

Setting the Standard for Automation™



Requesting and Achieving Software Assurance in Safety and Security Critical Applications

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

ISA Safety & Security Division
Symposium
14 April 2011

John A. Cusimano, CFSE, CISSP

- Director of Security Solutions for exida
- 20+ years experience in industrial automation
- Employment History:
 - Eastman Kodak
 - Moore Products
 - Siemens
- Certifications:
 - CFSE, Certified Functional Safety Expert
 - CISSP, Certified Information Systems Security Professional
- Industry Associations:
 - ISA S99 Committee (WG4, WG5, WG7, WG8)
 - ISA S84 Committee (WG9)
 - ISA Security Compliance Institute
 - ICSJWG Workforce Development & Vendor Subgroups



Stuxnet Response

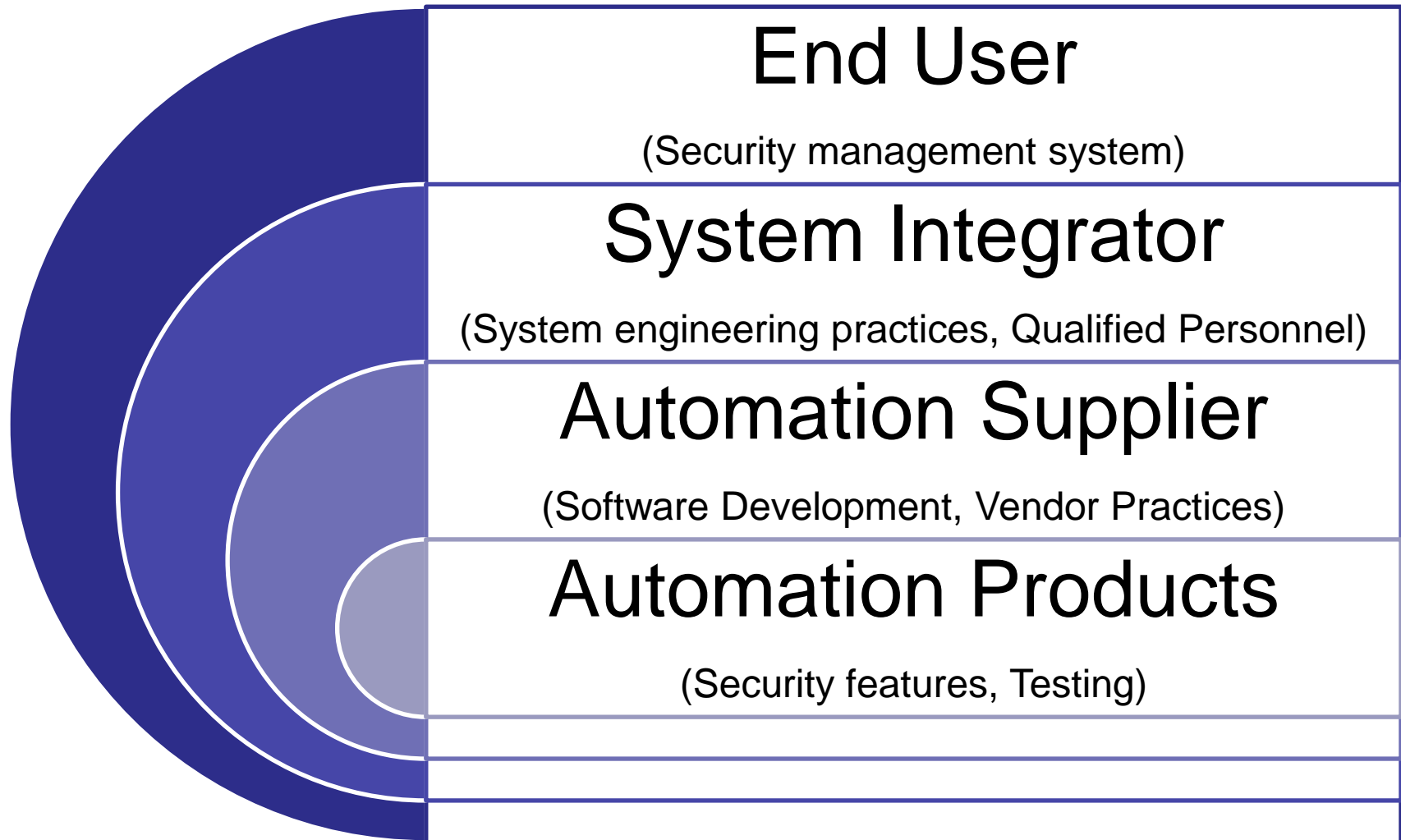
“Addressing Stuxnet goes beyond using quality security controls. The industry needs to demand higher quality software that is free from defects. Companies who develop products and write code need to continue to mature their development processes to become more secure.”

