

ICSJWG Fall 2011

Update on the ISASecure™ Certification Program

Graham Speake, Principal Systems Architect, Yokogawa

Kevin Staggs, Engineering Fellow, Honeywell Automation
and Control

ISASecure™

www.isasecure.org

www.ansi.org/isasecure

Agenda

- ISA Security Compliance Institute (ISCI) Organization
- *ISASecure* Embedded Device Security Assurance Program
- *ISASecure* System Security Assurance (SSA) Program
- Who to contact for more information
- Questions



ISA Security Compliance Institute (ISCI) Organization

ISA Security Compliance Institute (ISCI)

Who We Are

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

ISCI Member Companies

- ISCI membership is open to all organizations
 - Strategic membership level
 - Technical membership level
 - Informational membership level
- Governing board
 - Chevron
 - ExxonMobil
 - Honeywell
 - Invensys
 - Siemens
 - Yokogawa
 - ISA99 Liaison – Eric Cosman, Dow

ISASecure Designation



- Trademarked designation that provides instant recognition of product security characteristics and capabilities.
- Independent Industry stamp of approval.
- Similar to 'Safety Integrity Level' Certification (ISO/IEC 61508).

ANSI/ACCLASS Accredited Conformance Scheme

ISASecure Embedded Device Security Assurance (EDSA) certification accredited as an ISO/IEC Guide 65 conformance scheme by ANSI/ACCLASS. This includes both ISO/IEC 17025 and ISO/IEC 17011.

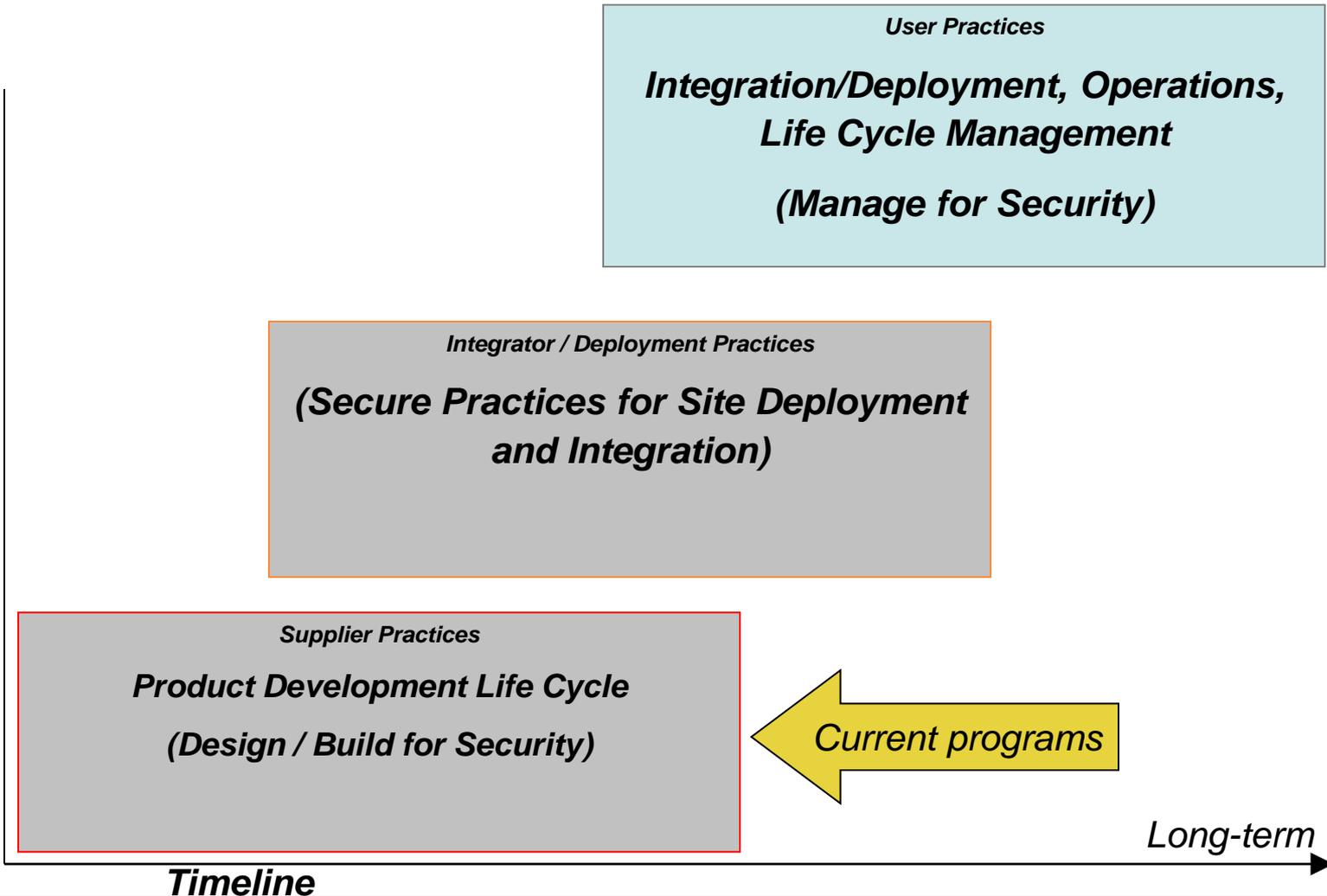
Go to www.ansi.org/isasecure for details.

