Ensuring Cybersecurity for O-PAS™ Certified Products using ISA/IEC 62443 standards

21 Aug 2024

International Society of Automation
and The Open Group

Susan Harper PgMP, PMP
Senior Manager, Standards and Certifications
s.harper@opengroup.org
https://publications.opengroup.org/standards/opa

Andre Ristaino
ISA Managing Director,
Conformance Programs and Consortia
aristaino@isa.org PH: +1 919-323-7660
www.isasecure.org

Susan Harper, PgMP, PMP

- Program Manager for Product and Process Certification Programs at The Open Group
- FACE Certification Authority
- Work with Forums/Consortium Regarding Conformance and Certification within the Standards Development
  - SOSA™ (Sensor Open Systems Architecture)
  - OPAF (Open Process Automation™ Forum)
  - OSDU™ (Oil and Gas Forum)
  - Open Footprint (Oil and Gas Forum)

Andre Ristaino

- Managing Director, Consortiums and Alliances, ISA
- Developing the ISASecure® control systems cybersecurity certification program since 2007, certifying automation and control system products to the IEC 62443 series of international standards
  - ISA Security Compliance Institute
  - ISA100 Wireless Compliance Institute
  - ISAGCA
  - ICS4CS

Camilo Gomez

- Global Cybersecurity Strategist at Yokogawa
- Chairs the Security Subcommittee of the Open Process Automation Forum (OPAF) developing the Open Process Automation Standard (O-PAS™).
- Chairs the Security Performance Metrics Working Group for ISA99
- Board member ISCI/ISASecure. Open Footprint (Oil and Gas Forum)

The O-PAS™ Standard

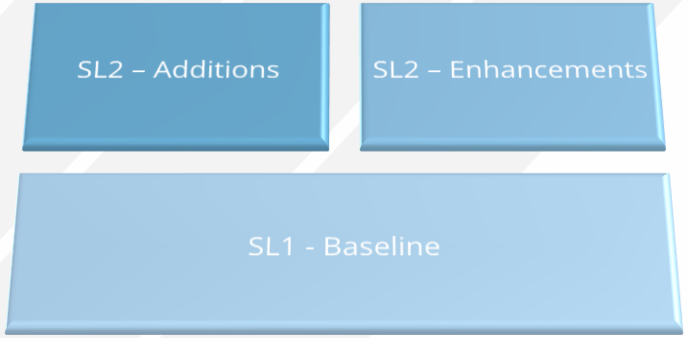
- The O-PAS standard defines an open, interoperable, secure process automation architecture. The standard enables development of fit-for-purpose systems consisting of cohesive functional elements acquired from independent suppliers and integrated easily via a modular architecture characterized by open standard interfaces between elements.
- The O-PAS standard has Profiles that define the various segments of the architecture. The O-PAS Certification program is based on these Profiles.
- Each Profile requires the SEC-F-001 Facet.
    - This equates to IEC/ISA 62443 standard Security Level 2
- The OPAF forum has selected ISASecure as the organization that will perform that verification.

O-PAS Motivation for SL2+

Drivers

- Required O-PAS OPC UA functionality matching SL2 capabilities.
- Interoperability issues of SL2 capabilities and above with SL1 generic capabilities
- Protection against **intended** violation instead of casual violation
- Supply-chain with mature SL1 secure-by-design experience

