Assurance in Models and Standards Panel – Relationships Between Models and Standards

Paul R. Croll

Computer Sciences Corporation
pcroll@csc.com

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

Industry Co-Chair, NDIA Systems Assurance Committee

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

Chair, IEEE Software and Systems Engineering Standards Committee

Workshop on “Assurance” with CMMI
August 7, 2007

Outline

- Assurance Defined
- The Assurance Problem
- The Engineering Challenge
- Process Maturity In Support Of Assurance
- Standardization In Support Of Assurance
- Summary

System and Software Assurance

System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.

Terms of Reference, ISO/IEC JTC1/SC7 WG9, System and Software Integrity

The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.

CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006

The Assurance Problem

- Assurance-related risks have 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 assurance
- There is a fundamental lack of both the scientific understanding of software risks, and the capabilities to effectively diagnose and mitigate them in the in a timely manner

Source: J. Jarzombek. DOD Software Assurance Initiative: Mitigating Risks Attributable to Software. DOD Software Assurance Forum, July 2004.

Or, More Succinctly . . .

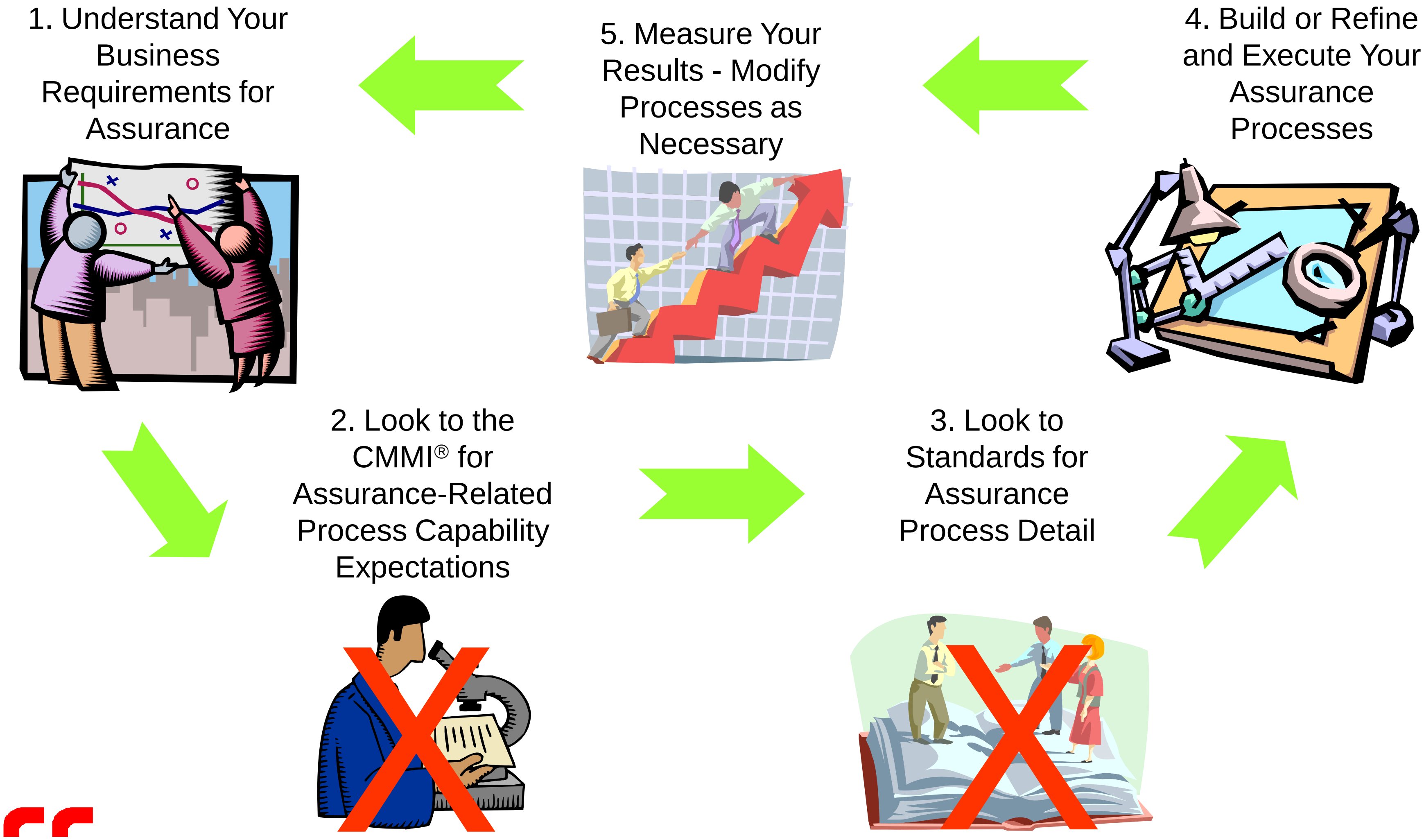
- There is a failure to assure correct, predictable, safe, secure execution of complex software in distributed environments
- Inadequate attention is given to the total lifecycle issues, including impacts on lifecycle cost and risk associated with the use of commercial or reused products and components

