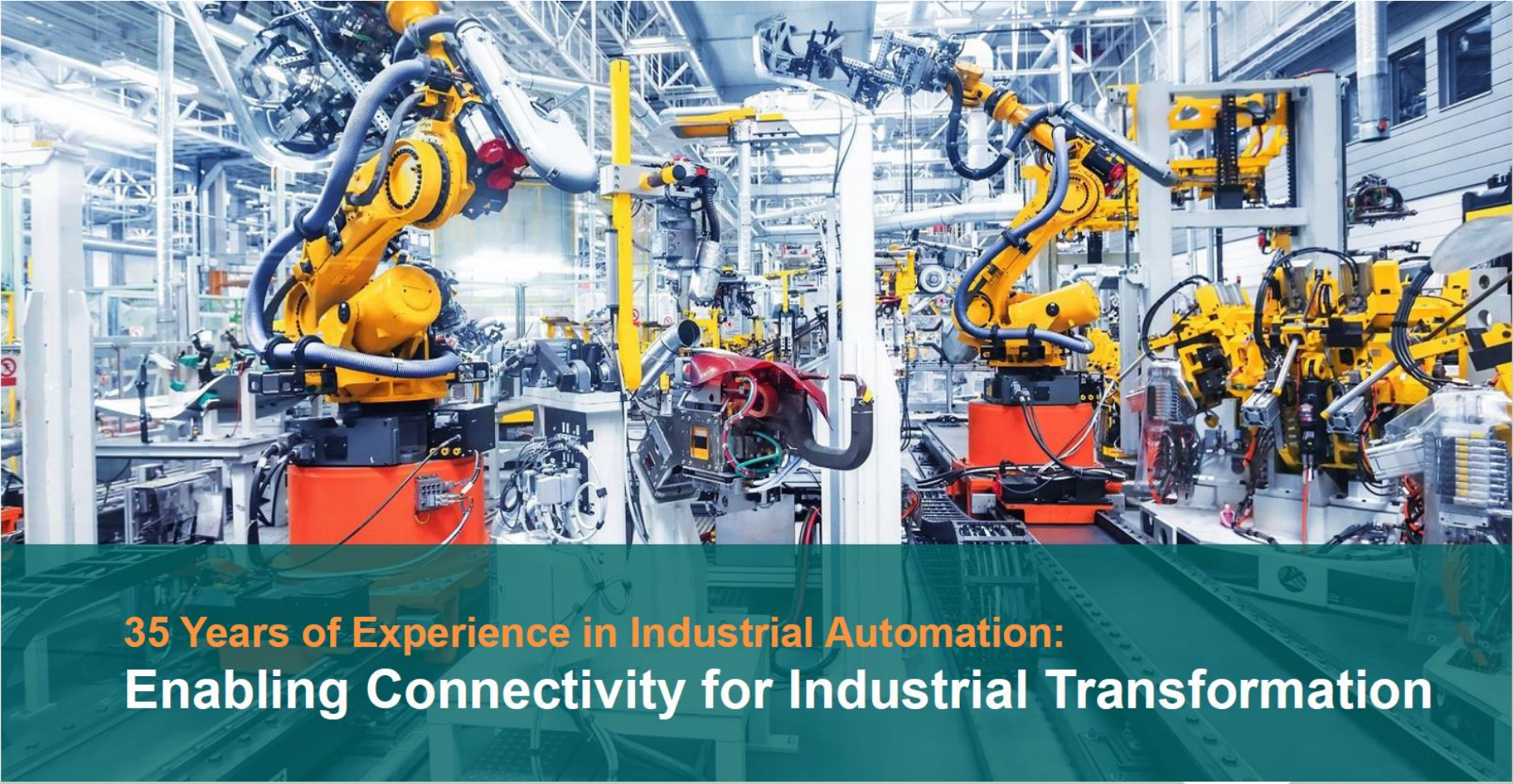
World's First ISA/IEC 62443-4-2 Certification for an Industrial Computer

