ISASecure webinar

ISASecure Certifications for Smart Buildings Technologies

Presented by Jon Williamson - JCI

Mike Medoff - exida

November 16, 2022

ISASecure®

exida

Johnson Controls

Smart Buildings

Power	HVAC	BMS	Security	Fire	Lighting / Other
Substations	Ventilation	Temperature Control	Video	Panels	Lighting
Microgrid	Chillers	Thermostats	Access Control	Detectors	Shade / Blind
Generators	Air Handlers	Analytics	Intrusion	Suppression	Roof
Power distribution	Purification	Air Quality / Health	Loss Prevention	Smoke	Digital Signage
Arc flash technology			Monitoring	Safety	Conference
Metering			Parking		Emergency
			Elevator / Lift		
			Occupant Health		

Monitoring (Workstations, Mobile, Alerts)

Analytics (Logging, Optimization, AI)

Connectivity (IT networks, Wireless, Mobile, Intranet, Cloud)

Smart Building Benefits

- Efficiency
- Comfort
- Experience
- Health

Smart Buildings need cybersecurity across all systems

Power	HVAC	BMS	Security	Fire	Lighting / Other
Substations	Ventilation	Temperature Control	Video	Panels	Lighting
Microgrid	Chillers	Thermostats	Access Control	Detectors	Shade / Blind
Generators	Air Handlers	Analytics	Intrusion	Monitoring	Digital Signage
Power distribution	Purification	Air Quality / Health	Loss Prevention	Suppression	Conference
Arc flash technology			Monitoring	Smoke	Emergency
Metering			Parking	Safety	
			Elevator / Lift		
			Occupant Health		

BACnet · Microsoft AD · Modbus · ONVIF · MQTT · DALI · LoRa · SIP · zigbee · Z-WAVE · Proprietary · SNMP · KNX · OSDP · M-Bus · http:// · DMX

ASHRAE BACnet® evolution

- 1995 – Initial release
- 2010 – Network Security “addendum G”
- 2019 – BACnet/SC “secure connect”

… regardless of protocol

Building systems utilize a layered architecture

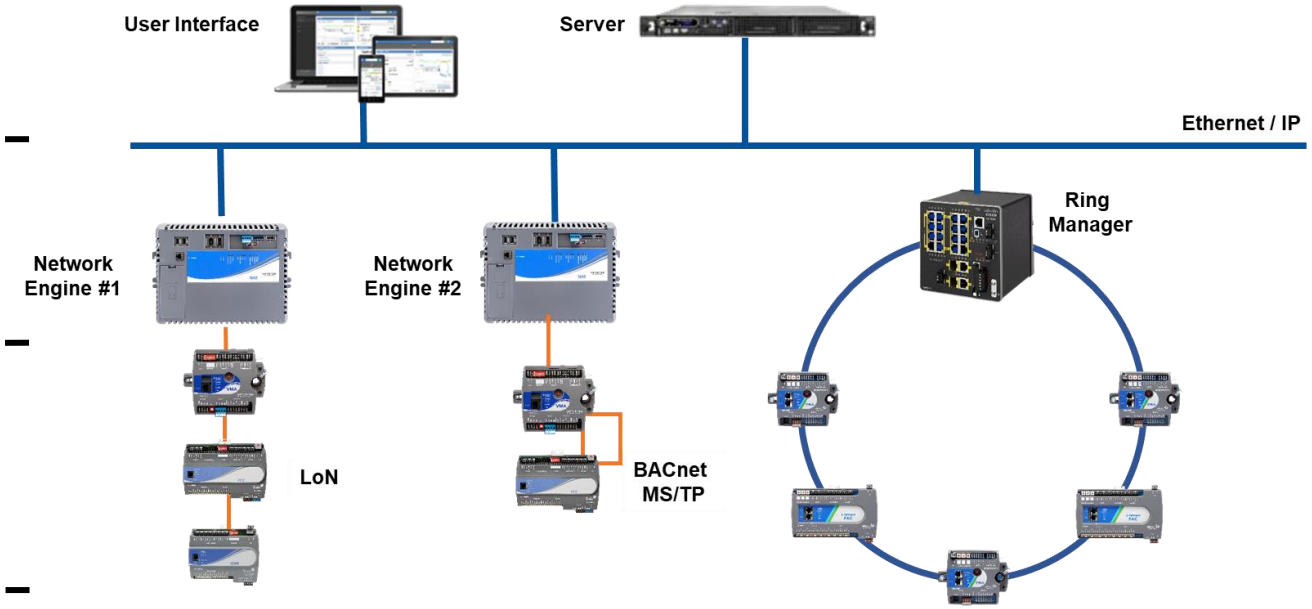
Power | HVAC | BMS | Security | Fire | Lighting / Other

Server / Application

Supervisory

Field

Input / Output



OT vs. IT

- More predictable failure modes
- Tighter time-criticality and determinism
- Higher availability
- More rigorous management of change
- Longer time periods between maintenance
- Significantly longer component lifetimes

- Certifications more important than ever

ISASecure Process and Product Certifications

Simplifies compliance and supplier selection

ISASecure®

process

SDLA

Security Development Lifecycle Assurance

ISA/IEC 62443-4-1

Certified Component ISASecure®

product

CSA

Component Security Assurance

ISA/IEC 62443-4-1, **ISA/IEC 62443-4-2**

Vulnerability Identification Test + Communication Robustness Test

Certified System ISASecure®

product

SSA

System Security Assurance

ISA/IEC 62443-4-1, ISA/IEC 62443-4-2, **ISA/IEC-62443-3-3**

Vulnerability Identification Test + Communication Robustness Test

Certified Component ISASecure®

product

ICSA

IIoT Component Security Assurance

ISA/IEC 62443-4-1, **ISA/IEC 62443-4-2 + additional requirements**

Vulnerability Identification Test + Communication Robustness Test

Development Process Maturity Levels

2. Managed- Written Policies, Trained Personnel

3. Defined (Practiced)- Maturity Level 2 and has been done (repeatably)

4. Improving- Develop continuous improvement based on appropriate metrics

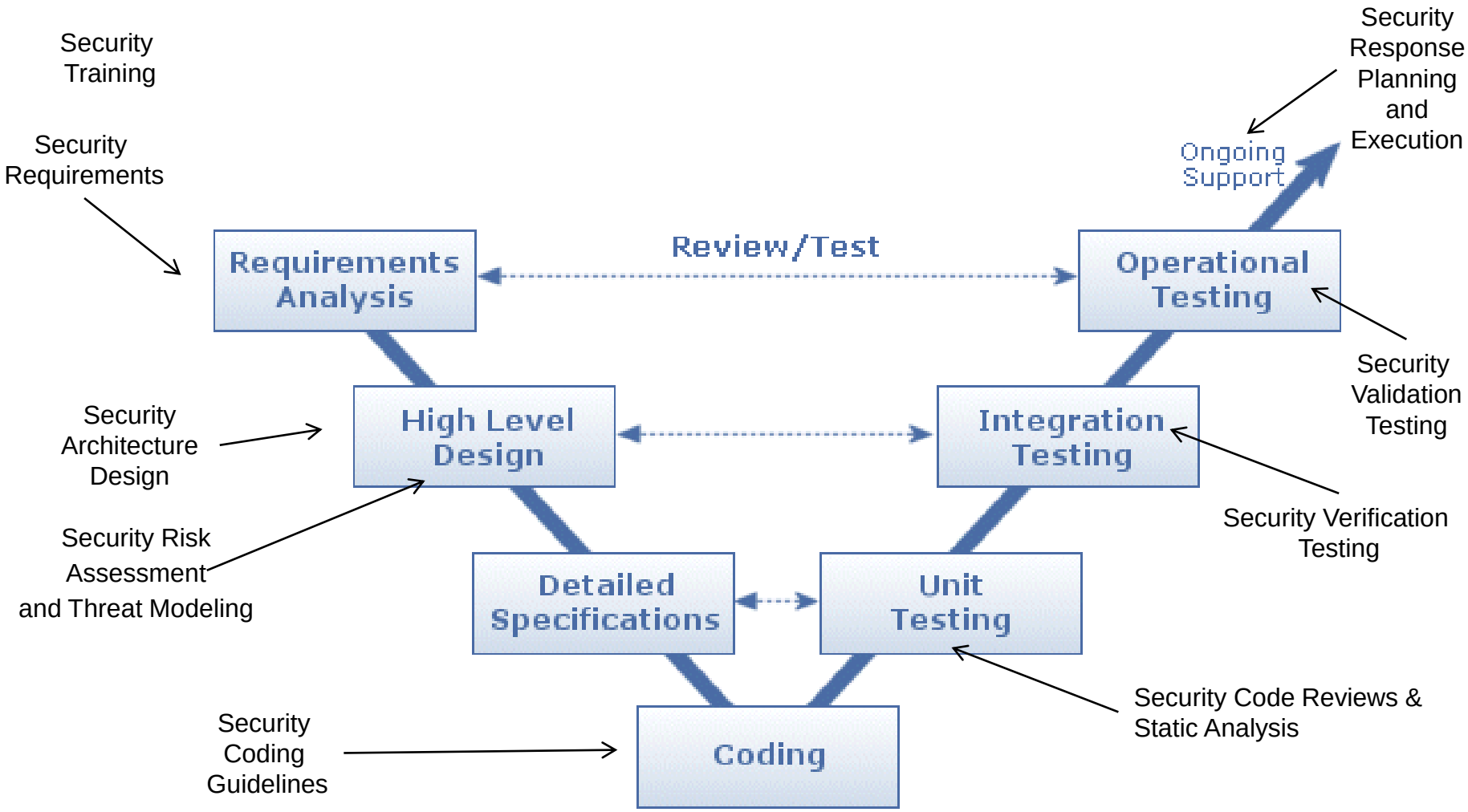
1. Initial- “ad hoc”

