Inspection and certification scheme documentation

4.9.1 Overview of documentation

Figure 3 shows the documents that define the ISASecure ACSSA inspection and certification programs. An arrowhead represents a referential dependency of a document on the contents of another document. Refer to Section 2 for the detailed listing of these documents. All ACSSA-nnn documents in the figure include content that applies to both the ACSSA inspection scheme and the ACSSA certification scheme. Applicability of specific content to these programs is indicated in each document.

In addition to these normative documents, the document ACSSA-101 *ISCI ACSSA – Evaluation planning for the asset owner* ([5] in the bibliography) provides informative guidance for an asset owner interested in preparing for an ACSSA evaluation.

NOTE The figure depicts all documents in Section 2 with the exception of the document version and errata list [ACSSA-102], and certificate form [ACSSA-205].

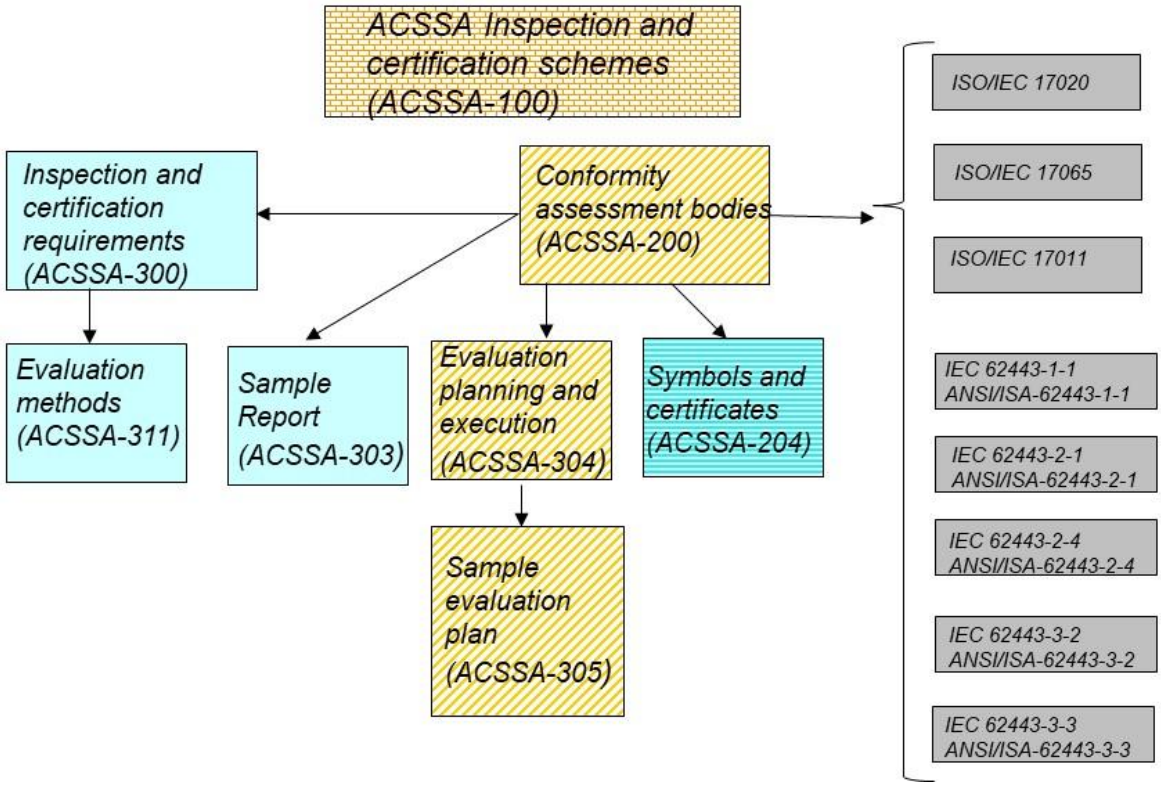

Figure 3. ISASecure ACSSA documents

There are five major categories of ISASecure ACSSA program documents:

- **Technical specifications**, shown with no pattern in light blue, that describe the technical criteria applied to determine conformity to 62443
- **Conformity assessment bodies**, shown in gold diagonal stripe, that describe how an organization can become a recognized ACSSA inspection body or certification body and carry out this role
- **Symbols and certificates**, shown in blue horizontal stripe, covers the topic of proper usage of the ISASecure symbols and certificates
- **Structure,** shown in an orange brick pattern, used to describe the overall ACSSA inspection and certification schemes. The present document falls in this category.
- **External references**, shown with no pattern in dark grey, are documents that apply to the ISASecure program but are maintained outside of the program.

