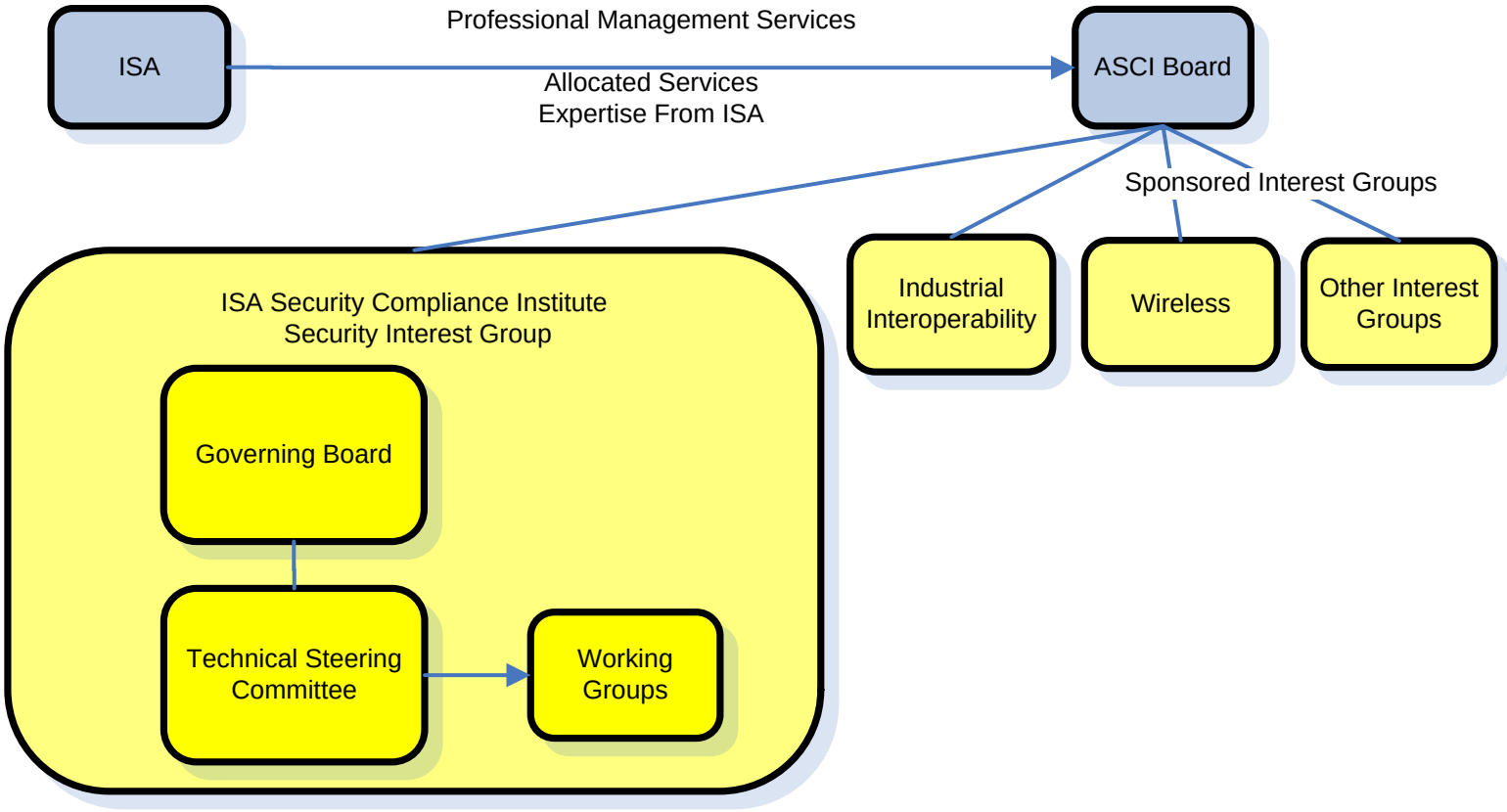
Role of Product Certification in an Overall Cyber Security Strategy

Tom Culling – Chevron
Andre Ristaino – ASCI
Kevin Staggs - Honeywell
John Cusimano – exida

