Engineering for System Assurance – Legacy, Life Cycle, Leadership

Paul R. Croll

Computer Sciences Corporation
pcroll@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
- Engineering Shortfalls
- Seven Systems Engineering Community Leadership Challenges
- Guidance For Systems Assurance
- Standardization In Support Of Systems Assurance
- Summary

System Assurance Defined

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
  - Can't 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 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.

System Assurance Engineering Shortfalls

- Current techniques for specifying, building, demonstrating, and verifying assured components with well understood properties are not cost-effective or scaleable
- Cannot easily infer the assurance properties of a system, or systems of systems, from component level assurance information
- Don’t know enough about composability problems and emergent behavior when components are interconnected in large-scale systems and systems of systems
- Exhaustive testing to rule out vulnerabilities is generally not feasible due to the size and complexity of our systems of interest

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

The 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.

Systems Engineering Community Leadership Challenges #1 – Acquisition

Collaboration to develop new approaches and improve existing approaches, standards, and tools that address systems assurance issues throughout the acquisition life cycle and the supply chain

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

Systems Engineering Community Leadership Challenges #2 – Engineering Practices

Integration of systems and software engineering practices for producing system architectures and resulting systems that are resistant to intrusion and compromise

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

Systems Engineering Community Leadership Challenges #3 – Research

Sponsor research into new modalities for system composition to meet specific assurance objectives

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

Systems Engineering Community Leadership Challenges #4 – Quality Attributes

Define systems and software assurance quality attributes that can be addressed during architectural tradeoffs

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

Systems Engineering Community Leadership Challenges #5 – Standardization

Encourage the development of commercial standards addressing vulnerability management throughout the supply chain, including product-level and component-level specifications and standards for detecting component vulnerabilities

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

Systems Engineering Community Leadership Challenges #6 – Policy and Guidance

Develop policy, guidance, and training for the acquisition of systems with desired assurance properties

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

Systems Engineering Community Leadership Challenges #7 – Life Cycle Planning

Ensure that life cycle issues and tradeoffs associated with the incorporation of commercial components and reused software into systems are clearly addressed in program plans, systems engineering plans, test and evaluations plans, and during periodic reviews

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

Guidance For Systems Assurance - 1

- ***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

NDIA/DoD System Assurance Guidebook – Scope

- Practical guidance for the Government acquisition community, industry, academia, and other commercial and government partners
- Synthesis of knowledge gained from existing practice, recommendations, policy, and mandate, rather than reinventing the wheel
- Recap of important concepts and principles from foundational documents, standards, and mandates, and discussion of them in the larger context of systems assurance as presented by the White Paper

