
Paul R. Croll

Computer Sciences Corporation
ccroll@csc.com

Industry Co-Chair, NDIA Systems Assurance Committee

Chair, DHS Software Assurance Forum Working Group on Processes and Practices

Past Convener, ISO/IEC JTC1/SC7 WG9, System and Software Assurance
Outline

- System Assurance Defined
- The System Assurance Problem Space
- Software As A Root Cause Problem
- The Systems Engineering Challenge
- The CMMI® and Assurance
- Bang-For-The-Buck CMMI-DEV® Process Areas
- Guidance For Systems Assurance
- Standardization In Support Of Systems Assurance
System assurance is the level of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system.
System Assurance Problem Space

- Large-scale systems and systems of systems represent a complex supply chain integrating
  - Proprietary and open-source software
  - Legacy systems
  - Hardware
  - Firmware

- These systems are sourced from multiple suppliers who employ people from around the world

- Most systems we encounter today contain software elements and most depend upon software for a good portion of their functionality

- Technologies to build reliable and secure software are inadequate
  - Our ability to develop software has not kept pace with hardware advances
  - Cannot construct complex software-intensive systems for which we can anticipate performance

- Assurance is a full life cycle systems-level problem
Software As A Root Cause Problem

- System risk has dramatically increased due to the simultaneous growth in software vulnerabilities and in threat opportunities
- Risk management processes inadequately address these threats and risks
- Threats presented by suppliers of software products and services are not adequately identified and analyzed
- Development and acquisition processes inadequately address software security
- There is a fundamental lack of both the scientific understanding of software risks and the capabilities to effectively diagnose and mitigate in a timely manner

More Succinctly . . .

- There is a failure to assure correct, predictable, safe, secure execution of complex software in distributed environments
- Inadequate attention is given to the total life cycle issues, including impacts on life cycle cost and risk associated with the use of commercial or reused products and components

Systems Engineering Challenge

Integrating a heterogeneous set of globally engineered and supplied proprietary, open-source, and other software; hardware; and firmware; as well as legacy systems; to create well-engineered integrated, interoperable, and extendable systems whose security, safety, and other risks are acceptable or at least tolerable.
1. Understand Your Business Requirements for Assurance

2. Look to the CMMI® for Assurance-Related Process Capability Expectations

3. Look to Standards for Assurance Process Detail

4. Build or Refine and Execute Your Assurance Processes

5. Measure Your Results - Modify Processes as Necessary
Inconsistent treatment of safety and security concerns

Insufficient assurance detail in required and expected components
  - Specific goals
  - Specific practices

Insufficient traceability to assurance source standards
<table>
<thead>
<tr>
<th>Name</th>
<th>Abbr</th>
<th>Safety</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements Management</td>
<td>REQM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Project Planning</td>
<td>PP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Project Monitoring and Control</td>
<td>PMC</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Supplier Agreement Management</td>
<td>SAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measurement and Analysis</td>
<td>MA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process and Product Quality Assurance</td>
<td>PPQA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td>CM</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Requirements Development</td>
<td>RD</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Technical Solution</td>
<td>TS</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Product Integration</td>
<td>PI</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>VER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation</td>
<td>VAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational Process Focus</td>
<td>OPF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational Process Definition +IPPD</td>
<td>OPD +IPPD</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Organizational Training</td>
<td>OT</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Integrated Project Management +IPPD</td>
<td>IPM +IPPD</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Risk Management</td>
<td>RSKM</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Decision Analysis and Resolution</td>
<td>DAR</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Organizational Process Performance</td>
<td>OPP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantitative Project Management</td>
<td>QPM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational Innovation and Deployment</td>
<td>OID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Causal Analysis and Resolution</td>
<td>CAR</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Safety and Security Extensions for Integrated Capability Maturity Models – Take 1

1. Ensure Safety and Security Competency
2. Establish Qualified Work Environment
3. Ensure Integrity of Safety and Security Information
4. Monitor Operations and Report Incidents
5. Ensure Business Continuity
6. Identify Safety and Security Risks
7. Analyze and Prioritize Risks
8. Determine, Implement, and Monitor Risk Mitigation Plan
10. Develop and Deploy Safe and Secure Products and Services
11. Objectively Evaluate Products
12. Establish Safety and Security Assurance Arguments
13. Establish Independent Safety and Security Reporting
14. Establish a Safety and Security Plan
15. Select and Manage Suppliers, Products, and Services
16. Monitor and Control Activities and Products

