ISA Security Compliance Institute

Andre Ristaino
ASCI Managing Director
May 2014

www.isasecure.org

Presentation objectives

- Introduction to ISA/IEC 62443 Standards (ISA99)
- Introduction to ISA Security Compliance Institute (ISCI)
- Description of ISASecure Certification Programs

- How can you help improve ICS security?
  - Certify your products using ISASecure
  - Specify ISASecure in your procurement specifications
  - Become involved in ISA99 standards development
  - Become a member of ISA Security Compliance Institute

Rewind to the 1980's

- Industry-wide focus on Safety due to some significant events
- Safety Instrumented Systems (SIS) technology changing from electrical relays to programmable electronic systems (PES)
- Limited skillset in asset owner organizations to assess SIS safety integrity
- Solution:
  - IEC 61508/61511 international standards
  - Independent 3rd party safety integrity assessment

Fast Forward to Today

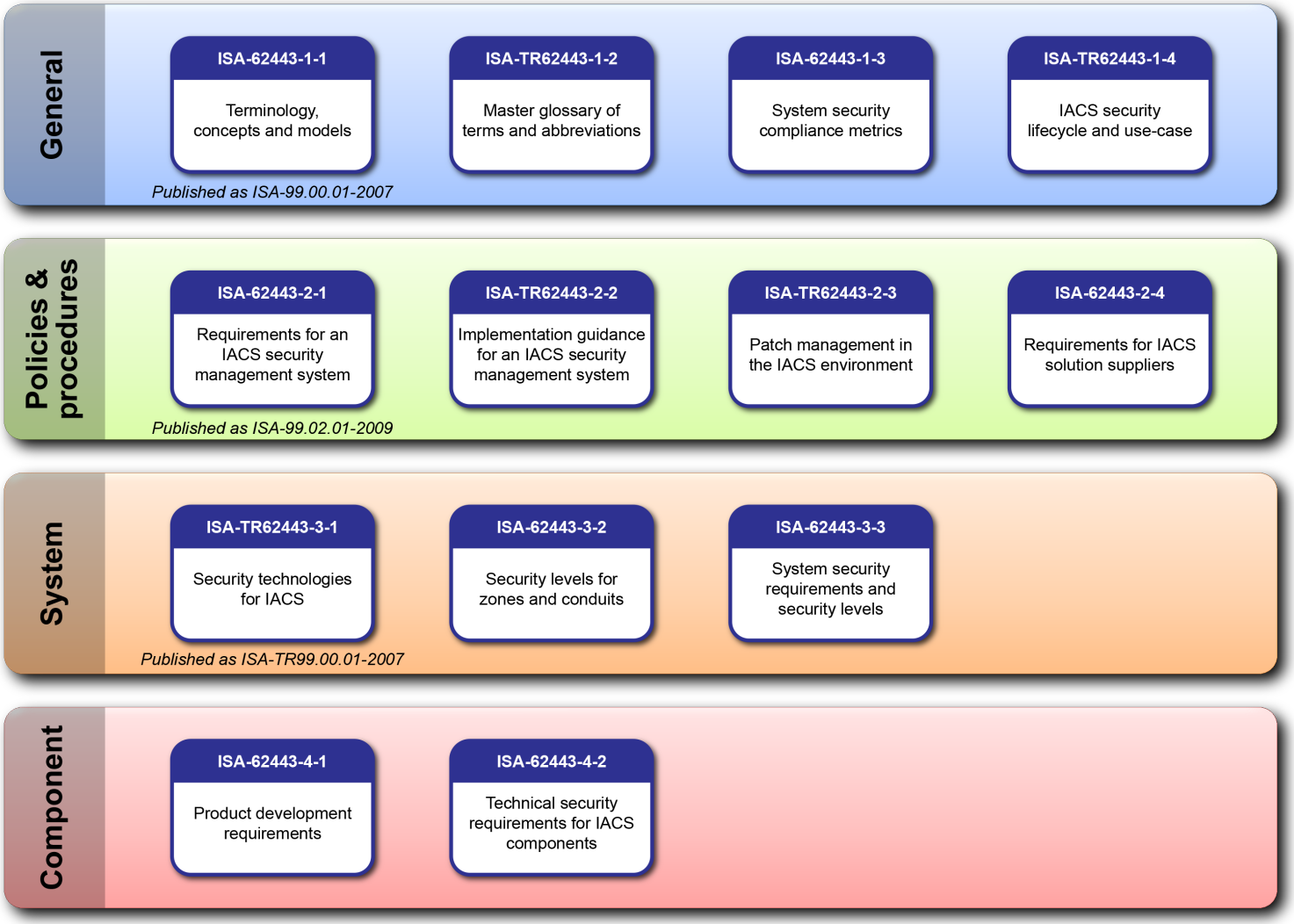
- Industry-wide focus on Security due to many significant events
- Industrial Automation and Control Systems (IACS) technology changing from vendor proprietary to IP networking and COTS hardware/OS
- Limited skillset in asset owner organizations to assess IACS cybersecurity capabilities
- Solution:
  - ISA/IEC 62443 international standards
  - Independent 3rd party security assessment - ISASecure™

