ISA Security Compliance Institute

FINAL REPORT SUMMARY

REPORT TITLE

ISA/IEC 62443 STANDARDS AND ISASECURE® CERTIFICATION: APPLICABILITY TO BUILDING CONTROL SYSTEMS

REPORT DATE: 16 JANUARY 2017

ISASecure BCS Cybersecurity Working Group (BCSWG)

www.isasecure.org

2016 ISASecure BCS Working Group

Participating Organizations

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

Background of Study

During an annual meeting at the Japanese Control Systems Security Center (a ISO/IEC 17065 accredited ISASecure certification body) a group of prominent BCS suppliers and BCS end users asked ISCI if the ISASecure cybersecurity certification scheme for control systems would be applicable to Building Control Systems (BCS). To answer the question, ISCI stood up a BCS working group (BCSWG) to study the topic and publish a report with their findings, analysis and, conclusions.

In Q1 2016 ISCI assembled a volunteer BCSWG with BCS cybersecurity subject matter experts from a cross-section of stakeholders representing BCS suppliers, academia, EPC firms, certification bodies, end-user consortia, system integrators and, consultants. ISCI is grateful to all of the organizations who supported this study.

The ISASecure certification scheme is designed to certify COTS control systems/components to the IEC 62443 control systems cybersecurity standards.

The IEC 62443 standards were written to address horizontal control system technologies; but not in any industry specific terms. 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 standards largely reflect the language of traditional process industries. Mapping the BCS industry terminology to the IEC 62443 terminology became a key startup task for the study group. Results of the BCSWG study are summarized in the following slides. Download the full study report for additional details on the study process, approach, references to documents reviewed and, other outside resources.

ISASecure BCS Study Group Objectives

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 .

The study group 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.

Analysis approach used for Objective 2

The study group 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.

Conclusions

- 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)

Conclusion

No other government or private sector BSC-specific cybersecurity guidelines, standards, or certifications for products in the BCS domain were identified by the working group.

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

Objective 4
Confirm applicability of ISASecure certification scheme to BCS

The group concluded that existing ISASecure EDSA, SSA, and 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
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

Objective 5
Identify existing BCS product cybersecurity certification schemes

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

Objective 6
Identify BCS coverage gaps in the ISASecure certification

The study group found that no BCS coverage gaps exist in the ISASecure certification scheme.

- The study group noted that for the CRT testing dimension of ISASecure, a new measurement capability would be needed to address some BCS product requirements.

Additional Findings

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

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

- 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.

IEC 62443 becoming defacto reference standards for OT

Published References to IEC 62443

- 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.

Conclusions

1. IEC 62443 Standards are applicable to BCS.
2. 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.

Additional Recommendation

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.

