International Society of Automation

ISASecure®

Why Security Level 2 of Industrial Control System Components?

March 28, 2024

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

Agenda

- Introduction of speaker
- Overview of 62443
- Component requirements and security levels
- Additional security level 2 requirements by foundational requirement
- Summary of key additional security capabilities
- Assurance of conformity

Kevin Staggs - introduction

- 47 years industrial control system experience
- 44 years with the same major control system product supplier
- Hardware, software, systems engineering experience
- 25 years cyber security experience
- Member of ISA99 since 2009
- Co-leader of ISA99 Working Group 4
- Founding member of ISCI – technical director for several years
- Currently part-time consultant in industrial cyber security

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. **55+ 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 and CISA; stood up as a new program under ISAGCA. **1,400 volunteers; over 900 companies** www.ics4ics.org

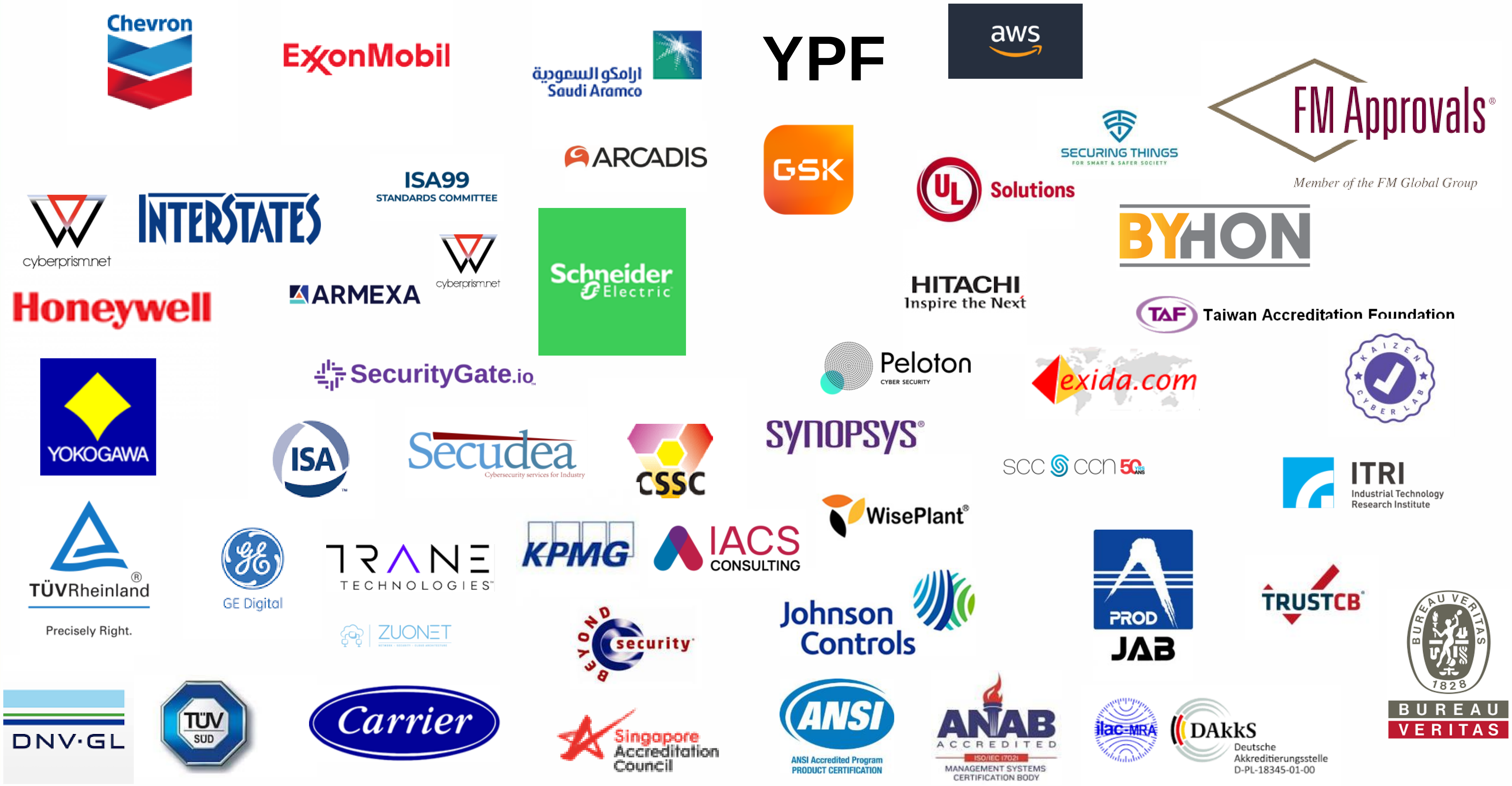
ISA99 Committee

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 1,500 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 **4,000 students in 2023**. https://www.isa.org/training

