International Society of Automation

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

ISA/IEC 62443 OT Cybersecurity Standards

ECL Virtual Summit
19 March 2024

Andre Ristaino
ISA Managing Director, Conformance Programs and Consortia

www.isa.org

15,822
MEMBERS

186
SECTIONS

109
COUNTRIES

350,000
CUSTOMERS

STANDARDS

EDUCATION

CERTIFICATION

CONFERENCES

PUBLICATIONS

COMPLIANCE

Andre Ristaino

ISA Managing Director, Conformance Programs and Consortia
aristaino@isa.org PH: +1 919-323-7660
https://isasecure.org/isasecure-site-assessment-0

- Mr. Ristaino directs ISA's consortiums and alliances, including, ISA Security Compliance Institute, ISA Wireless Compliance Institute, ISAGCA, ICS4ICS.

- 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.

- Mr. Ristaino earned a BS in Business Management from the University of Maryland, College Park and an MS in Applied Computing from the American University in Washington DC with a focus on expert systems and artificial intelligence.

aristaino@isa.org

ISASecure®

ISA Automation Cybersecurity Leadership

ISASecure - **ISA/IEC 62443 cybersecurity certification** of COTS products, supplier development processes and automation at asset owner operating sites. **45 companies**
www.isasecure.org

ISAGCA - **Bridge the gap between** ISA/IEC 62443 standards and market adoption. Lead cybersecurity culture transformation. **60 companies** https://isagca.org

ICS4ICS – **Incident Command System** for Industrial Control Systems (ICS4ICS) credentials incident leaders & trains teams for responding to cyber attacks on automation in critical infrastructure. Collaborates with FEMA, CISA, INL; stood up as a new program under ISAGCA. **1,400 volunteers; over 800 companies** www.ics4ics.org

ISA99 Committee

ISA99 Committee – The ISA99 Standards committee is the origin of the ISA/IEC 62443 Standards. ISA99 Working groups draft and approve the ISA/IEC 62443 standards for submission to ANSI and IEC for approval as international standards. **Over 1,400 volunteers**
www.isa.org/ISA99

ISA Education

ISA Education & Training – Education and training in all industrial automation and control systems topics, including cybersecurity. Trained over **3,000 students in 2022**.
https://www.isa.org/training

ISA/IEC 62443 Standards

System availability is prime objective; purpose built for OT cybersecurity

OT cybersecurity is a function of:

1. IACS system technical cybersecurity capabilities **plus**
2. Maturity of operational security policies and procedures **plus**
3. Cybersecurity skill level of personnel at all levels