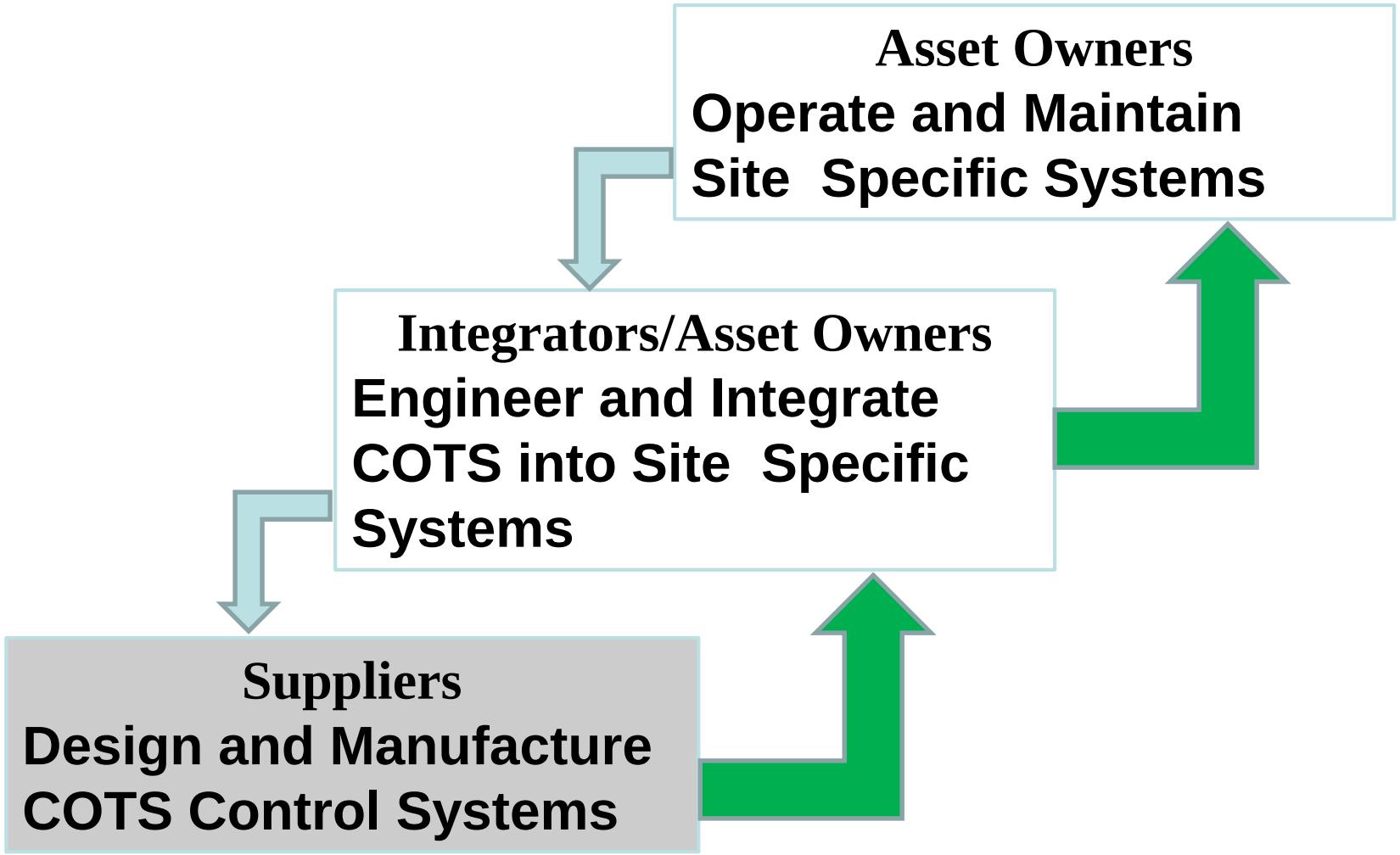
ASHRAE has established a BCS cybersecurity sub-committee but a completed BCS industry cybersecurity standard does not yet exist. The BCS industry should consider using IEC 62443 as an industry reference standard. This would reduce the scope of effort for BCS SDO's and duplication of work already completed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

