ISA Security Compliance Institute

Internationally Accredited Conformance Scheme

ISASecure certification programs are accredited as an ISO/IEC Guide 65 conformance scheme and ISO/IEC 17025 lab operations by ANSI/ACLASS.

- Provides global recognition for ISASecure certification

- Independent CB accreditation by ANSI/ACLASS and other global Accreditation Bodies such as JAB or UKAS

- ISASecure can scale on a global basis

- Ensures certification process is open, fair, credible, and robust.

- MOU's with AB's for ISASecure

ISASecure

ISA Security Compliance Institute

Global Acceptance of ISASecure

- One set of certification criteria

- One certification test/assessment

- One globally recognized mark

Economically efficient for both suppliers and asset owners

ISASecure

ISA Security Compliance Institute

Global Adoption Expands to Japan

Japan Information-technology Promotion Agency and Control System Security Center

- IPA Translated ISASecure specifications to Japanese

- CSSC set up a test lab in Sendai Japan - Control System Security Center Certification Laboratory (CSSC-CL)

- CSSC-CL was accredited by JAB (Japan Accreditation Board) to ISASecure in Q1 2014

- CSSC and CSSC-CL are promoting ISASecure as part of the Japanese critical infrastructure security scheme.

- CSSC-CL certified their first EDSA device in Q2 2014

ISASecure

ISA Security Compliance Institute

ISASecure™

Three certifications currently available.

1. **Embedded Device Security Assurance (EDSA)**

2. **System Security Assurance (SSA)**

3. **Security Development Lifecycle Assurance (SDLA)**

ISASecure™
Embedded Device Security Assurance (EDSA)

ISASecure
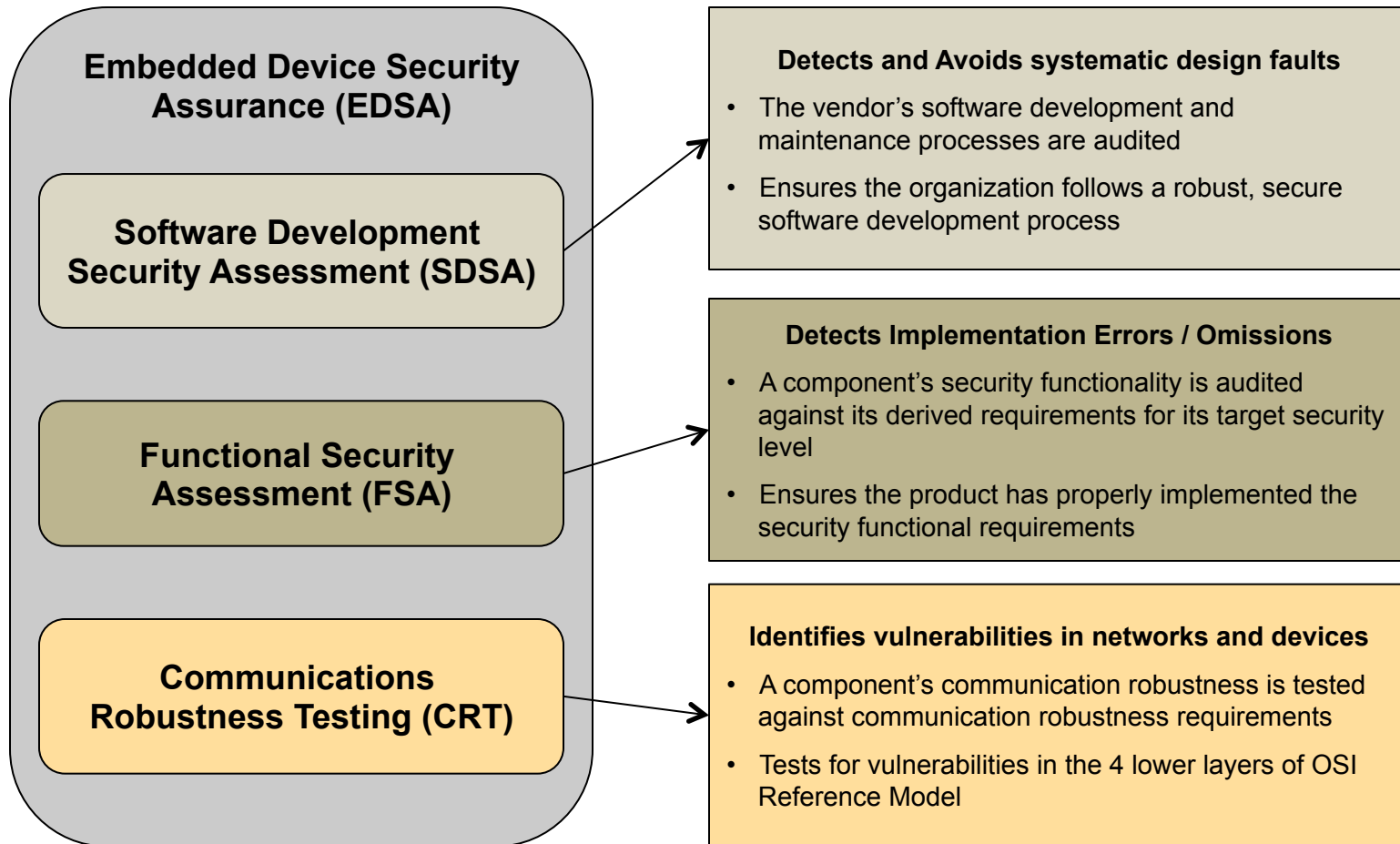
ISA Security Compliance Institute

