ISASecure Web Conference

ISA/IEC 62443 Series Overview

ISASecure®

Johan B Nye
ICS Guru LLC
October 5, 2020

About the Speaker

- Johan Nye
- johan.nye@ICS.guru
- Experience
  - Currently an independent ICS cybersecurity consultant
  - Currently part of ISA 99 committee leadership
  - Previously ICS Cybersecurity Advisor @ major petrochemical company
  - Previously Chairman @ ISA Security Compliance Institute (ISASecure.org)
  - MIT, BS/MS Mechanical Engineering

Agenda

- Introduction
  - Some notable IACS Cyber Attacks
  - Defining Industrial Automation and Control Systems (IACS)
  - Differences between IT and IACS
- ISA/IEC 62443 Series
  - Standards Development Organizations
  - ISA/IEC 62443 Series
- Key concepts
  - IACS Principal Roles and Responsibilities
  - Foundational Requirements
- Security Lifecycles
  - Security Lifecycle View[1]
  - Product Security Lifecycle
  - Automation Solution Security Lifecycle[1]
- Risk Management
  - IACS Risk Management
  - Zones and Conduits
  - Essential Functions
- ISASecure Certification Schemes
- ISA Cybersecurity Resources

Note 1: Some parts of this presentation are based on ISA 99 Committee drafts and are subject to change

Introduction

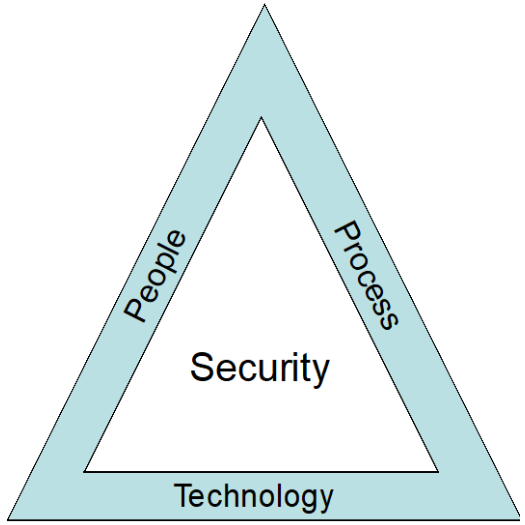
Some Notable IACS Cyber Attacks

Date	Target	Method
2000	Australian Sewage Plant	Insider
2010	Iran Uranium Enrichment	Stuxnet
2013	ICS Supply Chain attack	Havex
2014	German Steel Mill	
2015	Ukraine Power Grid	BlackEnergy, KillDisk
2016	Ukraine Substation	CrashOverride
2017	Global shipping company	NotPetya
2017	IoT DDoS attack	BrickerBot
2017	Health care, Automotive, many others	WannaCry
2017	Saudi Arabia Petrochemical	TRISIS
2019	Norwegian Aluminum Company	LockerGaga

Resource: www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Defining Industrial Automation and Control

- Component
  - an embedded device, host device, network device, or software application
  - e.g. field devices, PLC, historian, HMI
- Control System (or System)
  - the hardware and software components of an IACS
  - e.g. DCS, SIS, SCADA
- Automation Solution
  - an instance at an Asset Owner's facility
  - an integrated set of System and Component products
  - a set of zones and conduits
- Security Program
  - People (awareness and training)
  - Processes (policies and procedures)
- Industrial Automation and Control System (IACS)
  - a collection of personnel, hardware, software and policies involved in the operation of the Equipment Under Control and that can affect or influence its safe, secure and reliable operation
  - Automation Solution + Security Program