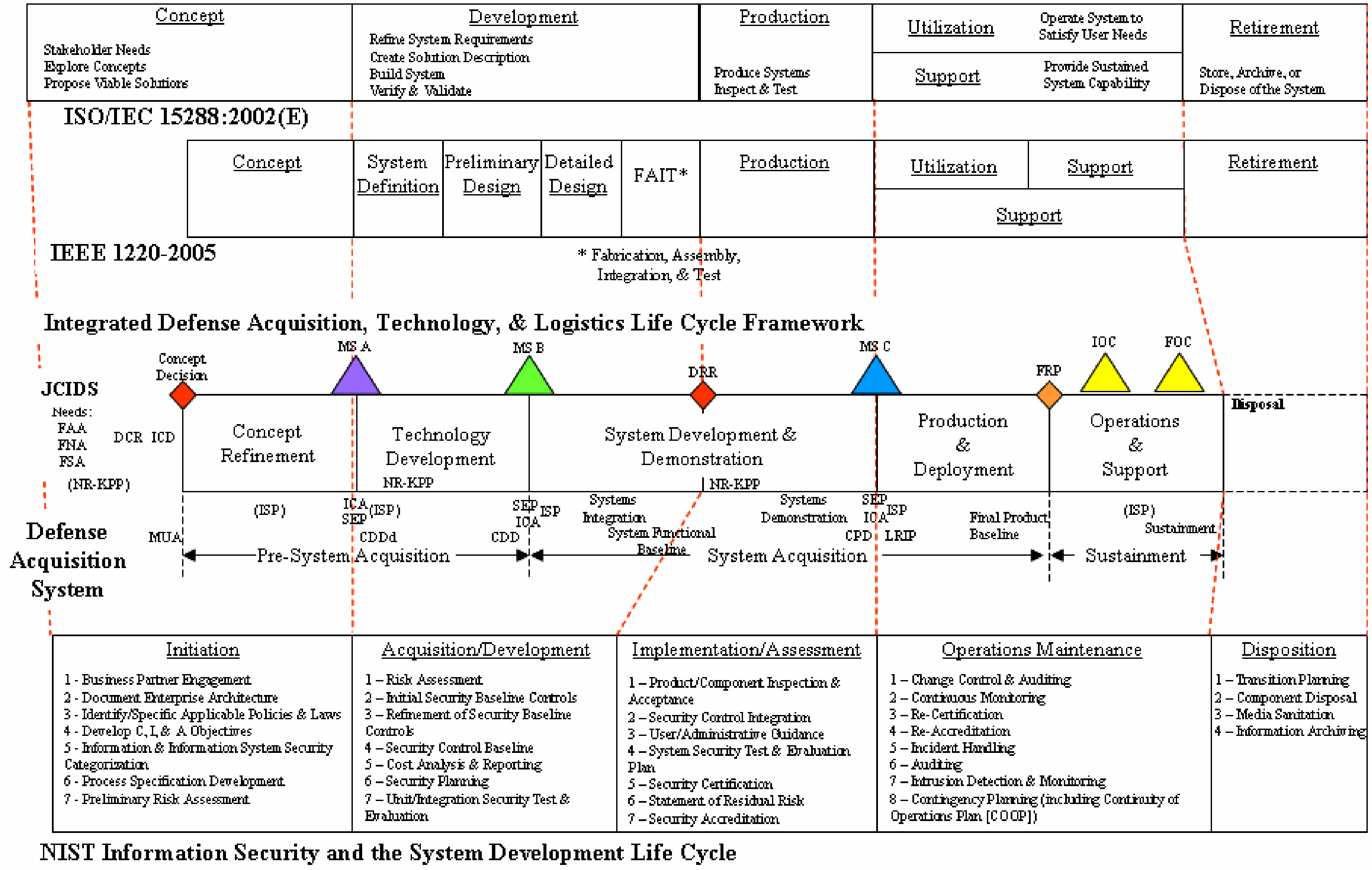
NDIA/DoD System Assurance Guidebook – Mapped To ISO/IEC/IEEE 15288

- 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

Alignment of Standards In The Guidebook



Concept	Development	Production	Utilization Support	Operate System to Satisfy User Needs Provide Sustained System Capability	Retirement
Stakeholder Needs Explore Concepts Propose Viable Solutions	Refine System Requirements Create Solution Description Build System Verify & Validate	Produce Systems Inspect & Test			Store, Archive, or Dispose of the System

ISO/IEC 15288:2002(E)

Concept	System Definition	Preliminary Design	Detailed Design	FAIT*	Production	Utilization	Support	Retirement
						Support		

IEEE 1220-2005

* Fabrication, Assembly, Integration, & Test

Integrated Defense Acquisition, Technology, & Logistics Life Cycle Framework

Defense Acquisition System

Initiation	Acquisition/Development	Implementation/Assessment	Operations Maintenance	Disposition
1 - Business Partner Engagement 2 - Document Enterprise Architecture 3 - Identify/Specific Applicable Policies & Laws 4 - Develop C, I, & A Objectives 5 - Information & Information System Security Categorization 6 - Process Specification Development 7 - Preliminary Risk Assessment	1 – Risk Assessment 2 – Initial Security Baseline Controls 3 – Refinement of Security Baseline Controls 4 – Security Control Baseline 5 – Cost Analysis & Reporting 6 – Security Planning 7 – Unit/Integration Security Test & Evaluation	1 – Product/Component Inspection & Acceptance 2 – Security Control Integration 3 – User/Administrative Guidance 4 – System Security Test & Evaluation Plan 5 – Security Certification 6 – Statement of Residual Risk 7 – Security Accreditation	1 – Change Control & Auditing 2 – Continuous Monitoring 3 – Re-Certification 4 – Re-Accreditation 5 – Incident Handling 6 – Auditing 7 – Intrusion Detection & Monitoring 8 – Contingency Planning (including Continuity of Operations Plan [COOP])	1 – Transition Planning 2 – Component Disposal 3 – Media Sanitation 4 – Information Archiving

NIST Information Security and the System Development Life Cycle

Guidance For Systems Assurance - 2

- ***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

Guidance For Systems Assurance - 3

- ***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

- ***Security in the Software Life Cycle: Making Software Development Processes – and the Software Produced by Them – More Secure***
  - 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