ISA / IEC-62443
International Standards

ISA/IEC 62443

- Scope is Industrial Automation and Control Systems (IACS)
- Scope is industry cross-sector
- Mostly developed by the ISA99 Committee and simultaneously submitted to IEC for international approval
- ISA99 Committee has a large volunteer membership from around the world
  - asset owners, suppliers, cybersecurity experts, IACS experts, and many others

About ISA99 Standards



ISA Security Compliance Institute (ISCI)

About ISCI

Organization

Consortium of Asset Owners, Suppliers, and Industry Organizations formed in 2007 under the ISA Automation Standards Compliance Institute (ASCI):

Mission

Establish a set of well-engineered specifications and processes for the testing and certification of industrial automation and control systems products

Decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders

ISCI Member Companies

ISCI membership is open to all organizations

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

Member organizations

- Chevron
- Aramco Services
- CSSC
- Codenomicon
- exida
- ExxonMobil
- Honeywell
- IT Promotion Agency, Japan
- Schneider Electric (Invensys)
- RTP Corp.
- Yokogawa
- ISA99 Committee Liaison

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

Objective of ISASecure

- One set of certification criteria
- One certification test/assessment
- One globally recognized mark

Economically efficient for both suppliers and asset owners

Global Adoption

Japan Information-technology Promotion Agency & Control System Security Center

- Translating ISASecure specifications to Japanese
- Setting up a test lab in Sendai Japan - Control Systems Security Center Certification Laboratory (CSSC-CL)
- JAB is undertaking the CSSC-CL accreditation process
- Promoting ISASecure as part of the Japanese critical infrastructure security scheme.

ISASecure™ Embedded Device Security Assurance (EDSA)