Presented by

George Hsiao, Moxa

SZ Lin (林上智), Bureau Veritas

May 3, 2023



35 Years of Experience in Industrial Automation:

Enabling Connectivity for Industrial Transformation

MOXA®

Global Presence and Reach

11
Branches in four Continents

1400+
Employees Worldwide

118
Distributors Worldwide

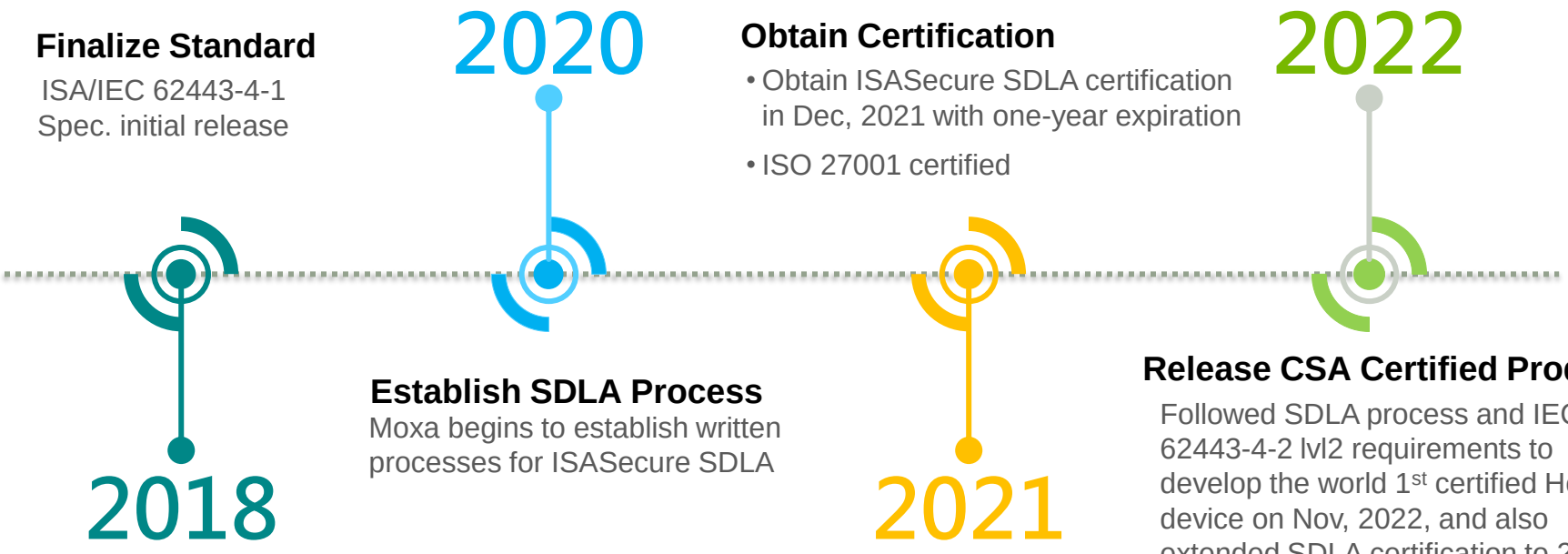
83
Countries of Distribution & Service Network

82M+
Devices Connected

Moxa Cybersecurity Progression

Process
SDLA
Security Development Lifecycle Assurance
ISA/IEC 62443-4-1

Product
CSA
Component Security Assurance
ISA/IEC 62443-4-2



Security Development Lifecycle Assurance (SDLA)

Phases	Activities
1. Security Management	1. Prepare security-related activities including personal training and infrastructure (e.g., HSM server) 2. Evaluate security risk of 3rd party component
2. Security Requirement	1. Generate product security context 2. Generate security requirements by : • Follow IEC 62443-4-2 functional security requirements • Perform threat modeling to find potential security threats and vulnerabilities
3. Security Design	1. Security design and architecture 2. Analyze new threat generate from design 3. Generate countermeasure and mitigation plan
4. Security Implementation	1. Secure implementation following secure coding guideline 2. Perform static code analysis and 3rd party component vulnerability review
5. Security Verification & Validation	1. Abuse case testing, Attack surface analysis, vulnerability scanning, software composition analysis, 2. Dynamic runtime resource management, Fuzz and network traffic load testing
6. Security Guideline	1. Security hardening guide
7. Security Defect Management	1. Security incident response procedure 2. Security update management

Why ISASecure Certification?

The **ISASecure** certification program is jointly participated by many industry leaders from security sensitive sectors such as Oil & Gas, Automation, and Energy.

These key drivers worked together to further defined **standardized validation criteria** based on their industrial experience and requirements

Carrier
Chevron
Johnson Controls
أرامكو السعودية saudi aramco
Honeywell
ExxonMobil
Schneider Electric
YOKOGAWA

https://www.isasecure.org/en-US/Current-Members

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity
		x		FSA-HDR 3.12	Provisioning product supplier roots of trust - protection	Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Examine supplier documentation of the component design and manufacturing process to verify that during the process for creating any roots of trust for the device, and thereafter, the product supplier keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity and authenticity of the roots of trust at the time of device manufacture and as used thereafter, and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met

MOXA

Why ISASecure Certification?

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity
		x		FSA-HDR 3.12	Provisioning product supplier roots of trust - protection	Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Examine supplier documentation of the component design and manufacturing process to verify that during the process for creating any roots of trust for the device, and thereafter, the product supplier keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity and authenticity of the roots of trust at the time of device manufacture and as used thereafter, and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met

Why ISASecure Certification?

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity
		x		FSA-HDR 3.12	Provisioning product supplier roots of trust - protection	Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.	Examine supplier documentation of the component design and manufacturing process to verify that during the process for creating any roots of trust for the device, and thereafter, the product supplier keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity and authenticity of the roots of trust at the time of device manufacture and as used thereafter, and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met

Moxa UC-8200 Industrial Computer

The World's 1st Host Devices Certified by ISA/IEC 62443-4-2 Lv 2

Secure by Design IEC 62443-4-1

Products that meet the requirements of security development lifecycle can be trusted now and into the future