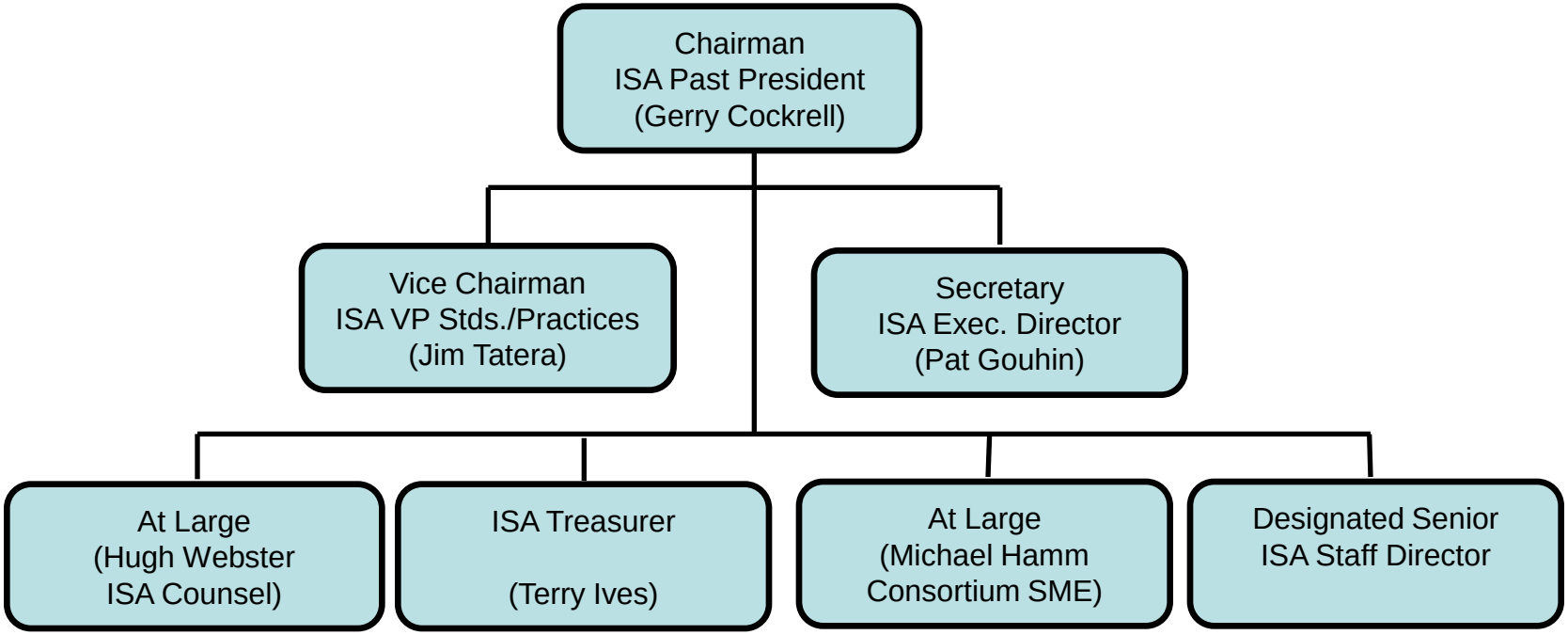
Agenda

- Who is the ISA Security Compliance Institute and Program Status
- Asset Owner – Role of Certifications
- EDSA Development Process and Relevance
- ISO/IEC accredited certification scheme
- Questions and Answers

An ISA Owned Organization



2010 ASCI Board of Directors



ISA Security Compliance Institute (ISCI)

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

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 - Who We Are

Founding Strategic Members

Chevron
ExxonMobil
Honeywell
Invensys
Siemens
Yokogawa

Technical Members

exida
Mu Dynamics
Rockwell Automation
Wurldtech Security Technologies

Industry Members

ISA99 Standards Committee (includes NIST, DHS, National Labs, Chemical Sector and others)

Informational Members

Egemin

What We Do

1. Collaboratively Define Industrial Automation Controls Security Test Specification (*ISASecure*)

2. Test Devices Against the ISASecure Requirements

3. Promote of the output of ISA99 IACS Security committee

4. Future initiatives expand aspects of the security lifecycle for security in deployment/integration and management/operation.

Expected Outcome

Provide the Automation Industry with conformance testing that can be integrated into the product development life cycle resulting in products that are intrinsically secure.

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).

ISASecure Program Status

Embedded Device Security Assurance

- Accreditations for Chartered Labs and CRT Tool Recognition start 30 May 2010
- Approved EDSA Certification Requirements and Specifications will be posted on www.isasecure.org website.

