ISASecure Web Conference

Address Smart Buildings Cybersecurity with ISA 62443

Jon Williamson, Director Cyber Experience
October 19, 2020

ISASecure®

About the Speaker

- **Jon Williamson**
- Director, Cyber Experience
  Johnson Controls

- Jon holds a Bachelor of Science degree in Mechanical Engineering from the University of New Hampshire and is an ISC2 Certified Secure Software Lifecycle Professional (CSSLP) and ISA/IEC 62443 Cybersecurity Expert. He has a diverse background with over 25 years' experience in operational technology, as an integrator, a product manager and a technology officer. As the Director of Cyber Experience, Jon is dedicated to driving the customer focused cyber experience with cybersecurity solutions to meet the evolving need for protecting the systems that run their building.

ISA Security Compliance Institute

Agenda

- Smart Buildings
  - systems and protocols
  - layered architecture
- Introduction to ISA/IEC 62443
  - Application to Building Control Systems
  - Standards Family
  - Standards Family Application
  - Overview of Component Requirements 62443-4-2
- ISASecure Certifications, Training & Certificates

ISA Security Compliance Institute

Smart Buildings … cyber framework regardless of protocol

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 · KNX · Proprietary · SNMP · OSDP · M-Bus · http:// · DMX

ASHRAE BACnet® evolution

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

ISA Security Compliance Institute

Smart Buildings … systems utilize a layered architecture

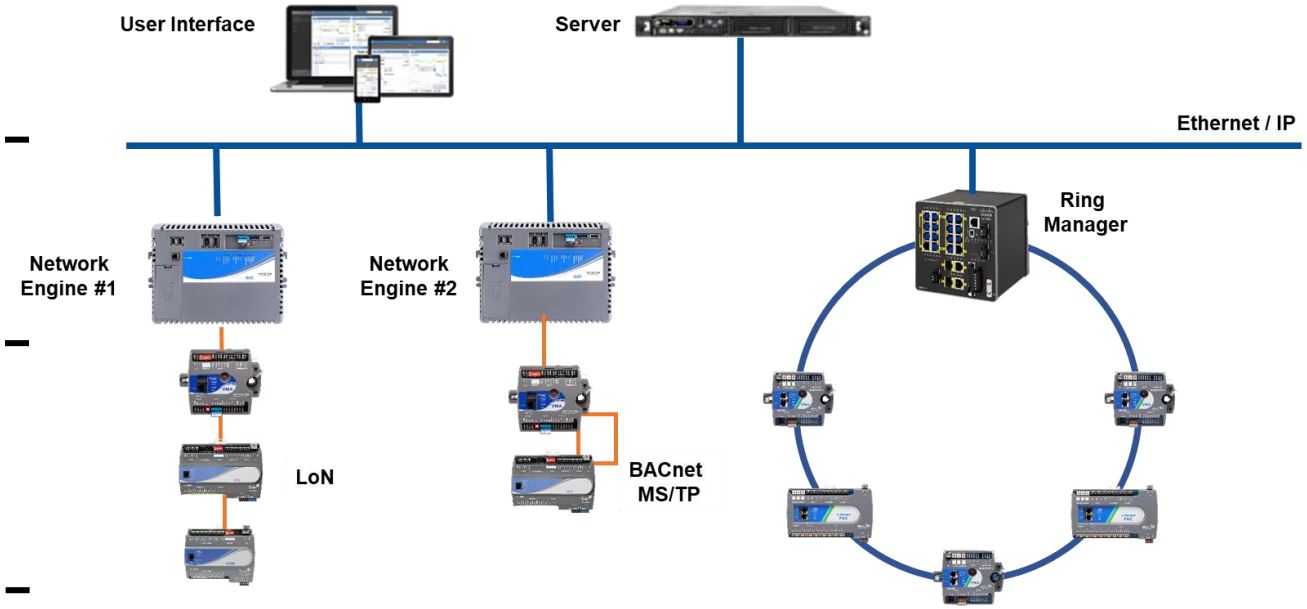
Power | HVAC | BMS | Security | Fire | Lighting / Other

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

ISA Security Compliance Institute

Introducing ISA/IEC 62443

- **ISA/IEC 62443**
  - Family of standards
  - Initiated in ISA99 committee – jointly developed with IEC
  - Provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems

- **ISA**
  - International Society of Automation
  - Non-profit professional association founded in 1945 to create a better world through automation.
  - Publishes 62443 as ANSI/ISA-62443
- **ISA Security Compliance Institute (ISCI)**
  - Wholly owned non-profit subsidiary of ISA
  - ISA**Secure** conformity assessment to ISA/IEC 62334 standards
- **International Electrotechnical Commission (IEC)**
  - Founded in 1906, world's leading organization for the preparation and publication of International Standards for all electrical, electronic and related technologies.
  - ISA/IEC 62443 developed in IEC Technical Committee 65/Working Group 10

IEC 62443 Standards and ISASecure® Certification Application to Building Control Systems

2016 ISASecure Building Control Systems Working Group

Download Working Group Final Report at
http://isasecure.org/en-US/Building-Control-Systems-Report

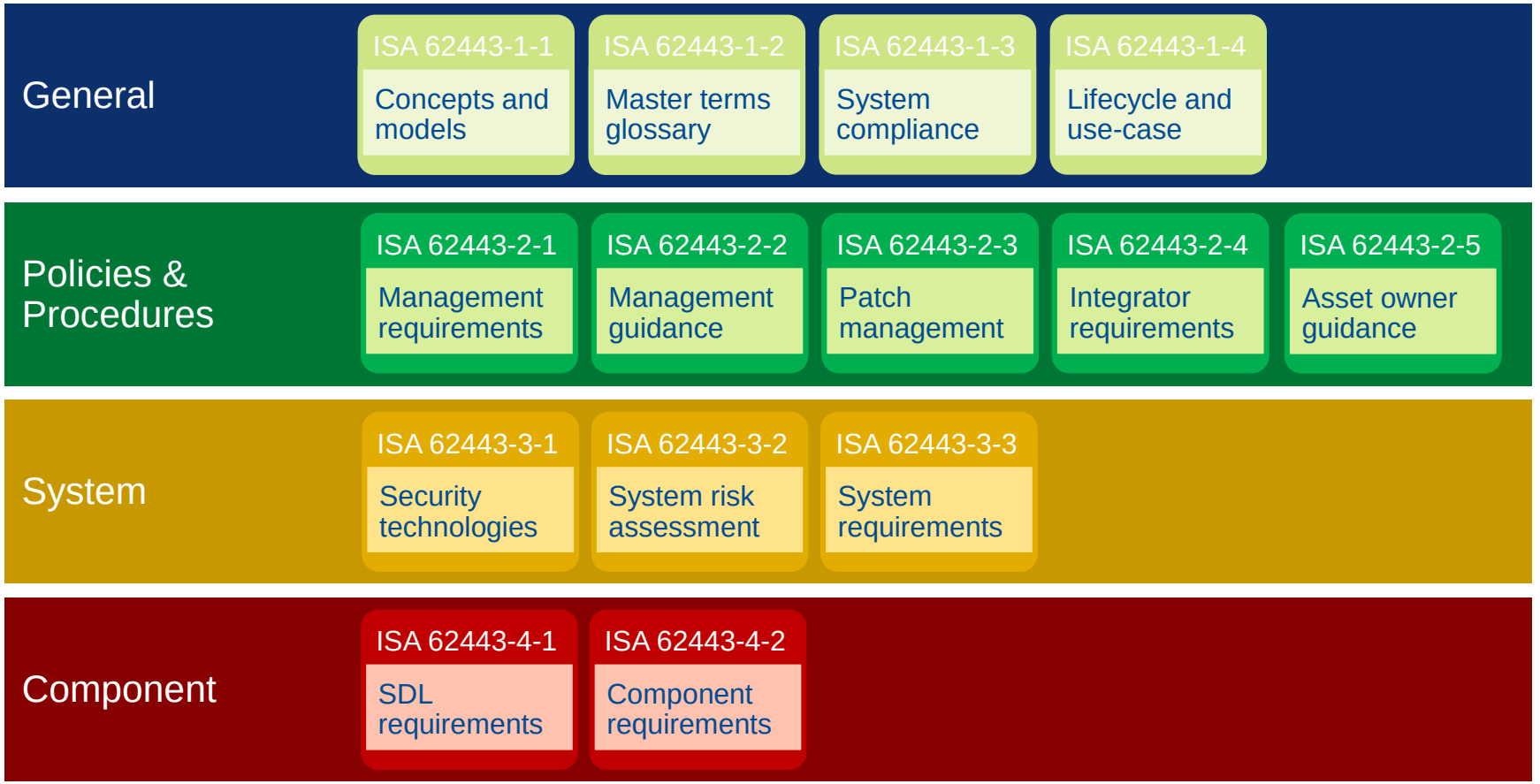
CABA Continental Automated Buildings Association · CSA Group · George Brown College · Honeywell · ireo · Johnson Controls · Maverick Technologies A Rockwell Automation Company · RBCG Ron Bernstein Consulting Group · Schneider Electric · Syska Hennessy Group