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

ISA/IEC 62443 Standards-15 parts-What's in Them

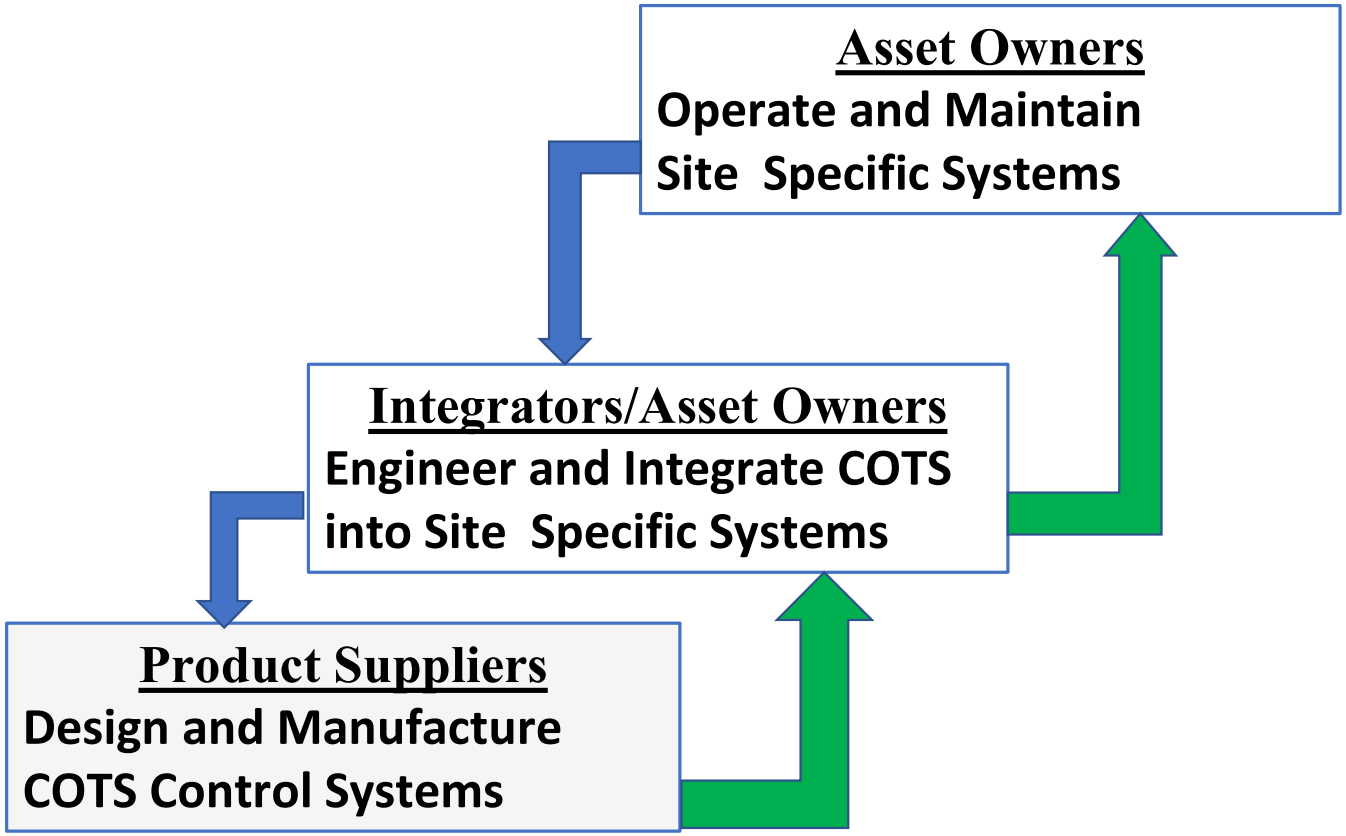
- **Concepts and Models**
- **Terms and Terminology**
- **Roles and Responsibilities**
- **Security Capability Level Definitions and Requirements**
- **Process Maturity Level Definitions and Requirements**

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

ISA/IEC 62443 Component and System Security Levels

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

ISA/IEC 62443 Concept of Roles-based Shared Responsibility for Cybersecurity



ISA/IEC 62443 Standards Structured by Roles for Shared Cybersecurity Responsibility

Asset Owner – Leverage Standards:

