June 2025

ACSSA: Achieving Security Assurance for Automation and Control Systems

www.isasecure.org

Achieving Security Assurance for Automation and Control Systems

Executive Summary

Asset owners rely on interconnected automation and control systems (ACS); ensuring their cybersecurity is not merely a compliance requirement but a critical operational necessity. Unlike traditional information technology (IT) environments, ACS introduces unique challenges due to its direct impact on physical processes, safety, and operational uptime. The convergence of IT and OT (Operational Technology) has widened the attack surface, making it imperative for asset owners to adopt a robust, risk-informed security assurance process.

While the ISASecure scheme (isasecure.org/certification) has established a comprehensive certification framework for security assurance of product supplier development lifecycles, systems, and components—including Industrial Internet of Things (IIoT) components—the missing link remains security assurance for operational sites. Currently, asset owners are forced to navigate a fragmented landscape of internal policies and third-party specifications that often lack consistency, leaving themselves and other stakeholders, such as insurance providers and government bodies, with the challenge of assessing facility risk.

This white paper introduces a practical and repeatable ACS security assurance process tailored to the unique needs of operational infrastructure facilities, enabling asset owners to mitigate cyber risks, safeguard critical processes, and demonstrate conformity to best security practices for stakeholders such as regulatory bodies and insurance companies.

Introduction: The Growing Threat Landscape in Automation and Control Systems

Asset owners running power plants, water treatment facilities, transportation systems, commercial real estate, and manufacturing operations rely on ACS to manage complex physical processes. The growing demands for system and information interconnectivity has expanded the cyber threat landscape, exposing critical assets to:

- Advanced Persistent Threats (APTs)—Nation-state actors and sophisticated attackers targeting critical infrastructure.
- Supply Chain Vulnerabilities—Security gaps in components, software, and supply chains.
- Insider Threats—Malicious or negligent insiders who compromise security.
- Operational Disruption—Cyber incidents impacting safety and uptime.

While there is consensus on the growing threat, the current methods to address the underlying issues focus on managing risk in the operational facility, implementing security controls around inherently insecure products and systems. The insecure nature of products and systems arises much earlier in the supply chain as shown below in Figure 1. For example, a lack of awareness of security issues in developers can lead to poorly designed software in components and systems. The resulting technical vulnerabilities can be exploited later in a cybersecurity attack or can inadvertently cause an incident because of human error. Vulnerabilities also exist in processes and procedures and in operational personnel training and oversight and these can also result in incidents.

