Securing the Supply Chain

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

www.isasecure.org

May 26, 2016

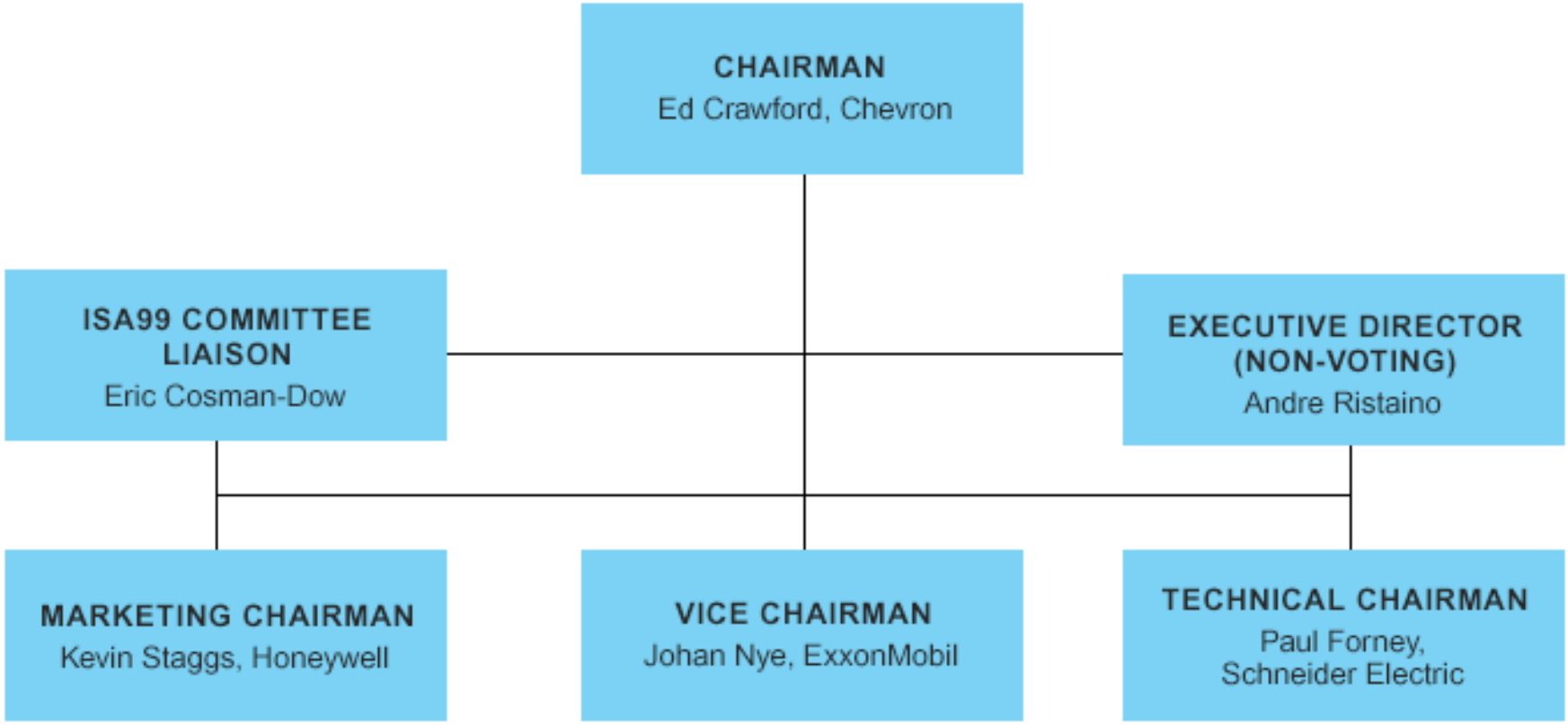
Andre Ristaino
Managing Director,
ISA Automation Standards Compliance Institute

Agenda

- About ISA Security Compliance Institute
- Structure of ISASecure scheme
- IEC 62443 Standards and structure
- Description of ISASecure Certifications
- ISASecure Roadmap

ISCI Organization

501 c 6 Not for profit
Conformity Assess Subsidiary of ISA



Supporters-ISCI Member Companies

ISCI membership is open to all organizations

- Strategic membership
- Technical membership
- Government membership
- Associate membership
- Informational membership

Member organizations

- Chevron
- Bedrock Automation
- Aramco Services
- CSSC
- Codenomicon
- exida
- ExxonMobil
- Honeywell
- IT Promotion Agency, Japan
- KPMG Consulting Ltd. Japan
- Schneider Electric
- TSC Advantage
- WisePlant HQ
- Yokogawa
- ISA99 Committee Liaison

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.
- ISCI is expanding MOU's with Accreditation Bodies and Labs

DaKKS

(Germany accreditation authority)

