# Using IEC 62443 Standards for Securing Building Management Systems

A quick look at building automation control systems
and how IEC-62443 can be applied

**Jason Christman**
Vice President, Chief Product Security Officer
Johnson Controls

**Andre Ristaino**
Managing Director, ISA Security Compliance Institute

www.isasecure.org

# Goals and Agenda

- **Webinar Goals**
  - Provide basic knowledge around BMS cybersecurity
  - Show similarity of building management systems to other industrial automation control systems
  - Illustrate applicability of IEC 62443 standards to BMS

- **Agenda**
  - Overview of IEC 62443 Standards and ISASecure Certifications
  - BMS Introduction
  - Brief history and terminology
  - IEC 62443-4-2 component alignment to technical security requirements
  - Future state of BMS

# Overview of IEC 62443 and ISASecure

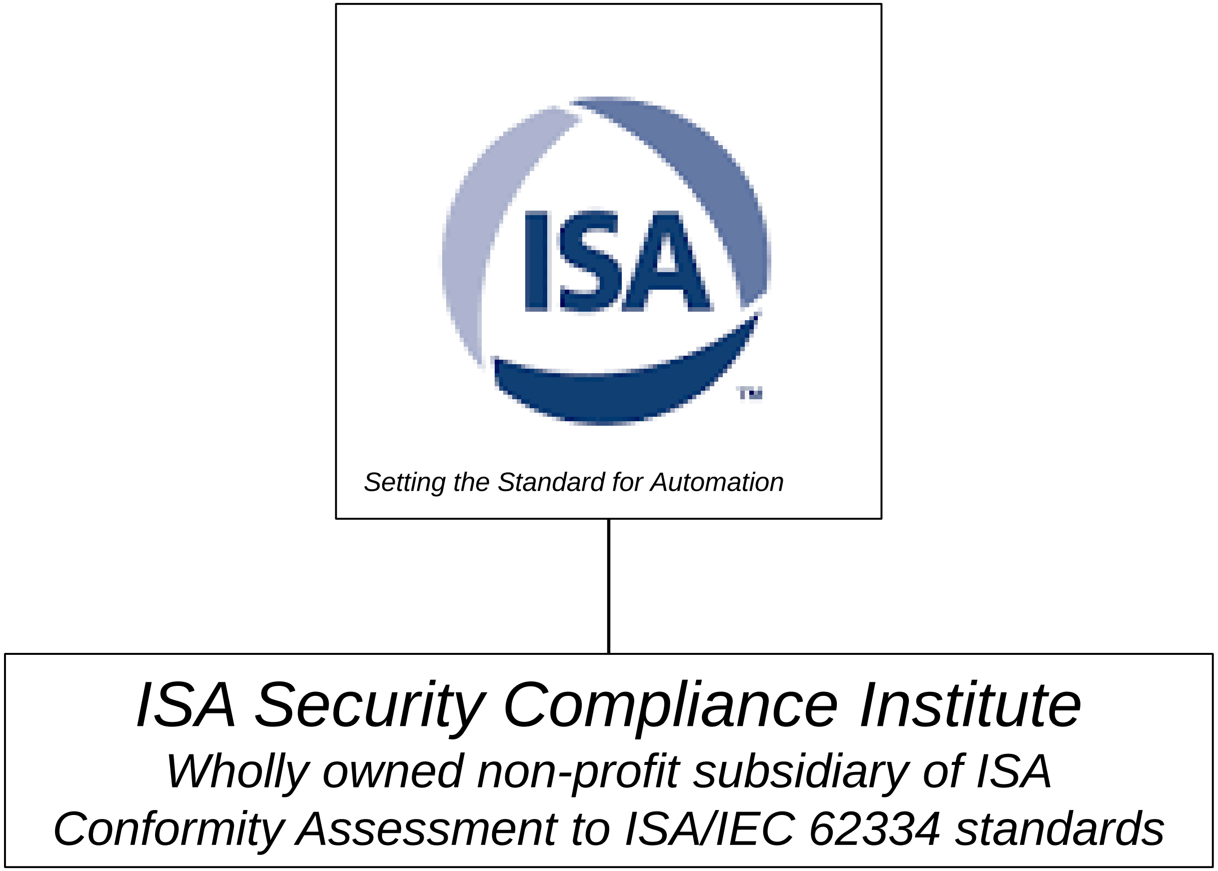
Andre Ristaino

# International Society of Automation

*Setting the Standard for Automation*

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

# ISA Security Compliance Institute



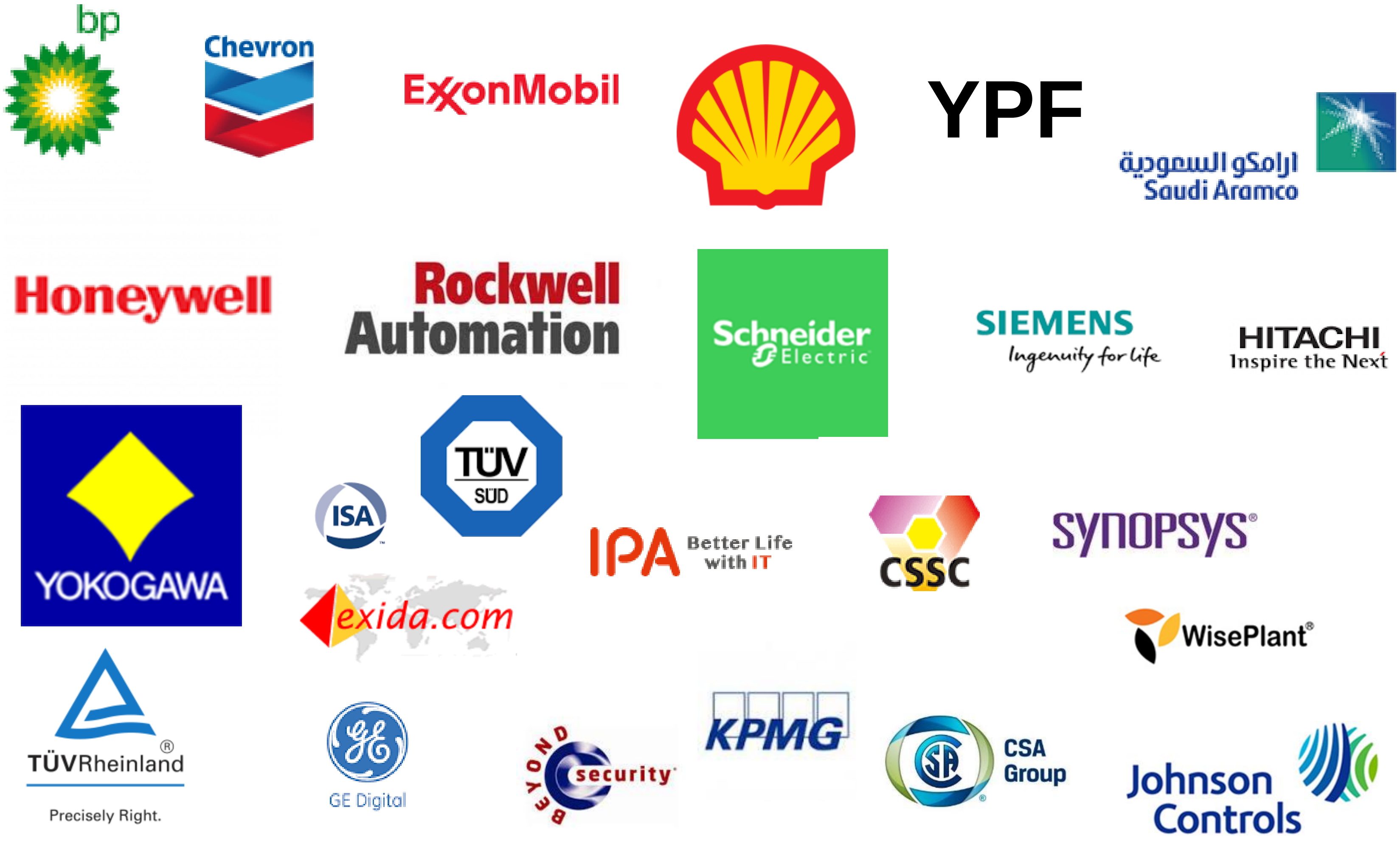
Setting the Standard for Automation

*ISA Security Compliance Institute*

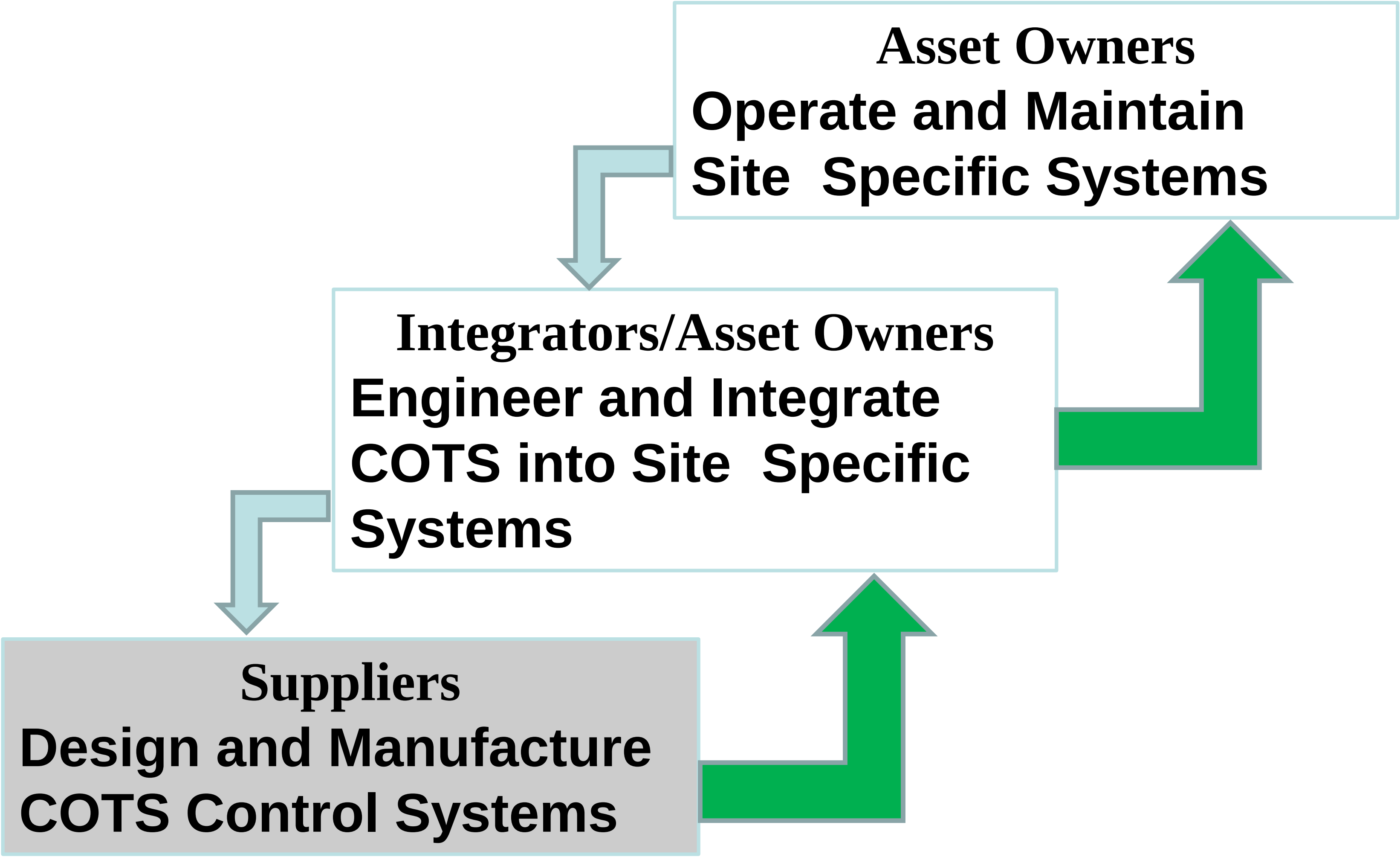
*Wholly owned non-profit subsidiary of ISA*

