Comparing Safety and Security Standards

Swedsoft Seminar

2016-04-05

Nicolás Martín-Vivaldi

addalot
QUALITY IMPROVEMENT

Addalot - 25 year experience

- History

Q-Labs DNV addalot

- Effect driven process improvement
  - 
- Services:
  - Process Improvement
  - Software Quality
  - Software Safety
  - Supplier Management
  - Open Source Software
- References:

Telecom	Ericsson, Nokia, Sony, ST-Ericsson, Telenor, Telia,
Automotive	AtlasCopco, Autoliv, BMW, BorgWarner, Bosch, Consat, GM, Mecel, Saab, Stoneridge, Volvo
Defense	BAE Systems, EADS, FMV, Kockums, Kongsberg, Saab, Terma, Thales
Finance & IT	Emric, Ikano, Ikea, Lawson, Nordstedt, Palette, Point, Qlik, Readsoft, SEB, Tieto, Visma
Offshore	ABB, Berg Propulsion, DNV, Dolphin, FMC, Fugro, Saipem, Statoil, Wilhelmsen

addalot QUALITY IMPROVEMENT

Background

- Definitions
  - **Safety** is the absence of unacceptable risk [Malfunction]
  - **Security** is degree of resistance to harm [Intentional failures]
- Used to be separated but are becoming more related
  - Telematics
  - Internet of Things

- Security risk ➔ Safety problem

Hackers Remotely Kill a Jeep on the Highway—With Me in It

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

addalot QUALITY IMPROVEMENT

Standard driven

- Both Safety & Security work are standard driven
- A large and quite confusing area with many ”standards”
- **What are the differences and how to combine?**

Safety Standards

- Many different standards, the majority from IEC 61508
  - Automotive ISO 26262
  - Medical device IEC 62304
  - Nuclear IEC 61513
  - Aerospace RTCA DO-178C
  - Machine IEC 620061
  - Process IEC 61511
  - Railroad EN 5012X

- In Brief
  - 5 summarizing principles for **Software** (*)
    1. Software safety requirements shall address the software contribution to system hazards
    2. The software safety requirements shall be maintained throughout decomposition
    3. Software safety requirements shall be satisfied
    4. Hazardous behavior of the software shall be identified and mitigated
    5. The confidence managed in relation system risk
  - Some requirements on organizational level:
    - Safety policy and culture, Safety lifecycle, QMS, Safety responsible, Training and qualification
  - High focus on the specific delivery

(*) Tim Kelly Fundamental Principles of Software Safety Assurance

addalot QUALITY IMPROVEMENT

Security Standards

Many different standards:

- ISO 27000 (ISO 27001 / ISO 27002 / ISO 27005)
- IEC 62443
- SSAE 16
- AICPA Trust Services
- Cybertrust
- CMM-I extensions
- CERT® Resilience Management Model
- Common Criteria
- Microsoft SDL

Summary of Security Standards

- Strong in Administrative systems / Data centers
- Mainly organizational aspects
  - Policy
  - Strategy
  - Roles & Responsibilities
  - Management awareness
  - Formalized handovers
- High focus on operations
  - Facilities
  - Personnel (screening, education)
  - Data management
  - Risks
- Little guidance on actual development (except SDL and IEC-62443)
- Most standards lack levels (Swedish Armed Forces have security classes)
- Models exist for checking different security threats: eg STRIDE
  - Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege

Conclusions

- Security and Safety standards have in general little overlap

➔ Meeting one will not cover the other…

- Exchange
  - Security can learn from Safety SILs and related techniques
  - Safety can learn from Security on organisational level

- Ongoing research / debate how to combine safety and security
  - Extend safety thinking to include security in hazard and risk activities
  - Merging of models or keep apart…

HEAVENS
HEALing Vulnerabilities to ENhance Software Security and Safety

FIA

PiiA
Strategic Innovation Programme
Process Industrial IT and Automation

addalot
QUALITY IMPROVEMENT

“Excellent firms don't believe in excellence - only in constant improvement and change.”

In Search of Excellence - Tom Peters

nicolas.martin-vivaldi@addalot.se
+46 706 800 521

addalot
QUALITY IMPROVEMENT

ISO 27000

- 27001:
  - ISO/IEC 27001:2005 formally specifies a **management system** that is intended to bring information security under explicit management control. Being a formal specification means that it **mandates** specific requirements.

- 27002:
  - ISO/IEC **27002**:2005 has developed from BS7799, published in the mid-1990s. The British Standard was adopted by ISO/IEC as ISO/IEC 17799:2000, revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27000-series standards.
  - ISO/IEC 27002 provides **best practice recommendations** on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).