1. Provides global recognition for ISASecure certification
2. Independent CB accreditation by ANSI/ACCLASS
3. ISASecure can scale on a global basis
4. Ensures certification process is open, fair, credible, and robust.

ISASecure Supplier Device Approval Process

- Supplier submits device to ANSI ACLASS chartered lab
- Chartered lab completes three part assessment
 - Physically evaluates device for functional security (FSA)
 - Conducts communication robustness test (CRT) using ISCI-approved test tool
 - Chartered lab completes supplier audit (SDSA) on software development practices
- Chartered lab issues final assessment report and certification upon successful test and audit

Scope and Direction of ISA Secure



ISA99 / IEC Reference Standards

General

<p>IEC 62443-1-1 (Ed. 2)</p> <p>ISA-62443.01.01 (99.01.01)</p> <p>Terminology, concepts and models</p> <p><i>Published as ISA-99.00.01-2007</i></p>	<p>IEC/TR 62443-1-2</p> <p>ISA-TR62443.01.02 (TR99.01.02)</p> <p>Master glossary of terms and abbreviations</p>	<p>IEC 62443-1-3</p> <p>ISA-62443.01.03 (99.01.03)</p> <p>System security compliance metrics</p>
---	---	--

Policies & procedures

<p>IEC 62443-2-1 (Ed. 2)</p> <p>ISA-62443.02.01 (99.02.01)</p> <p>Establishing an IACS security program</p>	<p>IEC 62443-2-2</p> <p>ISA-62443.02.02 (99.02.02)</p> <p>Operating an IACS security program</p>	<p>IEC/TR 62443-2-3</p> <p>ISA-TR62443.02.03 (TR99.02.03)</p> <p>Patch management in the IACS environment</p>	<p>IEC 62443-2-4</p> <p>MC 2784 - X-10</p> <p>Certification of IACS supplier security policies and practices</p>
---	--	---	--

“WIB Specification”

System

<p>IEC/TR 62443-3-1</p> <p>ISA-TR62443.03.01 (TR99.03.01)</p> <p>Security technologies for IACS</p> <p><i>Published as ISA-TR99.00.01-2007</i></p>	<p>IEC 62443-3-2</p> <p>ISA-62443.03.02 (99.03.02)</p> <p>Security assurance levels for zones and conduits</p>	<p>IEC 62443-3-3</p> <p>ISA-62443.03.03 (99.03.03)</p> <p>System security requirements and security assurance levels</p>
--	--	--

ISASecure SSA

Component

<p>IEC 62443-4-1</p> <p>ISA-62443.04.01 (99.04.01)</p> <p>Product development requirements</p>	<p>IEC 62443-4-2</p> <p>ISA-62443.04.02 (99.04.02)</p> <p>Technical security requirements for IACS components</p>
--	---

ISASecure EDSA

	Developed by ISA99		Published		In development
	Developed by WIB		Published (under review)		Out for comment/vote