*Conformity Assessment to ISA/IEC 62334 standards*

# ISASecure® Supporters – past & present



# Automation System Security Lifecycle



**Asset Owners**

**Operate and Maintain Site Specific Systems**

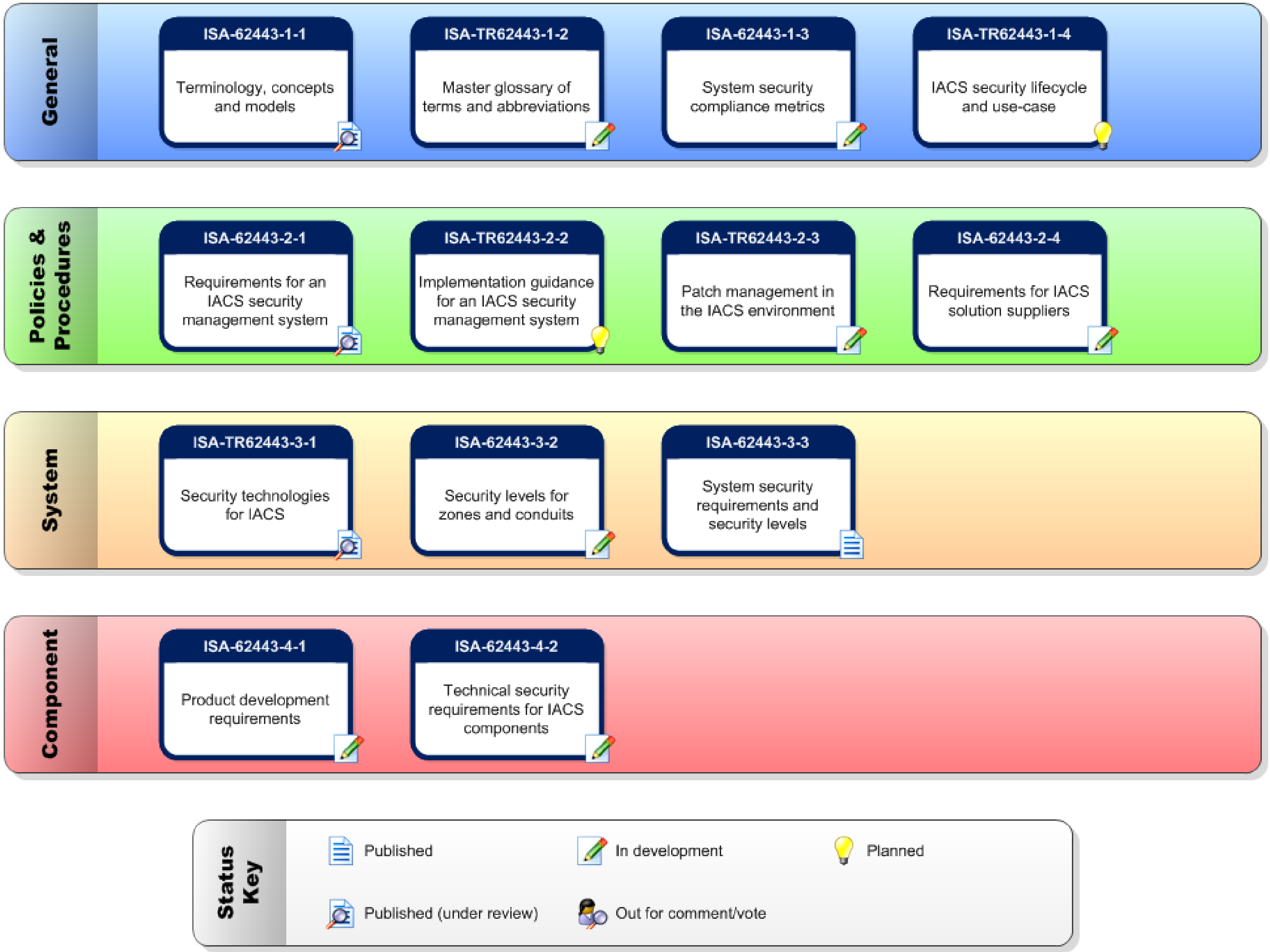
**Integrators/Asset Owners**

**Engineer and Integrate COTS into Site Specific Systems**

**Suppliers**

**Design and Manufacture COTS Control Systems**

# ISA/IEC 62443 Standards Family



**General**

- ISA-62443-1-1: Terminology, concepts and models
- ISA-TR62443-1-2: Master glossary of terms and abbreviations
- ISA-62443-1-3: System security compliance metrics
- ISA-TR62443-1-4: IACS security lifecycle and use-case

**Policies & Procedures**

- ISA-62443-2-1: Requirements for an IACS security management system
- ISA-TR62443-2-2: Implementation guidance for an IACS security management system
- ISA-TR62443-2-3: Patch management in the IACS environment
- ISA-62443-2-4: Requirements for IACS solution suppliers

**System**

- ISA-TR62443-3-1: Security technologies for IACS
- ISA-62443-3-2: Security levels for zones and conduits
- ISA-62443-3-3: System security requirements and security levels

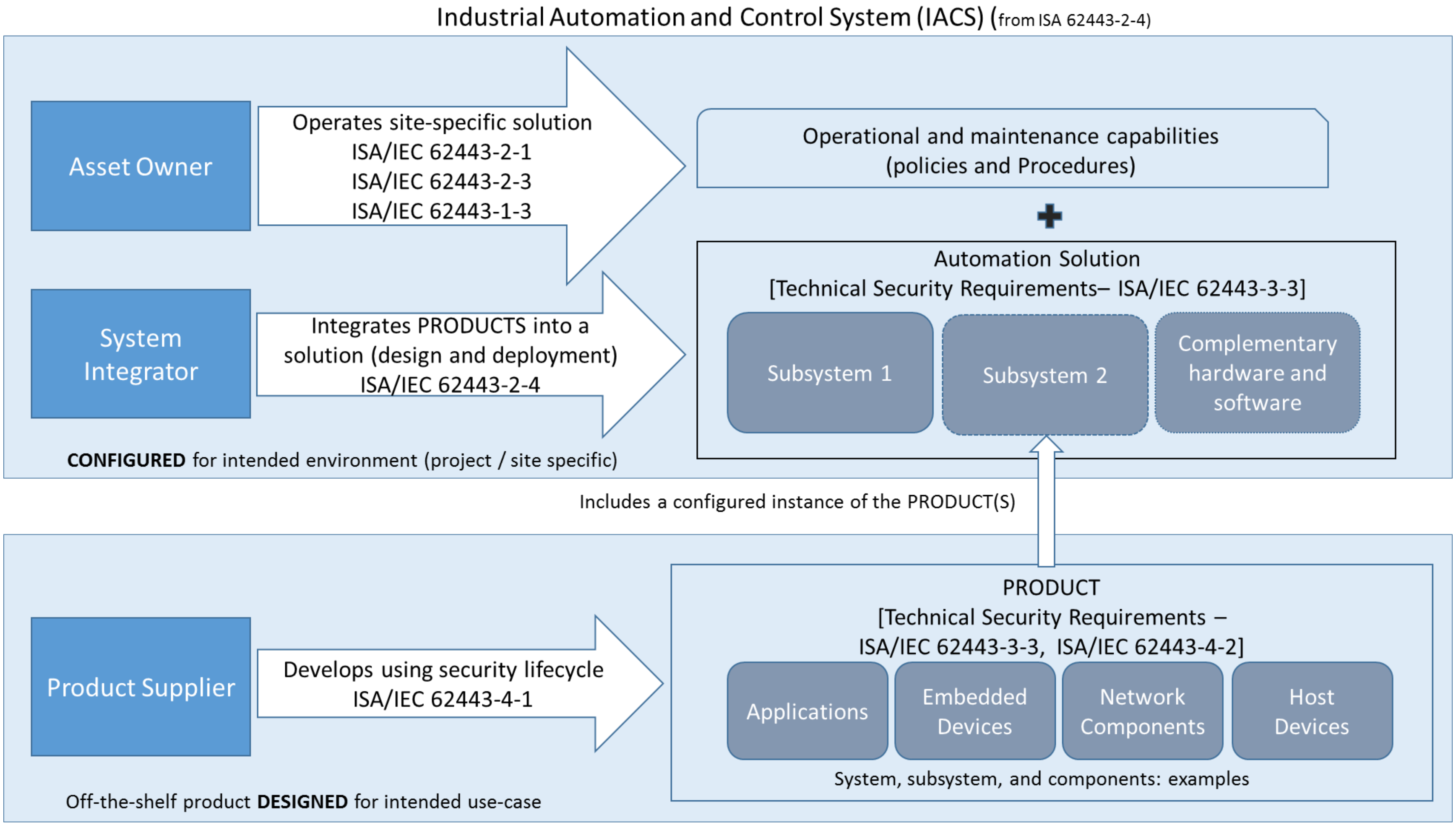
**Component**

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

**Status Key**

- Published
- In development
- Planned
- Published (under review)
- Out for comment/vote

# ISA/IEC 62443 Standards Family



Industrial Automation and Control System (IACS) (from ISA 62443-2-4)

Asset Owner

Operates site-specific solution
ISA/IEC 62443-2-1
ISA/IEC 62443-2-3
ISA/IEC 62443-1-3

Operational and maintenance capabilities
(policies and Procedures)

✚

System Integrator

Integrates PRODUCTS into a solution (design and deployment)
ISA/IEC 62443-2-4

Automation Solution
[Technical Security Requirements– ISA/IEC 62443-3-3]

Subsystem 1

Subsystem 2

Complementary hardware and software

**CONFIGURED** for intended environment (project / site specific)

Includes a configured instance of the PRODUCT(S)

Product Supplier

Develops using security lifecycle
ISA/IEC 62443-4-1

PRODUCT
[Technical Security Requirements –
ISA/IEC 62443-3-3, ISA/IEC 62443-4-2]

Applications

Embedded Devices

Network Components

Host Devices

System, subsystem, and components: examples

Off-the-shelf product **DESIGNED** for intended use-case

# Certification Bodies Internationally Accredited to ISO/IEC 17065 & ISO/IEC 17025

ANSI
ANSI Accredited Program
PRODUCT CERTIFICATION
ANAB
ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS
CERTIFICATION BODY
PROD
JAB
ilac-MRA
DAkkS
Deutsche
Akkreditierungsstelle
D-PL-18345-01-00
Singapore
Accreditation
Council
CSSC
exida.com
TÜVRheinland®
Precisely Right.

