

# International Society of Automation Global Cybersecurity Initiatives

Andre Ristaino

Managing Director, Alliances and Consortia

[aristaino@isa.org](mailto:aristaino@isa.org) 919-990-9222



**GLOBAL**  
CYBERSECURITY  
**ALLIANCE**





**38,500**  
MEMBERS

**135**  
SECTIONS

**44**  
COUNTRIES

**350,000**  
CUSTOMERS

STANDARDS

EDUCATION

CERTIFICATION

CONFERENCES

PUBLICATIONS

COMPLIANCE

# ISA99 Global Standards Committee

- The ISA99 committee was **formed in 2002** to define what is required to secure automation and control systems. For several years the committee has been working closely with technical committee 65 of the International Electrotechnical Commission (IEC) to develop and deliver the ISA/IEC 62443 series of standards that provide requirements and guidance in this area.
- The majority of standards in this series are now available, representing **over 500 normative requirements** and associated rationale that address all phases of the system life cycle, from development and delivery to operation and support.
- The **committee has over 1000 members**, representing a wide range of industry sectors and constituency groups from all areas of the world. Collectively this represents one of the largest and most diverse bodies of expertise in the subject of operations cybersecurity.
- While the committee's primary purpose is the development and enhancement of the ISA/IEC 62443 standards, it also includes work groups devoted to promoting increased awareness, promotion and adoption of proven and effective practices. This is further extended in the form of several **formal and informal liaison relationships with** other standards development organizations, consortia and interest groups such as ISASecure and ISAGCA.
- The ISA99 committee is **willing to engage with sector, industry, government and company programs** in their efforts to address automation systems cybersecurity. Those interested in pursuing such engagements are encouraged to contact the committee leadership at [ISA99chair@gmail.com](mailto:ISA99chair@gmail.com).








# ISA/IEC 62443 Standards


**General**

- ISA-62443-1-1: Concepts and models 
- ISA-TR62443-1-2: Master glossary of terms and abbreviations 
- ISA-62443-1-3: System security conformance metrics 
- ISA-TR62443-1-4: IACS security lifecycle and use-cases 



**Policies & Procedures**

- ISA-62443-2-1: Security program requirements for IACS asset owners 
- ISA-62443-2-2: IACS protection levels 
- ISA-TR62443-2-3: Patch management in the IACS environment 
- ISA-62443-2-4: Requirements for IACS service providers 
- ISA-TR62443-2-5: Implementation guidance for IACS asset owners 

**System**

- ISA-TR62443-3-1: Security technologies for IACS 
- ISA-62443-3-2: Security risk assessment and system design 
- ISA-62443-3-3: System security requirements and security levels 

