Applying the Global Automation Standard IEC 62443 to protect against cyber threats

Dr. William Goble,
Principal Engineer, Co-Founder
exida

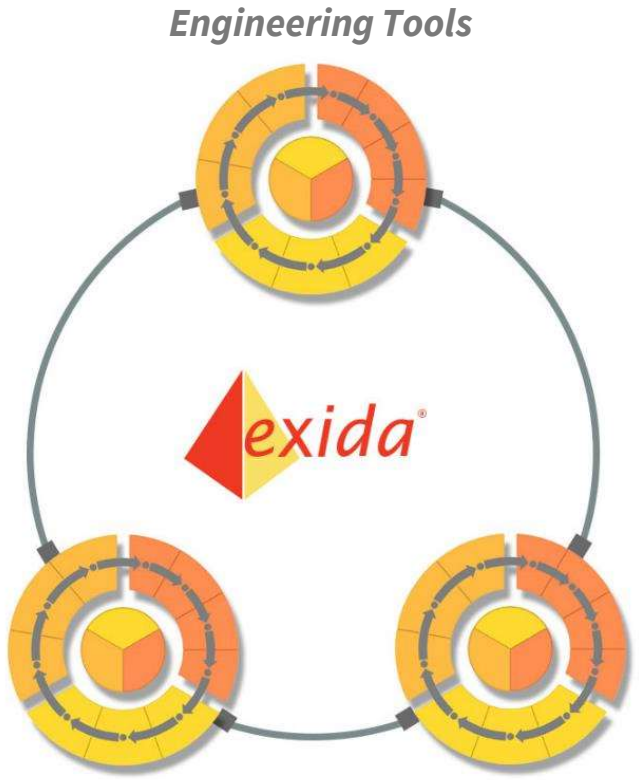
Dr. William Goble
Principal Engineer, Co-Founder
exida

Founded in 1999 by several of the world's top reliability and safety experts, professionals around the world turn to exida for help and guidance related to **functional safety**, **alarm management**, and **ISA/IEC-62443** based **ICS Cybersecurity** services.

exida . . . A Customer Focused Company

exida helps our customers achieve safe, reliable, and secure automation solutions through:

- Powerful engineering tools that efficiently deliver technically correct results
- Thorough certification and assessment schemes that achieve compliance through a pragmatic approach
- Comprehensive system lifecycle services that deploy experts to solve your toughest problems



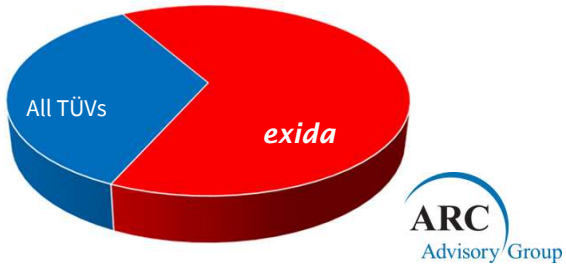
exida Certification

exida is the industry leader in the certification of personnel, products, systems, and processes to the following international standards and guidelines:

- IEC 61508 Certification
- IEC 61511 Certification
- ISO 26262 Certification and Tool Qualification
- IEC62443 Cyber Security Certification
- Machinery Safety Certification (IEC 62061, ISO 13849)
- Certified Functional Safety Expert (CFSE) - Personnel Certification Program

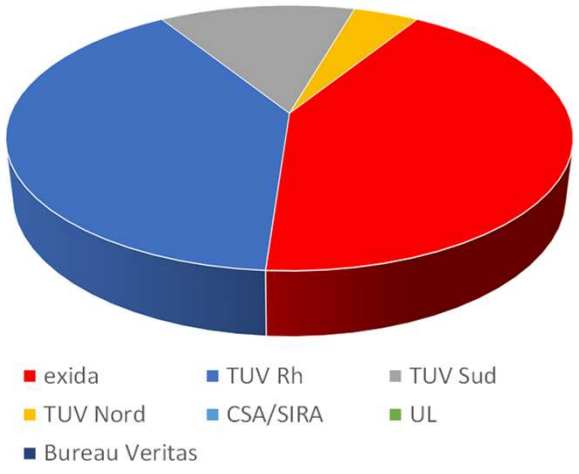
exida - Global Leader in Functional Safety Certification

All Safety Device Certifications
2004 - 2014



An ARC Market Report from 2015 showed ***exida*** was the global leader in safety device certifications.

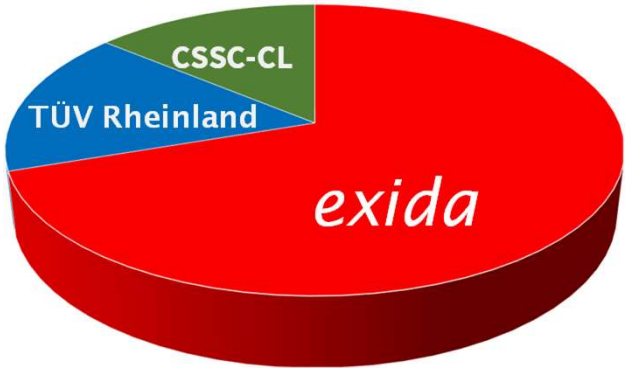
Safety Logic Solver Certifications



Even in the Logic Solver category where the first certifications were done in 1982 by TÜV Product Service (now TÜV Süd), ***exida*** has overcome a twenty year head start to become the leader.

exida - Global Leader in Automation Cybersecurity Certification

exida has pioneered automation cybersecurity and remains the clear world's leader in automation cybersecurity certification.



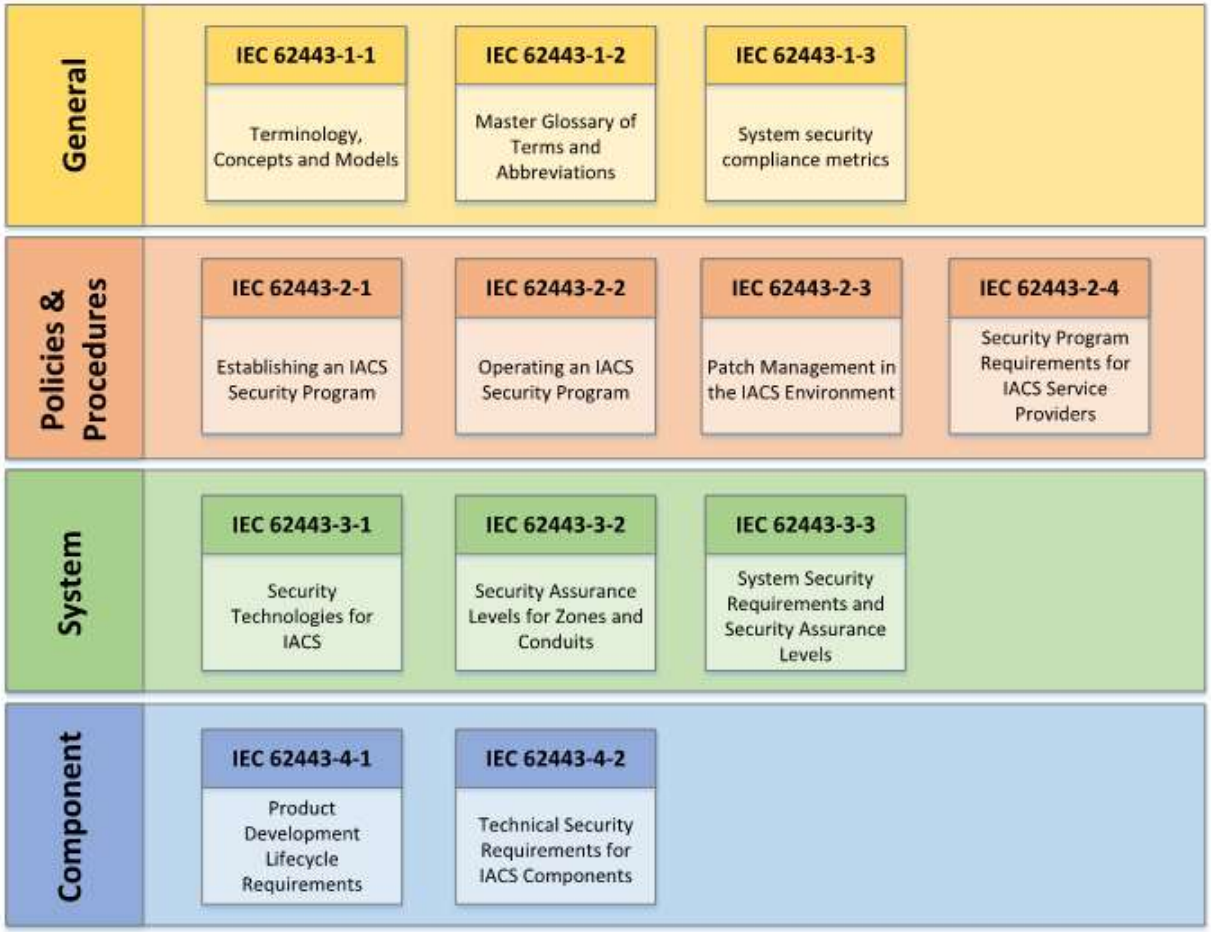
Based on a certificate count from the ISCI website.

