What’s new in ISA/IEC 62443-4-2

And what does it mean with respect to ISASecure Certifications

www.isasecure.org

Kevin Staggs
Honeywell

About the Presenter – Kevin Staggs

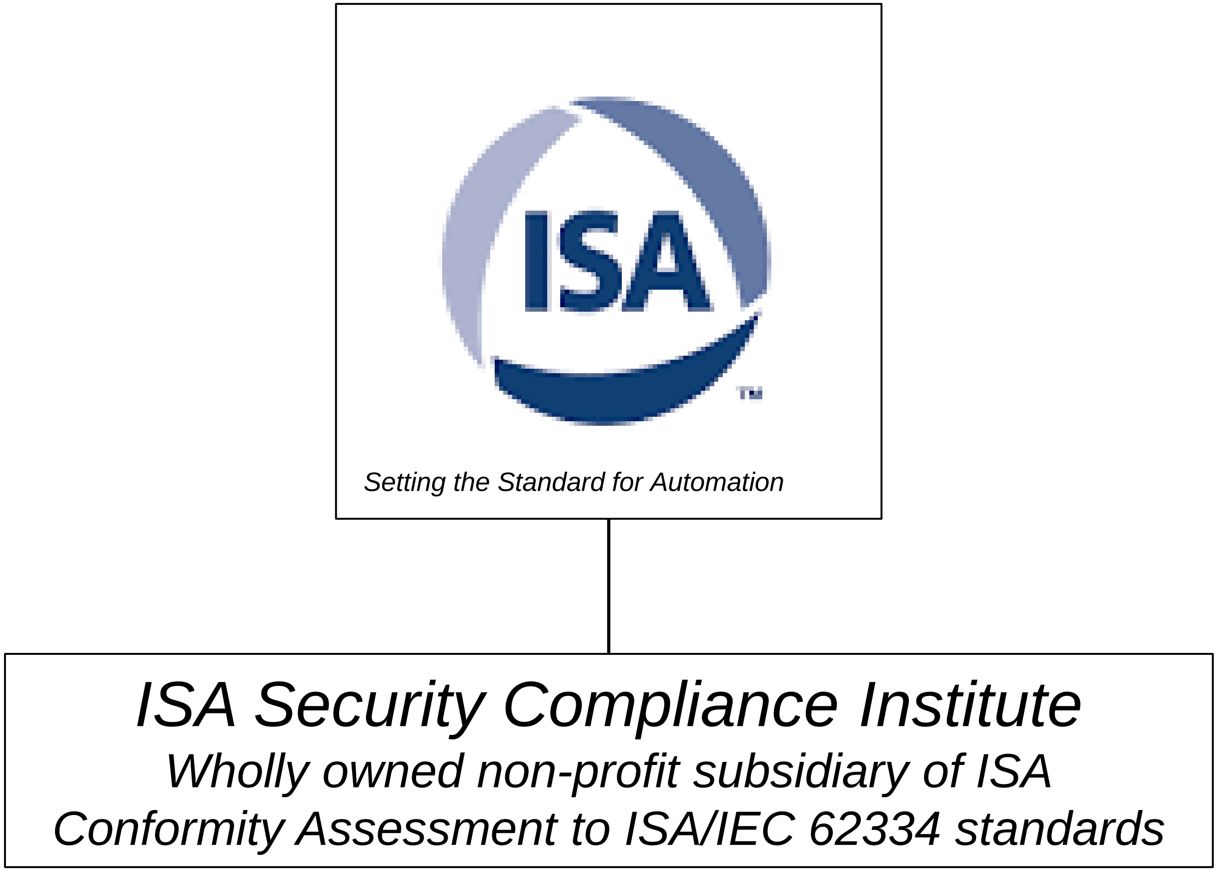
- Honeywell employee for 43 years
  - Senior Engineering Fellow
  - Hardware, software and system design experience
  - 20 years experience in IACS cybersecurity
- 15 years with ISA-99 committee
  - Co-chairman of Working Group 4
- Founding member of ISA Security Compliance Institute
  - Currently Technical Committee chairman
- CISSP, CSSLP and CCSP Certified