ANSI Accredited Program
PRODUCT CERTIFICATION

ACLASS
ANSI-ASQ National Accreditation Board

PROD
JAB

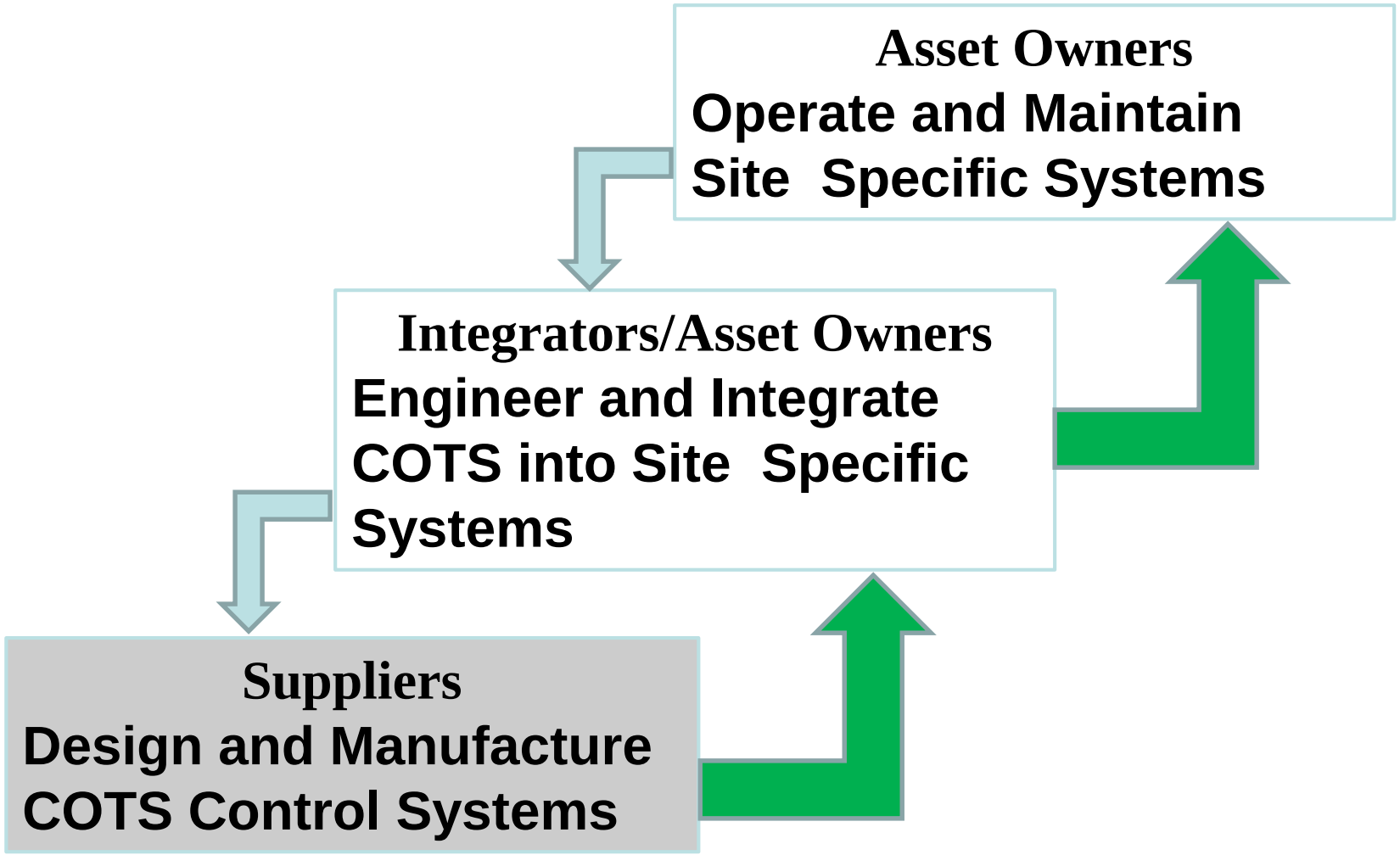
Why Certify COTS Products?

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

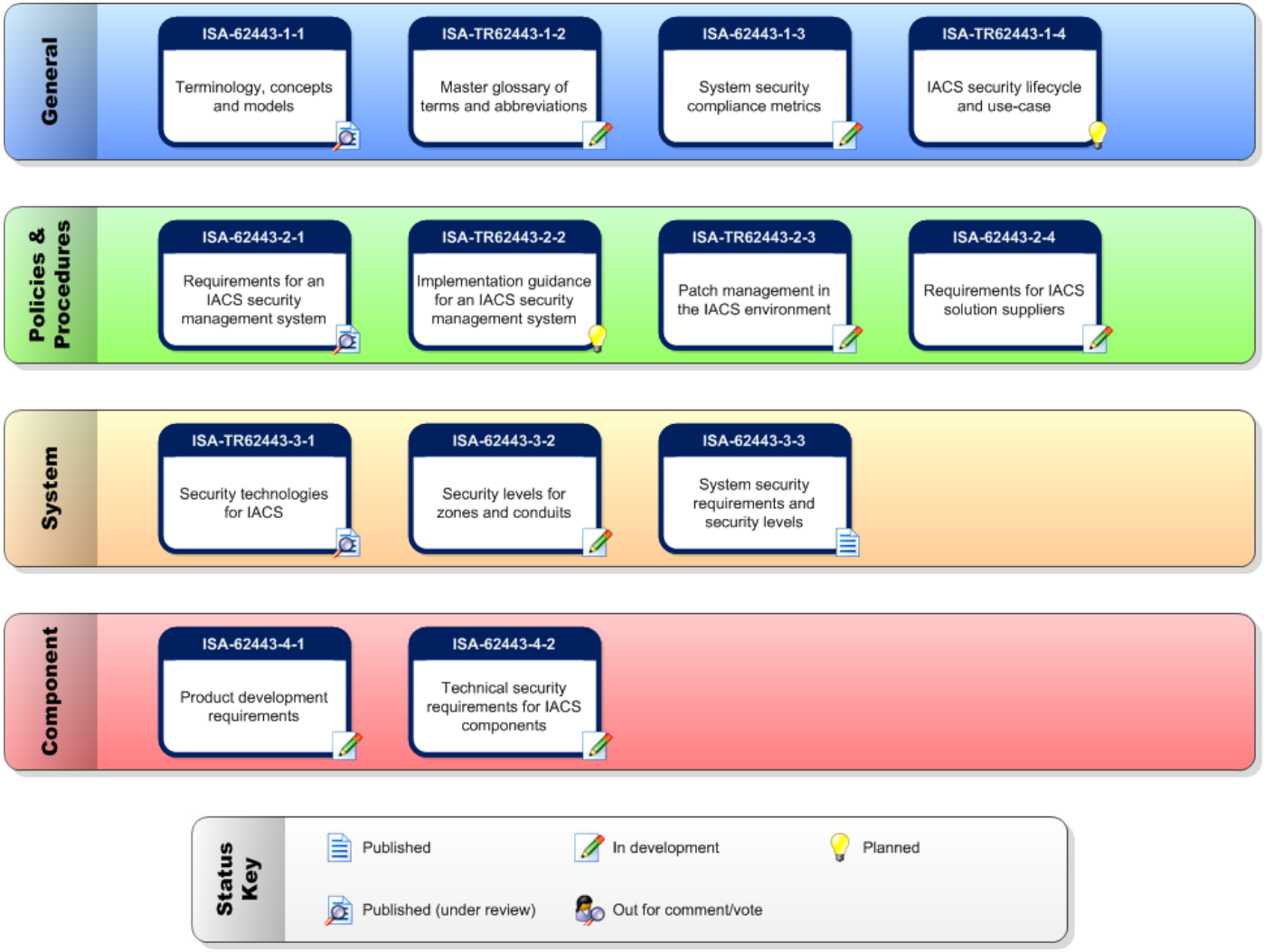
2. Reduces effort for end user to validate and verify security capabilities

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.)