The following sections describe all documents in each category in further detail.

4.9.2 Technical specifications

The document *ACSSA-300 ISCI ACSSA – Inspection and certification requirements,* defines at a high level the technical criteria for IACS conformity to 62443 under both the ACSSA inspection and certification programs, by reference to *ACSSA-311 ISCI ACSSA – Evaluation methods* [ACSSA-311]. ACSSA-300 also defines the concepts of certification validity period and periodic surveillance activity for a certified IACS to maintain its ACSSA certification over time. ACSSA-311 defines the criteria used to determine whether an IACS conforms

to each individual requirement in 62443-2-1 at asset owner ML 2 or 3. The conformity criteria in ACSSA-311 for a 62443-2-1 requirement include conformity criteria for associated requirements in other parts of 62443 (62443-2-4, 62443-3-2, 62443-3-3) that must be met to claim conformity to a requirement in 62443-2-1 at each asset owner maturity level.

ACSSA-311 includes all requirements that appear in either 62443-2-1, 62443-2-4, 62443-3-2, or 62443-3-3. It also adds a few additional requirements. These are requirements for asset owner policies and procedures that describe when and how to use a technical system capability that appears in 62443-3-3. Such "policy and procedure support" requirements are added for cases in which the existing 62443-2-1 standard does not require such related policies and procedures for some 62443-3-3 technical capability. Requiring these policies and procedures allows evaluation of whether a technical capability has been utilized appropriately in a system under evaluation.

These documents are used by:

- asset owners, to understand the criteria against which an IACS will be evaluated under ACSSA, and if a certification is achieved, how to maintain it
- integration service providers, to understand how their activities and outputs performed during the integration phase can support demonstration of conformity under ACSSA
- maintenance service providers, to understand how their plans and activities are evaluated under ACSSA, for an IACS for which they will be providing maintenance services
- product suppliers, to understand how their product capabilities, documentation, and certifications can support demonstration of conformity under ACSSA
- inspection bodies and certification bodies, to define ACSSA evaluation criteria and processes they will carry out
- ACSSA accreditation bodies, as the end reference for technical readiness assessment requirements when evaluating candidate organizations for inspection body or certification body status.

The ACSSA evaluation report requirements embodied in the sample report *ACSSA-303 Sample inspection and certification reports* [ACSSA-303] will be followed by inspection bodies and certification bodies. This sample document provides asset owners, external stakeholders, service providers, and component/system suppliers with an understanding of the type of information that will be provided to asset owners following all ISASecure ACSSA evaluations.

4.9.3 Conformity assessment bodies

ISASecure ACSSA conformity assessment bodies, which are inspection bodies and certification bodies, implement the technical aspects of the inspection and certification programs. The documents in this category define how they obtain and carry out these roles.

ACSSA-200 ISCI ACSSA – Operations and accreditation for conformity assessment bodies describes the accreditation criteria and process that organizations will follow to become an ACSSA inspection and/or certification body. To be granted full status as an inspection body for the ISASecure ACSSA program, an organization shall attain the following internationally recognized accreditation, performed by an ACSSA accreditation body:

- accredited to ISO/IEC 17020 (to either type A or type C as described in that standard), with technology scope of accreditation covering the ISASecure ACSSA inspection scheme.

To be granted full status as a certification body for the ISASecure ACSSA program, an organization shall attain the following internationally recognized accreditation, performed by an ACSSA accreditation body:

- accredited to ISO/IEC 17065, with technology scope of accreditation covering the ISASecure ACSSA certification scheme.

ASCI grants provisional recognition to an organization when an accreditation body informally reports to ISCI that the candidate organization has met all requirements for accreditation. Full inspection or certification body status is granted when the accreditation body formally grants the above accreditations to the candidate organization.

ACSSA-200 details the requirements for both provisional and fully accredited CAB status, including conformity to the above international standards for the ISASecure ACSSA program scope. This document is used by:

- organizations that are candidate inspection or certification bodies, to understand the accreditation requirements and process, as well as ongoing requirements on their operations
- ACSSA accreditation bodies, as the source for ACSSA program specific requirements for the accreditations described above.

