International Society of Automation

ISASecure Program Status

Webinar starts at 11:04 a.m.

20 Sept 2023

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

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

ISASecure®

Andre Ristaino

ISA Managing Director, Conformance Programs and Consortia

aristaino@isa.org PH: +1 919-323-7660

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

- Mr. Ristaino directs ISA's consortiums and alliances, including, ISA Security Compliance Institute, ISA Wireless Compliance Institute, ISAGCA, and LOGIIC.
- Advisory roles include ERNCIP EU OT security labeling scheme, DOE S2G solar security IAB
- Prior to ISA, Mr. Ristaino held positions at NEMA, Renaissance Worldwide and, Deloitte's Advanced Manufacturing Technology Group where he was a recognized leader in system lifecycle methodologies.
- Mr. Ristaino earned a BS in Business Management from the University of Maryland, College Park and an MS in Applied Computing from the American University in Washington DC with a focus on expert systems and artificial intelligence.

ISASecure®

ISA Consortia Summary

LOGIIC - Research and development on cybersecurity topics for automation used by the oil and gas industry. O&G majors are members. www.Logiic.org

ISAGCA - Bridge the gap between ISA/IEC 62443 standards and market adoption. Lead cybersecurity culture transformation. https://isagca.org

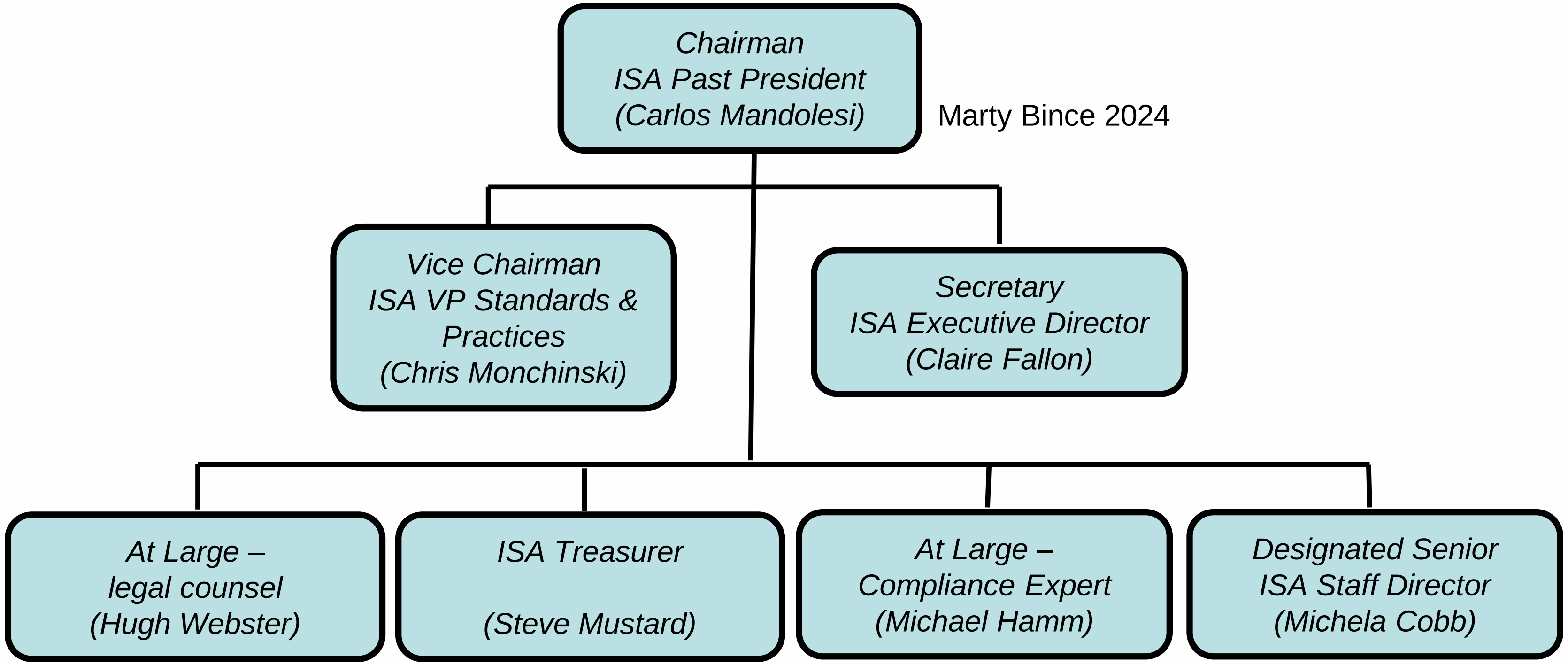
ISASecure - ISA/IEC 62443 cybersecurity certification of COTS products, supplier development processes and automation at asset owner operating sites www.isasecure.org

ICS4ICS – Incident Command System for Industrial Control Systems establishes a standing organization and playbook for responding to cyber attacks on automation in critical infrastructure. Collaborating with FEMA and CISA; began as a program under ISAGCA. www.ics4ics.org

ISA100 WCI – ISA100 Wireless Compliance Institute provides assured interoperability for wireless products conforming to the ISA100.11a (IEC62734) international wireless standard. www.isa100wci.org

2023 ASCI Board of Directors

Oversees ISA Conformity Assessment Programs



Chairman
ISA Past President
(Carlos Mandolesi)

Marty Bince 2024

Vice Chairman
ISA VP Standards & Practices
(Chris Monchinski)

Secretary
ISA Executive Director
(Claire Fallon)

At Large –
legal counsel
(Hugh Webster)

ISA Treasurer
(Steve Mustard)

At Large –
Compliance Expert
(Michael Hamm)