EDSA Overview

- Certification that the supplier's product is robust against network attacks and is free from known security vulnerabilities

- Meets requirements of ISA/IEC-62443-4-2 for embedded devices (will be aligned with 4-2 when formally approved by IEC)

- Currently available – 7 devices certified with more devices under assessment

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
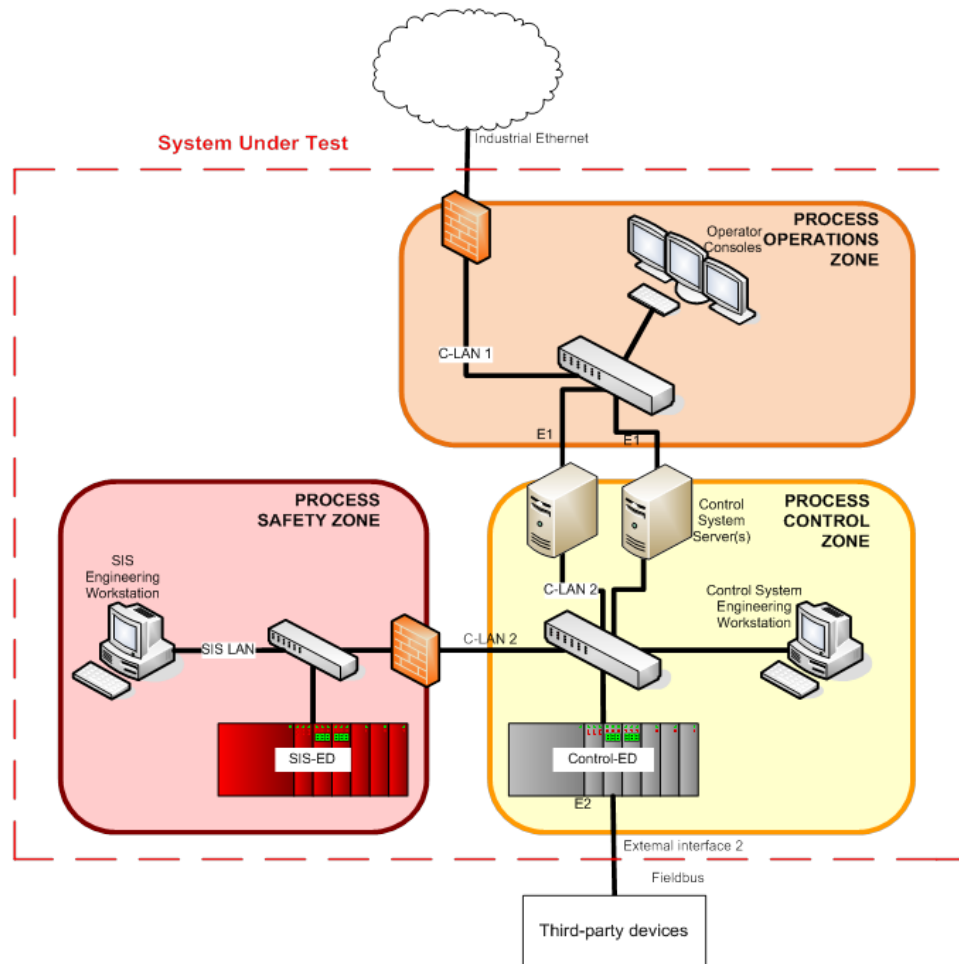
ISASecure EDSA Certification Program