International Society of Automation

Setting the Standard for Automation

- Professional Automation Engineering Society
- 40,000 Global Members
- ANSI Accredited SDO

ISA Security Compliance Institute



Setting the Standard for Automation

ISA Security Compliance Institute

Wholly owned non-profit subsidiary of ISA

Conformity Assessment to ISA/IEC 62334 standards

Contributors to ISASecure® Certification Specifications for the ISA/IEC 62443 standards

bp

Chevron

ExxonMobil

YPF

ارامكو السعودية
Saudi Aramco

Honeywell

Rockwell
Automation

Schneider
Electric

SIEMENS
Ingenuity for life

HITACHI
Inspire the Next

YOKOGAWA

ISA

exida.com

IPA Better Life
with IT

CSSC

SYNOPSYS®

WisePlant®

TÜVRheinland®
Precisely Right.

GE Digital

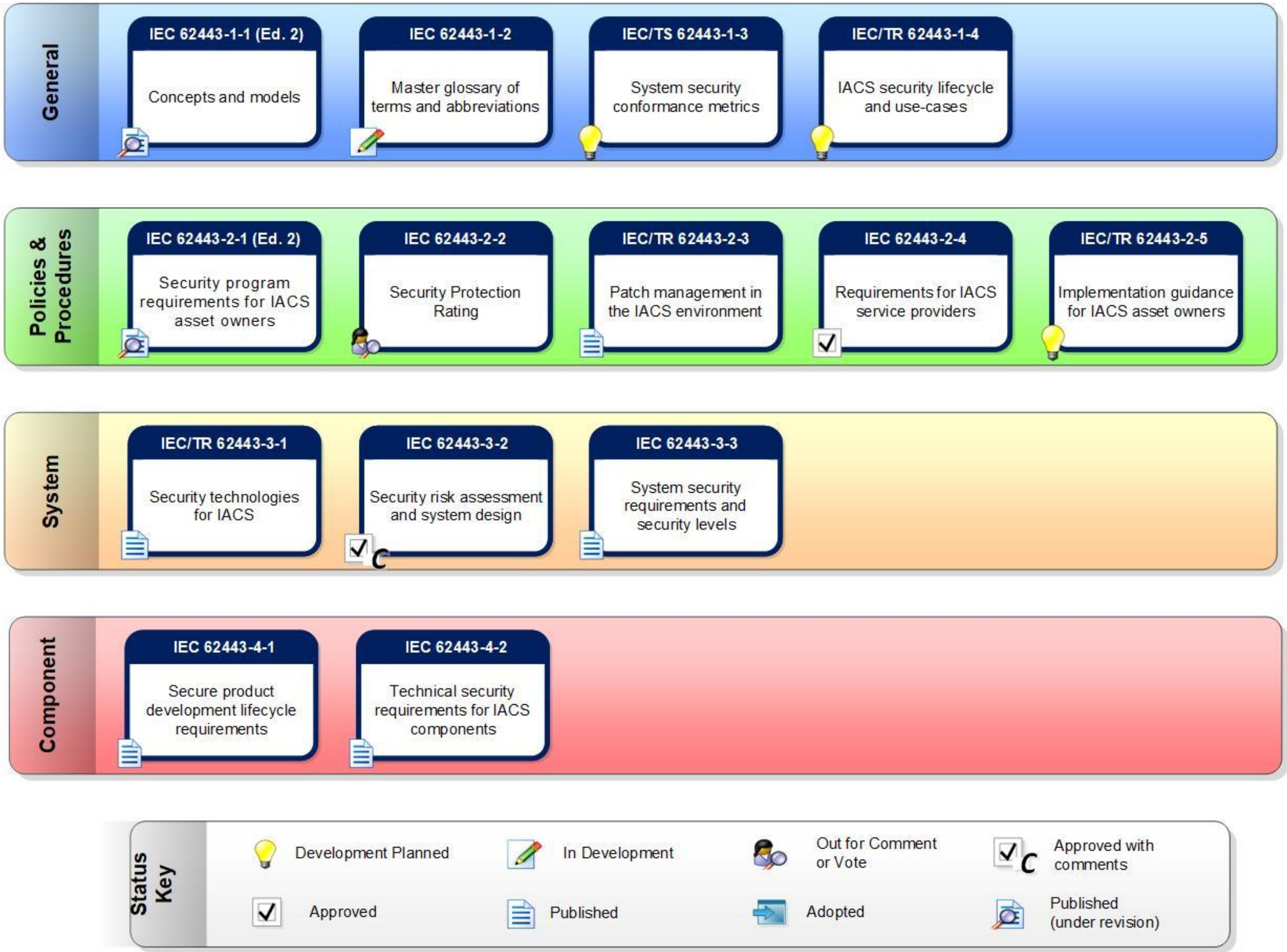
BEYOND security

KPMG

CSA
Group

Johnson
Controls

ISA/IEC 62443 Standards Family



General		
IEC 62443-1-1 (Ed. 2)	Concepts and models	🔍
IEC 62443-1-2	Master glossary of terms and abbreviations	✎
IEC/TS 62443-1-3	System security conformance metrics	💡
IEC/TR 62443-1-4	IACS security lifecycle and use-cases	💡

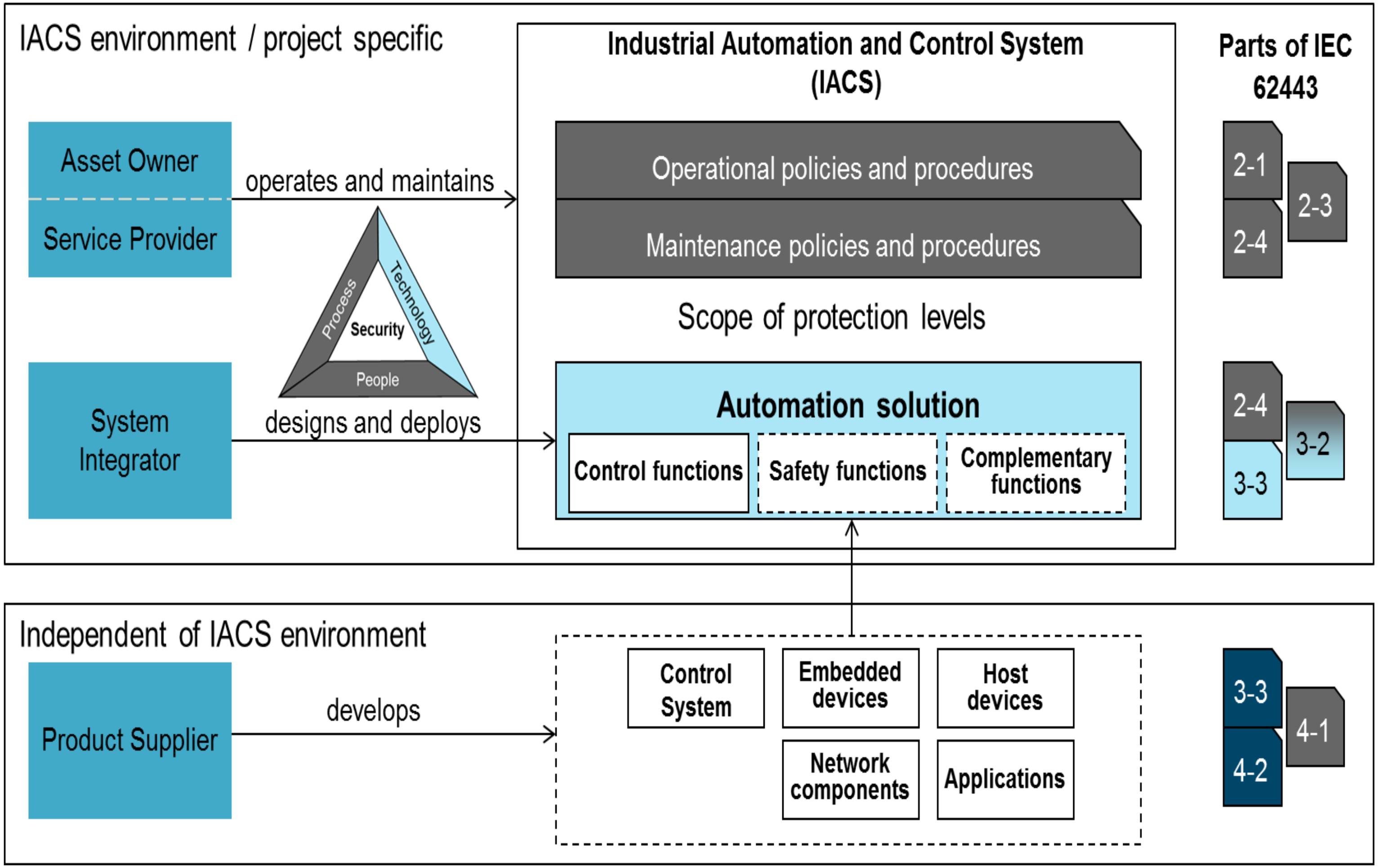
Policies & Procedures		
IEC 62443-2-1 (Ed. 2)	Security program requirements for IACS asset owners	🔍
IEC 62443-2-2	Security Protection Rating	🕵
IEC/TR 62443-2-3	Patch management in the IACS environment	📄
IEC 62443-2-4	Requirements for IACS service providers	☑
IEC/TR 62443-2-5	Implementation guidance for IACS asset owners	💡