EDSA Overview

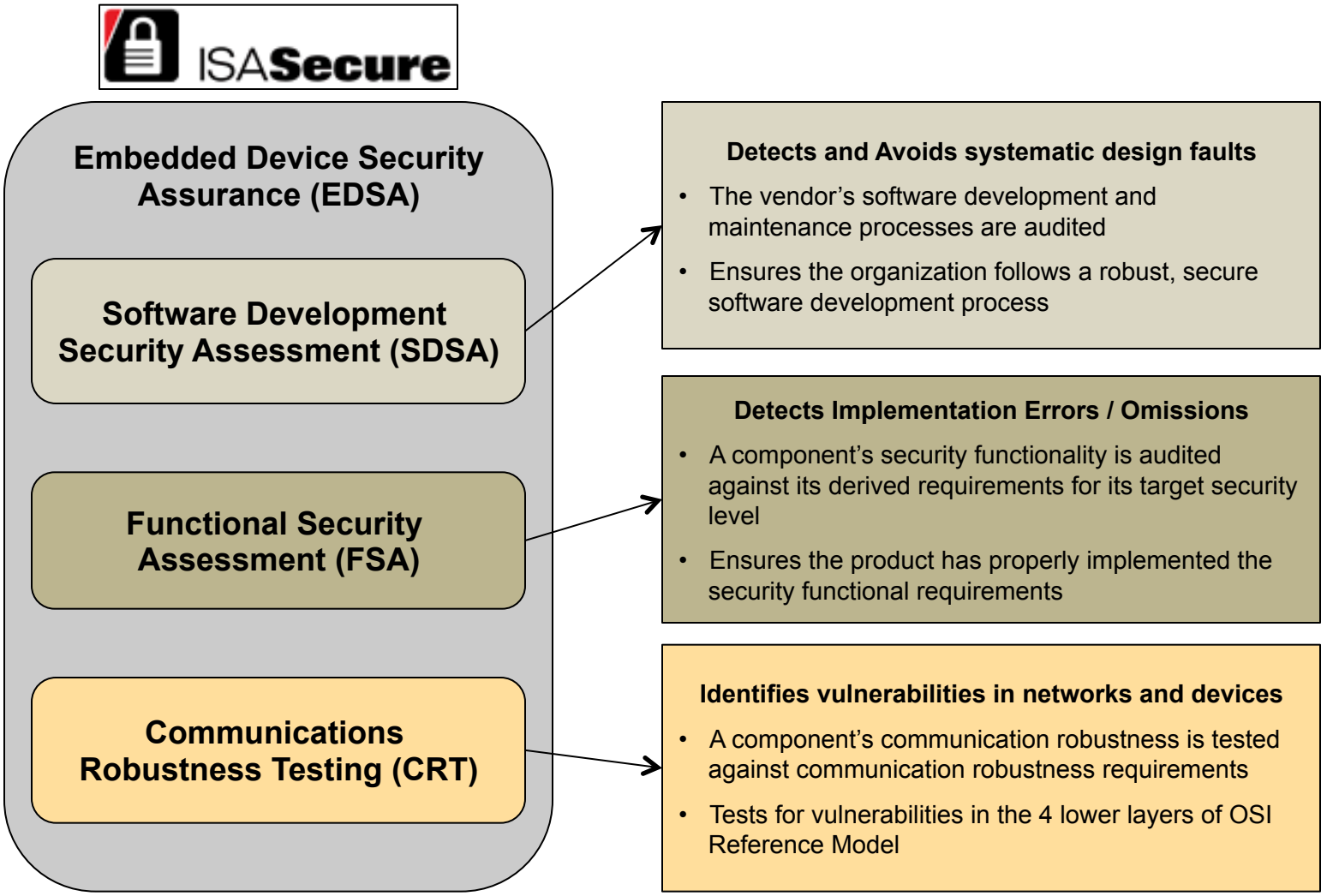
- Certification that the supplier's product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of ISA/IEC-62443-4-2 for embedded devices (will be aligned with 4-2 when formally approved by IEC)
- Currently available

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



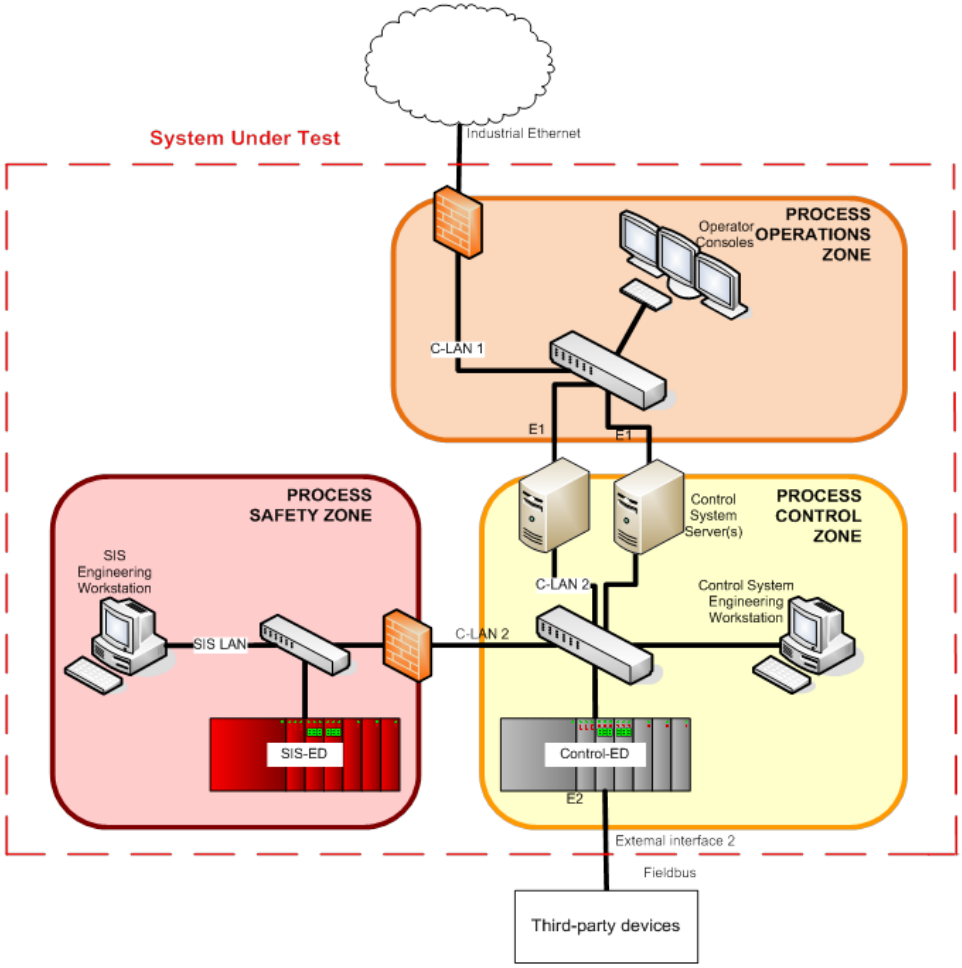
ISASecure™ System Security Assurance (SSA)

