

# ISA Security Compliance Institute

Andre Ristaino, Managing Director, ISCI

28 May 2013

CSSC

# agenda topics

---

- About ISA Security Compliance Institute (ISCI)
- About ISA 99 Standards
- 2013 ISCI Certification Programs:
  - Embedded Device Security Assurance (EDSA)
  - System Security Assurance (SSA)
  - Security Development Lifecycle Assurance (SDLA)

# 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 critical 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

# 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.

# Global Adoption

---

## Information-technology Promotion Agency, Japan

- Translated ISASecure specifications to Japanese
- Setting up a test lab in Tagajo city Japan
- JAB is undertaking the lab accreditation process
- Promoting ISASecure as part of the Japanese critical infrastructure security scheme.

# ISCI Member Companies

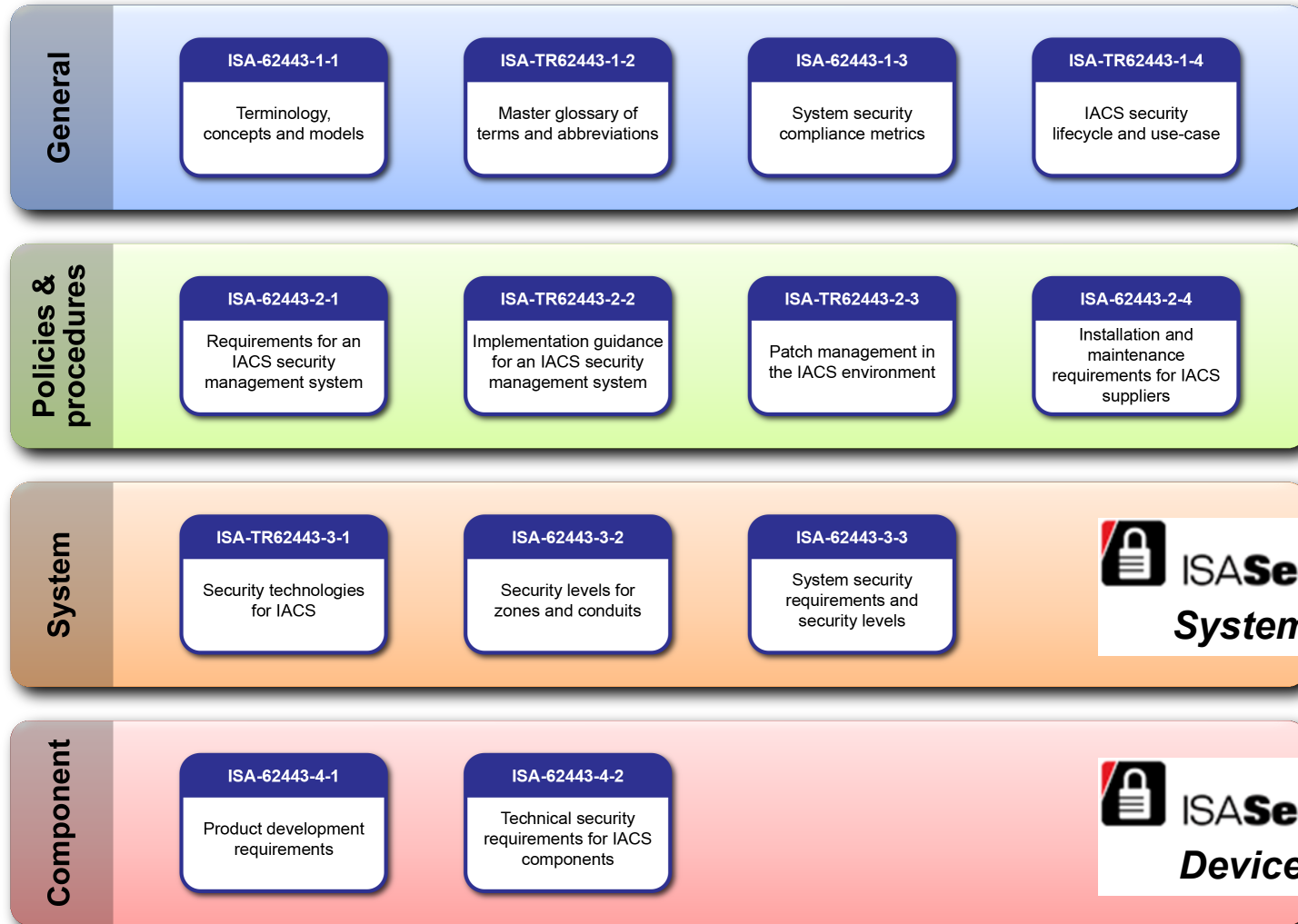
- ISCI membership is open to all organizations
  - Strategic membership
  - Technical membership
  - Government membership
  - Associate membership
  - Informational membership
- Member organizations
  - Chevron
  - exida
  - ExxonMobil
  - Honeywell
  - IT Promotion Agency, Japan (IPA)
  - Invensys
  - RTP Corp.
  - Siemens
  - Yokogawa
  - ISA99 Committee Liaison