System		
IEC/TR 62443-3-1	Security technologies for IACS	📄
IEC 62443-3-2	Security risk assessment and system design	☑C
IEC 62443-3-3	System security requirements and security levels	📄

Component		
IEC 62443-4-1	Secure product development lifecycle requirements	📄
IEC 62443-4-2	Technical security requirements for IACS components	📄

Status Key			
💡 Development Planned	✎ In Development	🕵 Out for Comment or Vote	☑C Approved with comments
☑ Approved	📄 Published	➡ Adopted	🔍 Published (under revision)

ISA/IEC 62443 Standards Family



What is ISA/IEC 62443-4-2

- 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
- Introduces additional component specific integrity requirements
- 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
- Requirements based on 7 foundational requirements
  - Derived from 62443-3-3
    - Not all requirements have derived requirements
  - Follows the Security Level – Capability model from 62443-3-3
    - Mapping of requirements to SL in Annex B
  - Most requirements are common for all component types
  - Designated by CR in requirements
- Component specific requirements
  - Designated by SAR, EDR, HDR, and NDR
  - Introduction of component specific integrity requirements

Derived Requirement Example

- 62443-3-3 requirement

  SR 1.3 – Account management

  The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

- 62443-4-2 derived requirement

  CR 1.3 – Account management

  Components shall provide the capability to support the management of all accounts directly or integrate into a system that manages accounts according to ISA-62443-3-3 [11] SR 1.3.

Cases of no Derived Requirements

- 62443-3-3 requirement
  - SR 2.3 – Use control for portable and mobile devices
  - SR 5.4 – Application partitioning
  - SR 7.5 – Emergency power

Type Specific Derived Requirements

- 62443-3-3 requirement

  SR 3.2 – Malicious code protection

  The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.

- 62443-4-2 derived requirement

  CR 3.2 – Protection from malicious code

  The protection from malicious code requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

Type Specific Derived Requirements

- 62443-4-2 type specific derived requirement

  SAR 3.2 – Protection from malicious code

  The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.

  EDR 3.2 – Protection from malicious code

  The embedded device shall provide the capability to protect from installation and execution of unauthorized software.

  HDR 3.2 – Protection from malicious code

  There shall be mechanisms on host devices that are qualified by the IACS product supplier to provide protection from malicious code. The IACS product supplier shall document any special configuration requirements related to protection from malicious code.

  NDR 3.2 – Protection from malicious code

  The network device shall provide for protection from malicious code.