Agenda:

1. IEC 62443 Standards
2. IEC 62443 Requirements Overview
3. IEC 62443 Certification
   - Certification Types
   - Assessment Steps

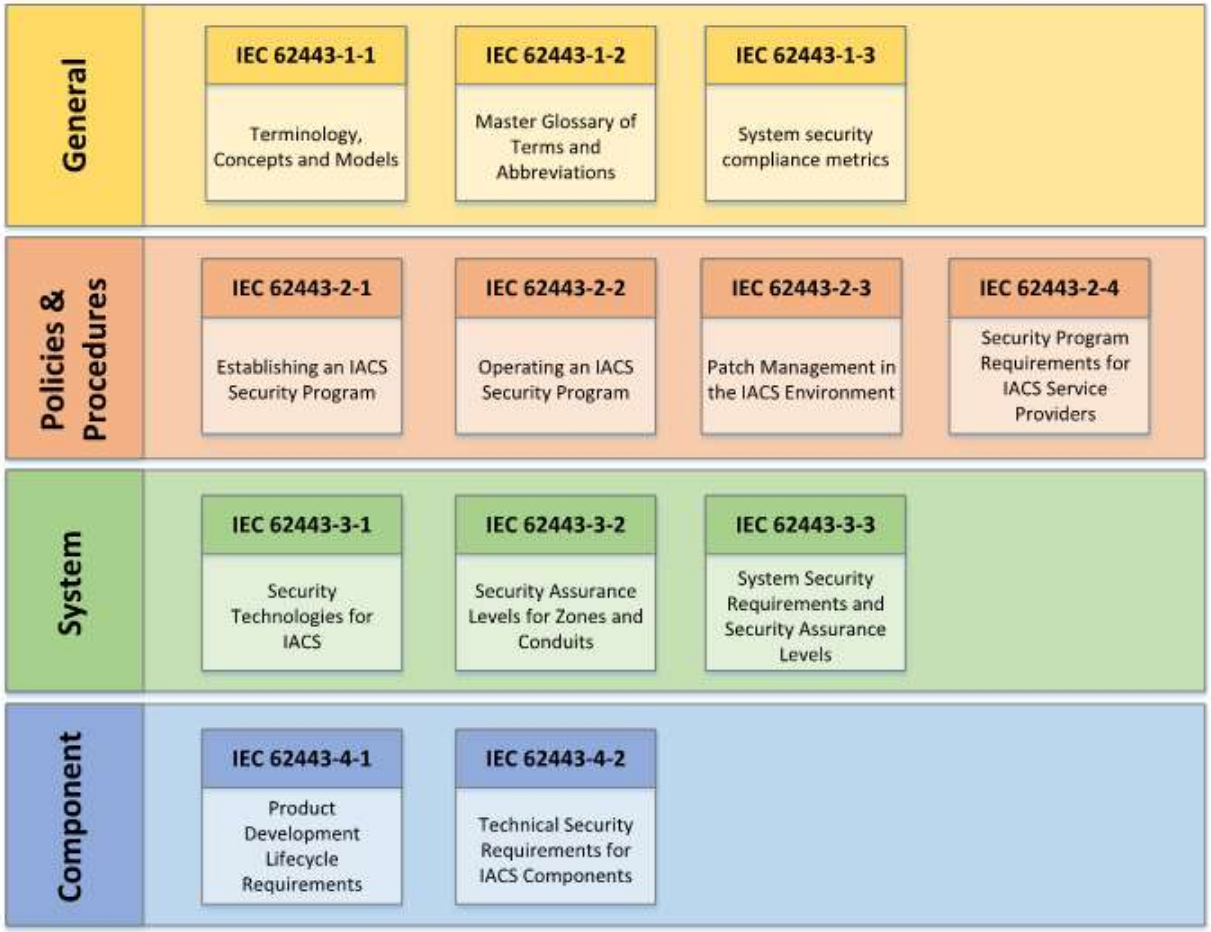
IEC 62443 Standards Organization

Unlike older standards (e.g. IEC 61508 functional safety) which covered everything in one document, ISA/IEC 62443 was broken up into multiple documents. This allows faster release and updating, something important for the fast moving field of cybersecurity. IEC 62443 standards were based on the ISA 99 series.