# Key Global Challenges

---

- International Cybersecurity standards not yet complete.
- International baseline cybersecurity conformance scheme not fully adopted.
- Need Internationally recognized:
  - 1 standard
  - 1 conformance specification and test
  - 1 certification mark

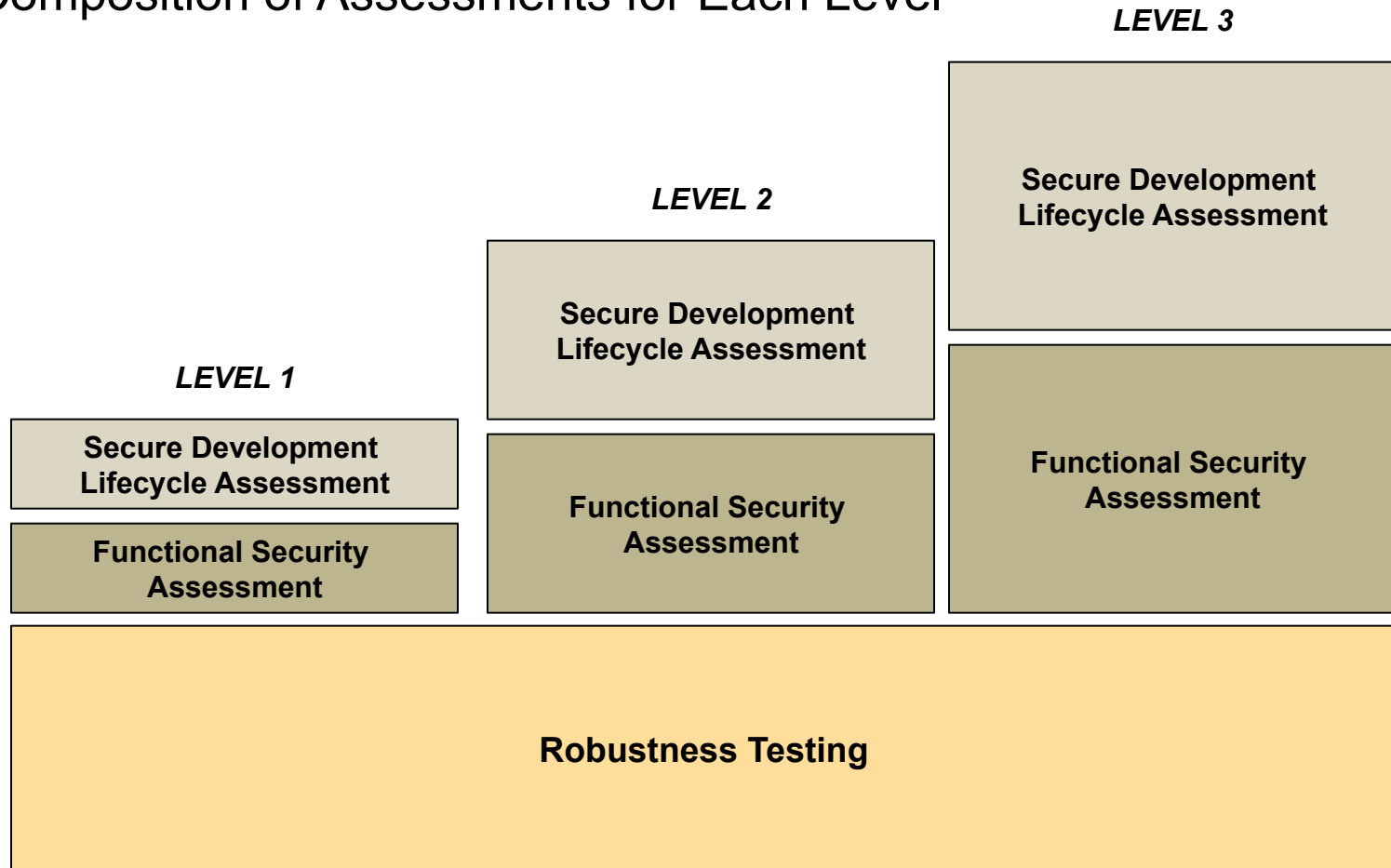
# About ISA99 Standards





# ISASecure Security Levels

## Composition of Assessments for Each Level





---

# **ISASecure™**

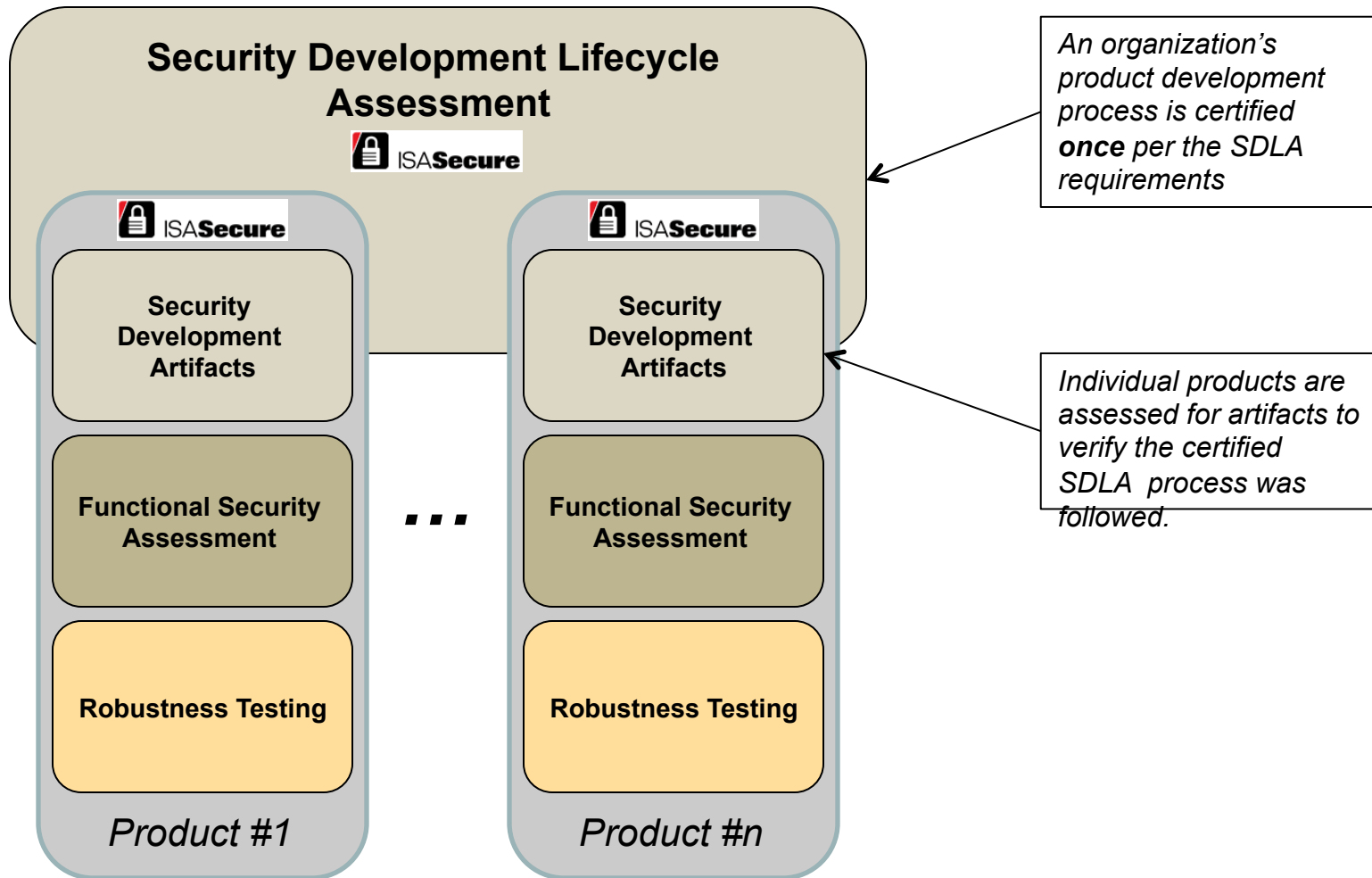
## **Security Development Lifecycle Assurance (SDLA)**