Guidance For Systems Assurance - 5

- ***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 Systems Assurance - Languages

- ISO/IEC SC22 (Languages)
  - ISO/IEC Technical Report – Guidance for Avoiding Vulnerabilities through Language Selection and Use
    - Comparative guidance spanning multiple programming languages
    - Goal: Avoidance of programming errors that lead to vulnerabilities

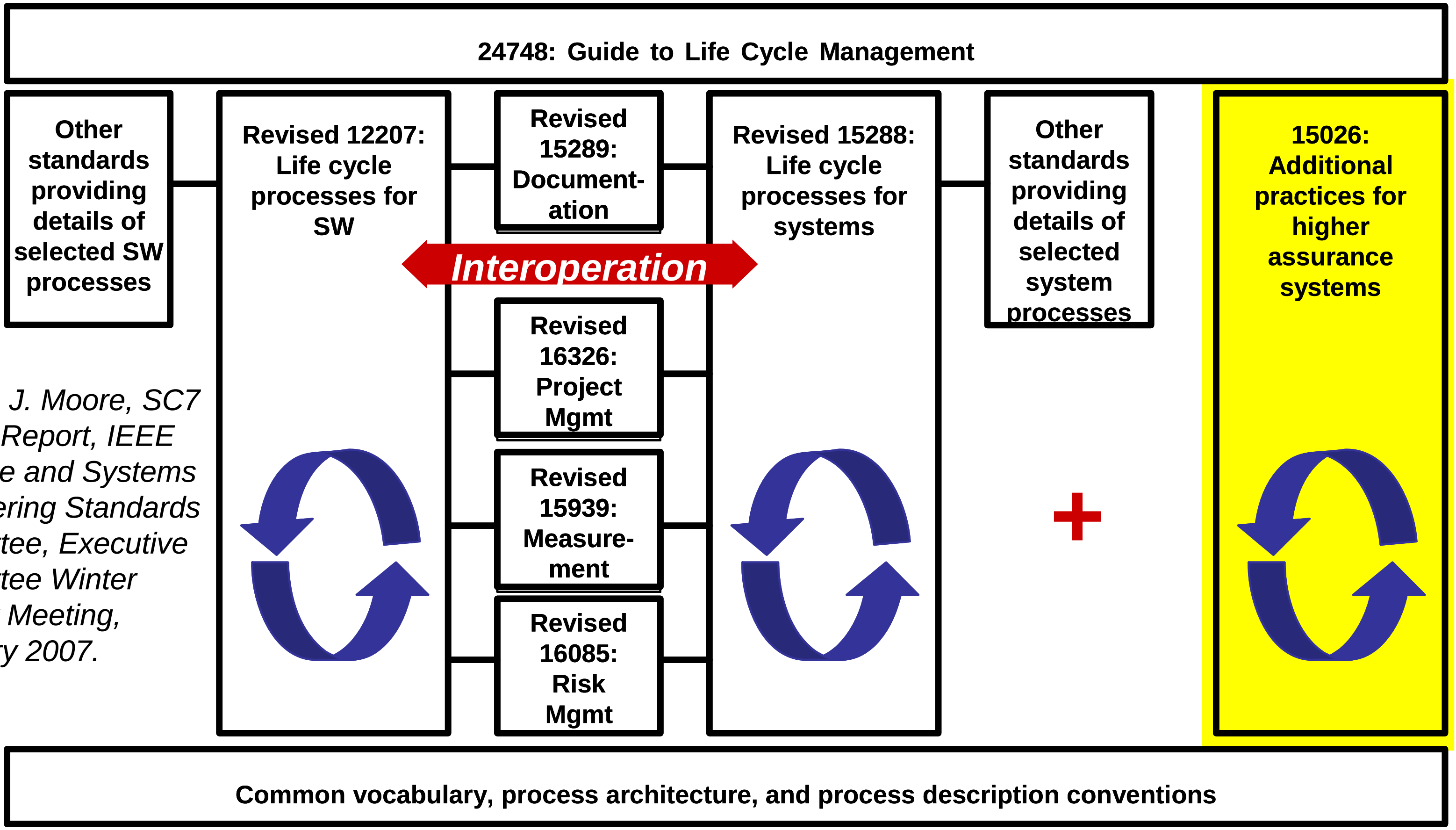
Standardization In Support Of Systems Assurance - Security