IEC 62443 Standards Organization

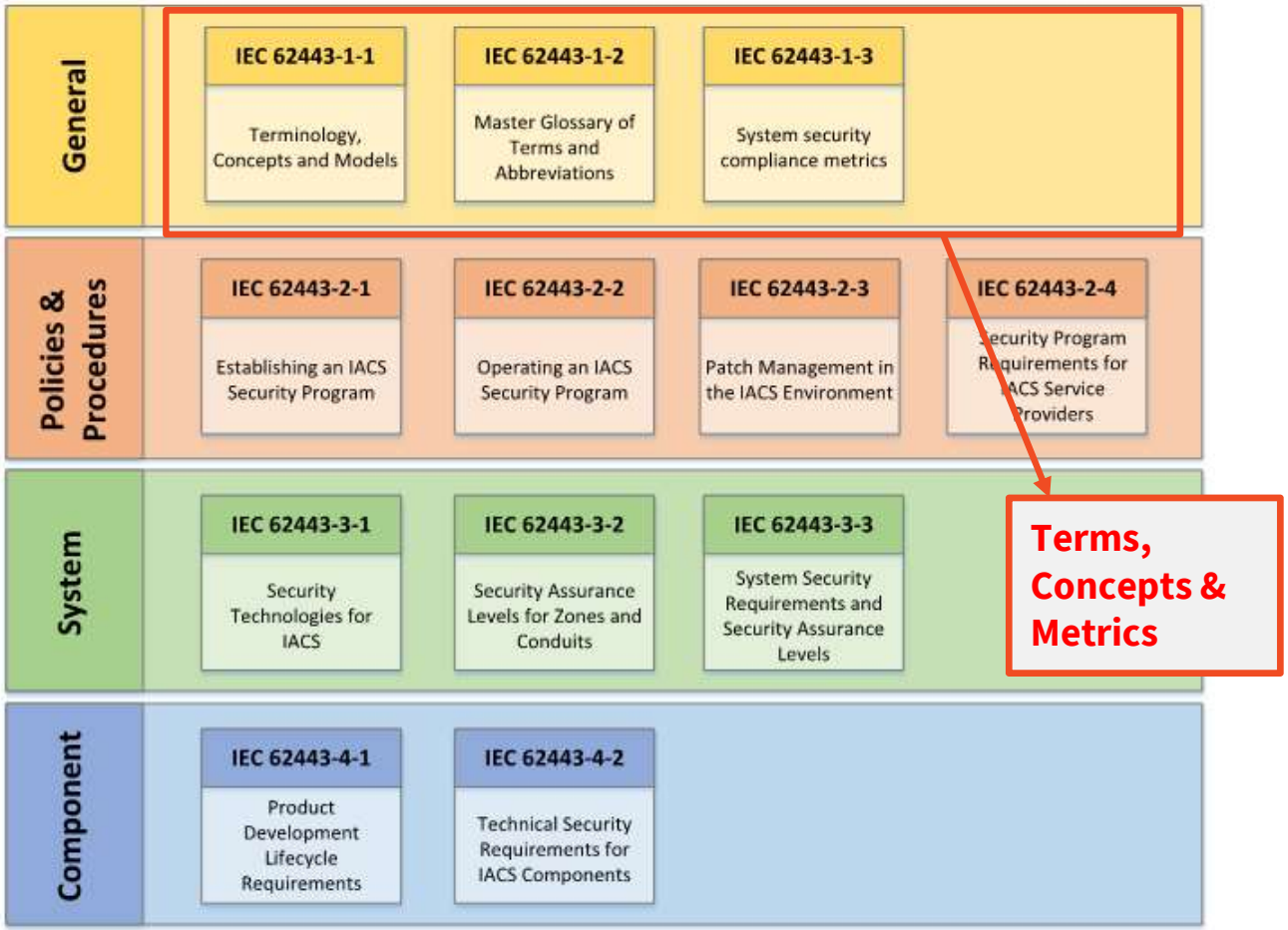
The IEC 62443 series of standards are based on the ISA S99 standards which began development in 2001. Many hours of thought have gone into these documents.



IEC 62443 Standards Organization

IEC 62443 is focused on Automation Systems (Operational Technology – OT) rather than Information Technology - IT.

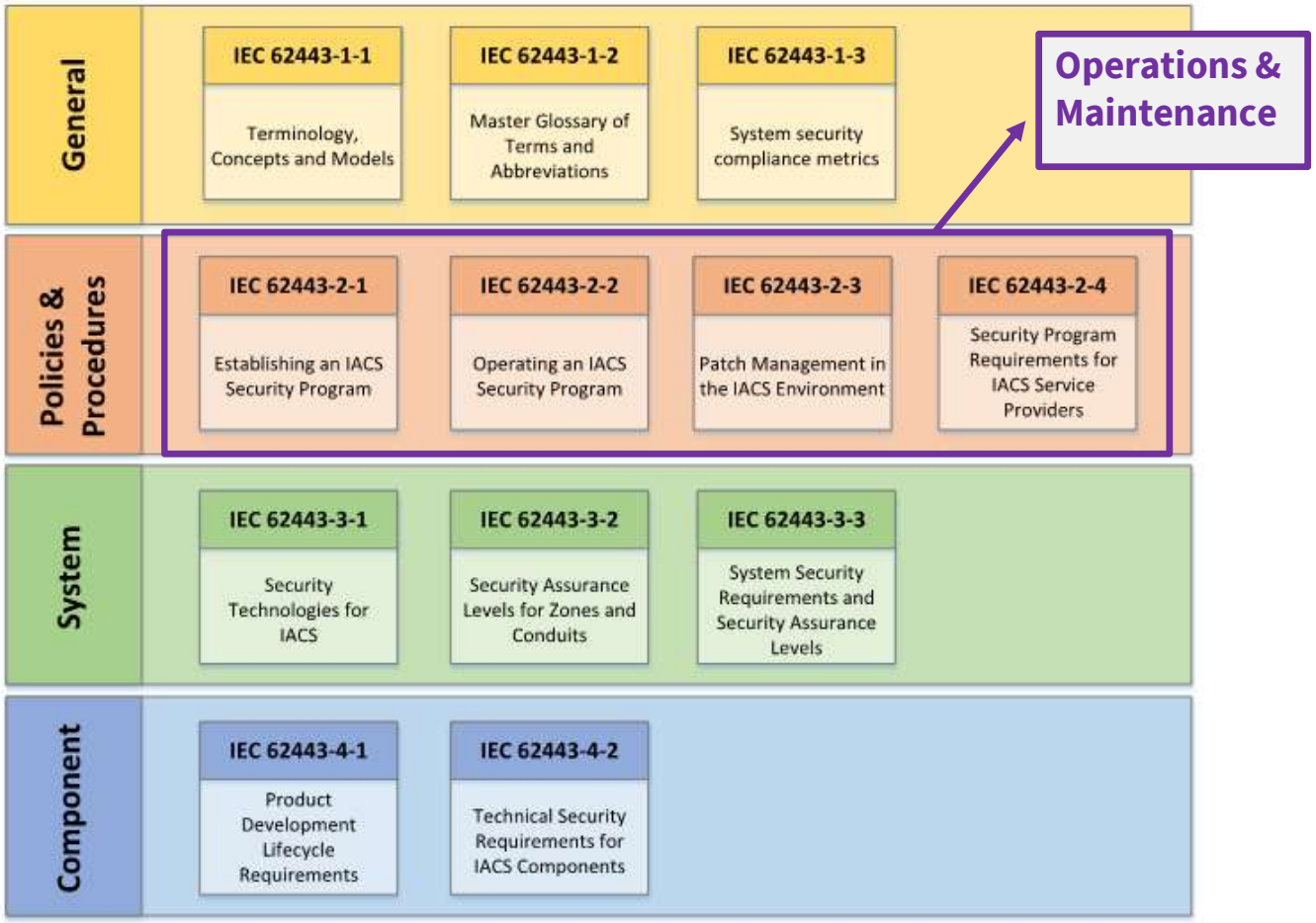
The “-1” series covers terms, concepts, and metrics.



IEC 62443 Organization

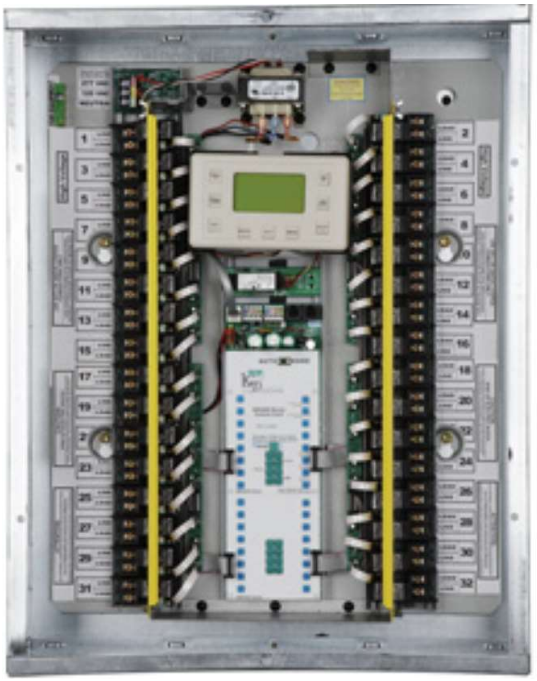
IEC 62443 is focused on Automation Systems (Operational Technology – OT) rather than Information Technology - IT.