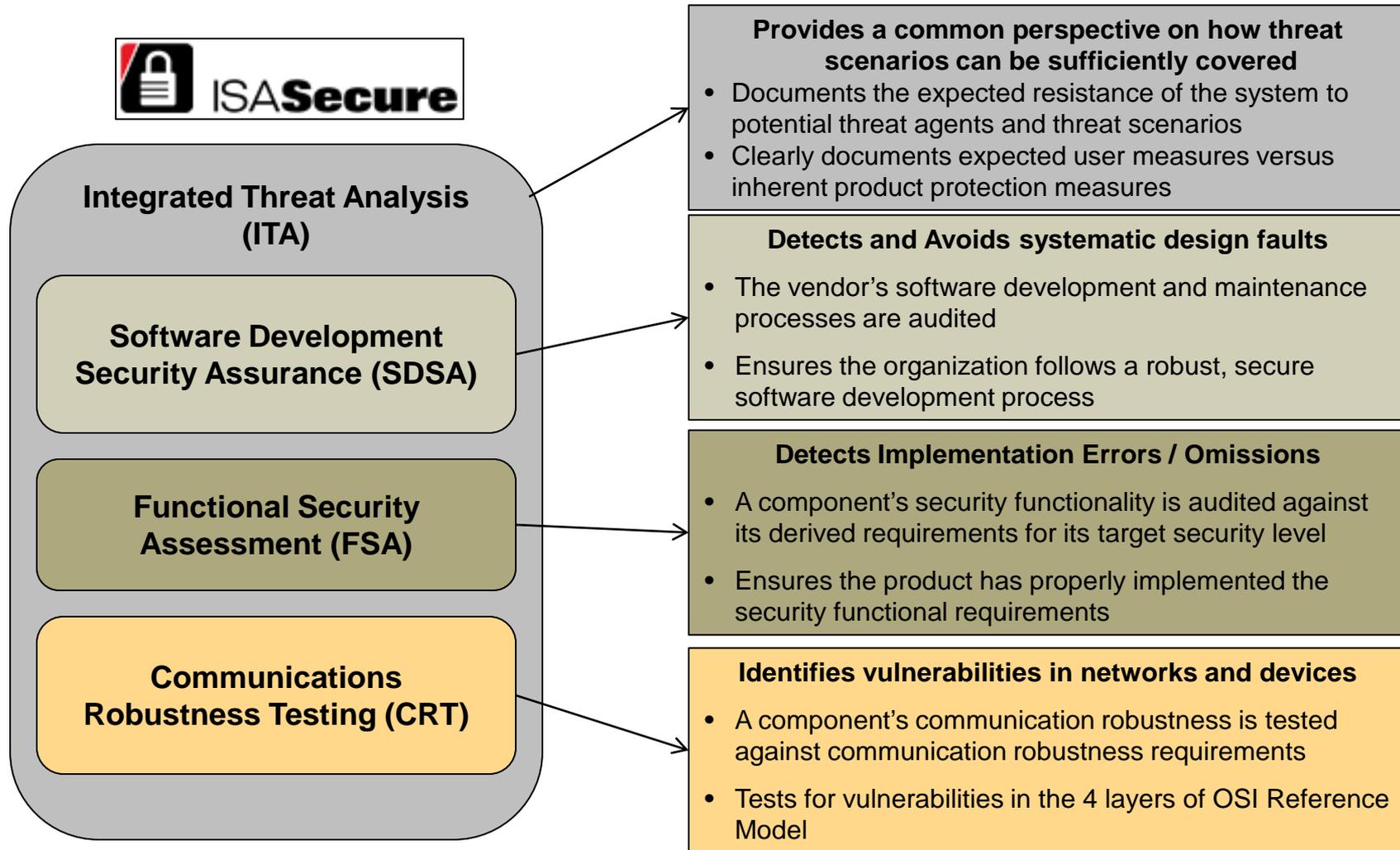


ISASecure Embedded Device Security Assurance Program

Embedded Device

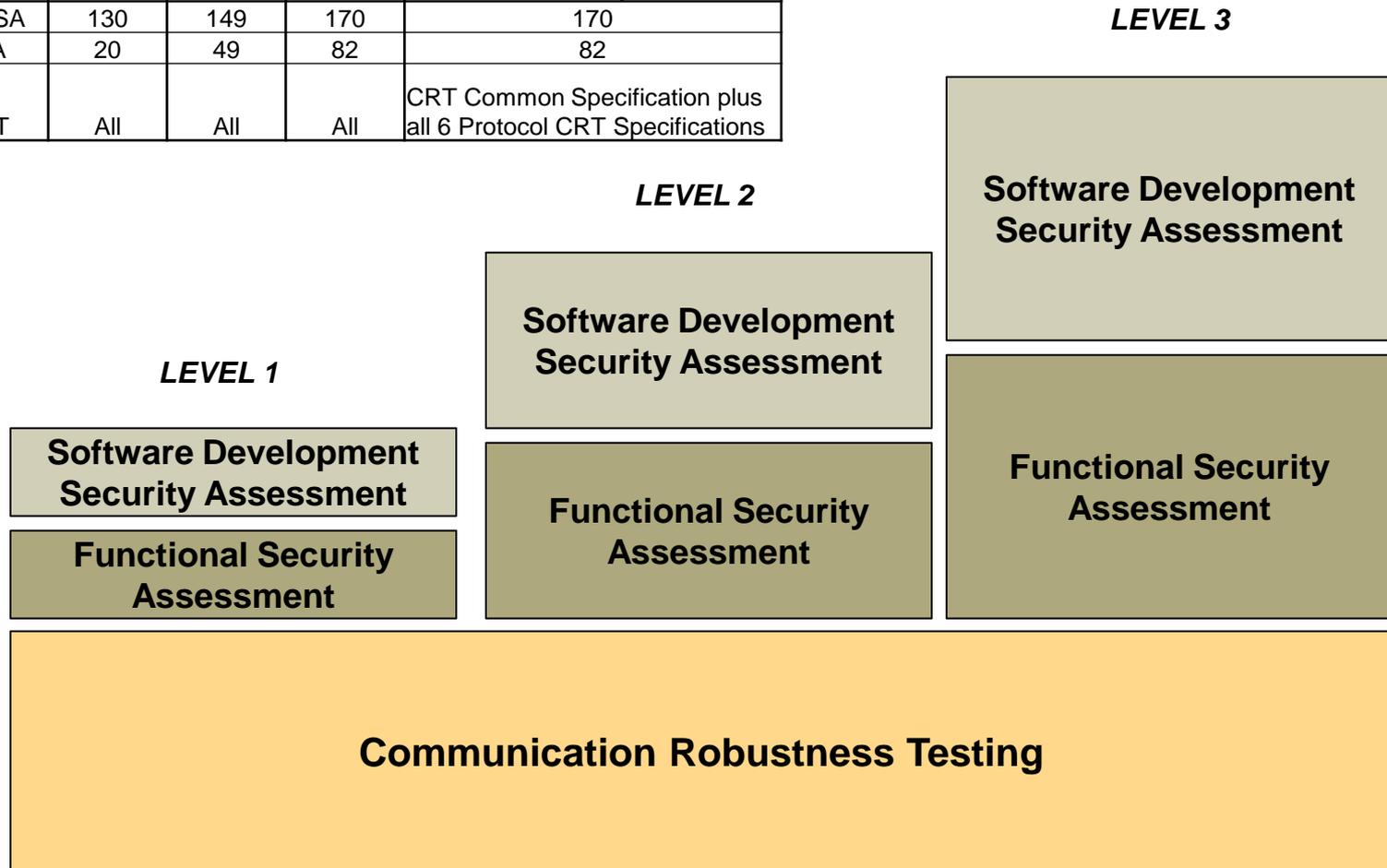
- Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process
- Examples:
 - Programmable Logic Controller (PLC)
 - Distributed Control System (DCS) controller
 - Safety Logic Solver
 - Programmable Automation Controller (PAC)
 - Intelligent Electronic Device (IED)
 - Digital Protective Relay
 - Smart Motor Starter/Controller
 - SCADA Controller
 - Remote Terminal Unit (RTU)
 - Turbine controller
 - Vibration monitoring controller
 - Compressor controller

Embedded Device Security Assurance Certification



ISASecure Levels

Requirements Necessary to Achieve Certification Levels				
	Level 1	Level 2	Level 3	Total Count in Specification
SDSA	130	149	170	170
FSA	20	49	82	82
CRT	All	All	All	CRT Common Specification plus all 6 Protocol CRT Specifications