Source: G. Draper (ed.), Top Software Engineering Issues Within Department of Defense and Defense Industry. National Defense Industrial Association, Arlington, VA, August 2006.

The 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.

Achieving System and Software Assurance Through CMMI®-Compliant Processes



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

CMMI®- DEV Assurance Shortfalls

- 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

CSC

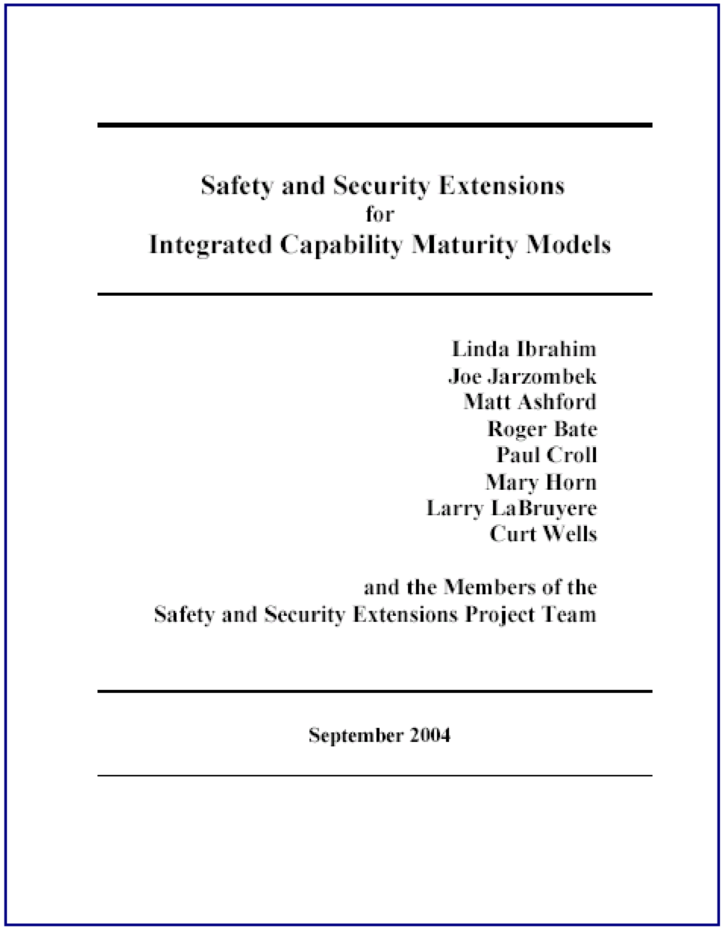
CMMI® – DEV Process Areas and Assurance

Name	*Abbr*	*Safety*	*Security*
Requirements Management	**REQM**	√	√
Project Planning	**PP**	√	√
Project Monitoring and Control	**PMC**		√
Supplier Agreement Management	**SAM**		√
Measurement and Analysis	**MA**		√
Process and Product Quality Assurance	**PPQA**		
Configuration Management	**CM**	√	√
Requirements Development	**RD**	√	√
Technical Solution	**TS**	√	√
Product Integration	**PI**	√	√
Verification	**VER**		
Validation	**VAL**		
Organizational Process Focus	**OPF**		
Organizational Process Definition +IPPD	**OPD +IPPD**	√	√
Organizational Training	**OT**	√	√
Integrated Project Management +IPPD	**IPM +IPPD**	√	√
Risk Management	**RSKM**	√	√
Decision Analysis and Resolution	**DAR**	√	
Organizational Process Performance	**OPP**		
Quantitative Project Management	**QPM**		
Organizational Innovation and Deployment	**OID**		
Causal Analysis and Resolution	**CAR**	√	

Source: CMMI® for Development, Version 1.2, CMU/SEI-2006-TR-008, August 2006

Safety and Security Extensions for Integrated Capability Maturity Models

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**
9. **Determine Regulatory Requirements, Laws, and Standards**
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**



Safety and Security Extensions
for
Integrated Capability Maturity Models

Linda Ibrahim
Joe Jarzombek
Matt Ashford
Roger Bate
Paul Croll
Mary Horn
Larry LaBruyere
Curt Wells

and the Members of the
Safety and Security Extensions Project Team

September 2004