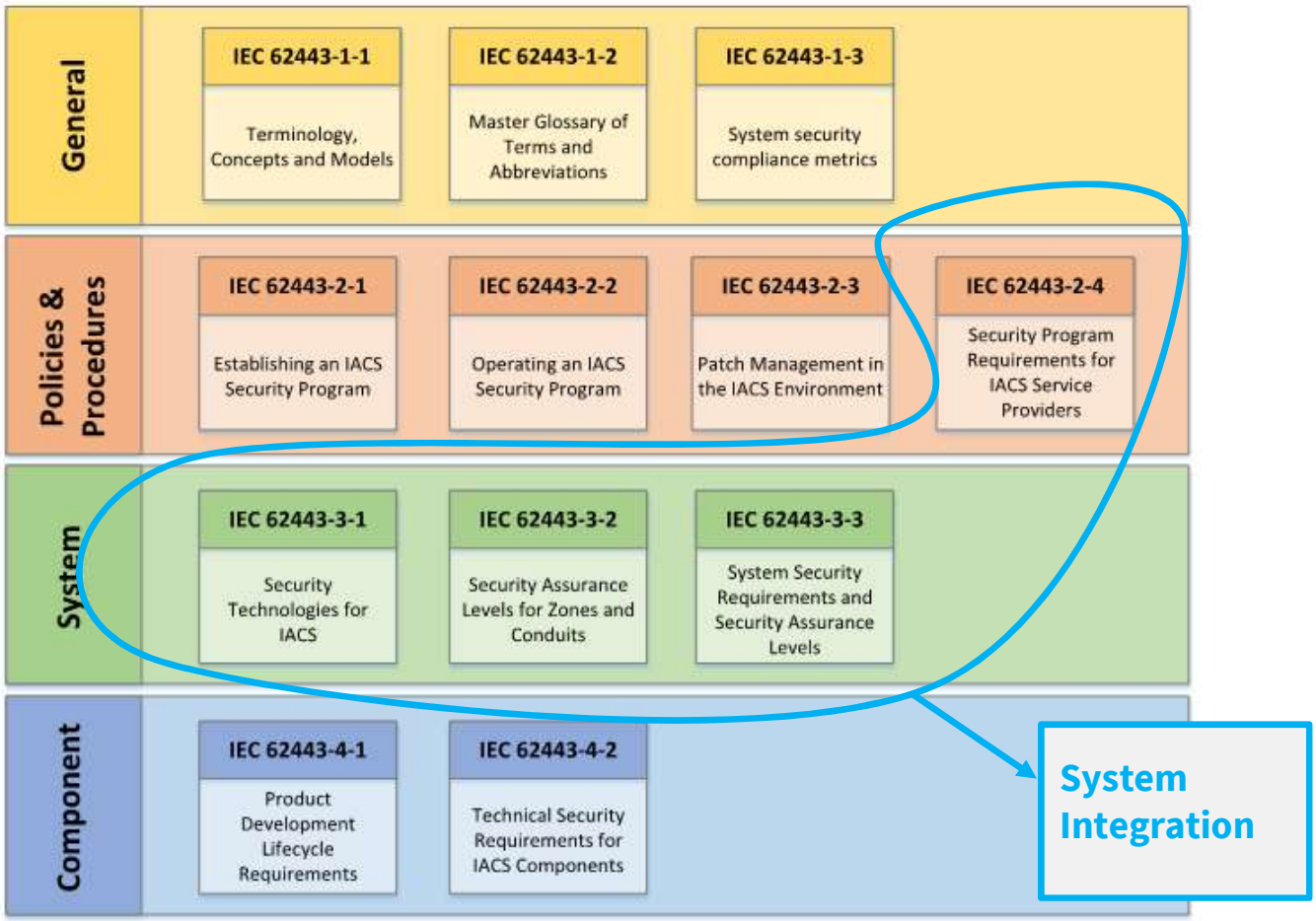
The “-2” series covers operations and maintenance.



IEC 62443 Organization

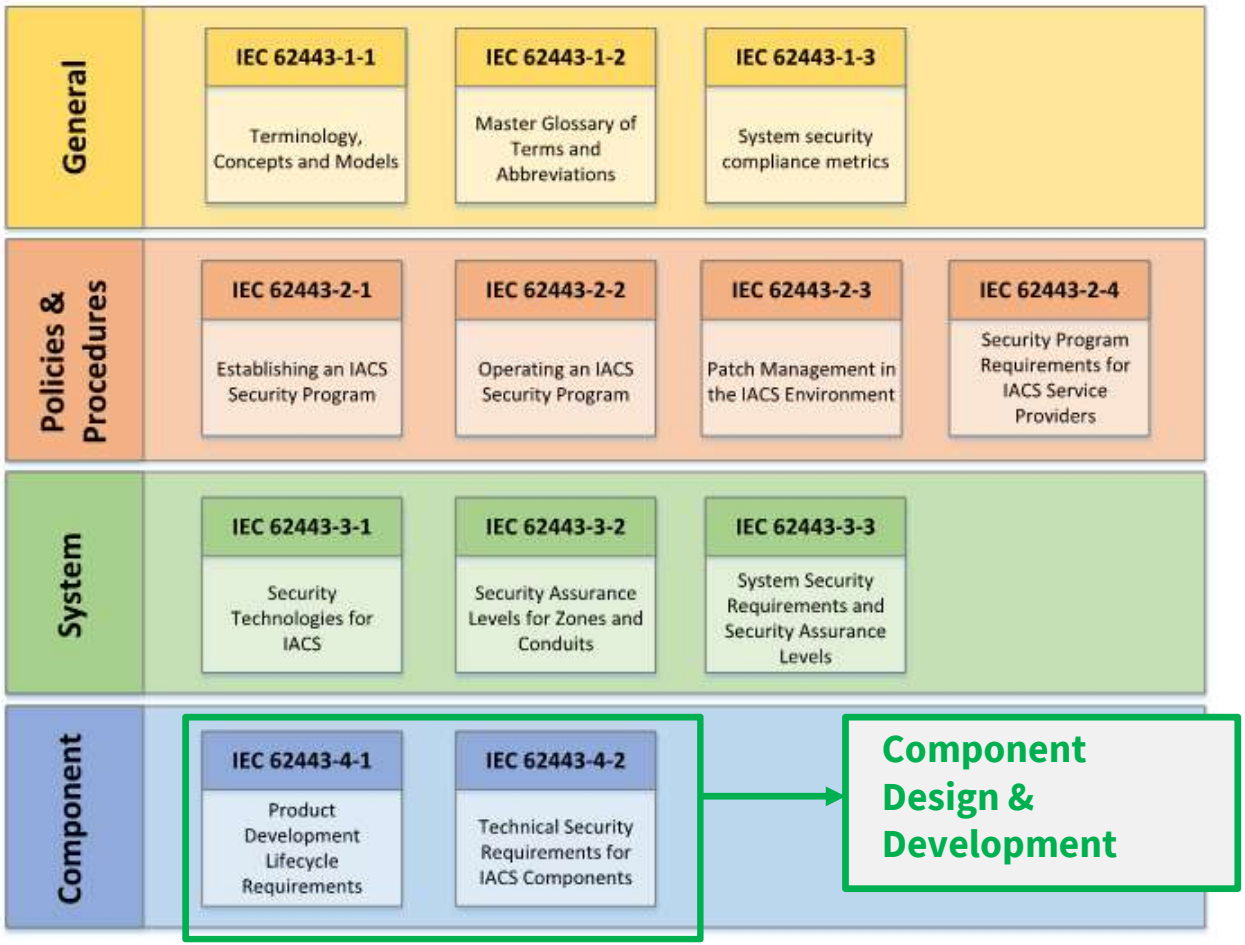
Systems – both OEM and Bespoke Integrations are the focus of the “-3” series.





