Executive Summary

IEC 62443 Standards and ISASecure® Certification: Applicability to Building Control Systems

Download the full report from www.isasecure.org

The ISA Security Compliance Institute (ISCI) Building Controls Systems Working Group (BCSWG) recently completed a study to determine the applicability of ISA/IEC 62443 control systems cybersecurity standards to Building Control Systems (BCS). This project was initiated at the request of leading building owners and BCS suppliers based in Japan.

The objectives of the study were to determine if BCS industry initiatives for securing BCS from cyber incidents could be accelerated using ISA/IEC 62443 control systems cybersecurity standards as reference standards; and evaluate the applicability of the ISCI ISASecure® control systems cybersecurity certification scheme for BCS. The ISASecure certification scheme is designed to certify commercial-off-the-shelf (COTS) control systems/component products and security development lifecycle processes to the IEC 62443 control systems cybersecurity standards.

Supporters/participants of the study group included cybersecurity subject matter experts (SME) from Honeywell, Siemens, Schneider Electric, Johnson Controls, CABA, CSA Group, Maverick Technologies, Syska Hennessey, several consultants who are subject matter experts on BCS cybersecurity in both the commercial sector and US DoD sector and, IREO, a leading property developer/asset owner in India.

The IEC 62443 standards were written to address 'horizontal' control system technologies and not intended to be specific to a single industry sector. However, the ISA99 standards committee where the IEC 62443 standards are drafted, is heavily weighted with process industry volunteers. As a result, the vocabulary and lexicons in the IEC 62443 standards largely reflect the language of traditional process industries. A key startup task for the study group was to map the BCS industry terminology to terminology used in the IEC 62443 family of standards. The goals of the study were to:

1. Confirm that IEC 62443 standards adequately cover BCS cybersecurity requirements.
2. Identify use-cases (application areas) where IEC 62443 standards are relevant to BCS.
3. Inventory existing BCS cybersecurity standards to determine if IEC 62443 duplicates them.
4. Determine applicability of ISASecure certifications to BCS.
5. Identify duplicate/competing BAS cybersecurity certifications already in place.
6. Identify gaps in ISASecure coverage for BCS.

Study Results

1. Confirm that IEC 62443 standards adequately cover BCS cybersecurity requirements.

The study did not identify any clearly inapplicable or missing technical requirements in IEC 62443 for BCS products, noting that:

- The major difficulty in reviewing the standards was achieving a common understanding of terminology.

- Four types of components are defined in IEC 62443-4-2 including embedded devices, hosts, network devices, and applications. BCS components fit into the device type groupings as defined by the standard.
- Several members of the group are already basing their BCS product cybersecurity requirements on IEC 62443.

2. Identify use-cases where IEC 62443 are relevant to BCS

The study analyzed BCS system/device definitions using the ASHRAE Guideline 13 ‘tiers’ and ‘component types’ as a basis for comparison to control system/device definitions in IEC 62443 and concluded that:

- Many types of embedded devices involved in (HVAC) functions both at supervisory and I/O levels are relevant.
- Noted that **physical** HVAC items controlled include dampers, fans, heating and cooling coils, chillers, and boilers.
- Beyond HVAC, BCS embedded devices are relevant. They include controllers and sensors involved in "smart buildings" systems which encompass just about every BCS. Examples from a US DoD list include:

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)

3. Identify BCS cybersecurity standards that duplicate IEC 62443.

The study did not identify any other government or private sector BSC-specific cybersecurity guidelines, standards, or certifications for products in the BCS domain.

The study found that the US DoD is defining a process for listing approved operational technology (OT) products that support cyber security guidance for US DoD facilities. The requirements will drive future product cybersecurity capabilities.

4. Confirm applicability of the ISASecure certification scheme to BCS.

The group concluded that existing ISASecure Embedded Device Security Assurance (EDSA), System Security Assurance (SSA), and Security Development Lifecycle Assurance (SDLA) certifications can be applied to BCS.

The ISASecure product certifications use a 360-degree view that includes 3 assessment dimensions:

1. Audit the supplier's security development lifecycle process
2. Assess product security features and capabilities against IEC 62443 standards
3. Perform standardized testing using ISASecure-recognized test tools. Testing includes:
   a) Communication Robustness Testing (CRT).
   b) Vulnerability Identification Testing (VIT), based on US-CERT National Vulnerability Database (NVDB.)

5. Identify existing BCS product cybersecurity certification schemes.

The study found that no other BCS product cybersecurity certification scheme exists today that would be duplicated by ISASecure.

6. Identify BCS coverage gaps in the ISASecure certification scheme.

The study found that no BCS coverage gaps exist in the ISASecure certification scheme, observing that for the CRT testing dimension of ISASecure, a new measurement capability would be needed to address some BCS product requirements.

BCSWG Study Conclusions

1. IEC 62443 Standards are applicable to BCS.
2. The ISASecure certification scheme is applicable to BCS.
3. BCS cybersecurity standards and guidelines are under development by other entities but no **product-specific cybersecurity** standards exist yet.
4. The IEC 62443 standards do not duplicate any BCS industry cybersecurity standards.
5. No BCS cybersecurity certification scheme exists that would be duplicated by the ISASecure certification scheme for BCS.

Other Relevant Findings

1. BACnet (Building Automation and Control networks) will soon release a set of cybersecurity specification improvements for the commonly used BCS protocol.

2. Efforts by NIST (National Institute of Standards and Technology) on the Internet of Things (IoT) and cyber physical systems may ultimately impact BCS.

3. ASHRAE and CABA recently initiated education efforts on BCS cyber security topics, and have launched efforts to study the needs of their members related to BCS cyber security.

4. IEC 62443 is emerging as a defacto reference standard for operational technology (OT). Published References to IEC 62443 include:

   - NIST *Framework for Improving Infrastructure Cybersecurity* includes ten specific references to ISA 62443-3-3.

- NIST 800-82 *Guide to Industrial Control System Security* and NIST *Framework for Cyber Physical Systems* provide ISA 62443 a general reference.
- CABA's 2015-16 landmark study *Intelligent Buildings and Cybersecurity*, IEC 62443 is first in a list of "prominent building control cybersecurity standards".
- The Industrial Internet Consortium September 2016 *Volume G4: Security Framework* includes 42 references to IEC 62443.

Recommendation for Standards Development Organization (SDO) liaisons among industry groups

The BCSWG recognized the lengthy and expensive development process for control system cybersecurity standards, noting that the International Society for Automation ISA99 committee started the ISA/IEC 62443 standards in 2005.

ASHRAE has established a BCS cybersecurity sub-committee but a completed BCS industry cybersecurity standard does not yet exist. The BCS industry should consider using IEC 62443 as an industry reference standard. This would reduce the scope of effort for BCS SDO's and duplication of work already completed in IEC 62443 and accelerate the time to benefit for the BCS industry.

The BCSWG recommends that BCS industry SDO groups such as ASHRAE establish a formal liaison to the ISA99 standards committee to formally evaluate IEC 62443 as a reference BCS industry cybersecurity standard.