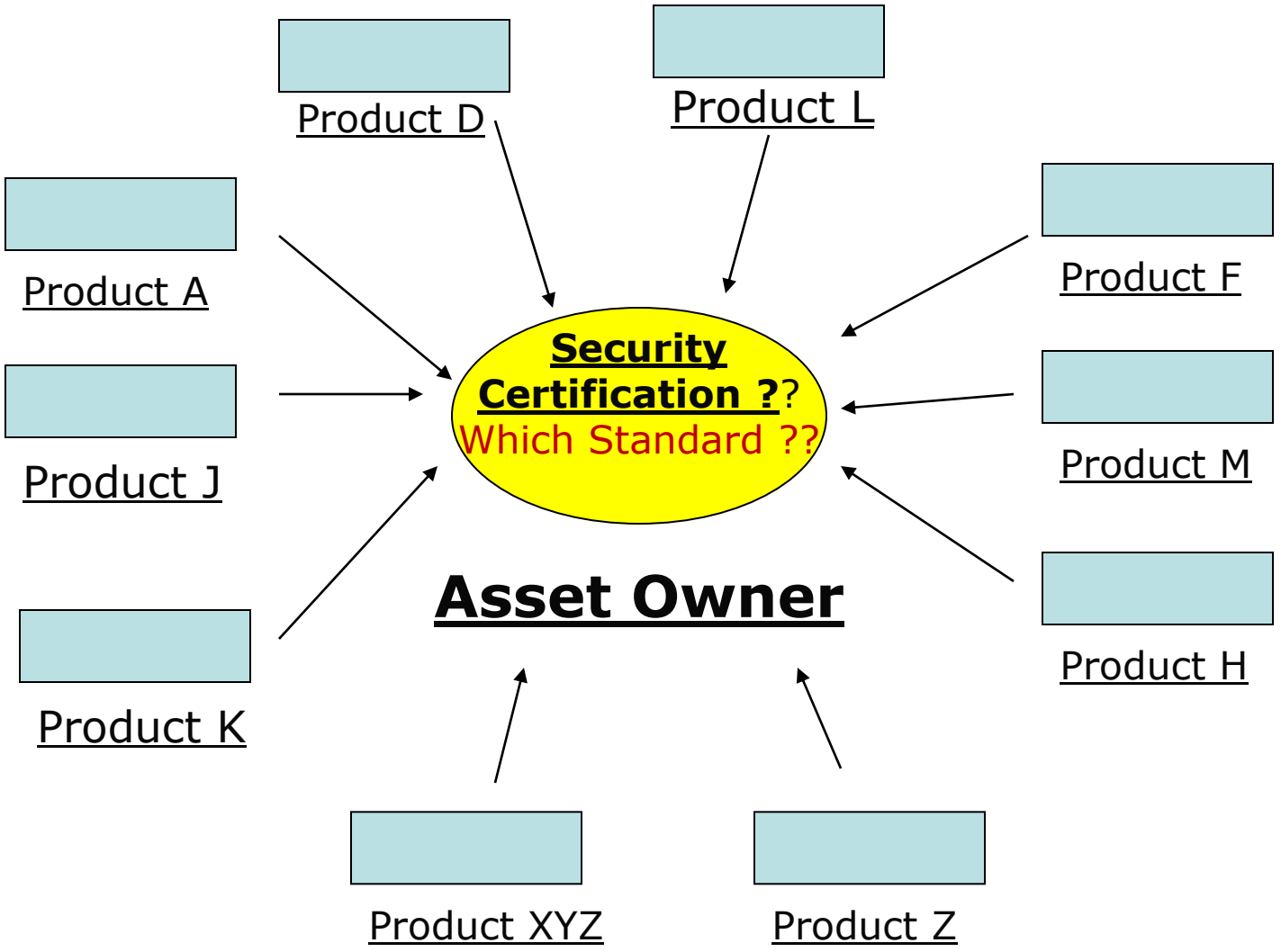
Asset Owner Perspective

Tom Culling – Chevron

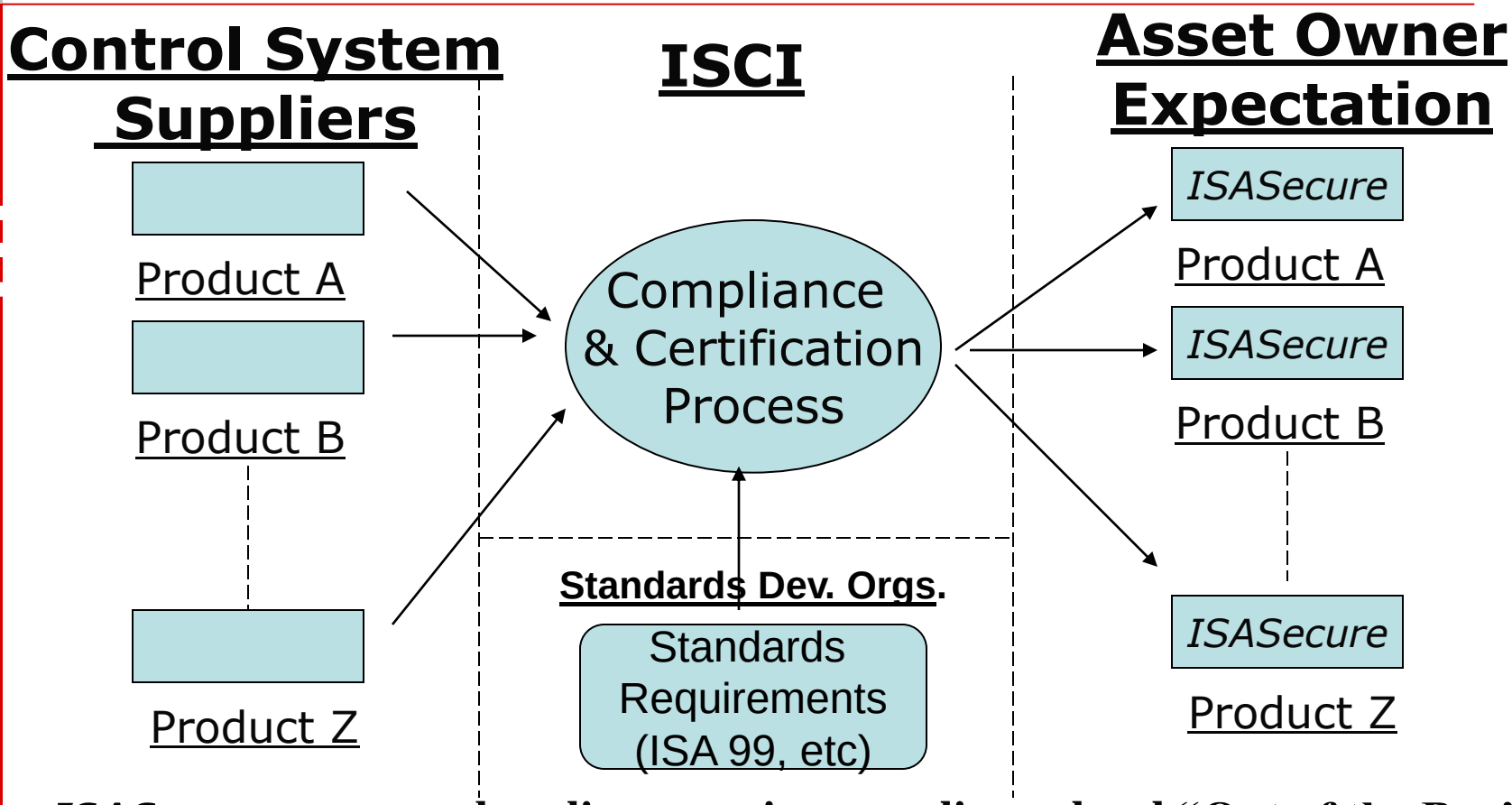
Control Systems Security

Subject Matter Expert

Current Condition



Asset Owner Expectation



ISASecure **assures a baseline security compliance level "Out of the Box" for Control System Products**

