Security Lifecycles in ISA/IEC 62443 Cybersecurity Standards

ISASecure®

Johan B Nye
ICS Guru LLC
September 23, 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

- Key messages
- Principal roles and responsibilities
- Industrial Automation and Control Systems (IACS)
- ISA/IEC 62443 series of standards
- Product Security Lifecycle
- Automation Solution Security Lifecycle

Note: this presentation is based on ISA 99 Committee draft documents and is subject to change

Key messages

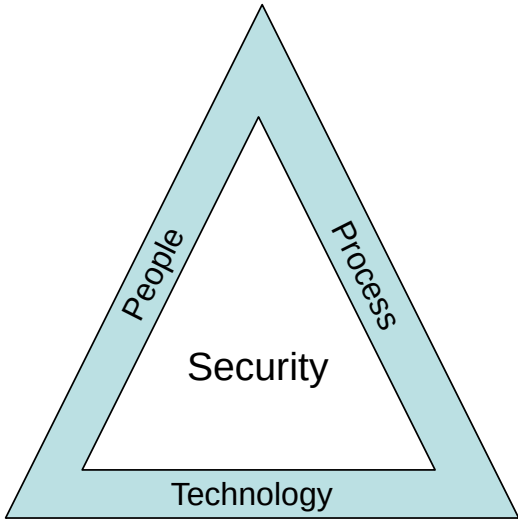
- Asset Owner is *accountable* for the cybersecurity risk of the IACS and the Equipment Under Control
- IACS cybersecurity is a *shared responsibility* between Asset Owner, Product Supplier and Service Providers
- IACS cybersecurity is required *throughout the Product Security Lifecycle*
- IACS cybersecurity is required *throughout the Automation Solution Security Lifecycle*

IACS Principal Roles

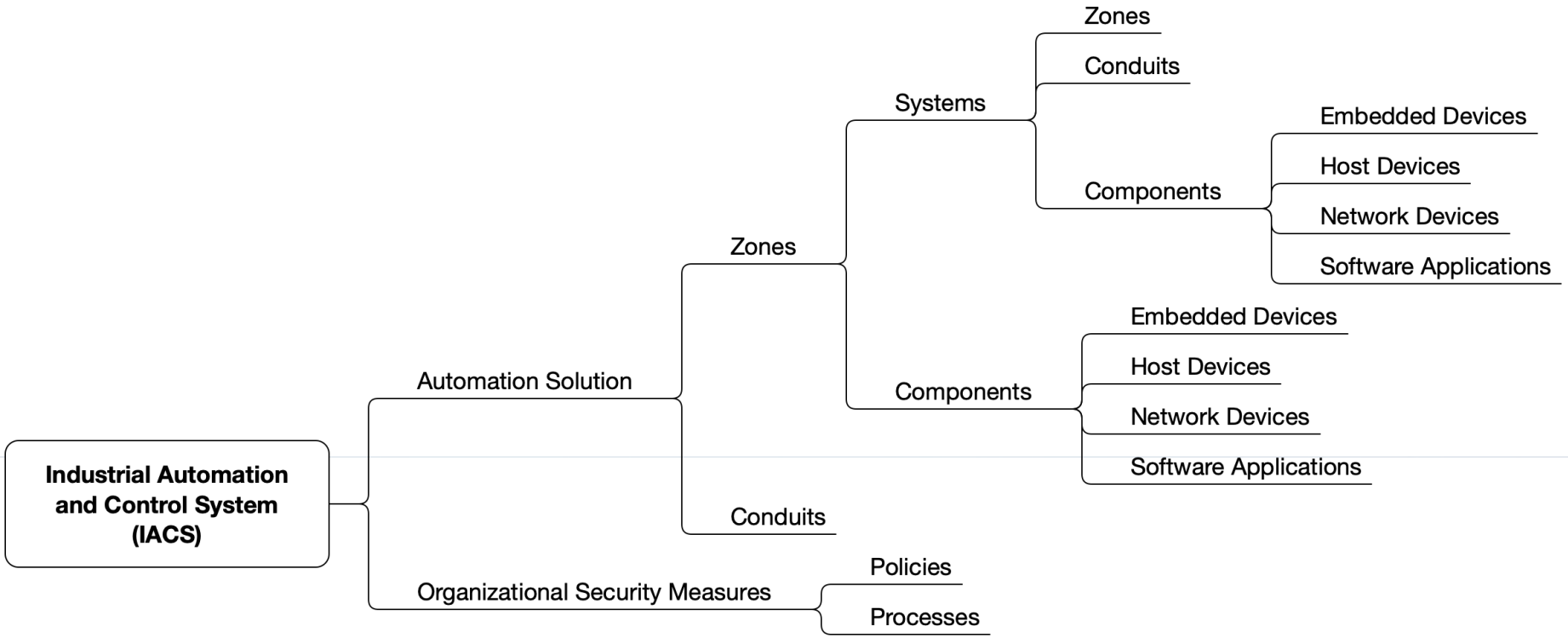
- Asset owner
  - is accountable and responsible for one or more IACSs
  - operates the IACS and the Equipment under Control
- Product Supplier
  - manufactures and supports an IACS hardware and/or software product
- Service Providers
  - Integration Service Provider (System Integrator)
    - provides system integration activities for an Automation Solution
      - design, installation, configuration, testing, commissioning and handover to the Asset Owner
  - Maintenance Service Provider (Support 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