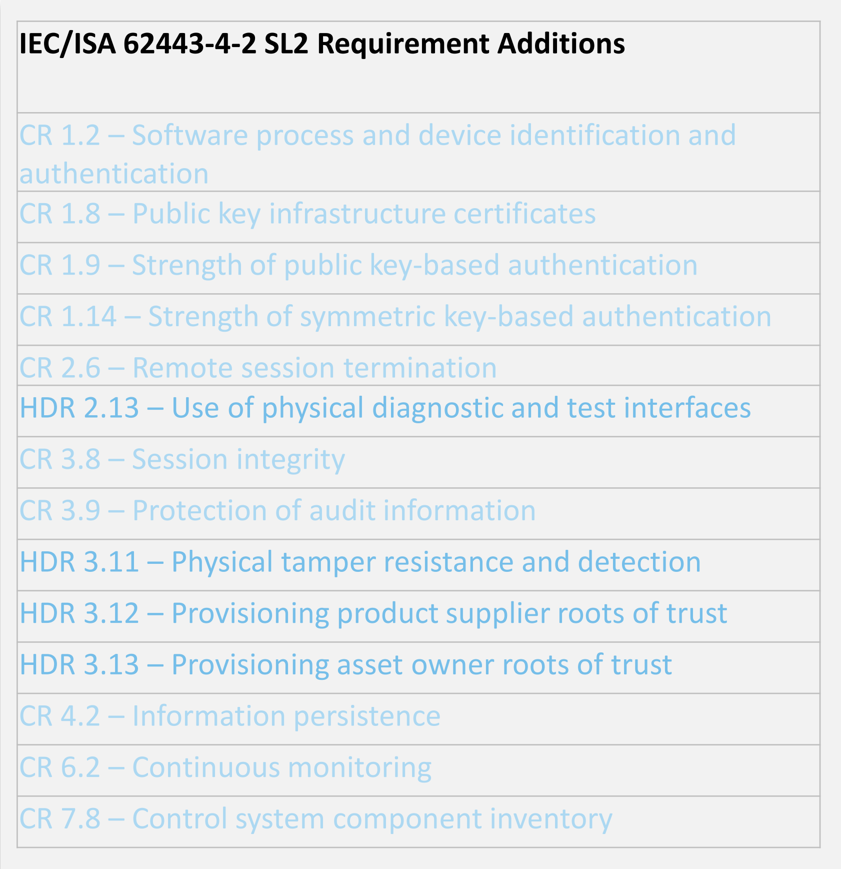
Supplier Effort



Incremental effort for product suppliers

- 62443-4-2 SL2 = SL1 Baseline + SL2 Enhancements + SL2 Additions

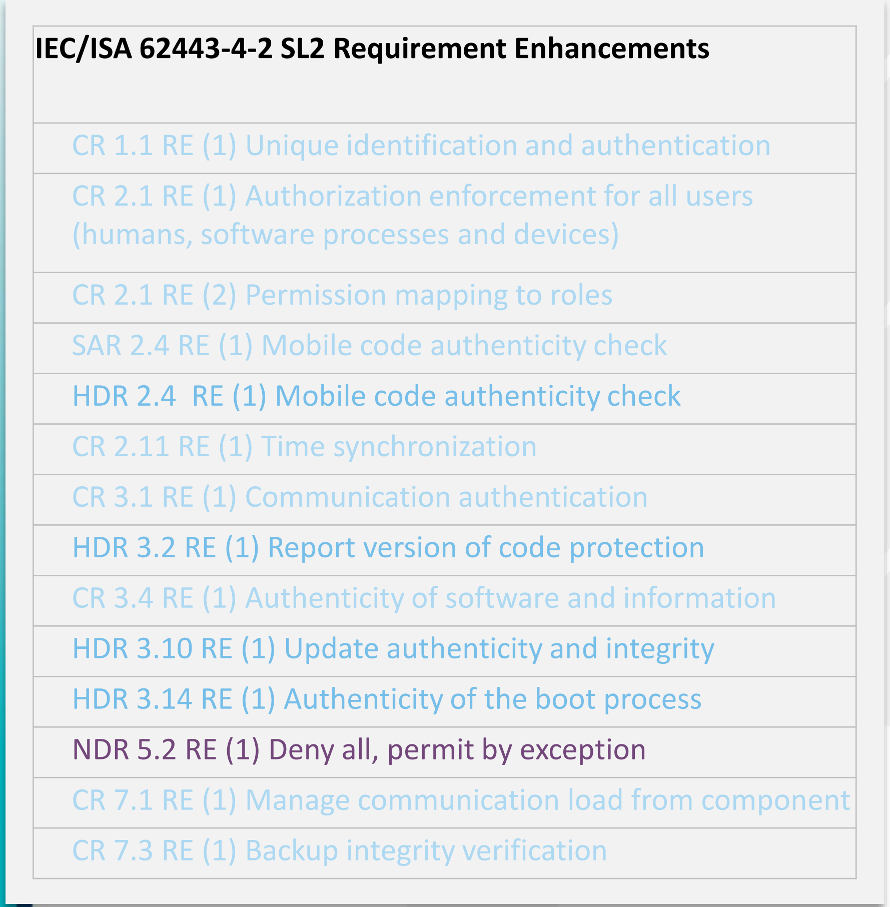
62443-4-2 SL2 Additions



IEC/ISA 62443-4-2 SL2 Requirement Additions
CR 1.2 – Software process and device identification and authentication
CR 1.8 – Public key infrastructure certificates
CR 1.9 – Strength of public key-based authentication
CR 1.14 – Strength of symmetric key-based authentication
CR 2.6 – Remote session termination
HDR 2.13 – Use of physical diagnostic and test interfaces
CR 3.8 – Session integrity
CR 3.9 – Protection of audit information
HDR 3.11 – Physical tamper resistance and detection
HDR 3.12 – Provisioning product supplier roots of trust
HDR 3.13 – Provisioning asset owner roots of trust
CR 4.2 – Information persistence
CR 6.2 – Continuous monitoring
CR 7.8 – Control system component inventory