New Requirements for Components

- Required for all types of components
  - CR 1.14 – Strength of symmetric key-based authentication

- Required for embedded devices, host devices and network devices
  - CR 2.13 – Use of physical diagnostic and test interfaces
  - CR 3.10 – Support for updates
  - CR 3.11 – Physical tamper resistance and detection
  - CR 3.12 – Provisioning product supplier roots of trust
  - CR 3.13 – Provisioning asset owner roots of trust
  - CR 3.14 – Integrity of the boot process

CR 1.14 Details

- CR 1.14 – Strength of symmetric key-based authentication

  For components that utilize symmetric keys, the component shall provide the capability to:

  a) establish the mutual trust using the symmetric key;

  b) store securely the shared secret (the authentication is valid as long as the shared secret remains secret);

  c) restrict access to the shared secret; and

  d) ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3 – Use of cryptography Subclause 8.5.

- Required for SL-C Level 2 and above
- One requirement enhancement required for SL-C Level 3 and above

  Components shall provide the capability to protect critical, long lived symmetric keys via hardware mechanisms

CR 3.10 Details

- CR 3.10 – Support for updates

  Devices shall support the ability to be updated and upgraded.

- Required for SL-C Level 1 and above

- One requirement enhancement required for SL-C Level 2 and above

  Devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.

CR 3.11 Details

- CR 3.11 – Physical tamper resistance and detection

  Devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

- Required for SL-C Level 2 and above
- One requirement enhancement required for SL-C Level 3 and above

  Devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

CR 3.12 Details

- CR 3.12 – Provisioning product supplier roots of trust

  Devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

- Required for SL-C Level 2 and above

CR 3.13 Details

- CR 3.13 – Provisioning asset owner roots of trust

  Devices shall

  a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and

  b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

- Required for SL-C Level 2 and above

CR 3.14 Details

- CR 3.14 – Integrity of the boot process

  Devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to use.

- Required for SL-C Level 1 and above
- One requirement enhancement required for SL-C Level 2 and above

  Devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

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			✓	✓

ISASecure Component Certification

- ISASecure Component Security Assessment (CSA) released
  - ISA/IEC 62443-4-2 Security Capability Assessment
  - ISA/IEC 62443-4-1 Process Assessment
  - Vulnerability Identification Test
- Replacing EDSA Certification program
  - Functional Security Assessment (pre 62443-4-2)
  - ISA/IEC 62443-4-1 Process Assessment
  - Communications Robustness Testing (CRT)
- Note: ISA/IEC 62443-4-1 requires CRT
  - Testing performed as part of product development
  - Testing and results validated as part of process assessment

Security Capability Assessment

- For components:
  - Independent certification of security capability level (SL) as defined by the ISA/IEC 62443-4-2 standard
  - All component types within the component have been assessed
  - Free from known security vulnerabilities at time of assessment
  - Developed using a secure development lifecycle as defined by ISA/IEC 62443-4-1 standard

Process Assessment

- Independent certification of suppliers Secure Software Development Lifecycle as defined by the ISA/IEC 62443-4-1 standard
- As long as ISASecure SDLA certificate is valid:
  - Supplier has a process for responding to security issues discovered in supported products
  - Product updates and upgrades have been created using an assessed secure development lifecycle

Three ISASecure® certifications available

1. **Component Security Assurance (CSA)** **product certification**

   ISA/IEC 62443-4-2
   ISA/IEC 62443-4-1
   Vulnerability Identification Test

2. **System Security Assurance (SSA)** **product certification**

   ISA/IEC-62443-3-3
   ISA/IEC 62443-4-1
   Vulnerability Identification Test

3. **Security Development Lifecycle Assurance (SDLA)**

   process certification
   ISA/IEC-62443-4-1

Acronyms Used Today

- CR – Component requirement
- SR – System requirement
- SL-C – Capability security level
- SAR – Software application requirement
- EDR – Embedded device requirement
- HDR – Host device requirement
- NDR – Network device requirement

Help us secure our world.

We invite you to join this industry led initiative.

Andre Ristaino
67 Alexander Drive
Research Triangle Park, NC 27709 USA
Phone: +1 919-990-9222 Mobile: +1 919-323-7660
Email: aristaino@isa.org
Web Site: www.isasecure.org