SSA Overview

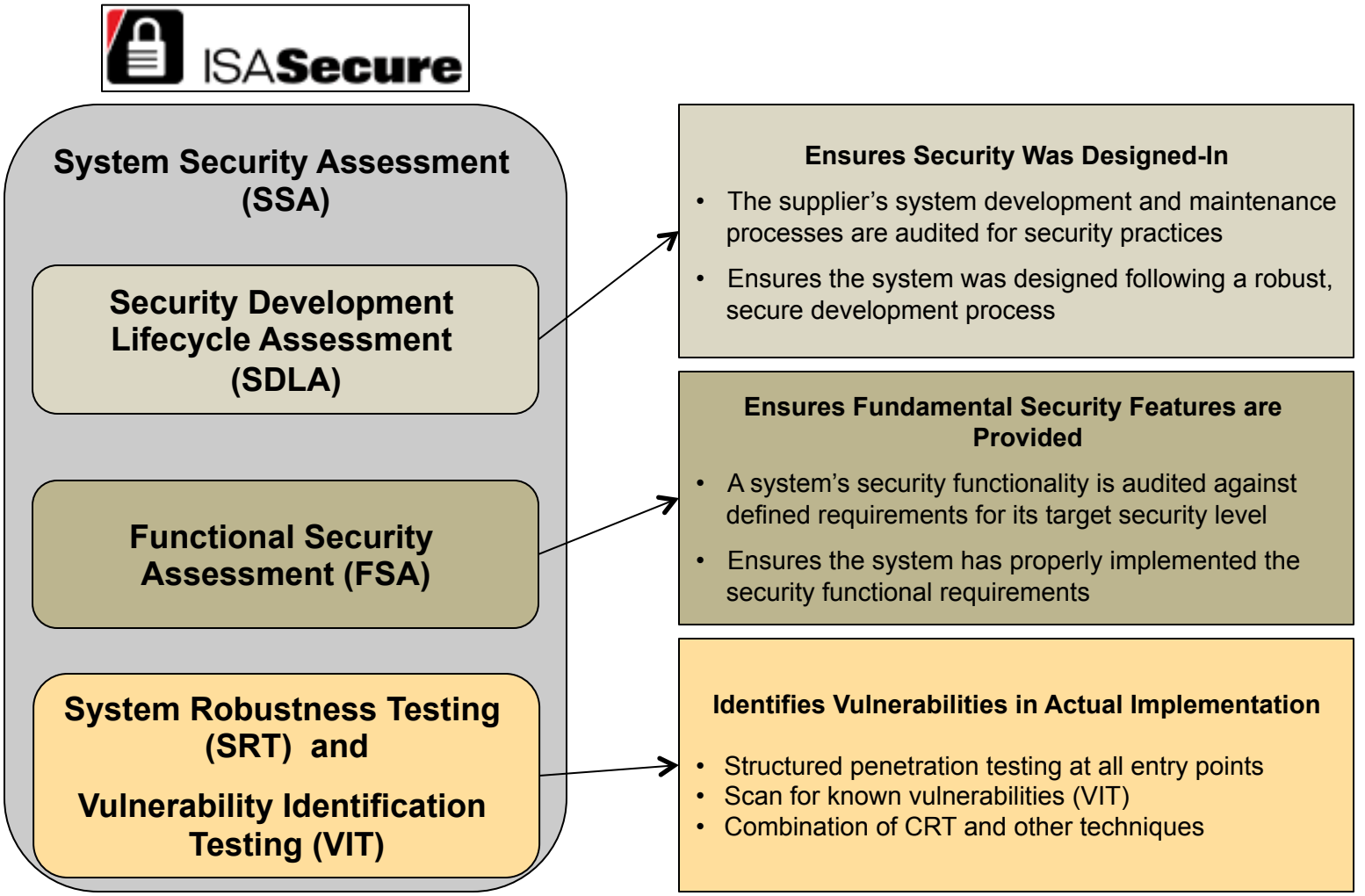
- Certification that the supplier's product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of ISA/IEC-62443-3-3
  (SSA was aligned with 3-3 by ISCI when it was approved by IEC)
- Available as of Q1 2014