**Component**

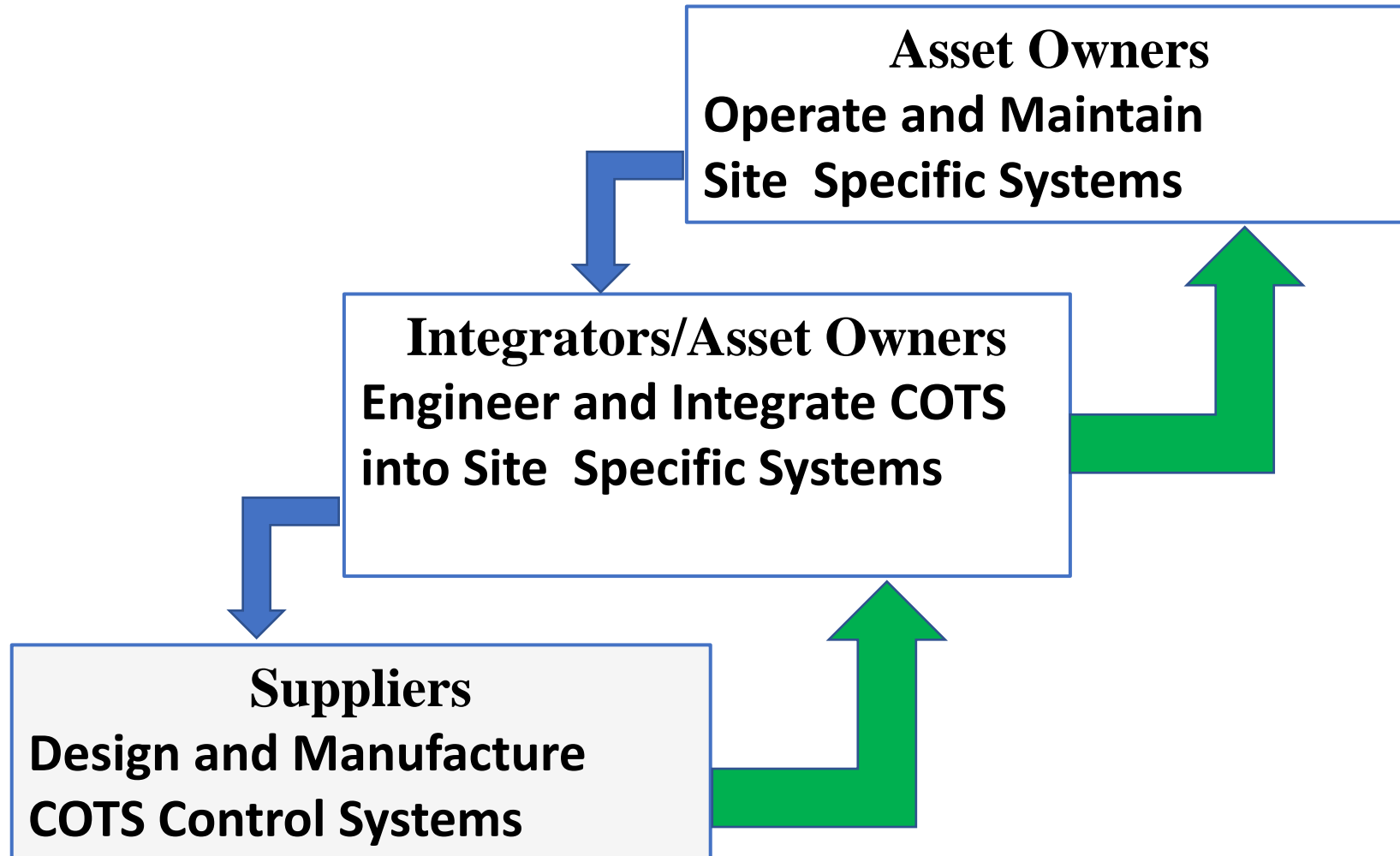
- ISA-62443-4-1: Secure product development lifecycle requirements 
- ISA-62443-4-2: Technical security requirements for IACS components 

