International Society of Automation

IIoT Component Security Assurance

Brandon Price
Chair
ISCI Governing Board
brandon.p.price@exxonmobil.com

Andre Ristaino
ISA Managing Director
Consortia and Conformity Assessment
aristaino@isa.org 919-990-9222

Carol Muehrcke
Program Manager
ISCI
cmuehrcke@isa.org
423-451-4122

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

September 2022

Case for Action

Growing ecosystem of ‘connected’ industrial devices (IIoT)

- Hardware-based business models → data / services-based
- Evolving threat landscape
- Expanding attack surface

Business & operations implications

- Safety & security
- Data ownership
- 3rd party connectivity / processing of company data
- Contract language

Standards-based component certification scheme to assure security requirement compliance needed

Certified IIOT Component
ISASecure

ISASecure®

Background

- ISA Global Cybersecurity Alliance and ISA Security Compliance Institute recognized urgent need for IIoT certification programs
- Conducted study to assess feasibility of applying ISA/IEC 62443 standards to IIoT components & systems
- Confirmed certification feasibility based on ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 with manageable program enhancements
- Program developed by team of ISCI member companies

2020

- Program initiation

2021

- Feasibility study
- Program development

2022

- ISASecure **IIoT Component Security Assurance (ICSA)** certification approval & launch

Certified IIOT Component
ISASecure

ISASecure
IIoT Component Security Assurance (ICSA) Program Readiness

ISASecure® Supporters

bp
Chevron
ExxonMobil
YPF
ارامكو السعودية
Saudi Aramco
aws
Honeywell
Rockwell Automation
Schneider Electric
SIEMENS
Ingenuity for life
HITACHI
Inspire the Next
FM Approvals
Member of the FM Global Group
FORTRESS
Critical Infrastructure. Secured.
Johnson Controls
INGENUITY WELCOME
exida.com
Security Compass
BUREAU VERITAS 1828
BUREAU VERITAS
YOKOGAWA
ISA
IPA Better Life with IT
CSSC
SYNOPSYS®
WisePlant®
Applied Risk
TÜVRheinland®
Precisely Right.
GE Digital
BEYOND security
KPMG
Carrier
Johnson Controls
PROD JAB
TRUSTCB
ikerlan
TÜV SÜD
DNV
Singapore Accreditation Council
ANSI
ANSI Accredited Program PRODUCT CERTIFICATION
ANAB ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS CERTIFICATION BODY
ilac-MRA
DAkkS
Deutsche Akkreditierungsstelle
D-PL-18345-01-00
BYHON
ISASecure®

ISAecure® ISO 17011 Accreditation Bodies

(Must be IAF Signatories for global MLA)

1. ANSI/ANAB-North America, Global
2. DAkkS-Germany
3. Japan Accreditation Board-Japan
4. RvA Dutch Accreditation Council – Netherlands
5. Singapore Accreditation Council - Singapore
6. Standards Council of Canada
7. Taiwan Accreditation Foundation
8. A2LA-USA/Global

ANSI Accredited Program PRODUCT CERTIFICATION

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

ilac-MRA

DAkkS Deutsche Akkreditierungsstelle D-PL-18345-01-00

PROD JAB

scc ccn 50 ANS

Singapore Accreditation Council

TAF Taiwan Accreditation Foundation

ISASecure®

ISASecure® Certification Bodies Accredited to ISO 17065/ISO 17025

Certification Body	Geographic Coverage	Accreditation Status
CSSC	Japan	Accredited
Exida	USA / Global	Accredited
TUV Rheinland	Germany / Global	Accredited
FM Approvals	USA / Global	Accredited
TUV SUD	Singapore / Global	Accredited
BYHON	Italy / Global	Accredited
Bureau Veritas	Taiwan / Global	Accredited
TrustCB	Netherlands / Global	In progress
DNV	Singapore / Global	In progress
Ikerlan	Spain / Global	In progress

ISASecure Certification Bodies Ready for ICSA

- Certification Body *accreditation requirements* to conduct ICSA certifications are the same as for CSA.

- Current certification bodies are immediately ready and able to accept IIOT devices and gateways for ISASecure ICSA assessments when launched in October 2022.

- *ICSA Certification specifications are* based on ISA/IEC 62443-4-2 and ISA/IEC 62443-4-1 with selected modifications to accommodate IIOT characteristics.

- Formal ICSA product certification specifications will be posted to the www.isasecure.org website in 1st half of October 2022. At that time, CB's will be accepting IIOT product submittals for certification.