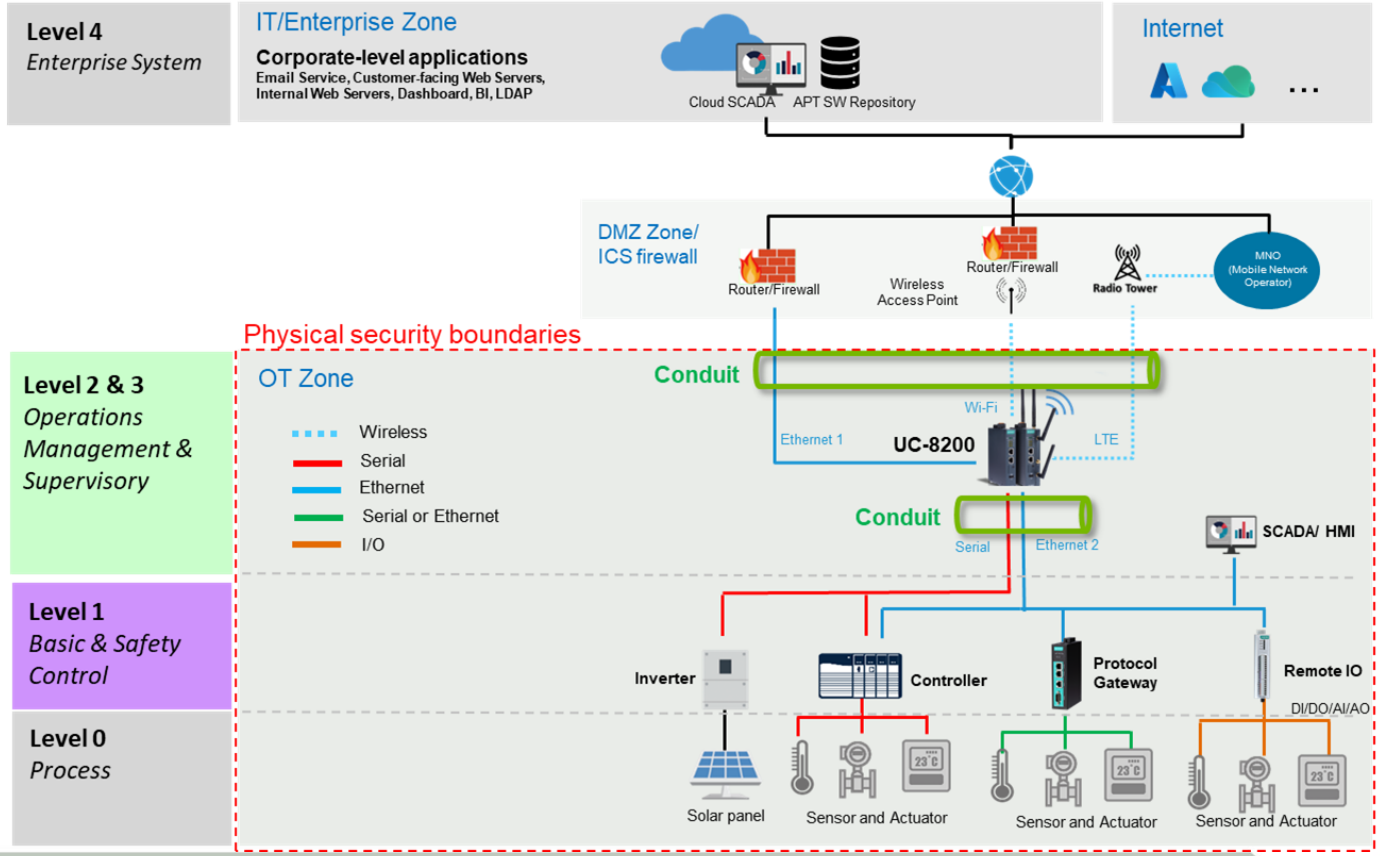
Secure by Function IEC 62443-4-2

Technical Security Requirements for Industrial Automation and Control Systems (IACS)

Certified by ISASecure Certification Body

ISASecure scheme is the highest global recognition for ISA/IEC 62443 IACS cybersecurity standard

UC-8200 Security Context



What is a Certified Host Device?

ISASecure CSA (Component Security Assurance) certification covers four type of components:

- Network Device (routers, Switch, data diodes, etc.)
- Embedded Device (PLC, controller, sensor, etc.)
- Host Device (industrial computer, HMI panel, embedded PCs, etc.)
- Software Application (HMI software, data acquisition software, etc.)

Host Device refers to device running an operating system (e.g., Linux) capable of hosting software applications.

Why Moxa UC-8200 Industrial Computer

Serial and CAN Port
- RS-232/422/485 Serial x 2
- CAN 2.0A/B

Digital I/O
DI x 4, DO x 4

Gigabit (GE) Ports
10/100/1000BaseT(X) ports x 2

microSD & SD
For storage/port expansion

Secure Element
TPM 2.0

Cellular
- LTE Cat. 4 for US/EU/APAC
- Dual SIM

Wi-Fi
802.11ac/a/b/g/n WiFi 5, 2T2R

GPS
GPS/GLONASS/Galileo

Application
- Customer developed application

Utilities & Libraries
- Network connection and management tool
- Middleware for communicating and controlling I/O
- Security tool (HIDS, diagnosis tool, firewall, etc.)
- Backup& recovery tool

