International Society of Automation ISASecure® Program Status and Roadmap

www.isasecure.org

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.

Andre Ristaino

Mr. Ristaino is the Managing Director of Global Alliances, Consortia and Conformance programs for the International Society of Automation (ISA) based in RTP, North Carolina. Starting in 2007, Mr. Ristaino developed ISA's conformance certification programs including the ISASecure® control systems cybersecurity certification program that certifies automation and control system products to the IEC 62443 series of international standards. Mr. Ristaino directs ISA's consortiums and alliances, including, ISA Security Compliance Institute, ISA Wireless Compliance Institute, ISAGCA, LOGIIC, FCG collaboration, OPAF collaboration, FDT collaboration, ISA Bulk Power Systems WG, Building Cybersecurity (BCS), and Fundacion Chile. Mr. Ristaino is an international presenter on the ISA/IEC 62443 standards and automation/control systems security certifications.

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. Industries served include state and local government, utilities, USAF-LC, discrete manufacturing and, pharmaceutical and FDA regulated manufacturing sites.

Mr. Ristaino earned a BS in Business Management from the University of Maryland, College Park and an MS in Computer Systems Applications from the American University in Washington DC with a focus on expert systems and artificial intelligence. Mr. Ristaino holds an APICS CPIM certification.

Contact: aristaino@isa.org

+1 919-323-7660

15,822
MEMBERS

186
SECTIONS

109
COUNTRIES

350,000
CUSTOMERS

- STANDARDS
- EDUCATION
- CERTIFICATION
- CONFERENCES
- PUBLICATIONS
- COMPLIANCE

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

ISA99 Global Cybersecurity Standards Committee (ISA/IEC 62443)

- ISA/IEC 62443 standards address OT in 16 CI sectors, non-telecom & finance. Water & Wastewater, power generation & distribution, O&G, pipelines, building automation (smart buildings & smart cities), medical equipment, food & pharma, manufacturing & industrial…and maritime on-board controls.

- The ISA99 committee was **formed in 2002 –** works closely with technical committee 65 of the International Electrotechnical Commission (IEC).

- ISA/IEC 62443 standards contain **over 500 normative requirements** and associated rationale that address all phases of the system life cycle,

- The **committee has over 1,000 volunteer members,** representing a wide range of industry sectors and constituency groups from all areas of the world.

- The ISA99 committee includes **formal and informal liaison relationships with** other standards development organizations, consortia and interest groups such as IEC, OPAF, NAMUR, WIB, NIST, DHS, INL, ISASecure, and ISAGCA.

- **ISA/IEC 62443 is the most referenced standard in the NIST CSF**

ISA/IEC 62443 Status

ISA/IEC 62443 is a technical horizontal standard as of 2021.

Industry sectors must adopt ISA/IEC 62443 for their cybersecurity requirement in IEC industry sector standards by creating sector specific **'security profiles'.**

Sectors that we know are adopting ISA/IEC 62443:

1. BCS-Smart Buildings/Smart Cities (building control/building management systems).
   BCS Framework completed in 2021 by ISCI/NEMA/BCS.
2. Medical Devices – Usage guide for applying ISA/IEC 62443 for securing medical devices. **Completed in 2015** by MDISS.
3. Electric Power –**Security profile development** for substations started 16 June ISA99 WG14
4. **DER** (Distributed Electric Resources-wind/solar) – Security profile in start up phase in USA.
5. **Water and Wastewater** industry is evaluating ISA/IEC 62443 for a WWW sector profile**.**
6. **International Association of Classification Societies (IACS)** – Maritime standards UR-E26 and UR-E27 mandatory conformance for onboard controls effective 01 Jan 2024 referencing ISA/IEC 62443.

Global IOT Cybersecurity Legislation

European Union ETSI EN 303 645 is a globally applicable standard for **consumer IoT** cyber security; it covers all consumer IoT devices while establishing a good security baseline. The standard is based on 13 high-level recommendations, used to establish 68 provisions, 33 mandatory requirements and 35 recommendations.

EO 14028 - USA Voluntary Consumer IOT Labeling Scheme is one of the directives in EO 14028. Strategy meetings held at White House in October 2022. 50 Member advisory board formed to lead the initiative with an aggressive startup date in March 2023. Largely based on *NISTIR 8425 Profile of the IoT Core Baseline for Consumer Products* and *ETSI 303 645*. NIST's Katarina Megas suggests including ISA/IEC 62443 requirements as well.