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



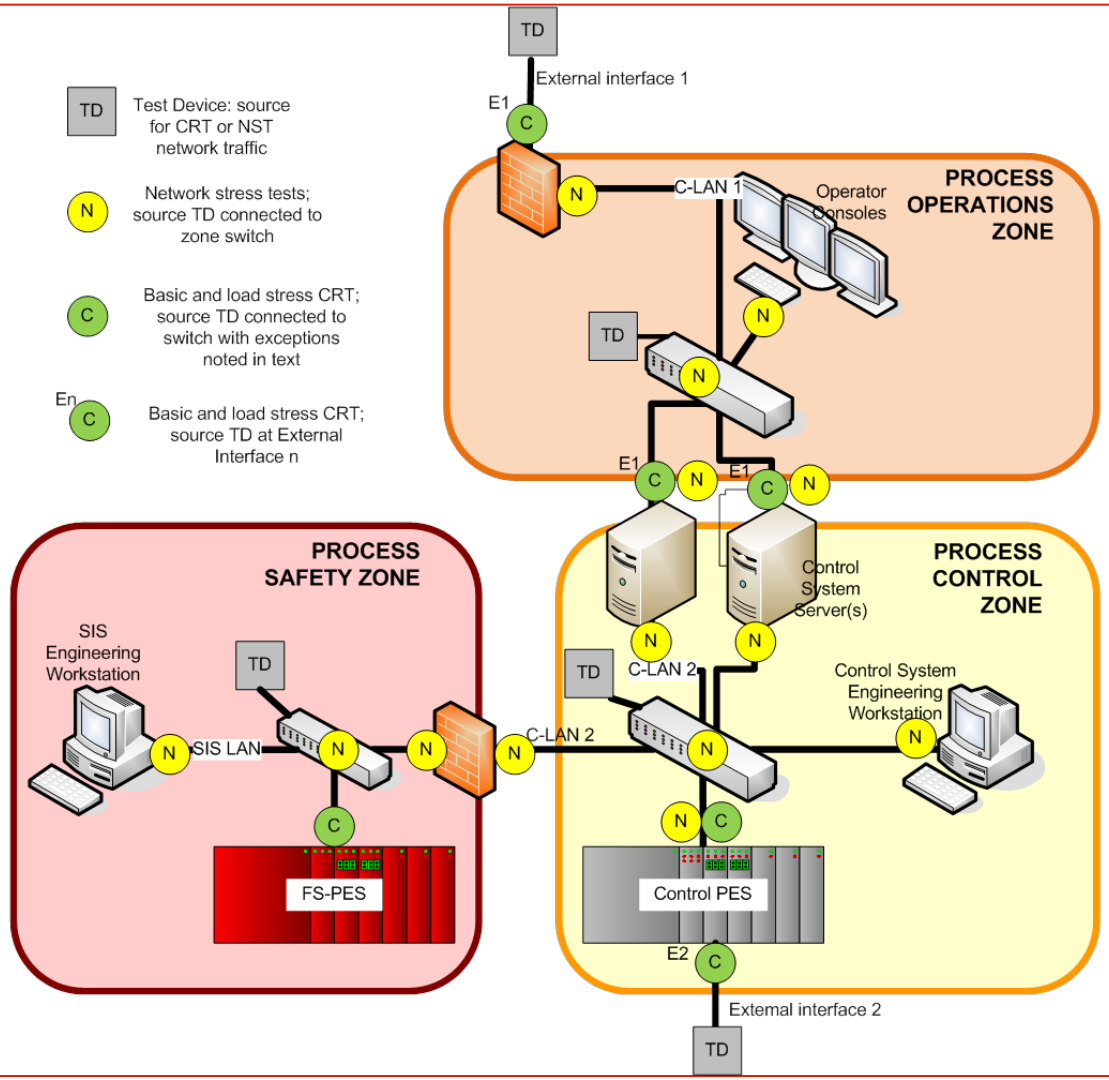
ISASecure SSA Certification Program



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



ISASecure™ Security Development Lifecycle Assurance (SDLA)