IEC 62443-4-2

OS
- Hardware root-of-trust secure boot
- Secure by default configuration
- Encrypted filesystem
- 10 years lifecycle support (security patches)

IEC 62443-4-2

Hardware
- Trusted platform module (TPM)
- Security screw and seal
- 5-year warranty

IEC 62443-4-2

The Benefit of a Certified Industrial Computer

1. Saving up to **six months** of security validation and development effort and significantly reduced cost and risk.

2. Greatly reduce the cost when a customer decides to acquire ISA/IEC 62443-4-2 certification again with their added software (e.g., IIoT software) included

Re-certifying a Host Device with Add-on Software

Scenario :

- An ISV have to data acquisition software that collects data from sensor and actuator via Modbus and transmits it to a remote Cloud SCADA via MQTT
- This ISV like to deploy this software on ISA/IEC 62443-4-2 certified UC-8200 industrial computer and resell the device to their customers while maintaining the certification

Re-certifying Efforts :

- Perform a vulnerability scan
- Perform gap analysis on SDLA artifacts
- Perform gap analysis on ISA/IEC 62443-4-2 function security requirements

UC-8200 Security Features Overview

MIL3 Secure

Secure-by-design
IEC-62443-4-2 compliance diagnosis tool and security hardening guide for secure deployment

Network Redundancy
Tri-network interfaces (Wi-Fi, LTE, ethernet) with automatic connection failover to reduce downtime from network failure or attack

Automatic System Failover
Automatic system failback to recover device to the last known secure state

Network and Device Protection
Host-based Intrusion detection system (HIDS) and network security monitoring

Secure Boot
Chain of trust with Hardware as root-of-trust to prevent malware from taking over the device at startup.

Challenges of Host Device Certification

The highly programmable nature of host devices is significantly different from embedded devices, network devices, and software applications, making it almost impossible to meet some of the IEC 62443-4-2 requirements.

- BV has been an exceptionally active participant in the ISASecure technical committee, collaborating closely to bridge the gap and address challenges
- Moxa was able to obtain the certification in just 11 months by partnering with BV, which is much quicker than originally anticipated.

Non-repudiation for All Users

CSA-311 v1.11

Requirement ID	Original Validation Activity
FSA-CR 2.12	If the component provides such a human user interface, verify component requirements documentation states that all actions taken by human users, and the human user responsible for those actions, are logged in the audit records

CSA-311 v2.3

Requirement ID	Adjusted Validation Activity
FSA-CR 2.12	If the component provides such a human user interface, verify component requirements documentation states that actions taken by human users, and the human user responsible for those actions, are logged in the audit records. At a minimum, this applies to actions related to security functions required by this standard and to example actions shown under Rationale and Supplemental Guidance

WEBINAR

ISA/ IEC 62443 CERTIFICATION PRACTICE AND SUCCESS STORIES

ISASECURE CERTIFICATIONS

2023

INTRODUCTION TO ISA/IEC62443

Testing • Inspections • Audits • Certification • Advisory • Actionable Insights

AGENDA

01

ISA/IEC 62443 Certification Scheme

02

CSA Certification Process

03

The Challenging in Host Devices Assessment

01

ISA/IEC 62443 CERTIFICATION SCHEME

ISA/ IEC62443 IN THE INDUSTRIAL ECOSYSTEM

MANY STANDARDS REFER TO ISA/IEC 62443

Energy Power System

IEC 62351
TC57

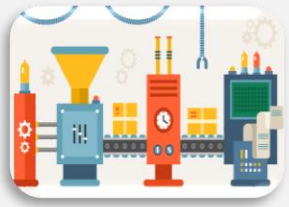
Medical

IEC 80001
IEC 60601
SC62A

Smart Manufacture

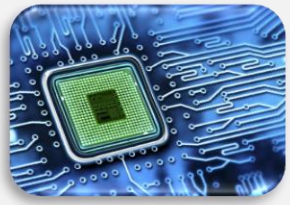
IEC 63283-3
TC65

Process



IEC TR 63069
TC65

Semiconductor



SEMI E187
SEMI

Nuclear

IEC 62645
IEC 62859
IEC 63096
SC45A

RED

Harmonised
Standards
CEN-
CENELEC

Lifts, Escalators

ISO 8102-20
ISO/TC 178

Marine

UR E27
IACS

Railway

TS 50701
EN 50159
TC9X
DIN VDE
8031-104

ISA/IEC 62443 CERTIFICATION SCHEME

Part	Type	Title	Date
General			
1-1	TS	Terminology, Concepts, and Models	2007
1-2	TR	Master glossary of terms and abbreviations	
1-3		System cybersecurity conformance metrics	
1-4		IACS security lifecycle and use cases	
Policies & Procedures			
2-1	IS	Establishing an IACS security program	2009
2-2		IACS security program ratings	
2-3	TR	Patch management in the IACS environment	2015
2-4	IS	Security program requirements for IACS service providers	2018
2-5	TR	Implementation guidance for IACS asset owners	
System			
3-1	TR	Security technologies for IACS	
3-2	IS	Security risk assessment for system design	2020
3-3	IS	System security requirements and security levels	2013
Component			
4-1	IS	Product security development life-cycle requirements	2018
4-2	IS	Technical security requirements for IACS components	2019