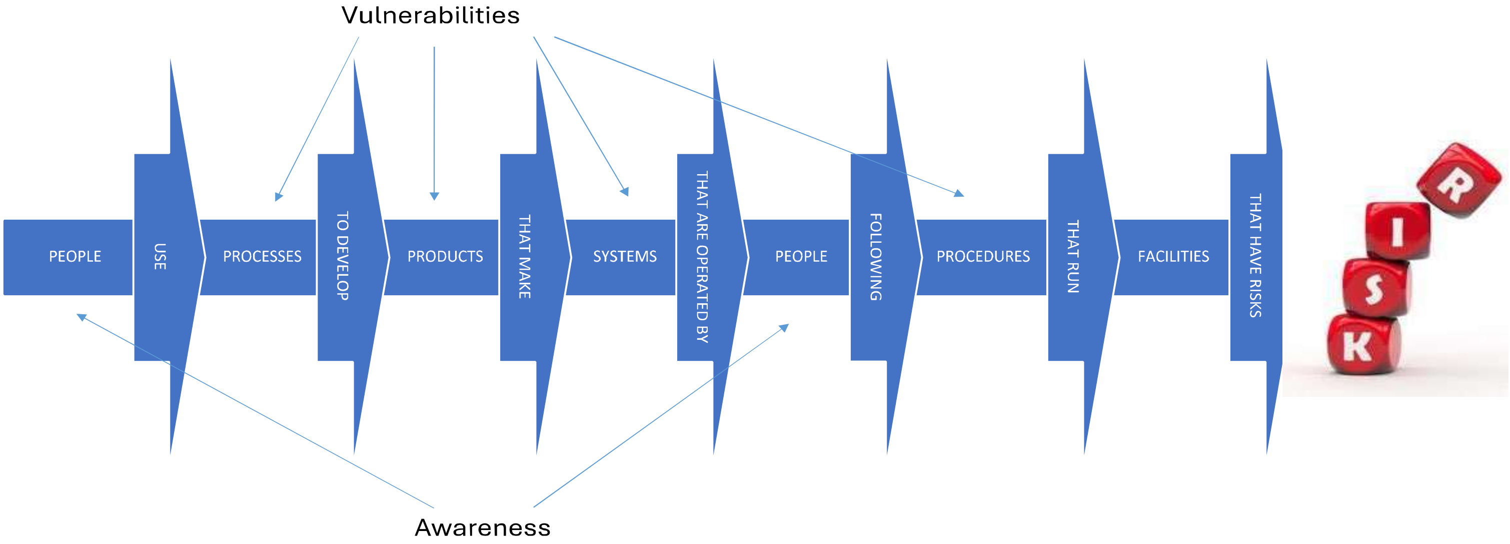


Figure 1. Without comprehensive cybersecuity practices throughout the supply chain, asset owners must address the cumulative vulnerabilities to manage facility risk.

Background: Limitations of Existing Security Assurance Methods

Many asset owners develop their own assurance methods, while other stakeholders—such as insurance providers and governmental risk management bodies—create their own frameworks. These approaches range from simple vulnerability assessment checklists to comprehensive regulatory requirements. However, these frameworks often adopt a one-size-fits-all methodology, applying uniform standards regardless of an asset's specific risk profile. As a result, low-risk environments are burdened with excessive requirements, while high-risk environments may lack sufficient security controls.

This fragmentation introduces a lack of comparability across asset owners, and even between facilities within the same organization. For insurance providers, this variability complicates the task of accurately assessing policyholder risk. Likewise, for governmental risk management bodies, it creates significant challenges in evaluating the security posture of national critical infrastructure.

Overview of ISASecure Certification

The ISASecure program is an internationally recognized certification framework based on the ISA/IEC 62443 series of standards, which defines security requirements for ACS (also known as industrial automation and control systems, or IACS in the standards series).

The ISA/IEC 62443 series of standards is widely adopted worldwide. Asset owners benefit from the risk-based approach to identifying security requirements throughout their ACS environment. In addition, asset owners can benefit from certification programs that provide independent assurance of elements of the ACS. At this point, ISASecure provides three primary certification schemes (certification programs):

- Product Supplier Security Development Lifecycle Assurance—Ensures secure development practices of vendors.
- Component Security Assurance—Verifies the security of individual system components, including IIoT devices, as off the shelf products.
- System Security Assurance—Validates the security of integrated systems and configurations, as off the shelf products.

Separately, a cybersecurity expert certificate program is offered by ISA, providing individuals working for product suppliers, system integrators, maintenance providers, or asset owners with the skills and knowledge needed to manage ACS cybersecurity risk.

ISA offers comprehensive industry consensus cybersecurity assurance solutions for the elements originally depicted in Figure 1. ISA cybersecurity assurance solutions are shown in Figure 2 for each element of the supply chain.

