ISASecure® ISA/IEC 62443 IACS Security Assurance (ACSSA) Program

PROPOSED ISA PROGRAM AIMS TO OFFER
THE WORLD'S FIRST CONSENSUS ISA/IEC 62443 OT SITE ASSESSMENT

The Problem:

Suppliers have rallied around and broadly adopted the leading international standard for Operational Technology (OT) cybersecurity, ISA/IEC 62443, as well as its certification scheme, ISASecure® for commercial off the shelf (COTS) automation and control system products.

But asset owners and plant managers have yet to coalesce around a single cybersecurity assessment scheme for OT deployed at operating sites…relying instead upon a patchwork of third-party solutions that may not promote Industrial Control System (ICS) security best practices and, may leave operating sites vulnerable.

The Solution:

The International Society of Automation (ISA) seeks to establish an ISA/IEC 62443 based operating site Industrial Automation Control Systems (IACS) cybersecurity assessment scheme that will become the global specification used by operating sites, certification bodies, internal auditors, and public policy makers. When fully adopted by all stakeholders, the scheme will be similar to GAAP rules (Generally Accepted Accounting Procedures) published by the FASB, used by any organization, financial auditors and, regulatory authorities. We anticipate the demand for this program to be even higher than the market for existing OT certifications.

Why ISA?

The International Society of Automation (ISA) is the global go-to organization for ISA/IEC 62443 standards, practices, and education for securing automation and control systems that affect our everyday lives.

ISA has offered the ISASecure certification scheme for the ISA/IEC 62443 standards, beginning with certifying commercial-off-the-shelf (COTS) automation and control systems since 2007—a program that is globally recognized as the gold standard for product certification in this arena. ISASecure continues to expand coverage with its recent announcement of certifications for IIOT components to the

ISA/IEC 62443 standards, and plans for a Certified ISASecure Assessor designation.

Taken together with ISASecure's existing position in the market, these plans and the proposed proposed on-site control system assessment program make the ISASecure family of certifications a recognized one-stop shop for OT cybersecurity conformity assessment.

Stakeholder Benefits

Asset Owners - Will have visibility into their operating sites' IACS security posture; and have an objective, consistent benchmark to determine their standing with their peers and their industry.

Insurance Underwriters - Will benefit from assessments that provide objective ISA/IEC 62443 standards-based metrics for inclusion in their underwriting risk and actuarial models for industrial environments.

Product Suppliers and Service Providers - Will gain clarity and transparency regarding their cybersecurity role in providing automation products, integration services, maintenance services, and operation support services; and provide structure to service level agreements (SLAs).

Certification and Assessment Organizations - Will benefit from increased demand in services due to the attractiveness of a global consensus OT assessment scheme based on trusted international ISA/IEC 62443 standards.

Government, Legislators, and Regulatory Authorities Will have an ISA/IEC 62443 standards-based cybersecurity metric that can be used as a reference in policy language for incentives and mandates for securing critical infrastructure.

Site Assessment Details

The OT cybersecurity IACS assessment scheme would certify individual automation and control systems that are in the operation and maintenance phase of their security lifecycle at end user sites. The scope would be all types of automation and control systems in all industries, beginning with traditional

process industries and adjacent industries in critical infrastructure like oil and gas, chemicals, and water/wastewater.

The second target market segments will include railways, ports, electric sector, EV infrastructure, DER, and pipelines.

The scheme will include an on-site control system *assessment* program and site *certification* program.

The result of an *ACSSA certification* will be a third-party *certificate of conformance* which independently confirms that a designated system in the scope of the evaluation is *conformant to all requirements* referenced in the five ISA/ IEC 62443 standards listed in the certification scheme. The full set of ISA/IEC 62443 requirements would have to be met in order to receive a **certification,** including requirements from ISA/IEC 62443 parts 2-1, 2-3, 2-4, 3-2, and 3-3.

The result of an operating *site assessment* will be a standardized *assessment report,* compiled by any entity licensed to use the specification including asset owners internally, consultants, or other third party. The report identifies the requirements to which the designated system in the scope of the evaluation is conformant and lists the requirements to which the system is non-conformant.

Going forward, this program will include a training component and will fund the ISA training department to build and oversee related training and credentialing programs. These credentials will be highly sought after, similar to the existing ISA/IEC 62443 cybersecurity training pathways and other professional cybersecurity designations.

The intended outcome is to encourage broad industry adoption of the ISA/IEC 62443 operating site cybersecurity standards and best practices by companies, inclusion of them in internal operating standards, and expansion to multiple industry sectors. *This broad adoption is what is needed to secure automation that affects our everyday lives.*

How to Support

We are encouraging stakeholders like asset owners, consultants, engineering services, inspection/certification bodies, and industry groups to participate. We anticipate a development schedule of 12-14 months and plan to launch the program in 1H 2025.

Organizations Supporting the ISASecure Site Assessment Scheme include:

International Society of Automation

Building Cybersecurity LLC

ISA Global Cybersecurity Alliance

ISA Security Compliance Institute (ISCI)-supporting members include:

Asset Owners: ExxonMobil, Chevron, GSK, Saudi Aramco

Suppliers: Carrier, Honeywell, Johnson Controls, Schneider Electric, Trane, Yokogawa

General Members: AC&E**,** Arcadis, Armexa, Bureau Veritas, BYHON, Control System Security Center, Cyberprism, DNV, Enaxy, exida, FM Approvals, Ikerlan, IriusRisk, Interstates, IACS Consulting, ITRI, MIAN, Synopsis, SecurityGate, Secudia, Optiv, Peloton Cyber Solution, Securing Things, TUV Rheinland, TUV SUD, TrustCB, UL Solutions WisePlant, Zuonet.

To set up a briefing, complete the information tab on this web page or contact the ISASecure managing director, Andre Ristaino to schedule a call. Contact email: aristaino@isa.org