# 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





---

# **ISASecure™**

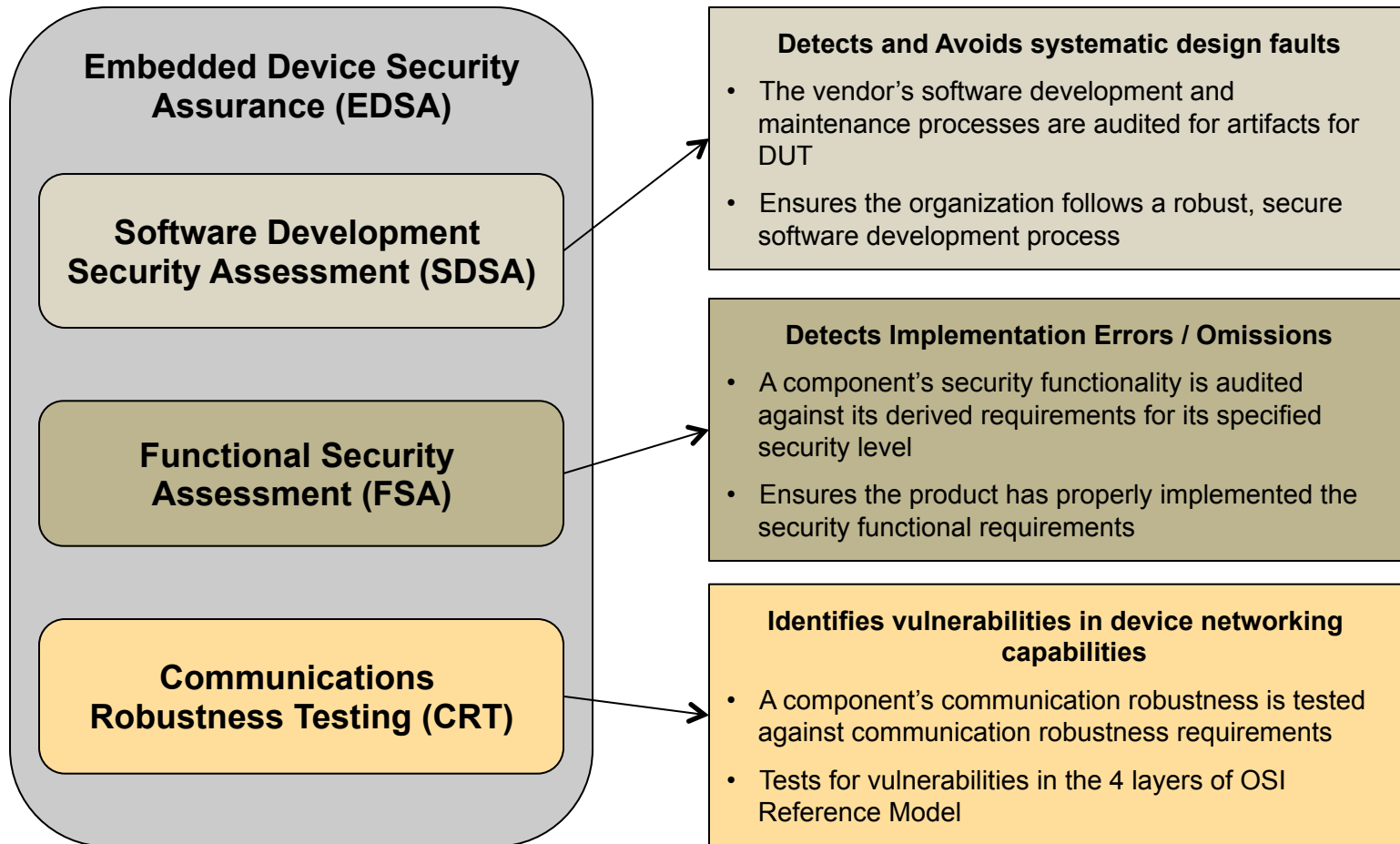
## **Embedded Device Security Assurance (EDSA)**