SDLA Development Process certification Process

- Review written development procedures – identify gaps to IEC 62443-4-1
- Once gaps are addressed, review process changes to confirm that they addressed gaps
- Review **Readiness** to follow process
  - Have people been trained
  - Are checklists, templates and tools in place

- If process documented, but not executed yet **(ML-2)** can issue certificate with 1 year expiration
- If process has been executed, review select artifacts that demonstrate the process has been followed. If these exist and comply, then a certificate can be issued with 3-year expiration (**ML-2+)**
- When certificate expires it can be renewed by
  - Reviewing Process Changes
  - Auditing project artifacts to ensure process is being followed consistently **(ML-3)**

Audit the Development Process




exida
Certificate / Certificat
Zertifikat / 合格証
SCH 1812099 C001
exida hereby confirms that the process entitled:
Security Development Lifecycle Process
Which is maintained and practiced by
Schneider Electric Systems USA, Inc.
Foxborough, MA, USA
Schneider Electric Systems India Pvt Ltd – SEZ Unit
Hyderabad, India
Has been assessed per the relevant requirements of:
ISASecure® Security Development Lifecycle Assurance (SDLA) Program Version 2.0.0
ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements
IEC 62443-4-1:2018 Secure product development lifecycle requirements
The normative documents and issue dates that define this certification are listed at www.isasecure.org.
This certification applies to the "Security Development Lifecycle Process (SDLP)" versioned documentation listed in the Certification Report.
Evaluating Assessor
Certifying Assessor

Cybersecurity Process Certification

Types of Components which can be certified

product

CSA

- **embedded device** - special purpose device running embedded software designed to directly monitor, control or actuate a physical process (e. g. Building Control systems such as PLCs, Chillers, Thermostats, Access Control, Video Surveillance, Generators, etc.)
- **host device** - general purpose device running a general purpose operating system (e.g. Windows OS, Linux) capable of hosting one or more applications, data stores or functions
- **network device** - device which facilitates data flow between devices, or restricts the flow of data, but does not directly interact with a control process (e.g. Gateways, Routers, Firewalls)
- **application** - software programs executing on the infrastructure that are used to interface with the process or the control system itself
- **IIoT device** - entity that is a sensor or actuator for a physical process, or communicates with sensors or actuators for a physical process, that directly connects to an untrusted network to support and/or use data collection and analytic functions accessible via that network
- **IIoT gateway** - entity of an IIoT system that connects one or more proximity networks and the IIoT devices on those networks to each other and directly connects to one or more untrusted access networks

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	ICS Specific	Moderate	Sophisticated (attack)	Moderate (Hacker Groups)
SL4 Nation State	ICS Specific	High	Sophisticated (campaign)	Extended (Multi-disciplinary Teams)

3. Analyze and Test Cybersecurity Features

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

Cybersecurity levels are defined with stronger requirements needed as the level goes from 1 to 4.

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

Component or System Certification Process

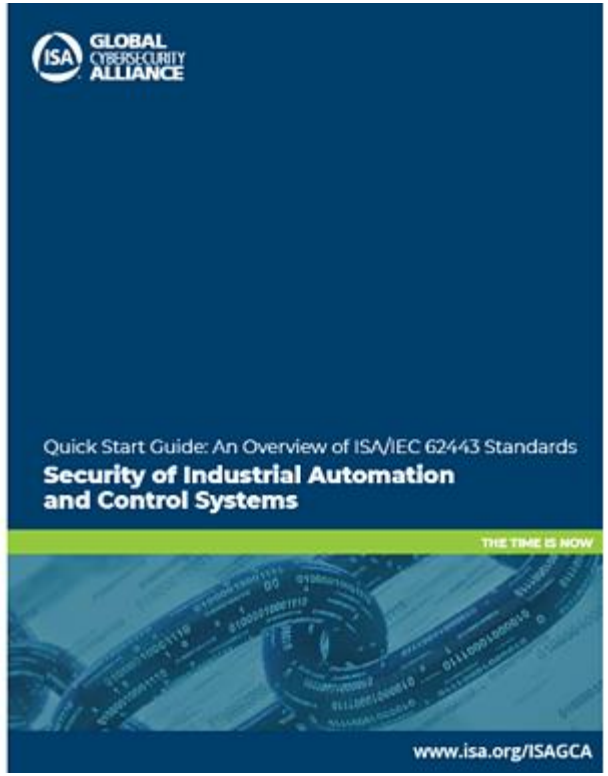
CSA and SSA Certification Schemes follow the same process steps to certify a component or system:

1. Audit the development process used to create the product
   - Verify that the development process used is SDLA Certified
   - Product Artifact Assessment – Verify that the product was developed using this certified development process
2. Analyze and test cybersecurity capabilities/features of the product to determine if they are sufficient for the target security level.
3. Perform or witness cybersecurity network stress testing to find product vulnerabilities (Fuzz Testing and Storm Testing)
4. Perform a Vulnerability Scan (VIT) using Nessus tool looking for known vulnerabilities in the product or system

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

ISA/IEC 62443 addresses Smart Building needs

Quick Start Guide



isa.org/cyberguide

Framework well suited for unique needs of Smart buildings

- More predictable failure modes
- Tighter time-criticality and determinism
- Higher availability
- More rigorous management of change
- Longer time periods between maintenance
- Significantly longer component lifetimes

Full lifecycle support

- Supplier
- Integrator
- Asset owner

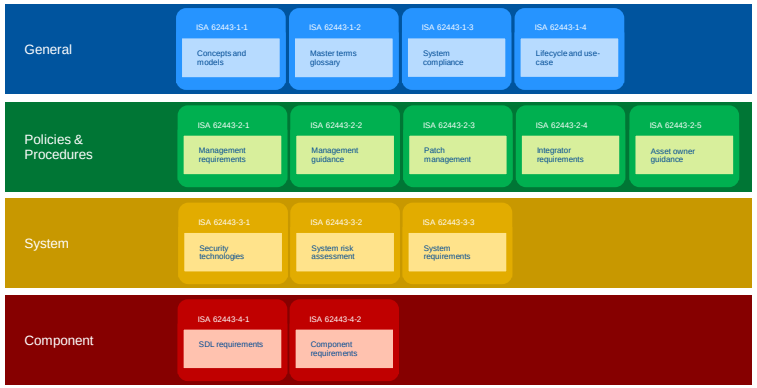
Conformance drives risk reduction

- Requirements
- Guidance
- Training
- Certificates

OT attacks on the rise

Applicable to all architecture levels

Host Devices	Network Components
Applications	Embedded Devices



Compliments existing Smart Building standards

Resources and Further Information

https://isasecure.org

https://isaautomation.isa.org/cybersecurity-alliance/

ISA/IEC 62443 Resources

ISAGCA produces free resources to spread awareness about the ISA/IEC 62443 series of standards.

- Quick Start Guide to ISA/IEC 62443 (fill out form to download)
- Guide to Security Lifecycles in ISA/IEC 62443 (fill out form to download)
- IACS Taxonomy Glossary (.pdf file)
- IACS Principal Roles and Responsibilities (.pdf file)
- From ISASecure®: Overview of ISASecure® Certification for ISA/IEC 62443 (.pdf file)

Resources and Further Information

Exida.com/resources/whitepapers

Contact Mike Medoff at
mmedoff@exida.com

IEC 62443 Cybersecurity Embedded Development Process

Incorporating Agile and Scrum into IEC 62443 posted: 2019-10-07
A Common Development Process for IEC 61508 and IEC 62443 posted: 2019-03-07

What is the IEC 62443 Certification Process?

IEC 62443 Cybersecurity Certification Programs Have Matured posted: 2019-10-07
The exida 61508 / Cybersecurity Certification Program FAQ posted: 2011-01-18

Cybersecurity (IEC 62443) Lifecycle

General

Cybersecurity Risk Assessment Strategies Based on Process Safety Risk Assessment Techniques posted: 2022-09-01
How is Cybersecurity Changing Process Safety? posted: 2022-08-15
Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process posted: 2015-08-07
The ICS Cybersecurity Lifecycle posted: 2013-11-16
The 7 Steps to ICS and SCADA System Security posted: 2013-09-23

ISASecure Certifications for Smart Buildings Technology
November 16, 2022

Questions?

ISASecure®

exida

Johnson Controls