→ **Simplify procurement requirements process**

Asset Owners Communicate in One Voice

- Requirements developed on a collaborative basis by asset owners.
- Include ISASecure in procurement documents
  - provides clear, simple and consistent security requirements to suppliers.
- ISASecure Specification available for download at www.isasecure.org

Single Security Specification for Suppliers

- A single coherent security specification (ISASecure) in RFP's provides guidance to suppliers
- Streamlines supplier effort to respond to security requirements

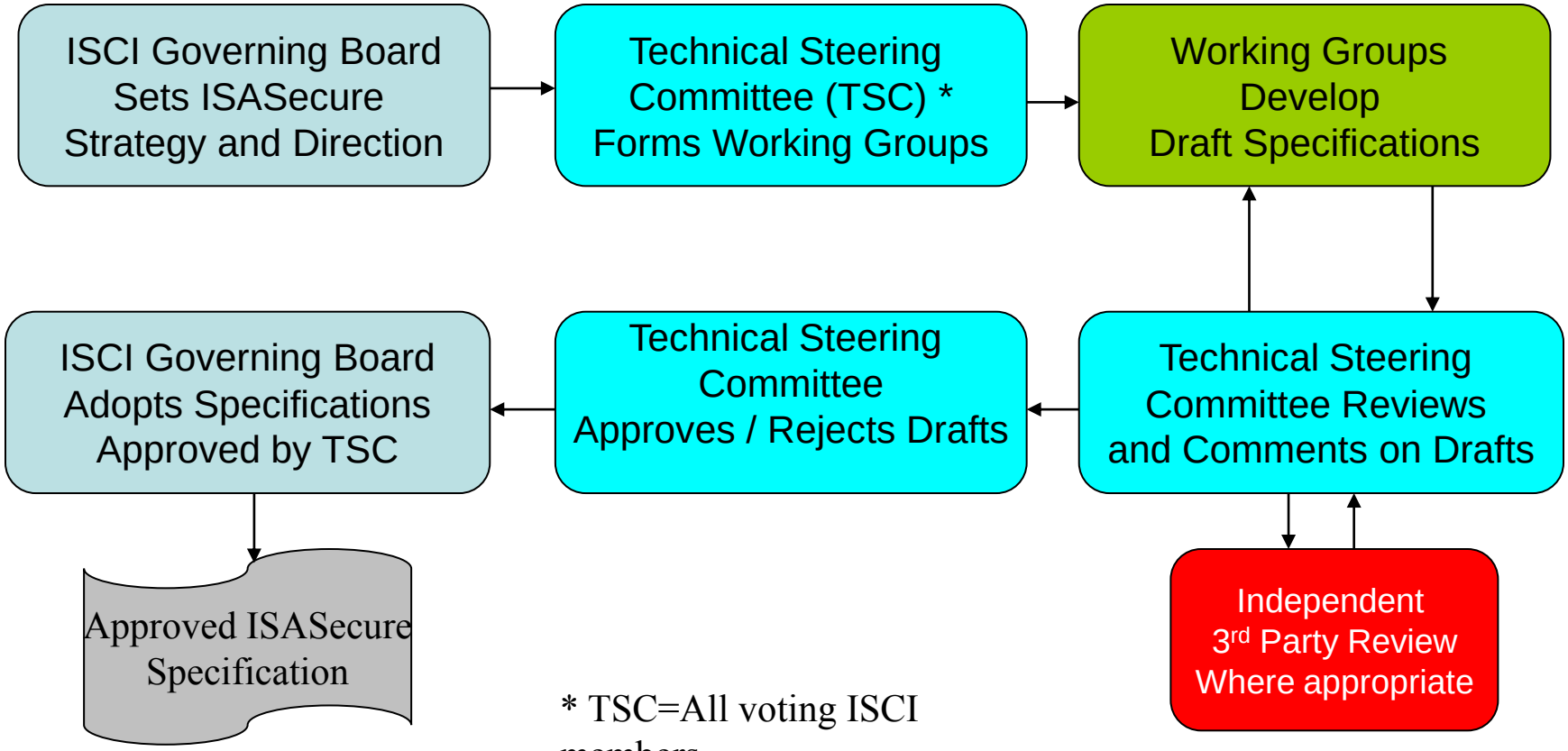
ISASecure EDSA Specification

John Cusimano – exida

Kevin Staggs - Honeywell

ISASecure Specification Development Process

ISCI is used draft ISA99 Derived Requirements framework as a basis for organizing ISASecure test specifications.