- 27005:
  - ISO/IEC 27005:2011provides guidelines for information security risk management and 'supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach

ISO 27001

- 4. Contextual Requirements
  - 4.3. Figure out what your ISMS should apply to and clarify its scope.
- 5. Leadership Requirements
  - 5.1. Provide leadership
  - 5.2. Security policy.
- 6. Planning Requirements
  - 6.1. Manage risks and address opportunities.
  - 6.2. Set security objectives and develop plans to achieve them.
- 7. Support Requirements
  - 7.1. Resources
  - 7.2. Competence
  - 7.3. Responsibilities.
  - 7.4. Communication needs
  - 7.5. Managing information
- 8. Operational Requirements
  - 8.1. Plan and control your processes.
  - 8.2. Security risk assessments.
  - 8.3. Security risk treatment plan.
- 9. Evaluation Requirements
  - 9.1. Monitor, measure, analyze, and evaluate
  - 9.2. Set up an internal audit program and use it to evaluate your ISMS.
  - 9.3. Review performance of your ISMS at planned intervals.
- 10. Improvement Requirements
  - 10.1. Identify nonconformities and take corrective actions.
  - 10.2. Enhance performance of your ISMS.

Generic Process management compliance - could replace Security with any other ”ity”.
Flexible when it comes to scope – has to be defined by section 4
Little guidance on specific techniques, e.g. ”Figure out how …”

addalot QUALITY IMPROVEMENT

ISO 27002 (2005)

- Structure
- Security Policy
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical And Environmental Security
- Operations security
- Communications Security
- **Information Systems Acquisition, Development, Maintenance**
- Supplier Relationships
- Information Security Incident management
- Information Security Aspects of Business Continuity
- Compliance

Structure has changes somewhat to 2013

addalot QUALITY IMPROVEMENT

27002: System acquisition, development and maintenance

- 14.1 Security **requirements** of information systems
- 14.2 Security in **development and support** processes
  - 14.2.1 Secure development policy
  - 14.2.2 System change control procedures
  - 14.2.3 Technical review of applications after operating platform changes
  - 14.2.4 Restrictions on changes to software packages
  - 14.2.5 Secure system engineering principles
    - *"Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts."*
  - 14.2.6 Secure development environment
  - 14.2.7 Outsourced development
  - 14.2.8 System security testing
  - 14.2.9 System acceptance testing
- 14.3 **Test data**

Still no specific guidelines

ISO 27005

- Information security risk management
- The standard doesn't specify, recommend or even name any specific risk management method. It does however imply a continual process consisting of a structured sequence of activities, some of which are iterative:
  - Establish the risk management context
  - Quantitatively or qualitatively assess
  - Treat the risks appropriately, using those ‘levels of risk’ to prioritize them;
  - Keep stakeholders informed throughout the process; and
  - Monitor and review risks,

IEC-62443 (formerly ISA-99)

- A series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS)
- It introduces the concepts of “zones” and “conduits” as a way to segment and isolate the various sub-systems in a control system.
  - A zone is defined as a grouping of assets that share common security requirements and has a security level capability.
  - Any communications between zones must be via a defined conduit.
- All ISA-62443 standards and technical reports are organized into four categories:
  - **General,** concepts, models, terminology, security metrics and security life cycles for IACS.
  - **Policies and Procedures,** creating and maintaining an effective IACS security program (Owner)
  - **System,** system design guidance and requirements for the secure integration of control systems
  - **Component,** specific product development of control system products
- 62443-4-1Product development requirements
  - Defines the development process that should be used to create products that make up the industrial automation and control system.
  - Covering requirements ➔ design ➔ implementation ➔ test & verification

addalot QUALITY IMPROVEMENT

SSAE 16

SSAE16 Completed Audit

- SSAE 16, **Statement on Standards for Attestation Engagements 16**, is a regulation created by the **Auditing Standards Board** (ASB) of the **American Institute of Certified Public Accountants (AICPA)** for redefining and updating how service companies report on compliance controls.
- SSAE 16 is the reporting standard for all service auditors' reports from June 15th, 2011, and beyond. SSAE 16 was preceded by **SAS 70**, which had been in effect since April 1992.