Mark Weatherford

Vice President and Chief Security Officer

NERC

Control System Security Layers of Responsibility



Software Security Assurance (SSA)



“Software Security Assurance (SSA) is the process of ensuring that software is designed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects.”

Life-critical / Safety-critical Applications

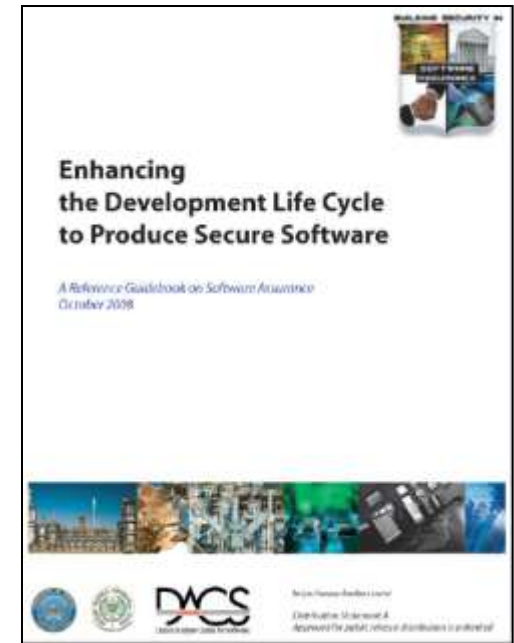
- Aviation
- Medical
- Nuclear Engineering
- Recreation
- Transportation
- Automotive
- Industrial Automation

Risks to Software Security Assurance

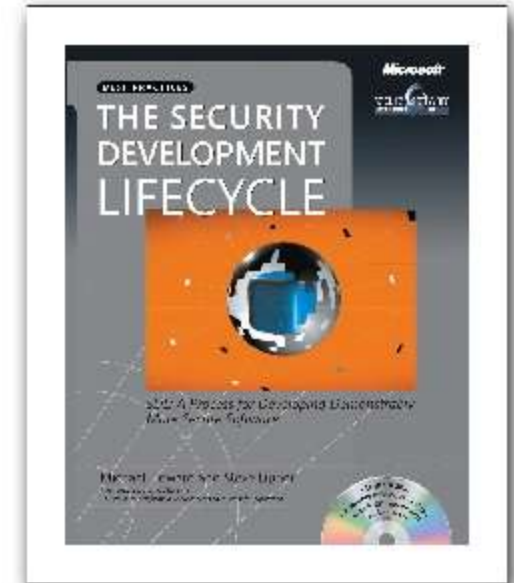
- Size and complexity of software
- Outsourcing of software development and reliance on unvetted software supply chains;
- Attack sophistication that eases exploitation of software weaknesses and vulnerabilities;
- Reuse and interfacing of legacy software with newer applications in increasingly complex, disparate networked environments resulting in unintended consequences and the increase of vulnerable software targets.

