ISASecure®

Securing the Supply Chain

for Commercial off the Shelf (COTS)
Automation, Control Devices and Systems
Using ISA/IEC 62443 Standards

www.isasecure.org

Andre Ristaino
Managing Director,
ISA Security Compliance Institute
aristaino@isa.org

About the 62443 Standards

- ISA99 committee chartered in 2005 at ISA to develop cybersecurity standards for industrial automation and controls. Technology horizontal applicable to almost any automation but written mostly by process engineers.
- In 2009 ISA99 committee adopted IEC naming conventions and formatting to accelerate completion of standards
- Standards published by ISA as ANSI/ISA 62443-x-x and adopted by the International Electrotechnical Commission (IEC) as IEC 62443-x-x
- ISA99 committee continues to develop additional standards for the 62443 family of standards; and perform periodic maintenance.

aristaino@isa.org

Important Definitions from IEC 62443-4-2

- Update - incremental hardware or software change in order to address a security vulnerability, a bug, 616 reliability or operability issue

- Upgrade - incremental hardware or software change in order to add a new feature

aristaino@isa.org

Assessment and Certification of a Product

First time Assessment

- Product must be in the scope of an ISASecure SDLA certification (development process certification to IEC 62443-4-1)
- Product meets security capability requirements of ISASecure CSA (IEC 62443-4-2)
- Product meets test requirements defined in 62443-4-1 and any additional testing done by certification body
- Certificate is issued for the product model/version number and declared/specified configuration.

aristaino@isa.org

Maintenance of Product Certification

Ongoing

- Product must be in the scope of an ISASecure SDLA certification (development process certification to IEC 62443-4-1)
- The product and any UPDATES remain certified as long as the product SDLA remains valid. The SDLA is audited every three years.
- The product must be re-assessed if an UPGRADE is issued
- A new certificate is issued for the UPGRADED product model/version number and declared/specified configuration

ISASecure EDSA is replaced by CSA

- EDSA was original ISASecure Embedded Device Security Assurance certification.
  - First standards-based cybersecurity certification for OT
  - Specific to embedded devices only
  - Created in 2008, prior to publication of IEC 62443-4-2 and ISASecure committed to aligning with IEC 62443-4-2 when published

- CSA is the ISASecure Component Security Assurance certification.
  - Certifies to the IEC 62443-4-2 and IEC 62443-4-1 standards
  - Addresses all four component types defined in IEC 62443-4-2
  - Hosts, embedded devices, applications, and network devices
  - ISASecure was aligned with IEC 62443-4-2 when published this year.

aristaino@isa.org

Third-party (CB) CRT testing discontinued

ISASecure continuously seeks to reduce the cost and effort to assess and certify COTS products; remove any non-value added activities

Removed third-party (CB) CRT testing

- Commercially available CRT tools do not cover all protocols
- Assessments used a combination of third party testing and then audits of supplier artifacts for the protocols not covered by the ISASecure recognized test tools
- This approach added cost; suppliers were doing the same testing as part of their SDL development and release processes
- ISASecure augmented assessor guidance for process audits (IEC 62443-4-1) on supplier testing practices. CB

Benefit

- Removes redundant testing (supplier + CB)
- Reduces CB assessment effort (and cost) by about 20%
- Aligns with the concept of improving supplier development and release processes

aristaino@isa.org

ISASecure Certification Fees Reduced

Net result of new registration/logo fee structure is more than 50% reduction over the life of a product.

Example
Old fee for embedded device

- Member fee $7,500 first time / $2,500 maintenance
- Non-member $12,500 first time / $3,000 maintenance

- **New fee for embedded device**
- Member and Non-member fee is the same: $1,200 annual logo fee starting with first time certification

Benefit

- Same price for members and non-members
- Reduces lifetime cost by over 50%
- Aligns with the lifecycle concept of IEC 62443 standards

aristaino@isa.org

Retiring CRT Tool Recognition Program

The policy in the latest version of ISASecure no longer requires CB's to perform independent CRT testing for ISASecure assessments

1. No new CRT tools will be evaluated
2. Recognized CRT tools currently listed and future releases will be recognized going forward for maintenance of certifications
3. These are all great CRT tools and we thank the CRT tool vendors for supporting the ISASecure certification program
4. CRT tools will continue to be valuable for product suppliers in their development and testing processes
5. The CB's assessors will audit supplier's test processes and results.

aristaino@isa.org

Transition Policies and Dates

The transition policy, new pricing, and effectivity dates will be published and posted on the ISASecure website by June 7, 2019.