- ISO/IEC SC27 (IT Security Techniques)
  - ISO/IEC 21827, System Security Engineering Capability Maturity Model (SSE CMM)
  - ISO/IEC 15443 (FRITSA), A framework for IT security assurance
  - ISO/IEC DTR 19791, Assessment of Operational Systems

Standardization In Support Of Systems Assurance - Safety

- IEC SC 65A (Functional Safety)
  - IEC 61508, Functional Safety
    - Risk-based approach for determining the required performance of safety-related systems
    - Requirements based on common underlying principles to facilitate:
      - Supply chain efficiencies
      - Clear communication of requirements
      - Development of techniques and measures
      - Development of conformity assessment models

Standardization In Support Of Systems Assurance – System and Software Assurance



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.

ISO/IEC/IEEE 15026, System and Software Assurance

- A 65-page draft has been balloted
  - It incorporates material from FCD 12207, FCD 15288, ISO/IEC 15289, IEEE Std 1228 and the safety and security extensions to CMMI
- The draft contains requirements and guidance for:
  - Assurance cases
  - Associated documents, e.g. assurance plan, reports, analyses
- The process view is comprehensive—it touches every process of 15288 and 12207 (except for the enterprise processes)
- Joint comment resolution is in progress

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.

Current Draft of Scope Clause

- This International Standard provides requirements for the life cycle including development, operation, maintenance, and disposal of systems and software products that are critically required to exhibit and be shown to possess properties related to safety, security, dependability, or other characteristics
- It defines an ***assurance case*** as the central artefact for planning, monitoring, achieving and showing the achievement and sustainment of the properties and for related support of other decision making
- ***The interaction of the requirements for the assurance case with life cycle processes implies a normative interpretation of the processes from ISO/IEC 15288 and ISO/IEC 12207***
- Finally, the standard provides requirements, in addition to those of ISO/IEC 15289, for information artefacts that result from those processes

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.

Relationships to Other Standards

- The provisions regarding process in this international standard make extensive normative references to **ISO/IEC 12207:2007 and ISO/IEC 15288:2007**, the international standards for software and system life cycle processes.
- Users of this international standard will probably require risk management and measurement processes that are more fully detailed than the treatment provided in ISO/IEC 15288. Two international standards, **ISO/IEC 16085** and **ISO/IEC 15939** are useful in this regard.
- The provisions regarding the assurance plan and assurance case are intended to be compatible with the provisions of ISO/IEC 15289:2006 for information items resulting from life cycle processes.
- Some material regarding assurance planning and its supporting analyses has been adapted from **IEEE Std 1228:1994**.
- The provisions regarding product characteristics are intended to be generally consistent with those of the **ISO/IEC 25000** series of standards related to product quality, the **ISO/IEC 27000** series of standards related to information security management systems, the **IEC 61508** standard on functional safety, and various standards of IEC TC 56 related to dependability.
- **ISO/IEC TR 15443**, Information technology--Security techniques--A framework for IT security assurance, discusses the need for arguments and evidence in the IT context.

Current Draft Conformance Clause

- This international standard is **intended to be used in conjunction with ISO/IEC 12207 and ISO/IEC 15288**. This standard provides requirements and guidance in addition to that of the referenced standards. To conform to this international standard, one conforms to the referenced standards and conforms to the additional requirements of this international standard.
- It is permitted to assert conformance for **specified properties of the system or to specified portions of the system** if the assertion is accompanied by a **clear statement of the limitations** ...
- ***One may assert conformance to this standard for specific product claims related to stated critical properties or characteristics for specifically identified versions of products or portions of products under specified conditions***. ... Assertions of conformance that relate only to the lack of limited categories of faults or weaknesses must not be stated as claims for more general properties such as security or safety. ...