ISASecure has been collaborating with the Consumer Technology Association on the US Consumer IOT labeling scheme initiative. Objective is to ensure the consumer and industrial IOT overlaps are properly addressed.

CRISP Act – **State of New York in USA** processing policy legislation that references ISA/IEC 62443 for securing critical infrastructure and for measuring conformance for owner/operator incentives and mandates.

Malaysia – ISA/IEC 62443 referenced in public policy language for securing critical infrastructure

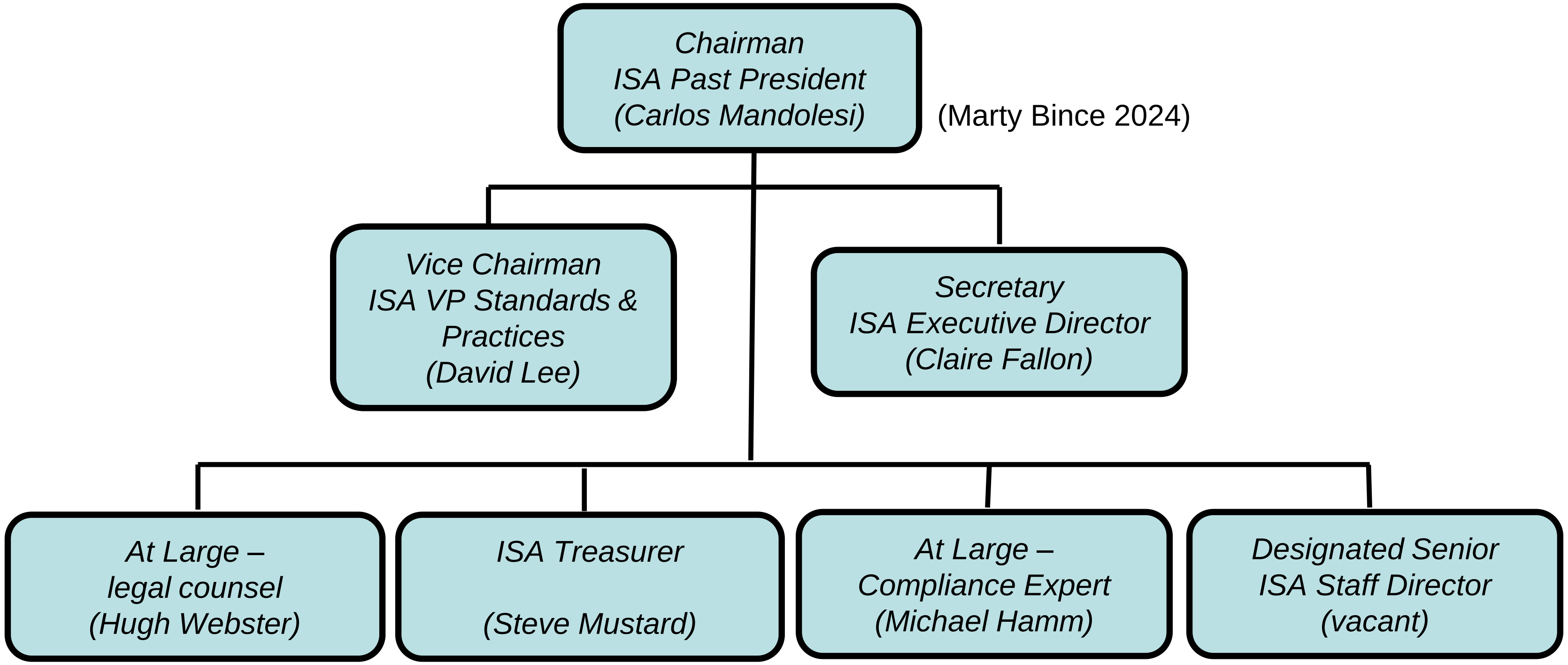
Singapore – ISA/IEC 62443 referenced in public policy language for securing critical infrastructure

International Association of Classification Societies (IACS) – Maritime standards UR-E26 and UR-E27 mandatory conformance for onboard controls effective 01 Jan 2024 referencing ISA/IEC 62443.