The new ISASecure certification specifications will be published and posted on the ISASecure website by June 7, 2019.

www.isasecure.org

aristaino@isa.org

New Initiatives for ISASecure

- ISCI rollout of BMS certification
- DoD Building Management Systems
- OPAF (Open Process Automation Forum)

aristaino@isa.org

International Society of Automation

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

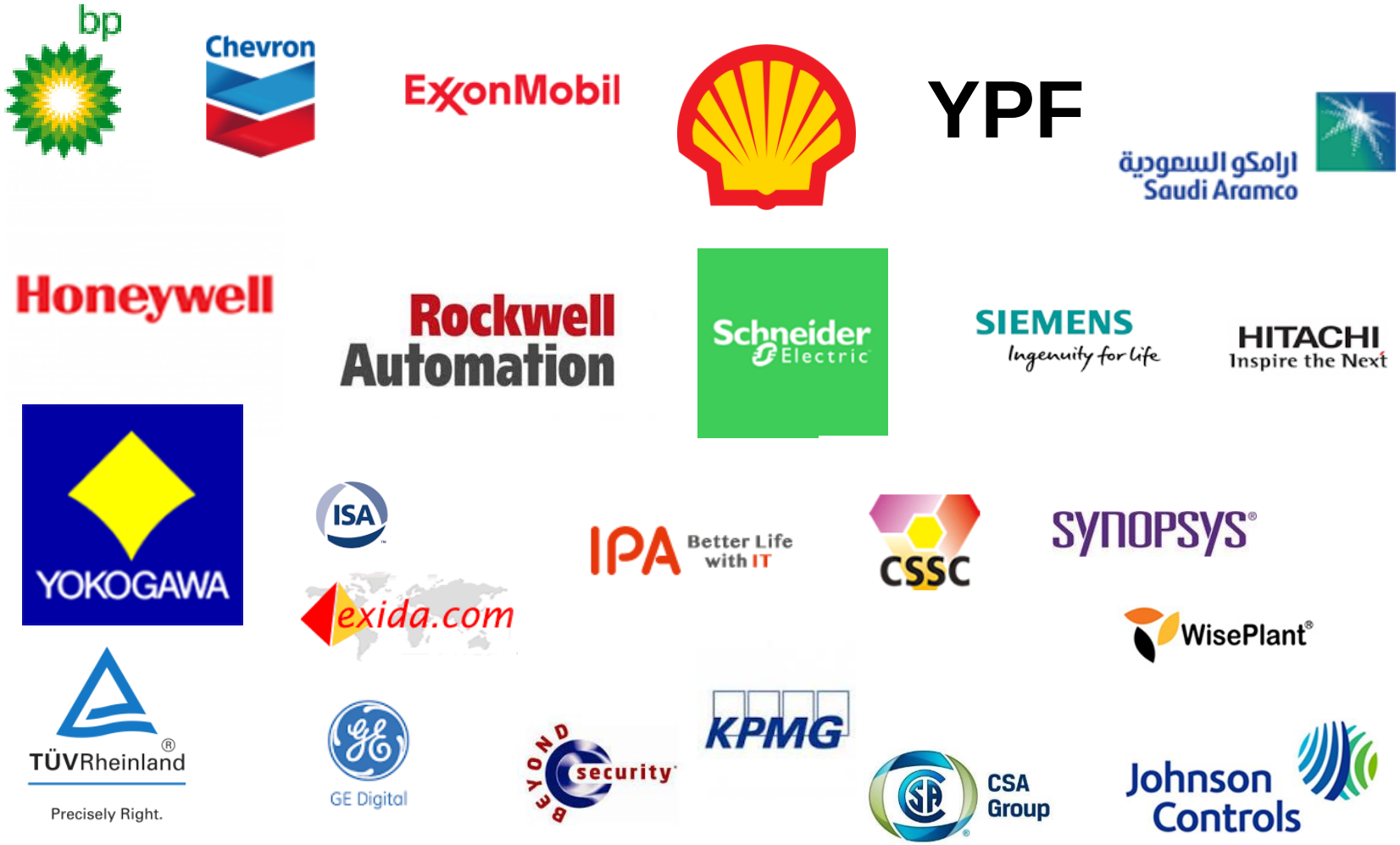
ISA Security Compliance Institute

ISA Security Compliance Institute

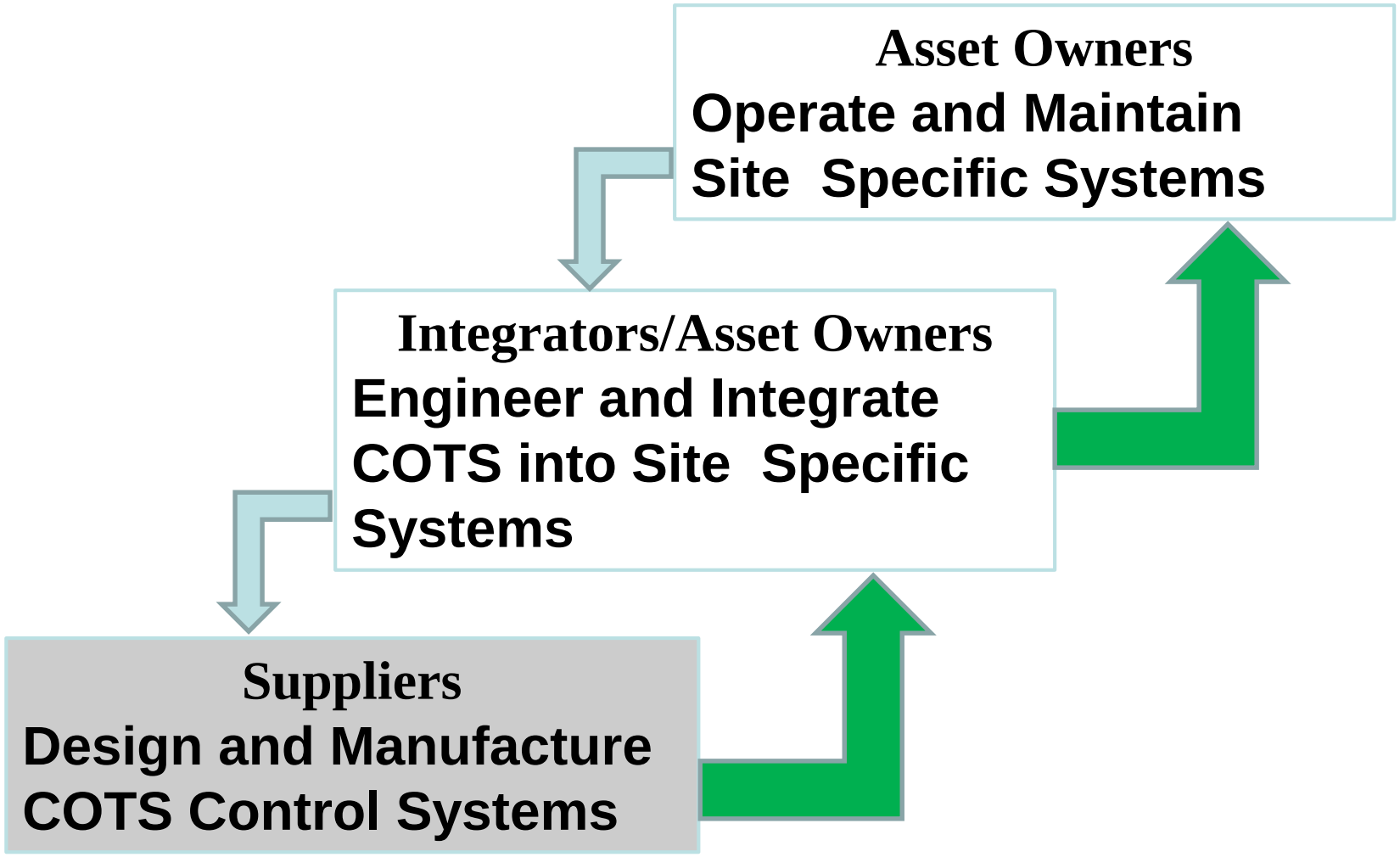
Wholly owned non-profit subsidiary of ISA