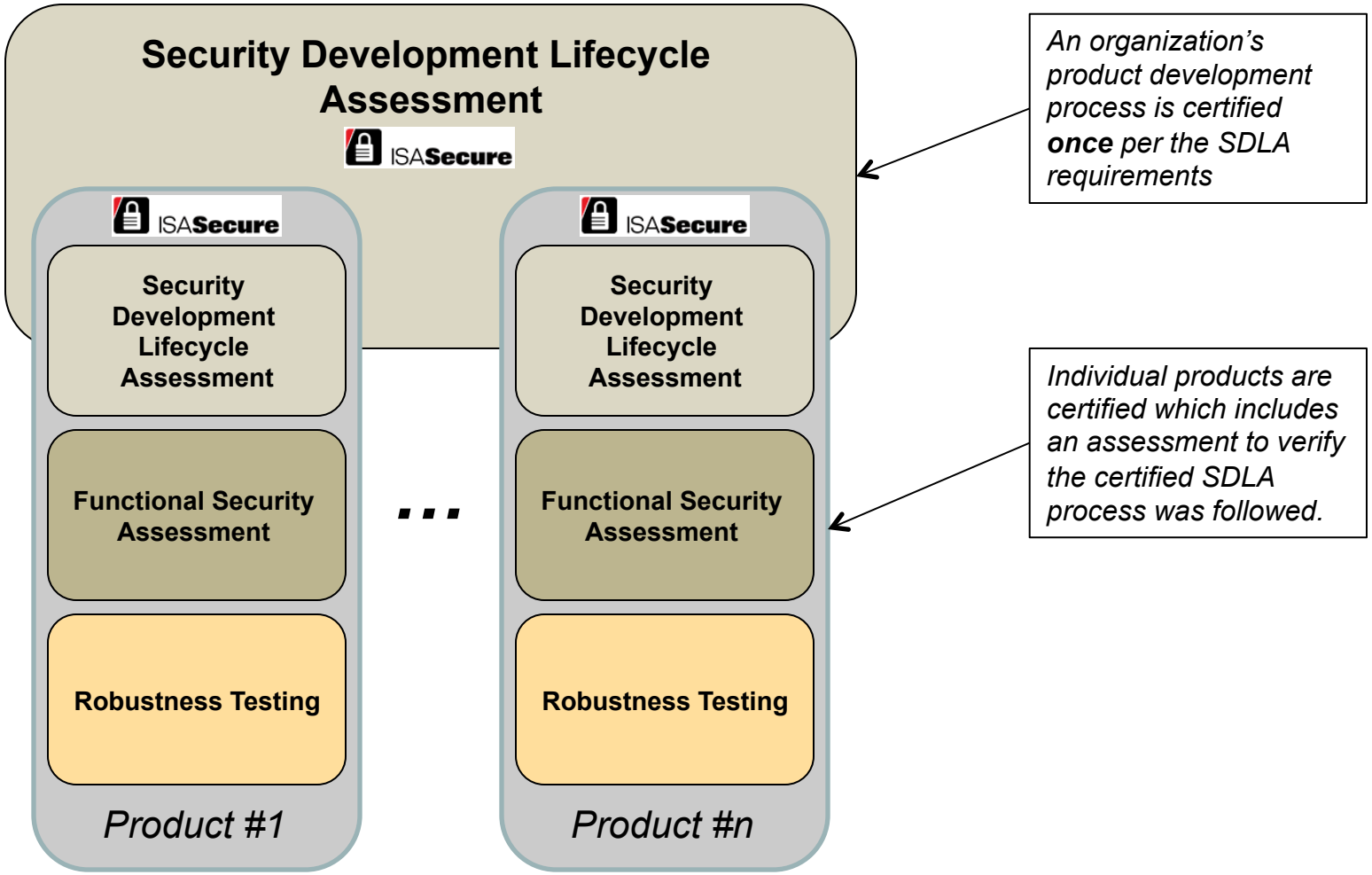
SDLA Overview

- 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 in June 2014

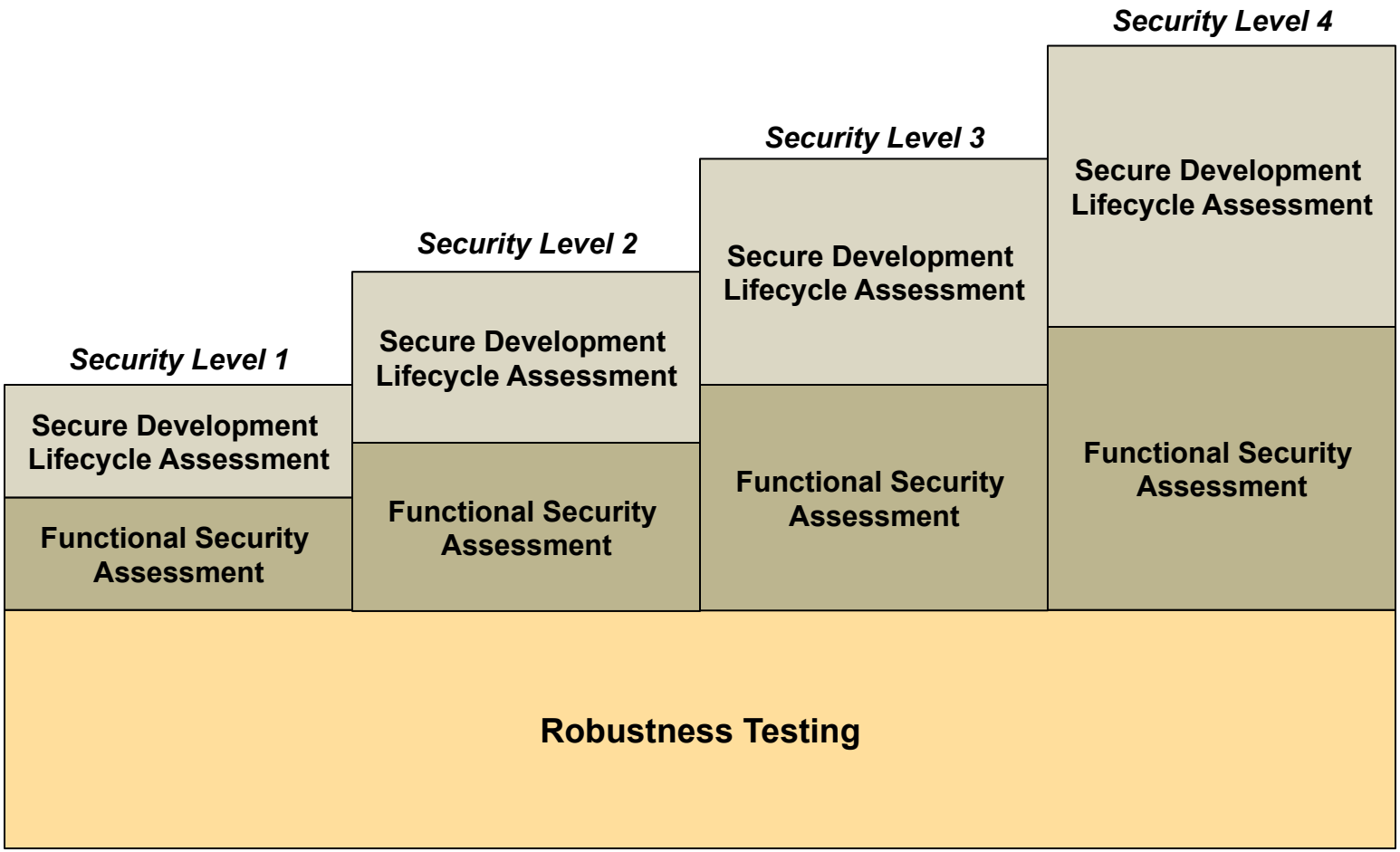
SDLA Phases

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 Levels



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

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)

ISA 62443 Status (Oct, 2013)