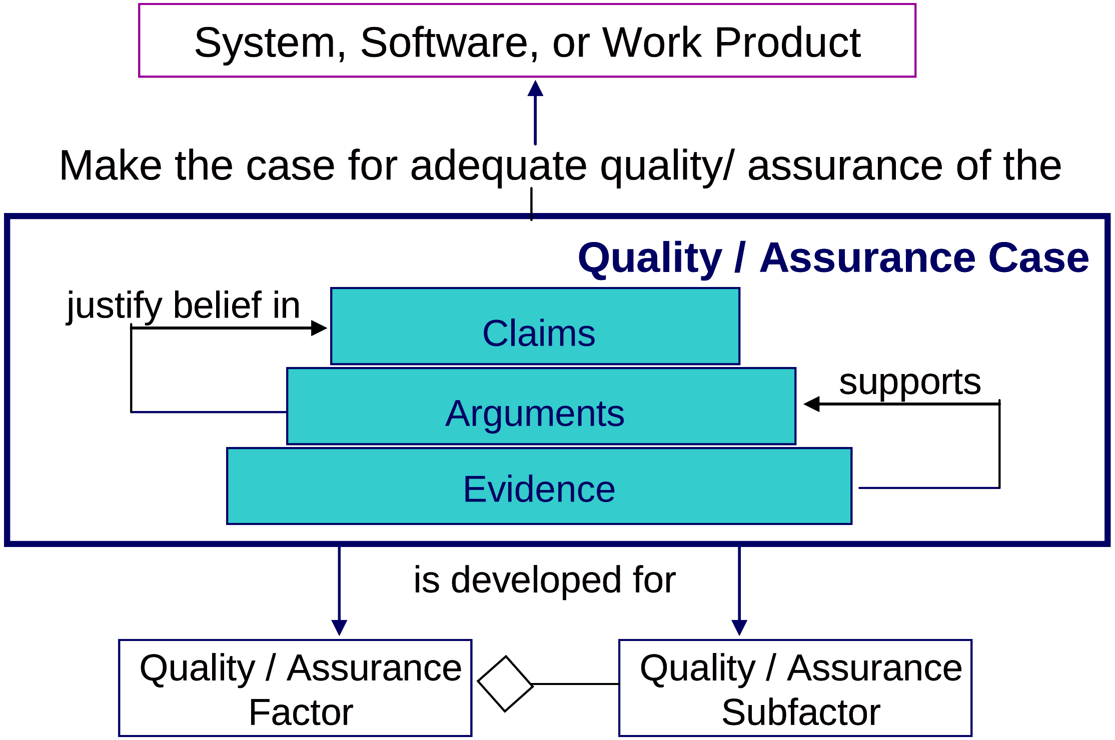
Source: J. Moore, Proposed Revision of ISO/IEC 15026: Status Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Summer Plenary Meeting, July 2007.

General Requirements on Assurance Cases

- **The project shall establish and maintain an assurance case**.
- **The project shall ensure that**:
  - Goals and objectives for safety, security, dependability and any other designated critical properties are formulated.
  - Product assurance-related objectives, properties, or characteristics are explicitly selected for special attention and application of this standard to address the goals and objectives.
  - Requirements for the achievement of these objectives, properties, or characteristics are defined.
  - Measures for the requirements are selected and related to the desired characteristics.
  - Criteria for the achievement or degree or achievement of these objectives, properties, or characteristics are selected and traced to requirements.
  - Approaches for achieving the objectives, properties, or characteristics are planned, designed, and implemented, as well as demonstrating and documenting that achievement.
  - The extent of achievement is continuously monitored, documented, and communicated to stakeholders and managers.
  - An assurance case documenting and communicating the extent of achievement is specified, developed, and maintained as an element of the system.
  - The artefacts for documenting, analyzing, and communicating the required or claimed properties and characteristics and the extent of achievement are specified, developed, and maintained.
  - Requirements of the approval authority are satisfied and necessary licenses or certifications are received.

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.

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
supports
Arguments
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

- The systems engineering challenge for systems assurance is in 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.
- Joint industry and Government efforts are ongoing to understand the strengths and weaknesses of current engineering practices and to provide appropriate guidance
- National and international standards efforts are also capturing and codifying minimum acceptable practice regarding engineering for systems assurance
- Systems engineers must lead the way in sensitizing their stakeholders to the assurance implications of engineering decisions made throughout the life cycle and instill practices in their own engineering organizations that facilitate system assurance

References

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

K. Goertzel (ed.), *State of the Art Report on Software Security Assurance, Draft*. DOD Information Assurance Technical Assistance Center (IATAC) and the DOD Data and Analysis Center for Software (DACS), March 2007.

K. Goertzel (ed.), *Security in the Software Life Cycle: Making Software Development Processes – and the Software Produced by Them – More Secure, Draft 1.1*. U.S. Department of Homeland Security, July 2006.

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

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

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

C. Powell and D. Kleiner (eds.), *Systems Assurance – Delivering Mission Success in the Face of Developing Threats*. National Defense Industrial Association, Arlington, VA, January 2007.

S. