ISASecure Web Conference

Deep dive into IEC62443-3-3, IEC62443-4-1, and IEC62443-4-2, IEC62443-3-2

Kevin Staggs – Senior Fellow

12 October 2020

ISASecure®

About the Speaker

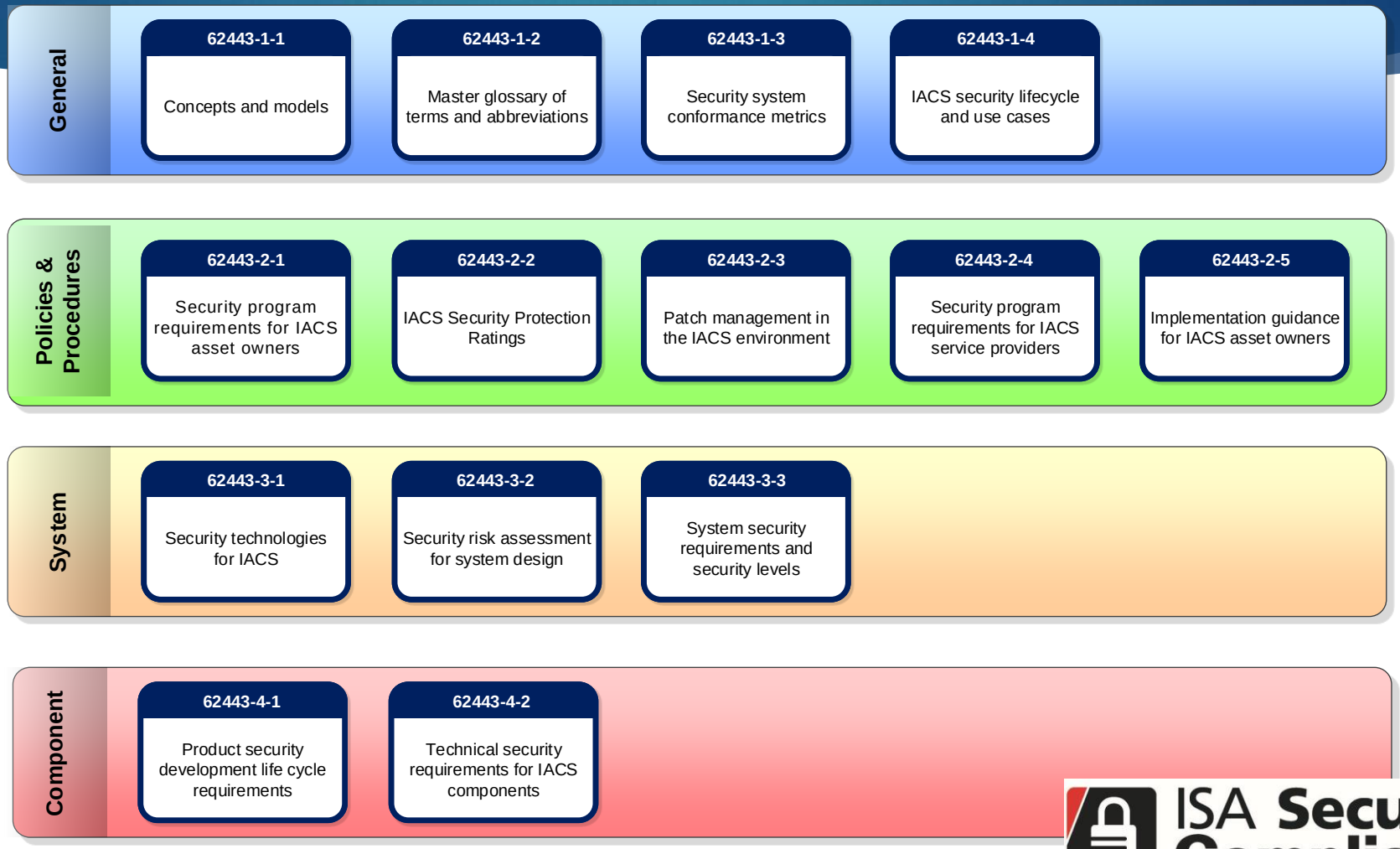
- **Kevin Staggs**
- **Senior Fellow**
- **Kevin Staggs** possesses over 43 years of experience in hardware, software and systems engineering at Honeywell with 39 years focused on control systems. Mr. Staggs has been driving product cybersecurity development since 1996. Mr. Staggs is currently a Senior Fellow in Honeywell's Advanced Connected Technology Solutions organization and serves as a cybersecurity consultant to Honeywell's product development organizations. Mr. Staggs currently serves as co-chairperson of ISA99 working group 4 and is also the technical Chairman of the ISA Security Compliance Institute - a non-profit organization seeking to improve ICS security through standards compliance.

ISA Security Compliance Institute

Agenda

- IEC 62443 Overview
- Roles and Relationship to Standard
- Control System Lifecycles
- IEC-62443-3-2 Overview
- IEC-62443-3-3 Overview
- IEC-62443-4-2 Overview
- IEC-62443-4-1 Overview
- Compliance to IEC-62443

IEC 62443 Standards Family



ISA Security Compliance Institute

General Principles

- Security Context
- Security Objectives
- Response Elements (People, Process Technolo
- Risk-Based Approach
- Compensating Countermeasures
- Least Privilege
- Defense in Depth
- Supply Chain Security
- Security and Safety

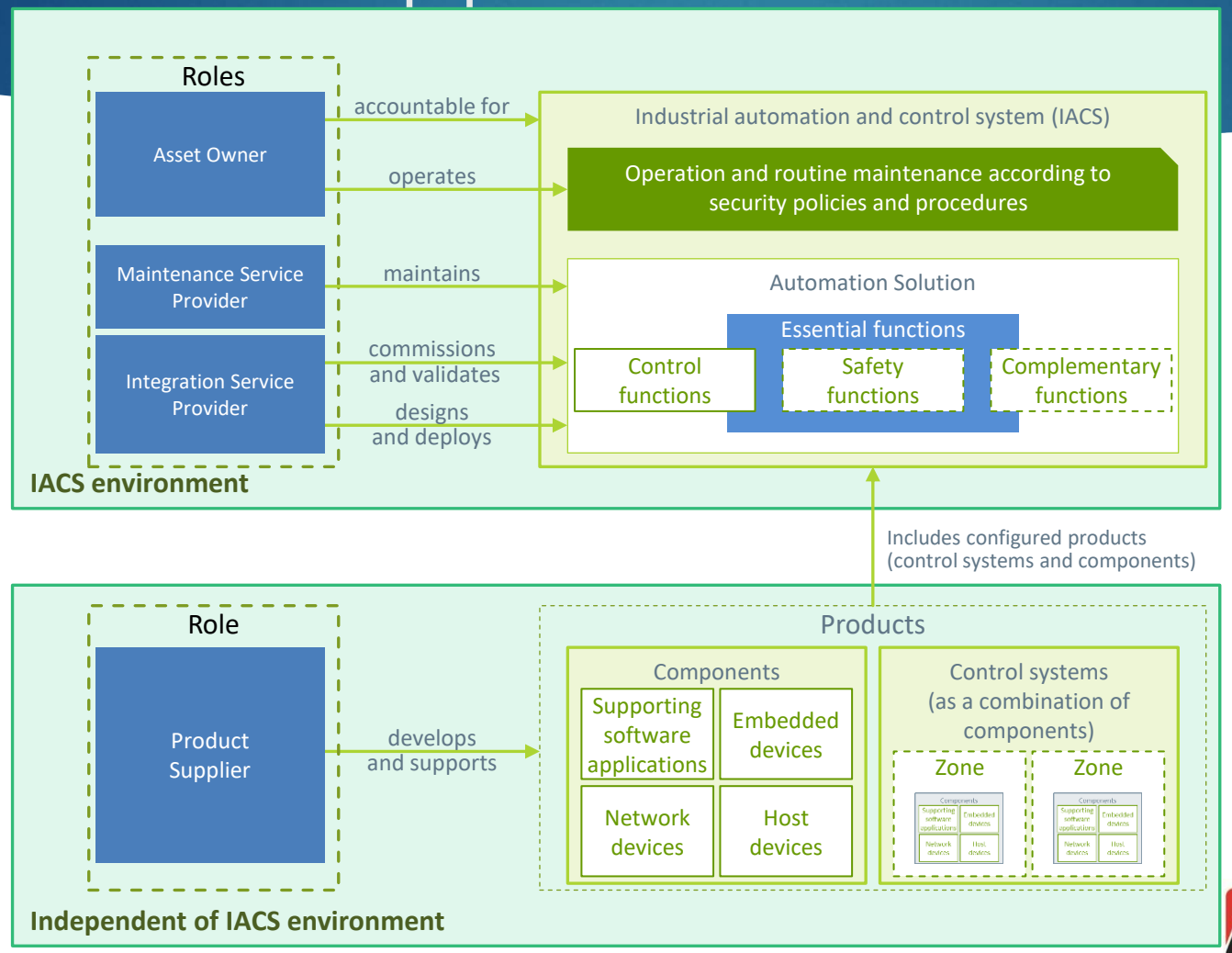
Source: ISA-62443-1-1, 2nd Edition (Under development)

Fundamental Concepts

- System Taxonomy
- Principal Roles
- Life Cycles and Processes
- Zones and Conduits
- Security Levels
- Maturity
- Security Program Rating

Source: ISA-62443-1-1, 2nd Edition (Under development)

Roles and Applicable Standards



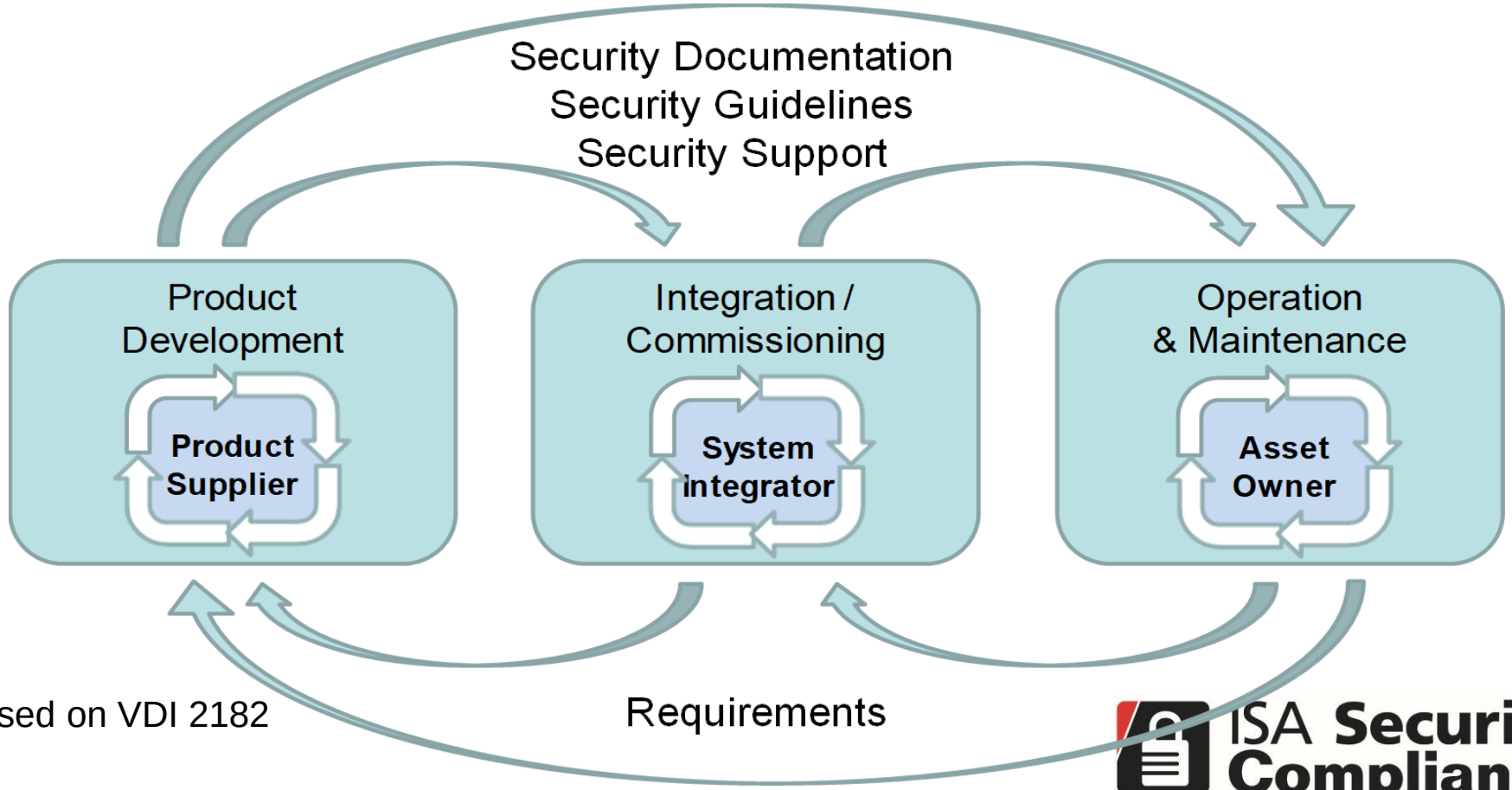
2-1

2-4 3-2 3-3

4-1 4-2 3-3

ISA Security Compliance Institute

Control System LIfecycles



Based on VDI 2182

ISA Security Compliance Institute

System Security

- 62443-3-1
  - Security Technologies
  - Technical Report
- 62443-3-2
  - Risk Assessment and System Design
  - International Standard
- 62443-3-3
  - System Requirements and Security Levels
  - International Standard

ISA Security Compliance Institute

Component Security

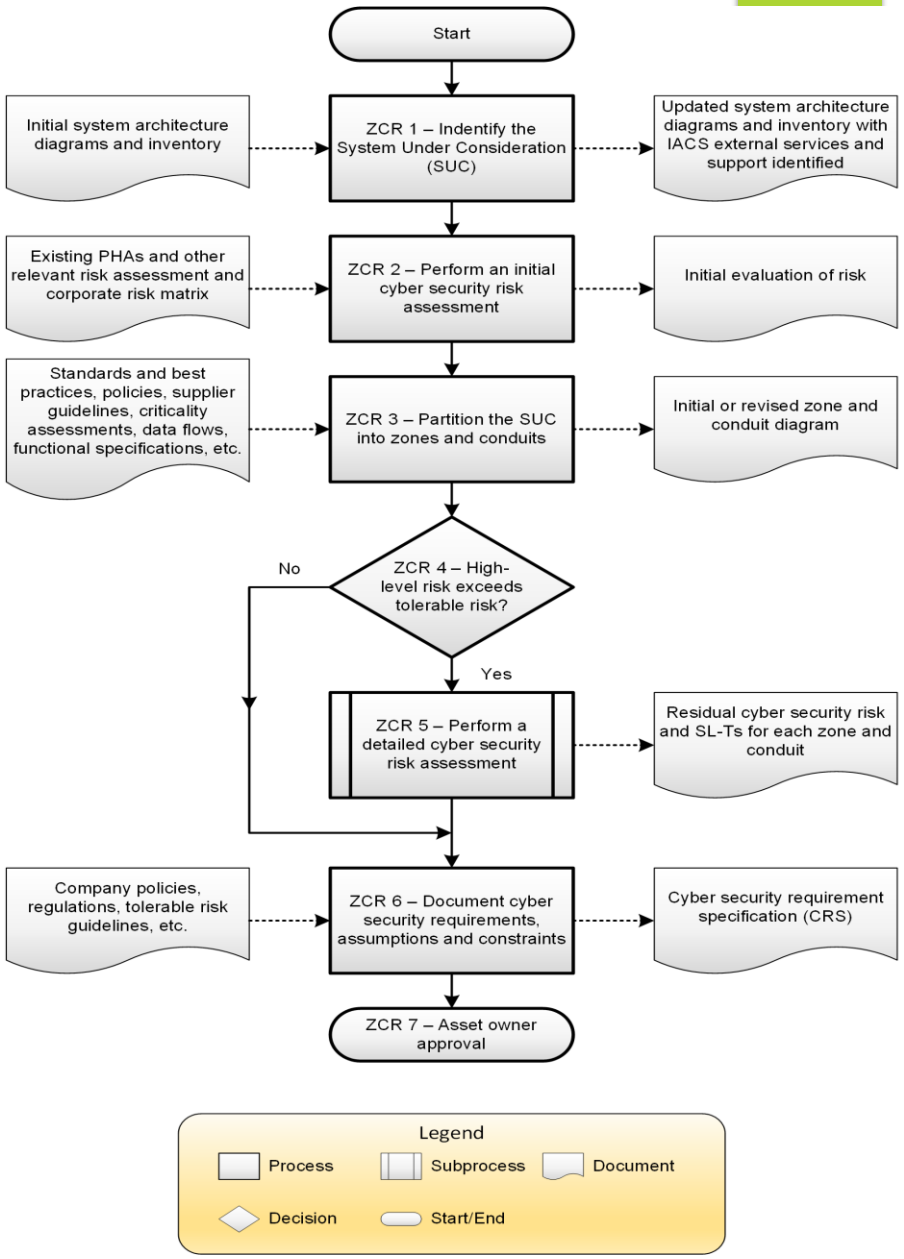
- 62443-4-1
  - Product Development Requirements
  - International Standard
- 62443-4-2
  - Technical Requirement for Components
  - International Standard

ISA Security Compliance Institute

IEC-62443-3-2 Overview

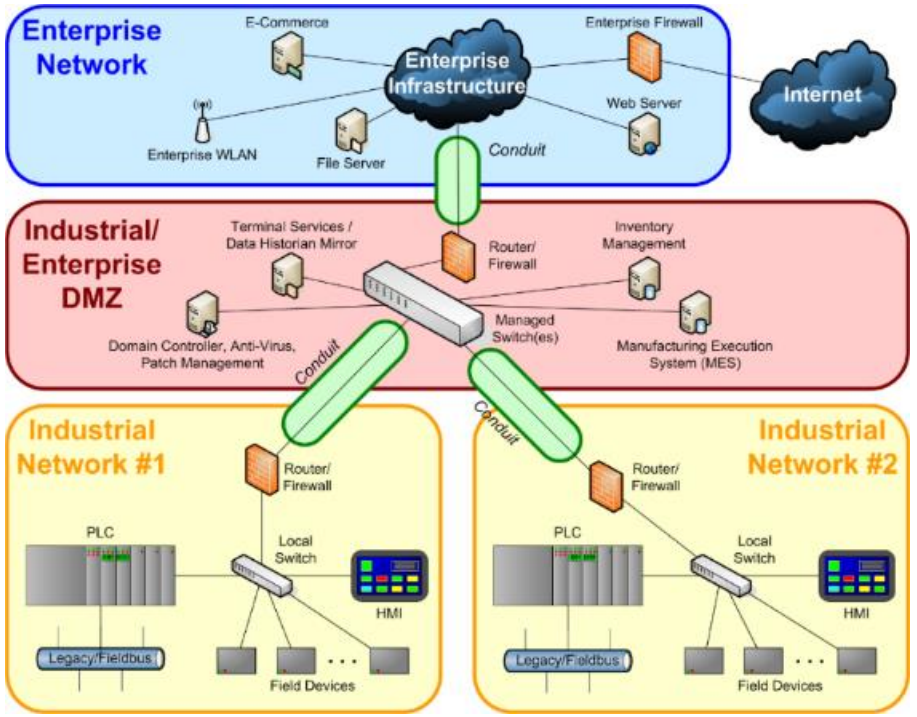
- Document title
  - **Security risk assessment for system design**
- Document defines a process for:
  - defining a system under consideration (SUC) for an industrial automation and control system (IACS);
  - partitioning the SUC into zones and conduits;
  - assessing risk for each zone and conduit;
  - establishing the target security level (SL-T) for each zone and conduit; and
  - documenting the security requirements.

IEC-62443-3-2 Process



Zones and Conduits

- A means for defining…
  - How different systems interact
  - Where information flows between systems
  - What form that information takes
  - What devices communicate
  - How fast/often those devices communicate
  - The security differences between system components
- Technology helps, but architecture is more important



ISA Security Compliance Institute

IEC-62443-3-3 Overview

- Document title
  - **System security requirements and security levels**
- Document defines:
  - Technical security capabilities for a control system;
    - Derived from the 62443 Foundational Requirements;
  - Defines system security capability levels;
    - Based on adversary capabilities;
    - Increasing security capability levels address increasing risk;
  - Organized as base requirements and requirement enhancements;
    - Requirement enhancements increase security capability level.

Foundational Requirements

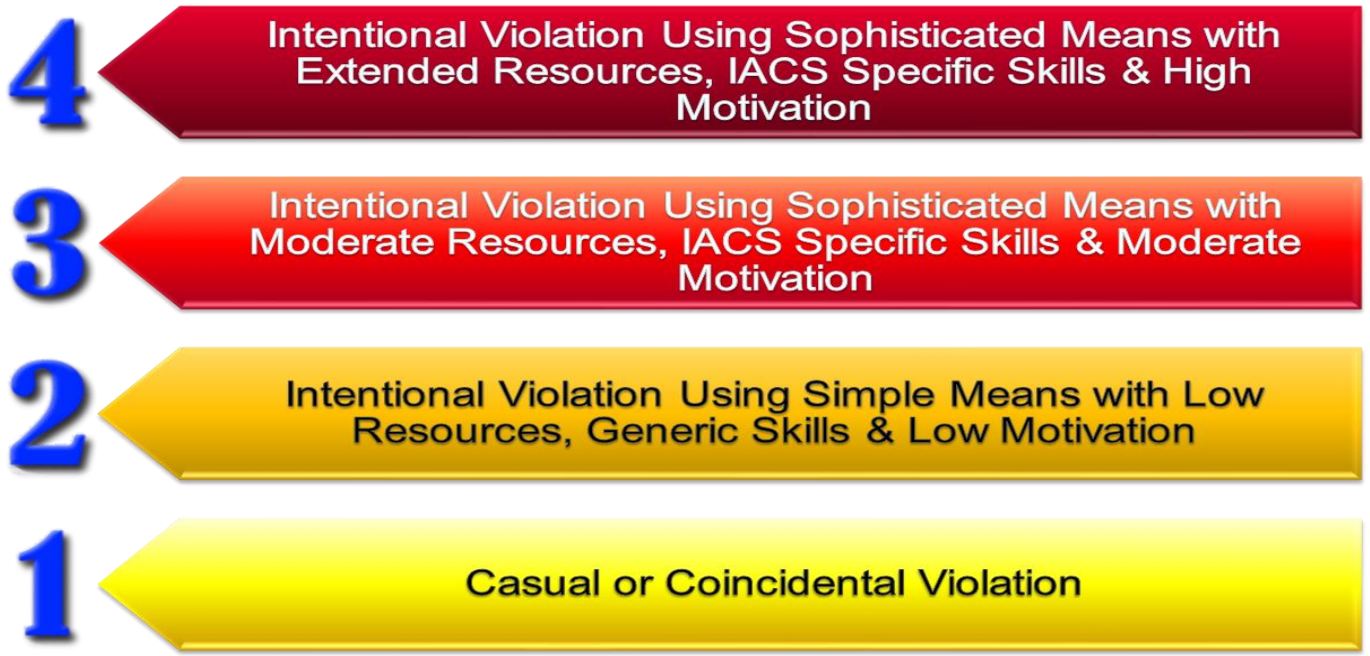
- FR 1 – Identification & authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

Foundational Requirements

- FR 1 – 13 system requirements – 11 requirement enhancements
- FR 2 – 12 system requirements – 12 requirement enhancements
- FR 3 – 9 system requirements – 10 requirement enhancements
- FR 4 – 3 system requirements – 3 requirement enhancements
- FR 5 – 4 system requirements – 7 requirement enhancements
- FR 6 – 2 system requirements – 1 requirement enhancement
- FR 7 – 8 system requirements – 5 requirement enhancements

Security Levels

Protection against…



IEC-62443-3-3 Security Levels

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all networks				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
RE (1) Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓
SR 1.5 – Authenticator management	✓	✓	✓	✓

IEC 62443-4-2 Overview

- Document title
  - **Technical security requirements for IACS components**
- Derived component requirements from 62443-3-3
- Defines component types that make up a control system:
  - Host device
  - Network device
  - Embedded device
  - Application
- ICS Component may contain multiple types
- Requires that components be developed with a Secure Software Development Process (62443-4-1)

Component Type Definitions

- Embedded device
  - special purpose device designed to directly monitor or control an industrial process
- Host device
  - general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers
- Network device
  - device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process
- Software application
  - one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)
- Examples included in Annex A of standard

ISA/IEC 62443-4-2 Requirements

- Common security constraints for all component types
  - Essential functions
  - Compensating countermeasures
  - Least privilege
  - Software development process
- Follows the Security Level – Capability model from 62443-3-3
- Most requirements are common for all component types
- Component specific requirements
  - Designated by SAR, EDR, HDR, and NDR
  - Introduction of component specific integrity requirements

Security Levels (Annex B)

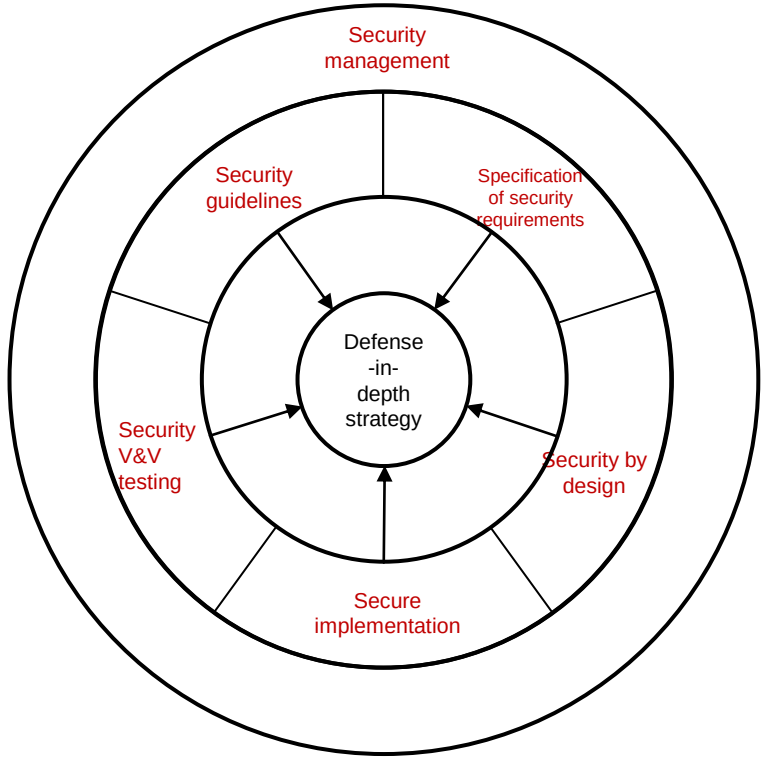
CRs and REs	SL 1	SL 2	SL 3	SL 4
FR 3 – System integrity (SI)				
CR 3.1 – Communication integrity	✓	✓	✓	✓
RE (1) Communication authentication		✓	✓	✓
SAR 3.2 – Protection from malicious code	✓	✓	✓	✓
EDR 3.2 – Protection from malicious code	✓	✓	✓	✓
HDR 3.2 – Protection from malicious code	✓	✓	✓	✓
RE (1) Report version of code protection		✓	✓	✓
NDR 3.2 – Protection from malicious code	✓	✓	✓	✓
CR 3.3 – Security functionality verification	✓	✓	✓	✓
RE (1) Security functionality verification during normal operation				✓
CR 3.4 – Software and information integrity	✓	✓	✓	✓
RE (1) Authenticity of software and information		✓	✓	✓
RE (2) Automated notification of integrity violations			✓	✓