*Source: United States Federal Aviation Administration, Safety and Security Extensions for Integrated Capability Maturity Models, September 2004 (**http://www.faa.gov/about/office_org/headquarters_offices/aio/documents/media/SafetyandSecurityExt-FINAL-web.pdf**)*

Source Standards

Safety

- Defence Standard 00-56, Safety Management Requirements for Defence Systems, Ministry of Defence, United Kingdom, December 1996.
- IEC 61508, Functional Safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, 1997.
- Military Standard System Safety Program Requirements, MIL-STD-882C, United States Department of Defense, January 1993.
- Standard Practice for System Safety, MIL-STD-882D, United States Department of Defense, February 2000.

Security

- ISO/IEC 21827, Systems Security Engineering Capability Maturity Model®, SSE-CMM®, Model Description Document, Version 3.0, June 15, 2003.
- ISO/IEC 15408:1999, Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1, 1999.
- ISO/IEC 17799:2000(E): Information technology – Code of practice for information security management, International Organization for Standardization, First edition 2000-12-01.
- Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Special Publication 800-30, 2001.

*Source: United States Federal Aviation Administration, Safety and Security Extensions for Integrated Capability Maturity Models, September 2004 (***http://www.faa.gov/about/office_org/headquarters_offices/aio/documents/media/SafetyandSecurityExt-FINAL-web.pdf***)*

Standardization In Support Of Assurance – 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

Standardization In Support Of Assurance – IT Security Techniques

- **ISO/IEC 15408**, Common Criteria for IT Security Evaluation
- **ISO/IEC 15443**, FRITSA
  - Part 1: A framework for IT security assurance
  - Part 2: Assurance methods
  - Part 3: Analysis of assurance methods
- **ISO/IEC 17799:2005,** Code of Practice for Information Security Management
- **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)

Standardization In Support Of Assurance – Functional Safety

- IEC SC 65A
  - **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)