* TSC=All voting ISCI members

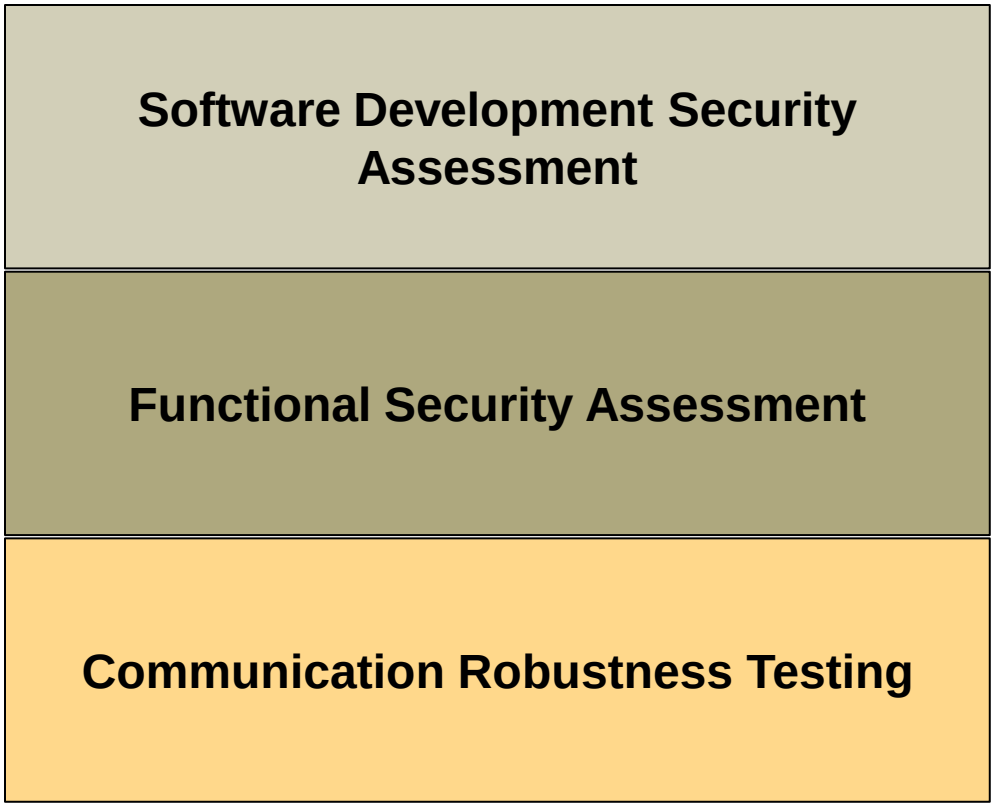
ISA99 Work Products

IEC 62443-xx-xx

July 2009

ISA99 Common	**ISA-99.01.01 Terminology, Concepts And Models**	**ISA-TR99.01.02** Master Glossary of Terms and Abbreviations	**ISA-99.01.03** System Security Compliance Metrics was ISA-99.03.03	
Security Program	**ISA-99.02.01** Establishing an IACS Security Program	**ISA-99.02.02** Operating an IACS Security Program	**ISA-TR99.02.03** Patch Management in the IACS Environment	
Technical - System	**ISA-TR99.03.01** Security Technologies for Industrial Automation and Control Systems was ISA-TR99.00.01-2007	**ISA-99.03.02** Security Assurance Levels for Zones and Conduits was Target Security Levels	**ISA-99.03.03** System Security Requirements and Security Assurance Levels was Foundational Requirements was ISA-99.01.03	**ISA-99.03.04** Product Development Requirements
Technical - Component	**ISA-99.04.01** Embedded Devices	**ISA-99.04.02** Host Devices	**ISA-99.04.03** Network Devices	**ISA-99.04.04** Applications, Data And Functions

Embedded Device Security Assurance Certification



Detects and Avoids systematic design faults

- The vendor's software development and maintenance processes are audited
- Ensures the organization follows a robust software development process

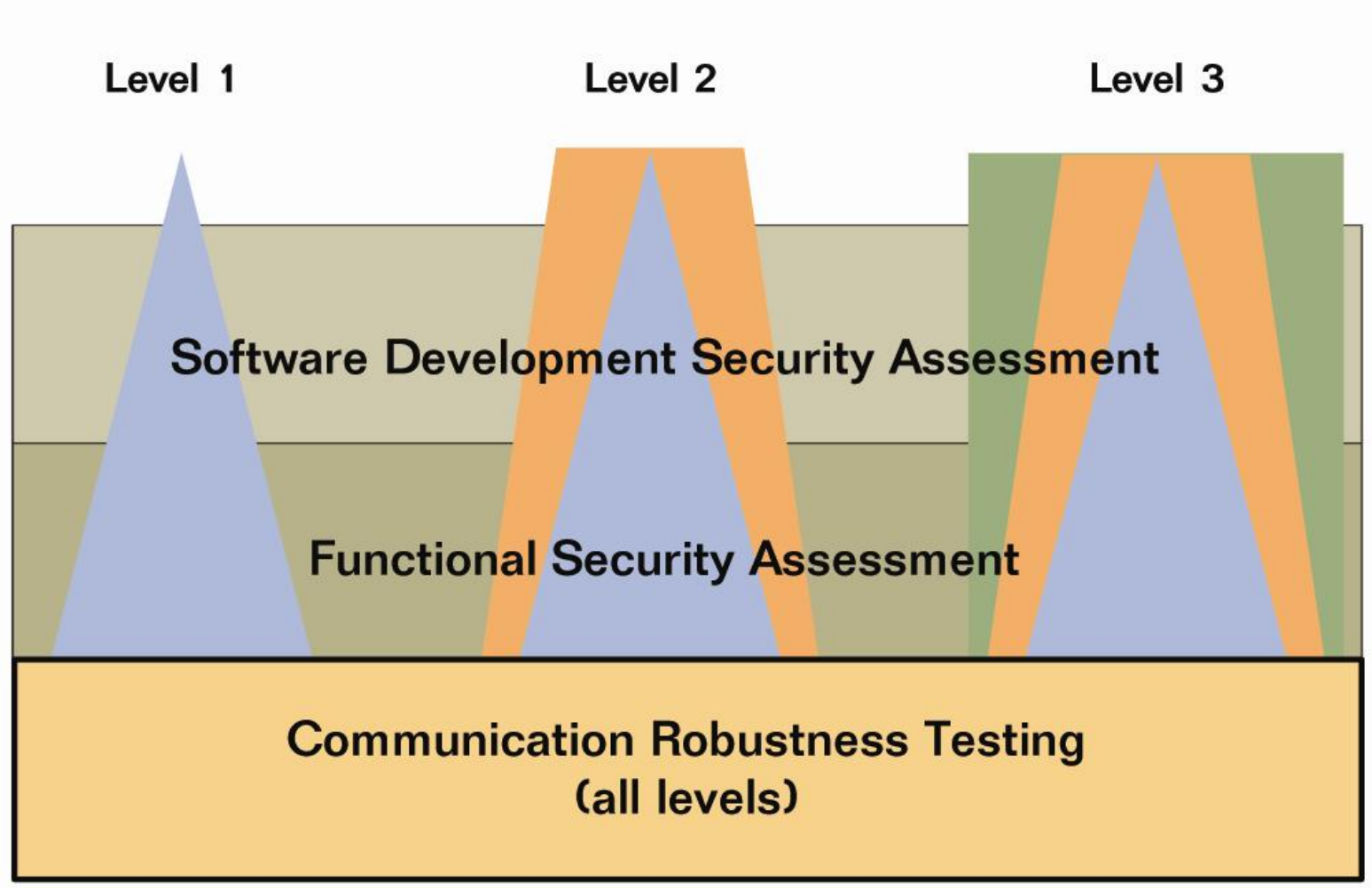
Detects Implementation Errors / Omissions

