www.isa.org/ISAGCA

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

Defines requirements and procedures for implementing electronically secure systems

Flexible framework to address and mitigate current and future security vulnerabilities

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

IEC 62443 Family of Standards

General

ISA-62443-1-1
Concepts and models

ISA-62443-1-2
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
Security Protection Rating

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
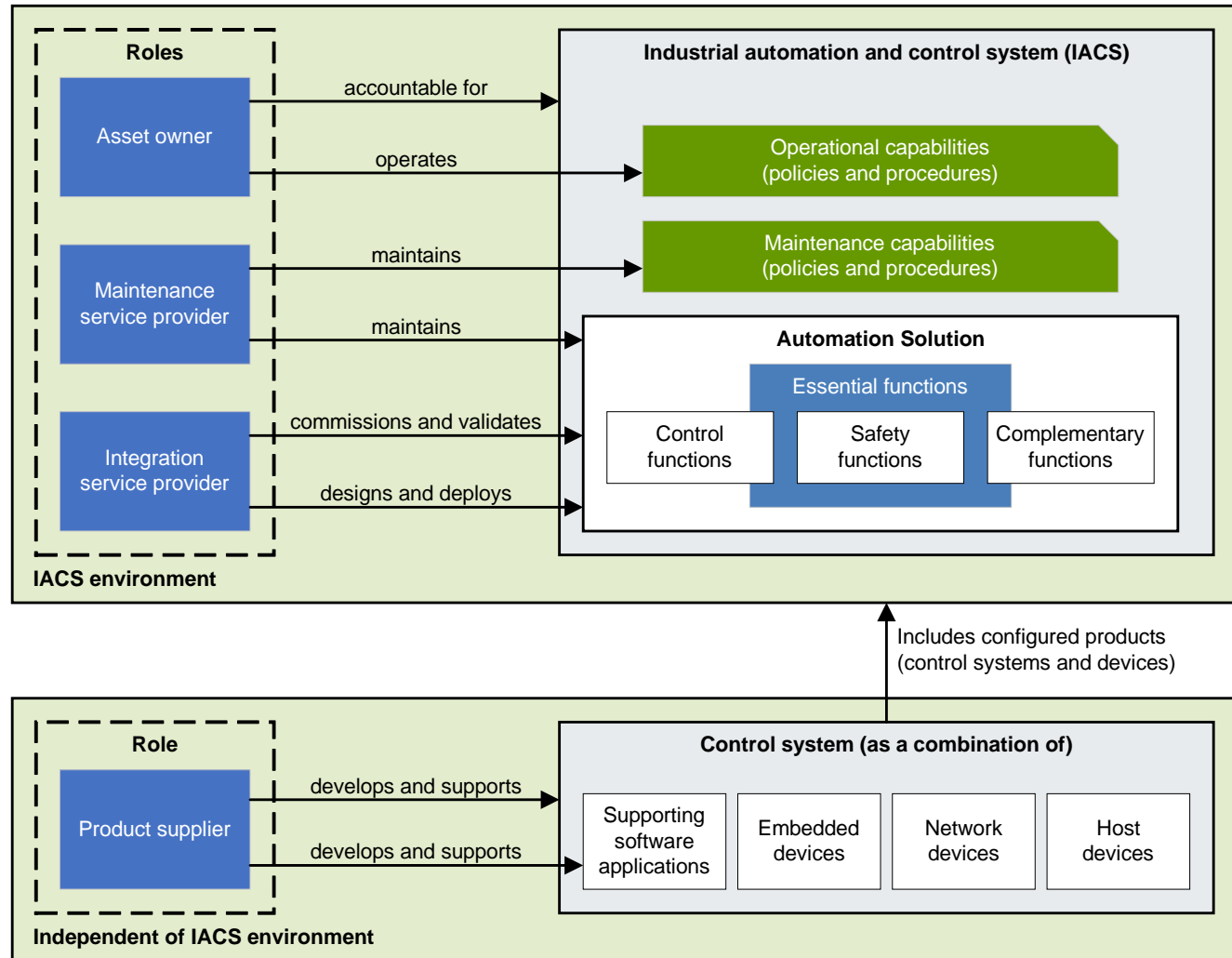System security requirements and security levels

Component

ISA-62443-4-1
Secure product development lifecycle requirements

ISA-62443-4-2
Technical security requirements for IACS components

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's Cybersecurity Consortia

LOGIIC

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

ISA GLOBAL CYBERSECURITY ALLIANCE

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

Digital transformation leverages innovative technologies but often undervalues security.

Consequence-driven, cyber-informed engineering is a business imperative.

Safety and cybersecurity are inseparable.

Cybersecurity improvement is a discussion about organizational culture, not just technology.

These challenges can only be handled by collaborating and working together in an open, inclusive environment.

Fast Facts

- ISAGCA launched 2nd 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	=
Shared threat intelligence and experience	=

Manufacturer 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

Top Reasons for Manufacturers to Join the ISAGCA

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

EXPONENTIAL KNOWLEDGE

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

AMPLIFIED VOICE

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

UNPARALLELED ACCESS

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

INFLUENCE SOLUTIONS

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

CONSISTENCY

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

EMPOWERMENT

06 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

#	Awareness and Outreach	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
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				Build phase							deploy 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				Going forward plan								
14	DHS CISA collaboration to stand up an incident response program				Started			Going forward plan									
15	Define the top 2-3 IIOT reference architectures and security certification. Collaborate with LOGIIC, WG9, ISASecure				Started												

Download a free overview of the ISA/IEC 62443 standards - courtesy of ISAGCA!

ISA GLOBAL CYBERSECURITY ALLIANCE

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