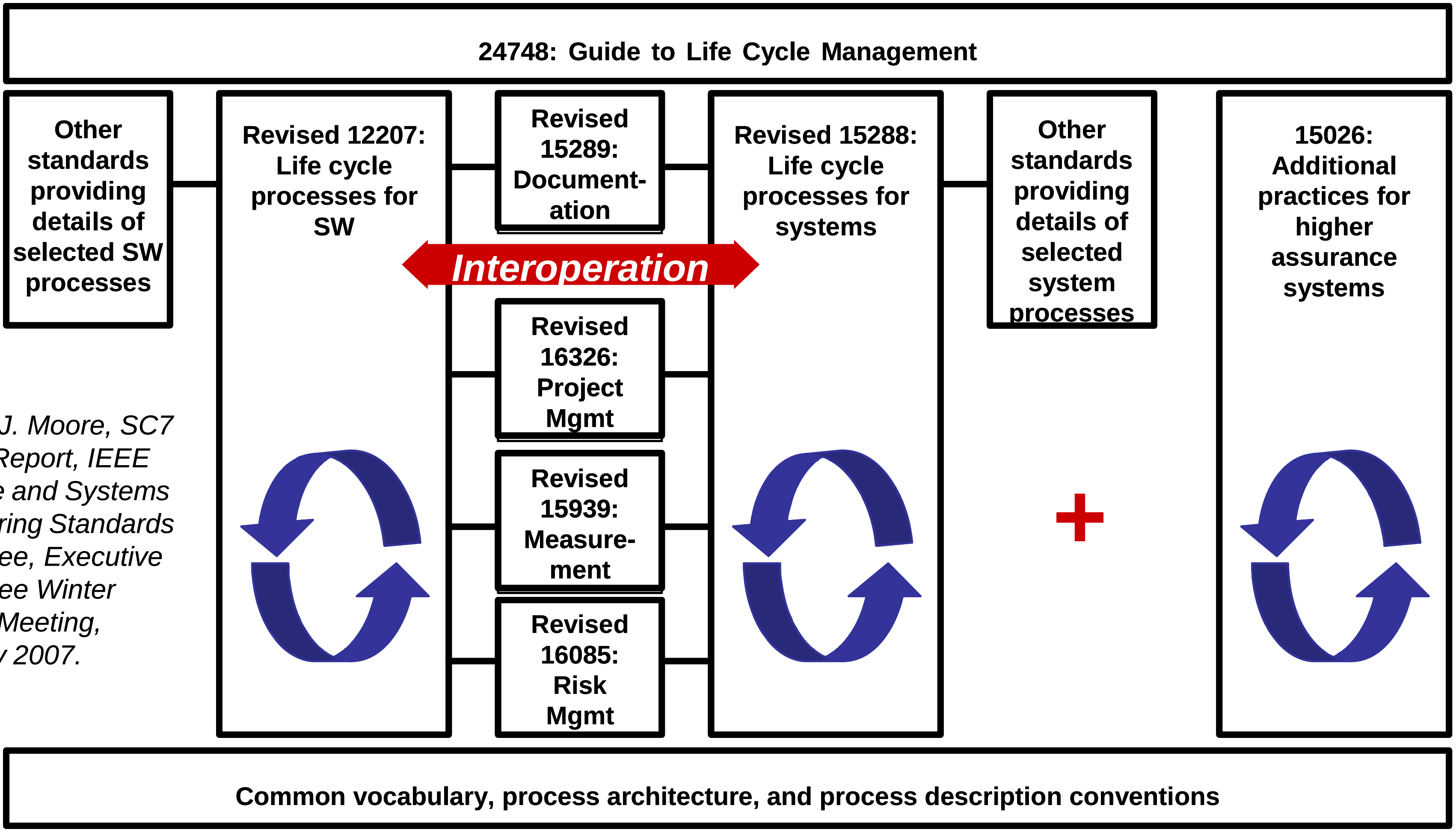
Standardization In Support of Assurance – FISMA[1] Implementation

- **FIPS Publication 199**, Standards for Security Categorization of Federal Information and Information System (Completed)
- **FIPS Publication 200**, Minimum Security Requirements for Federal Information and Federal Information Systems (Completed)
- **NIST Special Publication 800-30, Revision 1**, Risk Assessment Guideline (Completion December 2007)
- **NIST Special Publication 800-37**, Guide for the Security Certification and Accreditation of Federal Information Systems (Completed)
- **NIST Special Publication 800-39**, NIST Risk Management Framework (Completion December 2007)
- **NIST Special Publication 800-53 Revision 1**, Recommended Security Controls for Federal Information Systems (Completed)
- **NIST Special Publication 800-53A**, Guide for Assessing the Security Controls in Federal Information Systems (Completion July 2007)
- **NIST Special Publication 800-59**, Guide for Identifying an Information System as a National Security System (Completed)
- **NIST Special Publication 800-60**, Guide for Mapping Types of Information and Information Systems to Security Categories (Completed)