These documents also include *ACSSA-304 ISCI ACSSA – Evaluation planning and execution* [ACSSA-304], that specifies requirements for a conformity assessment body to create and document a plan to carry out an ACSSA evaluation. *ACSSA-305 ISCI ACSSA Sample evaluation plan* [ACSSA-305] provides an example of such a plan that meets these requirements.

4.9.4 Symbol and certificate

The document *ACSSA-204 ISCI ACSSA – Instructions and policies for use of the ISASecure symbols and certificates* [ACSSA-204] describes the format and correct usage for the ISASecure symbols and certificates under the ACSSA program. A specified ISASecure ACSSA symbol may be used by an asset owner to indicate a certified IACS. Likewise, a specified symbol may also be used by an accredited ACSSA inspection body or certification body to indicate its authorized participation in the ISASecure ACSSA program. It is used on ACSSA evaluation reports developed by ACSSA conformity assessment bodies.

Three types of ISASecure certificates are issued under the ACSSA program: for certified IACS, accredited inspection bodies, and accredited certification bodies.

The document in this category as it applies to an IACS that has undergone ACSSA inspection or has been certified, is used by:

- asset owners for an IACS that is a candidate for ACSSA inspection or certification, to understand requirements for symbol and certificate usage
- external stakeholders, to understand the meaning of a symbol or certificate displayed by an asset owner for an IACS
- certification bodies, to create certificates for certified IACS
- conformity assessment bodies (inspection bodies and certification bodies), to monitor for correct use of ACSSA symbols and certificates by client asset owners as required by ACSSA-200.

This document as it applies to conformity assessment bodies is used by:

- conformity assessment bodies, to understand requirements for symbol and certificate usage
- asset owners with IACS that are candidates for ACSSA, to understand the meaning of the symbol or certificate displayed by a conformity assessment body
- ASCI/ISCI, to create certificates for conformity assessment bodies
- ISCI, to monitor for correct use of the symbols and certificates for conformity assessment bodies.

4.9.5 Structure

The present document *ACSSA-100 ISCI ACSSA Inspection and certification schemes* is in the Structure category. ACSSA-100 is a publicly available reference to the structure and references of the overall ISASecure ACSSA inspection and certification schemes.

4.9.6 External references

[ISO/IEC 17020] is an international standard that defines its scope as “contains requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities.”

[ISO/IEC 17065] is an international standard that contains requirements for operating a product, process, or service certification program.

[ISO/IEC 17011] is an international standard that applies to the accreditation process itself. Thus, this document is used by ACSSA accreditation bodies and ASCI to define their accreditation operations for the ISASecure ACSSA schemes.

Figure 3 includes five standards from the 62443 series. The standard 62443-1-1 covers terminology and concepts for the 62443 series of standards.

The standard "IEC 62443-2-1 *Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners*" provides the primary list of requirements to which ACSSA evaluates conformity. The document ACSSA-311 lists these requirements and defines methods for evaluating conformity. The requirements in 62443-2-1 have associated requirements in 62443-2-4, 62443-3-2, and 62443-3-3. Conformity with these associated requirements is taken into account when evaluating conformity to a requirement in 62443-2-1.

The standard “IEC 62443-2-4 *Security for industrial automation and control systems Part 2-4: Security program requirements for IACS service providers”* states that it “specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.” To the extent that an asset owner relies upon service providers for aspects of an IACS security program, ACSSA verifies conformity to these requirements.

The standard "IEC 62443-3-3 *Security for industrial automation and control systems Part 3-3: System security requirements and security levels"* defines capability security levels for industrial control systems. ACSSA-311 specifies that for each requirement in 62443-2-1, validation of conformity to an associated 62443-3-3 requirement takes into account the security level assigned by the asset owner to each zone of an IACS. This assignment took place as required by “IEC 62443-3-2 *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design.”*

Bibliography

The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC. These 62443 standards that apply to a product supplier, are not in scope for an ACSSA evaluation. However, asset owners that use suppliers who hold certifications demonstrating conformance to these standards, will find this practice beneficial for achieving conformance to ACSSA requirements and for demonstrating that conformance. Section 4.7 discusses the relationship between ACSSA and other ANSI/ISA/IEC 62443 certifications such as ISASecure CSA, ISASecure SSA, and ISASecure SLDA.

[1] ANSI/ISA-62443-4-1-2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[2] IEC 62443-4-1:2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[3] ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[4] IEC 62443-4-2:2019 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[5] ACSSA-101 *ISA Security Compliance Institute Automation and Control System Security Assurance – Evaluation planning for the asset owner*, available at https://ISASecure.org