38,500 members
135 sections
44 countries
350,000 customers

Standards
Education
Certification
Conferences
Publications
Compliance
The Foundation of ISA's Work in Automation Cybersecurity

The ISA/IEC 62443 Series of Standards
Importance of the ISA/IEC 62443 Standards

Leveraging industry standards increases productivity, lowers costs, and keeps facilities safe

World's only consensus-based standard for automation and control system applications

Flexible framework to address and mitigate current and future security vulnerabilities

Defines requirements and procedures for implementing electronically secure systems

Leverages a holistic approach, bridging the gap between operations and information technology; and between safety and cybersecurity
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 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's Cybersecurity Consortia

LOGIC

Research and development on cybersecurity topics for automation used by the oil and gas industry

Current members include: BP, Chevron, ExxonMobil, Shell, Total, ConocoPhillips, and other large oil and gas companies that operate significant global energy infrastructure.

ISASecure®

ISA/IEC 62443 certification of supplier COTS products and development processes, and end user operating facilities

Notable members include: Chevron, ExxonMobil, Honeywell, Schneider Electric, Yokogawa, exida, Control System Security Center, YPF, Japan ITPA, Royal Dutch Shell plc, TUV Rheinland, DNV GL, and TUV SUD

Brings the automation cybersecurity ecosystem together to lead culture change, drive market adoption of industry standards
ISA is uniquely qualified to lead this effort

Unbiased 501c3
Independent, tax-exempt, global professional organization

Home of the ISA/IEC 62443 Standards
Developers of the world’s only consensus automation cybersecurity standards

Established Training and Certification Programs
Trusted industry resource for hands-on, vendor-neutral training and certification

Advocacy and Outreach Capabilities
ISA has extensive experience sharing knowledge across industries and stakeholder groups

Experience Managing Consortia
ISA has managed several consortia and industry groups, including LOGIIC, the ISA Secure® Program, and the ISA100 Wireless™ Program
ISA Global Cybersecurity Alliance is Different
Open, standards-based, and practical

All-Inclusive, Industry Wide
The challenge is so much bigger than any one organization - no matter how big or capable - can tackle alone. We see a need for an open, transparent body to bring all kinds of groups together.

Built Around Global Standards
A broad network of end users, vendors, government agencies, and other stakeholders will leverage the UN-endorsed, consensus-developed series of standards as a foundation.

Practical and Tactical
GCA will develop the training, tools and know-how to bridge the gap between the standards and implementation, making standards more approachable and user-friendly.
Our member companies hold and promote these five core beliefs:

1. Digital transformation leverages innovative technologies but often undervalues security.
2. Consequence-driven, cyber-informed engineering is a business imperative.
3. Safety and cybersecurity are inseparable.
4. Cybersecurity improvement is a discussion about organizational culture, not just technology.
5. These challenges can only be handled by collaborating and working together in an open, inclusive environment.
Fast Facts

• ISAGCA launched 2\textsuperscript{nd} half of 2019 as a global initiative

• Six initial members, over 35 today and growing

• Four major areas of focus, all operational with member champions

• One key deliverable released, with two more slated for release in summer 2020
ISAGCA is growing formal liaisons to collaborate with other industry groups:

- ISASecure
- LOGIIC
- ISA99 standards committee
- Others underway, to be announced
The ISA Global Cybersecurity Alliance will work together to develop solutions that address our biggest challenges.

**COLLABORATION**
When manufacturers, asset owners, vendor companies, government agencies, and other stakeholders join together in an open and transparent way, we can move industry forward faster and more effectively.

**STANDARDIZATION**
Standards exist, but aren’t well understood. Our companies need easy-to-follow guides for implementing best practices, and industry needs to increase the adoption of standards globally.

**EDUCATION**
Human error is the biggest factor in safety and security incidents around the world. Providing accessible, consistent training and education for professionals at all levels gives our companies a first line of defense.