## Source Standards

### Safety

### Security

Extensions for Integrated Capability Maturity Models - Take 2

- Workshop on Assurance with CMMI®, August 7, 2007
  - Relationships between Models and Standards
  - Industry experiences in extending models for assurance
    - Motorola's Secure Software Development Model
    - Lockheed Martin's Software Safety and Security Certification Best Practices
    - Booz Allen Hamilton's experience with multiple models
  - Community of interest feedback on security extensions to the CMMI®

- Security Model Harmonization Working Group
  - Harmonization of key security capability maturity models including but not limited to the SSE-CMM and the Motorola Secure Software Development Model (MSSDM)
  - Prototyping Assurance as a Focus Area
  - Assurance beginning with Security in Phase I, adding Safety and Dependability in Phase II
For-The-Buck CMMI®-DEV Project Management Process Areas

- **RSKM**
  - Identify, Evaluate, Categorize, and Prioritize Assurance Risks
  - Develop assurance risk mitigation strategies

- **PP**
  - Determine a technical approach for the project that supports the assurance requirements
  - Determine the level of security required for tasks, work products, hardware, software, personnel, and work environment

- **PMC**
  - Monitor significant changes in risk status
  - Monitor the security environment

- **SAM**
  - Evaluate COTS products for compliance with assurance requirements
  - Evaluate the trustworthiness of the supplier
- Establish and maintain training capability to address assurance-related training needs
- Provide training necessary to ensure the competency of individuals required to perform assurance-related roles effectively
Engineering Process Areas

- **RD**
  - Identify customer expectations for assurance
  - Define product assurance attributes

- **TS**
  - Identify and analyze alternative solutions based on proposed product architectures that address critical product qualities
  - Ensure that the detailed design adheres to applicable assurance standards and criteria

- **VER**
  - Select verification methods based on their ability to demonstrate that the work product properly reflects the specified assurance requirements
  - Establish and maintain the environment needed to support validation, including test tools and simulations

- **VAL**
  - Select validation methods based on their ability to demonstrate that customer expectations for assurance are satisfied
  - Establish and maintain the environment needed to support validation, including test tools and simulations
**Support Process Areas**

- **CM**
  - Create a baseline that can be changed only through formal change control procedures
  - Perform reviews to ensure that changes have not compromised the safety, security, or dependability

- **PPQA**
  - Objectively evaluate the work products against the applicable assurance process descriptions, standards, and procedures
Systems Assurance – Delivering Mission Success in the Face of Developing Threats

- An NDIA guidebook intended to supplement the knowledge of systems (and software) engineers who have responsibility for systems for which there are assurance concerns
Agreement Processes
- Acquisition
- Supply

Project Processes
- Project Planning
- Project Assessment
- Project Control
- Decision-making
- Risk Management
- Configuration Management
- Information Management

Assurance Case Process

Technical Processes
- Stakeholder Requirements Definition
- Requirements Analysis
- Architectural Design
- Implementation
- Integration
- Verification
- Transition
- Validation
- Operation
- Maintenance
- Disposal

Enterprise Processes
- Enterprise Environment Management
- Investment Management

- System Life Cycle Process Management
- Resource Management [including human resource training]
- Quality Management
Performance of Standards In The Guidebook

ISO/IEC 15288:2002(E)

IEEE 1220-2005

* Fabrication, Assembly, Integration, & Test

Integrated Defense Acquisition, Technology, & Logistics Life Cycle Framework

Defense Acquisition System

NIST Information Security and the System Development Life Cycle

CSC
State of the Art Report on Software Security Assurance

An IATAC/DACS report identifying and describing the current state of the art in software security assurance, including trends in:

- Techniques for the production of secure software
- Technologies that exist or are emerging to address the software security challenge
- Current activities and organizations in government, industry, and academia, in the U.S. and abroad, that are devoted to systematic improvement of software security
- Research trends worldwide that might improve the state of the art for software security
Secure Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software

- A DHS guidebook intended as a framework to identify workforce needs for competencies and leverage standards and best practices to guide software-related curriculum development
Guidance For Systems Assurance - 4


- An DHS report providing a compendium of methodologies, life cycle process models, sound practices, and supporting technologies that would, if adhered to, increase software security
Software Assurance in Acquisition: Mitigating Risks to the Enterprise

A DHS report intended to provide guidance on enhancing supply chain management through improved risk mitigation and contracting for secure software
Standardization In Support Of Assurance in Programming Languages

- ISO/IEC SC22/OWG: Vulnerabilities (OWGV)
  - Project 22.24772: Guidance for Avoiding Vulnerabilities through Language Selection and Use
    - Technical Report
    - Comparative guidance spanning multiple programming languages
    - Goal: Avoidance of programming errors that lead to vulnerabilities
ISO/IEC SC 27 IT Security Techniques