Designated Senior
ISA Staff Director
(Michela Cobb)

www.isasecure.org

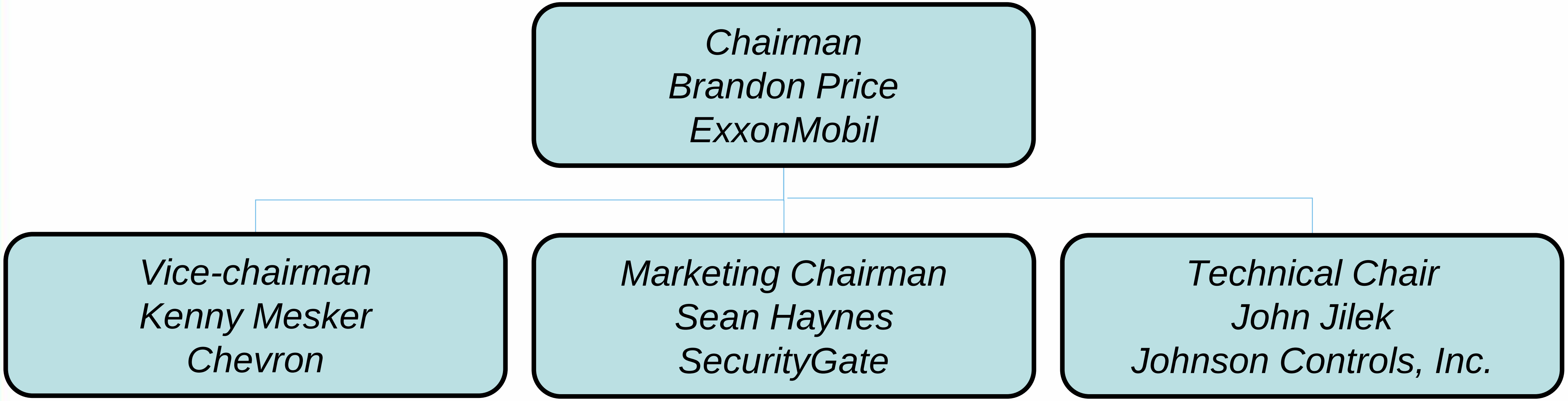
ISASecure - ISA/IEC 62443 cybersecurity certification of:

- COTS products and systems
- supplier development processes
- automation systems installed at asset owner operating sites.

ISO 17065 accredited product conformance scheme since 2007.

- Global operations
- Highly regarded network of certification bodies (CB)
- Expanding Certification coverage to Asset Owner Series of ISA/IEC 62443 Standards based on ISO 17020 standard for inspection bodies.

ISA Security Compliance Institute Governing Board



Chairman
Brandon Price
ExxonMobil

Vice-chairman
Kenny Mesker
Chevron

Marketing Chairman
Sean Haynes
SecurityGate

Technical Chair
John Jilek
Johnson Controls, Inc.

Governing Board Companies

Chevron
Honeywell
Yokogawa
ISA99 Committee Liaison

ExxonMobil
Johnson Controls, Inc.
Schneider Electric

Carrier Global
Saudi Aramco
Trane Technologies

ISASecure Supporters

bp
Chevron
ExxonMobil
YPF
أرامكو السعودية
Saudi Aramco
SecurityGate
FM Approvals
Member of the FM Global Group
SECURING THINGS
FOR SMART & SAFER SOCIETY
ISA99
STANDARDS COMMITTEE
aws
UL Solutions
cyberprism.net
INTERSTATES
ARMEXA
Rockwell Automation
Schneider Electric
SIEMENS
Ingenuity for life
HITACHI
Inspire the Next
BYHON
TAF Taiwan Accreditation Foundation
Honeywell
YOKOGAWA
SecurityGate.io
exida.com
KAIZEN CYBER LAB
ISA
Secudea
Cybersecurity services for Industry
CSSC
SYNOPSYS
SCC ccn 50
Applied Risk
WisePlant
TÜVRheinland
Precisely Right.
GE Digital
TRANE TECHNOLOGIES
KPMG
IACS CONSULTING
BEYOND security
Johnson Controls
PROD JAB
TRUSTCB
BUREAU VERITAS
1828
DNV·GL
TÜV SÜD
Carrier
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
ecure

2023 ISASecure New Member Additions

Strategic

Trane Technologies

Technical

SecurityGate
Secudea
Interstates
Armexa
Cyberprism.net
Securing Things
Radiflow
IACS Consulting