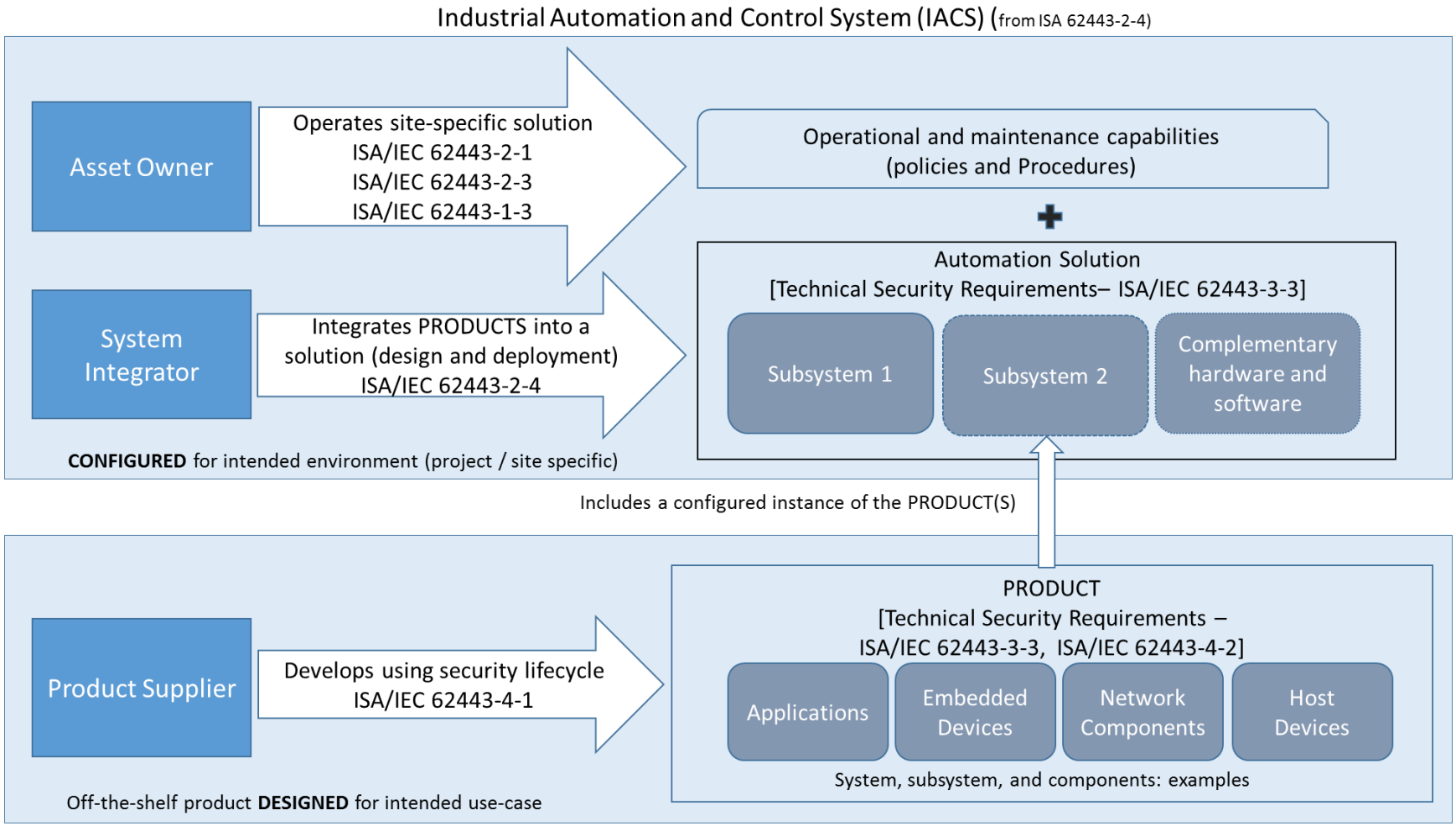
IACS Security Lifecycle



IEC 62443 Standards Family



IEC 62443 Standards Family



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

(Schneider Electric is worlds first vendor to achieve SDLA; at 3 different sites)

ISASecure®
Embedded Device Security Assurance (EDSA)

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

What is an Embedded Device?

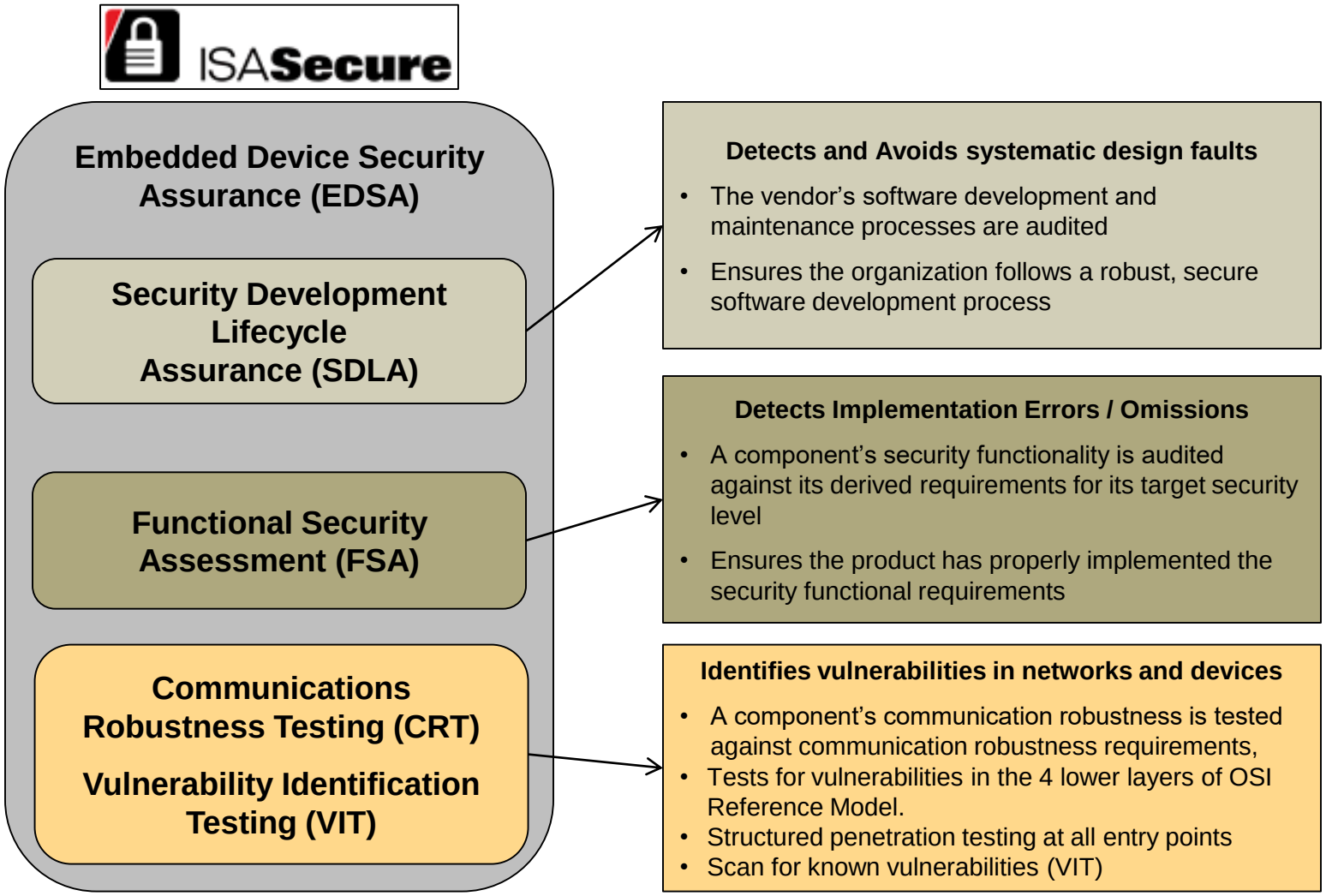
Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process, examples:

- Programmable Logic Controller (PLC)
- Distributed Control System (DCS) controller
- Safety Logic Solver
- Programmable Automation Controller (PAC)
- Intelligent Electronic Device (IED)
- Digital Protective Relay
- Smart Motor Starter/Controller
- SCADA Controller
- Remote Terminal Unit (RTU)
- Turbine controller
- Vibration monitoring controller
- Compressor controller

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 62443-4-1 and IEC 6443-4-2 are updated by IEC)
- Independent certification of the product's security capabilities and security level (SL) as defined by the IEC 62443 standards

ISASecure EDSA Certification Program



ISASecure®
System Security Assurance (SSA)

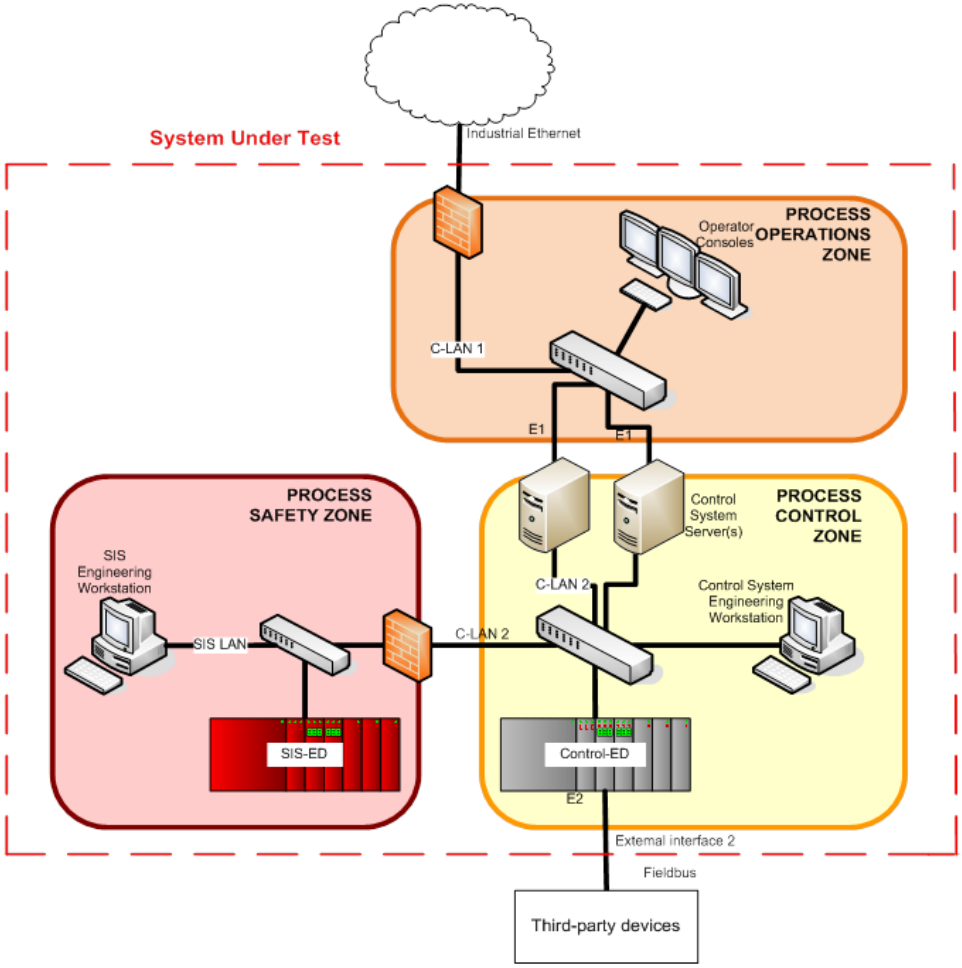
IEC 62443-3-3
IEC 62443-4-1
IEC 62443-4-2