[1] *Federal Information Security Management Act of 2002*

Source: ***http://csrc.nist.gov/sec-cert/ca-proj-phases.html***

Standardization In Support Of Assurance – Life Cycle Processes



24748: Guide to Life Cycle Management

Other standards providing details of selected SW processes

Revised 12207: Life cycle processes for SW

Revised 15289: Document-ation

Interoperation

Revised 16326: Project Mgmt

Revised 15939: Measure-ment

Revised 16085: Risk Mgmt

Revised 15288: Life cycle processes for systems

Other standards providing details of selected system processes

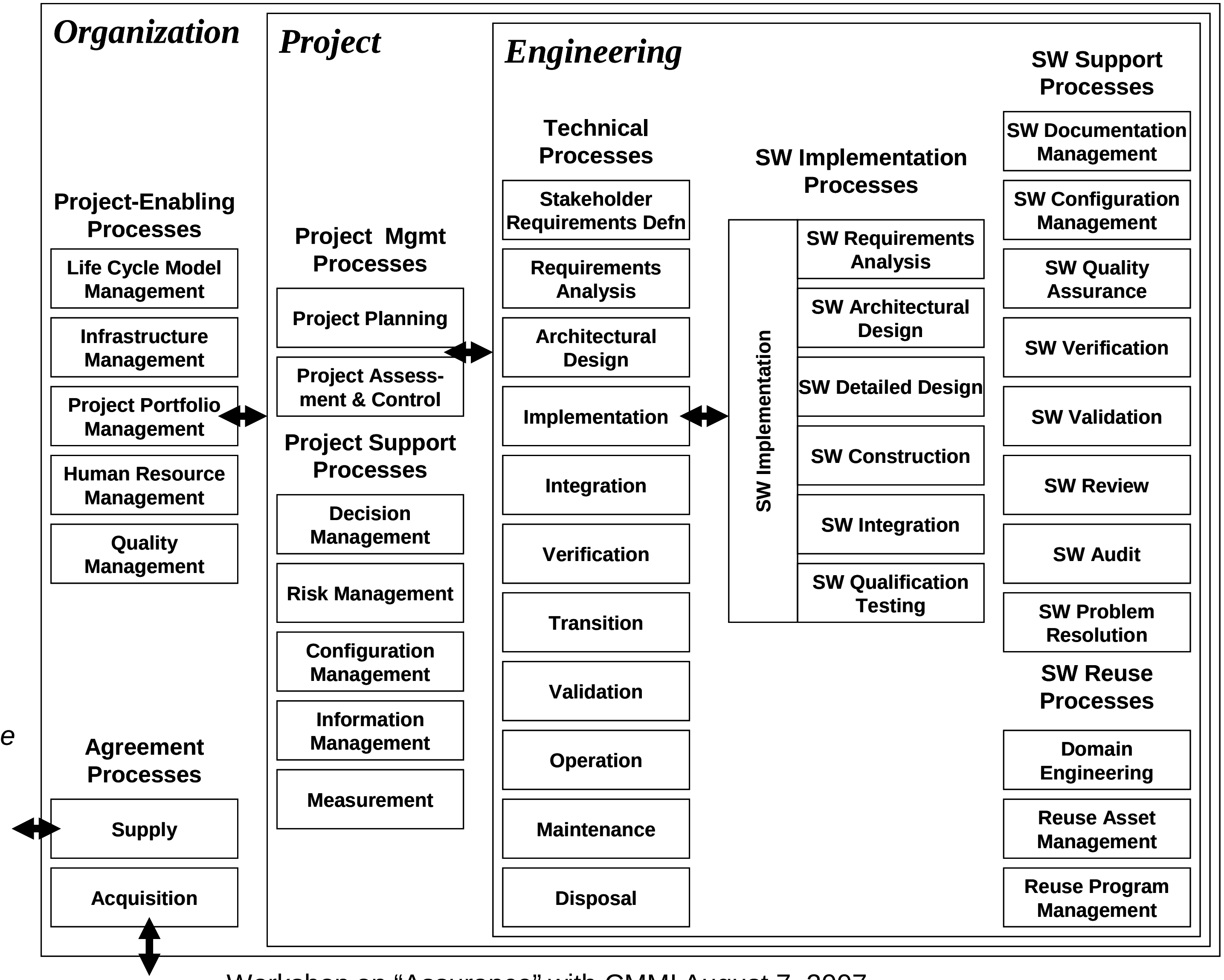
+

15026: Additional practices for higher assurance systems

Common vocabulary, process architecture, and process description conventions

Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.