Software Security Assurance Objectives

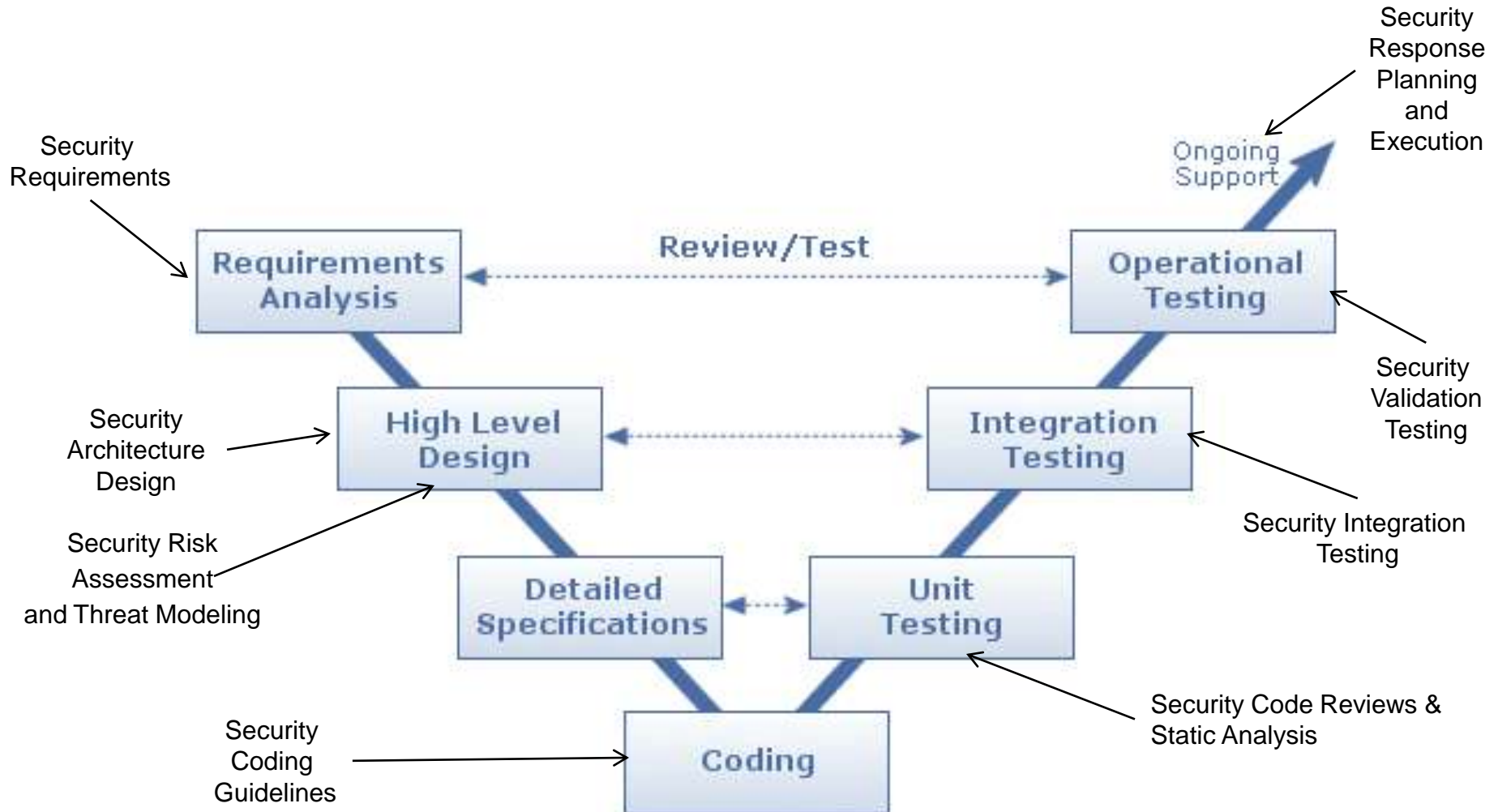
- **Dependability (Correct and Predictable Execution)**
 - Justifiable confidence can be attained that software, when executed, functions only as intended;
- **Trustworthiness**
 - No exploitable vulnerabilities or malicious logic exist in the software, either intentionally or unintentionally inserted;
- **Resilience (and Survivability)**
 - If compromised, damage to the software will be minimized, and it will recover quickly to an acceptable level of operating capacity;
- **Conformance**
 - A planned and systematic set of multi-disciplinary activities will be undertaken to ensure software processes and products conform to requirements and applicable standards and procedures.