IEC 62443-4-1 Overview

- Document title
  - **Product security development lifecycle requirements**
- Defines product development lifecycle requirements
  - Control system components and systems
- Drives security documentation for system integrators and end users
- Defines requirements for supplier response to discovered security vulnerabilities in products and systems
- Defense in depth approach applied to development processes
- Defines development process maturity levels

IEC 62443-4-1 Development Practices

- Security management
- Specification of security requirements
- Secure by design
- Secure implementation
- Security verification and validation testing
- Management of security-related issues
- Security update management
- Security guidelines



ISA Security Compliance Institute

Maturity of the Development Process

- A means of assessing capability
- Similar to Capability Maturity Models
  - e.g., SEI-CMM
- An evolving concept in the standards
  - Applicability to IACS-SMS

ISA Security Compliance Institute

IEC 62443-4-1 Maturity Levels

- Initial
  - Ad-hoc product development practices
- Managed
  - Documented development practices
  - Demonstration of repeatability of practices
- Defined (Practiced)
  - Evidence all practices are followed and managed
- Improving
  - Feedback for consistently improving practices

Summary of 4 standards

- IEC-62443-3-2 is a standard that should be:
  - Utilized by system integrators
- IEC-62443-3-3 is a standard that should be:
  - Implemented by system suppliers
  - Utilized by system integrators and end users as procurement language
- IEC-62443-4-2 is a standard that should be:
  - Implemented by control system component providers
  - Utilized by system integrators and end users as procurement language
- IEC-62443-4-1 is a standard that should be:
  - Implemented by developers of control systems and components
  - Required in procurement language of control systems and components

IEC-62443 Compliance Certifications

- **Compliance to IEC-62443 standards can be certified, for example:**
  1. **ISASecure® Component Security Assurance (CSA) product certification**
     - **ISA/IEC 62443-4-2**
     - **ISA/IEC 62443-4-1**
  2. **ISASecure® System Security Assurance (SSA) product certification**
     - **ISA/IEC-62443-3-3**
     - **ISA/IEC 62443-4-1**
  3. **ISASecure® Security Development Lifecycle Assurance (SDLA) process certification**
     - **ISA/IEC-62443-4-1**

Where to find certifications

- **ISASecure® (CSA) certified components**
  - https://isasecure.org/en-US/End-Users/IEC-62443-4-2-Certified-Components
- **ISASecure® (SSA) certified systems**
  - https://isasecure.org/en-US/End-Users/IEC-62443-3-3-Certified-Systems
- **ISASecure® (SDLA) certified product development lifecycles**
  - https://isasecure.org/en-US/End-Users/IEC-62443-4-1-Certified-Development-Organizations

Summary

- End users:
  - Utilize system integrators that utilize IEC-62443-3-2 methodologies;
  - Procure systems that are compliant (certified) with IEC-62443-3-3;
  - Procure control system components compliant (certified) with IEC-62443-4-2; and
  - Select vendors that have a product development lifecycle compliant (certified) with IEC-62443-4-1.

Thank you

- For more information visit:

https://isasecure.org/en-US/