ISASecure®

2023 Automation Standards Compliance Institute Board

Oversees ISA Conformity Assessment Programs



Chairman
ISA Past President
(Carlos Mandolesi)

(Marty Bince 2024)

Vice Chairman
ISA VP Standards & Practices
(David Lee)

Secretary
ISA Executive Director
(Claire Fallon)

At Large –
legal counsel
(Hugh Webster)

ISA Treasurer

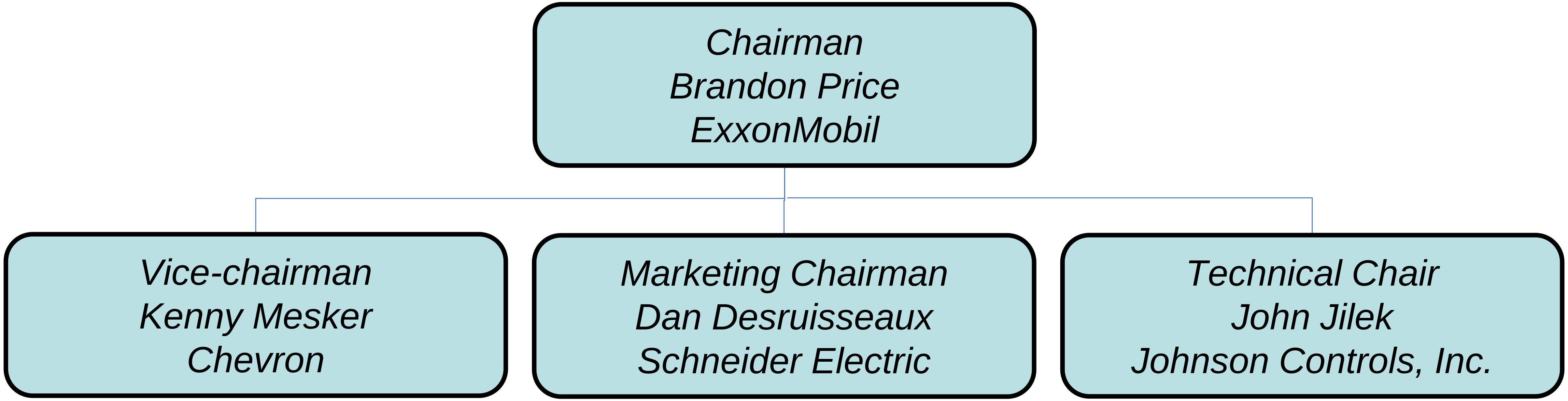
(Steve Mustard)

At Large –
Compliance Expert
(Michael Hamm)

Designated Senior
ISA Staff Director
(vacant)

ISASecure®

ISA Security Compliance Institute (ISCI) Governing Board



Chairman
Brandon Price
ExxonMobil

Vice-chairman
Kenny Mesker
Chevron

Marketing Chairman
Dan Desruisseaux
Schneider Electric

Technical Chair
John Jilek
Johnson Controls, Inc.

Governing Board Companies

Chevron
Honeywell
Yokogawa
ExxonMobil
Johnson Controls, Inc.
Schneider Electric
Carrier Global
Saudi Aramco
ISA99 Committee Liaison

ISASecure®

ISASecure Members

aws

bp

Chevron

ExxonMobil

YPF

ارامكو السعودية
Saudi Aramco

FM Approvals®
Member of the FM Global Group

Honeywell

Rockwell Automation

Schneider Electric

SIEMENS
Ingenuity for life

HITACHI
Inspire the Next

BYHON

TAF Taiwan Accreditation Foundation

exida.com

YOKOGAWA

ISA

CSSC

SYNOPSYS®

SCC ccn 50

Applied Risk

WisePlant®

TÜVRheinland®
Precisely Right.