- Reduce the number of security vulnerabilities
- Reduce the severity of remaining vulnerabilities



Incorporating Security into the Software Development Lifecycle





ISA Security Compliance Institute (ISCI)

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



ANSI/ACCLASS Accredited Conformance Scheme



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

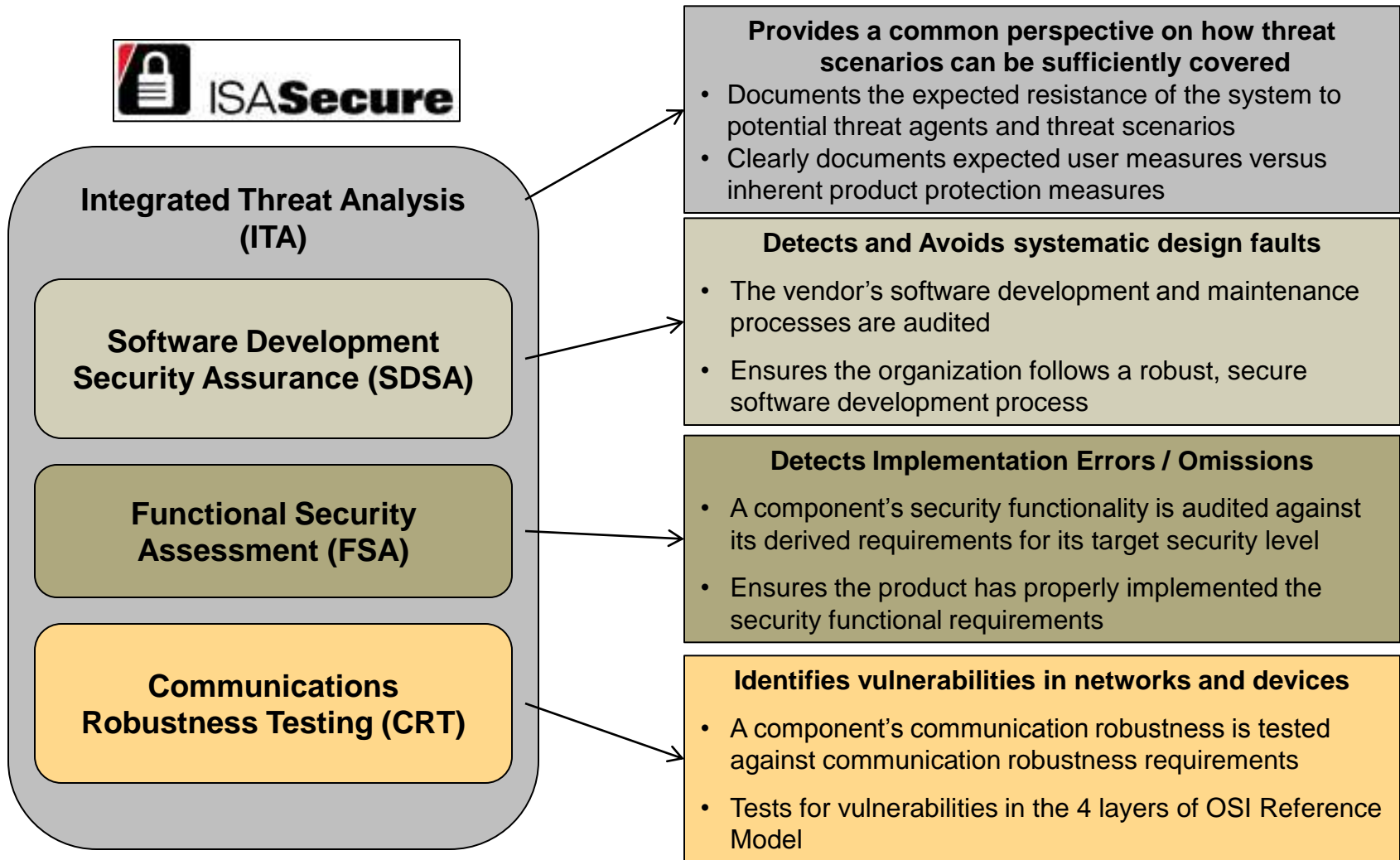
Go to www.ansi.org/isasecure for details.