# 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 EDSA Certified Devices

Supplier	Type	Model	Version	ISASecure Level
Honeywell	Safety System	Safety Manager	R145	Level 1
RTP Corp.	Safety System	RTP 3000	A4.36	Level 2
Honeywell	DCS Controller	Experion C300	R400	Level 1
Honeywell	Fieldbus Interface	Experion FIM	R400	Level 1

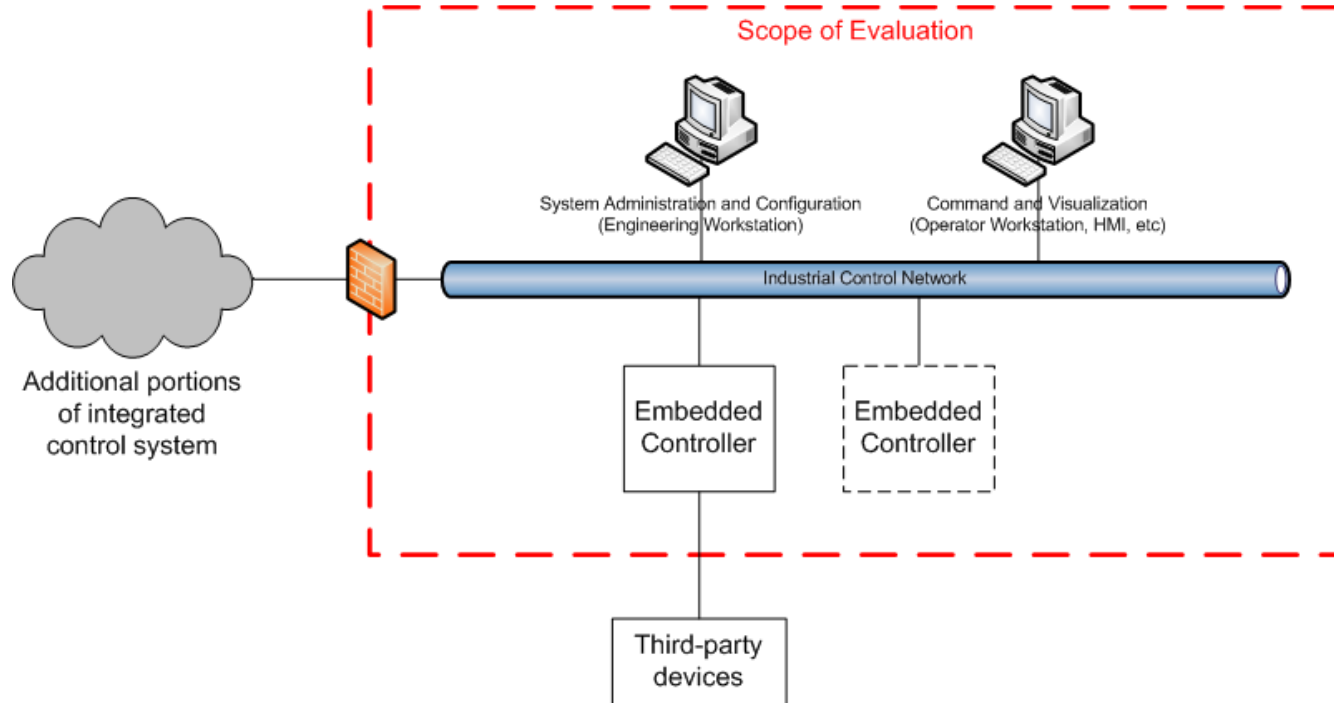




---

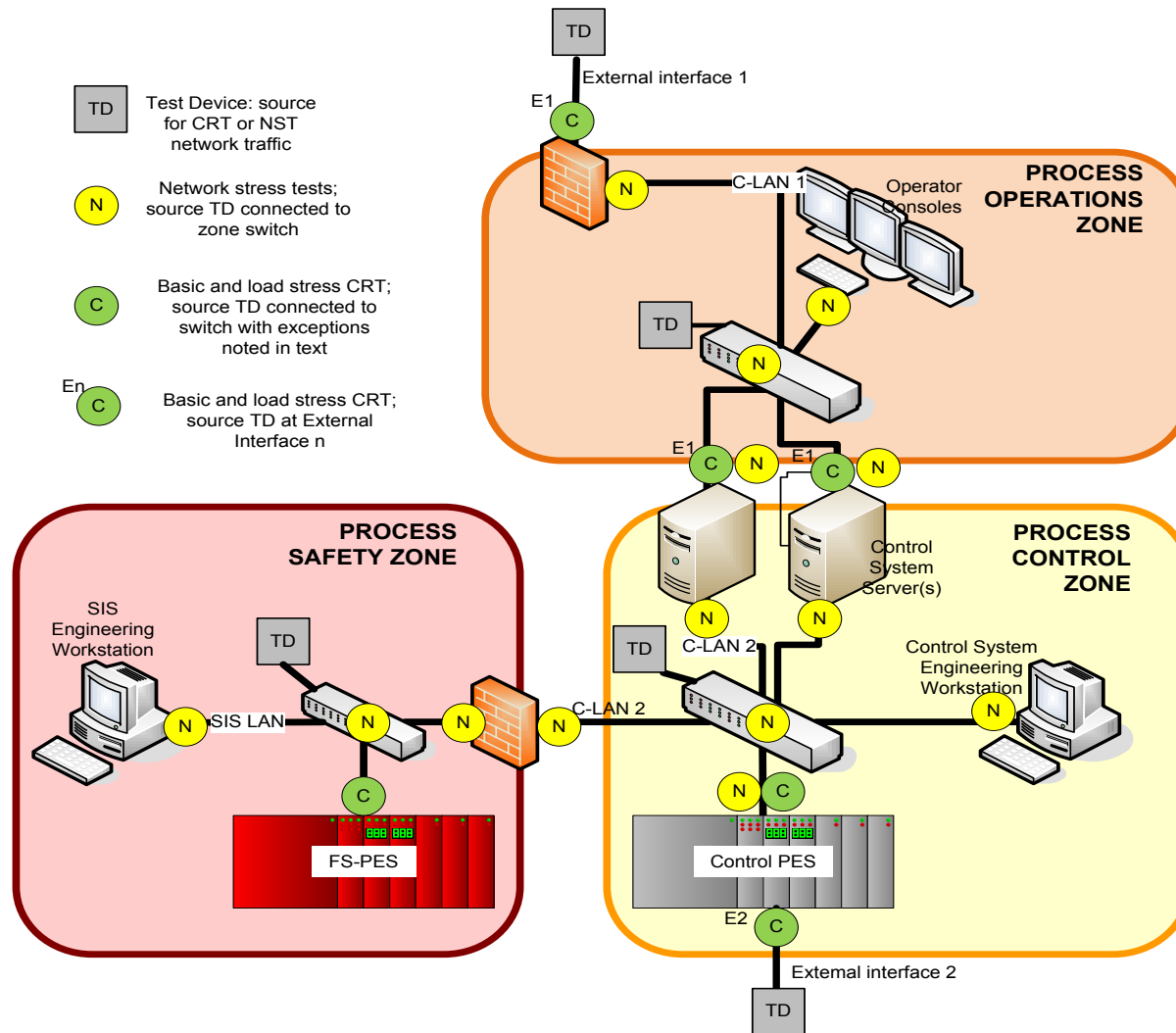
# **ISASecure™ System Security Assurance (SSA)**