Differences Between IT and IACS

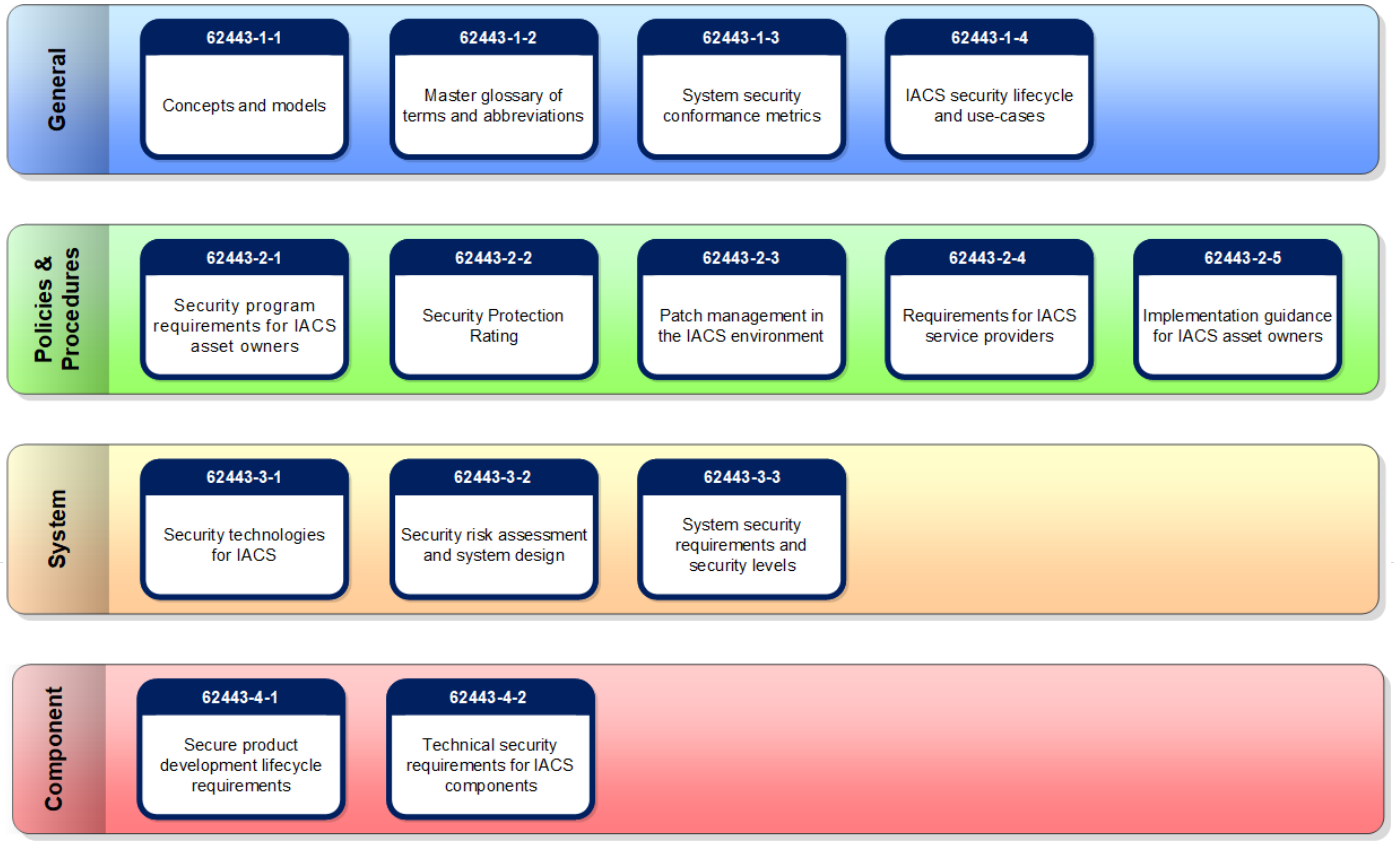
- Although the same technologies may be used in IACS and IT, the purpose and use is significantly different
- IACS cyber security must address additional considerations of health, safety, environmental protection and product integrity
- Potential consequences usually not found in IT:
  - Endangerment of public or employee safety or health
  - Damage to the environment
  - Damage to equipment
  - Loss of product integrity
- Other differences may include higher expectations of:
  - Availability, integrity, performance, change management and equipment lifetime

ISA/IEC 62442 Series

Standards Development Organizations

- ISA/IEC 62443 is a series of standards developed by two groups
  - ISA99 develops ANSI/ISA-62443 standards
  - IEC develops IEC 62443 standards
  - Each organization adopts the other's standard so that there is one version for each standard
- Working closely in consultation with:
  - ISO to be consistent with ISO/IEC 27000 series on Information Security
- ISA99 Committee has numerous liaison relationships with other SDO's

ISA/IEC 62443 Series



ISA/IEC 62443 Series Details

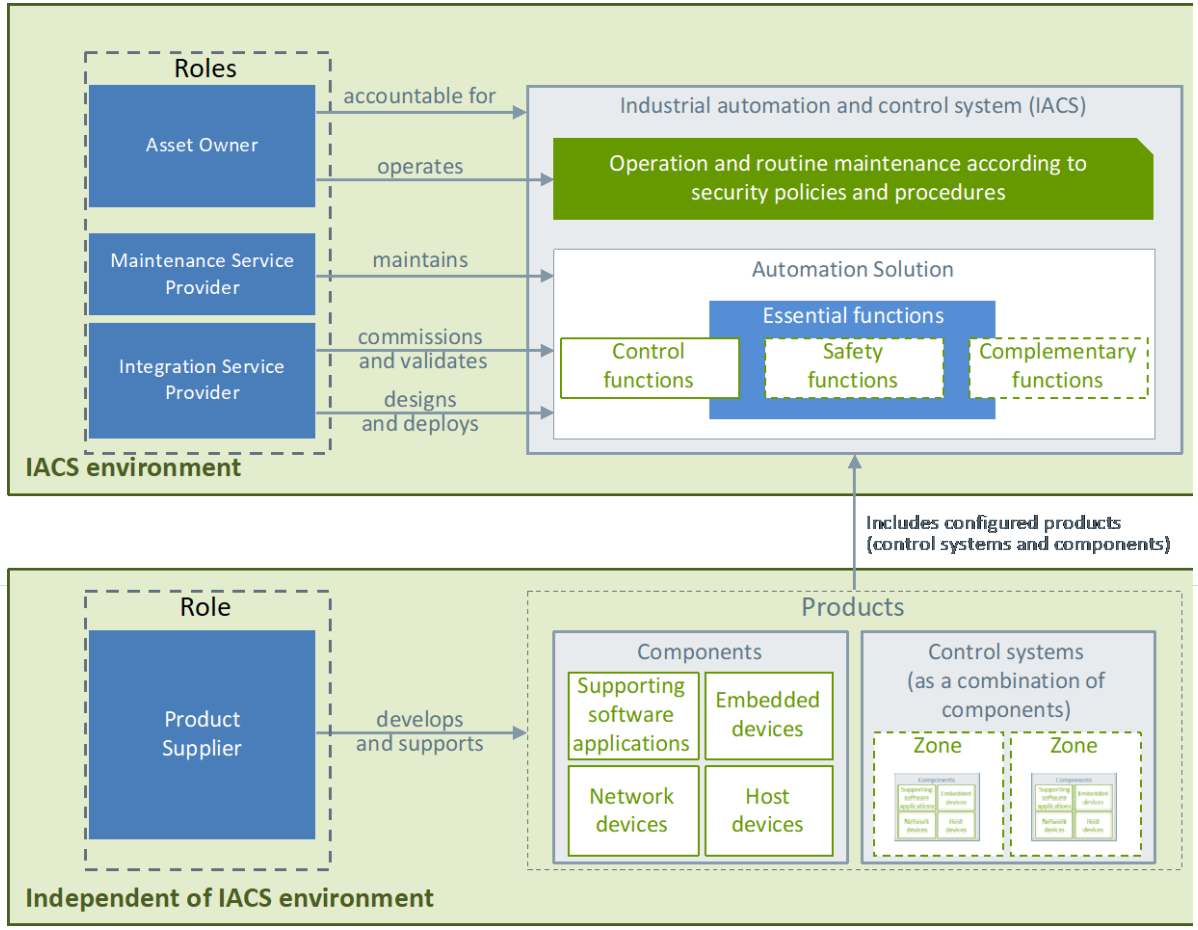
	Part	Type	Title	Date
General	1-1	TS	Terminology, concepts, and models	2007*
	1-2	TR	Master glossary of terms and abbreviations	
	1-3		System security conformance metrics	
	1-4		IACS security lifecycle and use cases	
Policies & Procedures	2-1	IS	Establishing an IACS security program	2009*
	2-2		IACS security program ratings	
	2-3	TR	Patch management in the IACS environment	2015*
	2-4	IS	Security program requirements for IACS service providers	2018
	2-5	TR	Implementation guidance for IACS asset owners	
System	3-1	TR	Security technologies for IACS	
	3-2	IS	Security risk assessment for system design	2020
	3-3	IS	System security requirements and security levels	2013*
Component	4-1	IS	Product security development life-cycle requirements	2018
	4-2	IS	Technical security requirements for IACS components	2018

Key concepts

IACS Principal Roles

- Asset owner
  - is accountable and responsible for one or more IACSs
  - operates the IACS and the Equipment under Control
- Product Supplier
  - manufactures and supports an IACS hardware and/or software product
- Service Providers
  - Integration Service Provider (System Integrator)
    - provides system integration activities for an Automation Solution
      - design, installation, configuration, testing, commissioning and handover to the Asset Owner
  - Maintenance Service Provider
    - provides support activities for an Automation Solution
- Remember *roles* and *organizations* are different
  - An individual or organization can have multiple roles
  - The responsibilities for a role can be split between organizations
  - The Asset Owner is responsible for documenting roles and responsibilities

IACS Principal Roles and Responsibilities



Foundational Requirements

- FR 1 – Identification and Authentication control (IAC)
- FR 2 – Use Control (UC)
- FR 3 – System Integrity (SI)
- FR 4 – Data Confidentiality (DC)
- FR 5 – Restricted Data Flow (RDF)
- FR 6 – Timely Response to Events (TRE)
- FR 7 – Resource Availability (RA)

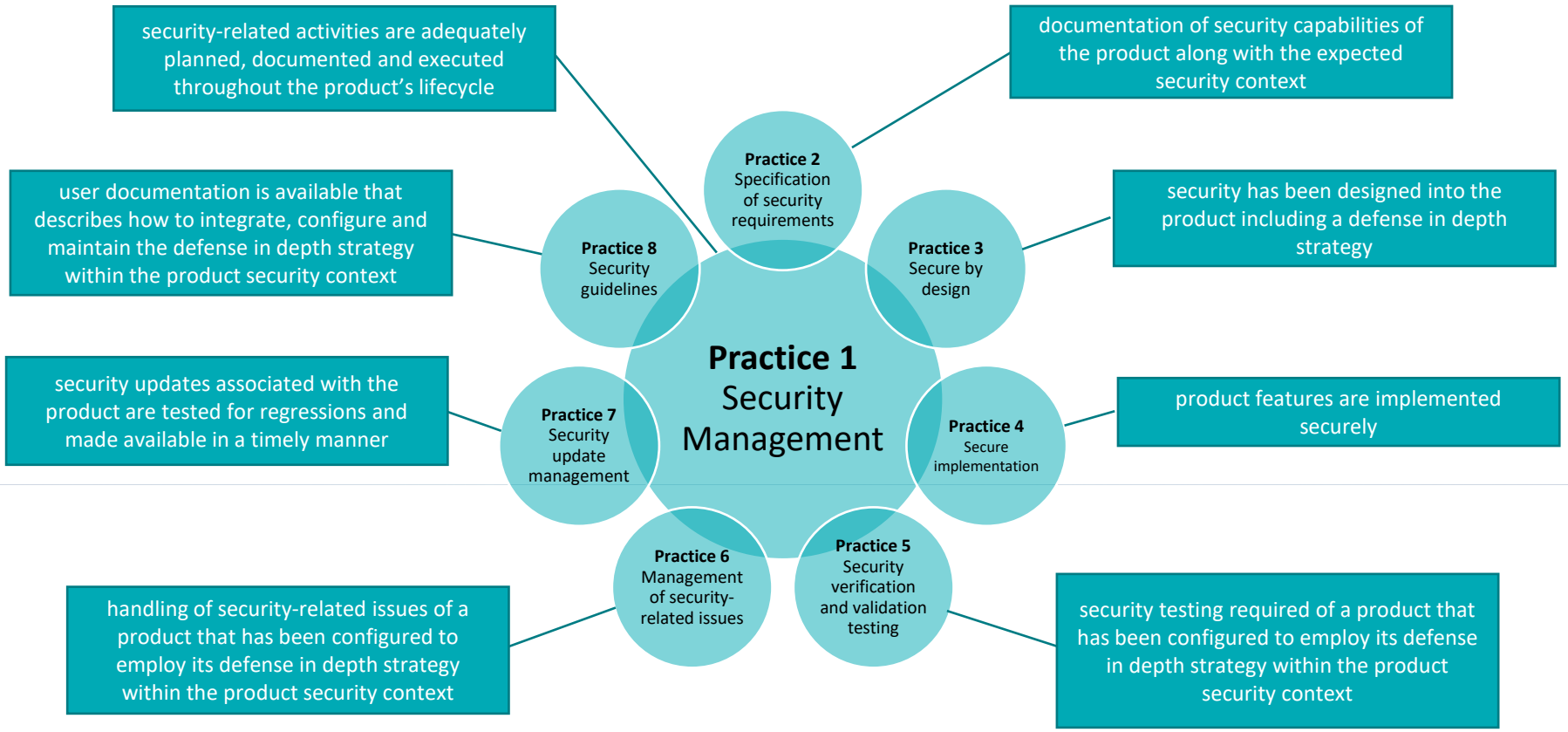
Security Lifecycles

IACS System Lifecycle View

Product Security Lifecycle	Automation Solution Security Lifecycle						
	Integration				Operation and Maintenance		
	Specify	Design	Implement	Verify & Validate	Operate	Maintain	Decommission
Part 1-1: Terminology, Concepts and Models							
	Part 2-1: Establishing an IACS Security Program						
	Part 2-2: IACS Security Program Rating						
	Part 2-3: Patch Management in the IACS environment						
	Part 2-4: Security program requirements for IACS service providers						
	Part 3-2: Security risk assessment for system design						
Part 3-3: System security requirements and security levels							
Part 4-1: Product security development lifecycle requirements							
Part 4-2: Technical security requirements for IACS components							

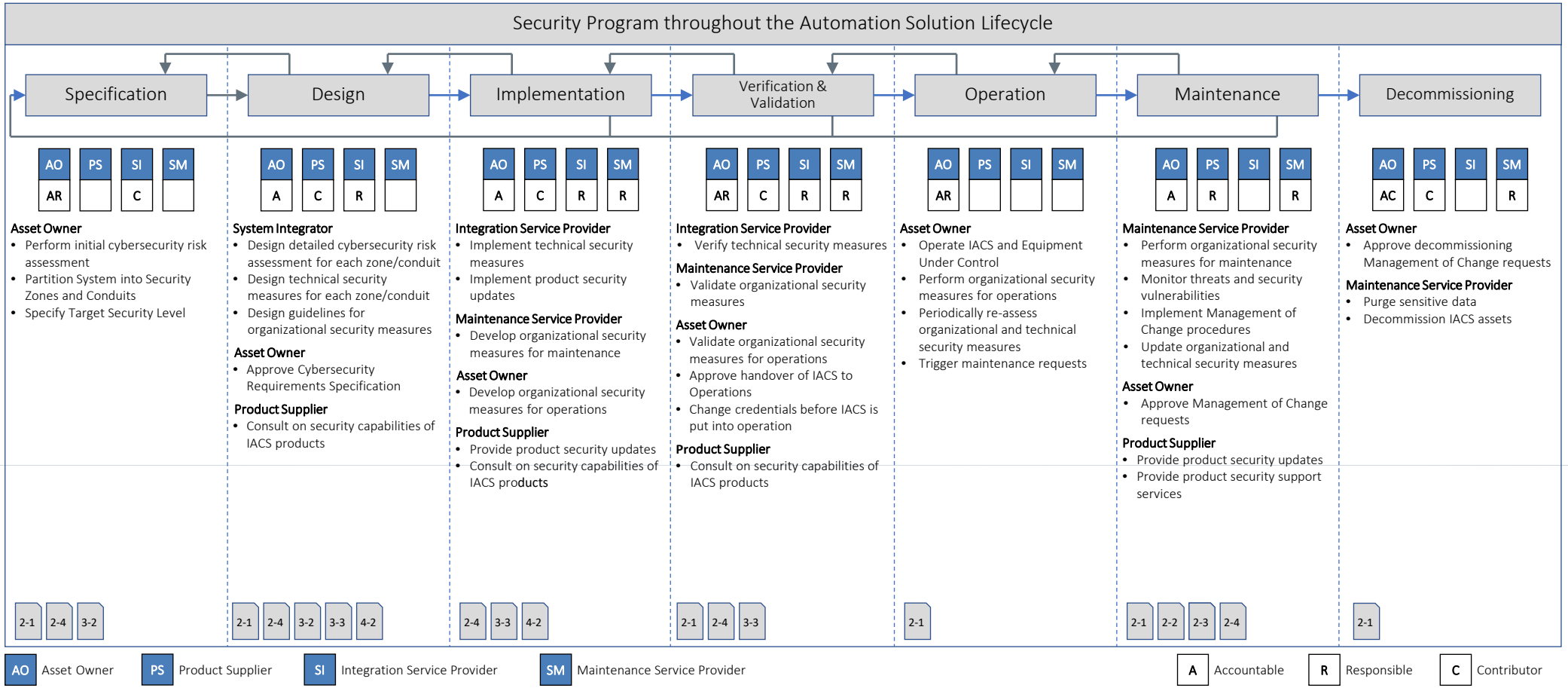
ISA Security Compliance Institute

Product Security Lifecycle



ISA Security Compliance Institute

Automation Solution Security Lifecycle



ISA Security Compliance Institute

Risk Management

IACS Risk Management

- IACS Security Program (Part 2-1)
  - Asset Owners
- Risk assessment (Part 3-2)
  - Zone and conduit partitioning
  - Target Security Levels
  - Cybersecurity Requirements Specification
- Technical requirements for systems and components (Parts 3-3, 4-2)
  - Security Level
  - Foundational Requirements
- Product Security Lifecycle (Part 4-1)
  - Threat modeling
- Automation Solution Security Lifecycle
  - Integration Service Provider (Part 2-4)
  - Maintenance Service Provider (Part 2-4)
  - Security Program Rating (Part 2-2)

Zones and Conduits

- Zone
  - a logical grouping of physical, informational, and application assets sharing common security requirements
  - A zone has a boundary between trusted and untrusted assets
- Conduit
  - a logical grouping of communication channels, connecting two or more zones, that share common security requirements
- Zone and Conduit requirements:
  - Separate business and IACS assets (Shall)
  - Separate safety related assets (Shall)
  - Separate temporarily connected devices (Should)
  - Separate wireless devices (Should)
  - Separate devices connected via external networks (Should)
- Consider both logical and physical separation
- Security is enforced by security measures at the boundary and in the Zone

Essential Functions

- Essential Function
  - A function or capability that is required to maintain health, safety, the environment, and availability of the Equipment under Control
  - protection, control, and view of the Equipment under Control
  - Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment

- Constraints on system design