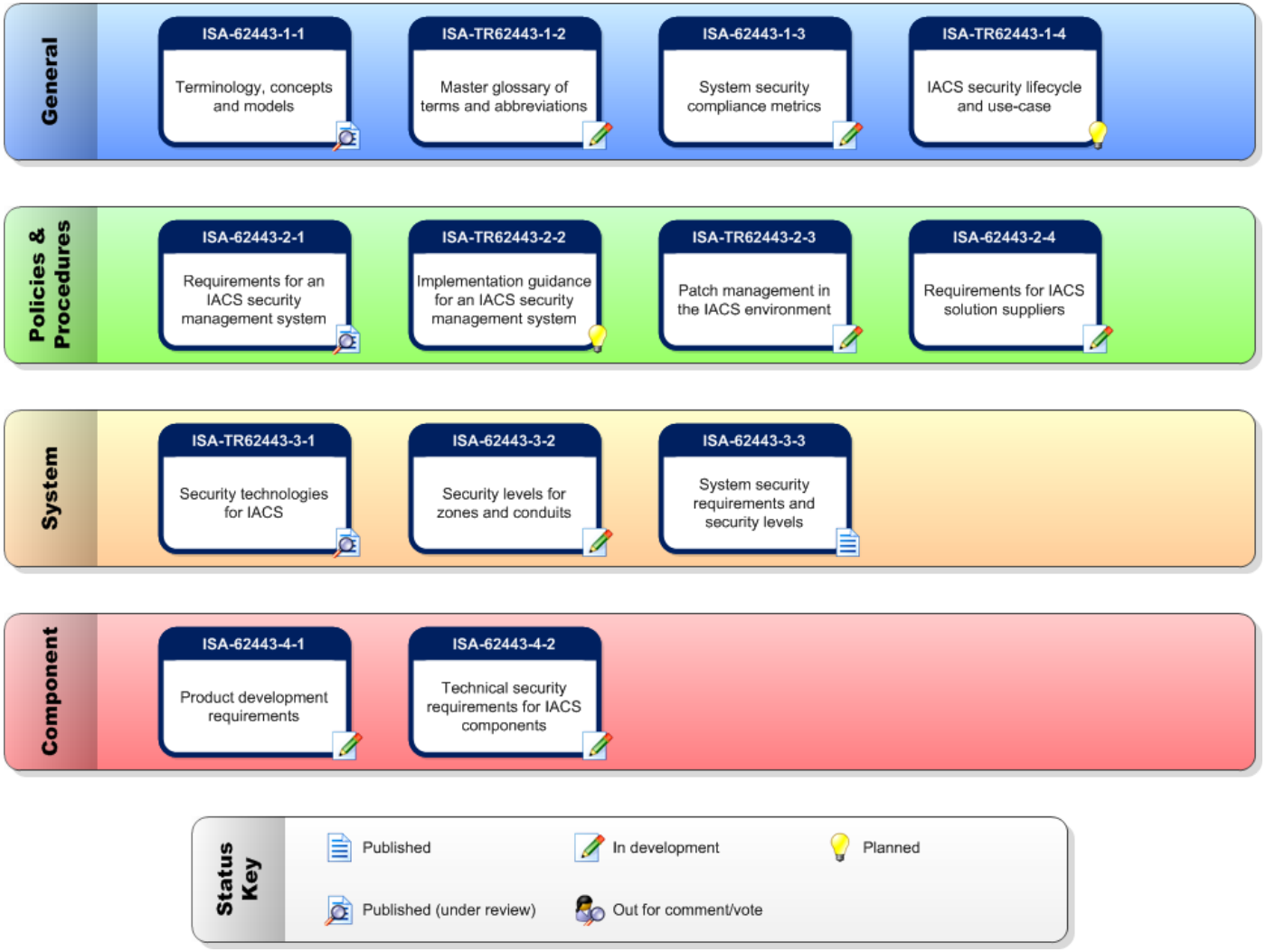
About IEC 62443 and ISASecure

- Summary of IEC 62443 Standards
- Summary of ISASecure Certifications

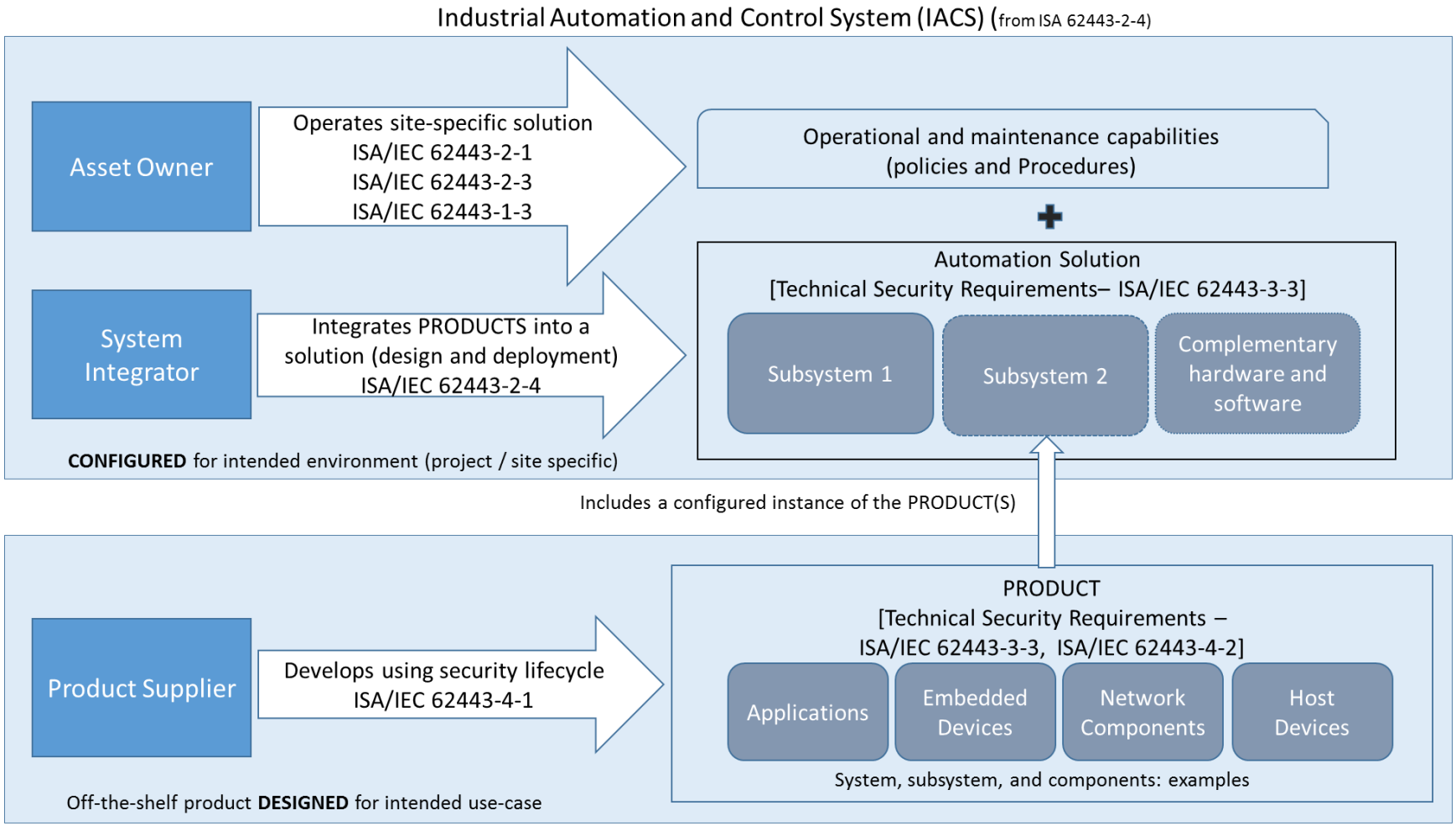
IACS Security Lifecycle



IEC 62443 Standards Family



IEC 62443 Standards Family



Certification….Why Certify COTS Products?

1) *Security capabilities are independently assessed and certified by experts at ISO17065 accredited ISASecure labs.*

2) *Reduces effort for end user (and integrators) to validate and verify security capabilities.*

3) *Objective metric for security capabilities based on industry standards. (hundreds of years of SME and knowledge codified into IEC 62443-x-x from hundreds of committee participants).*

COTS=Commercial Off the Shelf

Three ISASecure® certifications available

1. **Embedded Device Security Assurance (EDSA)**
   product certification
   IEC 62443-4-2
   IEC 62443-4-1

2. **System Security Assurance (SSA)**
   product certification
   IEC-62443-3-3, IEC 62443-4-1, IEC 62443-4-2

3. **Security Development Lifecycle Assurance (SDLA)**
   process certification
   IEC-62443-4-1

Copies of the complete study report are available for free download at:

www.isasecure.org

For more information please contact the ISCI managing director.

Andre Ristaino, ISCI Managing Director

67 T.W. 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