ISASecure™

System Security Assurance
(SSA) Program

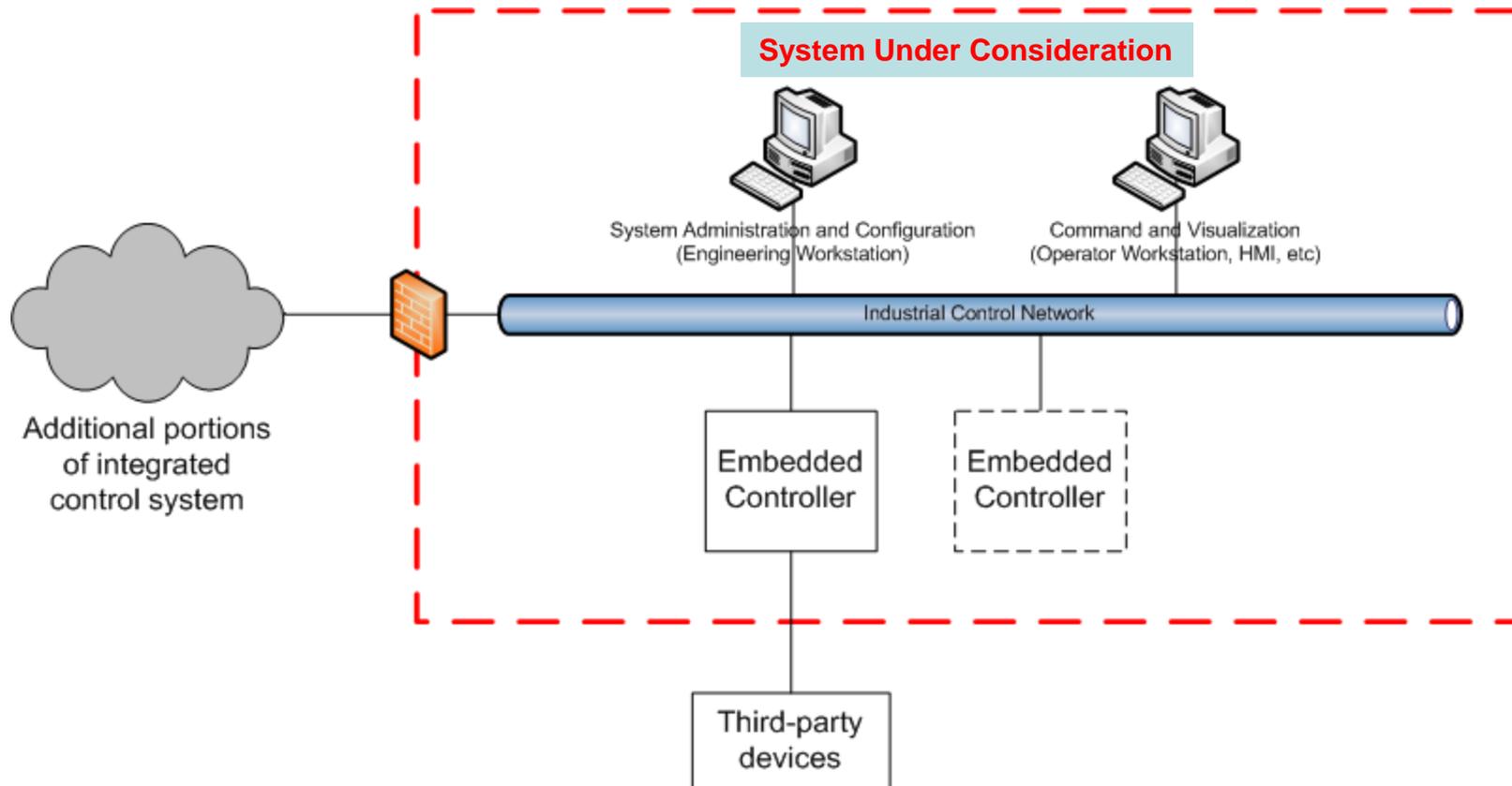
Objectives

- Move beyond device certification to a system-level security assessment including:
 - Security Feature Assessment
 - Threat Coverage Assessment
 - System Robustness Testing
- Provide a defined set of system-level security criteria allowing for consistent, unbiased evaluation of systems against that criteria
- Define levels of certification corresponding to the SAL levels defined in ANSI/ISA 99.03.03