ISASecure

Embedded Device Security Assurance (EDSA)

Software Development Security Assessment (SDSA)

Functional Security Assessment (FSA)

Communications Robustness Testing (CRT)

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

---

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

---

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

ISASecure™
System Security Assurance (SSA)

ISASecure
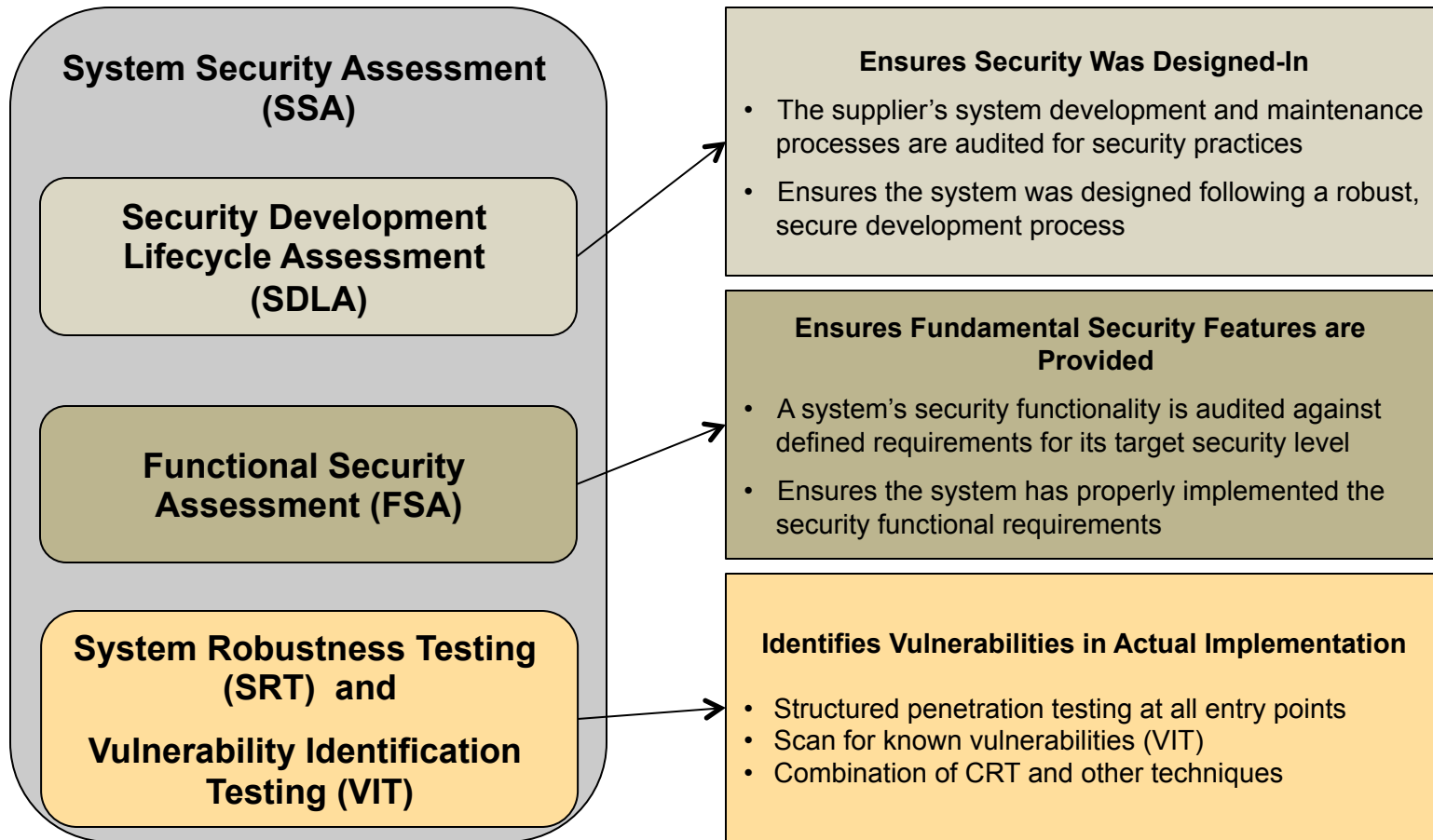
ISA Security Compliance Institute