  - Access controls shall not prevent operation of essential functions
  - Essential Functions shall be maintained if the zone boundary protection (firewall) goes into fail close / island mode
  - DoS event on the control system or safety system network shall not prevent safety functions from acting

ISASecure

ISASecure Certification Schemes

- SDLA – Security Development Lifecycle Assurance
  - Part 4-1
  - Product Supplier Security Lifecycle
- SSA – System Security Assurance
  - Part 4-1 and Part 3-3
  - Distributed Control Systems
  - SCADA Systems
  - Safety Instrumented Systems
- CSA – Component Security Assurance
  - Part 4-1 and Part 4-2
  - Software Applications (e.g. Historian)
  - Embedded Devices (e.g. PLC, SIS)
  - Host Devices (e.g. Windows, Linux)
  - Network Devices (e.g. routers, firewalls)

Certified System (SSA)

ISASecure

ISA/IEC 62443-4-1
ISA/IEC 62443-3-3

Certified Component (CSA)

ISASecure

ISA/IEC 62443-4-1
ISA/IEC 62443-4-2

ISA Resources

ISA Cybersecurity Resources

- Quick Start Guide: An Overview of the ISA/IEC 62443 Series of Standards
  - https://gca.isa.org/isagca-quick-start-guide-62443-standards
- Quick Start Guide: An Overview of ISASecure® Certification
  - TBD
- Security Lifecycles in the ISA/IEC 62443 Series
  - https://gca.isa.org/isagca-security-lifecycles-62443
- ISA/IEC 62443—Security for Industrial Automation and Control Systems
  - https://www.isa.org/standards-and-publications/isa-standards/
- ISASecure Product Certification
  - https://ISASecure.org
- ISA Training
  - https://www.isa.org/training-and-certification/isa-training/iacs-cybersecurity-training
- *Security PHA Review for Consequence-Based Cybersecurity*
  - https://www.isa.org/products/security-pha-review-for-consequence-based-cybe-1

Phone: +1 919-549-8411 **E-mail Address:** info@isa.org

ISA Security Compliance Institute

Thank You