ISA/IEC 62443 Organization

Products (devices sold and used by themselves) such as switches, firewalls, dedicated controllers, etc. are covered the in the “-4” series.

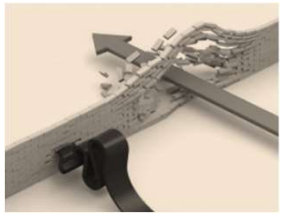


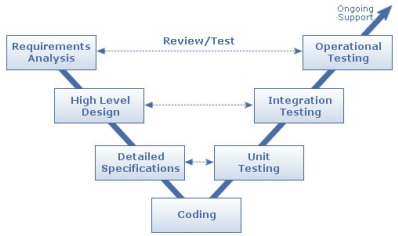
IEC 62443 Security Levels

Security Level	Skills	Motivation	Means	Resources
SL1 - Staff	No Attack Skills	Mistakes	Non-intentional	Individual
SL2 – Low Level Hacker	Generic	Low	Simple	Low (Isolated Individuals)
SL3 – Hacker, Terrorist	System Specific	Moderate	Sophisticated (attack)	Moderate (Hacker Groups)
SL4 Nation State	System Specific	High	Sophisticated (campaign)	Extended (Multi-disciplinary Teams)

IEC 62443 Requirements Overview

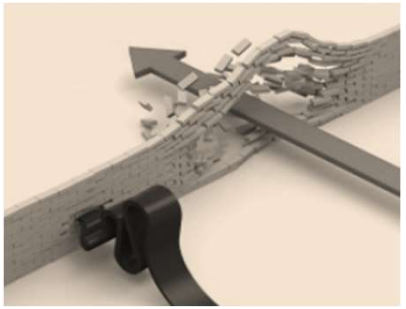
- **Network Robustness Testing** must be done to show safe, correct operation and identify any Cybersecurity Susceptibilities
- Products and Systems must have **Cybersecurity Protection Mechanisms**
- **Engineering Processes** must be defined and documented with sufficient steps to reduce design errors that impact cybersecurity strength



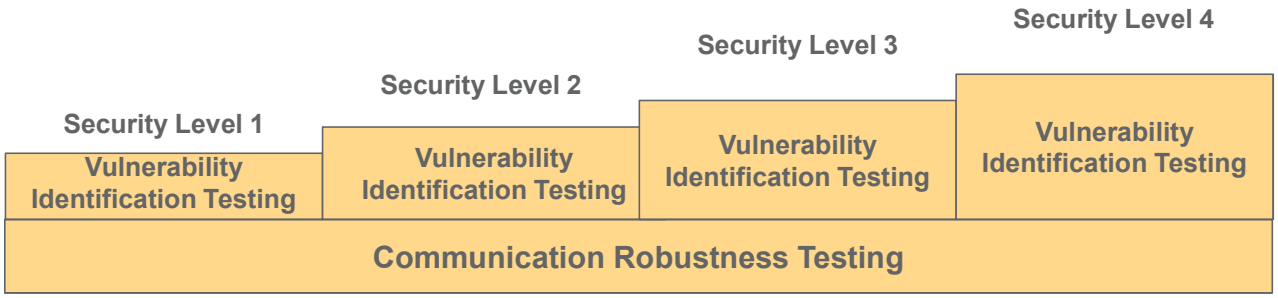


IEC 62443 Requirements – Network Robustness Testing

– **Network Robustness Testing** must be done to show safe, correct operation and identify any Cybersecurity Susceptibilities

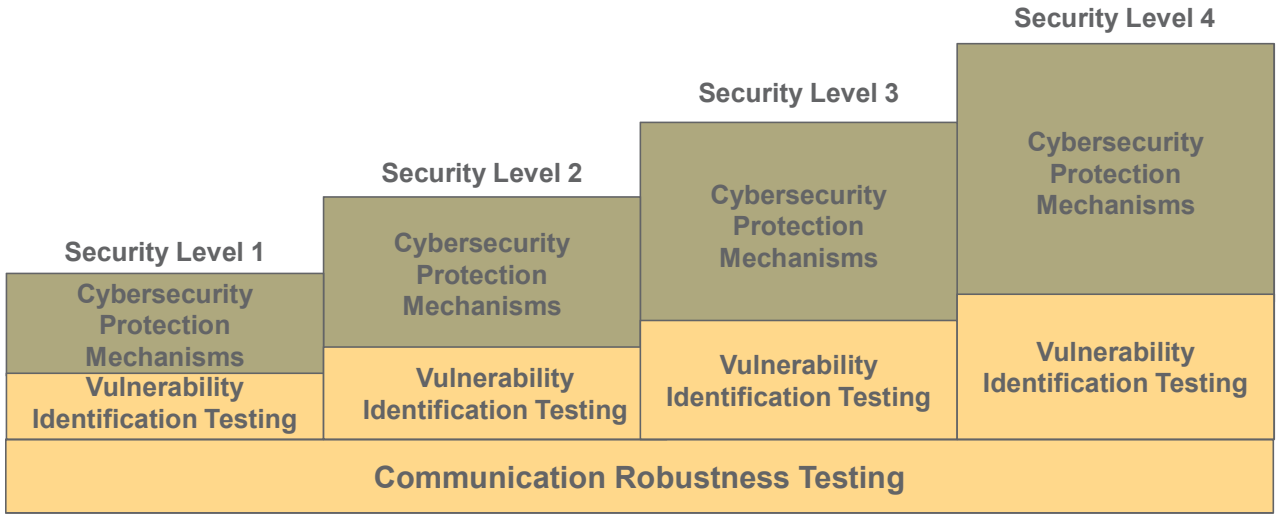


- **Fuzz Testing**
- **Penetration Testing**
- **Malformed Packet Testing**
- **Storm Testing**
- **…**



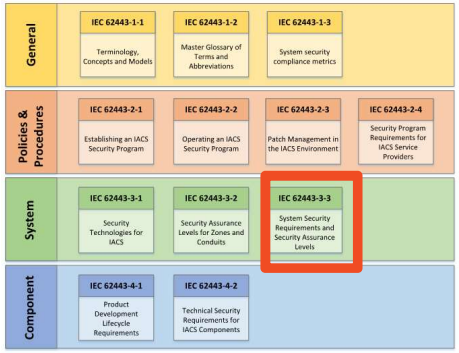
IEC 62443 Requirements – Cybersecurity Protection Mechanisms

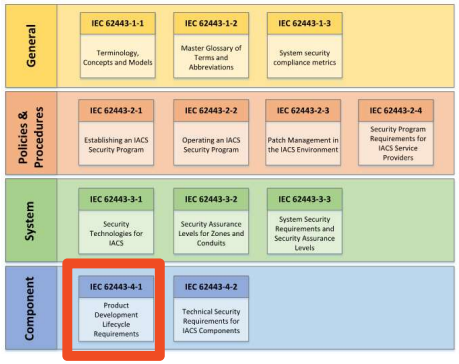
– Products and Systems must have **Cybersecurity Protection Mechanisms**



Cybersecurity Protection Mechanisms

- System Protection Mechanism Requirements specified by IEC 62443-3-3
- Component Protection Mechanism Requirements specified by IEC 62443-4-2
- Both provide list of requirements per security level. The lists are similar.