- ISO/IEC 15443, FRITSA
  - Part 1: A framework for IT security assurance
  - Part 2: Assurance methods
  - Part 3: Analysis of assurance methods
- ISO/IEC DTR 19791, Assessment of Operational Systems
- ISO/IEC 21827, System Security Engineering Capability Maturity Model (SSE CMM) revision
- ISO/IEC 27000 series
  - Information Security Management System (ISMS)
IEC SC 65A, Functional Safety

- IEC 61508, Functional Safety Of Electrical/Electronic/Programmable Electronic Safety-related Systems (7 parts)
  - Part 1: General requirements
  - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
  - Part 3: Software requirements
  - Part 4: Definitions and abbreviations
  - Part 5: Examples of methods for the determination of safety integrity levels
  - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
  - Part 7: Overview of techniques and measures

- Risk-based approach for determining the required performance of safety-related systems
Standardization In Support of Assurance 

Dependability

- IEC 60300 Series, Dependability Management
- IEC 61713, Software dependability through the software life-cycle processes - Application guide
- IEC 60812, Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
- IEC 61025, Fault tree analysis (FTA)
Standardization In Support of Assurance — FISMA\textsuperscript{1} Implementation

- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information System
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Federal Information Systems
- NIST Special Publication 800-30, Revision 1, Risk Assessment Guideline
- NIST Special Publication 800-39, NIST Risk Management Framework
- NIST Special Publication 800-53 Revision 1, Recommended Security Controls for Federal Information Systems
- NIST Special Publication 800-59, Guide for Identifying an Information System as a National Security System
- NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

\textsuperscript{1}Federal Information Security Management Act of 2002


7th Annual CMMI Technology Conference, 15 November 2007, Track 3, 1015
ISO/IEC/IEEE 15026, System and Software Assurance

24748: Guide to Life Cycle Management

Revised 12207: Life cycle processes for SW
Revised 15289: Documentation
Revised 15288: Life cycle processes for systems
Revised 15026: Additional practices for higher assurance systems

Other standards providing details of selected SW processes
Common vocabulary, process architecture, and process description conventions


15289: Document -
16326: Project Mgmt
15939: Measurement
16085: Risk Mgmt

Interoperation

15026: Additional practices for higher assurance systems
Life Cycle Processes

Organization

- Project-Enabling Processes
  - Life Cycle Model Management
  - Infrastructure Management
  - Project Portfolio Management
  - Human Resource Management
  - Quality Management

- Agreement Processes
  - Supply
  - Acquisition

Project

- Project Management Processes
  - Project Planning
  - Project Assessment & Control

- Project Support Processes
  - Decision Management
  - Risk Management
  - Configuration Management
  - Information Management
  - Measurement

Engineering

- Technical Processes
  - Stakeholder Requirements Definition
  - Requirements Analysis
  - Architectural Design
  - Implementation
  - Integration
  - Verification
  - Transition
  - Validation
  - Operation
  - Maintenance
  - Disposal

SW Implementation Processes

- SW Requirements Analysis
- SW Architectural Design
- SW Detailed Design
- SW Construction
- SW Integration
- SW Qualification Testing

SW Support Processes

- SW Documentation Management
- SW Configuration Management
- SW Quality Assurance
- SW Verification
- SW Validation
- SW Review
- SW Audit
- SW Problem Resolution
- SW Reuse Processes
  - Domain Engineering
  - Reuse Asset Management
  - Reuse Program Management

Source: ISO/IEC CD 15026/4 IEEE P15026/CD1, Systems and software engineering — Systems and software assurance
Set of structured assurance claims, supported by evidence and reasoning, that demonstrates how assurance needs have been satisfied.

- Shows compliance with assurance objectives
- Provides an argument for the safety and security of the product or service.
- Built, collected, and maintained throughout the life cycle
- Derived from multiple sources

Sub-parts

- A high level summary
- Justification that product or service is acceptably safe, secure, or dependable
- Rationale for claiming a specified level of safety and security
- Conformance with relevant standards and regulatory requirements
- The configuration baseline
- Identified hazards and threats and residual risk of each hazard and threat
- Operational and support assumptions

Attributes

- Clear
- Consistent
- Complete
- Comprehensible
- Defensible
- Bounded
- Addresses all life cycle stages

System, Software, or Work Product

Make the case for adequate quality/assurance of the System, Software, or Work Product

Quality / Assurance Case

- Claims
- Arguments
- Evidence

is developed for

Quality / Assurance Factor

Quality / Assurance Subfactor

supports

justify belief in
References


Paul R. Croll  
Computer Sciences Corporation  
5166 Potomac Drive  
King George, VA 22485-5824  

Phone: +1 540.644.6224  
Fax: +1 540.663.0276  
e-mail: pcroll@csc.com