Defining Industrial Automation and Control

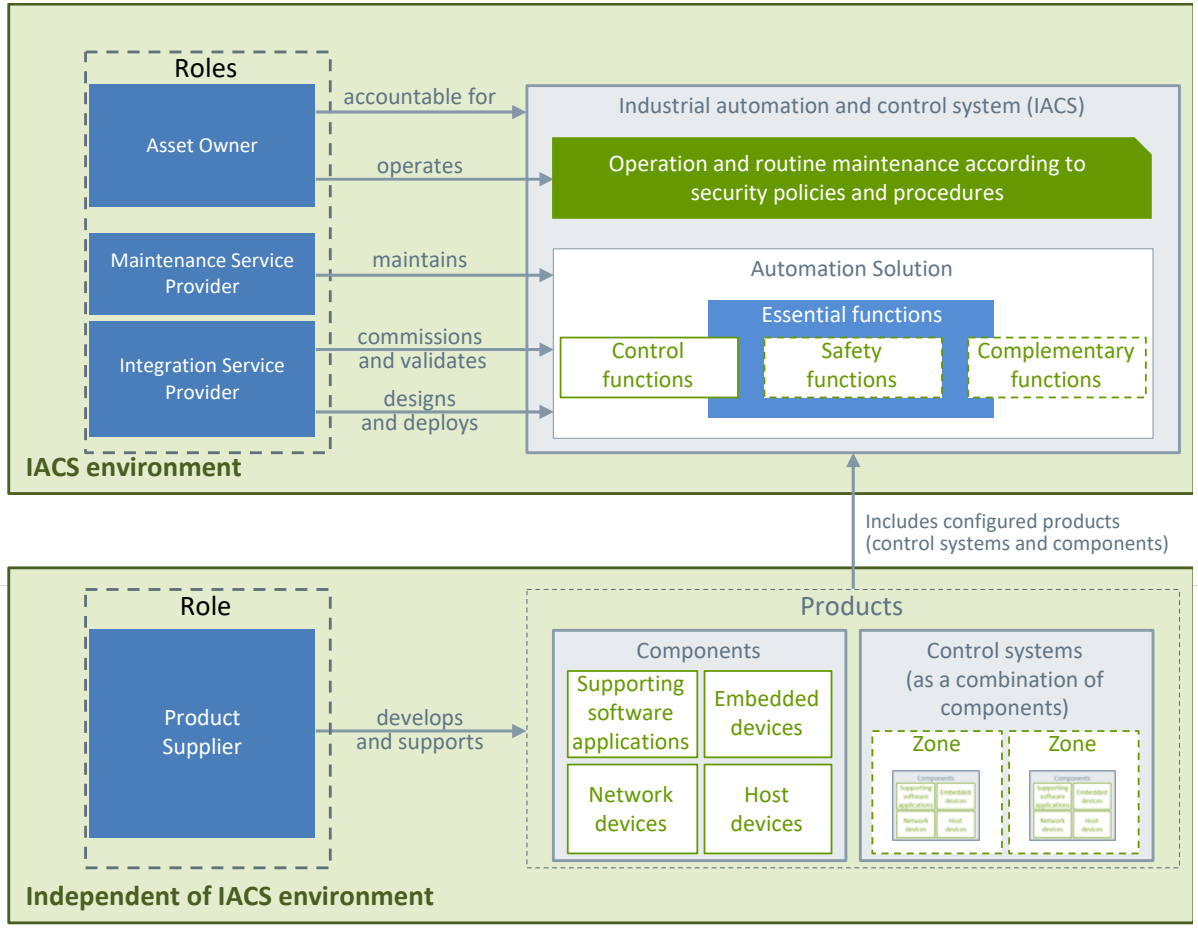
- Component
  - an embedded device, host device, network device, or software application
  - e.g. field devices, PLC, historian, HMI
- Control System (or System)
  - the hardware and software components of an IACS
  - e.g. DCS, SIS, SCADA
- Automation Solution
  - a set of zones and conduits
  - an integrated set of System and Component products
  - an instance at an end user's facility
- Security Program
  - People (training) and Processes (policies and procedures) to manage IACS security
- 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