**PROTECTION**
Ensuring the inherent security of vendor devices and systems, and exploring ways to increase compliance with best practices, offers real risk reduction in your operations.
**Alliance Objectives**

- Expansion and adoption of ISA/IEC 62443
- Industry reach and awareness
- Workforce training and development
- Optimized compliance and prevention

**Benefits**

- User-friendly, consistent standards implementation
- A vigilant, proactive cybersecurity culture in every facility
- A skilled, experienced workforce that drives results
- Reliable, secure, and interoperable devices and systems
- Stay ahead of increasing threats and vulnerabilities

**Manufacturer**
Top Reasons for Manufacturers to Join the ISAGCA

Leverage the power of a unified group of experts and thought leaders

01 EXPONENTIAL KNOWLEDGE
Leverage the collective knowledge, experience, and best practices across industries, facilities, and geographies

02 AMPLIFIED VOICE
Explore and define challenges with people who can take down barriers and solve problems

03 UNPARALLELED ACCESS
Access the experts and thought leaders that are shaping the future of cybersecurity in multiple industries

04 INFLUENCE SOLUTIONS
Influence the creation of the latest tools, guides, and best practices to help your company address cybersecurity challenges

05 CONSISTENCY
Develop a consistent approach to cybersecurity using the lens of people, processes, and technology

06 EMPOWERMENT
Empower your company to create and sustain a positive cyber-aware culture at every level of the organization
Initial Workgroups of the ISA Global Cybersecurity Alliance

**Awareness and Outreach**
- Cultivates awareness and engagement around important cybersecurity issues with industry and stakeholders across all relevant sectors
- Serves as primary marketing arm for the ISAGCA’s objectives and accomplishments

**Advocacy and Adoption**
- Expands and extends the adoption and use of cybersecurity standards worldwide
- Cultivates relationships with key global stakeholder groups and agencies
- Develops materials that help all sectors utilize standards and technical guidance

**Training and Education**
- Delivers specific workforce development initiatives with consideration to all relevant job functions and industry sectors
- Develops and promotes training courses, web seminars, educational events, certificates or certification programs, etc.

**Compliance and Prevention**
- Expands and develops compliance, prevention, and harmonization initiatives
- leverages collective expertise and intelligence of member companies for the good of industry
### ISA Global Cybersecurity Alliance Projects

<table>
<thead>
<tr>
<th>#</th>
<th>Milestone Description</th>
<th>Jan-20</th>
<th>Feb-20</th>
<th>Mar-20</th>
<th>Apr-20</th>
<th>May-20</th>
<th>Jun-20</th>
<th>Jul-20</th>
<th>Aug-20</th>
<th>Sep-20</th>
<th>Oct-20</th>
<th>Nov-20</th>
<th>Dec-20</th>
<th>Jan-21</th>
<th>Feb-21</th>
<th>Mar-21</th>
<th>Apr-21</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ongoing Marcom-web, social media, PR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Develop a speakers bureau</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>62443 Quick Start Guide - 15 page overview primer</td>
<td>Complete</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Regulatory and Legislative advocacy for 62443</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Table/software-Cross Reference 62443 to global standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>White paper-Map Supplier Product Security Programs to Relevant Standards; to evaluate health of programs</td>
<td>not started yet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>White paper-Map Singapore CCoP to 62443</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Whitepaper about securing plc’s: top 20 list</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Commercialize ISA99/62443 Workbench in Cloud</td>
<td>To design phase</td>
<td>Build phase</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>White paper-describing 62443 automation lifecycle in alignment to stakeholder roles for security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>White paper-How product certifications fit into security programs in each SDL phase ([SCI project])</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Workforce Development program-Roles, definitions, collaboration with other organizations, certifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Training and Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Insurance Industry collaboration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>DHS CISA collaboration to stand up an incident response program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Define the top 2-3 IIoT reference architectures and security certification. Collaborate with LOGIC, WG9, ISA Secure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Download a free overview of the ISA/IEC 62443 standards - courtesy of ISAGCA! 

GUIDE TO CYBERSECURITY STANDARDS 

WWW.ISA.ORG/CYBERGUIDE
PARTNER WITH US TO CHANGE THE WORLD OF AUTOMATION CYBERSECURITY

Join the ISA Global Cybersecurity Alliance to lead and influence direction, priorities, and work products.

Explore standards-based certification for your products and development processes through ISASecure.

Find resources: www.isa.org/cyberresources
Subscribe to our blogs: blog.isa.org
www.isa.org/isagcablog
Thank You

www.isa.org/isagca

General Inquiries:
Andre Ristaino
ISA Global Cybersecurity
Alliance Director
aristaino@isa.org

Membership Inquiries:
Elena Pitt
Strategic Business Development
epitt@isa.org
+1 919-323-4023

Education & Certification
Inquiries:
Geri McGrath
Global Education Director
gmcgrath@isa.org
+1 919-990-9381