Jim Sinopoli-Smart Buildings, LLC

Mike Chipley-PMC Group, LLC

ISA Security Compliance Institute

ISA/IEC 62443 Standards Family



ISA/IEC 62443 Standards Family Application

Smart Building (site specific)

Owner

Operate

ISA 62443-1-3
System compliance

ISA 62443-2-1
Management requirements

ISA 62443-2-3
Patch management

Integrator

Design/Deploy

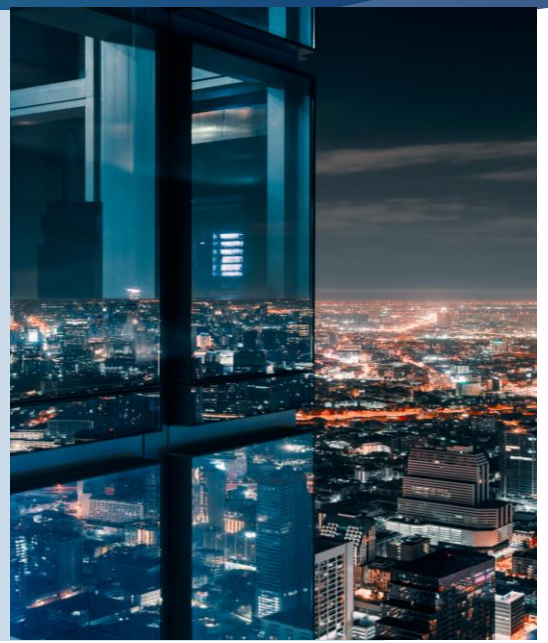
ISA 62443-2-4
Integrator requirements

Subsystem 1

Subsystem 2

Complementary components

ISA 62443-3-3
System requirements



Products (off-the-shelf)

Supplier

Develop

ISA 62443-4-1
SDL requirements

Applications

Embedded Devices

Network Components

Host Devices

ISA 62443-3-3
System requirements

ISA 62443-4-2
Component requirements

ISA/IEC 62443 Standards Family Application

ISA 62443-4-2

Component requirements

Component	Industrial Automation and Control System	Building Automation System	Video Surveillance System
Embedded device	Programmable Logic Controller Intelligent Electronic Device	Supervisory controllers Field controllers - Unitary - Terminal - General purpose	Video Camera Video Transceiver (analog to IP)
Network device	Switch VPN terminator	Switch Router / Gateway VPN	Switch Router / Gateway VPN
Host device/application	Operator workstation Data historian	Operator workstation (facility manager level) Advanced workstation (engineering level) Application Server (handles data storage)	Network Video Recorder Video Client / Workstation

ISA/IEC 62443-4-2
Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Foundational Requirement Groups

- **FR1** - Identification and authentication control (IAC)
- **FR2** - Use control (UC)
- **FR3** - System integrity (SI)
- **FR4** - Data confidentiality (DC)
- **FR5** - Restricted data flow (RDF)
- **FR6** - Timely response to events (TRE)
- **FR7** - Resource availability (RA)

Security Levels	Definition	Means	Resources	Skills	Motivation
SL1	Protection against casual or coincidental violation	simple	low	generic	low
SL2	Protection against intentional violation using simple means with low resources, generic skills and low motivation				
SL3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation	sophisticated	moderate	IACS-specific	moderate
SL4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation	sophisticated	extended	IACS-specific	high

ISA/IEC 62443-4-2
Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Foundational Requirement	Component Requirement
FR 1 – Identification and authentication control	CR 1.1 – Human user identification and authentication CR 1.2 – Software process & device identification and authentication CR 1.3 – Account management CR 1.4 – Identifier management CR 1.5 – Authenticator management CR 1.6 – Wireless access management CR 1.7 – Strength of password-based authentication CR 1.8 – Public key infrastructure certificates CR 1.9 – Strength of public key-based authentication CR 1.10 – Authenticator feedback CR 1.11 – Unsuccessful login attempts CR 1.12 – System use notification CR 1.13 – Access via untrusted networks CR 1.14 – Strength of symmetric key-based authentication