GE Digital

BEYOND security

KPMG

Johnson Controls

PROD JAB

TRUSTCB®

BUREAU VERITAS 1828

DNV·GL

TÜV SÜD

Carrier

Singapore Accreditation Council

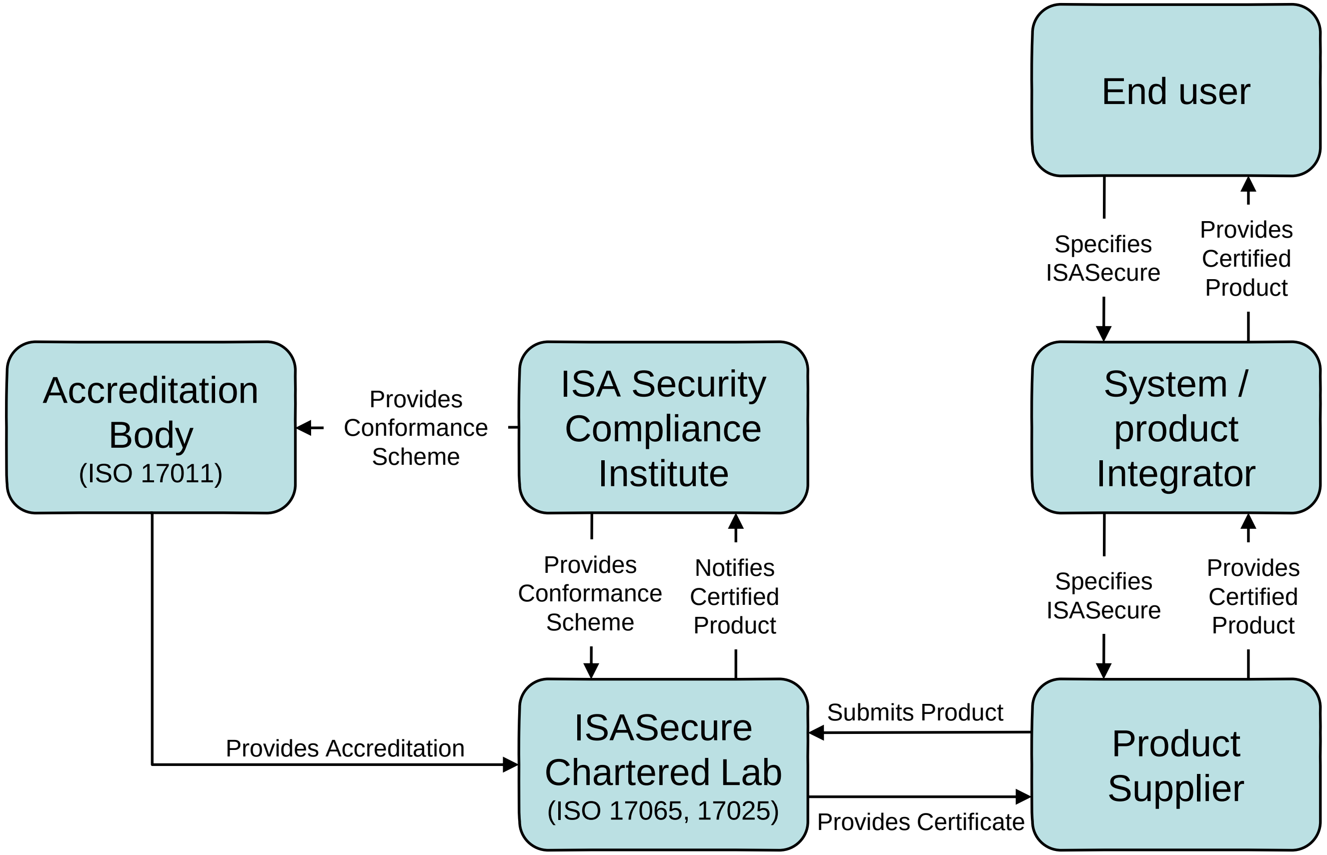
ANSI
ANSI Accredited Program
PRODUCT CERTIFICATION

ANAB
ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS CERTIFICATION BODY

ilac-MRA

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

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

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

a2la

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

PROD
JAB

SCC CCN 50 YRS 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 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

ISASecure®

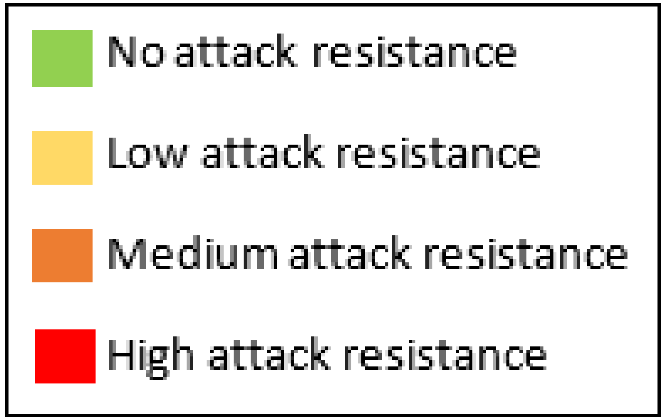
ISASecure Certification Expansion Roadmap

Certification Description	Certification Mark	Availability Date
IIOT System Security Assurance (ISSA) ISA/IEC 62443 4-1 and ISA/IEC 62443 3-3 plus 16 extensions	Certified IIOT System ISASecure	TBD
IACS Security Assurance (IACSSA) (formerly Site Assessment) ISA/IEC 62443 2-1, 2-3, 2-4, 3-2, 3-3	Certified IACS ISASecure	2H 2024