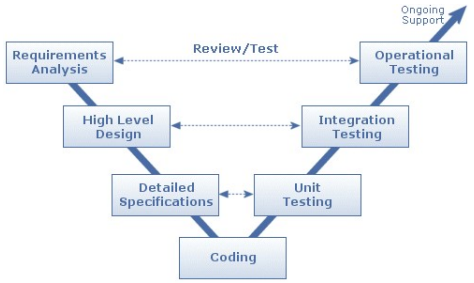
Cybersecurity Protection Mechanisms

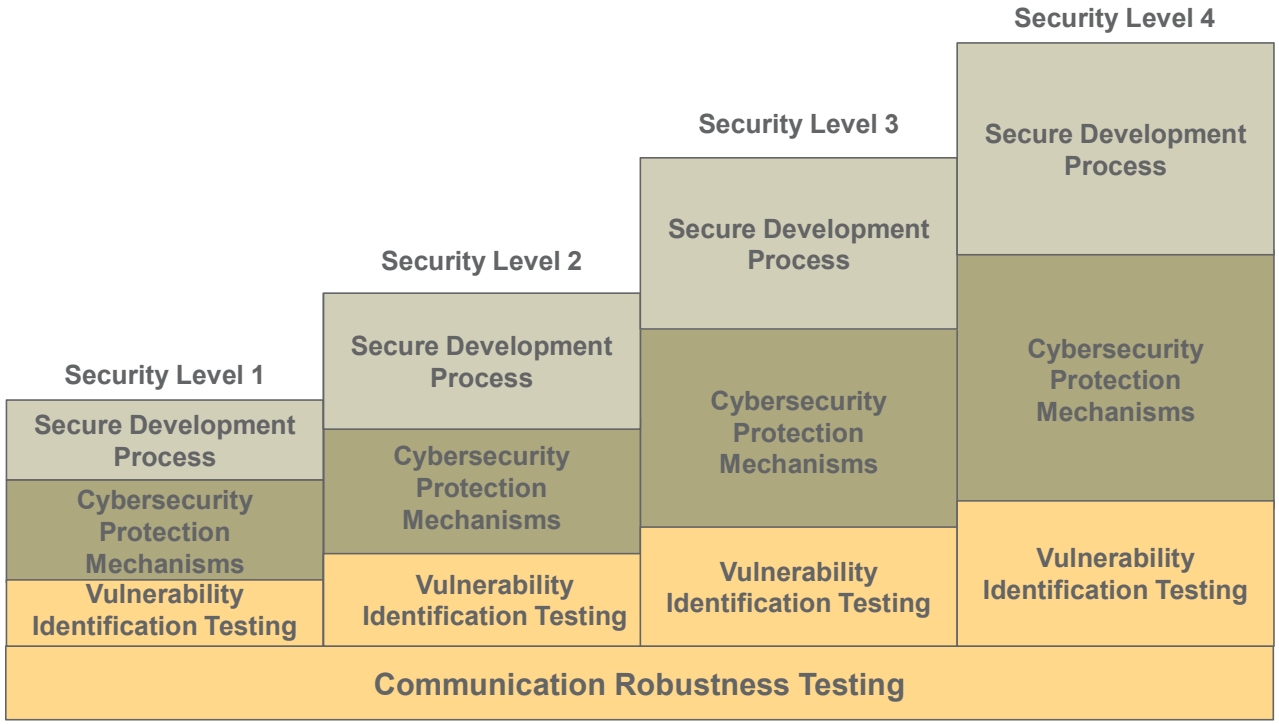
Foundational Requirement	SL-1	SL-2	SL-3	SL-4
FR 1 – Identification and Authentication Control	10	16	22	24
FR-2 Use Control	8	12	21	24
FR-3 System Integrity	5	10	16	19
FR-4 Data Confidentiality	2	4	5	6
FR-5 Restricted Data Flow	4	6	10	11
FR-6 Timely Response To Events	1	2	3	3
FR-7 Resource Availability	7	10	13	13

Example: A product meets all SL-1 requirements, and perhaps some SL-2 or SL-3. That certification will show SL-1.

IEC 62443 Requirements – Engineering Process

– **Engineering Processes** must be defined and documented with sufficient steps to reduce design errors that impact cybersecurity strength





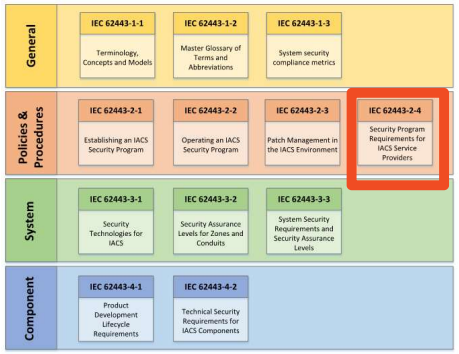
Engineering Process Maturity Levels

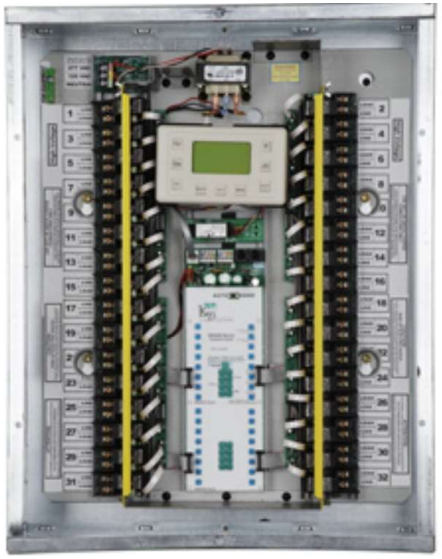
Level	IEC 62443-2-4	Description
1	Initial	Service providers typically perform the service in an ad-hoc and often undocumented (or not fully documented) manner. Requirements for the service are typically specified in a statement of work under contract with the asset owner. As a result, consistency across projects may not be able to be shown.
2	Managed	At this level, the service provider has the capability to manage the delivery and performance of the service according to written policies (including objectives). The service provider also has evidence to show that personnel have the expertise, are trained, and/or are capable of following written procedures to perform the service.
3	Defined (Practiced)	A service at Level 3 is a Level 2 service that the service provider has practiced for an asset owner at least once. The performance of a Level 3 service can be shown to be repeatable across the service provider's organization. Level 3 services may be tailored for individual projects based upon the contract and statement of work from the asset owner.
4	Improving	Using suitable process metrics, service providers control the effectiveness and performance of the service and demonstrate continuous improvement in these areas, such as more effective procedures or the installation of system capabilities with higher security levels (see IEC 62443-3-3). This results in a security program that improves the service through technological/procedural/management changes. See IEC 62443-1-3 for a discussion of metrics.

Engineering Processes - IEC 62443-2-4

System Integration Security Development Process

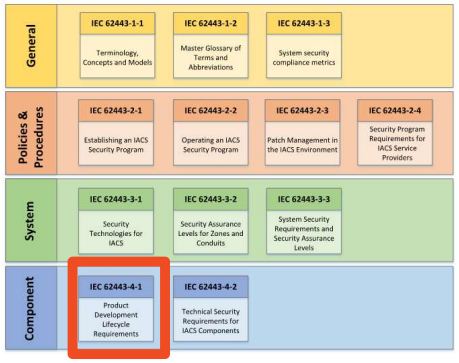
- Systems Level engineering process for Systems (OEM or Bespoke Integrators).
- Procedures
- Documentation Required
- Testing Requirements