SSA Overview

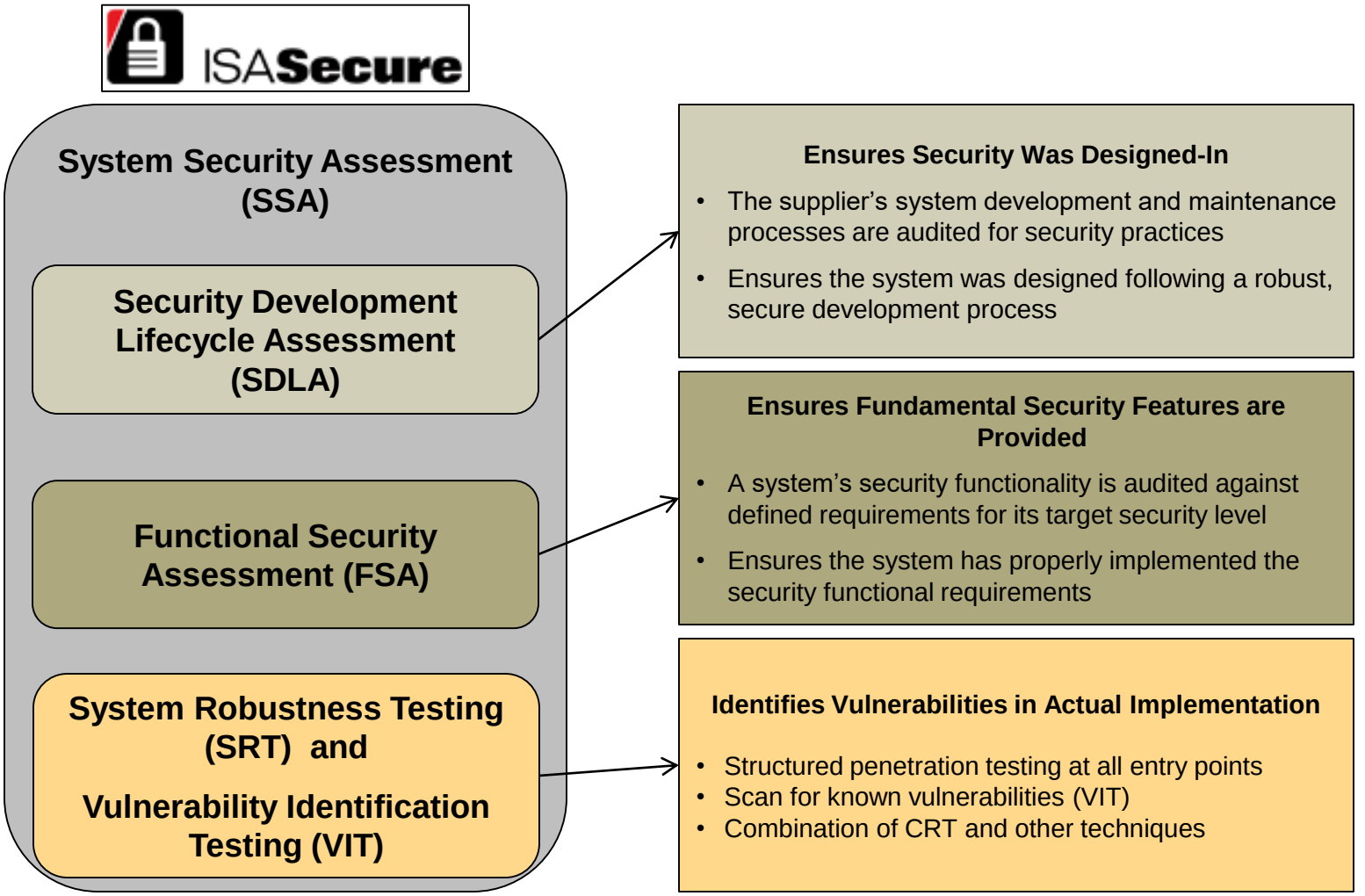
- Certification that the supplier's product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of IEC 62443-3-3, IEC 62443-4-1 and, IEC 62443-4-2 (SSA was revised in 2013 to align with IEC 62443-3-3 requirements after IEC approval)
- Independent certification of the product's security capabilities and security 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