15288 And 12207 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 Mgmt Processes

- Project Planning
- Project Assess-ment & Control

Project Support Processes

- Decision Management
- Risk Management
- Configuration Management
- Information Management
- Measurement

Engineering

Technical Processes

- Stakeholder Requirements Defn
- Requirements Analysis
- Architectural Design
- Implementation
- Integration
- Verification
- Transition
- Validation
- Operation
- Maintenance
- Disposal

SW Implementation Processes

SW Implementation

- 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

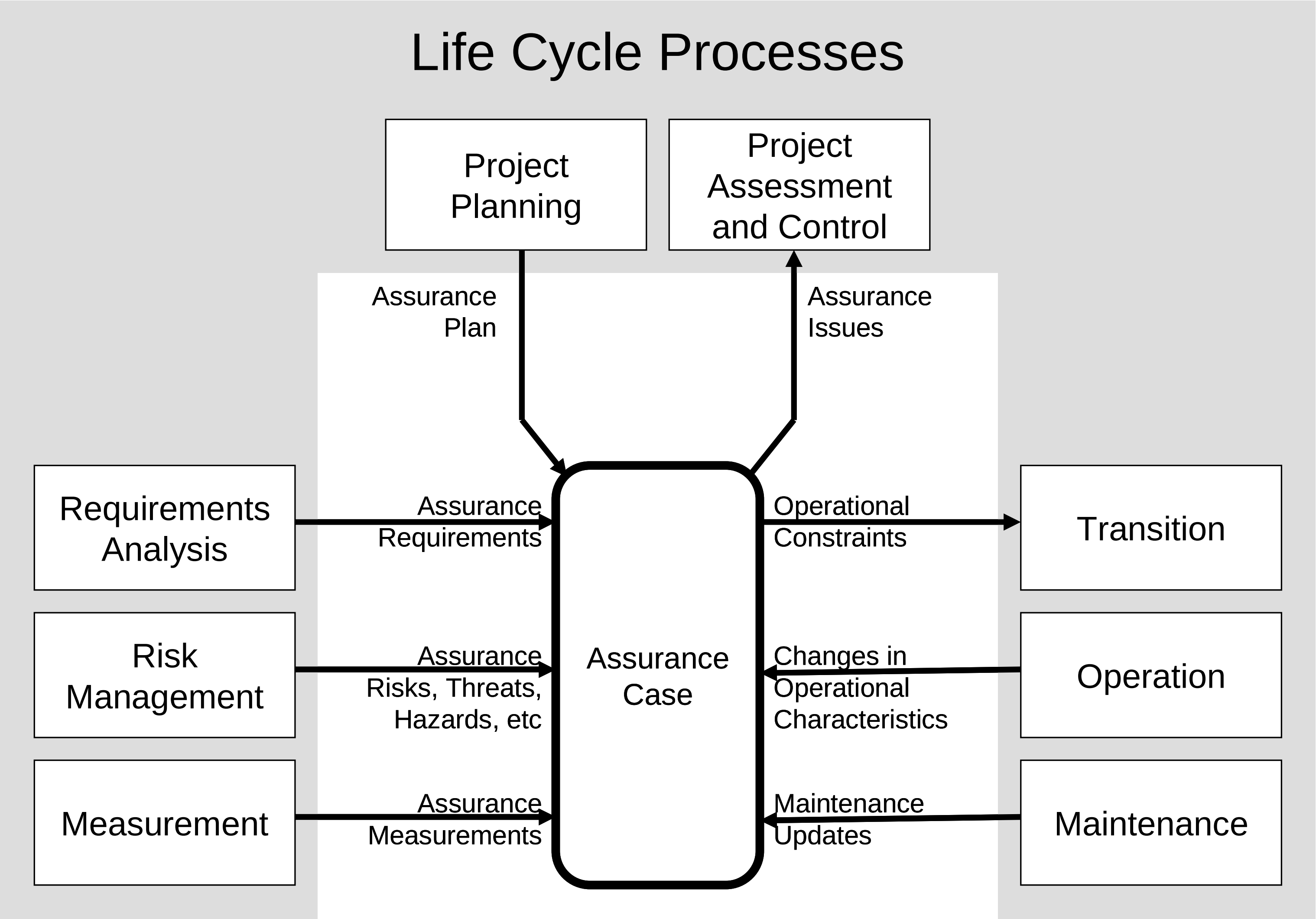
- Domain Engineering
- Reuse Asset Management
- Reuse Program Management