ISA/IEC 62443-4-2
Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Foundational Requirement	Component Requirement
FR 2 – Use control	CR 2.1 – Authorization enforcement CR 2.2 – Wireless use control CR 2.3 – Use control for portable and mobile devices CR 2.4 – Mobile code CR 2.5 – Session lock CR 2.6 – Remote session termination CR 2.7 – Concurrent session control CR 2.8 – Auditable events CR 2.9 – Audit storage capacity CR 2.10 – Response to audit processing failures CR 2.11 – Timestamps CR 2.12 – Non-repudiation CR 2.13 – Use of physical diagnostic and test interfaces
FR 3 – System integrity	CR 3.1 – Communication integrity CR 3.2 – Protection from malicious code CR 3.3 – Security functionality verification CR 3.4 – Software and information integrity CR 3.5 – Input validation CR 3.6 – Deterministic output CR 3.7 – Error handling CR 3.8 – Session integrity CR 3.9 – Protection of audit information 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

ISA/IEC 62443-4-2
Foundational requirements for components

Develop

ISA 62443-4-2

Component requirements

Foundational Requirement	Component Requirement
FR 4 – Data confidentiality	CR 4.1 – Information confidentiality CR 4.2 – Information persistence CR 4.3 – Use of cryptography
FR 5 – Restricted data flow	CR 5.1 – Network segmentation CR 5.2 – Zone boundary protection CR 5.3 – General purpose person-to-person communication restrictions
FR 6 – Time response to events	CR 6.1 – Audit log accessibility CR 6.2 – Continuous monitoring
FR 7 – Resource availability	CR 7.1 – Denial of service protection CR 7.2 – Resource management CR 7.3 – Control system backup CR 7.4 – Control system recovery and reconstitution CR 7.6 – Network and security configuration settings CR 7.7 – Least functionality CR 7.8 – Control system component inventory

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

ISASecure Training & Certificates

Qualifies cybersecurity experts
Aligns ISA/IEC 62443 practices

- ISASecure®

ISA Cybersecurity Training

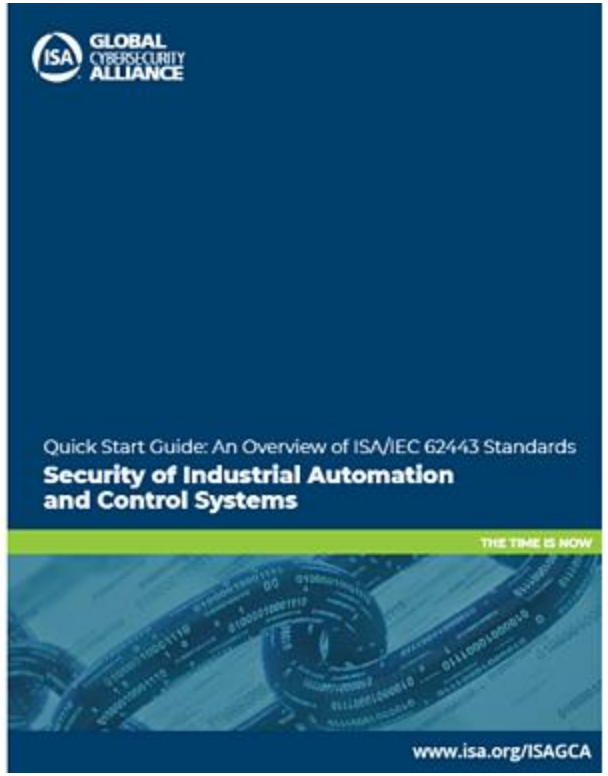
- ISA/IEC 62443 centric training – awareness, assessments, design, operation, maintenance, etc.

ISA Cybersecurity Certificates

- ISA certificates for students who complete ISA training courses and pass professional examinations.

ISA/IEC 62443 addresses Smart Building needs

New 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

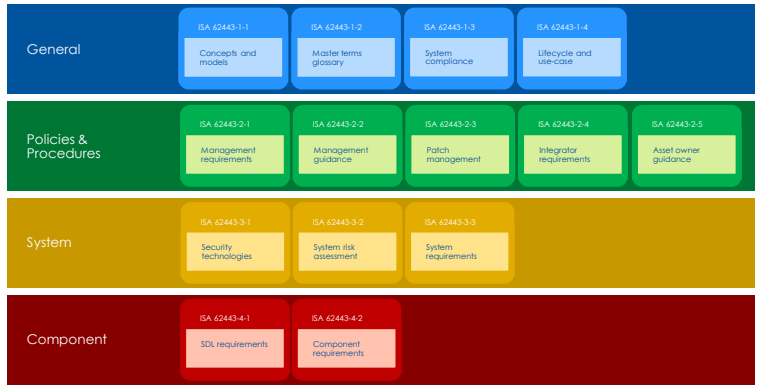
Conformance provides drives risk reduction

- 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

ISASecure Web Conference

Address Smart Buildings Cybersecurity with ISA 62443

Questions?