ISASecure Supporters



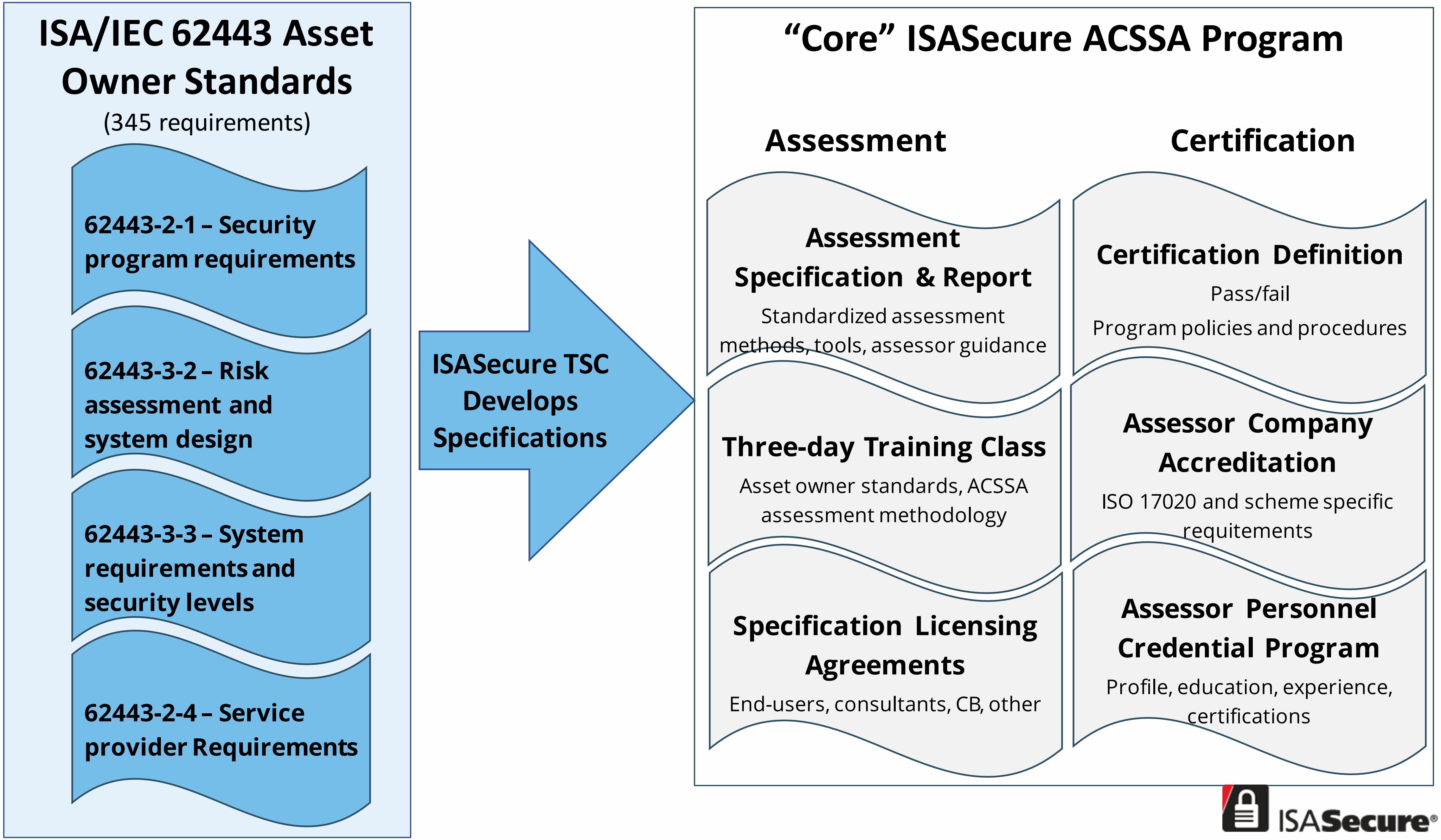
ISASecure Certifications Currently Available

Certification Description	Certification Mark	Availability Date
IIOT Component Security Assurance (ICSA) ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 plus 16 extensions	Certified IIOT Component ISASecure	Since Dec 2022
Component Security Assurance (CSA) ISA/IEC 62443 4-1 and ISA/IEC 62443 4-2	Certified Device ISASecure	Since Aug 2019
System Security Assurance (SSA) ISA/IEC 62443 3-3 and ISA/IEC 62443 4-2 ISA/IEC 62443-4-1	Certified System ISASecure	Since Oct 2018
Security Development Lifecycle Assurance (SDLA) ISA/IEC 62443 4-1	"An ISASecure Certified Development Organization"	Since July 2014

ISASecure Certifications Roadmap

Certification Description	Certification Mark	Availability Date
IIOT System Security Assurance (ISSA) ISA/IEC 62443 4-1 and ISA/IEC 62443 3-3		TBD
Automation and Control system Security Assurance (ACSSA) ISA/IEC 62443 2-1, 2-4, 3-2, 3-3	"ISASecure IEC 62443 Conformant Operating Site"	1H 2025

Automation and Control System Security Assurance (ACSSA)



ISA/IEC 62443 Asset Owner Standards

(345 requirements)

62443-2-1 – Security program requirements

62443-3-2 – Risk assessment and system design

62443-3-3 – System requirements and security levels

62443-2-4 – Service provider Requirements

ISASecure TSC Develops Specifications

"Core" ISASecure ACSSA Program

Assessment

Assessment Specification & Report

Standardized assessment methods, tools, assessor guidance

Three-day Training Class

Asset owner standards, ACSSA assessment methodology

Specification Licensing Agreements

End-users, consultants, CB, other

Certification

Certification Definition

Pass/fail

Program policies and procedures

Assessor Company Accreditation

ISO 17020 and scheme specific requitements

Assessor Personnel Credential Program

Profile, education, experience, certifications

ISASecure®

2023 Membership Additions

Strategic Members

GSK (asset owner)
Trane (technology provider)

Automation Suppliers and Service Providers

Technical

SecurityGate (technical)
Secudea (technical)
Walnut Creek Consulting (Technical)
Arcadis (Technical)
Peloton Cybersecurity (technical)
Enaxy (technical)
Optiv (technical)

Supporter

Generac(supporter)
Interstates (supporter)
Armexa (supporter)
Securing Things (supporter)
CyberPrism (supporter)
IACS Consulting (supporter)

Certification Bodies

Kaizen (India)
UL Solutions (Global)

Associate

Arnoud Soullie
John Kingsley
RBJ Consultancy
Zuonet

Q1 2024 Membership Additions

Certification Bodies

AC&E (Italy/Global)

Associate

ITRI – Representing the Taiwan Government
MIAN

2024 ISASecure Certifications
Majority are SL-2 or SL-3

	Supplier	Device	Model	Version	Level	Certification Date
1	Honeywell Building Technologies	Plant Controller	CPO-PC500/600 Plant Controller	4.1	Level 2	3/21/2024
2	Bitron Electronics S.p.A.	Smart Street Box Remote Terminal Unit	µUP	1.1.x	Level 3	2/26/2024
3	Eurotech	Industrial Edge AI Server	ReliaCOR 44-11	Ubuntu Linux 22.04.x ESF	Level 2	2/16/2024
4	Johnson Controls	Air-Cooled Screw Chiller Control Panel with GUI	YVAA/YVFA Style A	V05 and V06	Level 1	1/30/2024
5	GE Power Conversion	Power Controller	HPCi Controller	8.1.0	Level 3	12/31/2023
6	Honeywell Building Technologies	Controller	Honeywell Advanced Plant Controller	4.1	Level 2	12/29/2023