# ISASecure Recognized Test Tools

GE
GE Digital

HITACHI
Inspire the Next

信联科汇
XLKH TECHNOLOGY

tenable®
network security

BEYOND
security

# Three ISASecure® certifications available

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

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

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

   Vulnerability Identification Test
   + Communication Robustness Test

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

   **ISA/IEC-62443-3-3**

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

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

   Vulnerability Identification Test
   + Communication Robustness Test

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

   process certification

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

# 2016 ISASecure Building Control Systems Working Group

## Participating Organizations

Schneider Electric

CSA Group

Johnson Controls

MAVERICK TECHNOLOGIES
A Rockwell Automation Company

Honeywell

SIEMENS

GEORGE BROWN COLLEGE

RBCG
Ron Bernstein Consulting Group

SYSKA HENNESSY GROUP

ireo

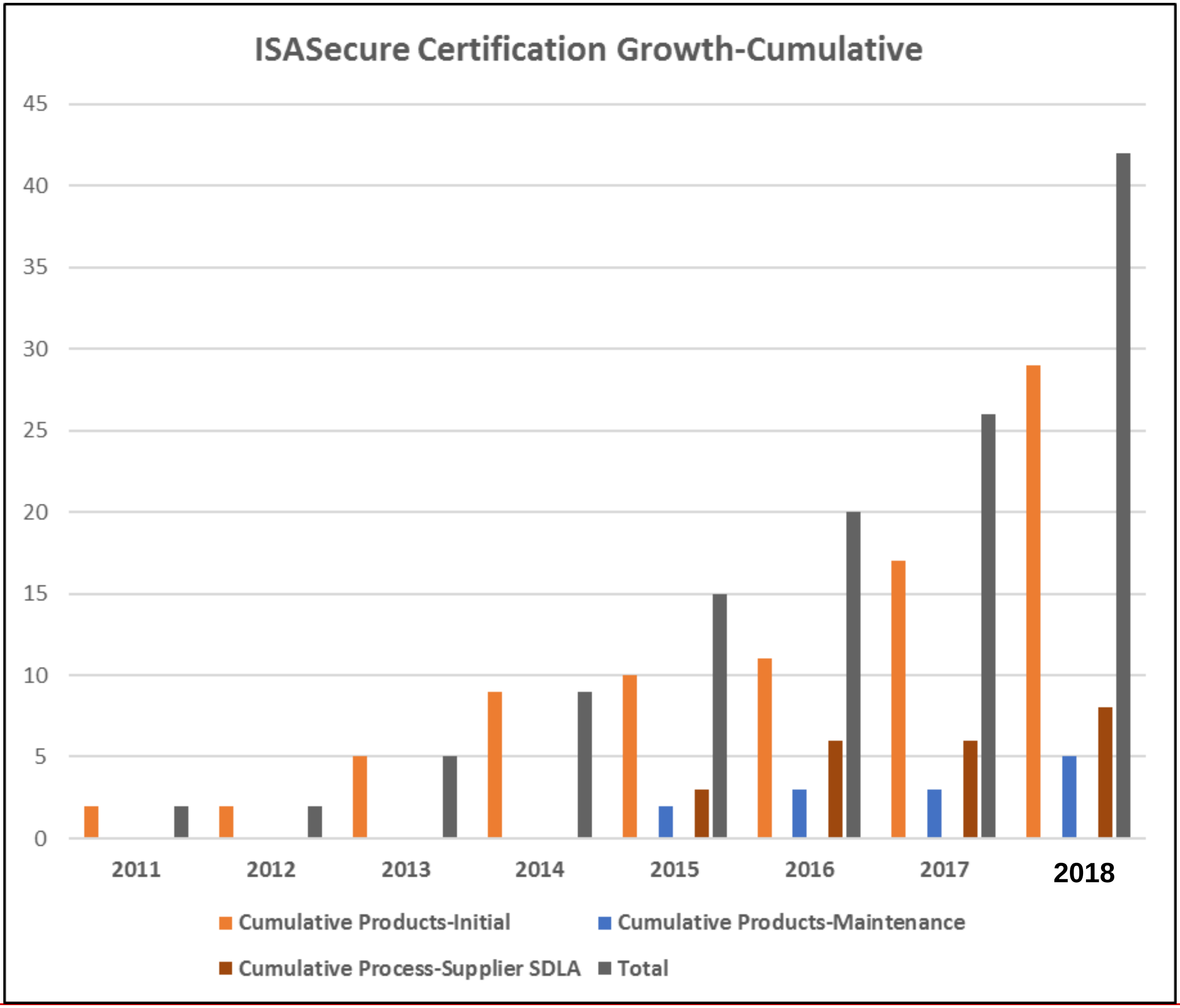
ISA Security Compliance Institute

CABA Continental Automated Buildings Association

*Mike Chipley-PMC Group, LLC*
*Jim Sinopoli-Smart Buildings, LLC*

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

# ISASecure Certification Growth

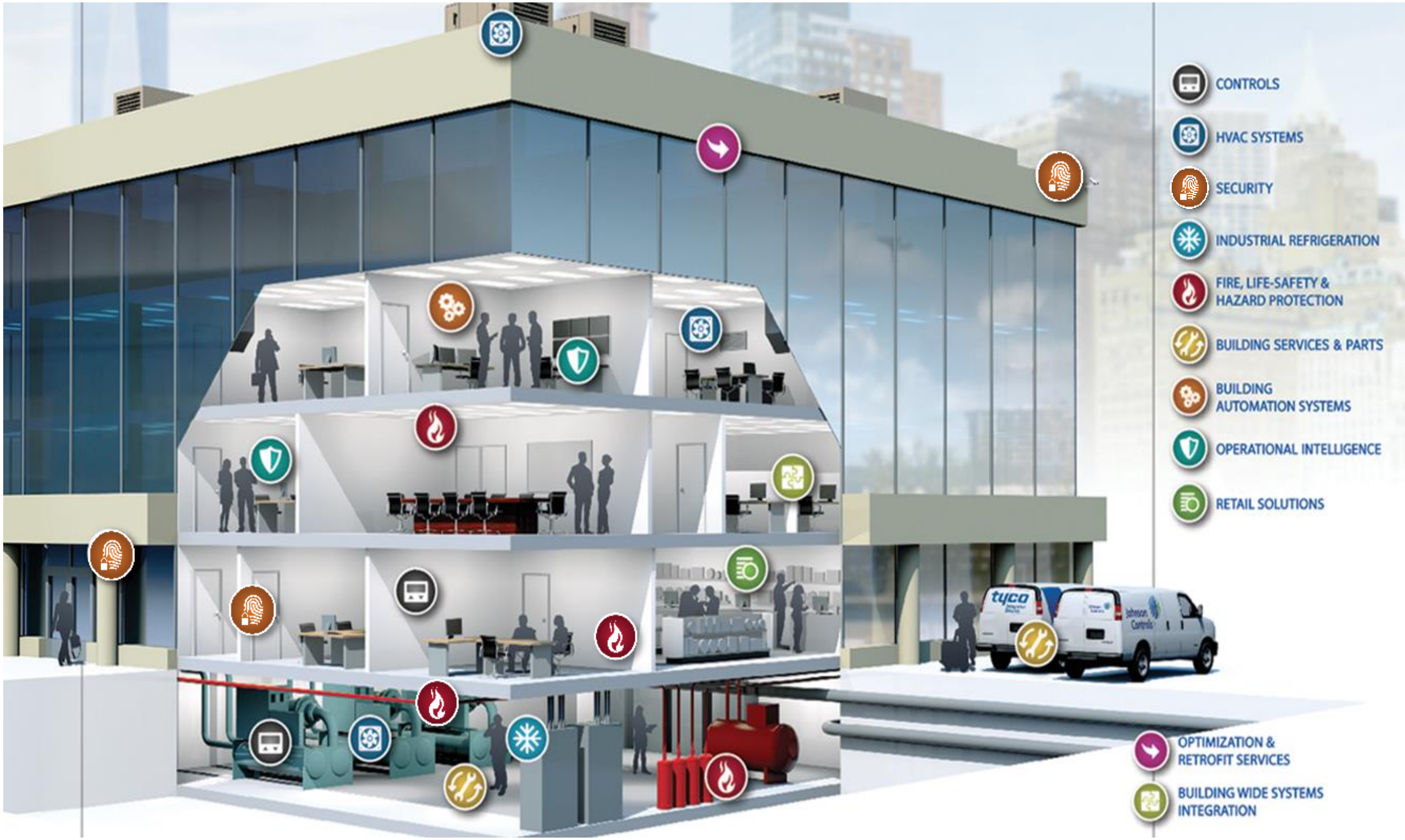


# Building Management Systems Discussion

Jason Christman

# Integrated & Intelligent Building Control Systems

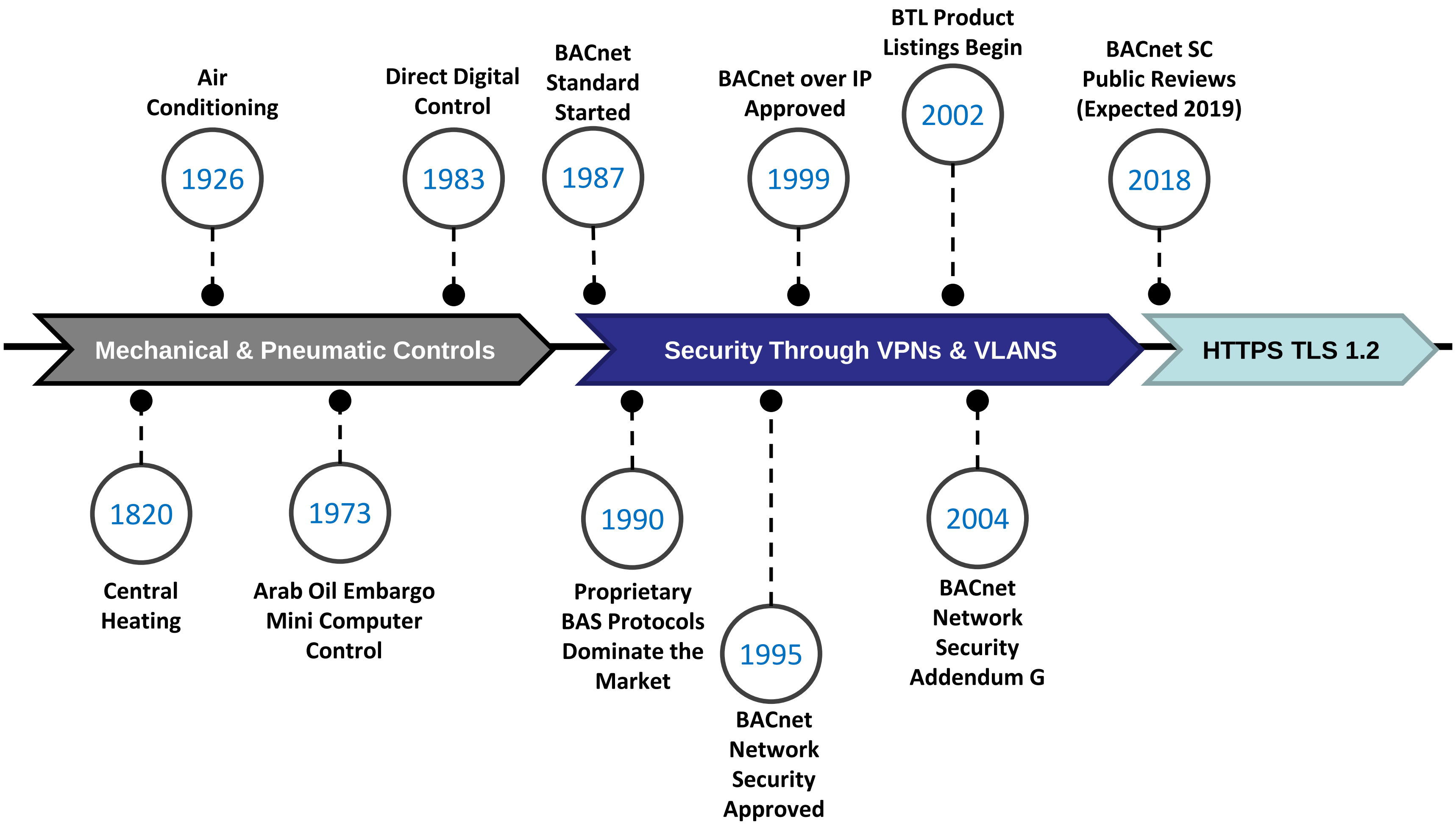
*An ecosystem of automation control technologies*