- 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 layers of OSI Reference Model

Embedded Device Security Assurance Certification



Communications Robustness Test (CRT)

Measures the extent to which network protocol implementations on an embedded device defends themselves and other device functions against unusual or intentionally malicious traffic received from the network.

Inappropriate message response (s), or failure of the device to continue to adequately maintain essential services, demonstrates potential security vulnerabilities within the device.

Communication Robustness Testing

Communications Robustness Testing Roadmap

Group 1	Group 2	Group 3	Group 4	Group 5
• IEEE 802.3 (Ethernet) • ARP • IPv4 • ICMPv4 • TCP • UDP	• BOOTP • DHCP • DNS • NTP, SNTP • FTP, TFTP • HTTP • SNMPv1-2 • Telnet	• HTTPS • TLS • Modbus/TCP	• IPv6 • OPC • Ethernet/IP/CIP • PROFINET • FFHSE • **Selected wireless** protocols/stacks with elements such as: IEEE 802.11 ISA100.11a WirelessHART	• SNMP v3 • SSH Server • OPC-UA • MMS • IEC 61850 • SMTP

Resources – Communication Robustness Testing

- ISO/IEC protocol standards and RFC's
- Centre for the Protection of National Infrastructure (CPNI) - Technical Note 3/2009 – Security Assessment of the Transmission Control Protocol (TCP)
- ISCI member vendor practices
- ISCI member asset owner protocol priorities

Functional Security Assessment (FSA)

Security Feature Tests

Purpose:

- Verification and validation that the device or system under test incorporates a minimum set of security features needed to counteract common security threats

Composition

- Set of requirements, derived from existing reference standards and traceable to source standard
- One or more acceptable solutions (countermeasures) identified for each requirement
- If applicable, procedures to verify the requirement has been satisfied

Functional Security Assessment Reference Standards

[N1]	ISA-99.01.03D2-20090527	Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels ISA-99.01.03
[N2]	NERC Standards CIP-001-1 through CIP-001-9	North American Electric Reliability Council Cyber Security Standards
[N3]	NIST 800-53	Recommended Security Controls for Federal Information Systems
[N4]	ISO/IEC 15408-1 through I5408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
[N5]		Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers

Software Security Development Assessment

Secure Software Engineering

Purpose:

- Verification and validation that software for the device or system under test was developed following appropriate engineering practices to minimize software errors that could lead to security vulnerabilities. **Not necessary to repeat the assessment if multiple products are developed by the same organization.**

Composition

- Set of requirements, derived from existing reference standards and traceable to source standard (IEC 61508, ISO/IEC 15408)
- One or more acceptable arguments identified for each requirement