**Status Key**

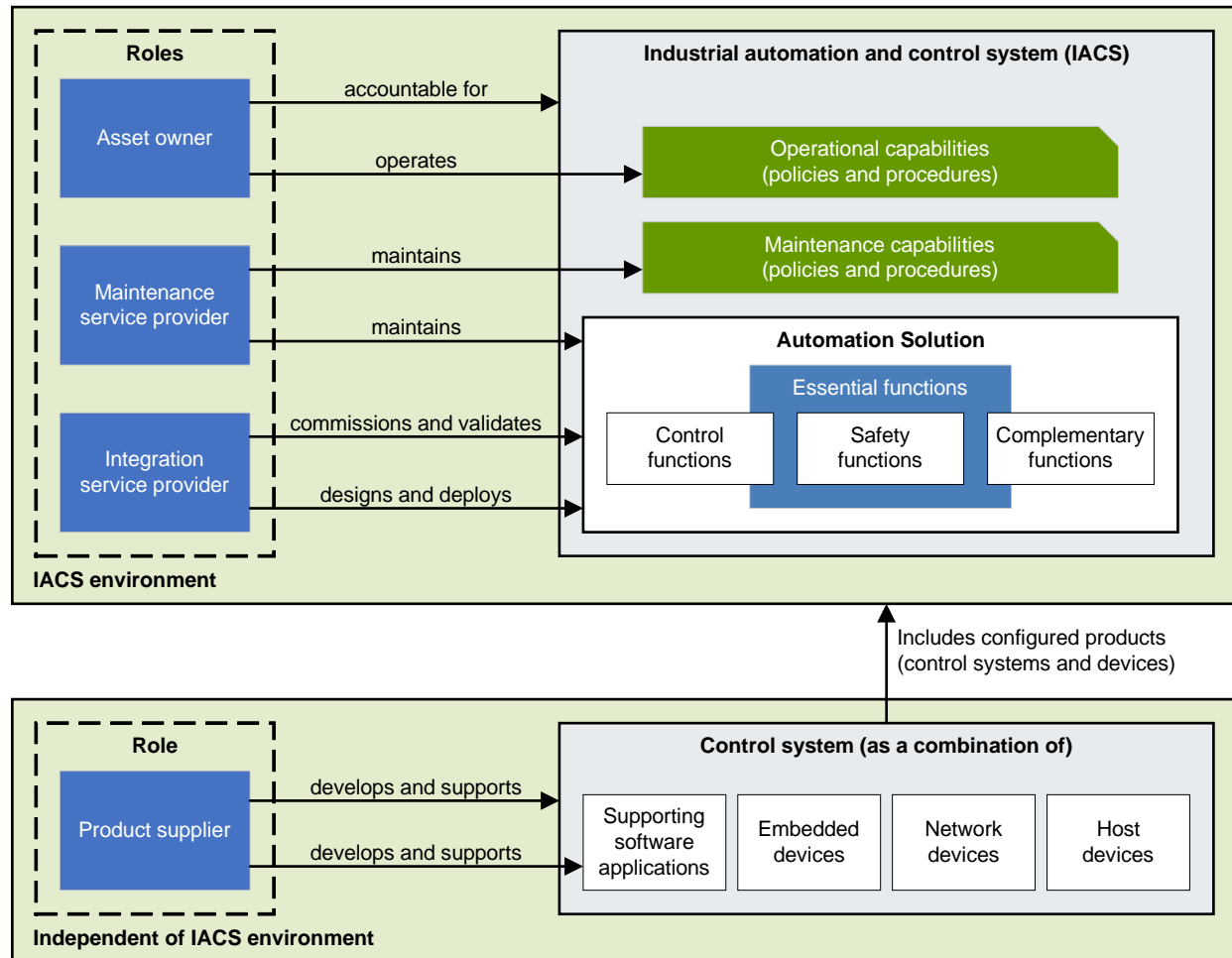
 Development Planned	 In Development	 Out for Comment or Vote	 Approved with comments
 Approved	 Published	 Adopted	 Published (under revision)



# ISA/IEC 62443 Automation Security Lifecycle



# Stakeholder Roles, Responsibilities and relevant 62443 standards



- **Asset Owner**
  - 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
- **Maintenance Service Provider**
  - Part 1-1 – Concepts and models
  - Part 2-4 – Service providers
- **Integration Service Provider**
  - 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
- **Product Supplier**
  - 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

# ISA Cybersecurity Consortiums - Missions



**LOGIIC** - (Linking the Oil and Gas Industry to Improve Cybersecurity)  
Research and development on cybersecurity topics for automation used by the oil and gas industry

<http://www.automationfederation.org/Logiic/Logiic>



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

<https://isaautomation.isa.org/cybersecurity-alliance/>



**ISASecure** - ISA/IEC 62443 cybersecurity certification of COTS products and supplier development processes

.....and ISA/IEC 62443 cybersecurity certification of end-user/asset owner operating sites/facilities (technology, people and process)

<https://www.isasecure.org/en-US/>

# LOGIIC

Research and development on cybersecurity for automation in Oil & Gas industry. Partners with DHS S&T Directorate. ExxonMobil, Shell, BP, Total, Conoco Phillips

- Currently assessing vulnerabilities in safety systems deployed in the O&G industry
- New projects will address 1) cybersecurity in O&G sub-sea exploration and production systems 2) IIOT system vulnerabilities.
- Project findings are published and available on the public facing LOGIIC website. Some sensitive product-specific findings remain confidential.