"Accountants know that they cannot test security which is probably why the TSPC are so vague. Security professionals have the right security standards, but they do not understand what assurance is, or how it is achieved." J. Long

addalot QUALITY IMPROVEMENT

SSAE 16, SOC's (Service Organization Controls)

- SSAE 16 SOC 1 report suffers from the same fundamental problem that the SAS 70 had before it: the controls are self-defined.
- SOC 2(internal) and SOC 3 (external) reports are aligned with the **AICPA Trust Services Principles and Criteria (TSPC).** These principles are focused on five areas:
  - **Security**: Unauthorized access to systems (physical and logical) is prevented through controls.
  - **Confidentiality**: Sensitive information labeled as confidential is protected with adequate controls (customer data and systems would likely fall into this category).
  - **Privacy**: Personal information is collected and managed in accordance with the AICPA Generally Accepted Privacy Principles.
  - **Availability**: Systems are designed with uptime and availability in mind, and continuity of system operations is maintained.
  - **Processing Integrity**: All system processing activities are accurate, authorized and complete.
- Types
  - Type 1: Snapshot
  - Type 2: Period, 6 or 12 months
- ISAE 3402 is the international version of the US SAEE16 (with some modifications)

addalot QUALITY IMPROVEMENT

AICPA Trust Services Principles and Criteria (TSPC)

CC1.2 **Responsibility and accountability** for designing, developing, implementing, operating, monitoring, maintaining, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated.

CC1.3 Personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system affecting [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality] **have the qualifications and resources** to fulfill their responsibilities.

CC1.4 The entity has established **employee conduct standards,** implemented employee candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality].

CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls

CC3.1 The entity (1) **identifies potential threats** that would impair system [*insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality*] commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).

CC3.2 The entity **designs,** develops, and implements controls, including policies and procedures, to **implement its risk mitigation strategy.**

CC3.3 The entity (1) **identifies and assesses changes** (for example, environmental, regulatory, and technological changes) that could significantly impact the system of internal control for [*insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality*] and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.

CC4.0 Common Criteria Related to Monitoring of Controls

CC4.1 The design and operating effectiveness of controls are **periodically evaluated** against [*insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality*] commitments and requirements.

addalot QUALITY IMPROVEMENT

Cybertrust by Verizon

Five critical control groups:

- **Policy:** should include areas as access control, antivirus, data handling, third-party communications, e-mail and Internet usage, and help desk policies.
- **Human:** Human resources that can affect the organization's overall security posture, such as security policies, management procedures, training, hiring, corrective actions and general information awareness.
- **Physical:** includes the power source, water supply, doors, alarms, ventilation. In addition, organization's backup, failover, and disaster recovery systems and locations.
- **Device:** Includes physical computers, operating systems deployed as Internet servers, database servers, firewalls, routers, switches and desktop computers.
- **Network:** Addresses the network interfaces that enable computers and other devices to provide Internet-based users with desired services. Examples of such devices include routers, firewalls, switches, hubs, security domains, wiring/cabling, modems, and DNS.

Little about development processes
Seems to be focused on ”operations”

Security by Design with CMMI

Extended CMMI with new areas:

- Process Management
  - SG1: Establish an Organizational Capability to Develop Secure Products
- Project Management
  - SG1: Prepare and Manage Project Activities for Security
  - SG2: Manage Product Security Risk
- Engineering: Security Requirements and Technical Solution
  - SG1: Develop Customer Security Requirements and Secure Architecture and Design
  - SG2: Implement the Secure Design
- Engineering: Security Verification and Validation
  - SG1: Perform Security Verification
  - SG2: Perform Security Validation

CERT® Resilience Management Model

- Engineering
  - Asset Definition and Management
  - Controls Management
  - Resilience Requirements Development
  - Resilience Requirements Management
  - Resilient Technical Solution Engineering
  - Service Continuity
- Enterprise Management
- Operations
- Process Management

TS ENG: Goals and Practices

- SG1 Establish Guidelines for Resilient TS Development
  - SP1 Identify General Guidelines
  - SP2 Identify Requirements Guidelines
  - SP3 Identify Arch and Design Guidelines
    - **Guidelines for designing resilience into software and systems are identified.**
  - SP4 Identify Implementation Guidelines
  - SP5 Identify Assembly and Integration Guidelines
- SG2 Develop Resilient TS Dev. Plans
- SG3 Execute the Dev. Plan

Not very informative

addalot QUALITY IMPROVEMENT

Common Critera (related ISO/IEC 15408)