SSA Overview

- Certification that the supplier's product is robust against network attacks and is free from known security vulnerabilities

- Meets requirements of ISA/IEC-62443-3-3
  (SSA was aligned with 3-3 by ISCI in 2013 when it was approved by IEC)

- Available as of Q1 2014

What is a "System" ?

- Industrial Control System (ICS) or SCADA system

- Available from a single supplier

- Supported by a single supplier

- Components are integrated into a single system

- May consist of multiple Security Zones

- Can be identified by a product name and version

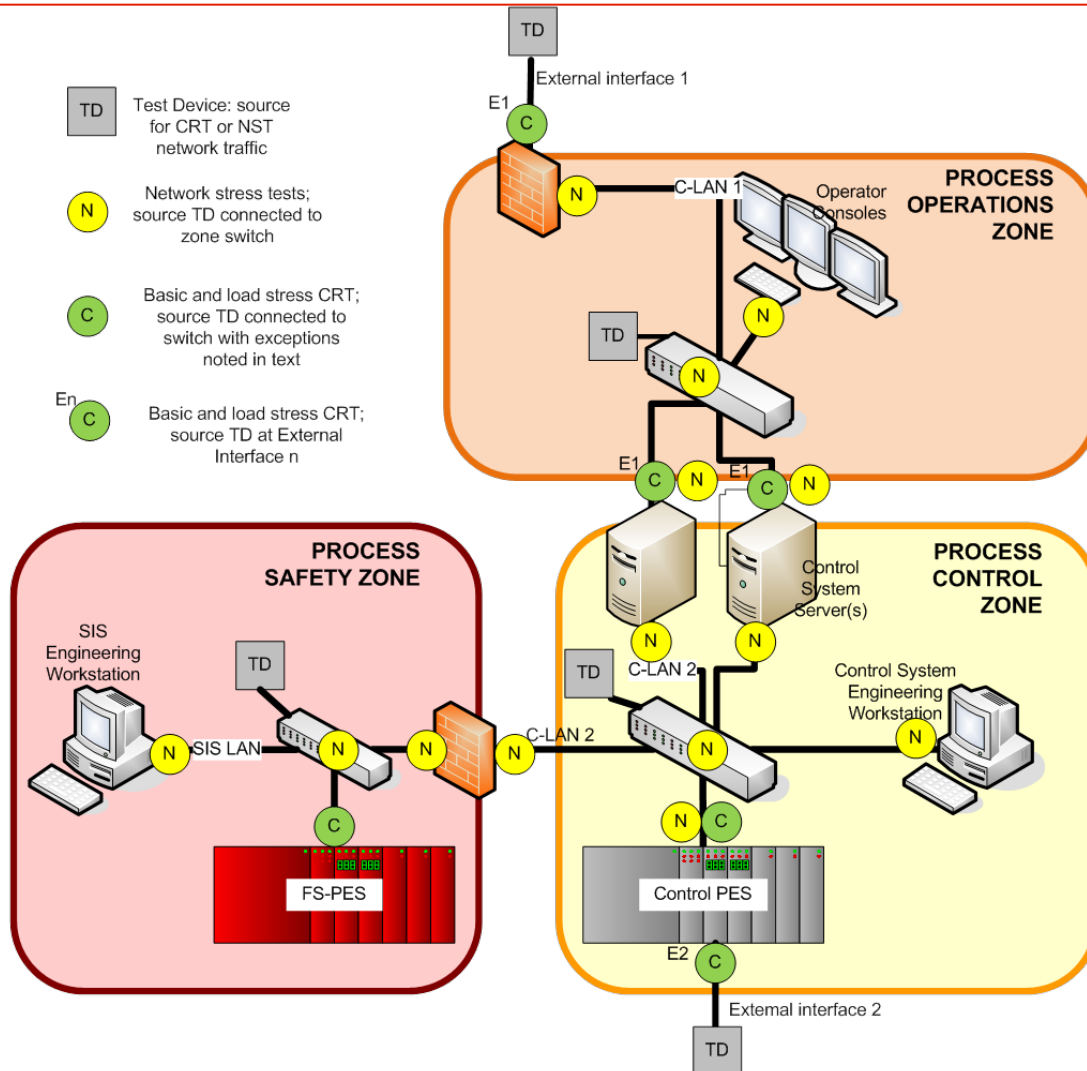- Off the shelf; not site or project engineered yet