Conformity Assessment to ISA/IEC 62334 standards

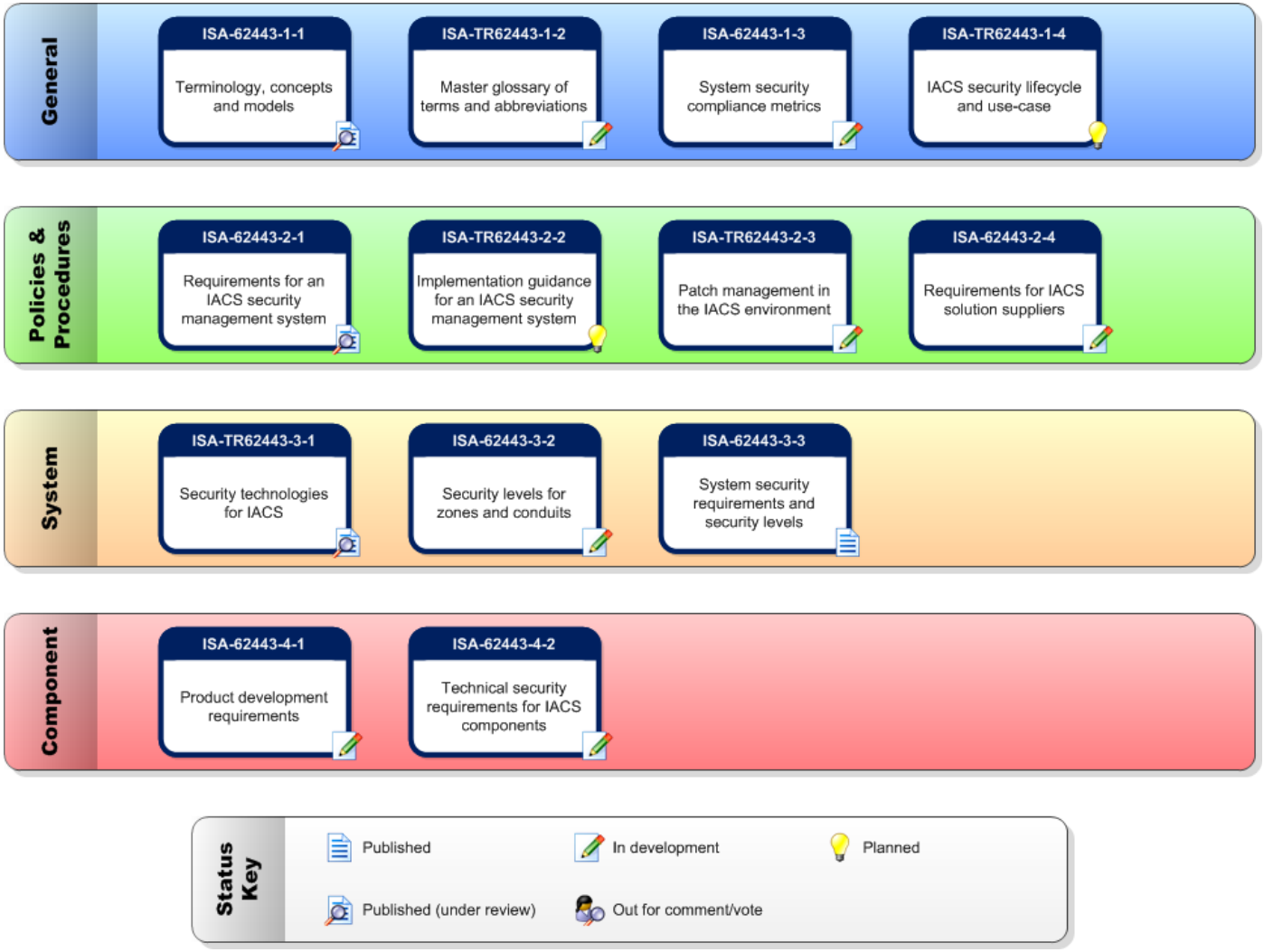
ISASecure® Supporters – past & present



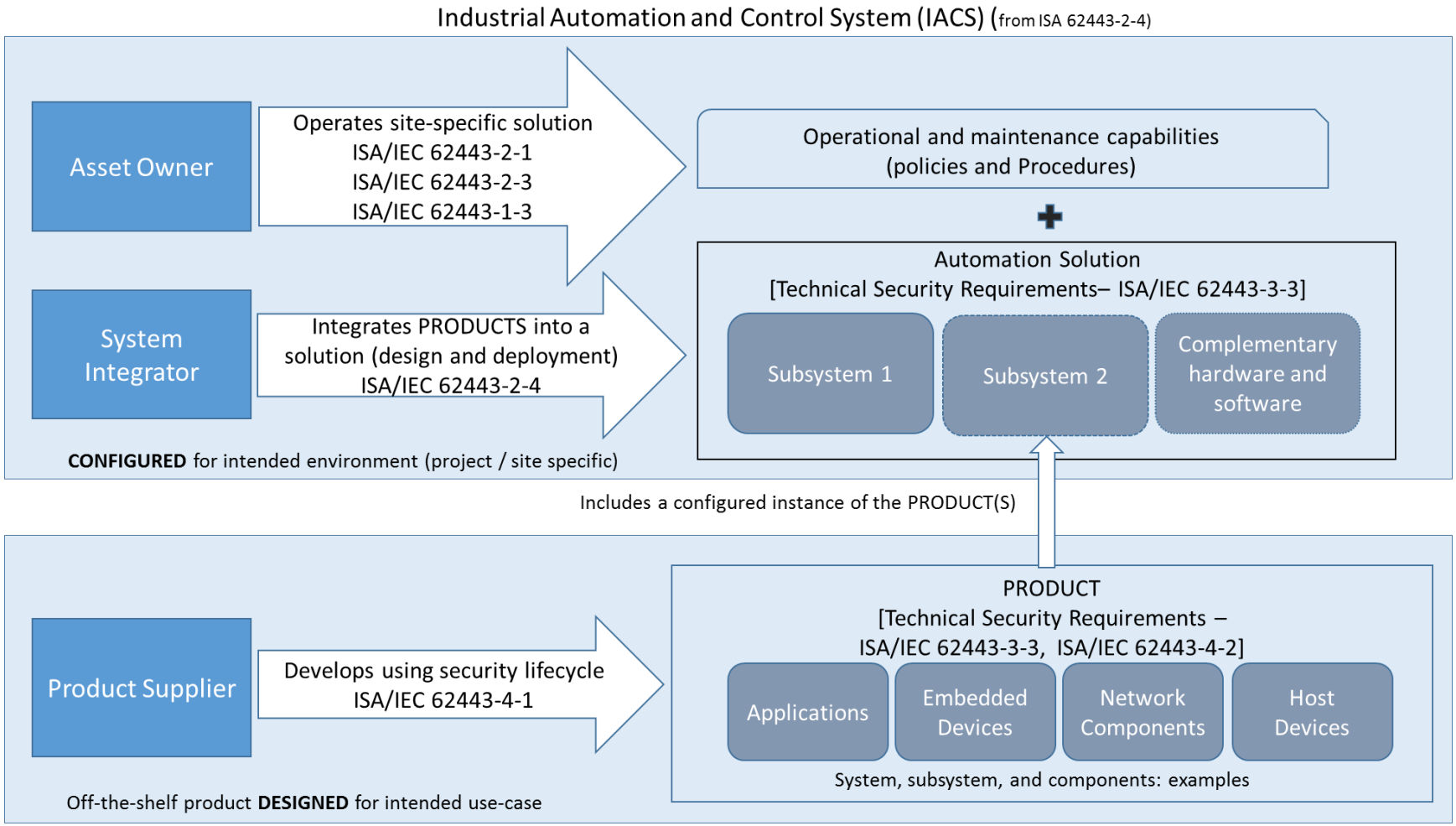
Automation System Security Lifecycle



ISA/IEC 62443 Standards Family



ISA/IEC 62443 Standards Family



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

ISASecure Recognized Test Tools

Why Assess and Certify Products?

- *Is this product robust?*
- *Is a crash survivable?*
- *Do the systems perform as advertised?*
- *Standards based measures.*

Why Certify Automation Products?