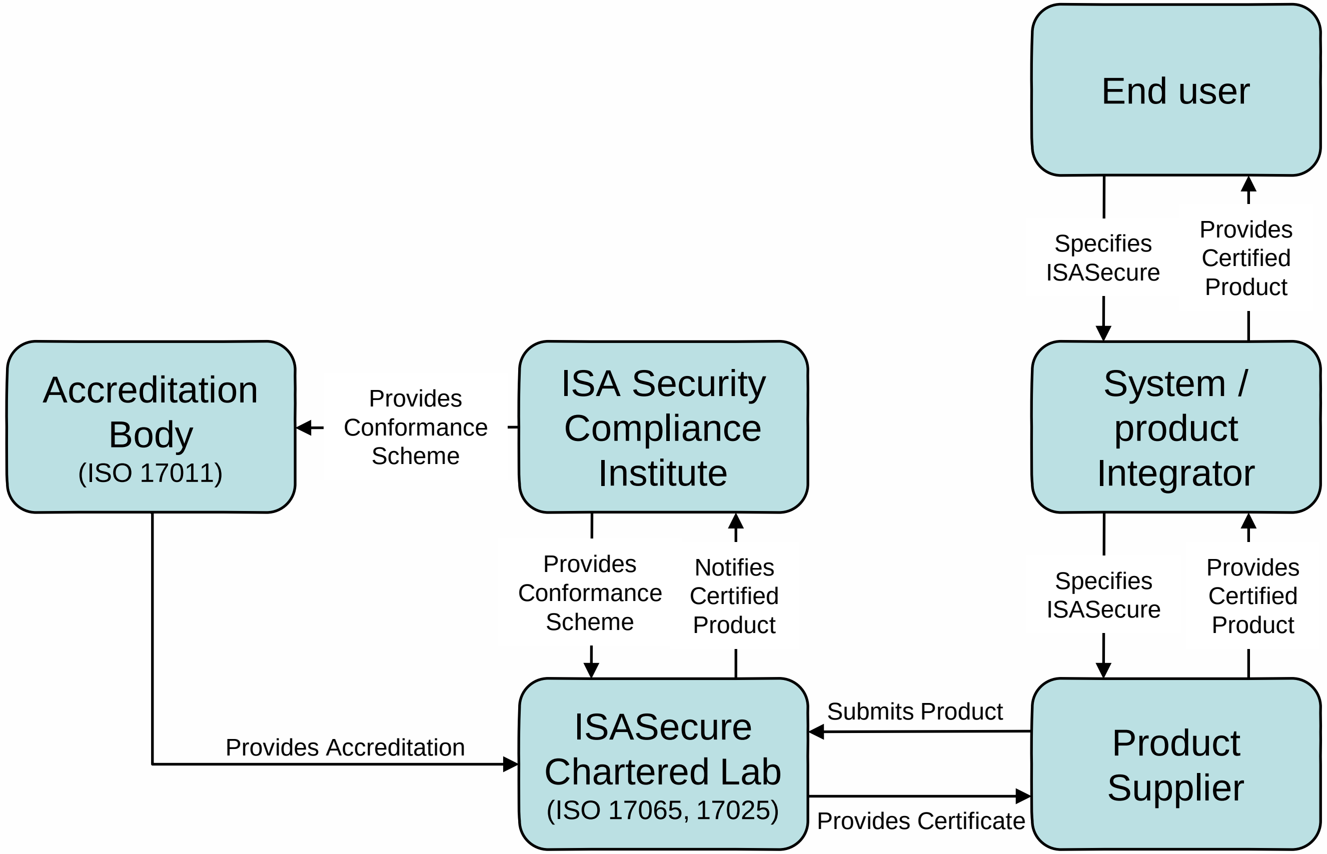
Certification Body

Underwriters Labs (UL)

Kaizen Cyberlab

More than 15 +/- additional companies are in the membership application process to support ISASecure and the Asset Owner ACSSA certification scheme.

ISASecure ISO 17065 conformance scheme for product suppliers


End user
Specifies ISASecure
Provides Certified Product
Accreditation Body
(ISO 17011)
Provides Conformance Scheme
ISA Security Compliance Institute
System / product Integrator
Provides Conformance Scheme
Notifies Certified Product
Specifies ISASecure
Provides Certified Product
Provides Accreditation
ISASecure Chartered Lab
(ISO 17065, 17025)
Submits Product
Provides Certificate
Product Supplier

ISASecure is structured to facilitate global scaling of certification operations

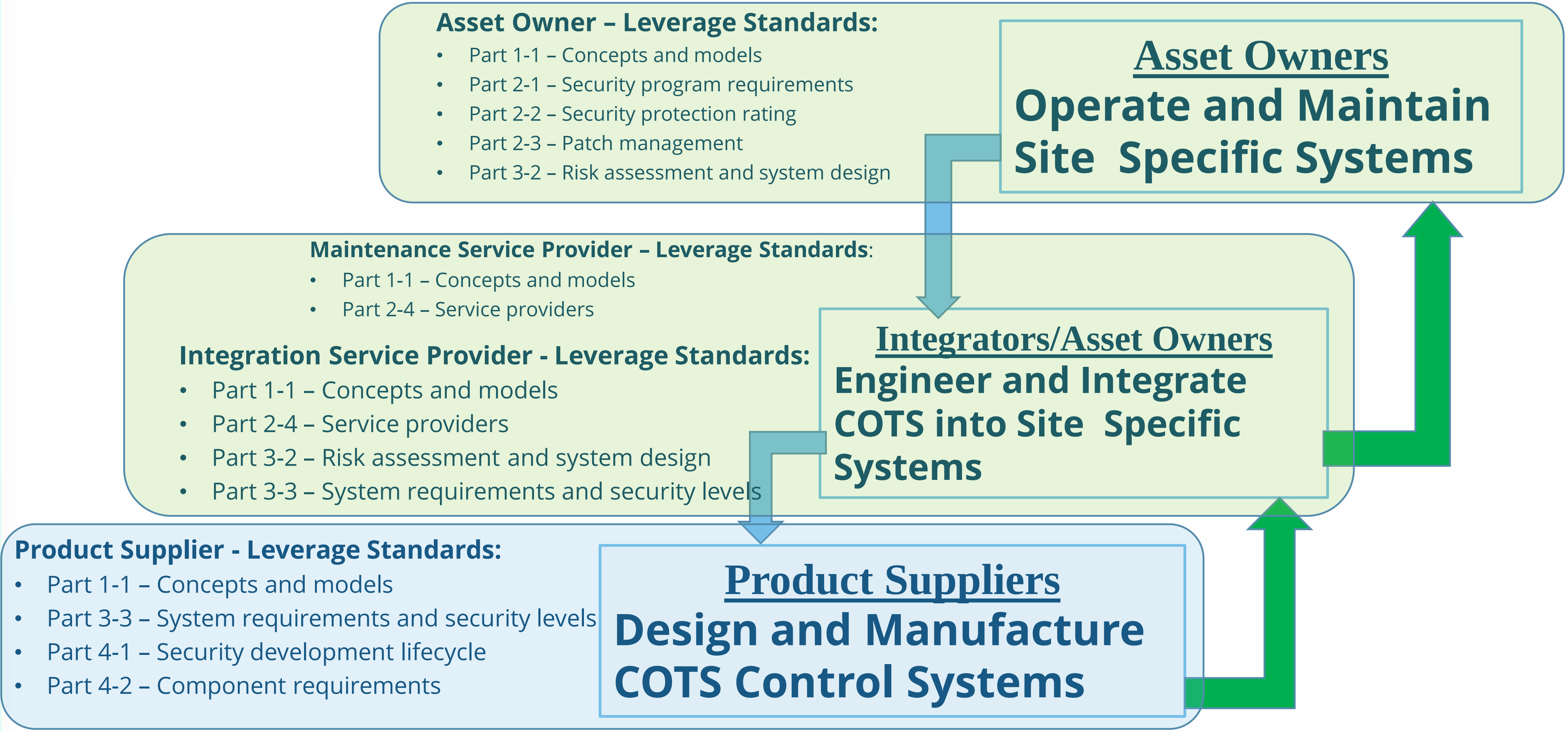
ISAecure® Accreditation Bodies and Certification Bodies