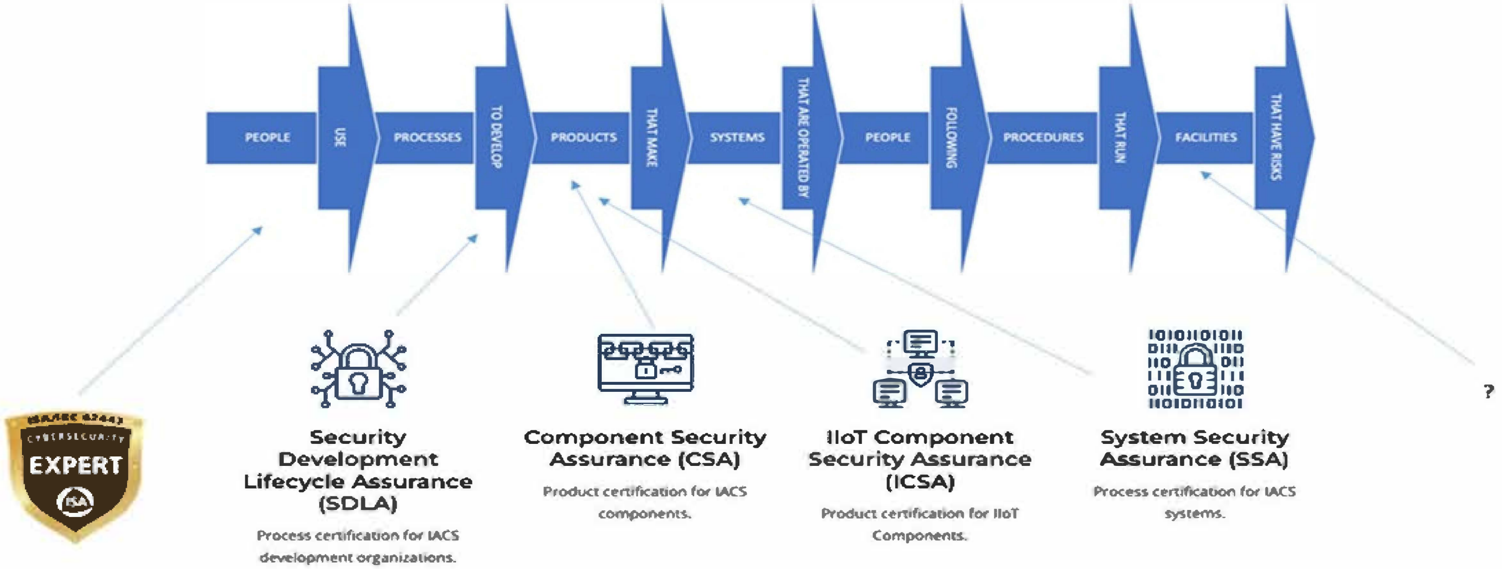

PEOPLE
USE
PROCESSES
TO DEVELOP
PRODUCTS
THAT MAKE
SYSTEMS
THAT ARE OPERATED BY
PEOPLE
FOLLOWING
PROCEDURES
THAT RUN
FACILITIES
THAT HAVE RISKS
ISA/IEC 62443
CYBERSECURITY
EXPERT
ISA
Security Development Lifecycle Assurance (SDLA)
Process certification for IACS development organizations.
Component Security Assurance (CSA)
Product certification for IACS components.
IIoT Component Security Assurance (ICSA)
Product certification for IIoT Components.
System Security Assurance (SSA)
Process certification for IACS systems.
?

Figure 2. ISASecure assurance solutions across the supply chain. The remaining element is to provide facility assurance.

Despite the comprehensive nature of ISASecure and cybersecurity expert programs, operational site assurance remains a gap. As already noted, asset owners rely on a patchwork of internal policies and third-party audits that vary across sites, leading to:

- Inconsistent Security Postures—Different sites implementing varied security controls.
- Compliance Gaps—Misalignment with industry standards and security best practices.
- Increased Risk Exposure—Sites operating with unknown or unmitigated vulnerabilities.

Without a unified, repeatable security assurance process for operational sites, asset owners face:

- Regulatory Non-Compliance—Difficulty demonstrating compliance with sector-specific cybersecurity regulations.
- Increased Liability—Exposure to legal and financial penalties following a cybersecurity incident.
- Higher Insurance Premiums—Lack of demonstrable due diligence can impact insurance terms and costs.

To address these gaps, a unified, risk-based approach to ACS security assurance is needed—one that considers operational constraints and provides consistency across diverse environments. An effective ACS security assurance process should:

- Standardize security across sites, ensuring consistent application of security controls appropriate to the risk involved.
- Align with international consensus-based standards, by incorporating ISA/IEC 62443 requirements.
- Mitigate cybersecurity risk proactively by identifying and addressing vulnerabilities before they can be exploited.
- Demonstrate due diligence by providing documented evidence of security control compliance.

Solution: The ISASecure ACS Security Assurance (ACSSA) Inspection and Certification Scheme

The ISASecure ACSSA inspection and certification scheme forms the newest ISASecure program that offers a common industry-vetted method for evaluating conformity to ISA/IEC 62443 for an IACS, which includes all policies and procedures, service providers, and technical security controls. With the addition of the ACSSA scheme, Figure 3 displays the current conformity assessment schemes offered by ISASecure.