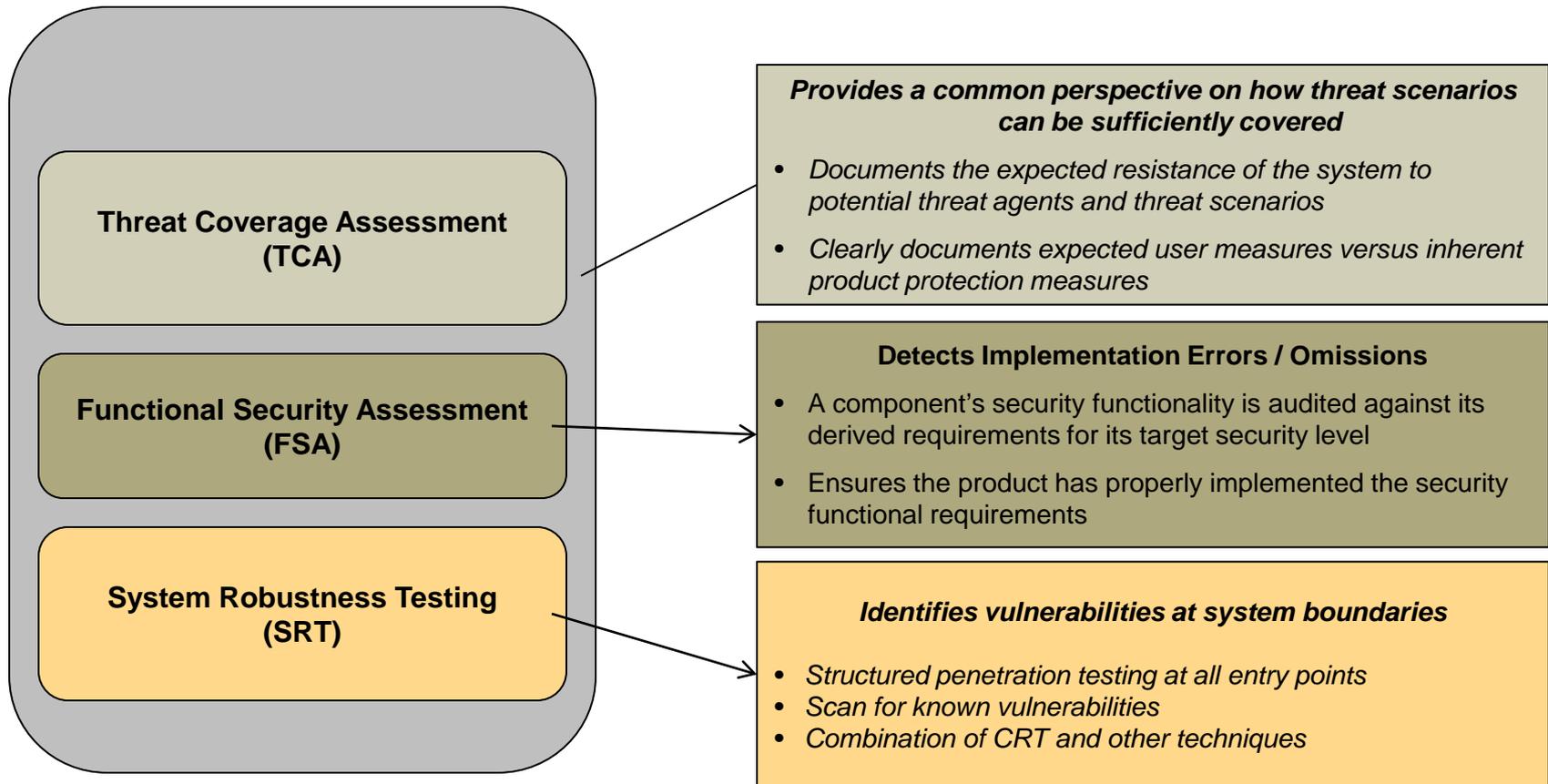
What is a ***System***?