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

(Must be IAF Signatories for global MLA)

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	Singapore / Global
Ikerlan	Spain / Global

ISA/IEC 62443 Automation Security Lifecycle and Shared Stakeholder Responsibility for Cybersecurity



Asset Owner – Leverage Standards:

- Part 1-1 – Concepts and models
- Part 2-1 – Security program requirements
- Part 2-2 – Security protection rating
- Part 2-3 – Patch management
- Part 3-2 – Risk assessment and system design

Asset Owners

Operate and Maintain Site Specific Systems

Maintenance Service Provider – Leverage Standards:

- Part 1-1 – Concepts and models
- Part 2-4 – Service providers

Integration Service Provider - Leverage Standards:

- Part 1-1 – Concepts and models
- Part 2-4 – Service providers
- Part 3-2 – Risk assessment and system design
- Part 3-3 – System requirements and security levels

Integrators/Asset Owners

Engineer and Integrate COTS into Site Specific Systems

Product Supplier - Leverage Standards:

- Part 1-1 – Concepts and models
- Part 3-3 – System requirements and security levels
- Part 4-1 – Security development lifecycle
- Part 4-2 – Component requirements

Product Suppliers

Design and Manufacture COTS Control Systems

Currently Available Certifications

Future Availability

ISASecure®

ISASecure Certifications CY2023 YTD

SDLA – Development Lifecycle Certification ISA/IEC 62443-4-1

1. Johnson Controls (Companywide/Cork Ireland)
2. Energy Team S.p.A. Milano, Italy
3. Emerson Austin, TX
4. Emerson Manila, Phiipines
5. Emerson Pune, India
6. Emerson Warsaw, Poland
7. Envision Digital International, Singapore
8. Envision Digital Co., Ltd. Shanghai PFTZ, China
9. Beijing Consen Technologies Ltd. Beijing, China
10. DigitalPlatforms S.p. A. Cadeo, Italy
11. Inductive Automation, Folsom, CA/Companywide
12. Cisco Systems, Inc., San Jose, CA / Bangalore, India
13. Honeywell Process Solutions, Phoenix, AZ USA
14. Schneider Electric, Companywide/(Rueil-Malmaison, FR)
15. Honeywell Building Technologies,

CSA/ICSA – Component Certification ISA/IEC 62443-4-2 & 4-1

1. DigitalPlatforms CPU STCE-SG Version Cybersecure

SSA – System Certification ISA/IEC 62443-3-3

1. Schneider Electric Tricon/Triconex
2. Emerson DeltaV DCS and SIS

ISASecure Certifications CY2022

SDLA – Development Lifecycle Certification
ISA/IEC 62443-4-1

1. Higeco S.r.l. Italy
2. Moxa Inc., New Taipei City Taiwan
3. Emerson Measurement Solutions Global Development Organizations
4. Valmet Automation Tampere, Finland
5. Carrier Corporation Palm Gardens, FL USA
6. Atop Technologies Zhubei, Taiwan
7. Schneider Electric Foxboro, MA USA
8. Schneider Electric Hyderabad, India
9. Schneider Electric, Lake Forest USA
10. Schweitzer Engineering Labs, Company Wide
11. ABB Malmo and Vasteras Sweden, Minden Germany, Bangalore India
12. Otis Elevator, Worldwide
13. Yokogawa, Singapore
14. Yokogawa, Tokyo
15. Hygec, Bullono Italy
16. ABB, Bangalore India

CSA/EDSA – Component Certification
ISA/IEC 62443-4-2 & 4-1

1. Moxa Industrial Computer
2. Hirschmann Firewall
3. JCI Centrifugal Chiller Controller
4. Honeywell Experion C300 DCS
5. Honeywell Experion CN100 DCS
6. Hirschmann Industrial Switch
7. JCI Centrifugal Chiller Controller YZ & YK
8. Yokogowa Prosafe-RS Lite
9. Higec, HSC-110-C V5.1 Embedded Device

SSA – System Certification
ISA/IEC 62443-3-3

1. ABB Ability System 800xA
2. Schneider Electric Tricon/Triconex
3. Emerson DeltaV DCS and SIS

ISASecure Certifications Currently Available

Certification Description	Certification Mark	Start 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