- ❑ Identification and authentication not only human but also process and device
- ❑ Digital keys - certificates
- ❑ Session integrity
- ❑ Protection of audit information
- ❑ Continuous monitoring and component inventory (SM)
- ❑ Information Persistence
- ❑ Physical tamper resistance
- ❑ Roots of Trust

62443-4-2 SL2 Enhancements



IEC/ISA 62443-4-2 SL2 Requirement Enhancements
CR 1.1 RE (1) Unique identification and authentication
CR 2.1 RE (1) Authorization enforcement for all users (humans, software processes and devices)
CR 2.1 RE (2) Permission mapping to roles
SAR 2.4 RE (1) Mobile code authenticity check
HDR 2.4 RE (1) Mobile code authenticity check
CR 2.11 RE (1) Time synchronization
CR 3.1 RE (1) Communication authentication
HDR 3.2 RE (1) Report version of code protection
CR 3.4 RE (1) Authenticity of software and information
HDR 3.10 RE (1) Update authenticity and integrity
HDR 3.14 RE (1) Authenticity of the boot process
NDR 5.2 RE (1) Deny all, permit by exception
CR 7.1 RE (1) Manage communication load from component
CR 7.3 RE (1) Backup integrity verification

□ Unique IDs

□ Authorization enforcement (humans, processes and devices) & permission mapping to Roles

□ Validation of Mobile code

□ Comms authentication & Time Sync

□ Authenticity (SW, info, updates, boot process)

□ Deny all by default

□ Communication overload

□ Integrity verification of backups

O-PAS Profiles for Certification

No.	Profile	Description
1	OCF-001	Connectivity Framework : OPC UA Client/Server Profile
2	GDS-001	Global Discovery Server (GDS)
3	OSM-003	System management profile for a standard REST interface based on the DMTF Redfish standard
4	PP-001	Base Physical Platform (Hardware)
5	PP-002	Regulatory Control Device (Hardware)
6	NET-101	Single Ethernet Profile with end-to-end measurement over Layer 3 (Internet Protocol) time sync.
7	NET-102	Single Ethernet Profile with peer-to-peer measurement over Layer 2 Ethernet time sync.

Why Do You Need a Certification Program?