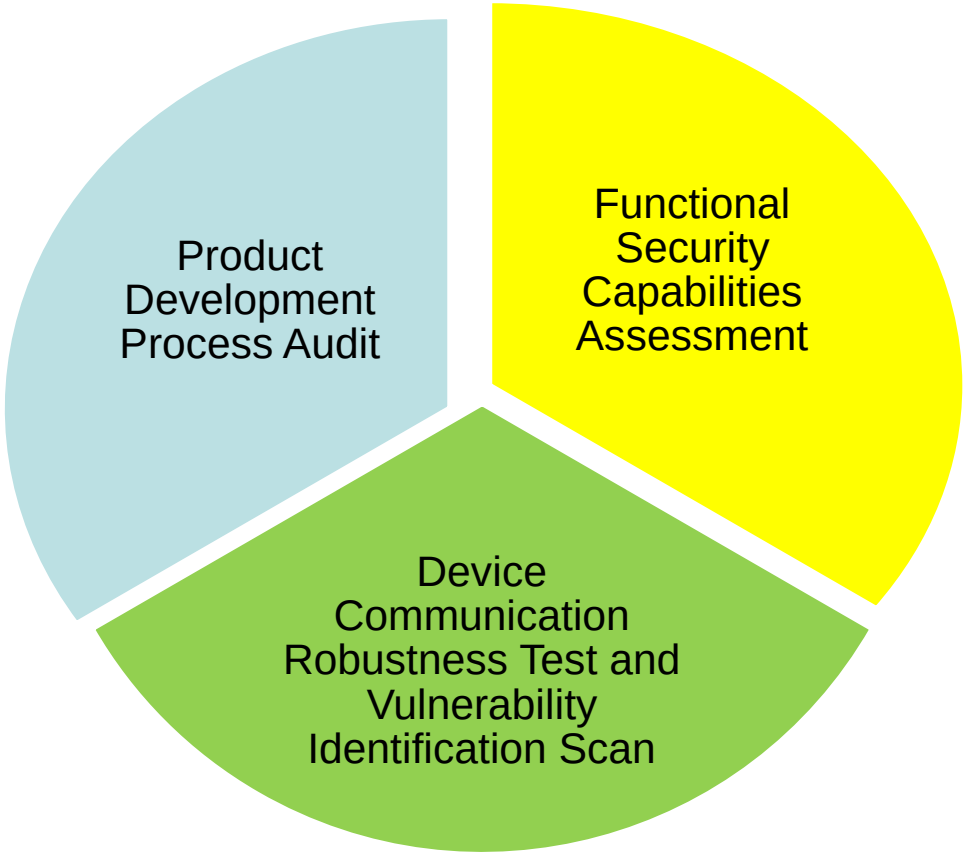
1. Security capabilities are independently assessed and certified by experts at accredited ISASecure labs

2. Reduces effort for end user to validate and verify security capabilities. (scarcity of talented cybersecurity expertise)

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

One specification, one service mark, one assessment

360 Degree Product Evaluation



More than just testing!

Product Certification – What you get.

- Robust against network attacks and free from known security vulnerabilities
- Meets requirements of ISA/IEC 62443 international standards
- Independent certification of security capability level (SL) as defined by the ISA/IEC 62443 standards

End-user Benefits and Value

- Simplifies procurement specification process
- End users easily understand standards-based product cybersecurity capabilities
- Capabilities independently validated by external entity
- Confidence that security features will evolve over time
- ISCI provides a forum where end-users can ensure that ISA/IEC 62443 standards are implemented as intended
- Forum where an end-user can include their company specific requirements in certification specifications

Supplier Benefits and Value

- Differentiate solutions to marketplace
- Assurance products meet standards-based (ISA/IEC 62443) cybersecurity requirements that are maintained over the product lifecycle
- Cybersecurity is a dimension of product quality
- Suppliers will soon face product liability accountabilities

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

Sampling of ISASecure® Certified Products

azbil

北京康吉森自动化设备技术有限责任公司
Beijing Consen Automation Control Co.,Ltd.