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

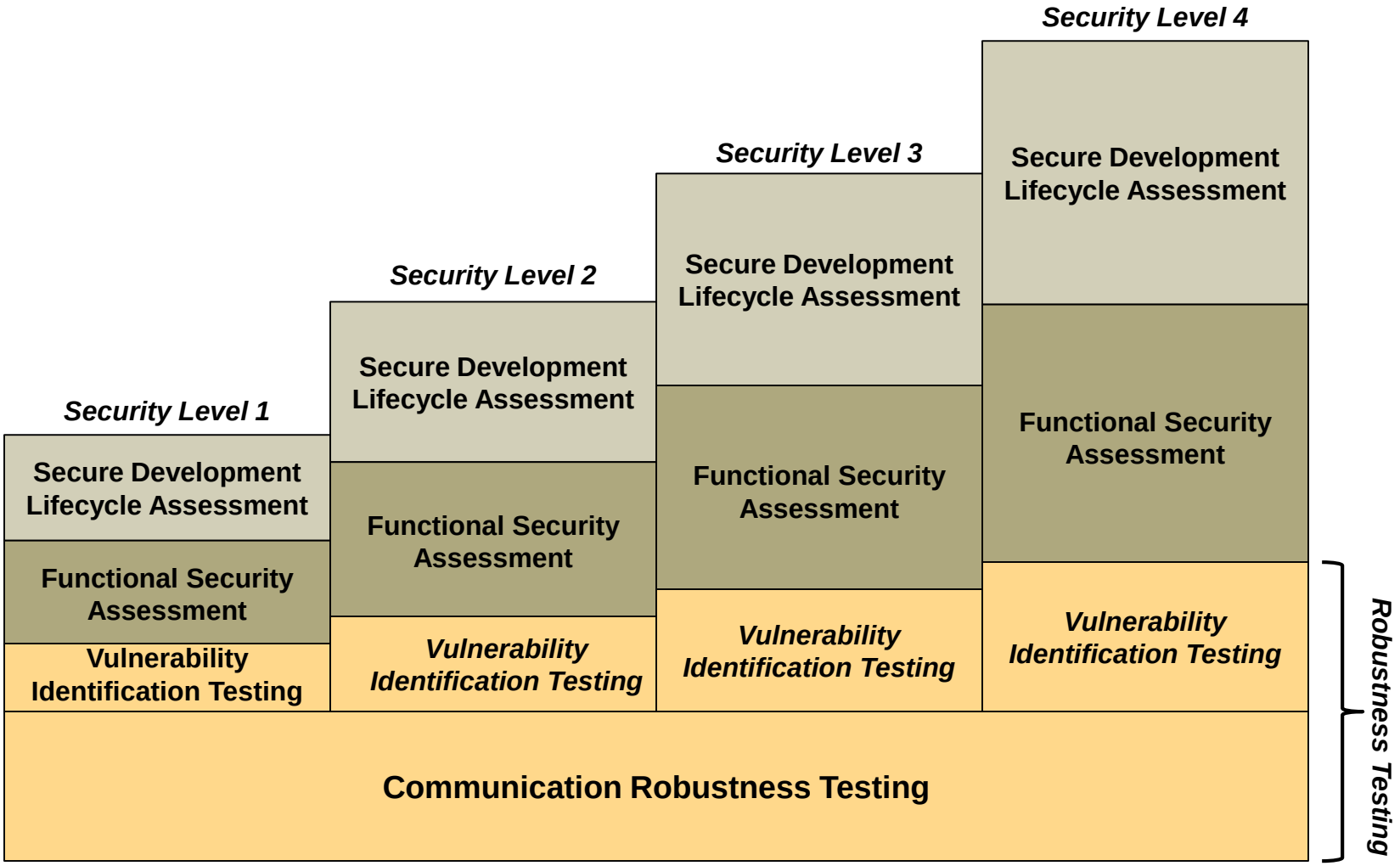
  (will be revised when IEC 62443-4-1 is maintained by IEC)

- Based on several industry-recognized security development lifecycle processes

SDLA Phases

1. Security Management Process
2. Security Requirements Specification
3. Security Architecture Design
4. Security Risk Assessment (Threat Model)
5. Detailed Software Design
6. Document Security Guidelines
7. Module Implementation & Verification
8. Security Integration Testing
9. Security Process Verification
10. Security Response Planning
11. Security Validation Testing
12. Security Response Execution