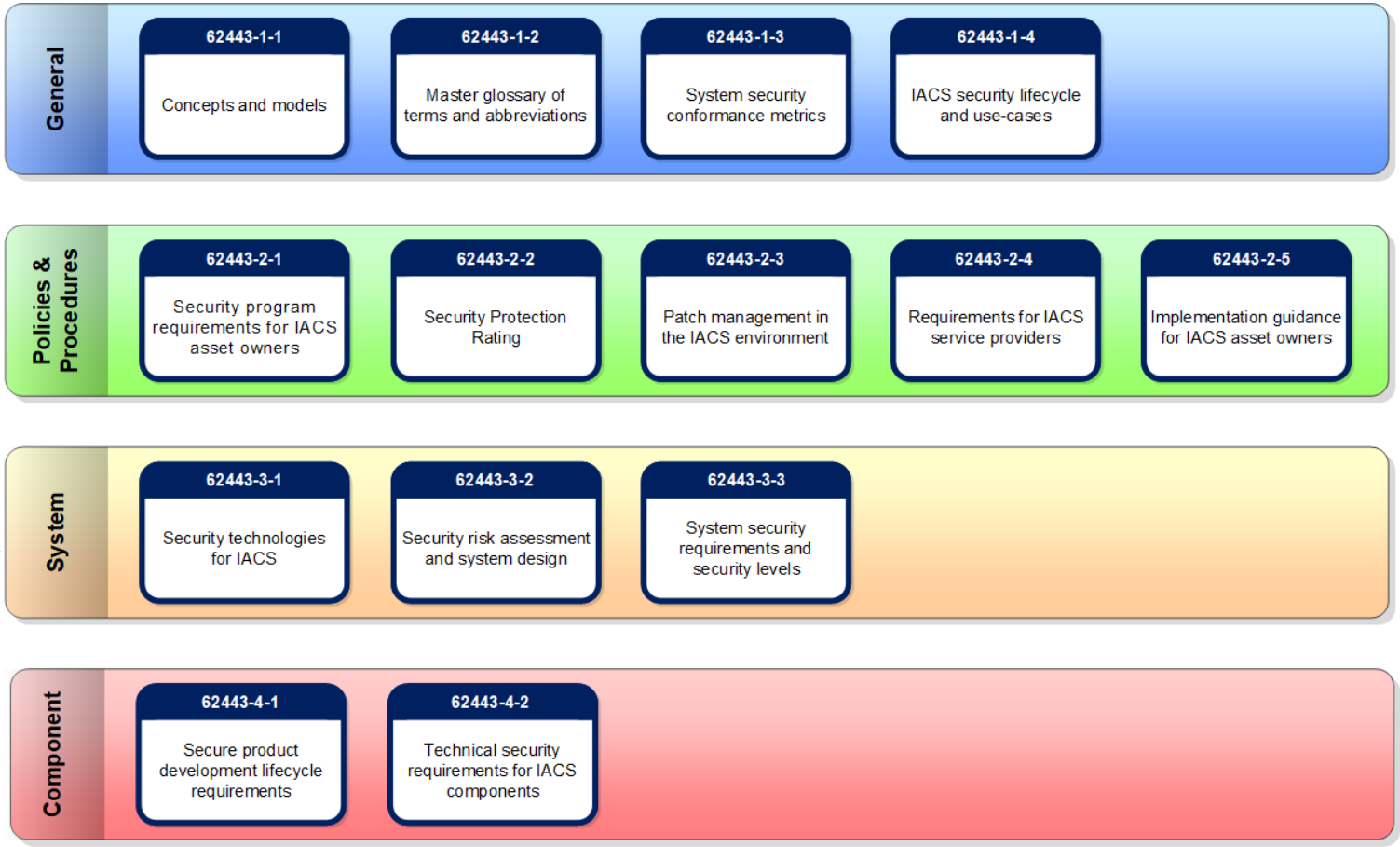
IACS Taxonomy



IACS Principal Roles and Responsibilities



ISA/IEC 62443 Series



ISA Security Compliance Institute

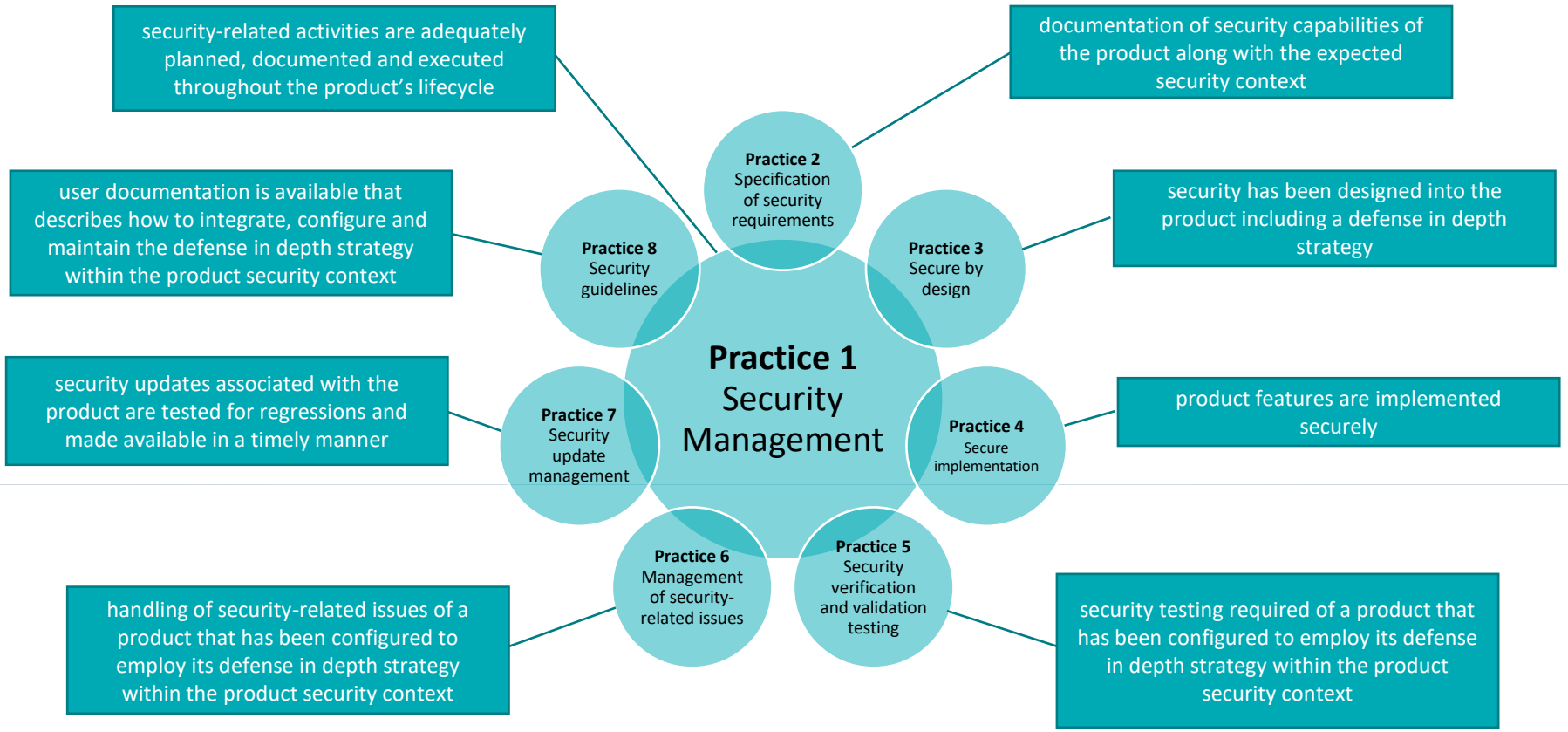
ISA/IEC 62443 Series Details

	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

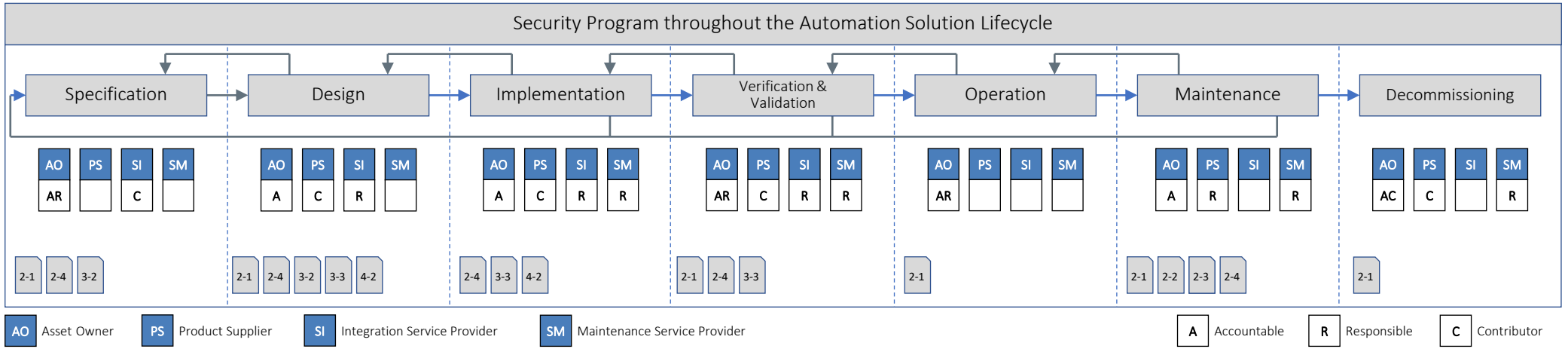
IACS System Lifecycle View

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							

Product Security Lifecycle



Automation Solution Security Lifecycle



ISASecure and the Security Lifecycle

- Product Security Lifecycle
  - Product Supplier submits products and receives certificates that their products conform to ISA/IEC 62443
    - ISASecure Security Development Lifecycle Assurance (SDLA)
    - ISASecure System Security Assurance (SSA)
    - ISASecure Component Security Assurance (CSA)
- Automation Solution Security Lifecycle
  - Specification phase
    - Asset Owner requires that products used in the Automation Solution have been certified to conform to ISA/IEC 62443
  - Design and Implementation phases
    - System Integrator selects products that have been certified to conform with ISA/IEC 62443

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 Cybersecurity Resources

- Quick Start Guide: An Overview of the ISA/IEC 62443 Series of Standards
  - www.isa.org/cyberguide
- Quick Start Guide: An Overview of ISASecure® Certification
  - TBD
- Security Lifecycles in the ISA/IEC 62443 Series
  - TBD
- 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