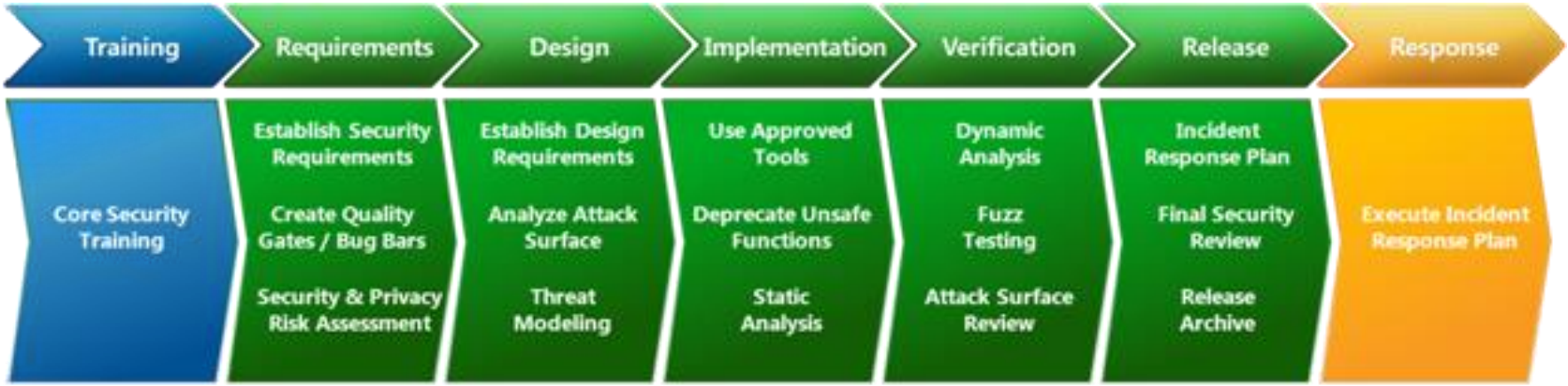
- Common Criteria is a framework in which computer system users can *specify* their security *functional* and *assurance* requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then *implement* and/or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims.
- Target Of Evaluation (TOE) – the product or system that is evaluated through
  - **Protection Profile (PP)** – a document, typically created by a user or user community, which identifies security requirements for a class of security devices relevant to that user
  - **Security Target (ST)** – the document that identifies the security properties of the target of evaluation
  - **Security Functional Requirements (SFRs)** – specify individual security **functions** which may be provided by a product. The Common Criteria presents a standard catalogue of such functions.

Focus on the security requirements
and the evaluation of the same!
Little focus on the implementation

addalot QUALITY IMPROVEMENT

Microsoft SDL

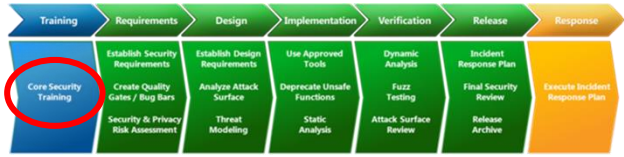
- SDL = Security Development Lifecycle
- Concrete development practices based on Microsoft's own development



- Can be integrated with other processes
- Each practice is supported by training and guidelines
- Concrete and "understandable"

addalot QUALITY IMPROVEMENT

Software security training



- **Secure design**
  - Attack surface reduction
  - Defense in depth
  - Principle of least privilege
  - Secure defaults
- **Threat modeling**
  - Overview of threat modeling
  - Design implications of a threat model
  - Coding constraints based on a threat model
- **Secure coding**
  - Buffer overruns (for applications using C and C++)
  - Integer arithmetic errors (for applications using C and C++)
  - Cross-site scripting (for managed code and Web applications)
  - SQL injection (for managed code and Web applications)
  - Weak cryptography
- **Security testing**
  - Differences between security testing and functional testing
  - Risk assessment
  - Security testing methods
- **Privacy**
  - Types of privacy-sensitive data
  - Privacy design best practices
  - Risk assessment
  - Privacy development best practices
  - Privacy testing best practices

addalot QUALITY IMPROVEMENT

SDL Practice 12: Fuzz Testing

- Fuzz testing is a specialized form of dynamic analysis used to induce program failure by deliberately introducing malformed or random data to an application.

SDL Practice #12: Perform Fuzz Testing

Inducing program failure by deliberately introducing malformed or random data to an application helps reveal potential security issues prior to release while requiring modest resource investment.

When should this practice be implemented?

Traditional Software development: Verification Phase
Agile development: Bucket Verification

⊖ Resources specific to this practice

REFERENCE

- Fuzz Testing: Create a Test Interface Provider for Visual Studio Team System
- Regular Expression Denial of Service Attacks and Defenses
- Automated Penetration Testing with White-Box Fuzzing

DOWNLOADS

- Basics of Secure Design, Development, and Test
- SDL Developer Starter Kit
- MiniFuzz File Fuzzer
- SDL Regex Fuzzer

VIDEOS

- File Fuzzing for Fun and Profit (Level 300)
- MiniFuzz File Fuzzer
- SDL Regex Fuzzer

TRAINING

- Basics of Secure Design, Development and Test
- SDL Quick Security References
- SDL Developer Starter Kit

addalot QUALITY IMPROVEMENT