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 plus 16 extensions	Certified IIOT System ISASecure	TBD
Automation System Security Assurance (ACSSA) ISA/IEC 62443 2-1, 2-4, 3-2, 3-3	"ISASecure IEC 62443 ACSSA"	2H 2024

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

IIOT 62443 Solution (includes cloud provider) study available in Q4 2023

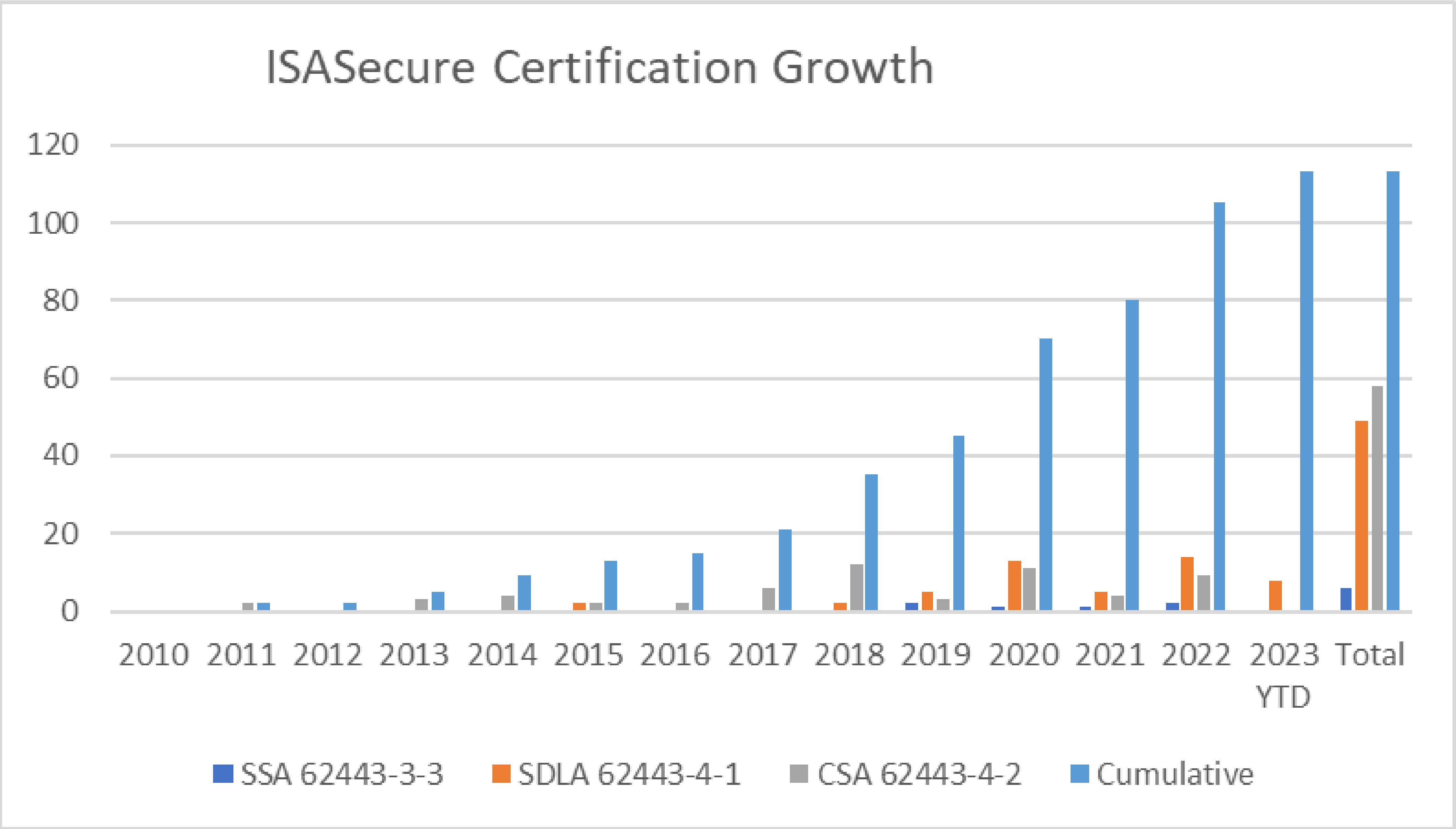
ISASecure Product Certification Enhancements

OEM (Re-label) certification policy – provides policies and procedures for CB’s, OEM’s and (re-labelers) suppliers to address:

1. initial certification
2. maintenance of certification
3. Security lifecycle (62443-4-1) integrity (responsibilities of OEM vs re-labeler)

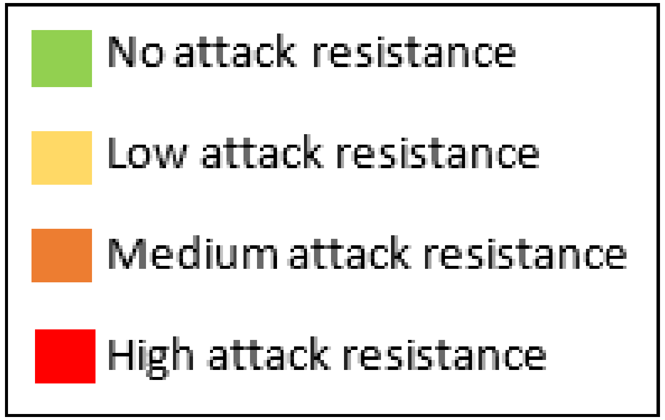
Product Family certification policy – provides policies and procedures for defining and certifying product families. This creates economic efficiencies for suppliers certifying products that have verifiable common attributes but offered in multiple versions (e.g. packaging).

Market surveillance certification policy for incident response– establishes a random audit process of supplier’s incident response artifacts to verify that the supplier is meeting response times and is following 62443-4-1 requirements.