Software Development Security Assessment

SDSA Specification Development

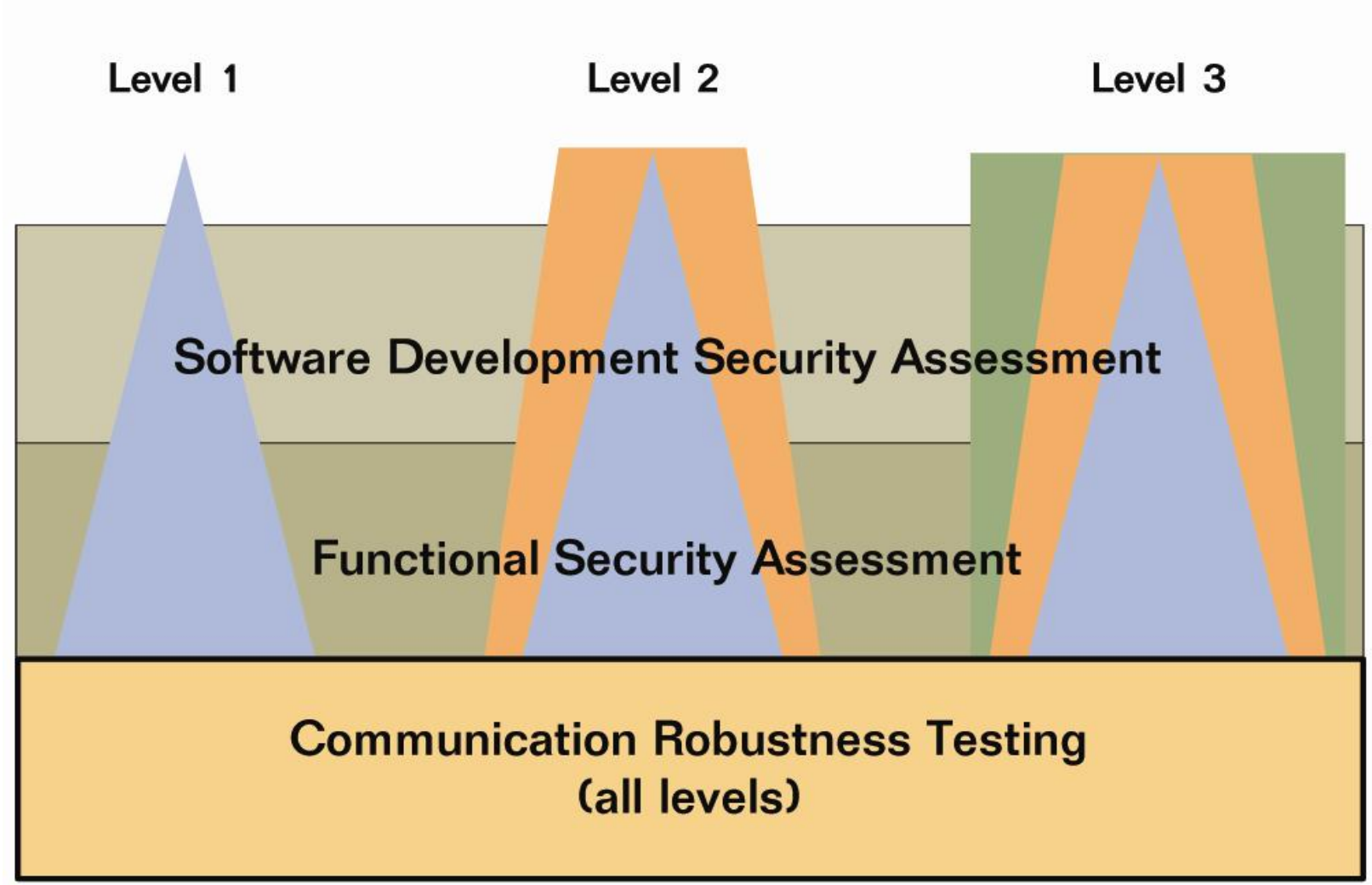
Reference Standards for Software Development Security Assessment		
[N4]	ISO/IEC 15408-1 through I5408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
[N6]	IEC 61508 Part 3	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software Development
[N7]	RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certifications
[N8]	ISBN-13: 978-0735622142	The Security Development Lifecycle, M. Howard, S. Lipner, Microsoft Press (June 28, 2006)
[N9]	OWASP CLASP	OWASP CLASP (Comprehensive, Lightweight Application Security Process)