- 1/3 of all ISASecure certifications are SL-2 or SL-3
- ISASecure requires supplier **62443-4-1 Maturity Level 3 or 4**
- Major O&G companies requiring minimum SL-2

WWW.ISASecure.org arisaino@isa.org

ISASecure®

Committee Description

The International Society of Automation (ISA) Committee on Security for Industrial Automation & Control Systems

- Members from around the world
- Multiple sectors and stakeholders
- Working in collaboration with IEC TC65 WG10
- Consistent leadership since c. 2002

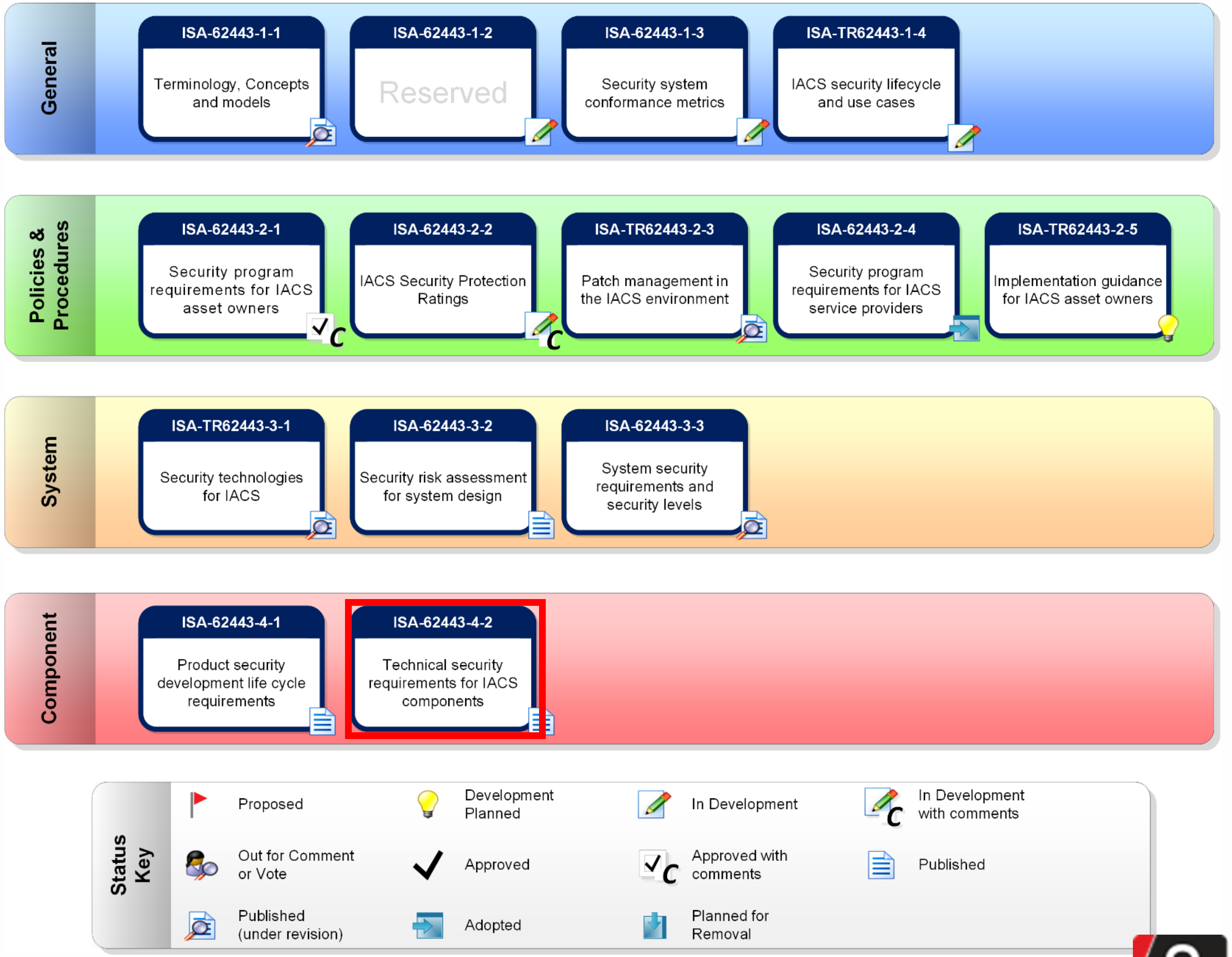
Committee Scope[*]

"… automation and control systems whose compromise could result in any or all of the following situations:

- endangerment of public or employee safety
- environmental protection
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on entity, local, state, or national security"

[*] Taken from the original committee scope description

Document Status



General

- ISA-62443-1-1: Terminology, Concepts and models
- ISA-62443-1-2: Reserved
- ISA-62443-1-3: Security system conformance metrics
- ISA-TR62443-1-4: IACS security lifecycle and use cases

Policies & Procedures

- ISA-62443-2-1: Security program requirements for IACS asset owners
- ISA-62443-2-2: IACS Security Protection Ratings
- ISA-TR62443-2-3: Patch management in the IACS environment
- ISA-62443-2-4: Security program requirements for IACS service providers
- ISA-TR62443-2-5: Implementation guidance for IACS asset owners

System

- ISA-TR62443-3-1: Security technologies for IACS
- ISA-62443-3-2: Security risk assessment for system design
- ISA-62443-3-3: System security requirements and security levels

Component

- ISA-62443-4-1: Product security development life cycle requirements
- ISA-62443-4-2: Technical security requirements for IACS components

Status Key

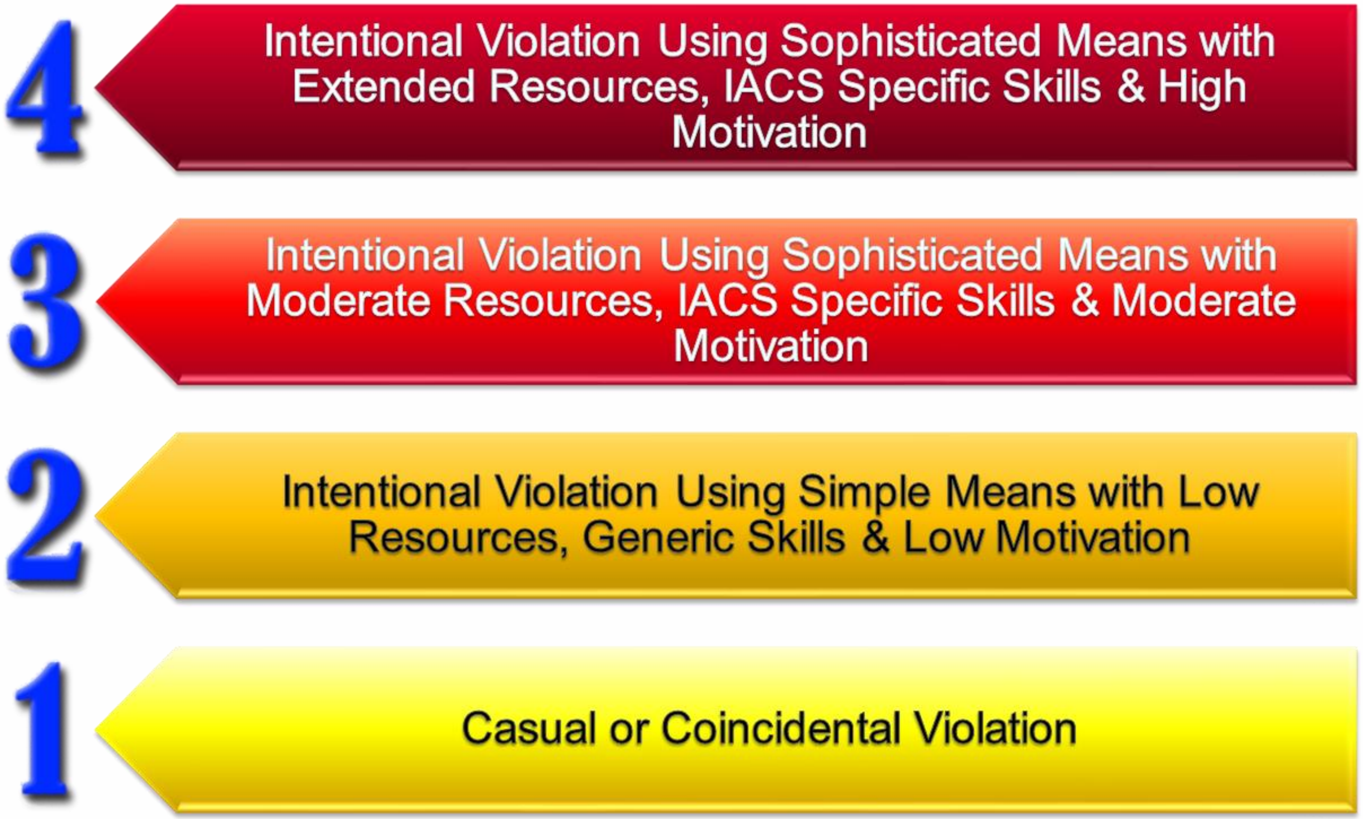
Proposed	Development Planned	In Development	In Development with comments
Out for Comment or Vote	Approved	Approved with comments	Published
Published (under revision)	Adopted	Planned for Removal	

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

Security Levels

Protection against…



4 Intentional Violation Using Sophisticated Means with Extended Resources, IACS Specific Skills & High Motivation

3 Intentional Violation Using Sophisticated Means with Moderate Resources, IACS Specific Skills & Moderate Motivation

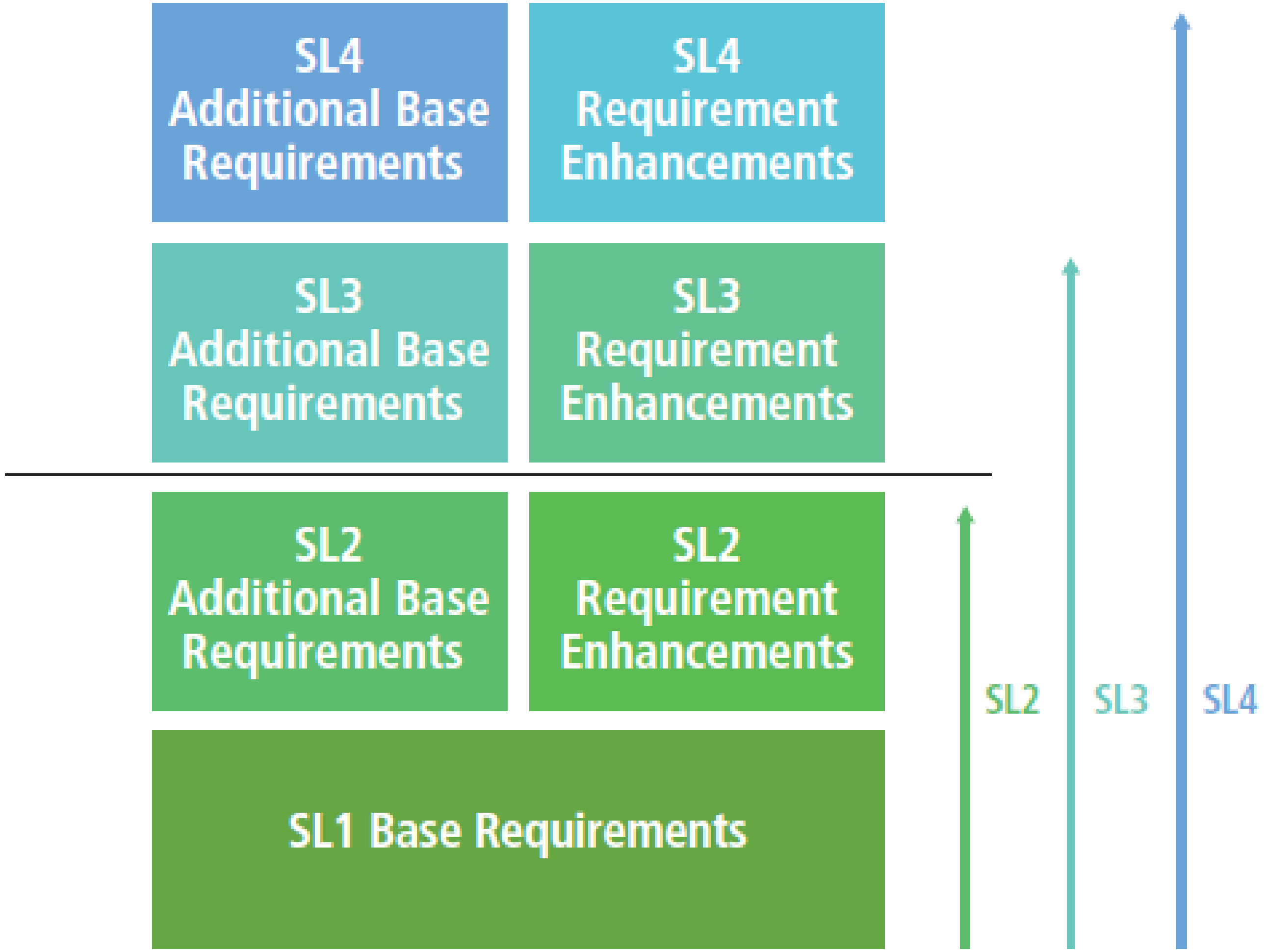
2 Intentional Violation Using Simple Means with Low Resources, Generic Skills & Low Motivation