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.

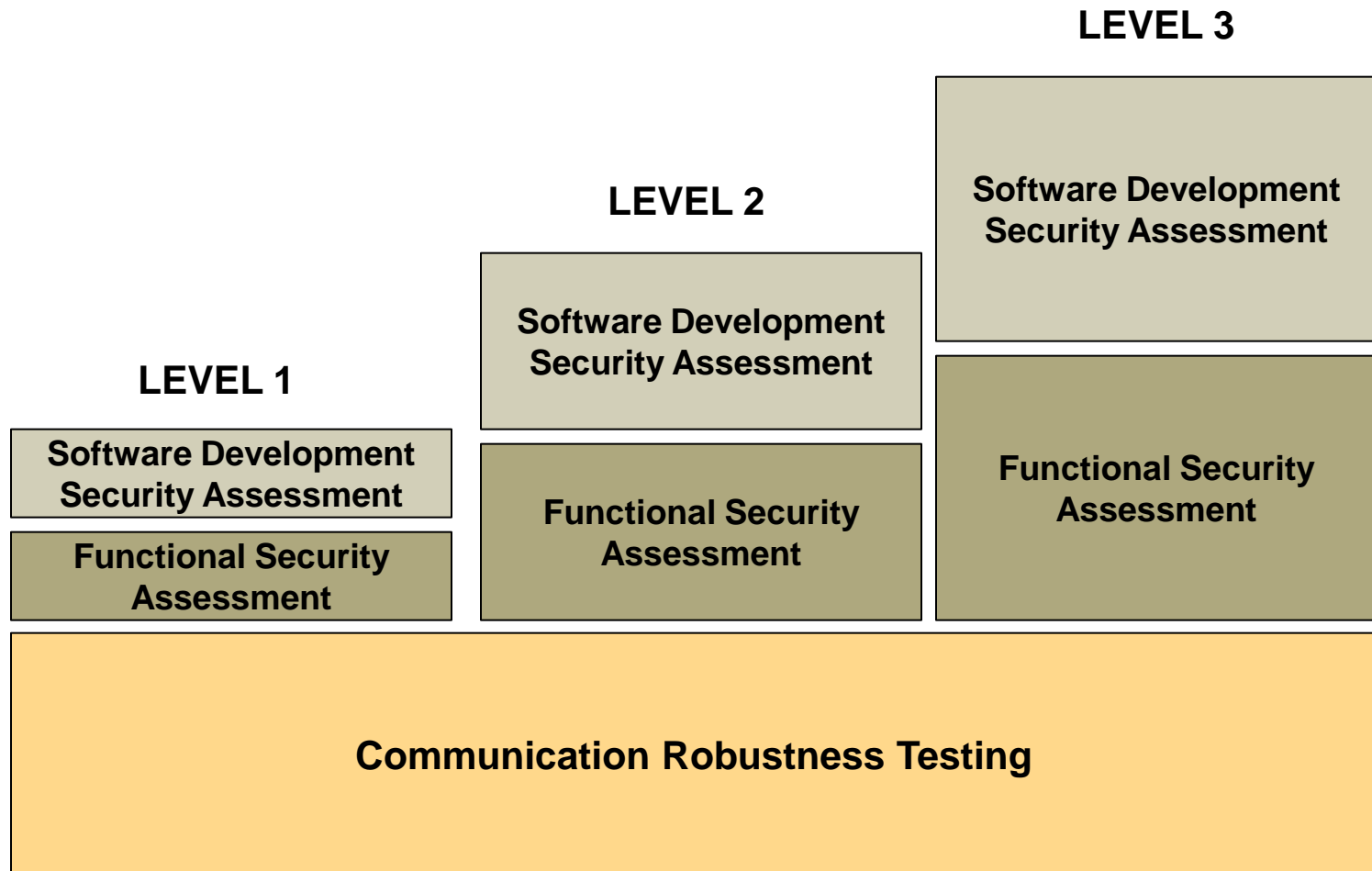


- Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process
- Examples:
 - Programmable Logic Controller (PLC)
 - Distributed Control System (DCS) controller
 - Safety Logic Solver
 - Programmable Automation Controller (PAC)
 - Intelligent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

ISASecure Embedded Device Certification



ISASecure Levels



SDSA Reference Standards



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)

ISASecure Software Development Security Assessment Phases



Security Management Process	This phase specifies a process for planning and managing security development activities to ensure that security is designed into a product. For example, this phase incorporates requirements that the development team have a security management plan and that the developers assigned to the project are competent and have been provided basic training in good security engineering practices and processes. Also includes requirements that the project team creates and follows a configuration management plan.
Security Requirements Specification	Most vulnerabilities and weaknesses in software intensive information systems can be traced to inadequate or incomplete requirements. This phase requires that the project team document customer driven security requirements, security features and the potential threats that drive the need for these features.
Software Architecture Design	Software architecture facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects. This phase requires the project team develop a top-level software design and ensures that security is included in the design.
Security Risk Assessment and Threat Modeling	This phase requires the project team determine which components can affect security and plan which components will require security code reviews and security testing. Also requires that a threat model be created and documented for the product.
Detailed Software Design	This phase requires the project team design the software down to the module level following security design best practices.
Document Security Guidelines	This phase requires the project team create guidelines that users of the product must follow to ensure security requirements are met.
Software Module Implementation & Verification	This phase requires the project team implement design by writing code following security coding guidelines. It ensures that software modules are implemented correctly by conducting security code reviews, static analysis and module testing.
Security Integration Testing	This phase requires that the project team perform security specific tests such as fuzz testing and penetration testing.
Security Process Verification	This phase requires an independent assessment that all required software development processes have been followed
Security Response Planning	This phase requires the project team establish a process to be able to quickly respond to security issues found in the field if and when they happen.
Security Validation Testing	This phase requires that the project team confirm that all security requirements have been met preferably by test or by analysis.
Security Response Execution	This phase requires the project team respond to security problems in the field by taking action to both preventative and corrective action.