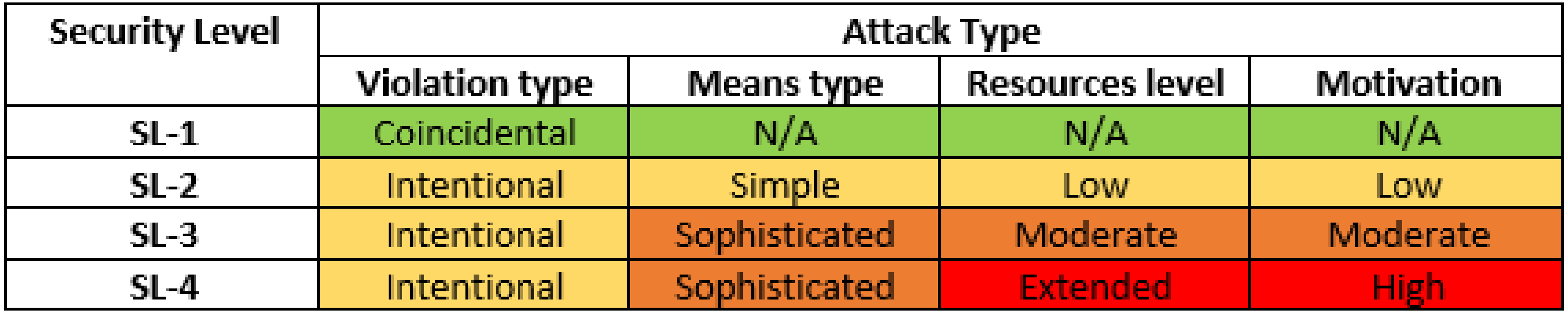

ISASecure Certification Growth
120
100
80
60
40
20
0
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023 YTD
Total
■ SSA 62443-3-3
■ SDLA 62443-4-1
■ CSA 62443-4-2
■ Cumulative

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 OPA Specification.

Industry Collaboration Initiatives

1. **ISA99 Standards committee** liaison for various initiatives (IIOT for example)
2. **DOE S2G IAB –** Advising on US DOE Solar DER security specification**.**
3. **OPAF**-providing ISASecure cybersecurity certifications for OPAS modules
4. **BCS** – Collaborating on a Smart Building Technology site deployed IACS certification based on ISA/IEC 62443 asset owner standards: 2-1, 3-2, 3-3, 2-3, 2-4
5. **LOGIIC –** sharing analysis results on IIOT solutions,
6. **BPS Working Group** - hosting forum for Bulk Power Systems (BPS) supply chain security, starting with response to *EO13920 Securing Bulk Power Systems. Posted a response to the critical software supply chain.*
7. **ISCI - ISAGCA** various collaborations including standards cross reference, joint study to determine how the **ISA/IEC 62443 standards can be applied to IIOT devices and systems**.
8. **NATF – North American Transmission Forum**-electric power transmission sector. Promote adoption of ISA/IEC 62443 in procurement specifications for electric sector.

ISASecure®

ISA/IEC 62443 Adoption by Suppliers

Product suppliers have been developing automation **products conformant to ISA/IEC 62443** cybersecurity standards since 2010. Company examples include:

ABB, Aveva, Azbil, Bayshore Networks, Carrier Corporation, CISCO, Eaton, Emerson Automation Solutions, Emerson Power & Water Solutions, GE Power Conversion, Hima, Hitachi, Honeywell, Johnson Controls, Nexus Controls, Rockwell Automation, Schneider Electric, Siemens, SEL, Toshiba, Yokogawa, Valmet, Wartsila, and many others.

(see examples on www.isasecure.org)

Certifications are offered by **ISASecure** and other global certification programs.

Automation and Control Systems Security Assurance (ACSSA) Certification

Based on ISA/IEC 62443

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

For Asset Owners

September 2023

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

Mission and Vision for ACSSA

Mission

Publish a consensus specification and establish a global scheme for assessing and certifying the cybersecurity of automation and control systems in use at asset owner sites based on the Asset Owner series of ISA/IEC 62443 standards.

Vision

The assessment specification and resulting standard report will become the de-facto foundational document of reference for assessing and certifying OT cybersecurity, globally, by asset owners, consultants, certification bodies and public policy makers….much like the GAAP standards developed by FASB for financial accounting.

Why ISA and ISASecure?

ISASecure has a successful track record in standing up globally recognized conformity assessment programs….ISASecure is the **FIRST** and most recognized international COTS product cybersecurity certification program for OT.

ISA is a global automation engineering professional society with over 15,000 members and has been developing world class standards for over 75 years, including ISA/IEC 62443….and is viewed as THE authoritative source.

ISA trains thousands of automation professionals around the globe every year on a variety of topics including automation cybersecurity.

Leading asset owners and automation suppliers agreed that ISA was the authoritative organization to develop the assessment program.

Automation and Control Systems Security Assurance (ACSSA) Certification

(Personnel, hardware, software, and policies)

ACSSA assesses and/or certifies automation and control systems at asset owner facilities

- Seeking visionary companies and thought leaders.

- Development of ACSSA assessment specification began in 2023.

- References the asset owner series of ISA/IEC 62443 Industrial Automation and Control Systems (IACS) cybersecurity standards.