1 Casual or Coincidental Violation

ISA-62443-4-2 Standard

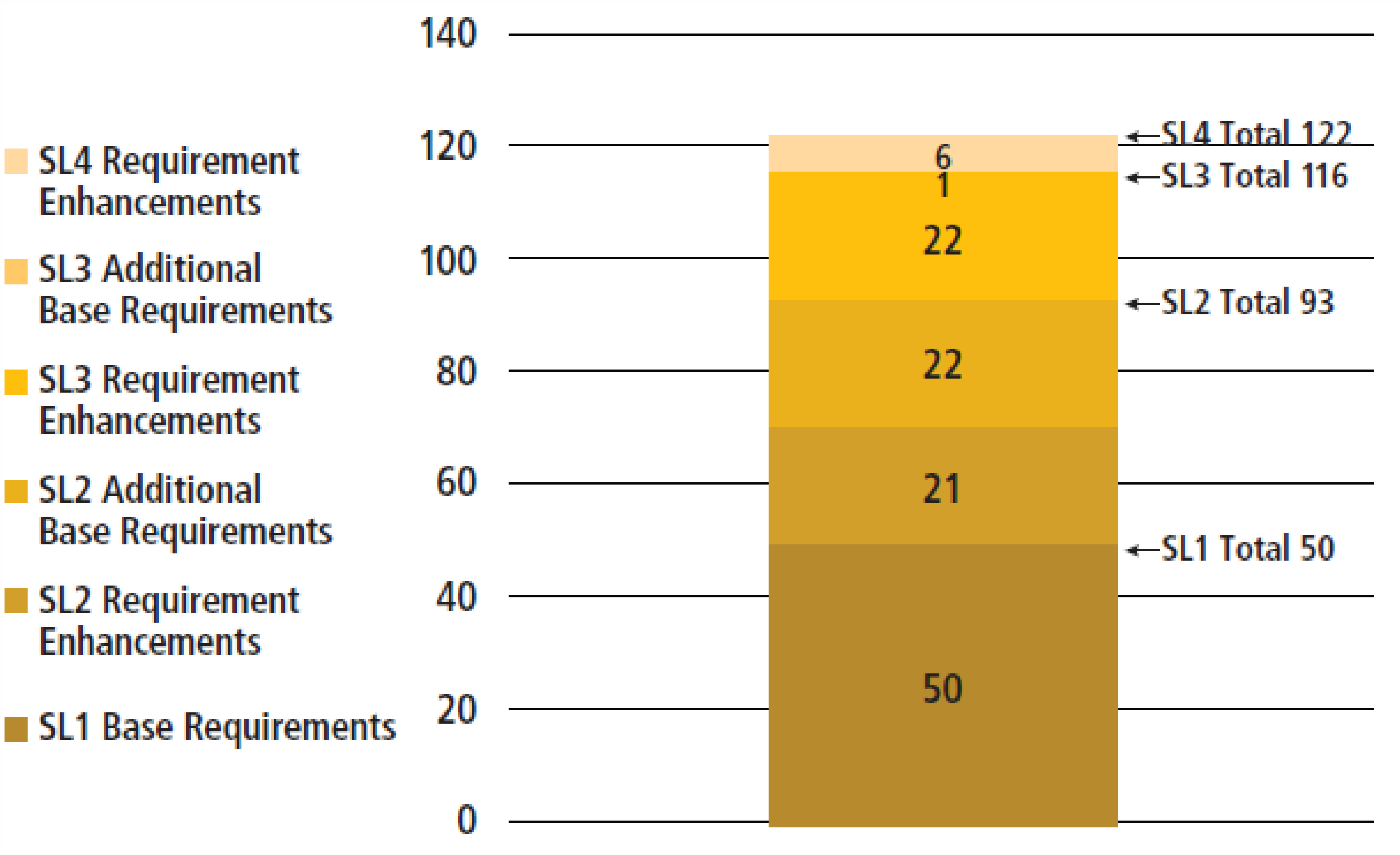
- Defines components that make up systems
  - Host components
  - Network components
  - Embedded devices
  - Application components
- Defines security capabilities of components through requirements
  - Organized by foundational requirements
- Adds additional requirements as capability security level increases
  - Requirement enhancements to strengthen base requirements
  - Additional base requirements

Security level structure



ISASecure®

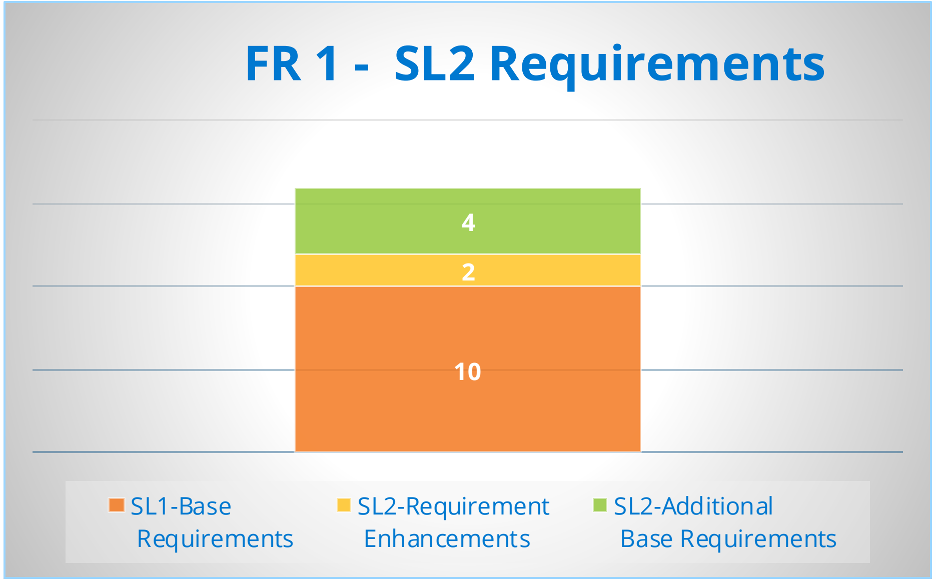
Requirements and security levels



Review requirements added by SL2

- For each foundational requirement
  - Review added requirement enhancements
    - How it strengthens the base requirement
  - Review added base requirements
    - Resulting increased security strength of a component

FR 1 - Identification and authentication



- 10 base requirements
- SL2 adds:
  - 2 requirement enhancements
  - 4 additional base requirements

SL2 adds to identification and authentication

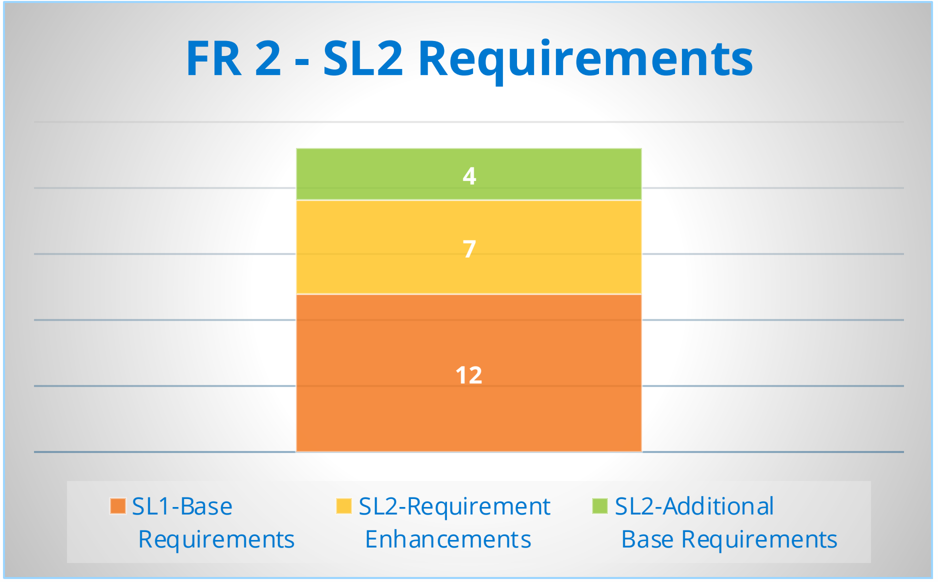
SL2 Requirement Enhancements (RE)

- CR 1.1 RE 1 Unique human user identification and authentication
- NDR 1.6 RE 1 Unique identification and authentication of wireless users and devices

SL2 Additional Base Requirements

- CR 1.2 Software process and device identification and authentication
- CR 1.8 Usage of public key infrastructure certificates
- CR 1.9 Strength of public key-based authentication
- CR 1.14 Strength of symmetric key based authentication

FR 2 – Use control



- 12 base requirements
- SL2 adds:
  - 7 requirement enhancements
  - 4 additional base requirements

SL2 adds to use control

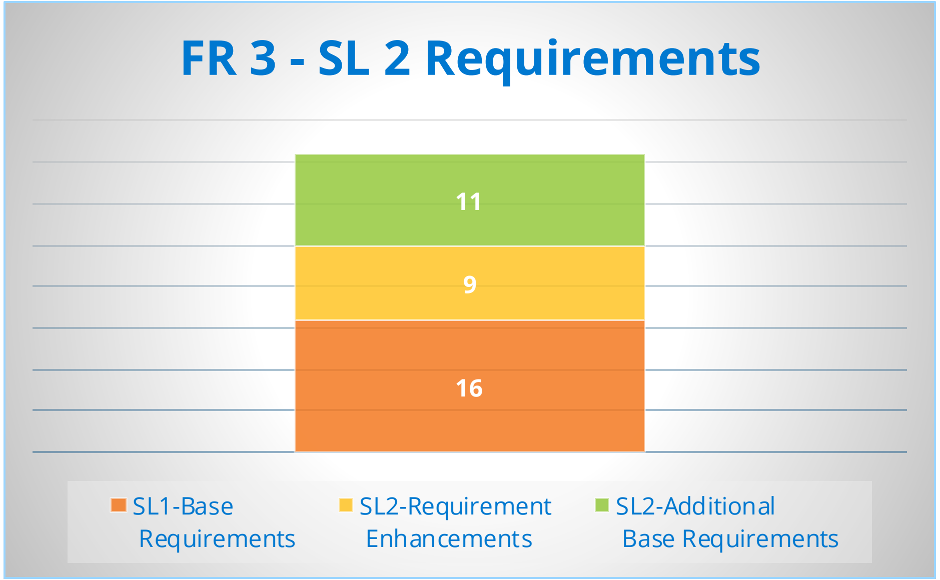
SL2 Requirement Enhancements (RE)