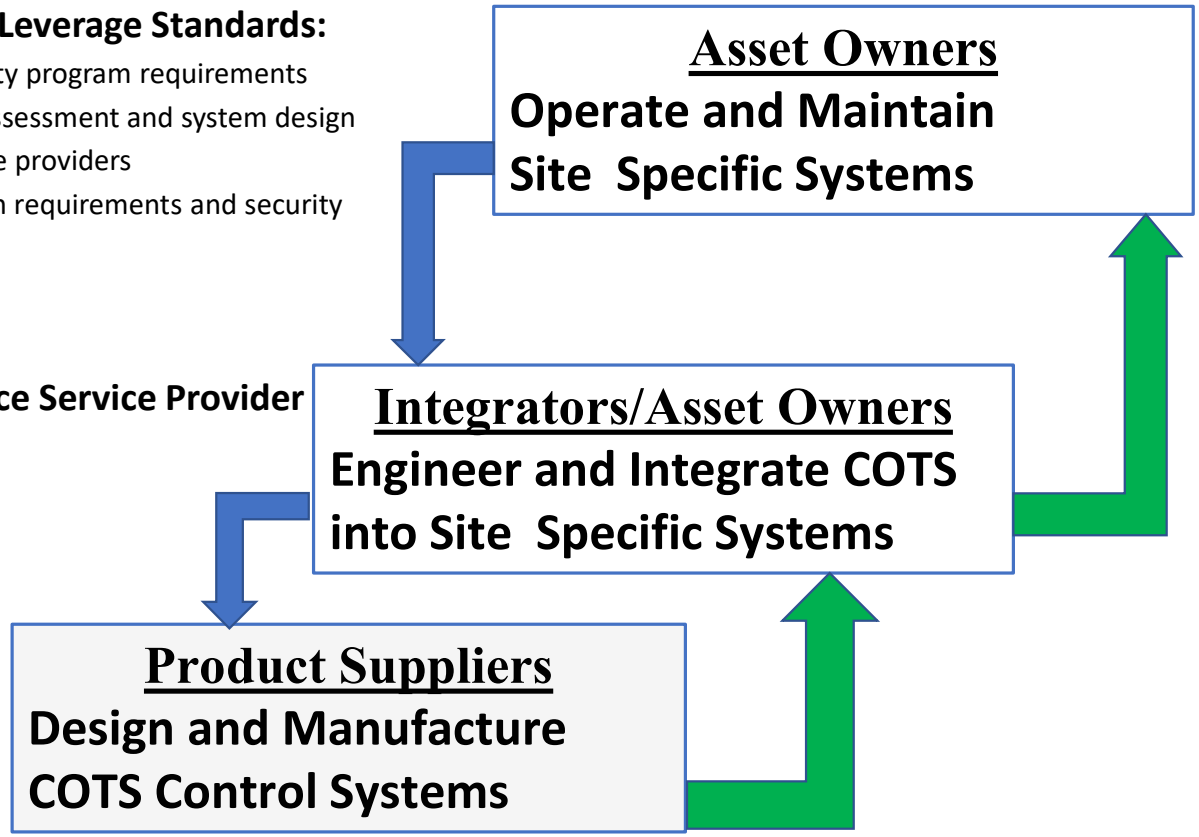
- Part 2-1 – Security program requirements
- Part 3-2 – Risk assessment and system design
- Part 2-4 – Service providers
- Part 3-3 – System requirements and security levels

Integration and Maintenance Service Provider - Leverage Standards:

- Part 2-4 – Service providers

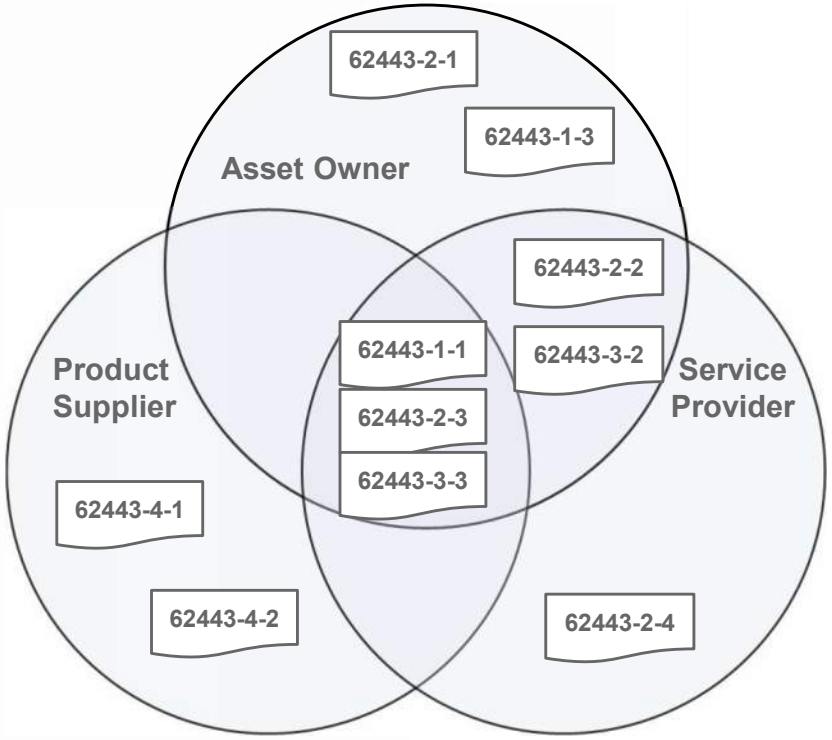
Product Supplier - Leverage Standards:

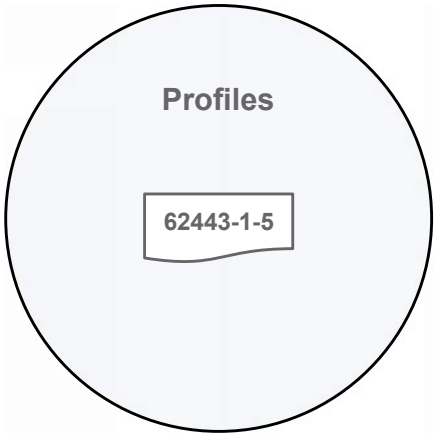
- Part 3-3 – System requirements and security levels
- Part 4-1 – Security development lifecycle
- Part 4-2 – Component requirements

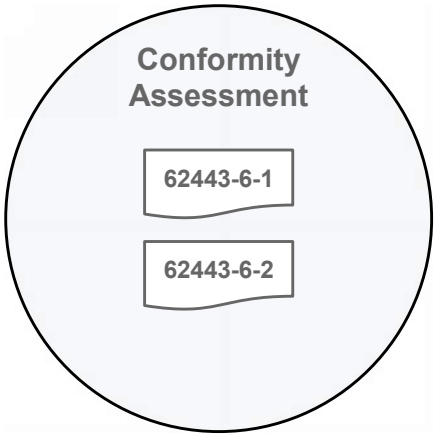


ISA99 Committee

ISA/IEC 62443 Parts by Role

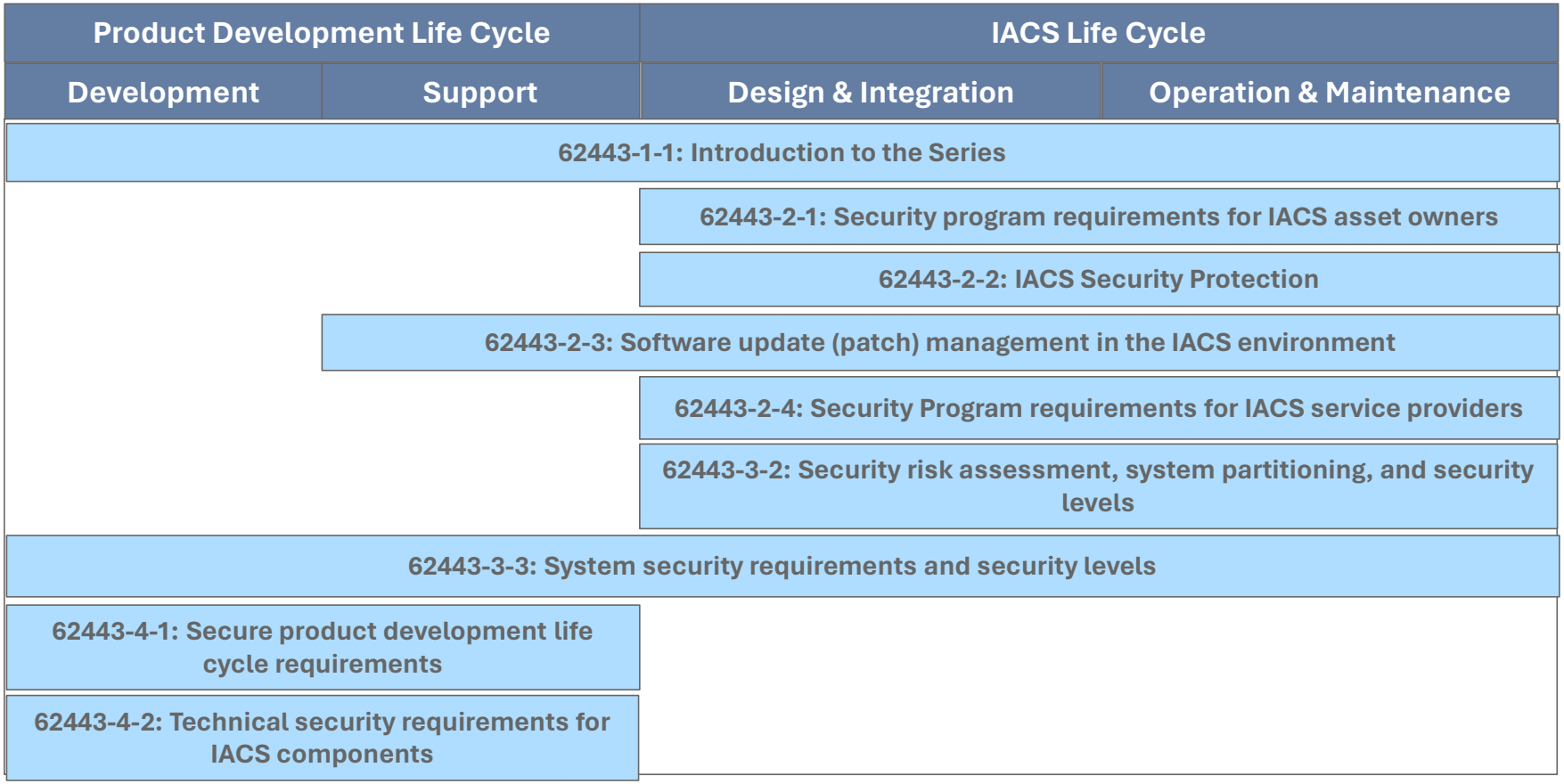




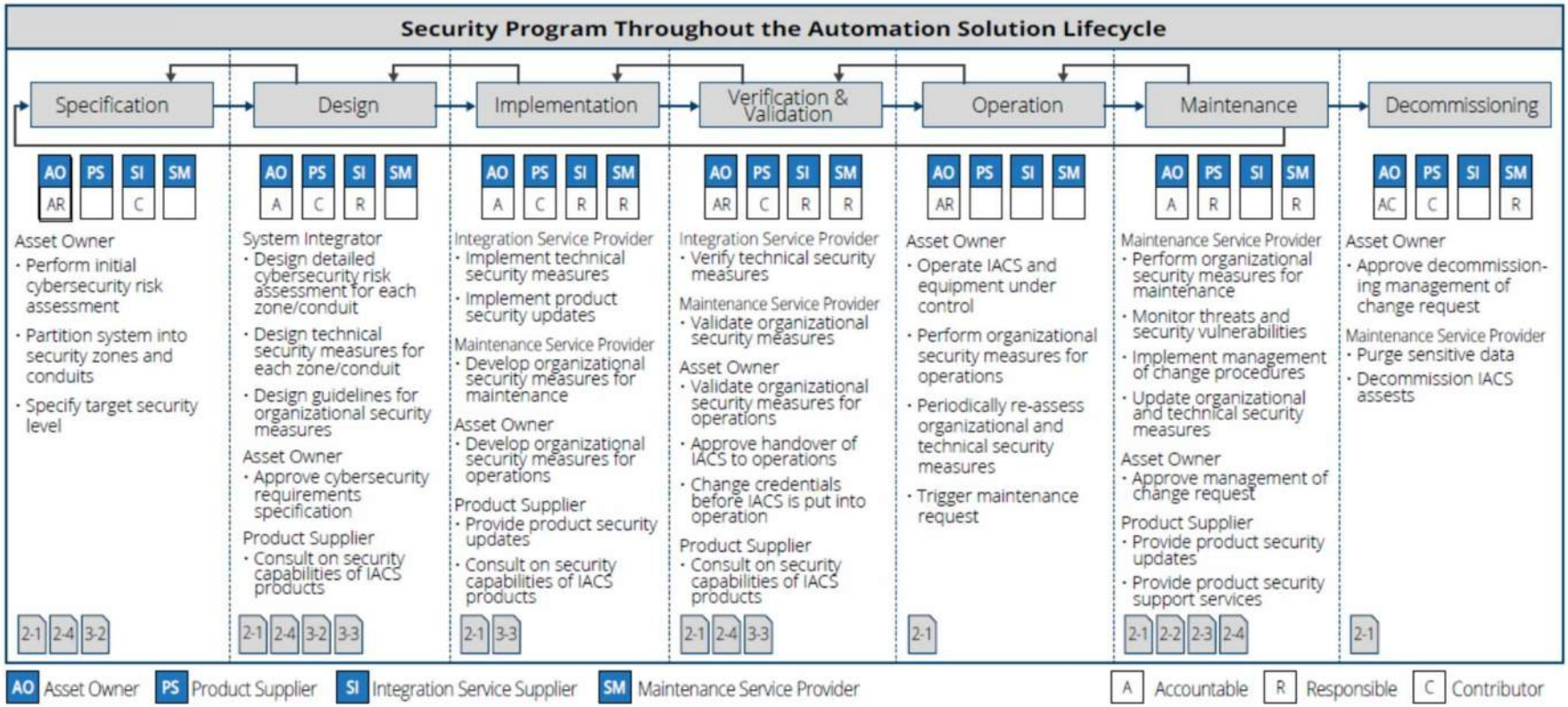


ISA99 Committee

ISA/IEC 62443 Parts by Life Cycle



Note: Currently, 62443-3-3 only covers the development life cycle


Security Program Throughout the Automation Solution Lifecycle
Specification
Design
Implementation
Verification & Validation
Operation
Maintenance
Decommissioning
AO PS SI SM
AR | | C |
Asset Owner
· Perform initial cybersecurity risk assessment
· Partition system into security zones and conduits
· Specify target security level
2-1 2-4 3-2
AO PS SI SM
A | C | R |
System Integrator
· Design detailed cybersecurity risk assessment for each zone/conduit
· Design technical security measures for each zone/conduit
· Design guidelines for organizational security measures
Asset Owner
· Approve cybersecurity requirements specification
Product Supplier
· Consult on security capabilities of IACS products
2-1 2-4 3-2 3-3
AO PS SI SM
A | C | R | R
Integration Service Provider
· Implement technical security measures
· Implement product security updates
Maintenance Service Provider
· Develop organizational security measures for maintenance
Asset Owner
· Develop organizational security measures for operations
Product Supplier