The ISASecure ACSSA evaluates conformity to the ISA/IEC 62443 requirements as follows:

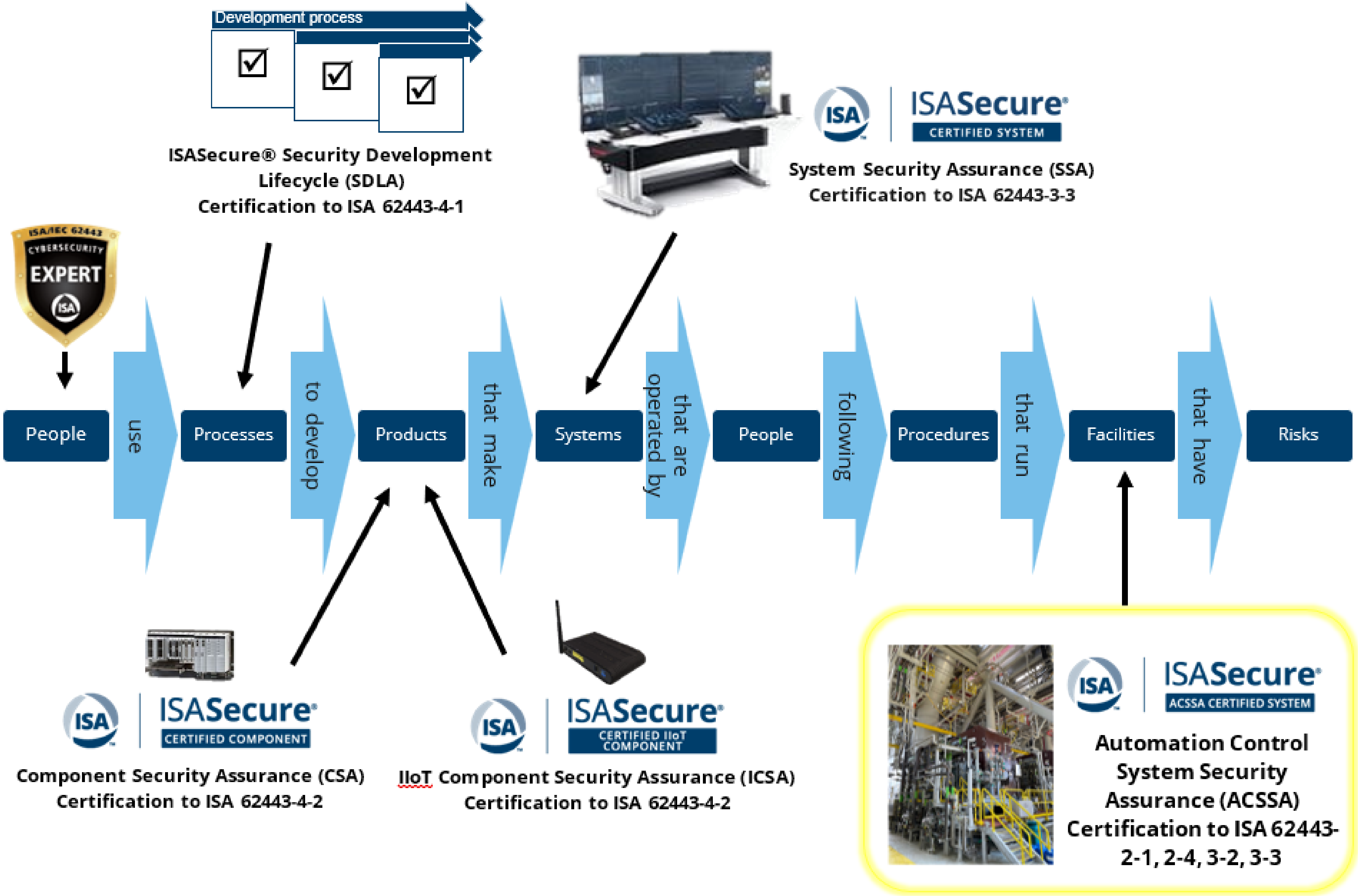
- Conformant processes and procedures—Verify that the asset owner has policies and procedures in place for their security program for the IACS, that meet the requirements for asset owners in ISA/IEC 62443-2-1, *Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners*.

- Conformant support from service providers—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 ISA/IEC 62443-2-4, *Security for industrial automation and control systems Part 2-4: Security program requirements for IACS service providers*.
- Conformant control system—Verify that the asset owner has configured and is utilizing technical capabilities described in ISA/IEC 62443-3-3, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*, provided by the hardware and software control system for the IACS.

The ISA/IEC 62443 is a risk-based approach to security management. The risk assessment process determines several fundamental aspects of the asset owner's IACS, including the zone and conduit arrangement and their associated target security levels. This in turn defines what required technical security capabilities must be in place and utilized in the hardware and software systems for these zones and conduits, to manage the risk. The ISASecure ACSSA evaluation process therefore begins with reviewing the asset owner's risk assessment process and the results of that process. This is performed against ISA/IEC 62443-3-2, *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design*.