Software Development Security Assessment

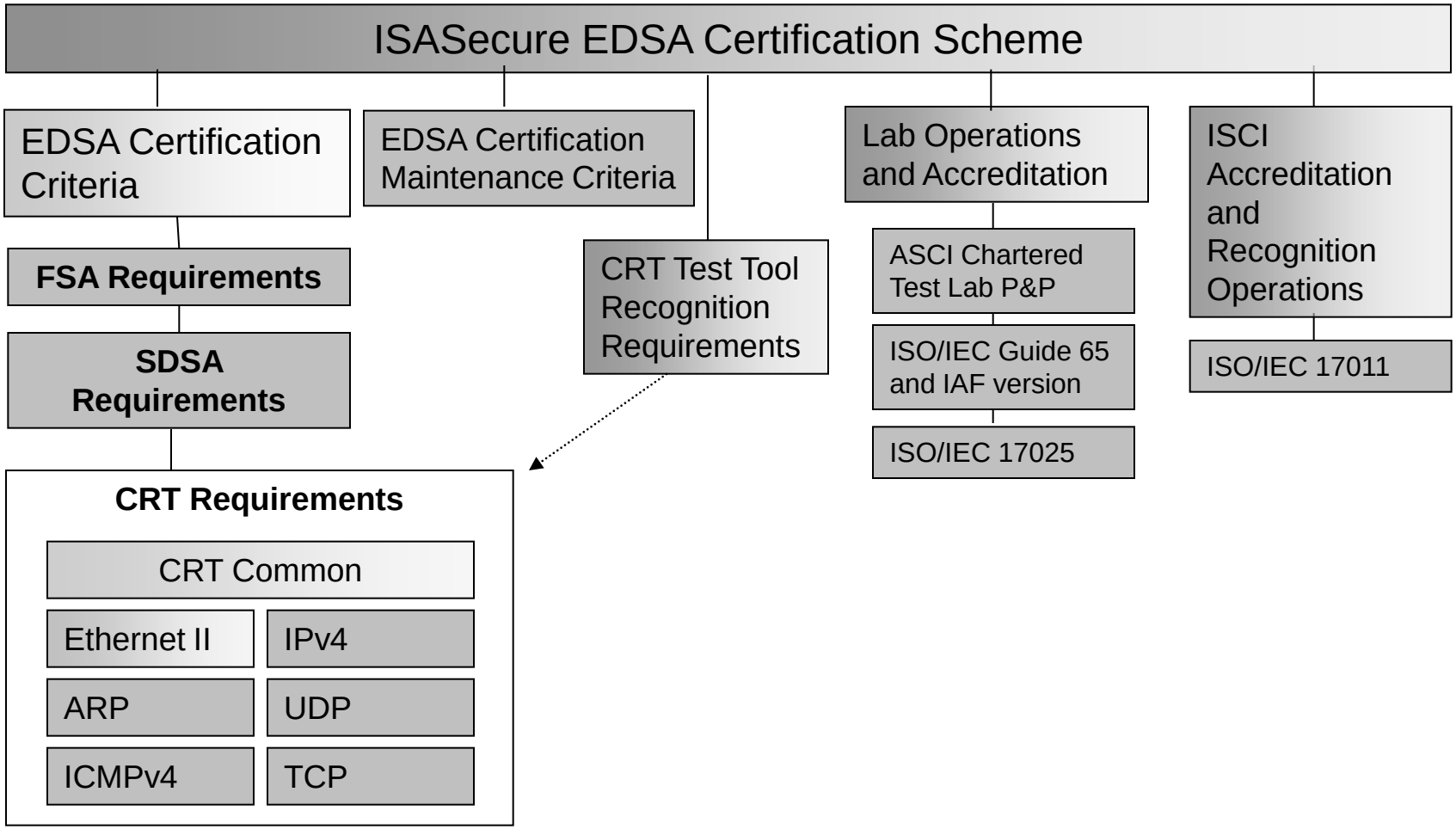
At all levels, the SDSA covers requirements for the following development lifecycle phases:

- Security Management Process
- Security Requirements Specification
- Software Architecture Design
- Security Risk Assessment and Threat Modeling
- Detailed Software Design
- Document Security Guidelines
- Software Module Implementation & Verification
- Security Integration Testing
- Security Process Verification
- Security Response Planning
- Security Validation Testing
- Security Response Execution

Embedded Device Security Assurance Certification



ISASecure EDSA Program Elements



FAQ's

1. **Who will perform ISASecure certification assessment and testing?**

   ASCI will accredit organizations (called "accredited labs") to perform ISASecure certification evaluations. ASCI will also recognize test platforms designed to perform communication robustness testing for use by these organizations and by device vendors in preparation for certification.

2. **Who will grant ISASecure certifications?**

   ASCI accredited labs will register ISASecure certified devices when the device has passed the ISASecure certification requirements. ISCI will publish a list of certified products on its web site.

3. **Describe the First ISASecure certification that will be available.**

   The ISASecure Embedded Device Security Assurance Certification is the first certification offered. The certification will include all three certification elements: software development security assessment, functional security assessment, and communication robustness testing. Communication robustness testing will include testing for the Group 1 protocols as shown in Table 1.

FAQ's

4. How were the ISASecure certification criteria developed?

The ISASecure effort has leveraged the substantial existing work in general cyber security and process control system cyber security. The SDSA and SFA criteria are aligned wherever possible with draft work products of the ISA SP-99 committee. The Software Development Security Assessment requirements are ultimately traceable to requirements in the following source documents:

Reference Standards for Software Development Security Assessment	
ISO/IEC 15408-1 through I5408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
IEC 61508 Part 3	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software Development
RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certifications
ISBN-13: 978-0735622142	The Security Development Lifecycle, M. Howard, S. Lipner, Microsoft Press (June 28, 2006)
OWASP CLASP	OWASP CLASP (Comprehensive, Lightweight Application Security Process)

FAQ's

The Functional Security Assessment requirements are ultimately traceable to requirements in the following source documents:

Reference Standards for Functional Security Assessment	
ISA-99.01.03D2-20090527	Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels ISA-99.01.03
NERC Standards CIP-001-1 through CIP-001-9	North American Electric Reliability Council Cyber Security Standards
NIST 800-53	Recommended Security Controls for Federal Information Systems
ISO/IEC 15408-1 through I5408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
	Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers

FAQ's

5. **Will a vendor that has already obtained a certification for a device be allowed to submit those results for ISASecure certifications?**

   Yes. ISCI has identified specific certifications from which pre-existing artifacts may be offered as evidence for meeting specific certification requirements in the ISASecure specification.

   1. An organization who has already received an IEC61508 certification for a device may submit artifacts on their software development practices to satisfy specific requirements in the ISASecure Software Development Security Assurance (SDSA) specification section of the EDSA certification.

   2. Results from a supplier's initial SDSA will be included by reference in subsequent device certifications where the supplier organization has already successfully met the SDSA requirements; **the full SDSA assessment will not have to be repeated for each device.**

Who to Contact

http://www.isasecure.org

Andre Ristaino

Managing Director, ASCI

Direct Phone: 919-990-9222

Fax: 919-549-8288

Email: aristaino@isa.org

ISASecure Embedded Controller Certification program specifications are available for review and download at www.isasecure.org