Honeywell

HIMA

HITACHI
Inspire the Next

Honeywell

Honeywell

Honeywell

More ISASecure® Certified Products

Schneider Electric

Schneider Electric

Schneider Electric

YOKOGAWA

YOKOGAWA

TOSHIBA

Leading Innovation

ABB

EMERSON

Delta V

ISASecure Certified Development Organizations

5 Sites

1 Site

2 Sites

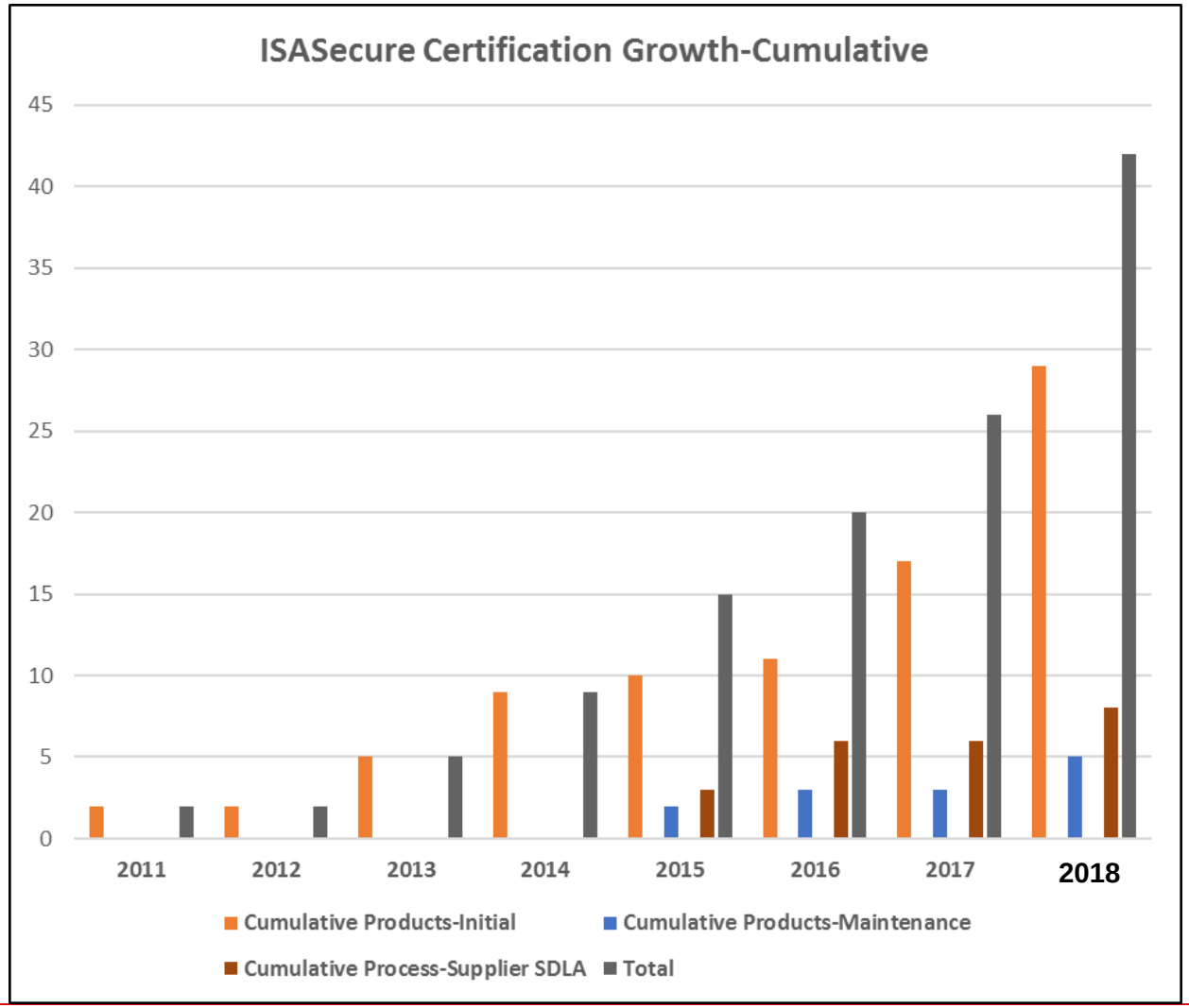
ISASecure Building Control Systems Working Group

Participating Organizations

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



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