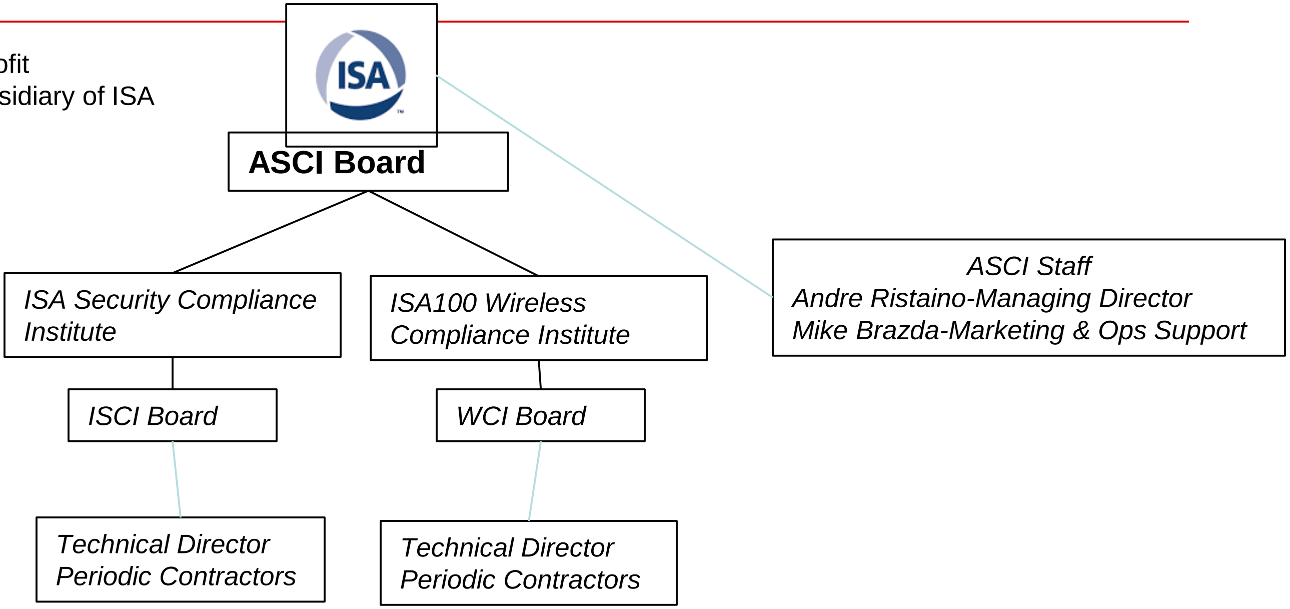
Automation Standards Compliance Institute

501 c 6 Not for profit
Conformity Assessment Subsidiary of ISA



ASCI Board

ISA Security Compliance Institute

ISA100 Wireless Compliance Institute

ASCI Staff
Andre Ristaino-Managing Director
Mike Brazda-Marketing & Ops Support

ISCI Board

WCI Board

Technical Director
Periodic Contractors

Technical Director
Periodic Contractors

Accreditation Bodies
- *ANSI/ANAB*
- *JAB*
- *DAkkS*

Certification Bodies
- *TUV Rheinland*
- *Exida*
- *CSSC-CL*
- *CSA Group*

Test Tool Suppliers
- *GE Digital-Achilles*
- *Synopsis-Defensics*
- *Hitachi-Raven*
- *See Beyond=Beyond Secure*
- *CNCERT-Acheron*

Certification In-house-via training; shared revenue

In-house developed test tools

ISASecure®

Securing the Supply Chain

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

www.isasecure.org

Andre Ristaino
Managing Director,
ISA Automation Standards Compliance Institute

Agenda

- About ISA Security Compliance Institute
- Structure of ISASecure scheme
- IEC 62443 Standards and structure
- Description of ISASecure Certifications
- ISASecure Roadmap
- Website www.isasecure.org

ISASecure® Founding Companies

SIEMENS
Ingenuity for life

ExxonMobil

Chevron

bp

Schneider Electric

YOKOGAWA

Honeywell

Rockwell Automation

ISA

ISA99 Committee Liaison

ISASecure® Supporter Companies

IPA Better Life with IT

ارامكو السعودية
Saudi Aramco

KPMG

CSSC

WisePlant®

CODENOMICON

YPF

Supporters-ISCI Member Companies

ISCI membership is open to all organizations

- Strategic membership
- Technical membership (includes CB's)
- Government/Associate membership
- Adopter/Supporter

Member organizations

- Chevron
- Bedrock Automation
- Aramco Services
- CSA Group
- CSSC
- exida
- ExxonMobil
- Honeywell
- IT Promotion Agency, Japan
- KPMG Consulting Ltd. Japan
- Schneider Electric
- Synopsis
- TUV Rheinland
- WisePlant HQ
- Yokogawa
- YPF
- ISA99 Committee Liaison

No Membership Required

Asset owners *specify* ***ISASecure*** *in procurement specifications and/or choose from list of certified products on ISASecure website.*

Suppliers *submit products to an ISASecure certification body of choice.*

Certified products are listed on ISASecure website and certification body website.

ISCI Organization

501 c 6 Not for profit
Conformity Assessment Subsidiary of ISA

ISCI Governing Board

Chairman – Kenny Mesker, Chevron

Vice-chairman – Johan Nye, ExxonMobil

Technical Chairman – Kevin Staggs, Honeywell

Marketing Chairman – Dan Desruisseaux, Schneider Electric

ISA99 Committee Liaison – Eric Cosman

Staff Managing Director – Andre Ristaino (non-voting)

Internationally Accredited ISO/IEC 17065 Conformance Scheme

ISASecure certification programs are supported by labs accredited to ISO/IEC 17065 and ISO/IEC 17025 lab operations by international ISO/IEC 17011 accreditation bodies (AB).

- Provides global recognition and acceptance of ISASecure certifications
- ISASecure can scale on a global basis using independent CB's
- Independent ISO/IEC 17011 accreditation by global accreditation bodies ensures certification process is open, fair, credible, and robust.
- AB and CB agreements continue to expand.

ilac-MRA

DAkkS
Deutsche
Akkreditierungsstelle
D-PL-18345-01-00

ANSI
ANSI Accredited Program
PRODUCT CERTIFICATION

ANAB
ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS
CERTIFICATION BODY

PROD
JAB

ISO/IEC 17065 / ISO/IEC 17025 Accredited Certification Bodies

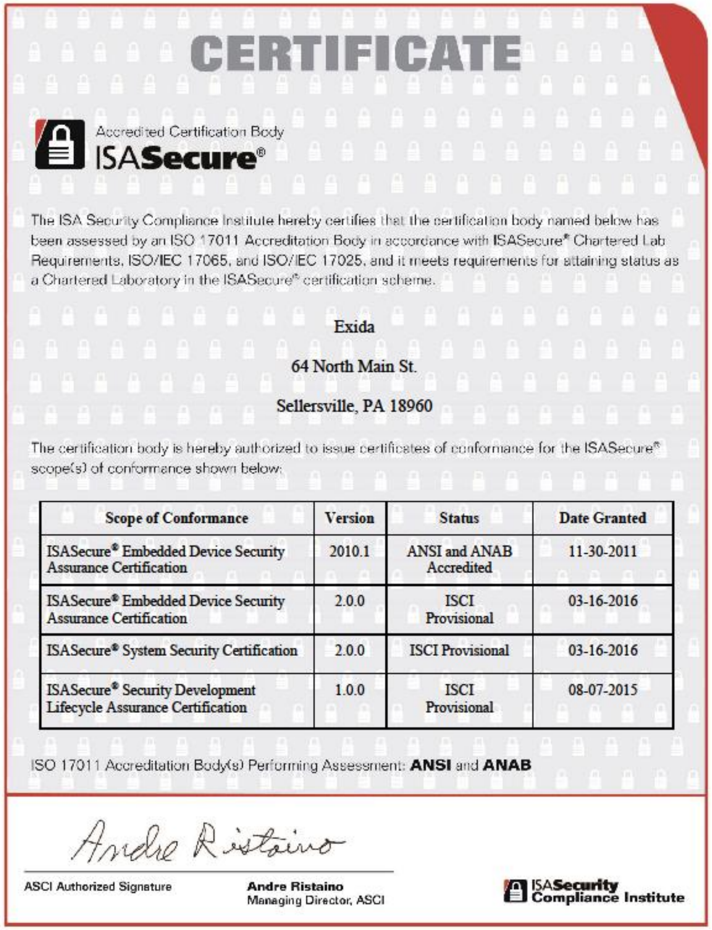
ISASecure Certification Body	Accrediting Authority	Location(s)
Exida, LLC	ANSI ANAB	Global operations – HQ Sellersville, PA USA
CSSC-CL	Japan Accreditation Board (JAB)	Japan and AP region- HQ Tokyo, Japan
TUV Rheinland	DAkkS	Global operations – HQ Cologne, Germany

Additional Certification Bodies are in Accreditation Process.

exida

exida.com, LLC
HQ Sellersville, PA/global locations

The first ISASecure chartered lab, accredited in 2011



CERTIFICATE

Accredited Certification Body
ISASecure®

The ISA Security Compliance Institute hereby certifies that the certification body named below has been assessed by an ISO 17011 Accreditation Body in accordance with ISASecure® Chartered Lab Requirements, ISO/IEC 17065, and ISO/IEC 17025, and it meets requirements for attaining status as a Chartered Laboratory in the ISASecure® certification scheme.