# What is a System?

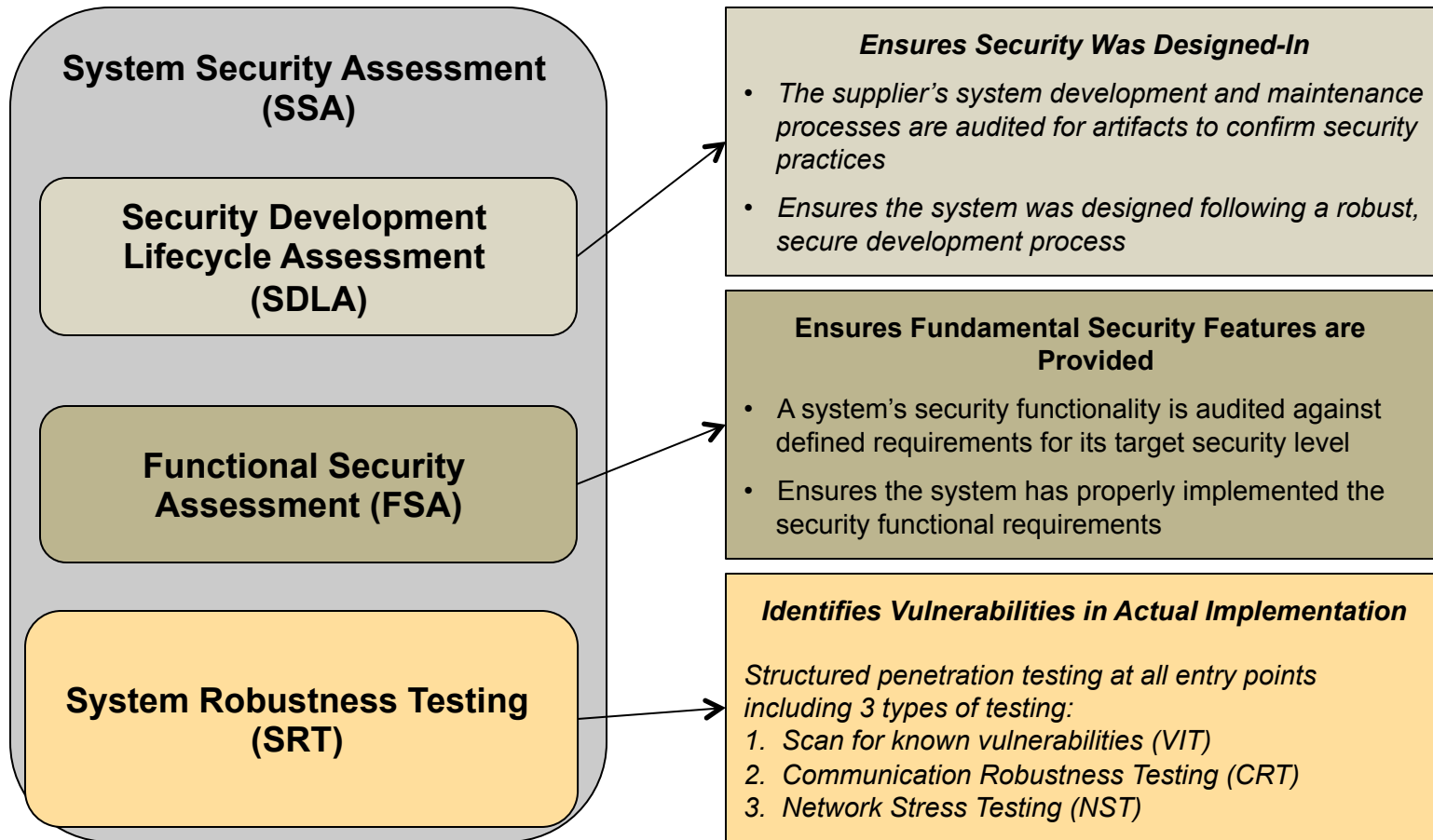


- An Industrial Control System (ICS) or SCADA system that is available from a single system supplier
- It may be comprised of hardware and software components from several manufacturers but must be integrated into a single system and supported, as a whole, by a single supplier

# Zones and Accessible Network Interfaces



# ISASecure SSA Certification Program



# Typical changes driven by the certification process

---

- Review / update Secure Development Lifecycle
- Security training for development and test teams
- Security experts identified for each development location
- New security documentation created
- Increased risk analysis and expanded threat modeling
- Expanded abuse case, DoS, and fuzz testing
- Tracking security issues / security impact of product issues

# Who to Contact to Certify Products

---

## 1. ISASecure EDSA Chartered Lab:

exida

John Cusimano

Director of Security Services

Phone: (215) 453-1720

Fax: (215) 257-1657

Email: [jcusimano@exida.com](mailto:jcusimano@exida.com)

Website: <http://www.exida.com>

## 2. Japan CSSC – Accepting submissions for product certifications starting 2014.

# Who to contact for ISCI Membership

---

Andre Ristaino

Managing Director, ASCI

Phone: 919-990-9222

Fax: 919-549-8288

Email: [aristaino@isa.org](mailto:aristaino@isa.org)

Website: <http://www.isasecure.org>