- CR 2.1 RE 1 Authorization enforcement for all users (humans, software processes and devices)
- CR 2.1 RE 2 Permission mapping to roles
- SAR 2.4 RE 1 Mobile code authenticity check
- EDR 2.4 RE 1 Mobile code authenticity check
- HDR 2.4 RE 1 Mobile code authenticity check
- NDR 2.4 RE 1 Mobile code authenticity check
- CR 2.11 RE 1 Time synchronization

SL2 Additional Base Requirements

- CR 2.6 Remote session termination
- EDR 2.13 Use of physical diagnostic and test interfaces
- HDR 2.13 Use of physical diagnostic and test interfaces
- ENDR 2.13 Use of physical diagnostic and test interfaces

FR 3 – System integrity



- 16 base requirements
- SL2 adds:
  - 9 requirement enhancements
  - 11 additional base requirements

SL2 adds to system integrity

SL2 Requirement Enhancements (RE)

- CR 3.1 RE 1 Communication authentication
- HDR 3.2 RE 1 Report version of code protection
- CR 3.4 RE 1 Authenticity of software and information
- EDR 3.10 RE 1 Update authenticity and integrity
- HDR 3.10 RE 1 Update authenticity and integrity
- NDR 3.10 RE 1 Update authenticity and integrity

SL2 Requirement Enhancements (RE)

- EDR 3.14 RE 1 Authenticity of the boot process
- HDR 3.14 RE 1 Authenticity of the boot process
- NDR 3.14 RE 1 Authenticity of the boot process

SL2 adds to system integrity

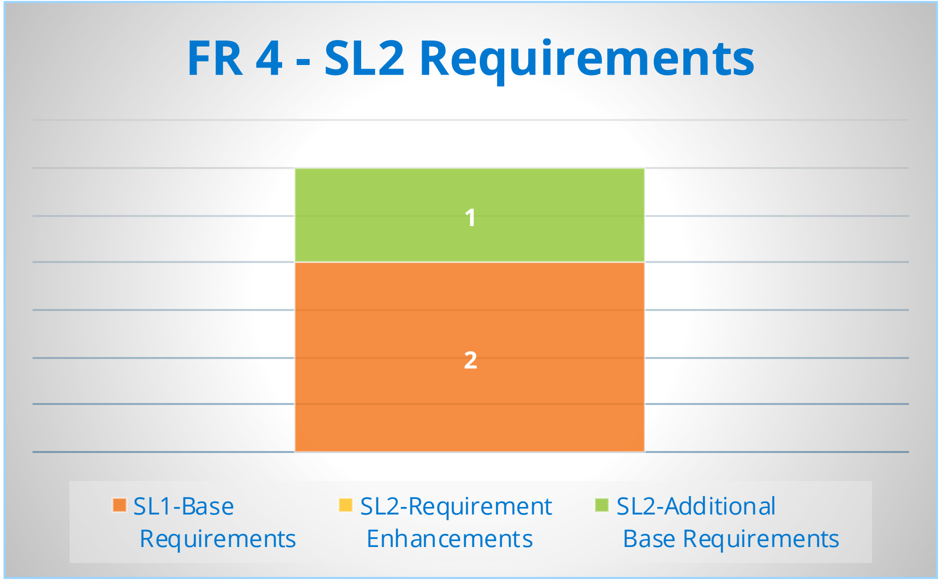
SL2 Additional Base Requirements

- CR 3.8 Session integrity
- CR 3.9 Protection of audit information
- EDR 3.11 Physical tamper resistance and detection
- HDR 3.11 Physical tamper resistance and detection
- NDR 3.11 Physical tamper resistance and detection

SL2 Additional Base Requirements

- EDR 3.12 Provisioning product supplier roots of trust
- HDR 3.12 Provisioning product supplier roots of trust
- NDR 3.12 Provisioning product supplier roots of trust
- EDR 3.13 Provisioning asset owner roots of trust
- HDR 3.13 Provisioning asset owner roots of trust
- NDR 3.13 Provisioning asset owner roots of trust

FR 4 – Data confidentiality



- 2 base requirements
- SL2 adds:
  - 0 requirement enhancements
  - 1 additional base requirements

SL2 adds to data confidentiality

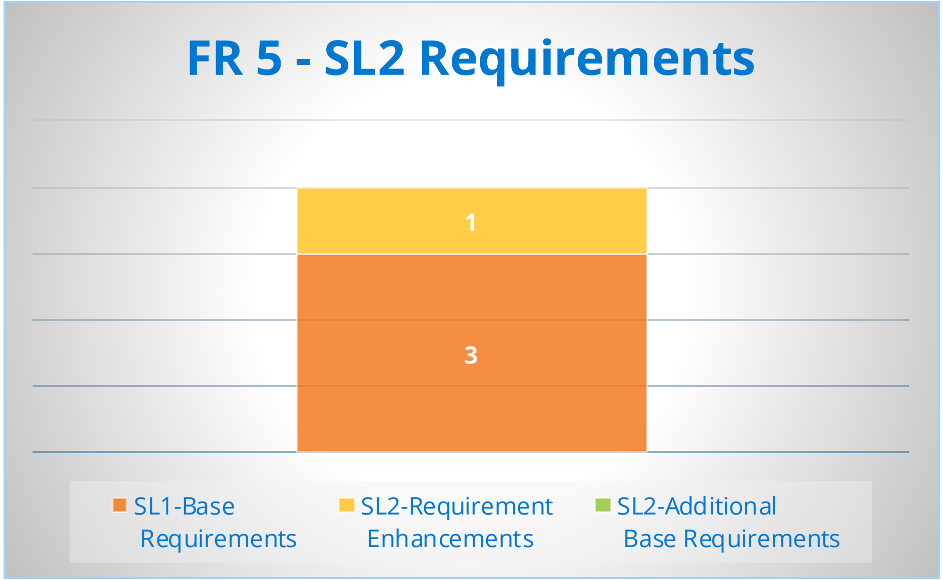
SL2 Requirement Enhancements (RE)