Exida
64 North Main St.
Sellersville, PA 18960

The certification body is hereby authorized to issue certificates of conformance for the ISASecure® scope(s) of conformance shown below:

Scope of Conformance	Version	Status	Date Granted
ISASecure® Embedded Device Security Assurance Certification	2010.1	ANSI and ANAB Accredited	11-30-2011
ISASecure® Embedded Device Security Assurance Certification	2.0.0	ISCI Provisional	03-16-2016
ISASecure® System Security Certification	2.0.0	ISCI Provisional	03-16-2016
ISASecure® Security Development Lifecycle Assurance Certification	1.0.0	ISCI Provisional	08-07-2015

ISO 17011 Accreditation Body(s) Performing Assessment: **ANSI** and **ANAB**

Andre Ristaino

ASCI Authorized Signature

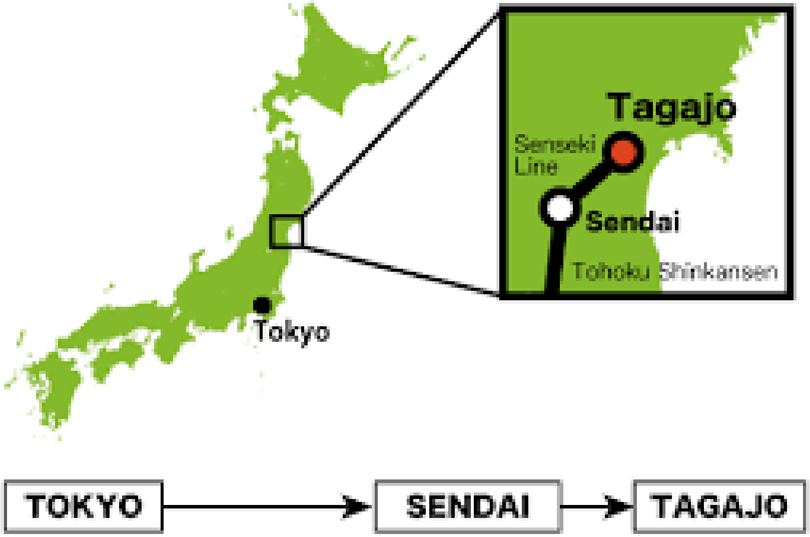
Andre Ristaino
Managing Director, ASCI

ISASecurity Compliance Institute

CSSC-CL

Control Systems Security Corporation
Tokyo & Tagajo City Japan

CSSC



TUV Rheinland

TUV Rheinland Headquarters
Cologne Germany

TÜVRheinland®

Precisely Right.

Why Certify COTS 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 IEC 62443-x-x from hundreds of committee participants.)

One specification, one service mark, one assessment

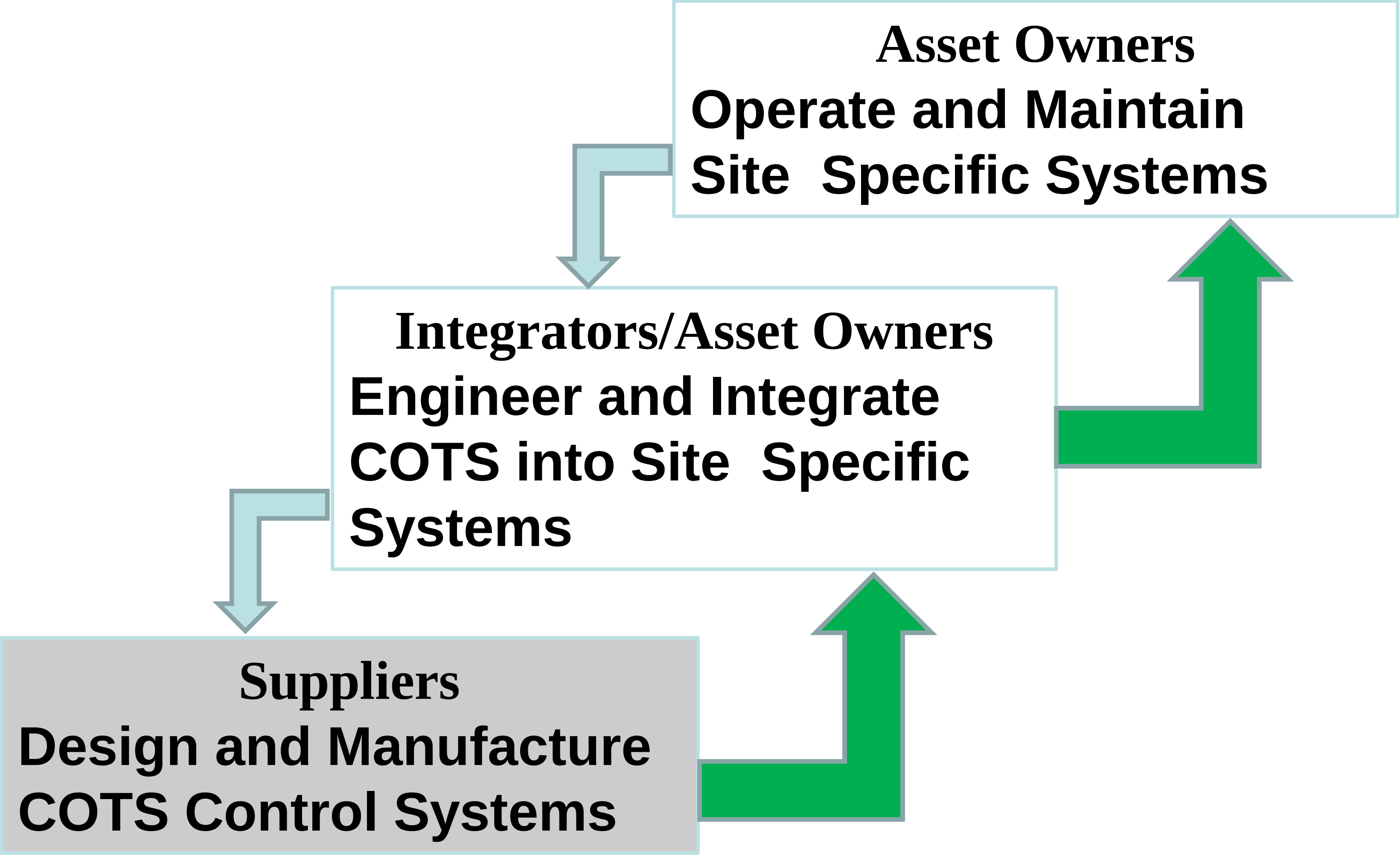
End-user Benefits and Value

- Simplifies procurement specification process
- End users 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 cybersecurity requirements that are maintained over the product lifecycle
- Cybersecurity is a dimension of product quality
- Suppliers will soon face product liability accountabilities