Certified IIOT Component
ISASecure

ISASecure Certifications Currently Available

Certification Description	Certification Mark	Availability Date
Embedded Device Security Assurance* (EDSA)	Certified Device ISASecure	Since 2010 (*replaced by CSA Aug 2019)
Component Security Assurance (CSA) ISA/IEC 62443 4-1 and ISA/IEC 62443 4-2	Certified Component ISASecure	Since Aug 2019
System Security Assurance (SSA) ISA/IEC 62443 3-3 and ISA/IEC 62443 4-2	Certified System ISASecure	Since Oct 2018
Security Development Lifecycle Assurance (SDLA) ISA/IEC 62443 4-1	"An ISASecure Certified Development Organization"	Since July 2014

ISASecure®

ISASecure Certification Expansion Roadmap

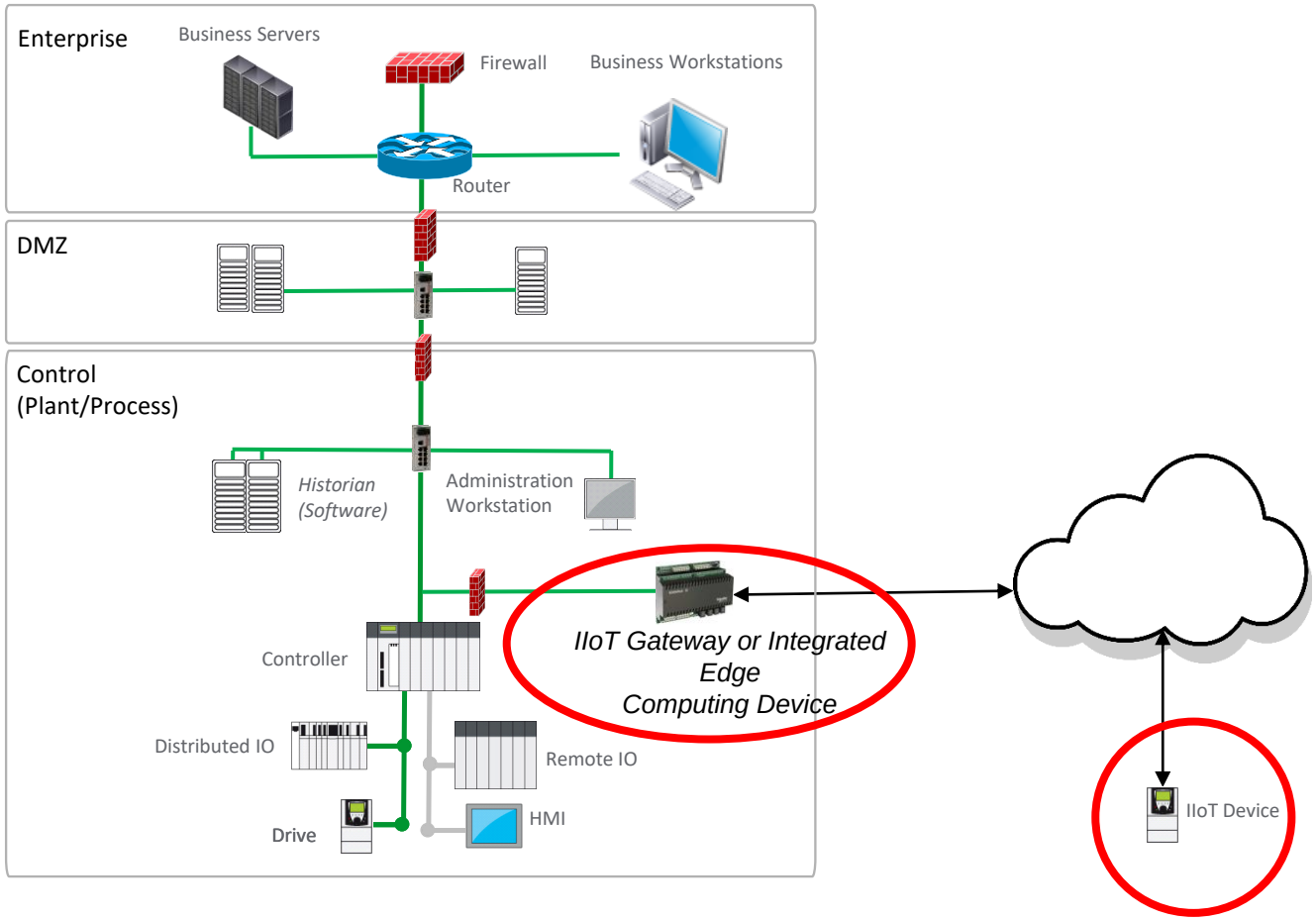
Certification Description	Certification Mark	Availability Date
IIoT Component Security Assurance (ICSA) ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 plus extensions	Certified IIOT Component ISASecure	Q4 2022
IIoT Automation Solution Assurance (IIoTSA) ISA/IEC 62443 2-1, 2-3, 2-4, 3-2, 3-3	Certified IIOT System ISASecure	2nd half 2023
Automation Solution Security Assurance (ASA) ISA/IEC 62443 2-1, 2-3, 2-4, 3-2, 3-3	Certified System ISASecure	2nd half 2023