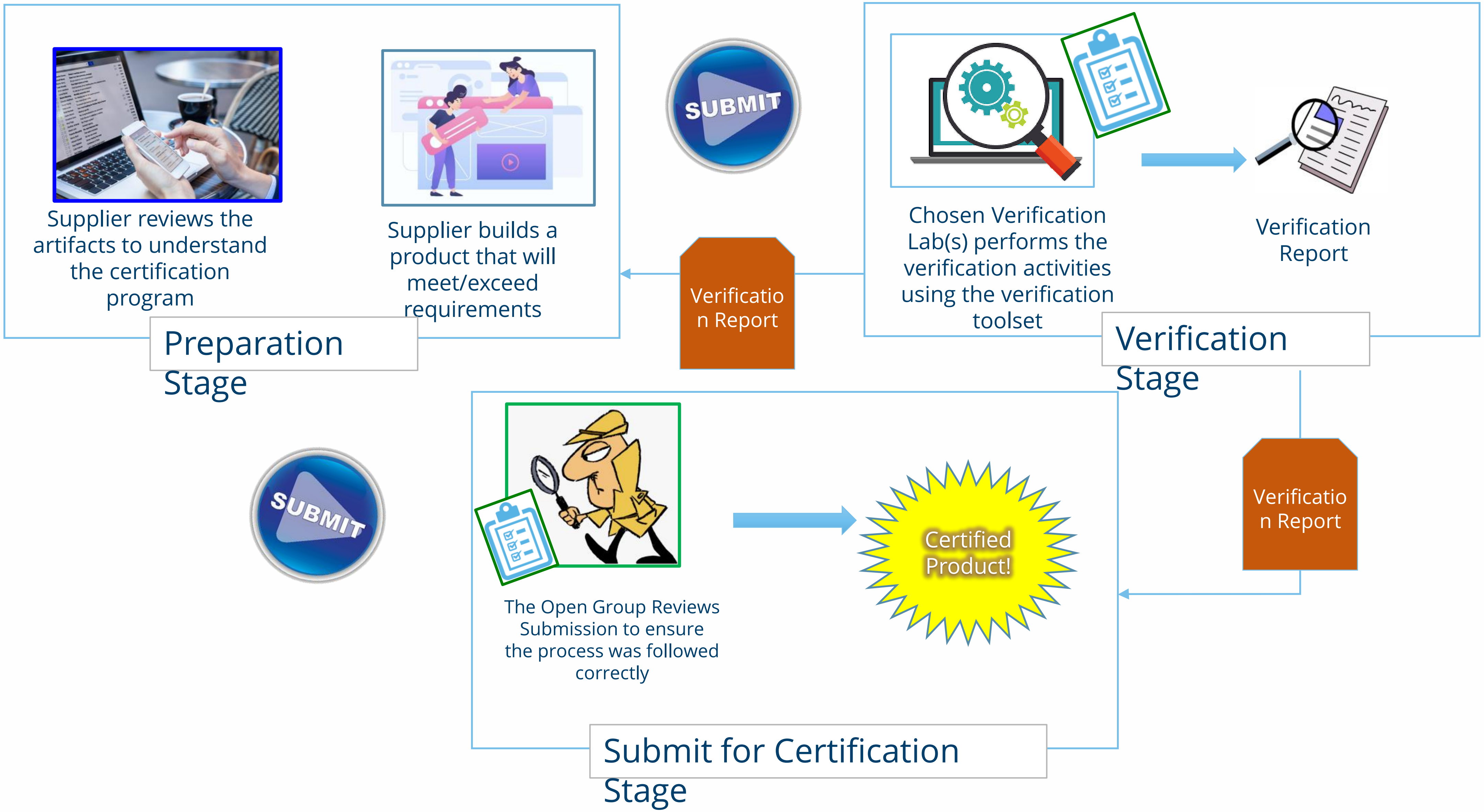
- Prove Standard ‘works’
- Tangible Market Adoption
- Provides a Marketplace
- Reduces/Eliminates Closed/Proprietary Systems
- Independent Verification of Supplier’s Claim (Uniform and Repeatable)
- Gives End User Assurance of What to Expect
- Enforces Best Practice
- Goes from Passive to Active

The Three Stages in the Certification Process

- Preparation (Supplier)
- Supplier develops a product (or modifies a current product)
- Uses Program Toolkit(s) and internal testing and QA processes
- Verification (Supplier, Verification Lab)
- Involves Verification Entities
- Independent entity
- Perform conformance assessment
    - Identical process across each VE
- Pass = 100% Conformance to Applicable Conformance Requirements
- Provides a Verification Report to the Supplier and the Certification Authority
- Submit for Certification (Supplier, Verification Lab, Certification Authority)
- One Certification Authority
- Ensures process was followed and verification completed correctly
- Certify Products
- Issues certificates and logos for Supplier’s use
- Maintain the Certification Register (Authoritative Source of Certification)

ISASecure

Product Certification Process



Supplier reviews the artifacts to understand the certification program

Supplier builds a product that will meet/exceed requirements

Preparation Stage

SUBMIT

Verificatio n Report

Chosen Verification Lab(s) performs the verification activities using the verification toolset

Verification Report

Verification Stage

Verificatio n Report

SUBMIT

The Open Group Reviews Submission to ensure the process was followed correctly

Certified Product!

Submit for Certification Stage

The Three Actors in the Certification Process

- Supplier
- Supplier develops a product (or modifies a current product)
- Uses all available resources for internal testing/QA
- Verification Entities
- Multiple Verification Entities will provide a provide market for Suppliers
- A Verification Entity can verify one or more Profiles
- Independent entity
- Certification Authority
- One Certification Authority
- Issues certificates and logos for Supplier’s use
- Maintain the Certification Register (Authoritative Source of Certification)
- Arbitrates any claims of non-conformance or trademark violations

How Certification Works

- Certification is to one or more Profiles
- Suppliers can build as they see fit
- Can be a simple or complex
- Implementation requirements determined by the End User
- Register will reflect the Profile(s) and Optional features it has implemented

ISA Automation Cybersecurity Programs

ISASecure - **ISA/IEC 62443 cybersecurity certification** of COTS products, supplier development processes and automation at asset owner operating sites.