ISASecure SSA Certification Program

ISASecure

System Security Assessment (SSA)

Security Development Lifecycle Assessment (SDLA)

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

Functional Security Assessment (FSA)

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

System Robustness Testing (SRT) and Vulnerability Identification Testing (VIT)

Identifies Vulnerabilities in Actual Implementation

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

SSA System Robustness Test

- ## Asset Discovery Scan
  - scan to discover the components on the network

- ## Communications Robustness Test
  - verify that essential functions continue to operate under high network load and malformed packets

- ## Network Stress Test
  - verify that essential functions continue to operate under high network load

- ## Vulnerability Identification Test
  - scan all components for the presence of known vulnerabilities (using Nessus)
  - based on National Vulnerability Database

SSA System Robustness Test

ISA Security Compliance Institute

ISASecure™
Security Development Lifecycle Assurance (SDLA)

ISASecure

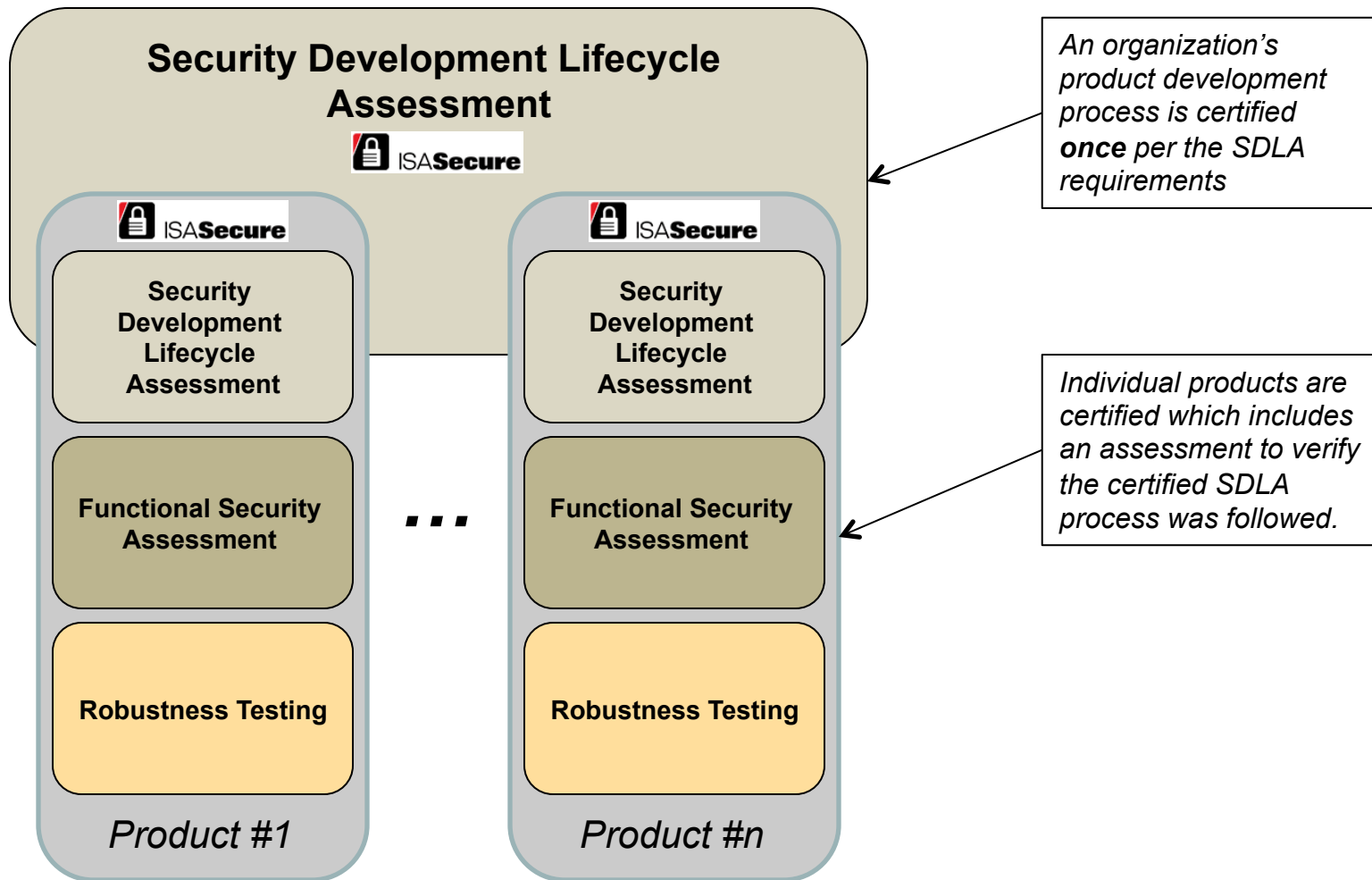*ISA Security Compliance Institute*

SDLA Overview

- Certification that the supplier's product development work process includes security considerations throughout the lifecycle. (Organization process certification)

- Meets requirements of ISA/IEC-62443-4-1
  (will be aligned with 4-1 when it is formally approved by IEC)

- Based on several industry-recognized security development lifecycle processes
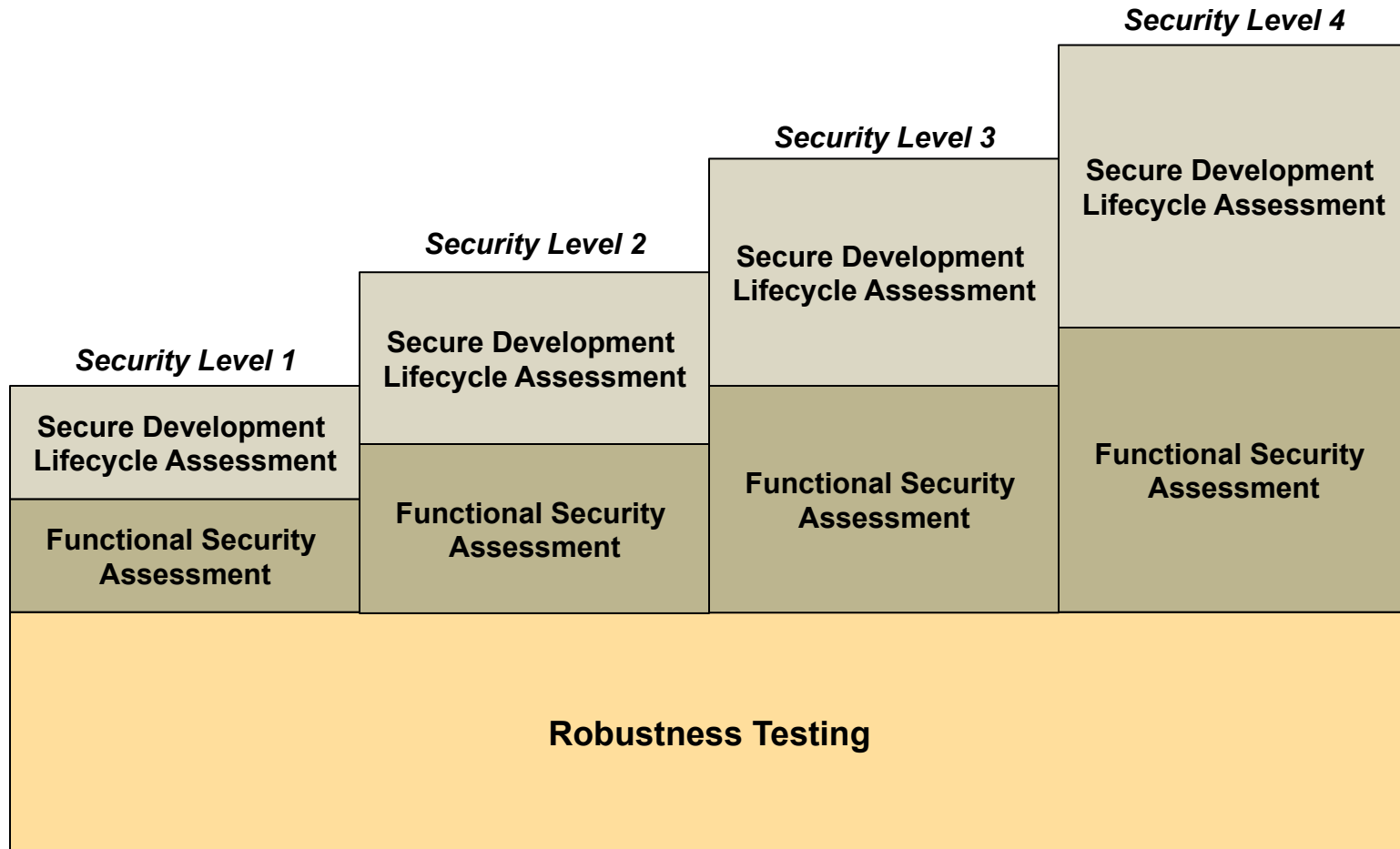
- Launched on 30 May 2014