- None

SL2 Additional Base Requirements

- CR 4.2 Information persistence

FR 5 – Restricted data flow



- 3 base requirements
- SL2 adds:
  - 1 requirement enhancement
  - 0 additional base requirements

SL2 adds to restricted data flow

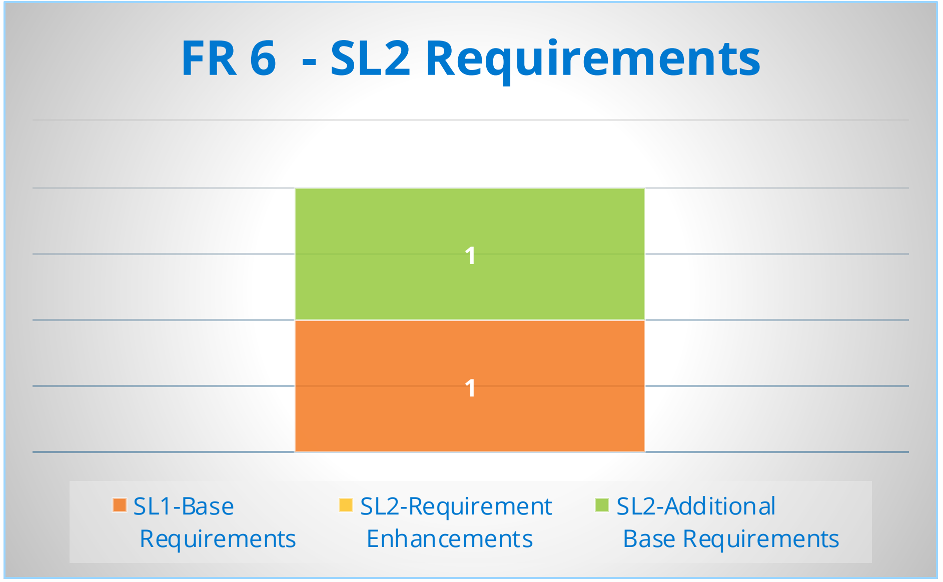
SL2 Requirement Enhancements (RE)

- NDR 5.2 RE 1 Deny all, permit by exception

SL2 Additional Base Requirements

- None

FR 6 – Timely response to events



- 1 base requirements
- SL2 adds:
  - 0 requirement enhancements
  - 1 additional base requirements

SL2 adds to timely response to events

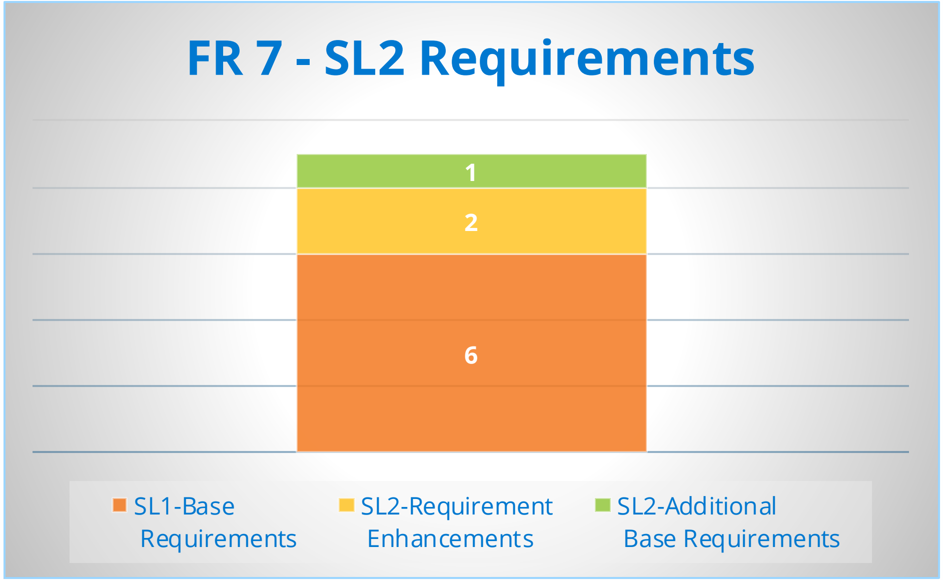
SL2 Requirement Enhancements (RE)

- None

SL2 Additional Base Requirements

- CR 6.2 Continuous monitoring

FR 7 – Resource availability



- 6 base requirements
- SL2 adds:
  - 2 requirement enhancements
  - 1 additional base requirement

SL2 adds to resource availability

SL2 Requirement Enhancements (RE)

- CR 7.1 RE 1 Manage communication load from component
- CR 7.3 RE 1 Backup integrity verification

SL2 Additional Base Requirements

- CR 7.8 Control system component inventory

Summary of added SL2 Capabilities

- Individual user identification, authentication, and accountability
- Software process and device identification, authentication, and accountability
- Authenticity checks
  - Adds ability for secure boot of components
- Physical access protection

Asset owner – assurance of conformity to SL2

- Trust product suppliers
- Build organization to determine if products are conformant
- Only procure components certified by an independent conformance body
  - ISASecure – https://www.isasecure.org

Product supplier – conformity to SL2

- Certify your products using an independent conformance body
  - ISASecure – https://www.isasecure.org
- Examples of components that can be certified can be found at:
  - What-Products-are-Certifiable-with-ISASecure.pdf

Want to know more?

- Read the ISASecure whitepaper titled “The Case for ISA/IEC 62443 Security Level 2 as a Minimum for COTS Components”
  - The-Case-for-ISA-IEC-62443-Security-Level-2-as-a-Minimum-FINAL.pdf

Questions