CONTROLS
HVAC SYSTEMS
SECURITY
INDUSTRIAL REFRIGERATION
FIRE, LIFE-SAFETY & HAZARD PROTECTION
BUILDING SERVICES & PARTS
BUILDING AUTOMATION SYSTEMS
OPERATIONAL INTELLIGENCE
RETAIL SOLUTIONS
OPTIMIZATION & RETROFIT SERVICES
BUILDING WIDE SYSTEMS INTEGRATION
tyco
Johnson Controls

# Building Automation Control Has Many Use Cases

- Advanced Metering Infrastructure
- Building Automation System
- Building Management Control System
- CCTV Surveillance System
- CO2 Monitoring
- Digital Signage Systems
- Electronic Security System
- Emergency Management System
- Energy Management System
- Exterior Lighting Control Systems
- Fire Alarm System
- Fire Sprinkler System
- Interior Lighting Control System
- Intrusion Detection Systems
- Physical Access Control System
- Public Safety/Land Mobile Radios
- Renewable Energy Geothermal Systems
- Renewable Energy Photo Voltaic Systems
- Shade Control System
- Smoke and Purge Systems
- Vertical Transport System (Elevators and Escalators)

# Historical Timeline for Building Automation Security



Mechanical & Pneumatic Controls

Security Through VPNs & VLANS

HTTPS TLS 1.2

1820 Central Heating

1926 Air Conditioning

1973 Arab Oil Embargo Mini Computer Control

1983 Direct Digital Control

1987 BACnet Standard Started

1990 Proprietary BAS Protocols Dominate the Market

1995 BACnet Network Security Approved

1999 BACnet over IP Approved

2002 BTL Product Listings Begin

2004 BACnet Network Security Addendum G

2018 BACnet SC Public Reviews (Expected 2019)

# Key Terms

- **Building Management System (BMS)**
  - Foundation of modern building efficiency
  - Provides system control and easy access to information
  - Enhances occupant comfort, safety, security, and productivity
  - Complete family of hardware and software control components designed to work together as one cohesive system

- **Synonymous with BMS**
  - Building Control System (BCS)
  - Building Automation System (BAS)
  - Building Automation Control System (BACS)
  - Facility Management System (FMS)
  - Energy Management Control System (ECMS)

# Key Terms

- **ASHRAE** – American Society of Heating, Refrigerating and Air-Conditioning Engineers
- “**Intelligent**” or “**Smart**” **Building –** a building controlled by a “data enabled” building automation system
- **Controller –** purpose-built computer with input/output capabilities; buildings typically have system/network controllers and terminal unit controllers; below the supervisory controller are field controllers, unitary controllers, or terminal controllers
- **Supervisory controller –** provides network management and system-wide control coordination over one or more networks of equipment
- **Direct digital control** (DDC) – automated control of a process by a digital device
- **Unitary controller –** an electronic device for digital control of packaged air handling units, unit ventilators, fan coils, heat pumps, and other terminal units serving a single zone or room
- **Terminal unit controller –** suited for control of lighting and/or simpler devices such as a package rooftop unit, heat pump, VAV box, fan coil, etc.