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

Multiple Product Certification

Security Development Lifecycle Assessment

ISASecure

Security Development Lifecycle Assessment

ISASecure

Functional Security Assessment

Robustness Testing

Product #1

ISASecure

Security Development Lifecycle Assessment

Functional Security Assessment

Robustness Testing

Product #n

. . .

*An organization's product development process is certified **once** per the SDLA requirements*

Individual products are certified which includes an assessment to verify the certified SDLA process was followed.

ISASecure

ISA Security Compliance Institute

Security Levels

Security Level 1

Secure Development Lifecycle Assessment

Functional Security Assessment

Security Level 2

Secure Development Lifecycle Assessment

Functional Security Assessment

Security Level 3

Secure Development Lifecycle Assessment

Functional Security Assessment

Security Level 4

Secure Development Lifecycle Assessment

Functional Security Assessment

Robustness Testing

Test Tools Available for Use in ISASecure

Communication Robustness Test tools

1. Codenomicon – Defensics X

2. FFR – Raven

3. Wurldtech – Achilles

Vulnerability Scanning Tools

1. Tenable - Nessus

In Summary

- ISA/IEC-62443 standards set the requirements for Industrial Automation and Control Systems

- ISASecure certifies that suppliers and products meet the ISA/IEC-62443 standards

- Asset Owners have confidence that the IACS products they purchase are robust against network attacks and are free from known security vulnerabilities

USA Government – Executive Order

- ISA under Automation Federation facilitating NIST effort to develop a cybersecurity framework.

- Draft framework 1.0 completed in 2013. IEC 62443 standards are prominent in the document.

- Cybersecurity Framework 2.0. Plans are underway for a meeting this Fall in Illinois by the White House and NIST

Who to contact for ISA99 committee

Eric Cosman

Co-Chairman ISA99 Committee

eric.cosman@gmail.com

Jim Gilsinn

Co-Chairman ISA99 Committee

jimgilsinn@gmail.com

ISA**Secure**

ISA Security Compliance Institute

Who to Contact to Certify Products

| ISASecure EDSA Chartered Lab:

Exida

Mike Medoff
Director of Security Services
Phone: (215) 453-1720
Fax: (215) 257-1657
Email: mmedoff@exida.com
Website: http://www.exida.com | ISASecure EDSA Chartered Lab:

CSSC - Japan

Kenzo Yoshimatsu

Phone: +81 (22) 353-6751
Email: kenzo.yoshimatsu@css-center.or.jp
Website: http://www.css-center.or.jp |

Who to contact for ISCI Membership

Andre Ristaino

Managing Director, ASCI

Phone: 919-990-9222

Fax: 919-549-8288

Email: aristaino@isa.org

Website: http://www.isasecure.org

Glossary

Acronym	Description
ACLASS	One of three brands of the ANSI-ASQ National Accreditation Board
ANSI	American National Standards Institute
CSSC	Control System Security Center, Japan-R&D and test lab in Sendai Japan
ISA	International Society of Automation
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IPA	Information-technology Promotion Agency, Japan
ISCI	ISA Security Compliance Institute
JAB	Japan Accreditation Bureau-Japan based IEC accreditation body (AB)

ISASecure

ISA Security Compliance Institute

ISA 62443 Status (Oct, 2013)

ISA Security Compliance Institute