International Society of Automation
Global Cybersecurity Initiatives

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

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** – 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.

• The ISA99 committee is **desires to engage with sector, industry, government and company programs** in their efforts to address automation systems cybersecurity. Contact the committee leadership at 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
- Published
- Adopted
- Published (under revision)

ISA
ISA/IEC 62443 Automation Security Lifecycle

Asset Owners
Operate and Maintain
Site Specific Systems

Integrators/Asset Owners
Engineer and Integrate COTS into Site Specific Systems

Suppliers
Design and Manufacture COTS Control Systems
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)
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.

• Annual member dues are $100,000 with matching funds from DHS S&T Directorate
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\textsuperscript{nd} 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
| Project Description                                                                 | Status             | Jan-20 | Feb-20 | Mar-20 | Apr-20 | May-20 | Jun-20 | Jul-20 | Aug-20 | Sep-20 | Oct-20 | Nov-20 | Dec-20 | Jan-21 | Feb-21 | Mar-21 | Apr-21 |
|-------------------------------------------------------------------------------------|--------------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| **Awareness and Outreach**                                                           |                    |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 1. Ongoing Marcom-web, social media, PR                                             | Ongoing            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 2. Develop a speakers bureau                                                         | Ongoing            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| **Advocacy and Adoption**                                                            |                    |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 3. 62443 Quick Start Guide - 15 page overview primer                                | Complete           |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 4. Regulatory and Legislative advocacy for 62443                                    | Ongoing            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 5. Table/software-Cross Reference 62443 to global standards                          | First 3 of 8 by Sept |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 6. White paper-Map Supplier Product Security Programs to Relevant Standards; to evaluate health of programs | not started yet    |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 7. White paper-Map Singapore CCoP to 62443                                          | Started             |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 8. Whitepaper about securing plc’s: top 20 list                                     | Started             |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 9. Commercialize ISA99/62443 Workbench in Cloud                                    | In design phase     |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| **Compliance and Prevention**                                                        |                    |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 10. White paper-describing 62443 automation lifecycle in alignment to stakeholder roles for security. | Started            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 11. White paper-How product certifications fit into security programs in eache SDL phase (ISCI project) | Started            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 12. Workforce Development program-Roles, definitions, collaboration with other organizations, certifications | Ongoing            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| **Training and Education**                                                           |                    |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 13. Insurance Industry collaboration                                                 | Started            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 14. DHS CISA collaboration to stand up an incident response program                  | Started            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
| 15. Define the top 2-3 IIOT reference architectures and security certification. (ongoing) with LOGIIC, WG9, ISA Secure | Started            |        |        |        |        |        |        |        |        |        |        |        |        |        |        |        |
ISASecure

Globally recognized ISA/IEC 62443 certification brand

• Started in 2007, first certification in 2011
• Eight certification global bodies in EU, ASEAN, Japan, USA, Canada
• Certifies systems, components, development organizations
• 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 Governing Board

Chair-Chevron, Kenny Mesker
Vice-Chair-ExxonMobil, James Hobbs
Technical Chair-Honeywell, Kevin Staggs
Marketing Chair-Schneider Electric, Dan Desruisseaux

Saudi Aramco
Johnson Controls, Inc.
Yokogawa
ISA99 Committee Liaison-Eric Cosman, ISA99 co-chairman
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. TUV Rheinland – Germany/Global
4. DNV GL – Singapore (in progress)
5. TUV SUD – Singapore (in progress)
6. Applied Risk – Netherlands/EU (in progress)
7. Trusted Labs – Netherlands/EU (in progress)
8. CSA Group – Canada/Global (in progress)
ISASecure Certification Bodies

Link to Certification Bodies Contact List

1. CSSC – Japan

2. Exida – USA/Global

3. TÜV 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/IEC 62443-4-1 and ISA/IEC 62443-3-3 (System Security Requirements and Security Levels)
ISASecure Annual Logo/Registration fee schedule

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

Certification Bodies invoice separately for professional fees incurred for the assessment services.
ISASecure® certificates of conformance issued


Benefits of ISASecure 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 Annual membership fees

Strategic Member (voting-governing board level)
- $50,000

Technical Member (voting-technical level)
- $20,000 (Annual Revenues over $500 million)
- $10,000 (Annual Revenues under $500 million)
- $5,000 (Annual Revenues under $50 million)
- $3,000 (Annual Revenues under $5 million)
- $5,000 (Certification Body)

Associate Member (non-voting)
- Government Agency/Industry Group/Other $5,000
- Individual $500

Adopter/Supporter Member (non-voting)
- $10,000 (Annual Revenues over $500 million)
- $5,000 (Annual Revenues under $500 million)
- $3,000 (Annual Revenues under $50 million)
- $1,500 (Annual Revenues under $5 million)
## ISAGCA Membership Dues for suppliers

<table>
<thead>
<tr>
<th>Annual Revenue</th>
<th>Founding Member Startup Contribution</th>
<th>2nd Year Contribution</th>
<th>3rd Year Contribution</th>
<th>Total for first 3 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; $5 billion</td>
<td>$250,000</td>
<td>$125,000</td>
<td>$125,000</td>
<td>$500,000</td>
</tr>
<tr>
<td>$1 - $5 billion</td>
<td>$100,000</td>
<td>$50,000</td>
<td>$50,000</td>
<td>$200,000</td>
</tr>
<tr>
<td>$500 million - $1 billion</td>
<td>$50,000</td>
<td>$25,000</td>
<td>$25,000</td>
<td>$100,000</td>
</tr>
<tr>
<td>$100 million - $500 million</td>
<td>$25,000</td>
<td>$12,500</td>
<td>$12,500</td>
<td>$50,000</td>
</tr>
<tr>
<td>$5 million – $100 million</td>
<td>$10,000</td>
<td>$5,000</td>
<td>$5,000</td>
<td>$20,000</td>
</tr>
<tr>
<td>&lt; $5 million</td>
<td>$5,000</td>
<td>$2,500</td>
<td>$2,500</td>
<td>$10,000</td>
</tr>
<tr>
<td>Associate-Govt, Industry Groups, Academia</td>
<td>$5,000</td>
<td>$1,250</td>
<td>$1,250</td>
<td>$7,500</td>
</tr>
</tbody>
</table>

Companies may join as a non-Founding Member by opting to pay only the annual fee starting in the first year.
Please join us in securing automation that affects our every day lives.

Andre Ristaino
Managing Director, Alliances and Consortia
aristaino@isa.org  919-990-9222