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

IIOT 62443 System Study (includes cloud provider) study will be available in Q2 2023

ISA/IEC 62443 Component and System Security Levels

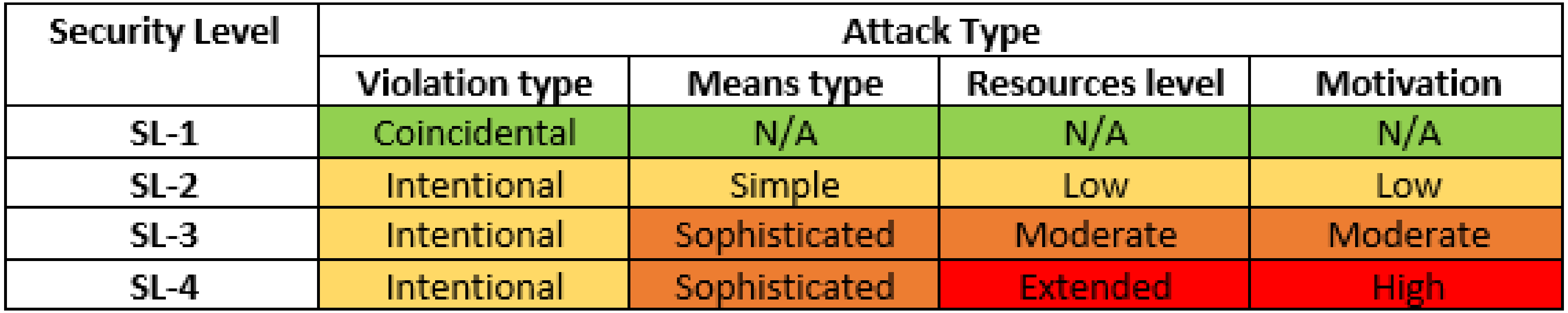


🟩 No attack resistance

🟨 Low attack resistance

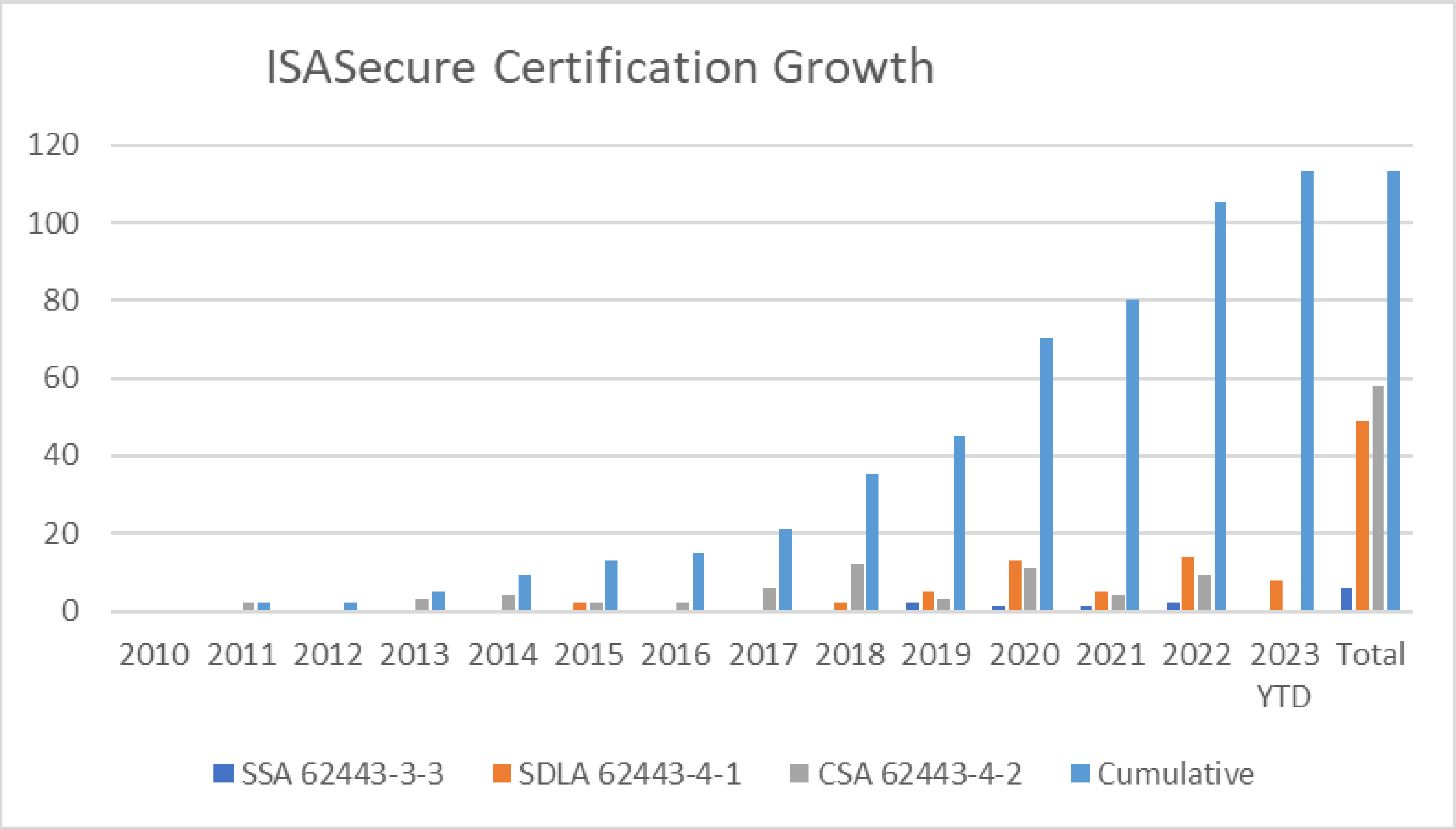
🟧 Medium attack resistance

🟥 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.


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®

Industry Collaboration Initiatives

1. **ISA99 Standards committee** liaison for various initiatives (IIOT for example)
2. **OPAF**-providing ISASecure cybersecurity certifications for OPAS modules
3. **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
4. **LOGIIC –** sharing analysis results on IIOT solutions,