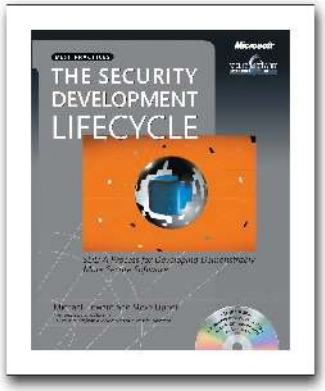


Engineering Processes - IEC 62443-4-1

Foundation in Microsoft Security Development Lifecycle

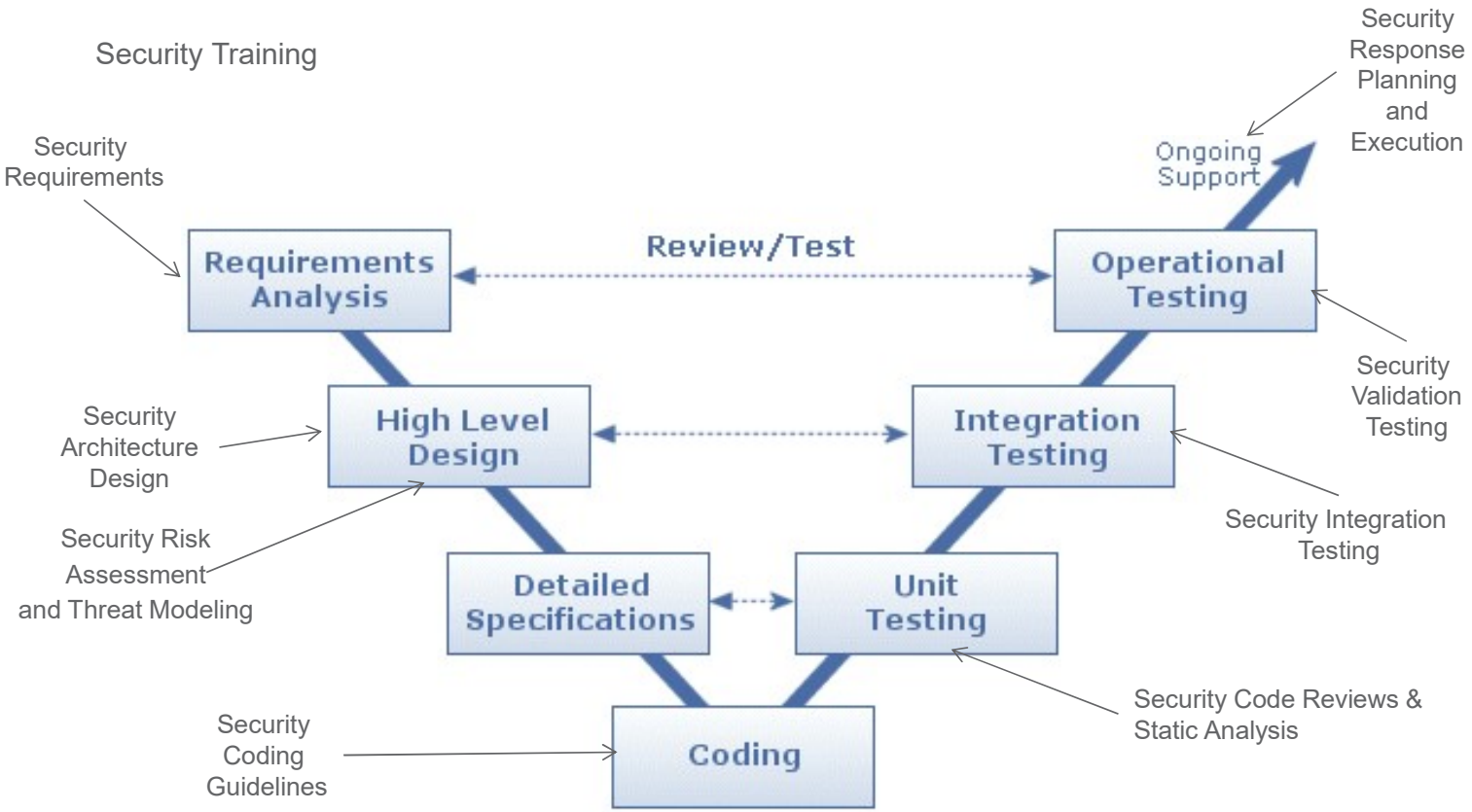


- Software engineering for security has also been developed over many years based on common software engineering principles with specific additions.
- Microsoft identified several key objectives:
  - Reduce the number of security vulnerabilities
  - Reduce the severity of remaining vulnerabilities
  - Implement strong software engineering procedures
  - Use design procedures and static analysis tools
    - Eliminate specific well known vulnerabilities



Howard, Michael, and Steve Lipner. The Security Development Lifecycle: SDL, a Process for Developing Demonstrably More Secure Software. Redmond, WA: Microsoft, 2006. Print.

Engineering Processes



Cybersecurity Process Certification

What is IEC 62443 Certification?

- Third party technical expert attestation of compliance against IEC 62443 requirements from three categories:
  - Detailed Analysis of engineering processes to determine Systematic Capability and Cybersecurity Strength
  - Detailed Analysis of product design and validation testing to show cybersecurity protection mechanisms in the product
  - Network Testing to show safe, correct operation and Cybersecurity Susceptibility

Who does Cybersecurity Certification?

OEM Self-Declaration?

- High confidence comes from certification by an impartial organization.

Any Third Party?

- High credibility comes when the certification organization has strong technical depth to understand not only the requirements but **why they exist.**

Certificate / Report – complete and publicly available

- Work done should be publicly available in a report

Accreditation of Third Party?

Strong Established Infrastructure

- An **Accreditation Body (AB)** will audit and accredit a **Certification Body (CB)**.
- Certification Bodies must operate any product certification program under ISO 17065 requirements.

ACLASS

CERTIFICATE OF ACCREDITATION

ANSI-ASQ National Accreditation Board/ACLASS
500 Montgomery Street, Suite 625, Alexandria, VA 22314, 877-344-3044

This is to certify that

exida.com, LLC

CERTIFICATE of ACCREDITATION
PRODUCT CERTIFICATION

The American National Standards Institute hereby affirms that

exida.com L.L.C
64 North Main Street, Sellersville, PA 18960, USA

ACCREDITATION ID# 1004

meets the ANSI accreditation program requirements and those set forth in
ISO/IEC Guide 65: 1996 General Requirements for Bodies Operating Product Certification Systems
EDSA-100 ISA Security Compliance Institute - Embedded Device Security Assurance - ISASecure certification scheme Version 1.1 June 2010

for programs within the following

SCOPE OF ACCREDITATION

GRANTED 2011-11-30
ISASecure Embedded Device Security Assurance (EDSA)

ANSI
ANSI Accredited Program
PRODUCT CERTIFICATION

2013-12-01

International Recognition

exida is fully accredited per ANSI, the United States IEC liaison, as a Certification Body for Cybersecurity and Functional Safety

ANSI is a member of the International Accreditation Forum (IAF). Most countries of the world are signatories of the IAF Multilateral Recognition Arrangement (MLA) which assures global certificate acceptance.

CERTIFICATE of ACCREDITATION
PRODUCT CERTIFICATION

The American National Standards Institute hereby affirms that

exida.com L.L.C.