Source: ISO/IEC CD 15026/4 IEEE P15026/CD1, Systems and software engineering — Systems and software assurance

Examples Of Additional Requirements – Risk Management

- The safety, security, or dependability risks ***shall*** be considered along with other risks in a similar, integrated fashion.
- The assurance case ***shall*** be integrated into the Risk Management process as containing essential information.

Role Of The Assurance Case

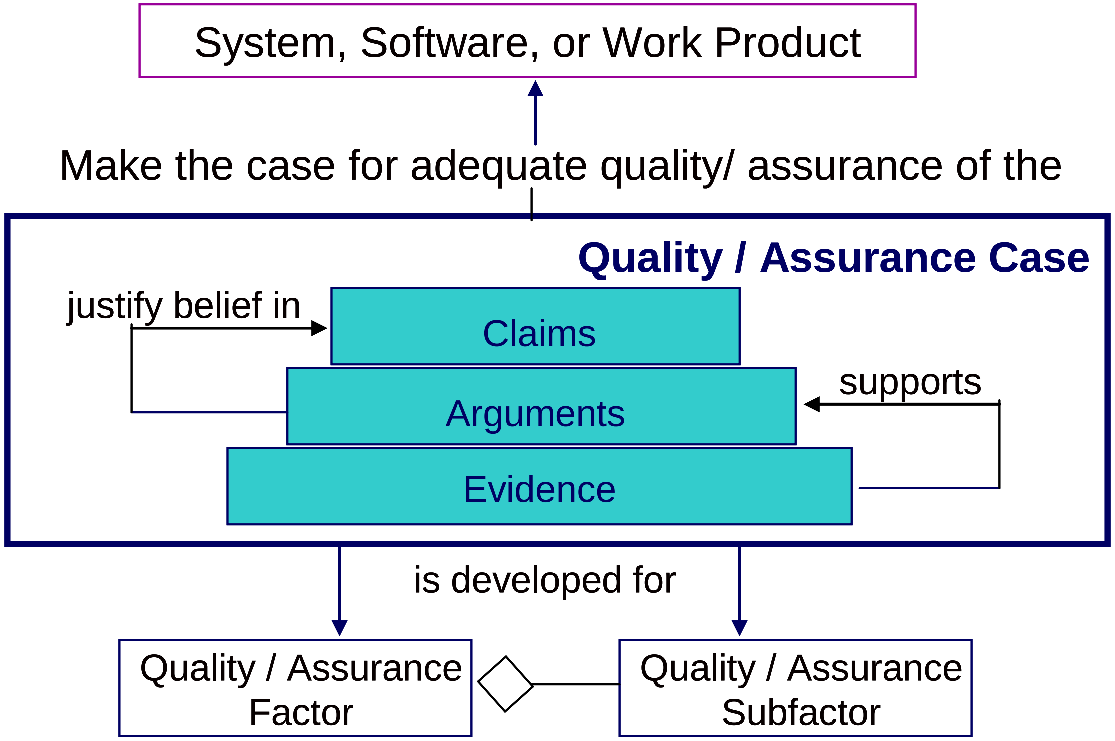


Source: J. Moore, Proposed Revision of ISO/IEC 15026: Status Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Summer Plenary Meeting, July 2007.