Certified Site (SDLA)

ISASecure

ISA/IEC 62443-4-1
Additional “SDLA-SMP” requirements

Certified System (SSA)

ISASecure

SDLA
ISA/IEC 62443-3-3
Vulnerability Identification Test
Fuzz and network Test

Certified Component (CSA)

ISASecure

SDLA
ISA/IEC 62443-4-2
Vulnerability Identification Test
Fuzz and network Test

Certified Component (ICSA)

ISASecure

SDLA
ISA/IEC 62443-4-2 plus “FSA-ICSA” 24 extensions
Vulnerability Identification Test
Fuzz and network Test

img src: Security Lifecycles in the ISA/IEC 62443 Series Security of Industrial Automation and Control Systems

ISASECURE

ISA SECURITY COMPLIANCE INSTITUTE (ISCI)

PRODUCT CERTIFICATION

CSA/ ICSA

Component Security Assurance Certification

Components (products) are developed according to the requirements of the **IEC 62443-4-1** process and meet the security requirements of **IEC 62443-4-2.** Components (products) to be certified can choose to comply with one of four safety assurance levels. (Different security assurance levels have different security requirements).

SYSTEM CERTIFICATION

SSA

System Security Assurance Certification

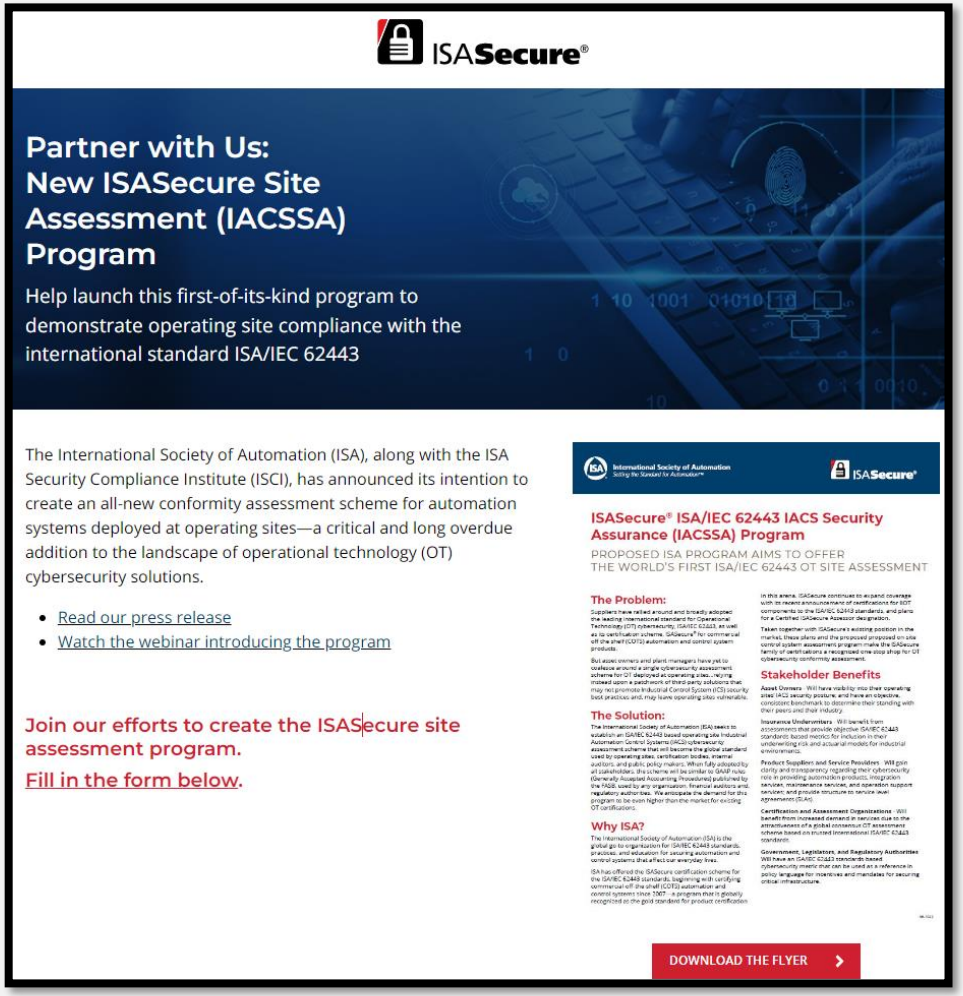
Whether the **certification system** is developed according to the process requirements of IEC 62443-4-1 and meets the security requirements of IEC 62443-3-3. **Systems to be certified can choose to comply with one of four security assurance levels.** (Different security assurance levels have different security requirements).