- An Industrial Control System (ICS) or SCADA system that is available for purchase as a standard offering 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
- Evaluation is performed on reference system deployed with a set of assumed user environment and management constraints
- The scope of the *System under Consideration* (SUC) limited to what is expected to be typically deployed in a single security zone

Example System



ISASecure System Security Assurance (SSA) Certification



Threat Coverage Assessment

- The purpose is to identify inherent vulnerabilities in the system by analyzing the impact of threats against the system and to verify that the system mitigates threats above a certain risk threshold
- The applicant will perform threat modeling per the ISASecure SSA requirements
- ISASecure SSA also provides a minimum list of threats with assigned SAL levels that must be demonstrated to be mitigated in the assessment.
- The ISCI accredited certification body will perform a detailed review of the applicants threat model to determine if the requirements have been satisfied for the target SAL level.

Functional Security Assessment

- Assessment of the system's inherent (i.e. "out-of-the-box") security features and functionality
- Requirements derived from draft IEC 62443-3-3 (ANSI/ISA 99.03.03)
- Organized by 7 Foundation Requirements
- The ISCI accredited certification body will perform a detailed review of the system to determine if the requirements have been satisfied for the target SAL level.

System Robustness Testing

- The purpose of SRT is to evaluate the ability of the system to tolerate or mitigate attacks designed to exploit known vulnerabilities in industrial control systems
- Structured penetration-style testing at all entry points to the system using a combination of ISASecure CRT and other techniques to detect and exploit known vulnerabilities

ISA99 / IEC Reference Standards

General

<p>IEC 62443-1-1 (Ed. 2)</p> <p>ISA-62443.01.01 (99.01.01)</p> <p>Terminology, concepts and models</p>	<p>IEC/TR 62443-1-2</p> <p>ISA-TR62443.01.02 (TR99.01.02)</p> <p>Master glossary of terms and abbreviations</p>	<p>IEC 62443-1-3</p> <p>ISA-62443.01.03 (99.01.03)</p> <p>System security compliance metrics</p>
--	---	--

Published as ISA-99.00.01-2007

Policies & procedures

<p>IEC 62443-2-1 (Ed. 2)</p> <p>ISA-62443.02.01 (99.02.01)</p> <p>Establishing an IACS security program</p>	<p>IEC 62443-2-2</p> <p>ISA-62443.02.02 (99.02.02)</p> <p>Operating an IACS security program</p>	<p>IEC/TR 62443-2-3</p> <p>ISA-TR62443.02.03 (TR99.02.03)</p> <p>Patch management in the IACS environment</p>	<p>IEC 62443-2-4</p> <p>MC 2784 - X-10</p> <p>Certification of IACS supplier security policies and practices</p>
---	--	---	--

"WIB Specification"

System

<p>IEC/TR 62443-3-1</p> <p>ISA-TR62443.03.01 (TR99.03.01)</p> <p>Security technologies for IACS</p>	<p>IEC 62443-3-2</p> <p>ISA-62443.03.02 (99.03.02)</p> <p>Security assurance levels for zones and conduits</p>	<p>IEC 62443-3-3</p> <p>ISA-62443.03.03 (99.03.03)</p> <p>System security requirements and security assurance levels</p>
---	--	--

Published as ISA-TR99.00.01-2007

ISASecure SSA

Component

<p>IEC 62443-4-1</p> <p>ISA-62443.04.01 (99.04.01)</p> <p>Product development requirements</p>	<p>IEC 62443-4-2</p> <p>ISA-62443.04.02 (99.04.02)</p> <p>Technical security requirements for IACS components</p>
--	---

ISASecure EDSA

	Developed by ISA99		Published		In development
	Developed by WIB		Published (under review)		Out for comment/vote



Who to contact for more information

Who to contact for ISCI Membership

Andre Ristaino

Managing Director, ASCI

Direct Phone: 919-990-9222

Fax: 919-549-8288

Email: aristaino@isa.org

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

Who to Contact to Certify Products

ISASecure EDSA Chartered Lab

exida

John Cusimano

Director of Security Services

Phone: (215) 453-1720

Fax: (215) 257-1657

Email: jcusimano@exida.com

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

Questions?