5. **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.*
6. **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**.
7. **NATF – North American Transmission Forum**-electric power transmission sector. Cross reference supplier questionnaire with ISA/IEC 62443 tPromote adoption of ISA/IEC 62443 in procurement specifications.
8. **NEMA** – Workforce Development for cybersecurity workers and advocating for ISA/IEC 62443 references in public policy language.
9. **AWWA** – Collaboration goals TBD; water/wastewater sector ISA/IEC 62443 security profile

ISASecure®

ISA/IEC 62443 Adoption by Suppliers

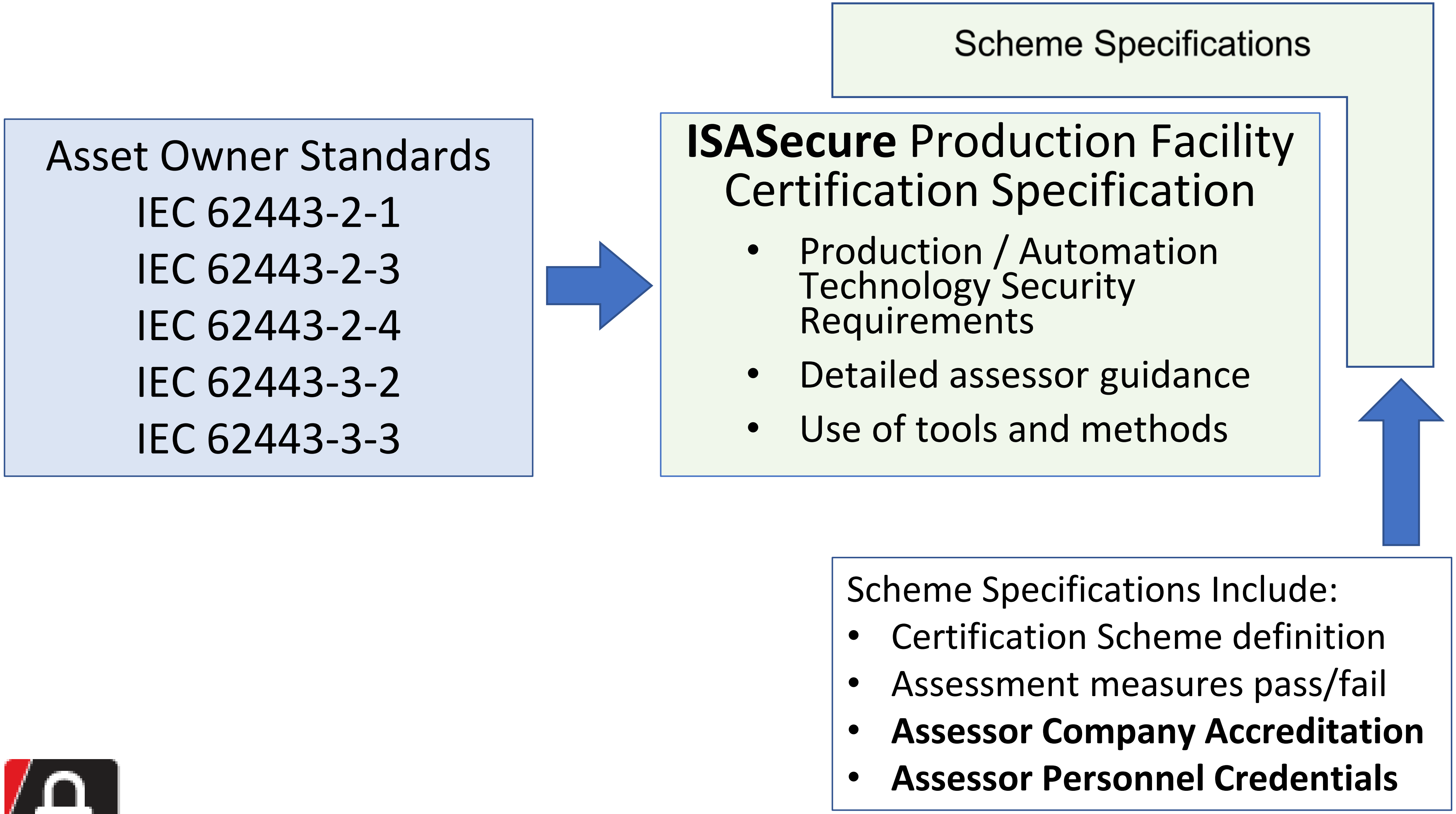
Product suppliers have been developing automation **products conformant to ISA/IEC 62443** cybersecurity standards since 2010. Company examples include:

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, Toshiba, Yokogawa, Valmet, Wartsila, and many others. (see examples on www.isasecure.org)

Certifications are offered by **ISASecure** and individual certification bodies around the globe.

ISASecure®

IACS Security Assurance Scheme (IACSSA)
(formerly *Site Assessment*)



Asset Owner Standards

IEC 62443-2-1

IEC 62443-2-3

IEC 62443-2-4

IEC 62443-3-2

IEC 62443-3-3

Scheme Specifications

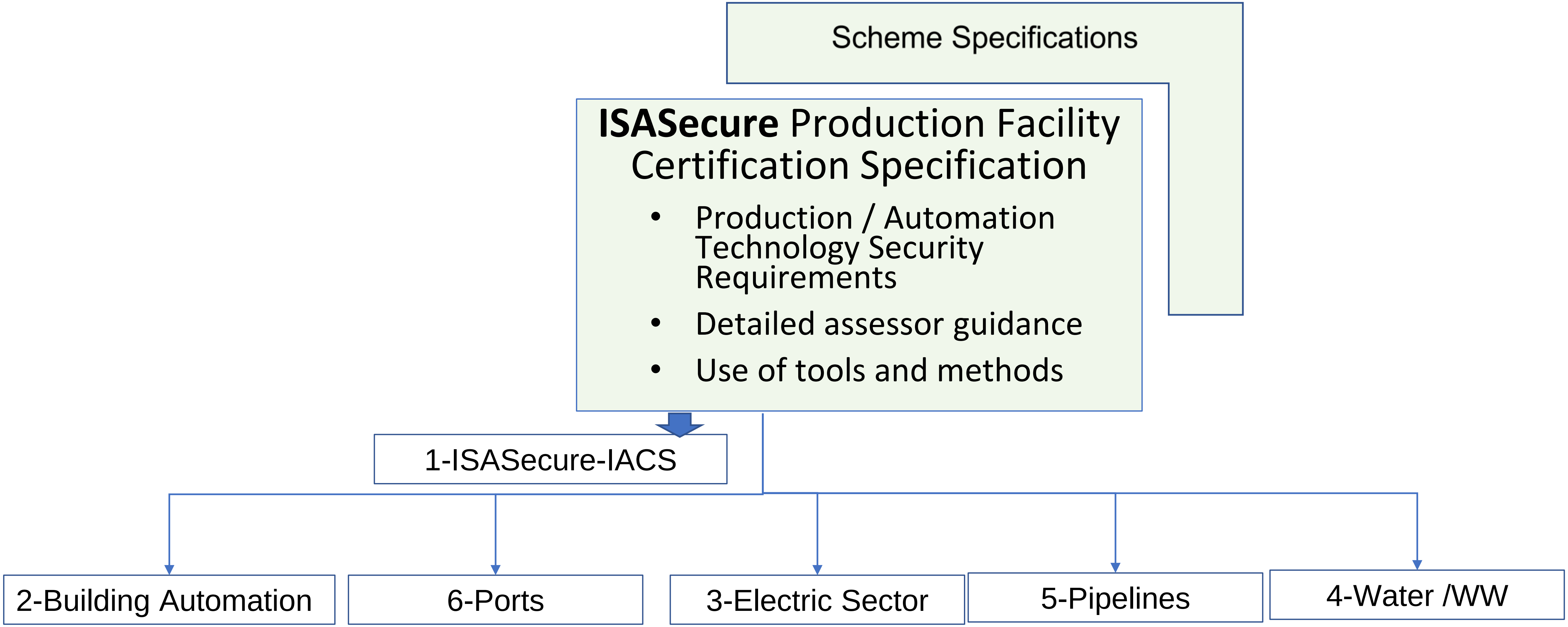
ISASecure Production Facility Certification Specification