· Provide product security updates
· Consult on security capabilities of IACS products
2-1 3-3
AO PS SI SM
AR | C | R | R
Integration Service Provider
· Verify technical security measures
Maintenance Service Provider
· Validate organizational security measures
Asset Owner
· Validate organizational security measures for operations
· Approve handover of IACS to operations
· Change credentials before IACS is put into operation
Product Supplier
· Consult on security capabilities of IACS products
2-1 2-4 3-3
AO PS SI SM
AR | | | |
Asset Owner
· Operate IACS and equipment under control
· Perform organizational security measures for operations
· Periodically re-assess organizational and technical security measures
· Trigger maintenance request
2-1
AO PS SI SM
A | R | | R
Maintenance Service Provider
· Perform organizational security measures for maintenance
· Monitor threats and security vulnerabilities
· Implement management of change procedures
· Update organizational and technical security measures
Asset Owner
· Approve management of change request
Product Supplier
· Provide product security updates
· Provide product security support services
2-1 2-2 2-3 2-4
AO PS SI SM
AC | C | | R
Asset Owner
· Approve decommissioning management of change request
Maintenance Service Provider
· Purge sensitive data
· Decommission IACS assests
2-1
AO Asset Owner
PS Product Supplier
SI Integration Service Supplier
SM Maintenance Service Provider
A Accountable
R Responsible
C Contributor

Greenfield vs As-built challenges

Greenfield

- Blank slate / can design-in security with modern technology
- However, much of current technology may not have security built-in

As-built (legacy / in operation)

- Difficult to change architecture (not a blank slate)
- Old technology difficult to retrofit or no longer supported

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

Industry and Government Collaboration

1. INL on CoP, CIE/and workforce development, FEMA
2. DOE, NREL, PNNL on substation/electric sector profiles and S2G
3. NATF
4. NEMA
5. OPAF
6. SMCC, TSMC, Maritime (IACS-Intl Assoc of Classification Societies)
7. Governments – Japan, Taiwan, Singapore, Malaysia

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

How should I approach OT cybersecurity challenge?

1. Take the ISA/IEC 62443 classes to learn the models and vocabulary…..get all personnel trained as needed.
2. Work with management to identify critical assets to protect (CIE)
3. Develop protection plan and funding (mitigate consequences)
4. Develop response and recovery plan (improve resilience)
5. Practice the plan and carry out the detailed ‘cyber hygiene’ activities per ISA/IEC 62443 standards

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

Cybersecurity Resources at ISA

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

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

ISA Global Cybersecurity Alliance - https://isagca.org/

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®