Structure Of The Assurance Case

- 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

The Assurance Case In Relation To The Product And Its Quality/Assurance Factors


System, Software, or Work Product
Make the case for adequate quality/ assurance of the
Quality / Assurance Case
justify belief in
Claims
Arguments
supports
Evidence
is developed for
Quality / Assurance Factor
Quality / Assurance Subfactor

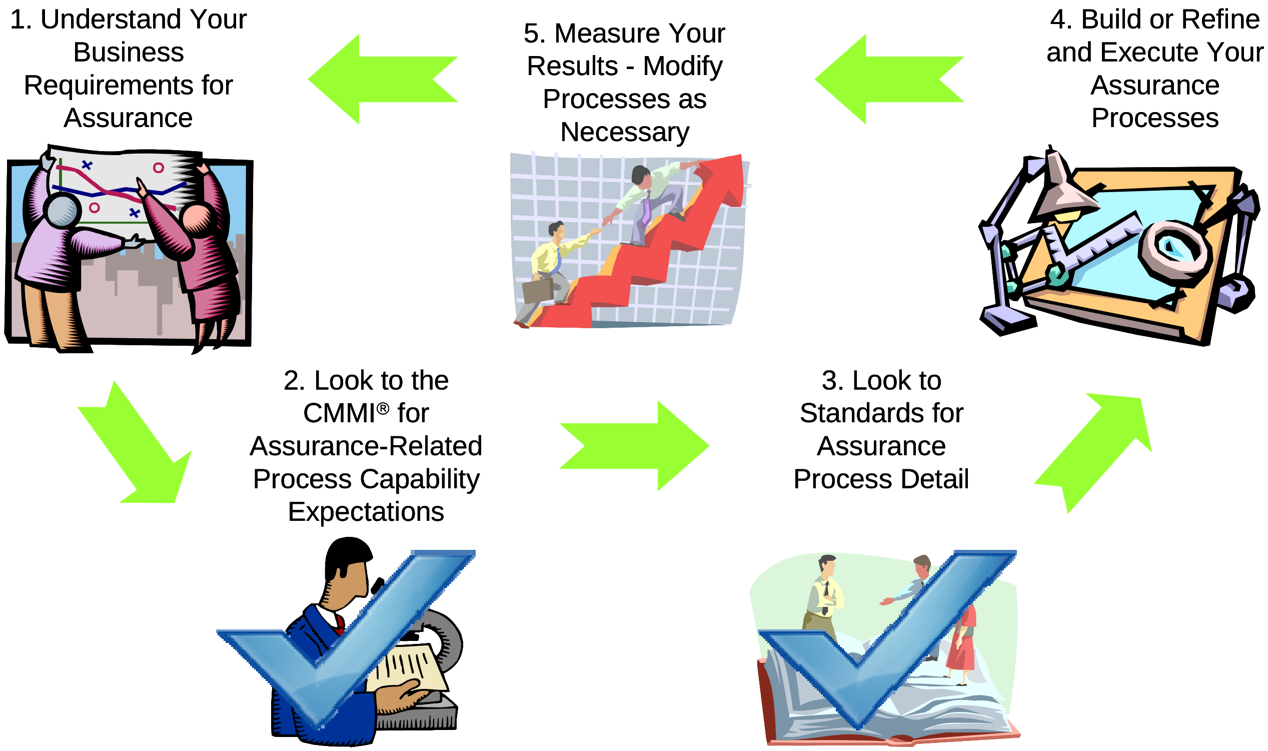
Attributes

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

Adapted from a slide by Joe Jarzombek who, in turn, credited IEEE CS alternative proposal for 15026 and CMU SEI QUASAR tutorial by Donald Firesmith, March 2007

Summary

Adding explicit assurance-related process requirements to the CMMI® and to supporting standards facilitates the development, integration, operation, maintenance, and disposal of systems and software which meet stakeholder expectations that 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

For More Information . . .

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