IACS Security Lifecycle



Asset Owners

Operate and Maintain Site Specific Systems

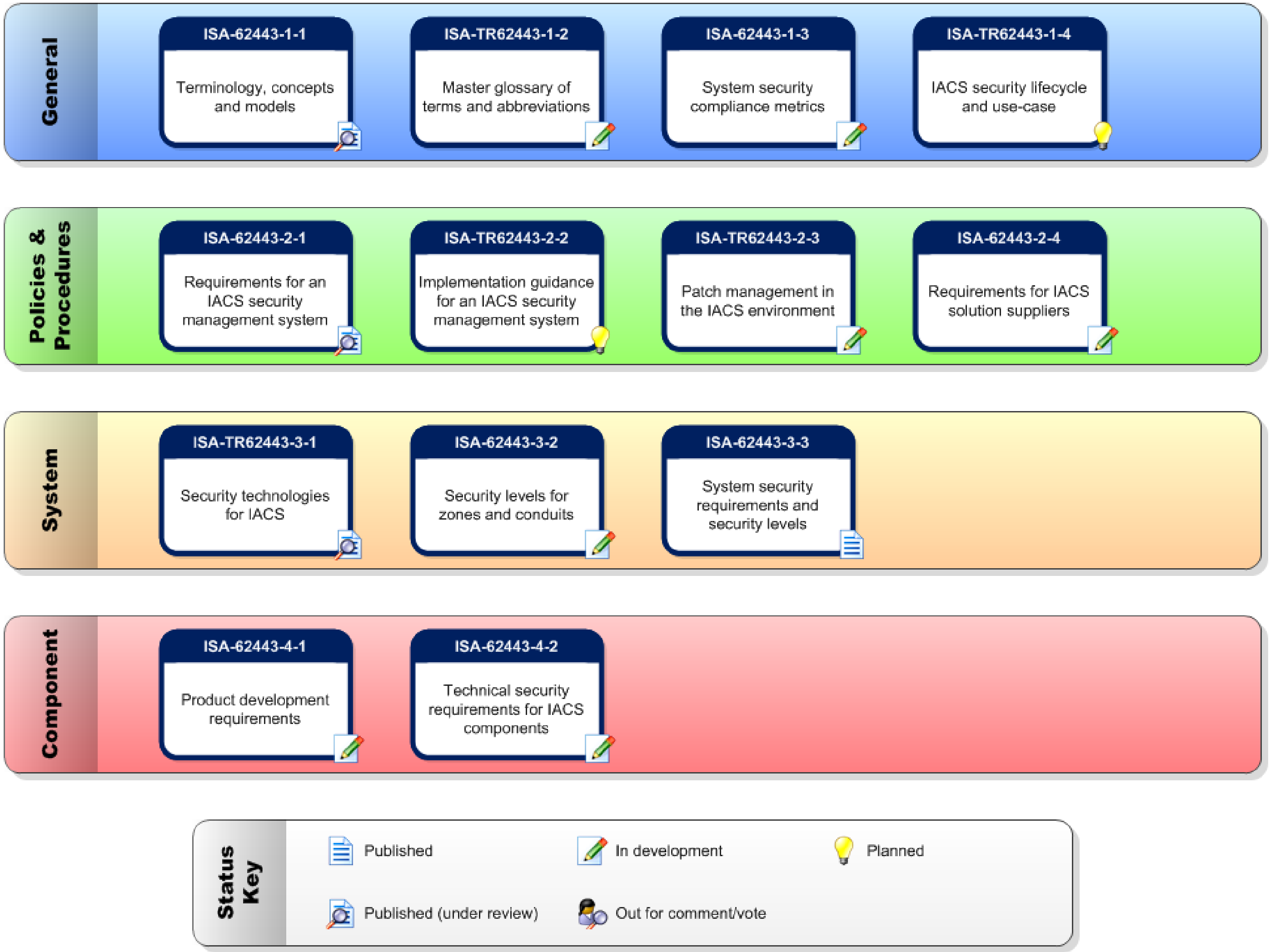
Integrators/Asset Owners

Engineer and Integrate COTS into Site Specific Systems

Suppliers

Design and Manufacture COTS Control Systems

IEC 62443 Standards Family

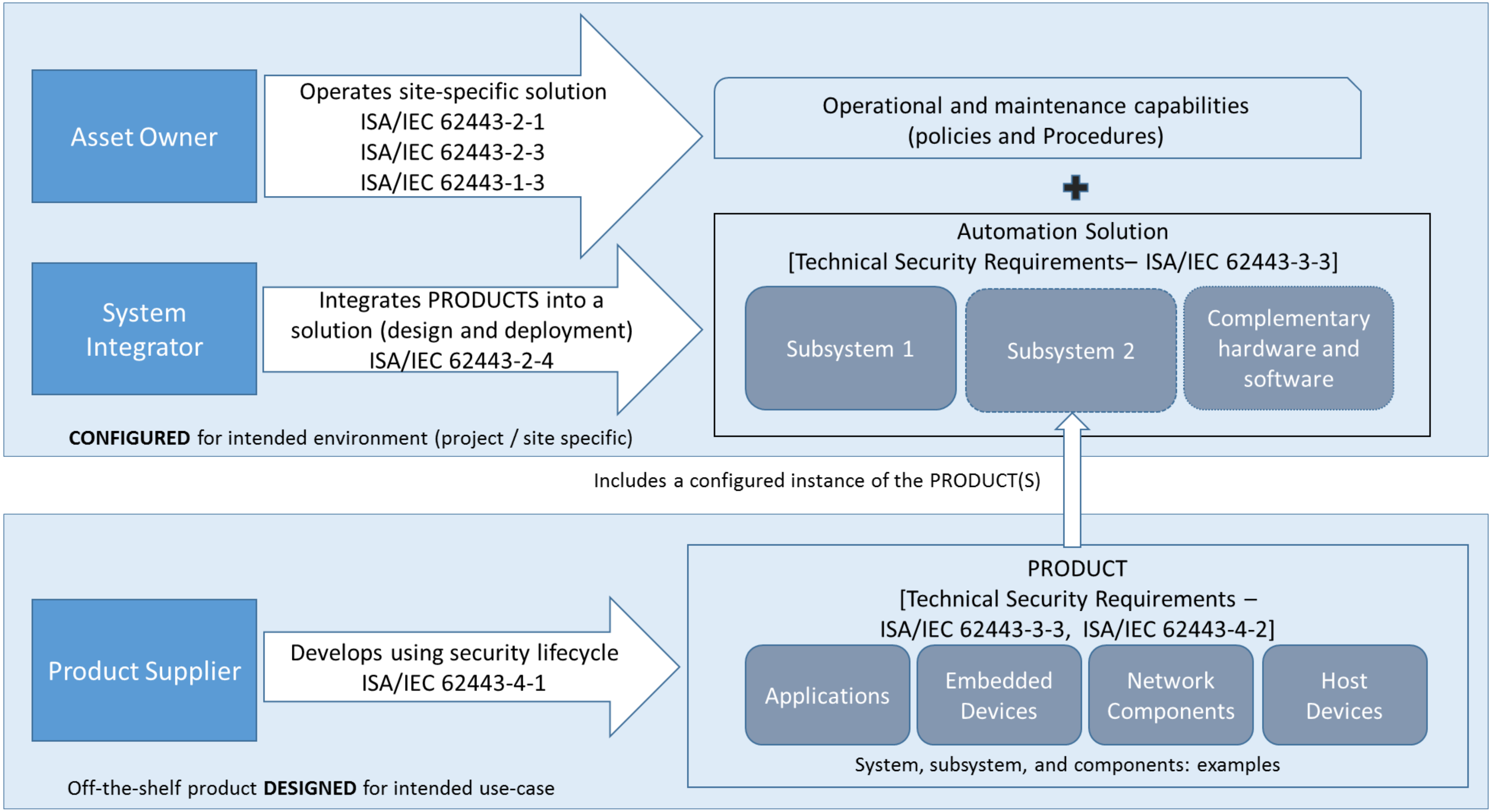


General	ISA-62443-1-1 Terminology, concepts and models 🔍	ISA-TR62443-1-2 Master glossary of terms and abbreviations ✎	ISA-62443-1-3 System security compliance metrics ✎	ISA-TR62443-1-4 IACS security lifecycle and use-case 💡
Policies & Procedures	ISA-62443-2-1 Requirements for an IACS security management 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	

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)