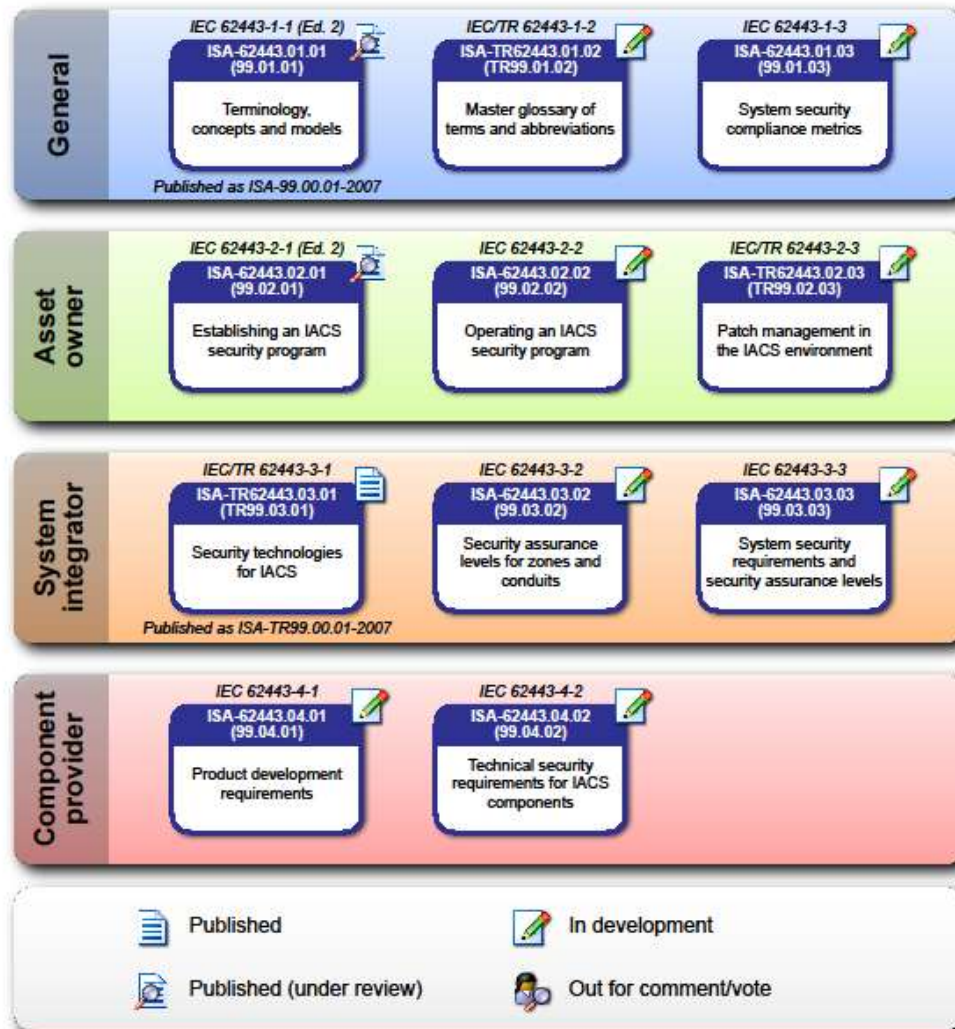
ISA 99 Work Products



Category	Product ID	Standard Title	Status
Common	IEC/TS 62443-1-1 ISA-99.01.01	Terminology, concepts and models	Published
	IEC/TR 62443-1-2 ISA-TR99.01.02	Master glossary of terms and abbreviations	Published (Under Review)
	IEC 62443-1-3 ISA-99.01.03	System security compliance metrics	In Development
<i>Published as ISA-99.00.01-2007</i>			
Security Program	IEC 62443-2-1 ISA-99.02.01	Establishing an IACS security program	Published
	IEC 62443-2-2 ISA-99.02.02	Operating an IACS security program	In Development
	IEC/TR 62443-2-3 ISA-TR99.02.03	Patch management in the IACS environment	Published (Under Review)
Technical - System	IEC/TR 62443-3-1 ISA-TR99.03.01	Security technologies for IACS	Published (Under Review)
	IEC 62443-3-2 ISA-99.03.02	Security assurance levels for zones and conduits	In Development
	IEC 62443-3-3 ISA-99.03.03	System security requirements and security assurance levels	In Development
	IEC 62443-3-4 ISA-99.03.04	Product development requirements	In Development
<i>Published as ISA-TR99.00.01-2007</i>			
Technical - Component	IEC 62443-4-1 ISA-99.04.01	Embedded devices	In Development
	IEC 62443-4-2 ISA-99.04.02	Host devices	In Development
	IEC 62443-4-3 ISA-99.04.03	Network devices	In Development
	IEC 62443-4-4 ISA-99.04.04	Applications, data and functions	In Development

Published Published (Under Review) In Development Comment/Vote

Proposed Organization (2011)



Summary



- The industry needs to demand software security assurance
- Supplier can achieve this by incorporating security practices into their software development life cycle
- ISASecure provides a mechanism to recognize products that have been developed following secure process