# ISA Global Cybersecurity Alliance

Bridge the gap between publication of the 62443 standards and adoption by stakeholders.

- Awareness & Outreach
  - Advocacy & Adoption
  - Compliance & Prevention
  - Training & Education
- 
- Launched July 2019
  - 25 members in 2<sup>nd</sup> half 2019; add 50 more in 2020
  - Added industry groups – LOGIIC, ISASecure, ISA99; in discussion with others
  - Globalize - Establish regional teams for outreach activities and regulatory tracking (NA, EU, Japan, MEA) in 2020
  - Complete 8 key projects in 2020



Life Is On

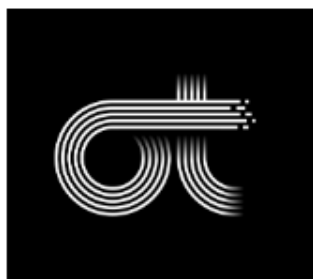
Schneider Electric



Rockwell Automation

Honeywell

Johnson Controls



CLAROTY  
Clarity for OT Networks



NOZOMI  
NETWORKS

munio  
SECURITY



BAYSHORE



DIGITAL IMMUNITY™  
STAY PRODUCTIVE, STAY SECURE

radiflow

MOCANA



xage  
SECURITY

DRAGO



WisePlant  
Smart, Safe & Secure

WALLIX  
CYBERSECURITY SIMPLIFIED

ae  
Solutions™

PAS



威努特  
WINICSSEC



tenable™



MSI  
Mission Secure, Inc.

tripwire

exida®

INL  
Idaho National Laboratory

senhasegura  
by MT4 TECHNOLOGY GROUP

Ti Safe

# 2019 ISAGCA Projects Underway

1. An easy-to-follow, condensed **how-to guide to using the ISA/IEC 62443** series of standards
2. A consolidated matrix that **cross-references Key global cybersecurity** standards to ISA/IEC 62443
3. A **coordinated program to educate and support** member's legislative affairs staff to ensure that ISA/IEC 62443 is the reference standard for OT cybersecurity in their regional regulatory requirements or recommended practices.
4. **Workforce development-** A multi-dimensional reference guide mapping system lifecycle phases and **stakeholder roles** to specific automation cybersecurity knowledge, skills, and abilities needed to manage each phase
5. **Industry vertical overlays** to the ISA/IEC 62443 standards for building automation, medical devices; other sectors to be determined.
6. **Speakers bureau** - A database of speakers with expertise and experience in automation cybersecurity and associated commitments to speaking opportunities at industry events.
7. **Insurance industry collaboration** to evaluate how ISA/IEC 62443 can be used as objective measures for underwriting.
8. **Collaborate with DHS CISA to standup incident response program** in USA. Can be a template for incident response programs in other global regions.
9. Published 15 page **ISA/IEC 62443 quick start guide**.
10. Drafting a 20 page **ISA/IEC 62443 application guide** organized by stakeholders including owner/operators, system integrators, service providers, automation component/system suppliers.
11. Collaborating with ISCI to develop **IOT reference architectures** (starting with ISA99 WG9 TR).
12. Fund and manage a **web-based ISA/IEC 62443 workbench** for easy reference use to accelerated adoption.
13. **Additional projects** in the evaluation/startup phase in 2020

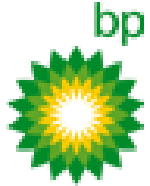
# ISASecure

Globally recognized ISA/IEC 62443 certification brand

- Started in 2007, first certification in 2011
- Certifies systems, components, development organizations
- Eight certification bodies around the globe
- Promotes adoption of ISA/IEC 62443 standards in collaboration with ISAGCA and ISA99 standards committee.
- OPAF agreement to use ISASecure scheme for assessing prototype components
- Can certify IOT components/devices today
- New certifications in development 1) IIOT system certification 2) facility certification for building management systems (BMS).