✚

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

Subsystem 1

Subsystem 2

Complementary hardware and software

System Integrator

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

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

Three ISASecure® certifications available

1. Embedded Device Security Assurance (EDSA) product certification

   IEC 62443-4-2

   IEC 62443-4-1

   Vulnerability Identification Test
   + Communication Robustness Test

2. System Security Assurance (SSA) product certification

   IEC-62443-3-3

   IEC 62443-4-1

   IEC 62443-4-2

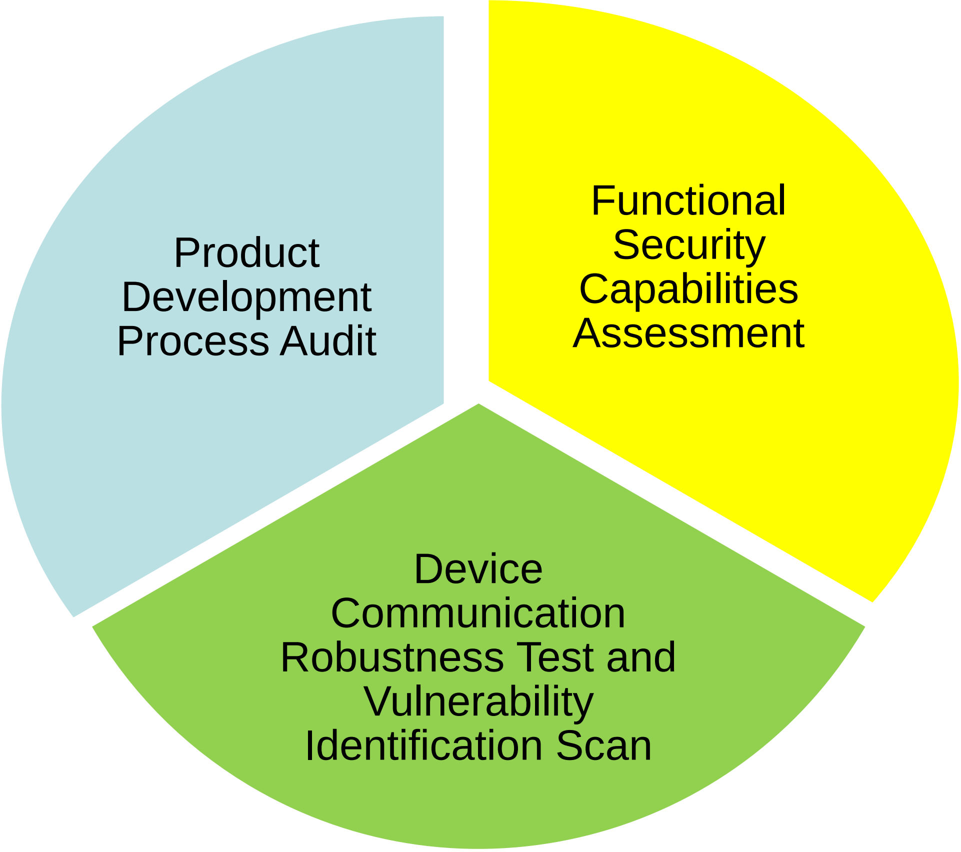
   Vulnerability Identification Test
   + Communication Robustness Test

3. Security Development Lifecycle Assurance (SDLA)

   process certification

   IEC-62443-4-1

360 Degree Product Evaluation



Product Development Process Audit

Functional Security Capabilities Assessment

Device Communication Robustness Test and Vulnerability Identification Scan

More than just testing!

ISASecure®
Embedded Device Security Assurance (EDSA)

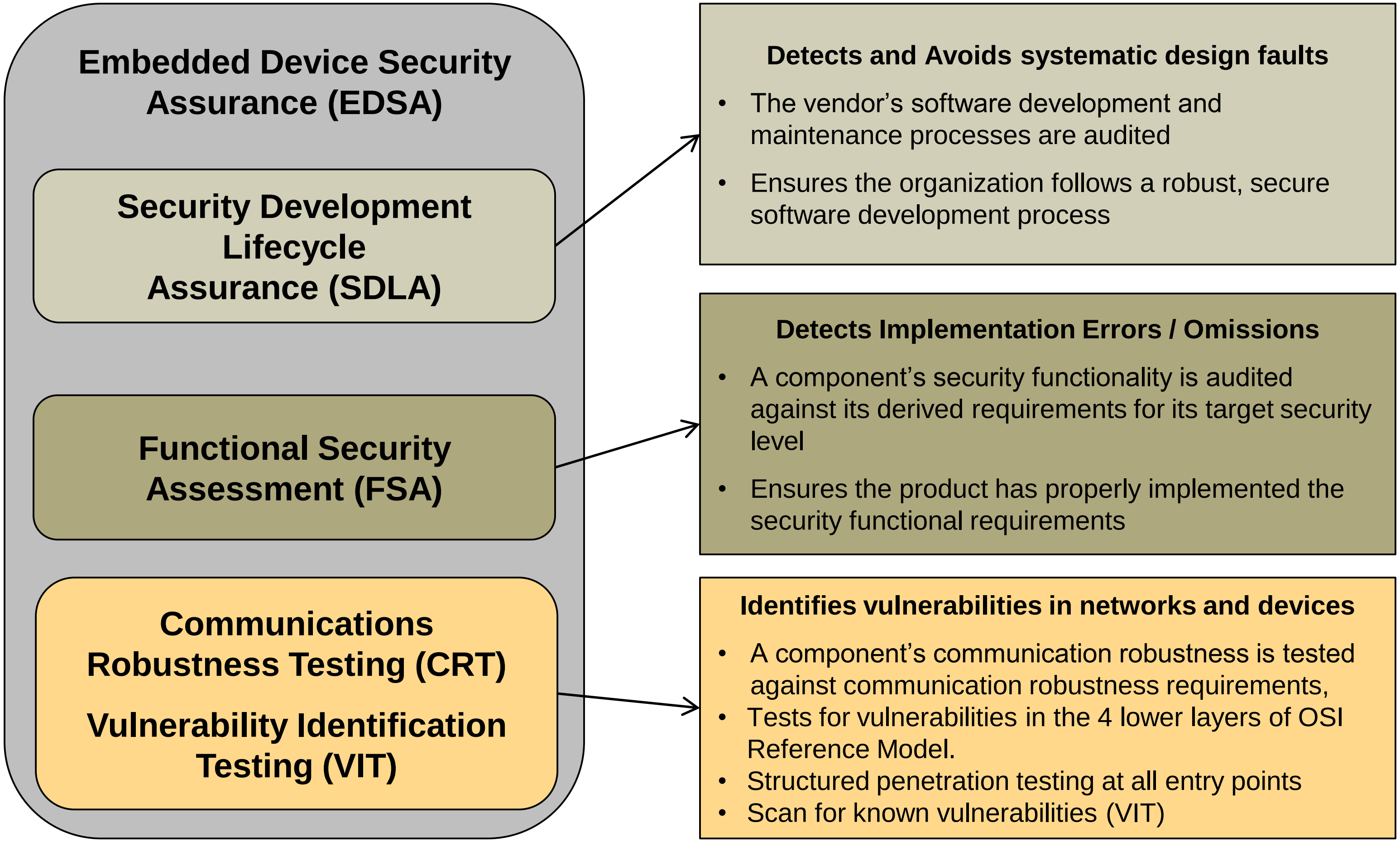
IEC 62443-4-1
IEC 62443-4-2

EDSA

- Certification that the supplier’s product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of IEC 62443-4-1 and IEC 62443-4-2 for embedded devices (will be revised when IEC 6443-4-2 is published)
- Independent certification of the product’s security capabilities and security capability level (SL) as defined by the IEC 62443 standards

ISASecure EDSA Certification Program

ISASecure



Embedded Device Security Assurance (EDSA)

Security Development Lifecycle Assurance (SDLA)

Detects and Avoids systematic design faults

- The vendor’s software development and maintenance processes are audited
- Ensures the organization follows a robust, secure software development process

Functional Security Assessment (FSA)

Detects Implementation Errors / Omissions

- A component’s security functionality is audited against its derived requirements for its target security level
- Ensures the product has properly implemented the security functional requirements

Communications Robustness Testing (CRT)

Vulnerability Identification Testing (VIT)

Identifies vulnerabilities in networks and devices

- A component’s communication robustness is tested against communication robustness requirements,
- Tests for vulnerabilities in the 4 lower layers of OSI Reference Model.
- Structured penetration testing at all entry points
- Scan for known vulnerabilities (VIT)

ISASecure®
System Security Assurance (SSA)