45+ companies www.isasecure.org

ISAGCA - **Bridge the gap between** ISA/IEC 62443 standards and market adoption. Lead cybersecurity culture transformation.

60+ companies https://isagca.org

ICS4ICS – Incident Command System for Industrial Control Systems (ICS4ICS) credentials incident leaders & trains teams for responding to cyber attacks on automation in critical infrastructure. Collaborates with FEMA and CISA; stood up under ISAGCA.

1,400 volunteers; over 850 companies www.ics4ics.org

ISA99 Committee

ISA99 Committee – The ISA99 Standards committee is the origin of the ISA/IEC 62443 Standards. ISA99 Working groups draft and approve the ISA/IEC 62443 standards for submission to ANSI and IEC for approval as international standards.

Over 1,400 volunteers www.isa.org/ISA99

ISA Education

ISA Education & Training – Education and training in all industrial automation and control systems topics, including cybersecurity.

Over 4,000 students in 2023. https://www.isa.org/training

ISASecure® Accreditation Bodies

ISASecure ISO 17011 AB	Geographic Coverage
ANSI/ANAB	North America/Global
DAkkS	Germany/EU
Japan Accreditation Board	Japan
RvA Dutch Accreditation Council	Netherlands
Singapore Accreditation Council	Singapore
Standards Council of Canada	Canada
Taiwan Accreditation Foundation	Taiwan
A2LA	USA/Global
National Accreditation Board for Certification Bodies (NABCB)	India

ISASecure® Certification Bodies

ISASecure CB ISO 17065/ISO 17025	Coverage
CSSC	Japan
Exida	USA / Global
TUV Rheinland	Germany / Global
FM Approvals	USA / Global
TUV SUD	Singapore / Global
BYHON	Italy / Global
Bureau Veritas	Taiwan / Global
Underwriters Labs (UL)	USA / Global
TrustCB	Netherlands / Global
DNV	India / Global
Ikerlan	Spain / Global
Kaizen Labs	India
AC&E	Italy / Global

ISASecure Certifications Currently Available

	Certification Description	Certification Mark	Availability Date
	IIOT Component Security Assurance (ICSA) ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 plus 16 extensions	Certified IIOT Component ISASecure	Since Dec 2022
✓	**Component Security Assurance (CSA)** ISA/IEC 62443 4-1 and ISA/IEC 62443 4-2	Certified Device ISASecure	Since Aug 2019
	System Security Assurance (SSA) ISA/IEC 62443 3-3 and ISA/IEC 62443 4-2 ISA/IEC 62443-4-1	Certified System ISASecure	Since Oct 2018
✓	**Security Development Lifecycle Assurance** (SDLA) ISA/IEC 62443 4-1	"An ISASecure Certified Development Organization"	Since July 2014

Go to the ISASecure website to get detailed descriptions of the ISASecure certifications. The link is: https://isasecure.org/certification

ISASecure®

ISASecure Certification Expansion Roadmap

Certification Description	Certification Mark	Availability Date
IIOT System Security Assurance (ISSA) ISA/IEC 62443 4-1 and ISA/IEC 62443 3-3	Certified IIOT System ISASecure	TBD
Automation and Control system Security Assurance (ACSSA) ISA/IEC 62443 2-1, 2-4, 3-2, 3-3	"ISASecure IEC 62443 Conformant Operating Site"	1H 2025

IIOT 62443 Component/Gateway Study – Download Link

IIOT 62443 Solution (includes cloud provider) study available in Q1 2023 –Download Link

ISASecure®

ISA/IEC 62443 Component and System Security Levels

- 🟩 No attack resistance
- 🟨 Low attack resistance
- 🟧 Medium attack resistance
- 🟥 High attack resistance

Security Level	Attack Type			
	Violation type	Means type	Resources level	Motivation
SL-1	Coincidental	N/A	N/A	N/A
SL-2	Intentional	Simple	Low	Low
SL-3	Intentional	Sophisticated	Moderate	Moderate
SL-4	Intentional	Sophisticated	Extended	High

- ISCI is now recommending that suppliers certify to level 2 or higher. ISCI SL-1 certifications still ensures that the supplier's SDLA is at maturity level 3 or higher.
- OPAF (Open Process Automation Forum) standardized on level 2 or higher for their O-PAS™ standard.