# ISASecure supporters past and present



ExxonMobil



YPF



Trust CB

Honeywell

Rockwell Automation



SIEMENS  
Ingenuity for life

HITACHI  
Inspire the Next



IPA  
Better Life with IT



SYNOPSYS®



# ISASecure Certification Bodies Internationally Accredited to ISO/IEC 17065 & ISO/IEC 17025

## Supporting Accreditation Bodies

1. Singapore Accreditation Council - Singapore
2. ANSI/ANAB-North America
3. Japan Accreditation Board-Japan
4. DAkkS-Germany
5. RvA Dutch Accreditation Council - Netherlands

## Certification Bodies

1. CSSC - Japan
2. Exida – USA/Global
3. TÜV Rheinland – Germany/Global
4. DNV GL – Singapore (in progress)
5. TÜV SUD – Singapore (in progress)
6. Applied Risk – Netherlands/EU
7. Trusted Labs – Netherlands/EU
8. CSA Group – Canada/Global



# ISASecure Certification Bodies

Link to [Certification Bodies Contact List](#)

1. *CSSC – Japan*



2. *Exida – USA/Global*



3. *TUV Rheinland – Germany/Global*



# 100% Aligned to ISA/IEC 62443 Standards

## **Process Certifications** - Security Development Lifecycle Assurance (**SDLA**)

- Shows that a company has a documented process that complies ISA/IEC 62443-4-1 (Product Development Lifecycle Requirements)
- Shows that this process is being followed by that company for a sampling of products

## **Product (Component) Certifications** – Component Security Assurance (**CSA**)

- Shows that a particular product is compliant with the requirements of ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 (Technical Security Requirements for IACS Components)
- ISASecure certifies 4 component categories described in the ISA/IEC 62443-4-2 standard including network devices, applications, embedded devices and host devices

## **System Certifications** - System Security Assurance (**SSA**)

- Shows that a system (collection of components) is compliant with the requirements ISA/IEC62443-4-1 and ISA/IEC 62443-3-3 (System Security Requirements and Security Levels)





# SDLA Changes in Progress (ISA/IEC 62443-4-1)

## **Current Process Certifications - Security Development Lifecycle Assurance (SDLA)**

- Shows that a company has a documented process that complies ISA/IEC 62443-4-1 (Product Development Lifecycle Requirements) **AND**
- Demonstration that the process is being followed by that company from a sampling of products

## **Enhanced Process Certification – Security Development Lifecycle Assurance (SDLA)**

- Assessment shows that a company has SDL process capabilities in place that comply with ISA/IEC 62443-4-1 (Product Development Lifecycle Requirements)
- Certificate is issued to organization for 12 months to allow transition of SDL activities to the certified process.
  - Gives companies credit for SDL program implementation progress while products are being transitioned into the SDL scheme.
  - Provides transition time for SDL artifacts to be created as products go through the SDL process

# ISASecure Annual Logo/Registration fee reductions

**SDLA** - ISA/IEC 62443-4-1    \$1,500/year

**CSA** – ISA/IEC 62443-4-2    \$1,200/year

**SSA** – ISA/IEC 62443-3-3    \$1,200/year

# Benefits of ISA Secure Certifications

Structured, auditable, repeatable approach to evaluating the security of an IACS product and the development practices of the manufacturer/integrator against an established benchmark.