PROCESS CERTIFICATION

SDLA

Security Development Lifecycle Assurance Certification

Whether the certification organization develops products according to **the security development life cycle** of **IEC 62443-4-1**. SDLA certification does not take into account the maturity of the process.



img src: https://isasecure.org/isasecure-site-assessment-0

02

CSA CERTIFICATION PROCESS

SDLA CERTIFICATION

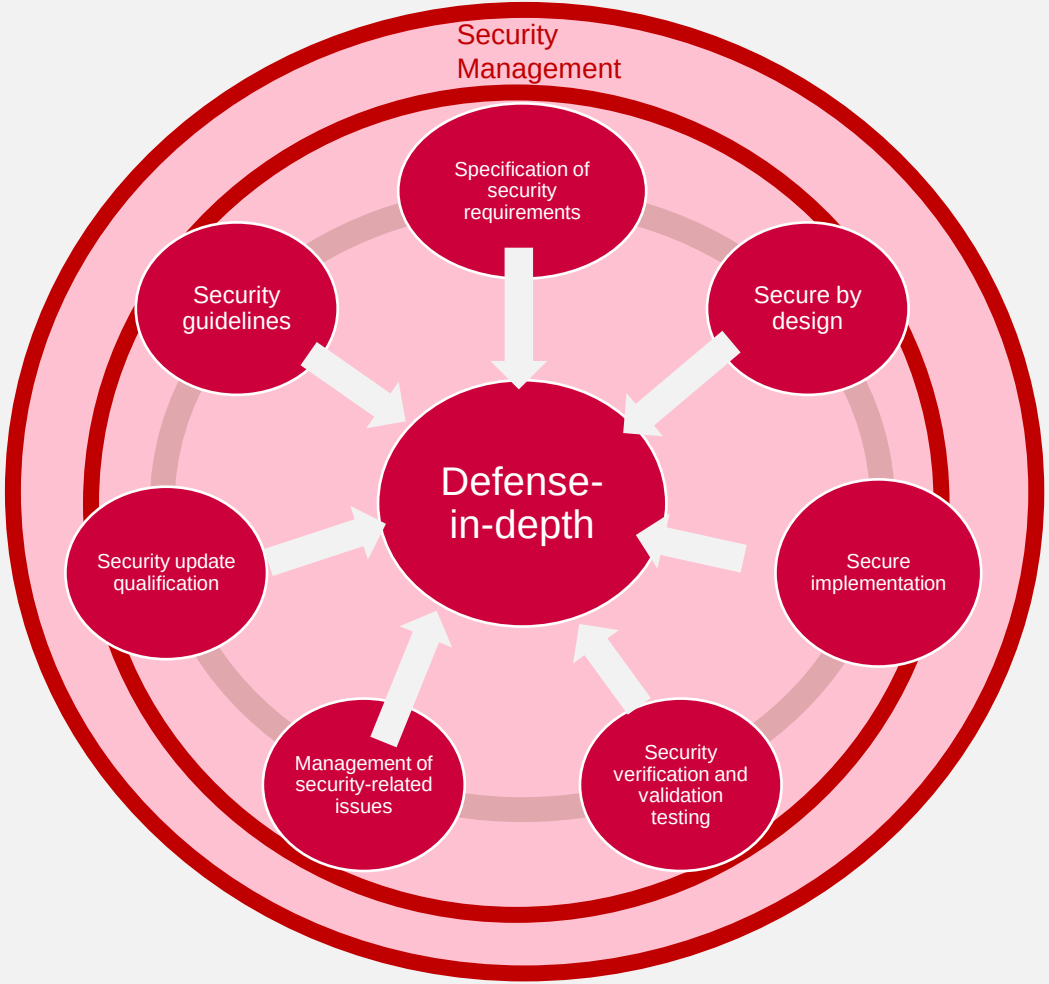
The ISASecure SDLA certification program certifies compliance to IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements (also published as ANSI/ISA-62443-4-1).

An SDLA certification is granted for:

- **a named development organization or organizations**
- **a specific version of a named, documented development lifecycle process under version control that is used by that organization(s).**

***Validity period – 3 Years.**

ISA/ IEC 62443-4-1 PRACTICES



ISASECURE SDLA CERTIFICATION

Applicant

Preparation

- SDLA application form
- Secure product development artifacts
- User Manual and other documents

BV (Accredited ISASecure Certification Bodies)

Security Development Lifecycle Assurance (SDLA)

- Assess the artifacts and conformity statement based on SDLA-312 validation activity.

CSA CERTIFICATION

The CSA certification is designed to certify to international standards IEC 62443-4-2 and IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development requirements.

An CSA certification is granted for:

- **Software application**
  - one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)
- **Embedded device**
  - special purpose device running embedded software designed to directly monitor, control or actuate an industrial process
- **Host device**
  - general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers
- **Network device**
  - that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

ISA/ IEC62443-4-2 TECHNICAL SECURITY REQUIREMENTS FOR IACS COMPONENTS

Foundational Requirement

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to evens
- Resource availability

Component Requirement (CR)

Software Application Requirement (SAR)

Embedded Device Requirement (EDR)

Host Device Requirement (HDR)

Network Device Requirement (NDR)

ISA/IEC 62443 COMPONENT AND SYSTEM SECURITY LEVELS

SL	Intention	Means	Resources	Skills	Motivation
SL0					
SL1	Incidental	Non-intentional	Individual	No attack skills	Mistakes
SL2	Intentional	Simple	Low	Low	Low
SL3	Intentional	Sophisticated	Moderate	High/IACS specific	Moderate
SL4	Intentional	Sophisticated	Extended	High/IACS specific	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