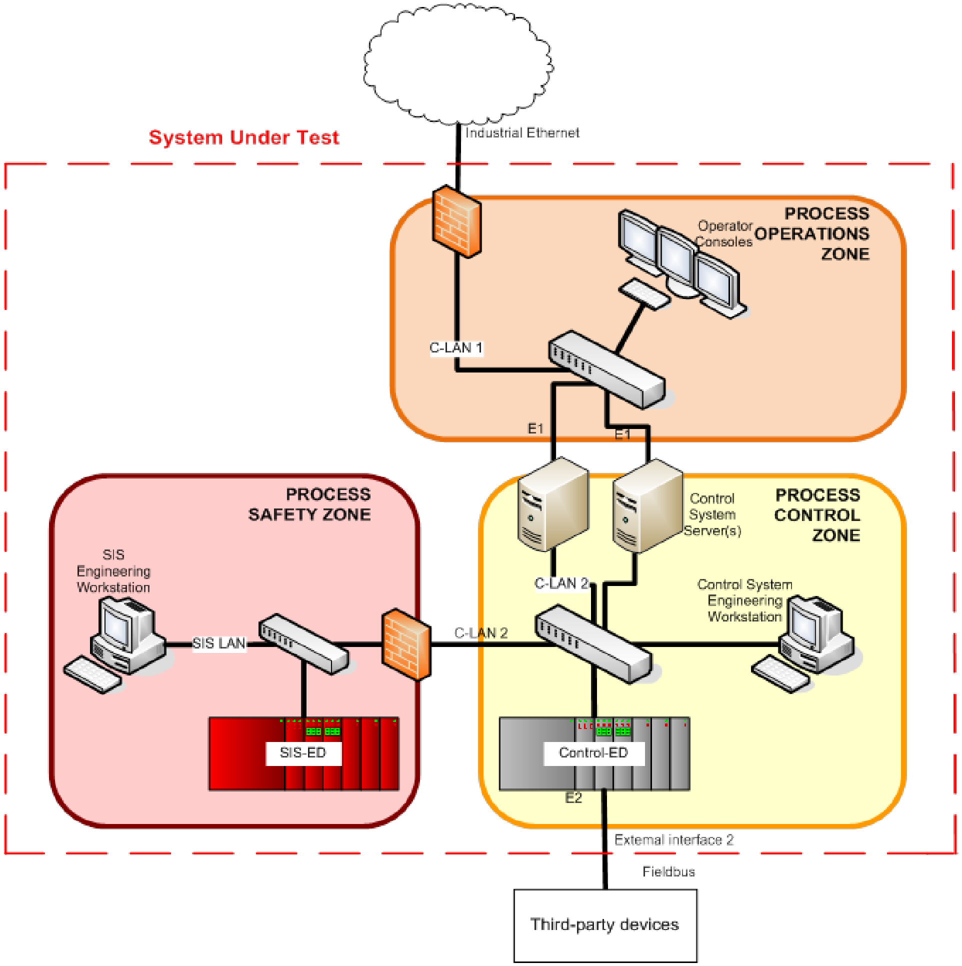
IEC 62443-3-3
IEC 62443-4-1
IEC 62443-4-2

SSA Overview

- Certification that the supplier’s product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of IEC 62443-3-3, IEC 62443-4-1 and, IEC 62443-4-2
- Independent certification of the product’s security capabilities and security capability level (SL) as defined by the IEC 62443 standards

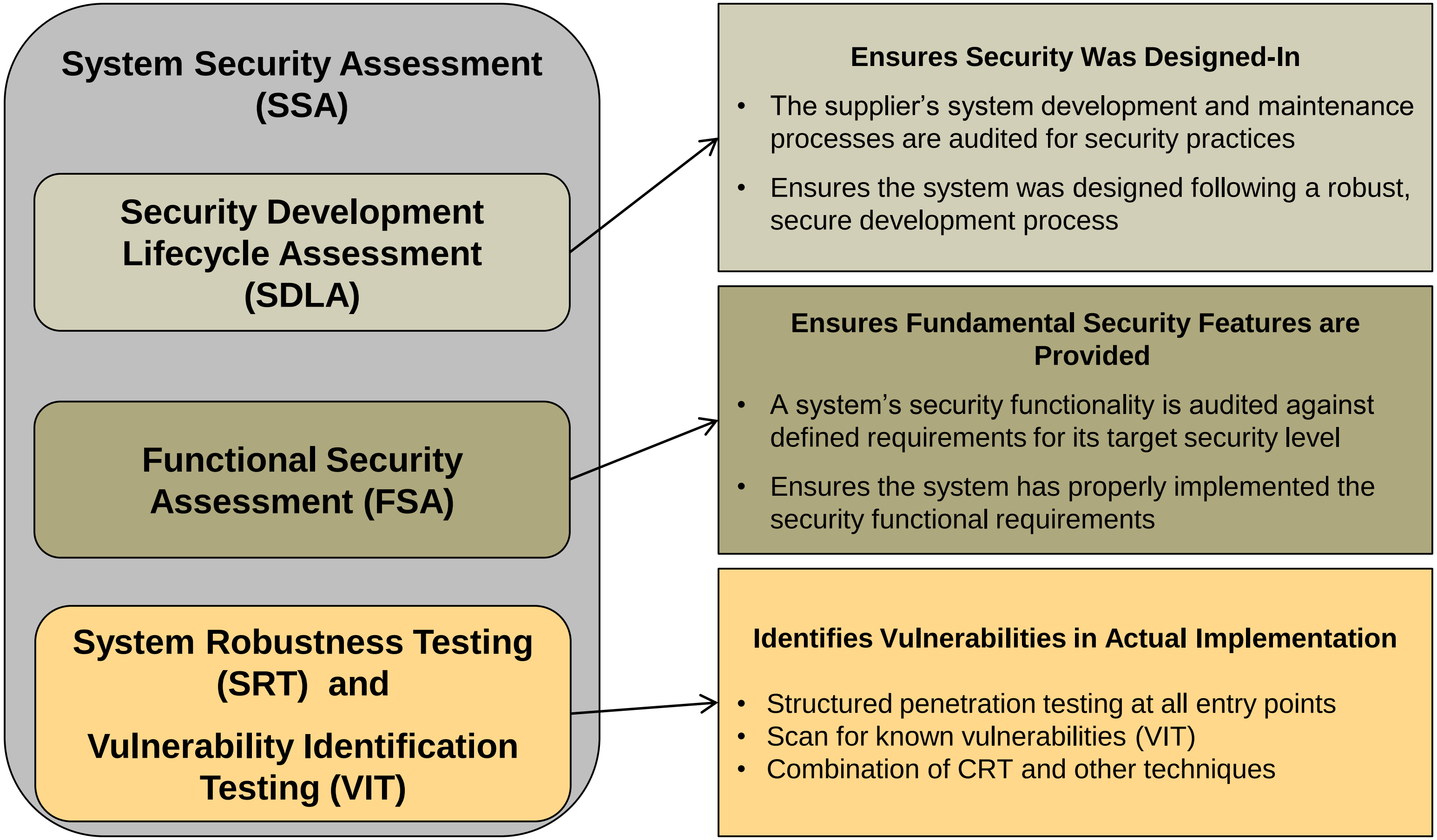
What is a “System” ?

- Industrial Control System (ICS) or SCADA system
- Available from a single supplier
- Supported by a single supplier (could be a system integrator)
- Components are integrated into a single system
- May consist of multiple Security Zones
- Can be identified by a product name and version
- Off the shelf; not site or project engineered yet



ISASecure SSA Certification Program

ISASecure



System Security Assessment (SSA)

Security Development Lifecycle Assessment (SDLA)

Functional Security Assessment (FSA)

System Robustness Testing (SRT) and

Vulnerability Identification Testing (VIT)

Ensures Security Was Designed-In

- The supplier's system development and maintenance processes are audited for security practices
- Ensures the system was designed following a robust, secure development process

Ensures Fundamental Security Features are Provided

- A system's security functionality is audited against defined requirements for its target security level
- Ensures the system has properly implemented the security functional requirements

Identifies Vulnerabilities in Actual Implementation

- Structured penetration testing at all entry points
- Scan for known vulnerabilities (VIT)
- Combination of CRT and other techniques

IEC 62443-4-1

ISASecure®
Security Development Lifecycle Assurance (SDLA)

SDLA Overview

- Certification that the supplier's product development sites have work process include security considerations throughout the lifecycle.