## End-user

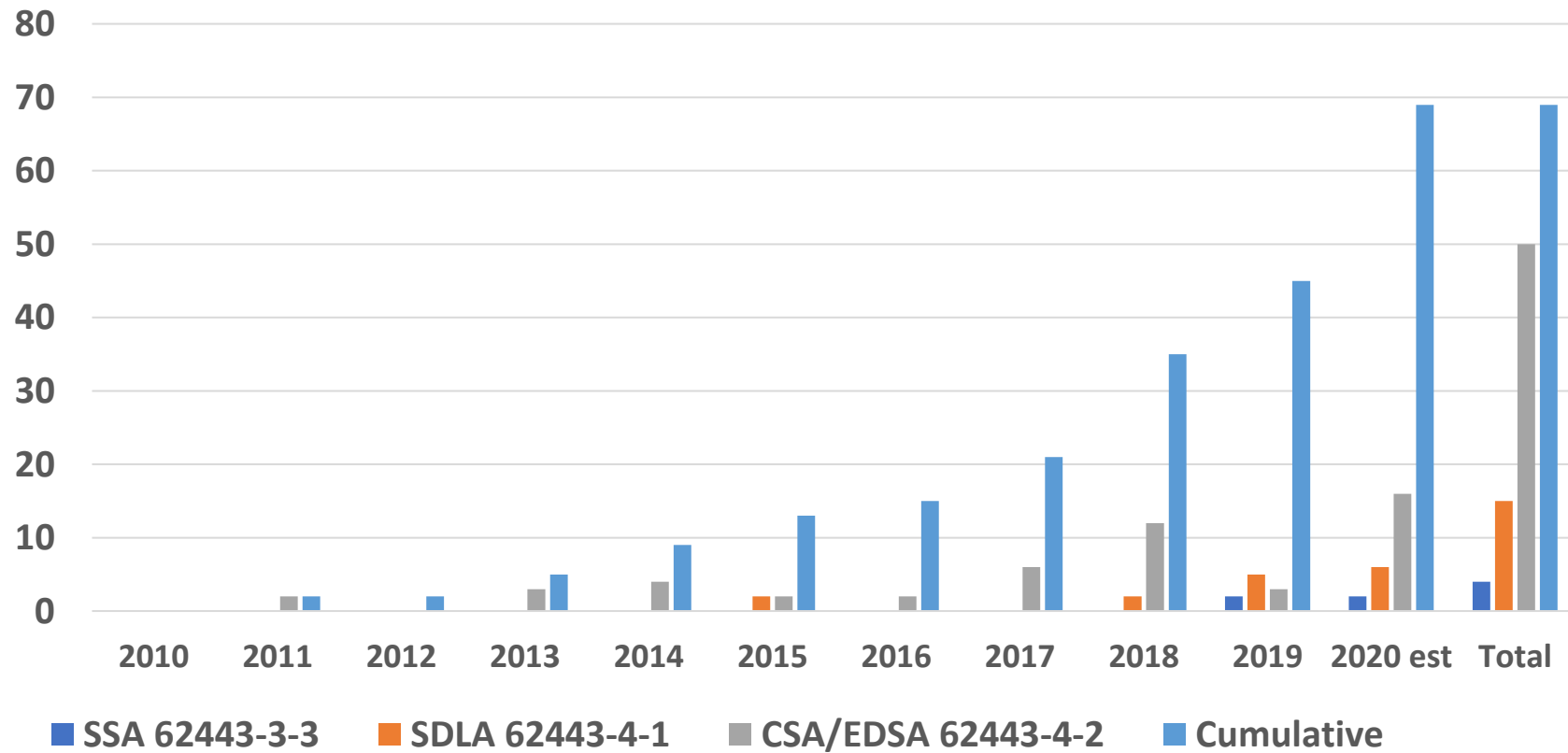
- Easy to specify security needs – security level
- Build security requirement into RFP
- Reduced time in FAT/SAT
- Know security level out of the box
- Better cybersecurity strength
- Provides confidence from independent expert technical assessment

## Supplier

- Evaluated once; does not have to be re-evaluated by each customer
- Recognition for effort
- Build in security
- Product differentiator
- Reduce support costs
- Enhance credibility
- Break the pen/patch cycle
- Can be applied globally

# ISASecure Certification Growth

ISASecure Certifications by Year



Please join us in securing automation  
that affects our every day lives.

Andre Ristaino

Managing Director, Alliances and Consortia

[aristaino@isa.org](mailto:aristaino@isa.org) 919-990-9222



**GLOBAL**  
CYBERSECURITY  
**ALLIANCE**