# Key Terms

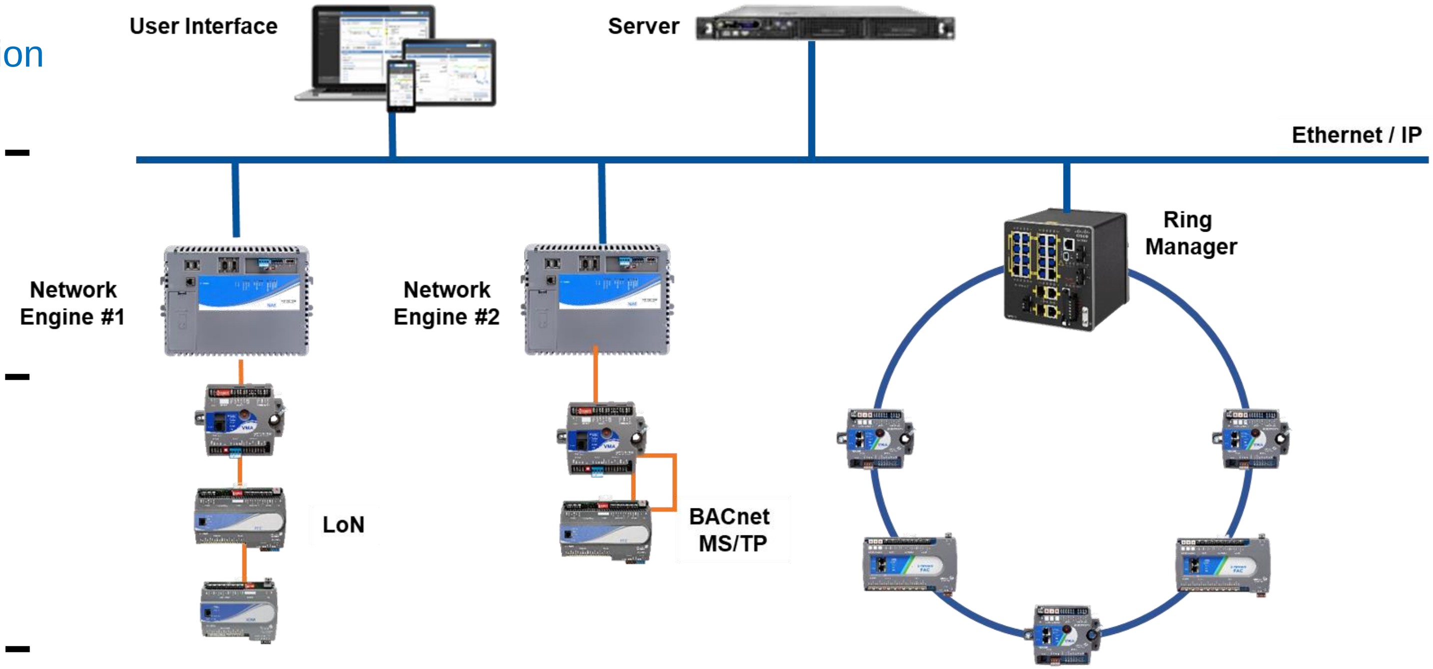
## Layered Architecture

Server / Application

Supervisory

Field Controller

Input / Output



# Common Building Automation Control Protocols

- **BACnet** – communications protocol for Building Automation and Control (BAC) networks that leverage the ASHRAE, ANSI, and ISO 16484-5 standard protocol
- **LonTalk** – protocol optimized for various functions in industrial control, home automation, transportation, and buildings systems such as lighting and HVAC
- **ZigBee** – short range, low-powered wireless mesh communication standard targeted at building automation
- **Modbus** – serial communications protocol commonly used to connect industrial electronic devices
- **M-Bus** (Meter-Bus) – European standard for the remote reading of gas, electricity, or other consumption meters

# IEC 62443-4-2 Component Alignment to Technical Security Requirements

- **Component types:**
  - Software applications
  - Embedded devices
  - Host devices
  - Network devices
- **Foundational requirements**
  - Identification and authentication control (IAC)
  - Use control (UC)
  - System integrity (SI)
  - Data confidentiality (DC)
  - Restricted data flow (RDF)
  - Timely response to events (TRE)
  - Resource availability (RA)

# IEC 62443-4-2 Component Alignment to Technical Security Requirements

**Software application requirements (SAR)**

- Mobile code
- Protection from malicious code

**Embedded device requirements (EDR)**

- Mobile code
- Use of physical diagnostic and test interfaces
- Protection from malicious code
- Support for updates
- Physical tamper resistance and detection
- Provisioning product supplier roots of trust
- Provisioning asset owner roots of trust
- Integrity of the boot process

**Host device requirements (HDR)**

- Mobile code
- Use of physical diagnostic and test interfaces
- Protection from malicious code
- Support for updates
- Physical tamper resistance and detection
- Provisioning product supplier roots of trust
- Provisioning asset owner roots of trust
- Integrity of the boot process

**Network device requirements (NDR)**

- Wireless access management
- Access via untrusted networks
- Mobile code
- Use of physical diagnostic and test interfaces
- Protection from malicious code
- Support for updates
- Physical tamper resistance and detection
- Provisioning product supplier roots of trust
- Provisioning asset owner roots of trust
- Integrity of the boot process
- Zone boundary protection
- Person-to-person communication restrictions

# IEC 62443-4-2 Component Alignment to Technical Security Requirements

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

# IEC 62443-4-2 Component Alignment to Technical Security Requirements

| Foundational Requirement | Component Requirement |
|---|---|
| FR 2 – Use control | CR 2.1 – Authorization enforcement<br>CR 2.2 – Wireless use control<br>CR 2.3 – Use control for portable and mobile devices<br>CR 2.4 – Mobile code<br>CR 2.5 – Session lock<br>CR 2.6 – Remote session termination<br>CR 2.7 – Concurrent session control<br>CR 2.8 – Auditable events<br>CR 2.9 – Audit storage capacity<br>CR 2.10 – Response to audit processing failures<br>CR 2.11 – Timestamps<br>CR 2.12 – Non-repudiation<br>CR 2.13 – Use of physical diagnostic and test interfaces |
| FR 3 – System integrity | CR 3.1 – Communication integrity<br>CR 3.2 – Protection from malicious code<br>CR 3.3 – Security functionality verification<br>CR 3.4 – Software and information integrity<br>CR 3.5 – Input validation<br>CR 3.6 – Deterministic output<br>CR 3.7 – Error handling<br>CR 3.8 – Session integrity<br>CR 3.9 – Protection of audit information<br>CR 3.10 – Support for updates<br>CR 3.11 – Physical tamper resistance and detection<br>CR 3.12 – Provisioning product supplier roots of trust<br>CR 3.13 – Provisioning asset owner roots of trust<br>CR 3.14 – Integrity of the boot process |

# IEC 62443-4-2 Component Alignment to Technical Security Requirements

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

# IEC 62443-4-2 Component Alignment to Technical Security Requirements

| Component | Industrial Automation and Control System | Building Automation System |
|---|---|---|
| Embedded device | Programmable Logic Controller<br>Intelligent Electronic Device | Supervisory controllers<br>Field controllers<br>- Unitary<br>- Terminal<br>- General purpose |
| Network device | Switch<br>VPN terminator | Switch<br>Router / Gateway<br>VPN |
| Host device/application | Operator workstation<br>Data historian | Operator workstation (facility manager level)<br>Advanced workstation (engineering level)<br>Application Server (handles data storage) |

# Future State of Building Automation

- **Greener & Smarter**
  - Monitoring, managing, and optimizing equipment and environments
  - Data-driven insights and decision using weather, usage, consumption, pricing, performance, etc.
- **Integrated & Automated**
  - Increased interoperability and data sharing between IT and OT, edge-to-edge, edge-to-cloud, cloud-to-cloud
- **Protected & Secure**
  - AI protects occupants and assets against physical and cyber threats
- **Enhanced Experience**
  - Easy deployment and management for facility managers
  - Intuitive and convenient for occupants

# Summary

1. IEC 62443 is relevant for building automation and controls at all levels.
2. IEC 62443 standards and ISASecure conformance certification scheme are applicable to building automation.
3. IEC 62443 standards do not duplicate any building automation cybersecurity standards.

# 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