80 North Main Street, Sellersville, PA 18960, United States

ACCREDITATION ID# 1104

meets the ANSI accreditation program requirements and those set forth in
ISO/IEC 17065:2012 Conformity assessment -- Requirements for Bodies certifying products, processes and service

LIST OF CERTIFICATION SCHEME(S)

ISA SSA (System Security Assurance)
ISA SDLA (Security Development Lifecycle Assurance)
ISA Secure EDSA
IEC 61508- Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
IEC 61511 Functional safety - Safety instrumented systems for the process industry sector
IEC 62061 Industrial networks - Wireless communication network and communication profiles
ISO 26262 Road Vehicles Functional Safety Package
ISO 13849 Safety of Machinery Package
EN 50128/EN 50129 Railway applications. Communication, signaling and processing systems
ESCP - IEC 62443-4-1, 62443-4-2 & 62443-2-4 (INDUSTRIAL NETWORK AND SYSTEM SECURITY)
ESTS exida Security Test Scheme (IEC 62443-4-1, Section 9)

for programs within the following

SCOPE OF ACCREDITATION

(please see page 2)

ANSI VICE PRESIDENT, ACCREDITATION SERVICES

2019-12-01
VALID THROUGH

ANSI ACCREDITED

ISA Security Compliance Institute created the first cybersecurity certification scheme before IEC 62443 existed

- exida has been directly involved
- exida was the first globally accredited cybersecurity Certification Body (CB)
- exida has completed more cybersecurity certifications than any other CB
- exida is a supporter of the ISCI Scheme

Copyright ISCI, used with permission

Who does IACS cybersecurity certification?

Several CBs now offer cybersecurity certification

Standard	Scheme	Scheme Owner	Accredited Certification Bodies (CB)
ISA S99	Original ISASecure	ISA Security Compliance Institute (ISCI)	exida, CSSC-CL, TÜV Rheinland
IEC 62443	ISASecure	ISCI	exida, CSSC-CL, TÜV Rheinland
IEC 62443	CB Scheme	CB	exida, TÜV Rheinland, TÜV Sud, SGS-TÜV Saar, TÜV Nord

Cybersecurity Certification Categories

IEC 62443 cybersecurity certification programs in four categories:

- **Process Certification**

Assessment of the engineering and test process used to design and integrate devices and networks

- **Device Certification**

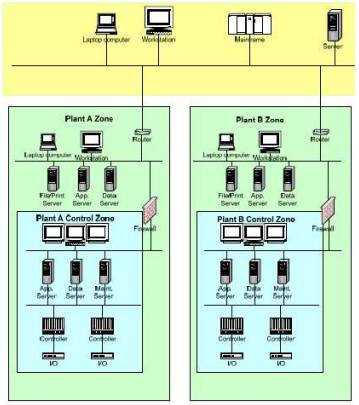
Assessment focused on a device, e.g. a PLC, Safety PLC, a Gateway, a Firewall, or DCS controller

- **System Certification**

Assessment of a system including multiple devices and networks

- **Personnel Certification**

Assessment of a system including multiple devices and networks



Cybersecurity Certification Process

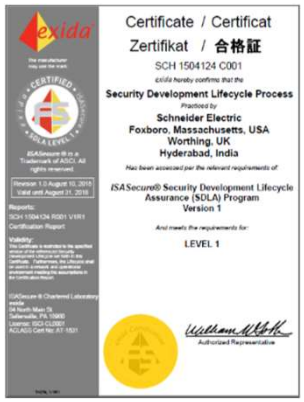
Any Cybersecurity Certification Scheme uses one or more of the following three process steps:

1. Audit the development process used to create the product
2. Analyze and test cybersecurity features of the product to determine if they are sufficient.
3. Perform cybersecurity network stress testing to find network vulnerabilities – focus on most effective tests

Security Level equates a minimum set of security features/capability as well as assurances for secure development process and security testing

IEC 62443 Cybersecurity Certification Schemes

Based On	Classification	Program Name	Applicable to
IEC 62443-4-1	Device Process Certification	Security Development Process	OEM New Product Development
IEC 62443-2-4	System Process Certification	System Integrator Process	System Integrator
IEC 62443-4-1, IEC 62443-4-2	Device and Application Certification	Security Device Certification	OEM Product
IEC 62443-2-4, IEC 62443-3-3	OEM System Certification	System Security Certification	OEM System
IEC 62443-2-4, IEC 62443-3-3	Integrated System Certification	Integrated System Certification	Integrated System
IEC 62443-4-1	ISCI SDLA	Security Development Process	OEM New Product Development
IEC 62443-4-1, IEC 62443-4-2	ISCI EDSA	Security Device Certification	OEM Product
IEC 62443-2-4, IEC 62443-3-3	ISCI SSA	System Security Certification	OEM System



exida offers a range of effective cybersecurity certification schemes to meet the needs of many industries. exida supports both the original ISCI schemes and exida schemes based on IEC 62443.

Benefits of IEC 62443 Cybersecurity Certification

Structured, auditable, repeatable approach to evaluating the security of an automation product and the development practices of the manufacturer/integrator against an established benchmark.

End-user

- Easy to specify security needs – security level
- Build security requirement into RFP
- Reduced time in FAT/SAT
- Know security level out of the box
- Better cybersecurity strength
- Provides confidence from independent expert technical assessment

Supplier

- Evaluated once
- Recognition for effort
- Build in security
- Product differentiator
- Reduce support costs
- Enhance credibility
- Break the pen/patch cycle

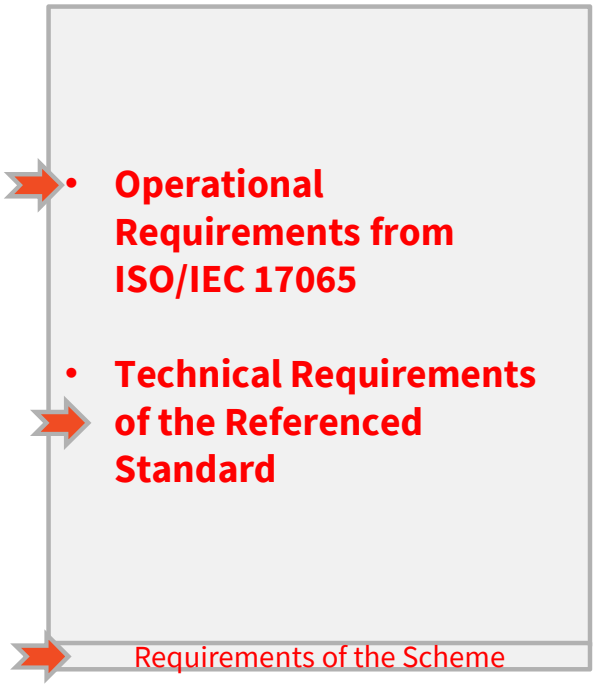
What is a Certification Scheme?

"Scheme" is a word defined in ISO/IEC 17065 which means:
"Certification system related to specified products, to which the same specified requirements, specific rules and procedures apply."

The operational requirements of ISO/IEC 17065 are extensive and exida is audited per those requirements every year by ANSI. However, 17065 has some options.

The chosen options must be defined in the Scheme. Therefore a Scheme should be:

- A list of referenced standards with certification requirements.
- Surveillance Audit required
- Any interpretations of the requirements in the referenced standards
- Any requirements in addition to the referenced standards
- Engineering Change requirements



Other Automation Cybersecurity Standards?

Other Automation Cybersecurity Standards exist. Questions to ask to evaluate one standard / scheme versus another:

1. Is the standard recognized internationally? The IEC standards have strong global recognition.
2. Is the standard supported by several Certification Bodies? Competition between CBs is good for business. Infrastructure has been established for IEC 62443 using several competing CBs.
3. Is the Certification Body specifically accredited for automation cybersecurity? exida is ANSI accredited for cybersecurity.
4. Does the Certification Body have sufficient technical depth? exida has been an active author in IEC 62443, has published a book on IEC 62443, and offers training courses.
5. Does the Certification Body have a reputation for service and support? exida has a strong service ethic and a reputation for support.

Personnel Certification

exida also operates an extensive personnel certification program for both functional safety and cybersecurity.

IEC 62443 cybersecurity exam types:

- Integration Cybersecurity
- Automation Cybersecurity
- Software Development Cybersecurity
- Design, Operate & Maintain: Robotics

wgoble@exida.com