  (Development organization process certification-site specific)

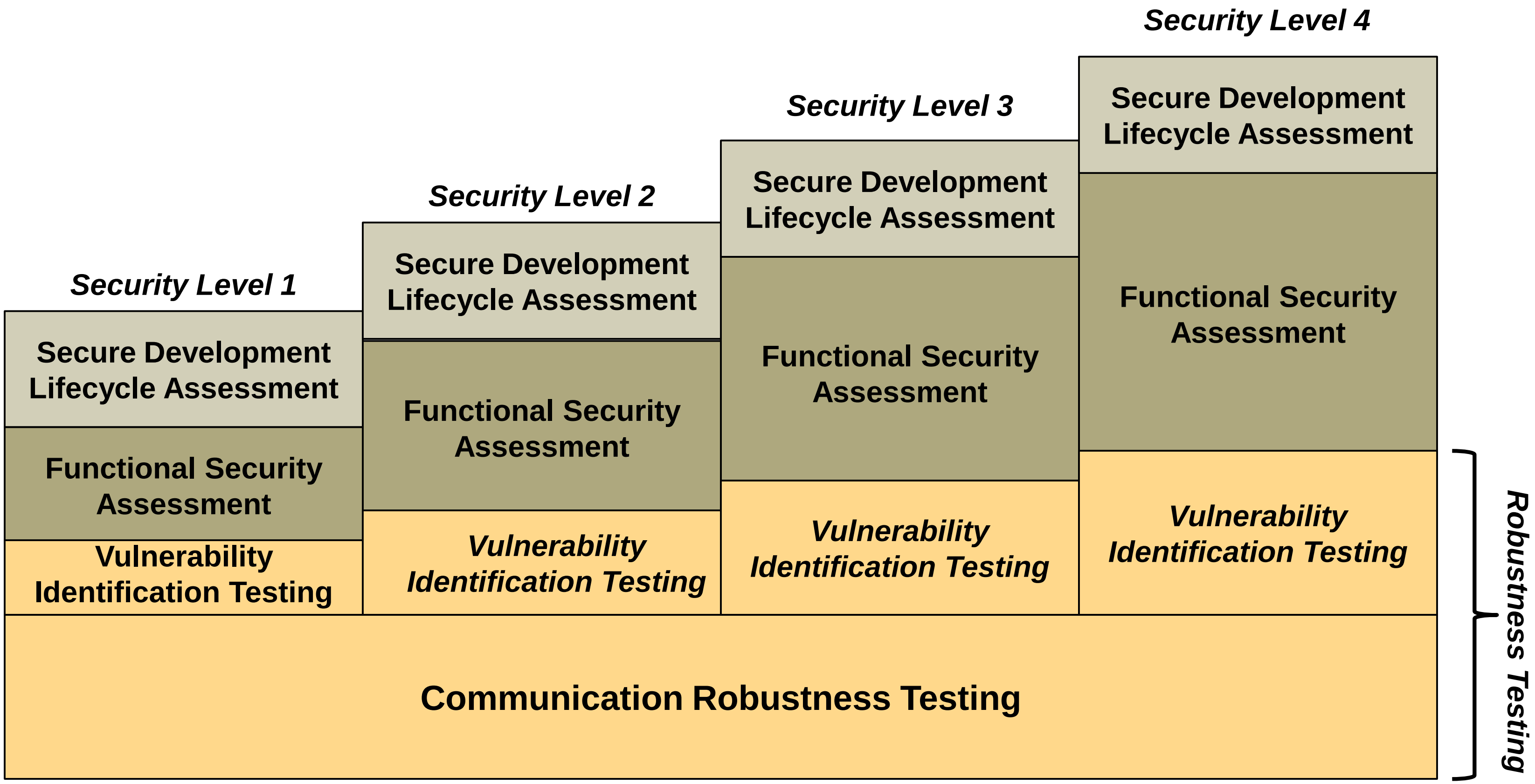
- Meets requirements of IEC 62443-4-1

- Based on several industry-recognized security development lifecycle processes

SDLA Practice Areas- ISA/IEC 64443-4-1

1	Security Management (SM)	The purpose of the security management practice is to ensure that the security-related activities are adequately planned, documented and executed throughout the product's lifecycle
2	Specification of Security Requirements (SR)	The processes specified by this practice are used to document the security capabilities that are required for a product along with the expected product security context
3	Secure by Design (SD)	The processes specified by this practice are used to ensure that the product is secure by design including defense in depth.
4	Secure Implementation (SI)	The processes specified by this practice are used to ensure that the product features are implemented securely.
5	Security Verification and Validation Testing (SVV)	The processes specified by this practice are used to document the security testing required to ensure that all of the security requirements have been met for the product and that the security of the product is maintained when it is used in its product security context.
6	Security Defect Management (DM)	The processes specified by this practice are used for handling security-related issues of a product that has been configured to employ its defense in depth strategy (Practice 3) within the product security context (Practice 2)
7	Security Update Management (SUM)	The processes specified by this practice are used to ensure security updates associated with the product are tested for regressions and made available to product users in a timely manner
8	Security Guidelines (SG)	The processes specified by this practice are used to provide documentation that describes how to integrate, configure, and maintain the defense in depth strategy of the product in accordance with its product security context

ISASecure Product Certification Levels



Security Level 1

Secure Development Lifecycle Assessment

Functional Security Assessment

Vulnerability Identification Testing

Security Level 2

Secure Development Lifecycle Assessment

Functional Security Assessment

Vulnerability Identification Testing

Security Level 3

Secure Development Lifecycle Assessment

Functional Security Assessment

Vulnerability Identification Testing

Security Level 4

Secure Development Lifecycle Assessment

Functional Security Assessment

Vulnerability Identification Testing

Communication Robustness Testing

Robustness Testing

ISASecure EDSA Certified Devices-March 2018

Supplier	Type	Model	Version	Level	Test Lab
Honeywell Process	Safety Manager	HPS 1009077 C001	R145.1	EDSA 2010.1 Level 1	exida
RTP Corporation	Safety manager	RTP 3000	A4.36	EDSA 2010.1 Level 2	exida
Honeywell Process Solutions	DCS Controller	Experion C300	R400	EDSA 2010.1 Level1	exida
Honeywell Process	Fieldbus Controller	Experion FIM	R400	EDSA 2010.1 Level 1	exida
Yokogawa	Safety Control System	ProSafe-RS	R3.02.10	EDSA2010.1 Level 1	exida
Yokogawa Electric	DCS Controller	CENTUM VP	R5.03.00	EDSA 2010.1 Level 1	CSSC-CL
Hitachi, Ltd.	DCS Controller	HISEC 04/R900E	01-08-A1	EDSA 2010.1 Level 1	CSSC-CL
AZBIL (formerly Yamatake)	DCS Controller	Harmonas / Industrial-DEO / Harmonas-DEO	R 4.1	EDSA 2010.1 Level 1	CSSC-CL
Schneider Electric	Field Process Controller	FCP280	S91061	EDSA 2010.1 Level 1	exida
Schneider Electric	Tricon CX			EDSA 2020.1 Level 1	TUV Rheinland
Beijing Consen Technologies	Safety Related PES	TSxPlus V1.0	CM01-A-V001	EDSA v20 Level1	TUV Rheinland
HIMA Paul Hildebrandt GmbH	Safety Related PES	HIMAX X	CPU 01 FW Version 8.8 & COM 01 FW Version 9.2	EDSA v2.0 Level T1	TUV Rheinland
TOSHIBA CORPORATION	DCS Controller	CIEMAC-DS/nv (TOSDIC-CIE DS/nv)		EDSA 2010.1 Level 1	CSSC-CL
Schneider Electric	Safety Related Programmable Electronic System	TRICONEX Communication Module TCM	4355X, Firmware Revision Build 290 (TCM2) 288	EDSA 2.0.0 Level	TUV Rheinland
ABB	Controller	HPC800 Controller	HCA800B1	EDSA 2010.1 Level 1	exida
Tri-Sen Systems Corporation	Safety Related Programmable Electronic System	TSxPlus V1.0	CM01-A-V001	EDSA 2.0.0 Level 1	TUV Rheinland

ISASecure® EDSA Certified Products

azbil

中國自動化 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

ISASecure® EDSA Certified Products

Schneider Electric

Schneider Electric

Schneider Electric

YOKOGAWA

YOKOGAWA

TOSHIBA

Leading Innovation »

ABB

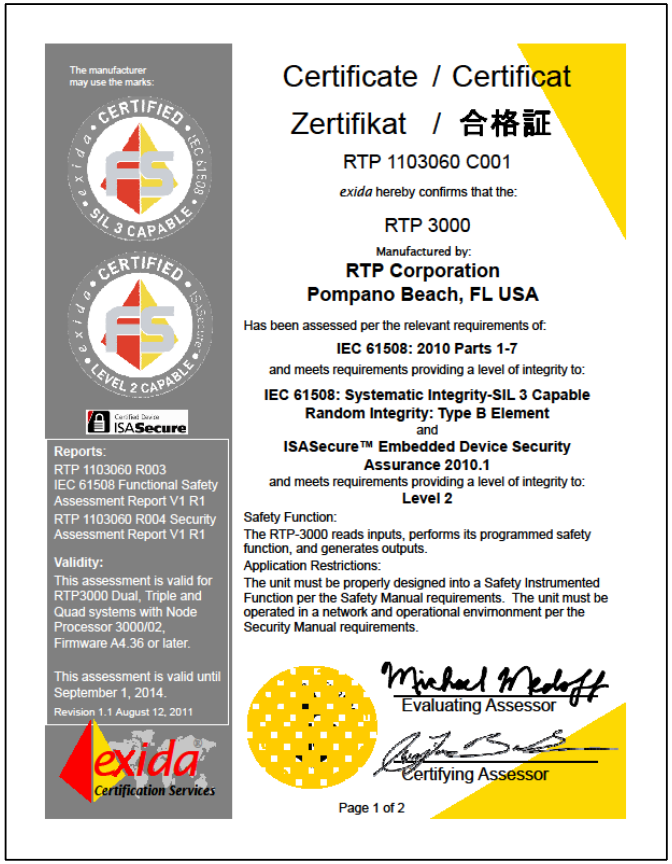
ISASecure SDLA Process Certified Development Organizations