ISASecure®

How to get your O-PAS™ standard product cybersecurity certified to ISASecure ISA/IEC 62443

1. Goto www.isasecure.org
2. Click the Get Certified button
3. Select the O-PAS™ Get Certified button
4. Complete the fill-in form and you will receive a response from a designated certification body within 24 hours.

Note: We will be piloting the O-PAS™ standard cybersecurity certification with exida for the first 12 months then open it up to all certification bodies in the ISASecure program.

Thank You!

THE Open® GROUP

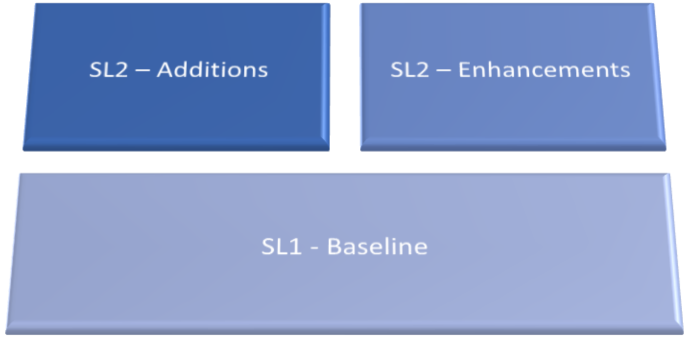
ISASecure®

O-PAS Motivation for SL2+

Drivers

- Required O-PAS OPC UA functionality matching SL2 capabilities.
- Interoperability issues of SL2 capabilities and above with SL1 generic capabilities
- Protection against **intended** violation instead of casual violation
- Supply-chain with mature SL1 secure-by-design experience

Supplier Effort



Incremental effort for product suppliers

- 62443-4-2 SL2 = SL1 Baseline + SL2 Enhancements + SL2 Additions

62443-4-2 SL2 Additions

IEC/ISA 62443-4-2 SL2 Requirement Additions
CR 1.2 – Software process and device identification and authentication
CR 1.8 – Public key infrastructure certificates
CR 1.9 – Strength of public key-based authentication
CR 1.14 – Strength of symmetric key-based authentication
CR 2.6 – Remote session termination
HDR 2.13 – Use of physical diagnostic and test interfaces
CR 3.8 – Session integrity
CR 3.9 – Protection of audit information
HDR 3.11 – Physical tamper resistance and detection
HDR 3.12 – Provisioning product supplier roots of trust
HDR 3.13 – Provisioning asset owner roots of trust
CR 4.2 – Information persistence
CR 6.2 – Continuous monitoring
CR 7.8 – Control system component inventory

- ❑ Identification and authentication not only human but also process and device
- ❑ Digital keys - certificates
- ❑ Session integrity
- ❑ Protection of audit information
- ❑ Continuous monitoring and component inventory (SM)
- ❑ Information Persistence
- ❑ Physical tamper resistance
- ❑ Roots of Trust

62443-4-2 SL2 Enhancements

IEC/ISA 62443-4-2 SL2 Requirement Enhancements
CR 1.1 RE (1) Unique identification and authentication
CR 2.1 RE (1) Authorization enforcement for all users (humans, software processes and devices)
CR 2.1 RE (2) Permission mapping to roles
SAR 2.4 RE (1) Mobile code authenticity check
HDR 2.4 RE (1) Mobile code authenticity check
CR 2.11 RE (1) Time synchronization
CR 3.1 RE (1) Communication authentication
HDR 3.2 RE (1) Report version of code protection
CR 3.4 RE (1) Authenticity of software and information
HDR 3.10 RE (1) Update authenticity and integrity
HDR 3.14 RE (1) Authenticity of the boot process
NDR 5.2 RE (1) Deny all, permit by exception
CR 7.1 RE (1) Manage communication load from component
CR 7.3 RE (1) Backup integrity verification

- ❑ Unique IDs
- ❑ Authorization enforcement (humans, processes and devices) & permission mapping to Roles
- ❑ Validation of Mobile code
- ❑ Comms authentication & Time Sync
- ❑ Authenticity (SW, info, updates, boot process)
- ❑ Deny all by default
- ❑ Communication overload
- ❑ Integrity verification of backups