- Assesses hardware, software, personnel, and policies per ISA/IEC 62443:

  - 62443-2-1 – Security program requirements
  - 62443-2-4 – Service providers
  - 62443-3-2 – Risk assessment and system design
  - 62443-3-3 – System requirements and security levels

Who will use the ACSSA Assessment Specification

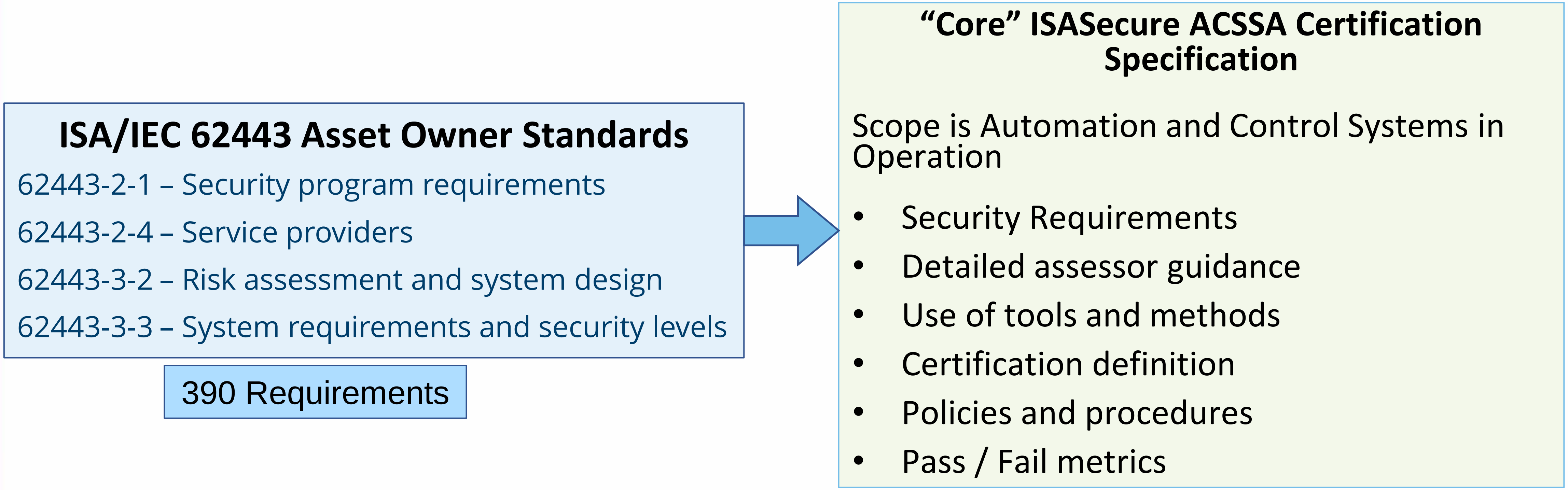
- **Asset owners**, internally, for self assessments or for consultants and other third parties doing the assessments on the asset owner's behalf to standardize the process and reports.

- **Consultants** when doing assessments for clients, resulting in an industry standard assessment process and report.

- **Certification Bodies** (CB) to conduct conformity assessments to the ACSSA specification, certifying conformance to the referenced ISA/IEC 62443 asset owner standards. Based on ISO 17020 Inspection Body standard.

- **Public policy makers** such as regulatory and legislative authorities, ACSSA becomes the definitive reference program when creating public cybersecurity policy.

Development of ACSSA Scheme from ISA/IEC 62443



ISA/IEC 62443 Asset Owner Standards

62443-2-1 – Security program requirements

62443-2-4 – Service providers

62443-3-2 – Risk assessment and system design

62443-3-3 – System requirements and security levels

390 Requirements

“Core” ISASecure ACSSA Certification Specification

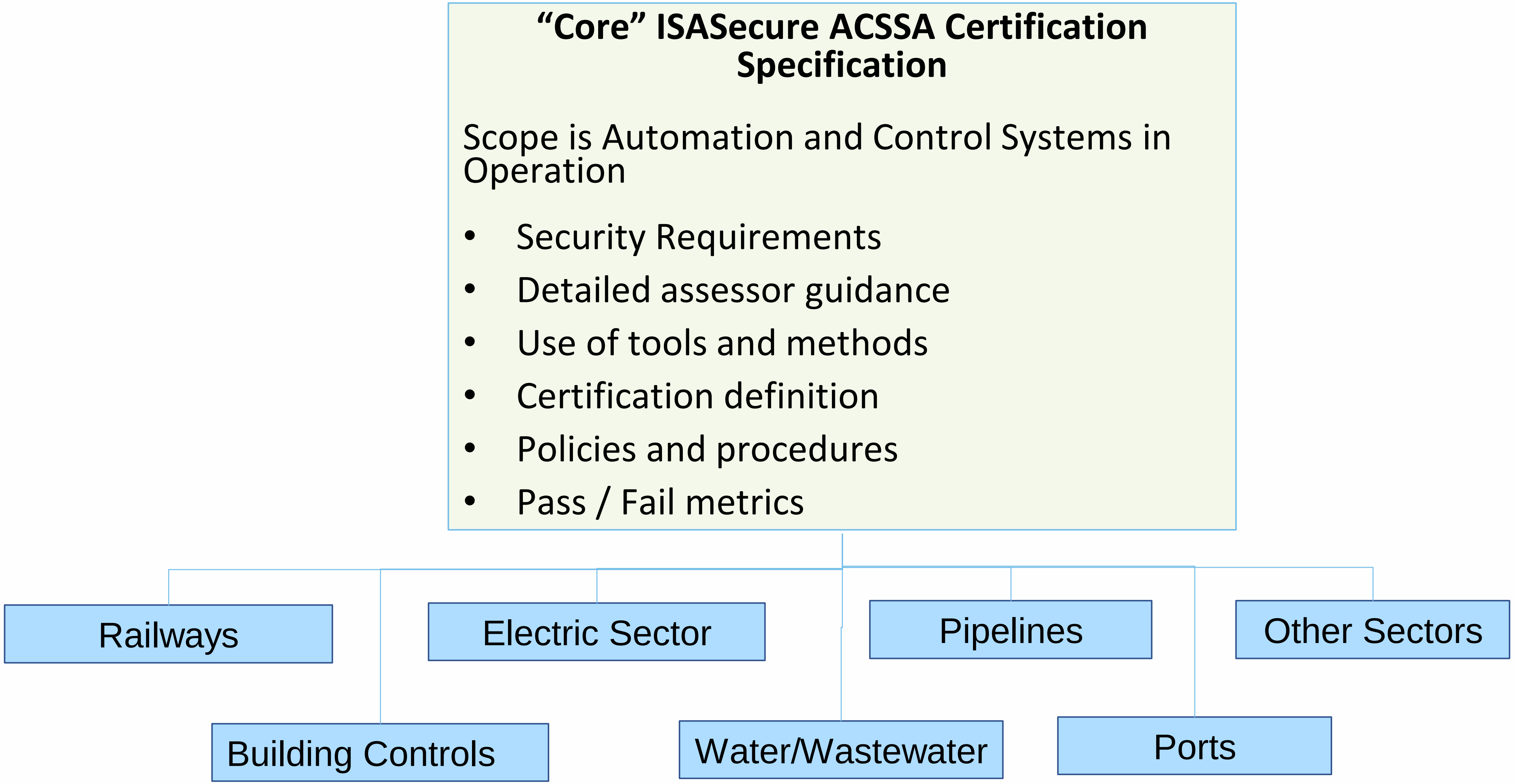
Scope is Automation and Control Systems in Operation