Supplier	Locations	SDLA Version	Security Level (1-4)	Certification Body
Schneider-Electric	Foxboro, MA, USA	Version 1	SDLA Level 1	exida
Schneider-Electric	Worthing, UK	Version 1	SDLA Level 1	exida
Schneider-Electric	Lake Forest, CA USA	Version 1	SDLA Level 1	exida
Schneider-Electric	Calgary AB, Canada	Version 1	SDLA Level 1	exida
Schneider-Electric	Hyderabad, India	Version 1	SDLA Level 1	exida
Honeywell Process Solutions	Phoenix, AZ	Version 1	SDLA Level 1	exida

Schneider Electric

Honeywell

ISASecure® EDSA Product Certificates



The manufacturer may use the marks:

CERTIFIED • IEC 61508 • SIL 3 CAPABLE • exida

CERTIFIED • ISASecure • LEVEL 2 CAPABLE • exida

Certified Device ISASecure

Reports:
RTP 1103060 R003
IEC 61508 Functional Safety Assessment Report V1 R1
RTP 1103060 R004 Security Assessment Report V1 R1

Validity:
This assessment is valid for RTP3000 Dual, Triple and Quad systems with Node Processor 3000/02, Firmware A4.36 or later.

This assessment is valid until September 1, 2014.

Revision 1.1 August 12, 2011

exida Certification Services

Certificate / Certificat
Zertifikat / 合格証

RTP 1103060 C001

exida hereby confirms that the:

RTP 3000

Manufactured by:

RTP Corporation
Pompano Beach, FL USA

Has been assessed per the relevant requirements of:

IEC 61508: 2010 Parts 1-7

and meets requirements providing a level of integrity to:

IEC 61508: Systematic Integrity-SIL 3 Capable
Random Integrity: Type B Element
and
ISASecure™ Embedded Device Security Assurance 2010.1
and meets requirements providing a level of integrity to:
Level 2

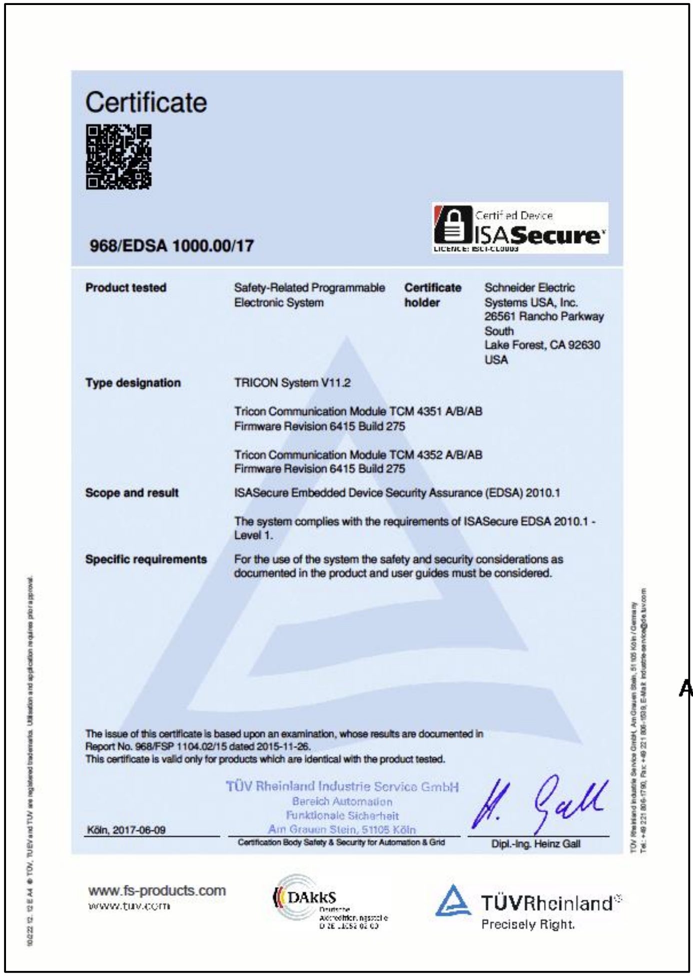
Safety Function:
The RTP-3000 reads inputs, performs its programmed safety function, and generates outputs.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements. The unit must be operated in a network and operational envimonment per the Security Manual requirements.

Michael Medoff
Evaluating Assessor

Certifying Assessor

Page 1 of 2



Certificate

968/EDSA 1000.00/17

Certified Device ISASecure
LICENCE: ISCI-CL0003

Product tested Safety-Related Programmable Electronic System

Certificate holder Schneider Electric
Systems USA, Inc.
26561 Rancho Parkway South
Lake Forest, CA 92630
USA

Type designation TRICON System V11.2

Tricon Communication Module TCM 4351 A/B/AB
Firmware Revision 6415 Build 275

Tricon Communication Module TCM 4352 A/B/AB
Firmware Revision 6415 Build 275

Scope and result ISASecure Embedded Device Security Assurance (EDSA) 2010.1

The system complies with the requirements of ISASecure EDSA 2010.1 - Level 1.

Specific requirements For the use of the system the safety and security considerations as documented in the product and user guides must be considered.

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1104.02/15 dated 2015-11-26.
This certificate is valid only for products which are identical with the product tested.

Köln, 2017-06-09

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln
Certification Body Safety & Security for Automation & Grid

H. Gall
Dipl.-Ing. Heinz Gall

www.fs-products.com
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZE-11052-02-00

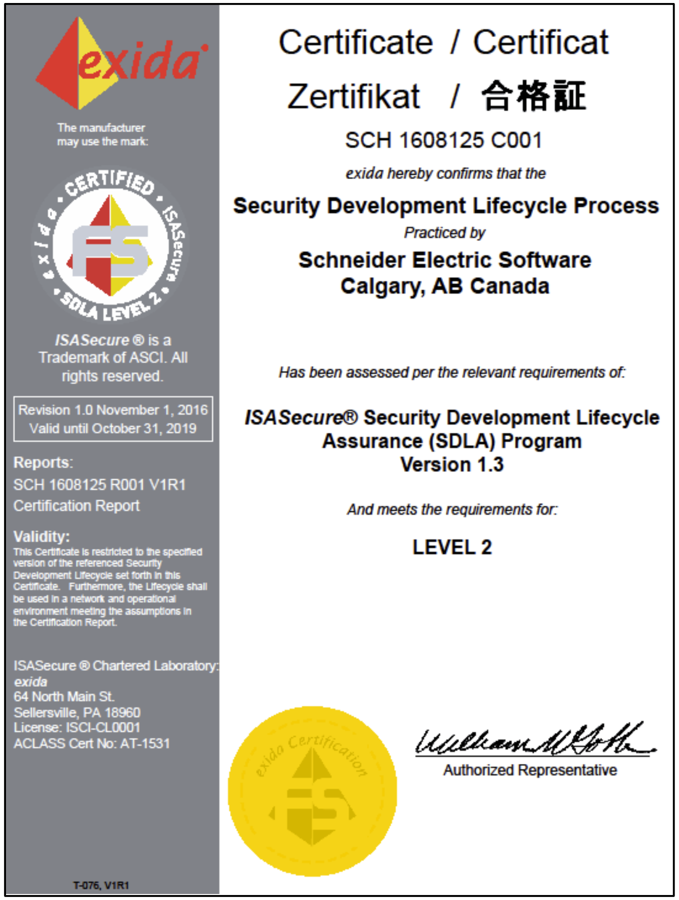
TÜVRheinland® Precisely Right.

10/222 12.12 E A4 © TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

Adobe Acrobat Document

ISASecure® SDLA Process Certificates



The manufacturer may use the mark:

ISASecure ® is a Trademark of ASCI. All rights reserved.

Revision 1.0 November 1, 2016
Valid until October 31, 2019

Reports:
SCH 1608125 R001 V1R1
Certification Report

Validity:
This Certificate is restricted to the specified version of the referenced Security Development Lifecycle set forth in this Certificate. Furthermore, the Lifecycle shall be used in a network and operational environment meeting the assumptions in the Certification Report.