An asset owner with an IACS that has been certified under the ISASecure ACSSA program and shown to meet these technical criteria may display the ISASecure symbol and a certificate granting certification, in accordance with program procedures. ACSSA certified asset owners are then subject to ongoing surveillance to maintain their certification, ensuring that the ISA/IEC 62443 requirements remain in place, and any changes in risk posture are reflected by changes in requirements. An asset owner may also choose to undergo one-or multiple ACSSA inspections, or refer to the ACSSA specifications to support their internal security efforts.

Figure 3. ISASecure conformity assessement schemes to ISA/IEC 62443 standards.


Development process
ISASecure® Security Development Lifecycle (SDLA) Certification to ISA 62443-4-1
ISA ISASecure CERTIFIED SYSTEM
System Security Assurance (SSA) Certification to ISA 62443-3-3
ISA/IEC 62443 CYBERSECURITY EXPERT ISA
People
use
Processes
to develop
Products
that make
Systems
that are operated by
People
following
Procedures
that run
Facilities
that have
Risks
ISA ISASecure CERTIFIED COMPONENT
Component Security Assurance (CSA) Certification to ISA 62443-4-2
ISA ISASecure CERTIFIED IIoT COMPONENT
IIoT Component Security Assurance (ICSA) Certification to ISA 62443-4-2
ISA ISASecure ACSSA CERTIFIED SYSTEM
Automation Control System Security Assurance (ACSSA) Certification to ISA 62443-2-1, 2-4, 3-2, 3-3

ISASecure ACSSA Stakeholder Benefits

While the primary beneficiary of ISASecure ACSSA is the asset owner, they are not the only stakeholder who benefits from the introduction of such a program. Table 1 lists all the stakeholders and their key benefits from ISASecure ACSSA.

Table 1. Stakeholder Benefits of the ISASecure ACSSA Program

Stakeholder	**Benefits**
Asset owner	• Integrated evaluation of risk assessment process and corresponding controls executed by people, process, and technology • Holistic view of site security posture • Objective, consistent benchmark • Comparison to peers and industry • Defined vendor support required for security program, in turn driving development of procurement requirements
Insurance providers	• Objective assessment metrics for underwriting risk and actuarial models
Product suppliers and service providers	• Clarity and transparency of role in supporting security programs for client asset owners • Standardization of industry model for structure and content of procurement requirements
Conformity assessment bodies (inspection bodies and certification bodies)	• Increased demand for services due to the attractiveness of a global standards-based scheme
Government bodies	• Standards-based metrics for use in policy language

Summary: Building a Secure Future for Critical Infrastructure

Asset owners rely on interconnected automation and control systems (ACS); ensuring their cybersecurity is not merely a compliance requirement but a critical operational necessity, making it imperative for asset owners to adopt a robust, risk-informed security assurance process.

The ISASecure program is an internationally recognized certification framework based on the ISA/IEC 62443 series of standards, which defines security requirements for ACS. Asset owners benefit from the risk-based approach to identifying security requirements throughout their ACS environment and can benefit from certification programs that provide independent assurance of elements of the ACS.

All parts of ISA/IEC62443 come together at a site. To realize the full potential of the standards series, asset owners need an integrated evaluation method. Otherwise, comparing security risk across facilities using fragmented, inconsistent assessments is impossible.

The evolving threat landscape demands that critical infrastructure operators adopt a comprehensive, repeatable ACS security assurance process such as ISASecure ACSSA to protect their assets and maintain operational resilience.

By adopting ISASecure ACSSA, asset owners can:

- Develop independently verified evidence of the use of best security practices measured against an international standard, which will contribute to the demonstration of regulatory and compliance requirements.
- Increase confidence that their cybersecurity management system will address their cybersecurity risk, by identifying gaps that need to be addressed.
- Demonstrate due diligence to insurers and potentially reducing insurance premiums by showcasing a proactive security posture that can be compared across asset owners, sectors, and countries.

By aligning all stakeholders around a consistent, standards-based program, these benefits contribute to a more secure and resilient environment for asset owners. The consistent approach benefits other stakeholders, including insurance providers, product suppliers, service providers, conformity assessment bodies, and government bodies, allowing everyone to share a common understanding of facility risk.