Security Levels in ISASecure Certifications

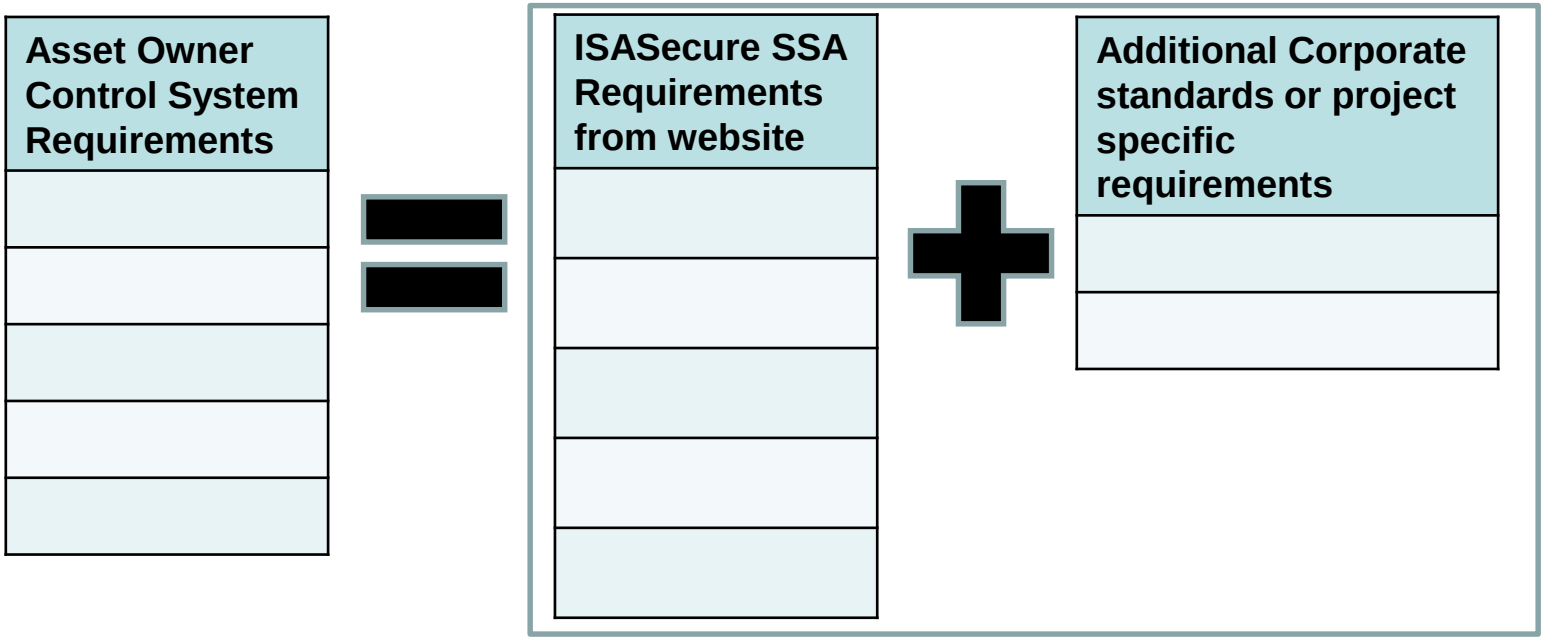


How to Use ISASecure in Procurement

1. Asset Owner assesses risk and determines required security levels (similar to SIL requirements analysis) for COTS application categories / systems

2. Asset owner downloads and reviews ISASecure certification requirements, noting SL levels.

3. Specify matching ISASecure SL level in COTS procurement document plus any company or project specific additions.



ISASecure EDSA Certified Devices

Supplier	Type	Model	Version	Level	Test Lab
Honeywell Process Solutions	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 Solutions	Fieldbus Controller	Experion FIM	R400	EDSA 2010.1 Level 1	exida
Yokogawa Electric Corporation	Safety Control System	ProSafe-RS	R3.02.10	EDSA2010.1 Level 1	exida
Yokogawa Electric Corporation	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 system Process Controller DOPC IV (Redundant type)	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

ISASecure 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	Hyderabad, India	Version 1	SDLA Level 1	exida

ISASecure Recognized Test Tools

Supplier	Product Name	Test Coverage
Tenable	Nessus	Vulnerability Identification Testing against US-CERT NVDB
Beyond Security	beSTORM EDSA	CRT, SRT and network robustness testing
Hitachi	Raven	CRT, SRT and network robustness testing
Synopsys	Defensics X	CRT, SRT and network robustness testing
Wurldtech	Achilles Satellite	CRT, SRT and network robustness testing

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

Additional CB accreditation in progress in Germany (DAkkS)

ISASecure Roadmap-new work

1. Developing an application software only certification (Application Security Assurance-ASA)
2. Collaborating with Building Automation Systems (BAS) stakeholders to expand IEC 62443 certification to BAS control systems.
3. Collaborating with European Union – ERNCIP CA program
4. Reaching out to other stakeholders including UL, industry groups such as LOGIIC, CABA, NAMUR, WIB; seek to harmonize certifications globally-EU, Japan, USA
5. Expanding protocols to include in CRT test requirements

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