ISASECURE CSA CERTIFICATION

Applicant

Preparation

- CSA application form
- ISASecure SDLA certification
- Secure product development artifacts
- User Manual and other documents
- Devices x 3

Test Lab

Test

- SVV 1 Security Requirements Testing
- SVV 2 Threat Mitigation Testing
- SVV 3 Vulnerability Testing
- SVV 4 Penetration Test
- VIT-C Testing (Black Box Known Vulnerability Test)
- Fuzz and Networking Testing
- ISA/IEC 62443-4-2 Security Function Testing

BV (Accredited ISASecure Certification Bodies)

Component Security Assessment (CSA)

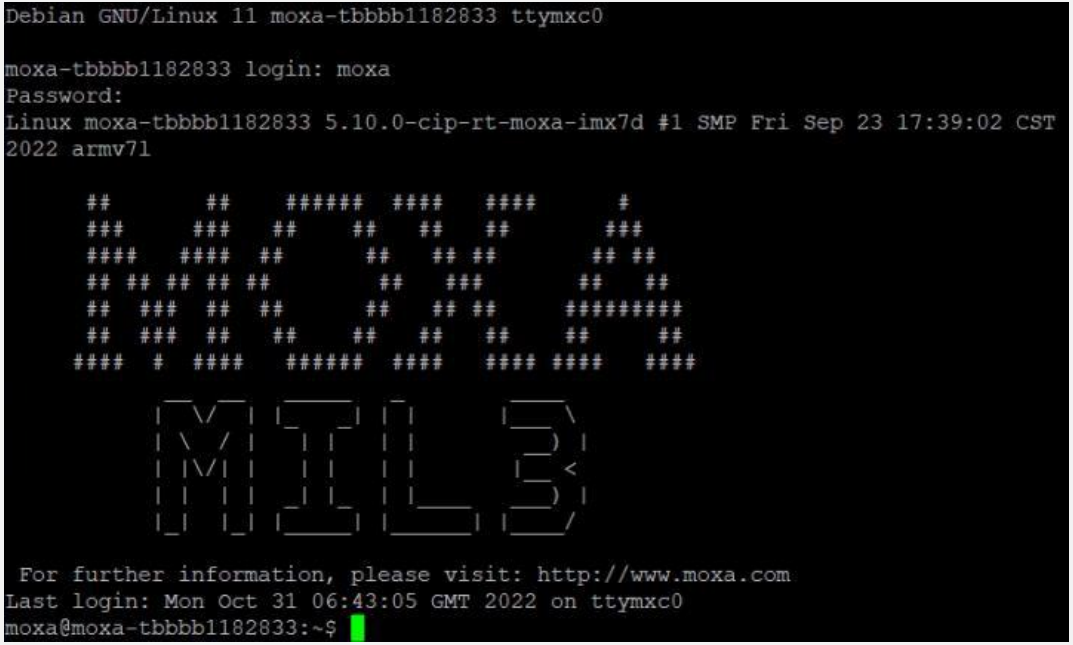
- Security Development Lifecycle Process Assessment (SDLPA-C)
- Security Development Artifacts for Components (SDA-C)
- Functional Security Assessment for Components (FSA-C)
- Vulnerability Identification Testing (VIT-C)

03

THE CHALLENGING IN HOST DEVICES ASSESSMENT

Human Interface

COMMAND-LINE INTERFACE



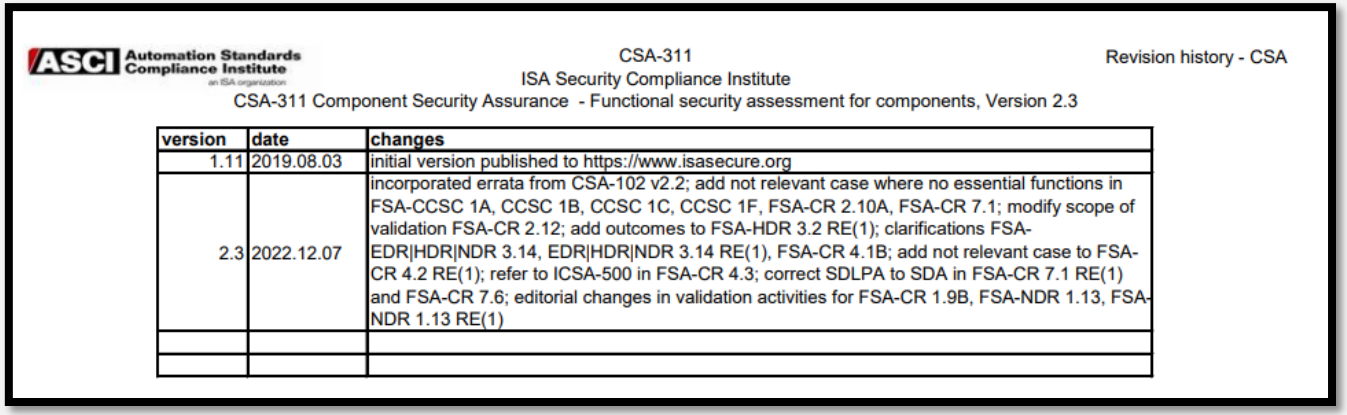
HDR Validation Activity

ESSENTIAL FUNCTION OF HOST DEVICE

There are several requirements in CSA-311 that required component supplier to define **Essential Function**. For host device such as UC-8200 that doesn't pre-install with industrial protocol and applications by default, what is ISASecure's recommendation for Essential Function declaration?