- Production / Automation Technology Security Requirements
- Detailed assessor guidance
- Use of tools and methods

Scheme Specifications Include:

- Certification Scheme definition
- Assessment measures pass/fail
- **Assessor Company Accreditation**
- **Assessor Personnel Credentials**

Future - Adapt IACSSA Specification to Other Industry Sectors



Scheme Specifications

ISASecure Production Facility Certification Specification

- Production / Automation Technology Security Requirements
- Detailed assessor guidance
- Use of tools and methods

Societal Benefits of IACSSA Certification Program-Why Now?

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. We have been in discussions with insurers who see the value of a standardized 62443 assessment report.

- **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. Global organizations will realize benefits for being accountable to one set of international standards.

- **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

Supporting Functions -Assessor Company Accreditation

- An accreditation function will be established for the site assessment companies using ISO 170xx accrediting standards, aligned with activities for site inspections
- ISCI has MOUs in place with seven global ISO 17011 accrediting authorities
- Assessment scheme will allow for certification activities or assessment only activities
  - **Certification**-certifies entity conforms to all requirements in a standard
  - **Assessment**-provides report that describes the extent to which an entity conforms

Supporting Functions -Assessor Personnel Credentialing

- ISA Training will administer site assessor training, credentialing and, continuing education

- **Two assessor training classes** will be developed for the Site Assessment program
  - ISASecure Production Facility Assessor **5 class days**
  - ISASecure Building Technology Assessor **5 class days**

- **Professional assessor designations / credentialing** will be established for the program:
  - ISASecure Certified ISA/IEC 62443 Product Assessor
  - ISASecure Certified ISA/IEC 62443 Operating Site Assessor
  - ISASecure Certified ISA/IEC 62443 Service Provider Assessor

Supporting Functions –Compliance Software Applications

- Software vendors already exist that can add the ISASecure site assessment specification to their application. (institutionalizes the specification in owner’s and assessor’s processes)

- ISCI will license the site assessment specification to interested parties (ISASecure product certification specifications already licensed to a limited number of vendors)

- ISCI responsible for developing, maintaining, expanding specifications economically; assures lower cost to licensees due to shared effort in ISASecure consortium

- Software vendors update their applications on a prescribed cadence as program expands

- Consensus specification standardizes ISA/IEC 62443 based assessments globally.

ISASecure Member Benefits

- Members receive discounts on selected ISA cybersecurity training classes

  https://www.isa.org/cybersecurity-training-volume-discount-program

- Members receive discounts on specification license fees and assessor training based on their contribution level (TBD).

- Lower development costs for assessment organizations for an ISA/IEC 62443 standards-based site assessment services offering. Share the burden with other ISCI members.

- ISCI carries the cost to establish and maintain assessor training and credentialing.

The Ask

Support the development and launch of the IACSSA program (formerly *Site Assessment*).

- Donate funding
- Donate resource for specification development
- Publicly endorse site assessment program
- Recruit peers to support the program
- Any one of the above.

1. Complete and submit the ISCI membership application
   - Indicate your membership level desired and donation amount on the form.

2. ISCI will onboard your company and add your representative to the working group(s)

Cybersecurity Resources at ISA

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

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

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

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

ISASecure®