ISASecure ® Chartered Laboratory:
exida
64 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

T-076, V1R1

Certificate / Certificat

Zertifikat / 合格証

SCH 1608125 C001

exida hereby confirms that the

Security Development Lifecycle Process

Practiced by

Schneider Electric Software
Calgary, AB Canada

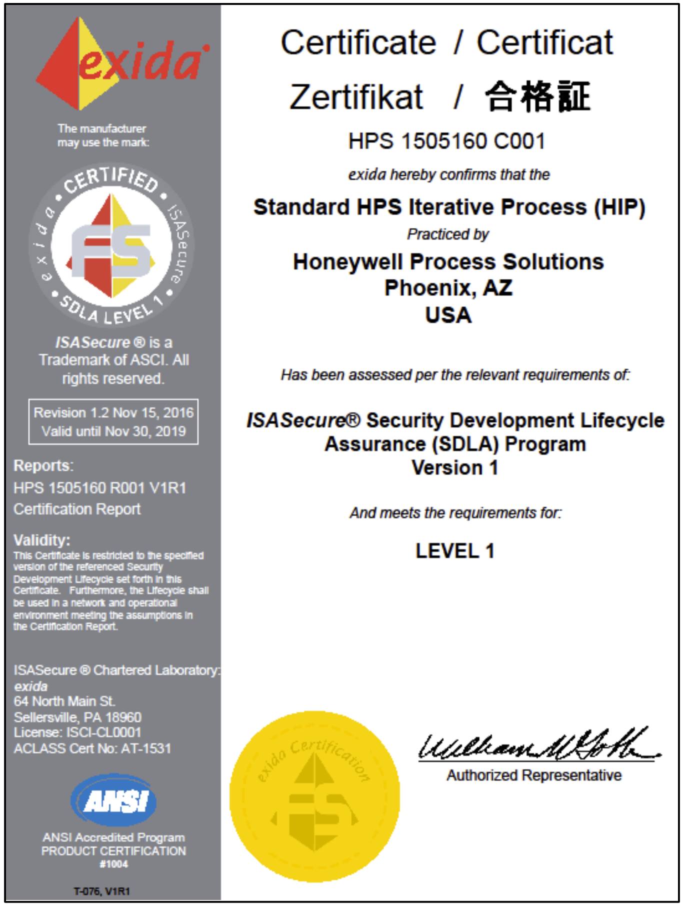
Has been assessed per the relevant requirements of:

***ISASecure*® Security Development Lifecycle Assurance (SDLA) Program**
Version 1.3

And meets the requirements for:

LEVEL 2

Authorized Representative



The manufacturer may use the mark:

ISASecure ® is a Trademark of ASCI. All rights reserved.

Revision 1.2 Nov 15, 2016
Valid until Nov 30, 2019

Reports:
HPS 1505160 R001 V1R1
Certification Report

Validity:
This Certificate is restricted to the specified version of the referenced Security Development Lifecycle set forth in this Certificate. Furthermore, the Lifecycle shall be used in a network and operational environment meeting the assumptions in the Certification Report.

ISASecure ® Chartered Laboratory:
exida
64 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

T-076, V1R1

Certificate / Certificat

Zertifikat / 合格証

HPS 1505160 C001

exida hereby confirms that the

Standard HPS Iterative Process (HIP)

Practiced by

Honeywell Process Solutions
Phoenix, AZ
USA

Has been assessed per the relevant requirements of:

***ISASecure*® Security Development Lifecycle Assurance (SDLA) Program**
Version 1

And meets the requirements for:

LEVEL 1

Authorized Representative

ISASecure Recognized Test Tools

ISASecure test tool specifications and recognition process ensures that all test tools meet ISASecure requirements and provide consistent test outcomes.

Supplier	Product Name	Test Coverage
Tenable	Nessus	Vulnerability Identification Testing against US-CERT NVDB
Beyond Security	beSTORM EDSA	CRT, SRT and network robustness
Hitachi	Raven	CRT, SRT and network robustness
Synopsys	Defensics X	CRT, SRT and network robustness
Wurldtech	Achilles Satellite	CRT, SRT and network robustness
CNCERT/CC & Beijing Xinlian Kehui Technology Co., LTD	Acheron 2.2	CRT, SRT, and network robustness

ISASecure Roadmap-new work

1. Collaborating with Building Control Systems (BCS) stakeholders to ensure ISASecure certifications properly address BCS.
2. Align EDSA with ISA/IEC 62443-4-2 Component requirements
   a) Include network components, applications, and host systems
3. Collaborating with European Union – ERNCIP CA program
4. Reaching out to other stakeholders including UL, industry groups such as ASHRAE, LOGIIC, CABA, NAMUR, DoD;
5. Seek to harmonize certifications globally-EU, Japan, USA, AP
6. Expanding protocols to include in CRT test requirements

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

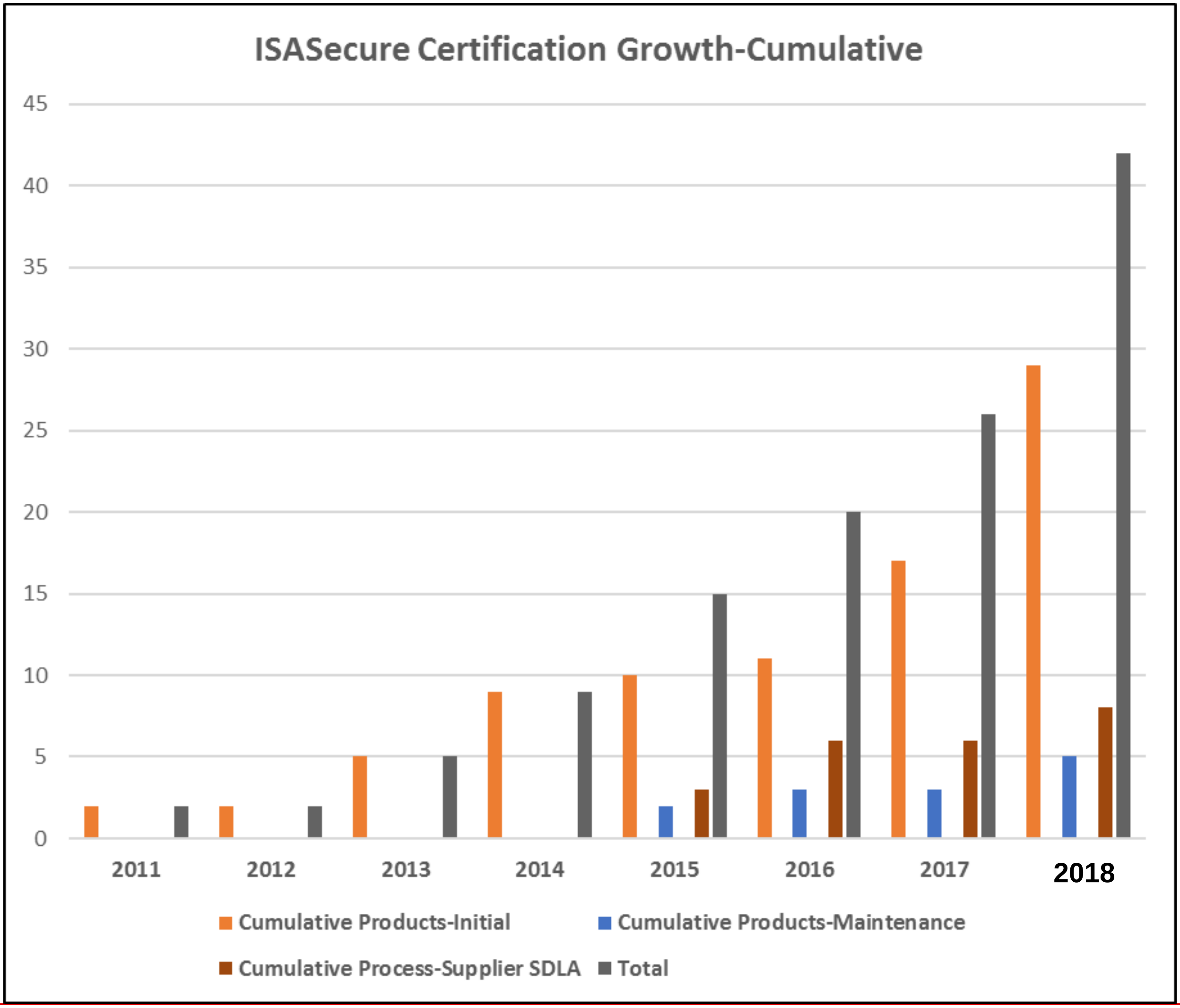
ISA Security Compliance Institute

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



Thank You

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