IIOT 62443 Component/Gateway Study - https://gca.isa.org/iiot-component-certification-based-on-62443

ISASecure®

ISASecure
IIoT Component Security Assurance (ICSA) Description

Scope of ICSA certification



IIoT device: interface to physical process AND interface to untrusted network
IIoT gateway: connects devices on control network with untrusted network

Certified IIOT Component
ISASecure

IIoT Component Certification Study -> ICSA Certification Program

- Study concluded: Existing IEC 62443-4-2 certifications cover ~90% of desired criteria for IIoT certification

- To achieve the 10%:
  - Create two certification tiers instead of four security levels
  - Add certification requirements
  - Remove some existing requirements
  - Refine evaluation methods for existing requirements

- Above recommendations define ICSA

- 90% of ICSA is existing CSA program

Certified IIOT Component
ISASecure

ISA/IEC 62443 Capability Security Levels to ICSA Tiers

IIoT

Core Tier

Advanced Tier

Security Level (SL-C)	Definition	Means	Resources	Skills	Motivation
1	Protection against casual or coincidental violation				
2	Protection against intentional violation using simple means with low resources, generic skills and low motivation	*simple*	*low*	*generic*	*low*
3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation	*sophisticated*	*moderate*	*IACS specific*	*moderate*
4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation	*sophisticated*	*extended*	*IACS specific*	*high*

Certified IIOT Component
ISASecure

Add certification requirements

- 23 functional requirements added
  - 7 about compartmentalization
- Added functional requirements – other examples
  - Supplier root of trust in hardware
  - Remote update and upgrade
  - Protection from untrusted management traffic
- Example added lifecycle requirements
  - Secure design practice about failing securely
  - Advance notification of withdrawal from security update process
  - Security Maintenance Audit (SMA): Ongoing certifier surveillance of maintenance of product security

Certified IIOT Component
ISASecure

ISA/IEC 62443 requirements removed for ICSA program

62443-4-2 Reference	62443-4-2 requirement	Rationale for not including
CR 1.7 RE(1)	Password generation and lifetime restrictions for human users	Periodic password change no longer considered best practice
CR 2.1 RE(3)	Supervisor override	Not useful for limited device functionality, introduces risk
CR 2.1 RE(4)	Dual approval	Not used in many cases
CR 3.9 RE(1)	Audit records on write-once media	Records typically sent to other systems

Security Maintenance Audit (SMA) Added for ICSA Program

- SMA addresses end user concern for the “security future” of a product post-certification
- Unforgiving IIoT threat environment
- 62443-4-1 practices cannot be fully evaluated at initial certification
  - Defect management (DM)
  - Security update management (SUM)
- SMA = time-driven evaluation of key DM and SUM practices for product AFTER initial ICSA certification
- Typical: 1 year after initial certification and every three years thereafter
- Passing SMA required to maintain ICSA certification

Certified IIOT Component
ISASecure

Cybersecurity Resources at ISA

ISASecure product certifications – https://www.isasecure.org/en-US/

ISA Global Cybersecurity Alliance - https://isaautomation.isa.org/cybersecurity-alliance/

ISAGCA Blogs (tons of great info and free downloads) - https://gca.isa.org/blog

ISA/IEC 62443 Training - https://www.isa.org/training-and-certification/isa-training

Andre Ristaino
ISA Managing Director
Consortia and Conformity Assessment
aristaino@isa.org O: +1 919-990-9222 M: +1 919-323-7660

Elevating OT cybersecurity from an art, to a science, to an engineering discipline

ISASecure®

Question and Answers

ISASecure®