- Security Requirements
- Detailed assessor guidance
- Use of tools and methods
- Certification definition
- Policies and procedures
- Pass / Fail metrics

Supporting Program Elements:

- Assessor Company Accreditation
- Assessor Personnel Credentialing
- Three-day ACSSA training class

Core Specification will be baseline for any other ISA/IEC 62443 sector security profiles



“Core” ISASecure ACSSA Certification Specification

Scope is Automation and Control Systems in Operation

- Security Requirements
- Detailed assessor guidance
- Use of tools and methods
- Certification definition
- Policies and procedures
- Pass / Fail metrics

The Ask for Funding and/or Resources

Sign-on as an ISASecure Member

Company Size in Annual Revenues (USD)	Annual Dues
Revenues (Under $5M)	$3,000
Revenues (Under 50M)	$5,000
Revenues (under $500M)	$10,000
Revenues ($500M- $1 billion)	$20,000
Revenues ($1-5 billion)	$30,000
Revenues (over $5 billion)	$40,000
Strategic Members (Governing board voting)	$50,000

Valuable member benefits described on next slides.

Member Benefits

- **Publicly demonstrate contributions to industry OT cybersecurity initiatives**. Supporters participate in joint marketing and outreach activities and are listed on the ISASecure website for supporting this industry initiative.
- **Seat at the table**: Participate in the drafting, reviewing, and approval of program/specifications. Help shape the scheme that will become the de-facto global reference specification used by operating sites, certification bodies, internal auditors, and public policy makers.
- **Cost Savings**: Internal cost for an individual company to develop the ACSSA program would exceed $500,000 to develop and $200,000 per year to maintain.
- **Discounts on ISA products and services**: Members receive discounts on ISA cybersecurity training, ISASecure assessor training, and specification licensing.
    - ISA Cybersecurity Volume Training discount **25%** - **40%**
    - ISASecure assessor training discount **30%**
    - ISASecure ACSSA specification annual license – **free to ISASecure members**
    - ISASecure Product Certification Specifications **free**

Member Benefits (continued)

- **Formal, Standardized Reports**: Using the ISASecure specification and its standardized reporting format provides a consistent basis for assessing IACS regardless of who does the work; any employee and/or any third-party assessor.

- **Objective basis for multi-year cybersecurity plans and budgets**: Provides basis for company cybersecurity plan; standardized gap reporting across the OT enterprise establishes mitigation priorities, workforce development, plans, and budgets.

- **Credible basis for insurance negotiations**: An objective, industry consensus assessment specification provides credibility for assessing risk and insurability.

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

ISASecure®

Planned Milestone Dates

- **June 2024 – ACSSA assessment specifications complete**
- **Dec 2024 – ACSSA program definition, policies/procedures, CB accreditation specifications complete**
- **Dec 2024 – Assessor Training class complete (3-day class)**
- **Jan 2025 – ACSSA available for asset owners, consultants, certification bodies**

Cybersecurity Resources at ISA

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

ISASecure web page with ACSSA program details https://isasecure.org/isasecure-site-assessment-0

ISA Global Cybersecurity Alliance - https://isagca.org/

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

In 2021, ISA established a cybersecurity incident command system for industrial control systems. www.ics4ics.org

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

Societal Benefits of ACSSA Certification

A consistent set of requirements and associated assessment scheme will provide objective reporting that will be useful for all stakeholder groups including:

- **Asset Owners** who will have visibility into their operating sites' security posture; and have an objective, consistent benchmark to determine their standing with their peers and their industry. This will also provide guidance for selecting technology, service providers, organizational development, and negotiating with insurers.

- **Insurance Underwriters** where the assessments will provide objective, consistent metrics to include in their underwriting risk models for industrial environments. Over time, the data can be used as input to actuarial models for analysis.

- **Service Providers and Product Suppliers** who will get clarity and transparency regarding their cybersecurity role in automation products, integration, maintenance, and operation support services; and provide structure to SLA agreements.

- **Assessment Organizations** will benefit from increased demand in services due to the attractiveness of a consensus OT assessment scheme based on trusted 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 for incentives and mandates to secure critical infrastructure. TSA, NERC, others