Requirement ID	Requirement Description
FSA-CCSC 1A	Support of essential functions - account lock out
FSA-CCSC 1B	Support of essential functions - non-repudiation
FSA-CCSC 1C	Support of essential functions - failure of certificate authority
FSA-CCSC 1F	Support of essential functions - incorrect timestamps
FSA-CR 2.10A	Response to audit processing failures - maintain essential functions
FSA-CR 7.1	Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.

ESSENTIAL FUNCTION OF HOST DEVICE

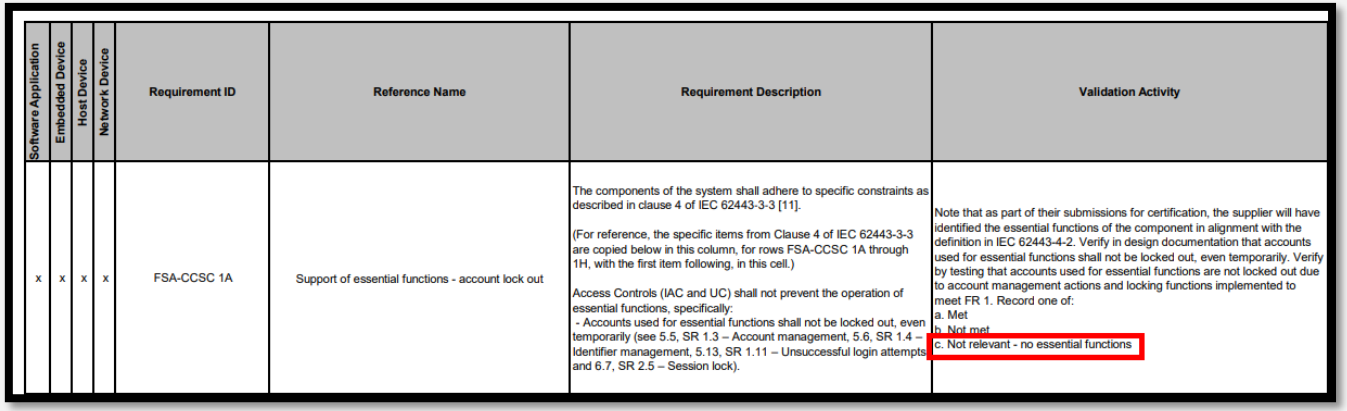


ASCI Automation Standards Compliance Institute
an ISA organization

CSA-311
ISA Security Compliance Institute
CSA-311 Component Security Assurance - Functional security assessment for components, Version 2.3

Revision history - CSA

version	date	changes
1.11	2019.08.03	initial version published to https://www.isasecure.org
2.3	2022.12.07	incorporated errata from CSA-102 v2.2; add not relevant case where no essential functions in FSA-CCSC 1A, CCSC 1B, CCSC 1C, CCSC 1F, FSA-CR 2.10A, FSA-CR 7.1; modify scope of validation FSA-CR 2.12; add outcomes to FSA-HDR 3.2 RE(1); clarifications FSA-EDR|HDR|NDR 3.14, EDR|HDR|NDR 3.14 RE(1), FSA-CR 4.1B; add not relevant case to FSA-CR 4.2 RE(1); refer to ICSA-500 in FSA-CR 4.3; correct SDLPA to SDA in FSA-CR 7.1 RE(1) and FSA-CR 7.6; editorial changes in validation activities for FSA-CR 1.9B, FSA-NDR 1.13, FSA-NDR 1.13 RE(1)



Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity
x	x	x	x	FSA-CCSC 1A	Support of essential functions - account lock out	The components of the system shall adhere to specific constraints as described in clause 4 of IEC 62443-3-3 [11]. (For reference, the specific items from Clause 4 of IEC 62443-3-3 are copied below in this column, for rows FSA-CCSC 1A through 1H, with the first item following, in this cell.) Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically: - Accounts used for essential functions shall not be locked out, even temporarily (see 5.5, SR 1.3 – Account management, 5.6, SR 1.4 – Identifier management, 5.13, SR 1.11 – Unsuccessful login attempts and 6.7, SR 2.5 – Session lock).	Note that as part of their submissions for certification, the supplier will have identified the essential functions of the component in alignment with the definition in IEC 62443-4-2. Verify in design documentation that accounts used for essential functions shall not be locked out, even temporarily. Verify by testing that accounts used for essential functions are not locked out due to account management actions and locking functions implemented to meet FR 1. Record one of: a. Met b. Not met c. Not relevant - no essential functions

img src: CSA-311 ISA Security Compliance Institute — Component Security Assurance Functional security assessment for components Version 2.3

FURTHER INFORMATION

Contact SZ Lin (林上智) via

shangjyh.lin@bureauveritas.com

THANK YOU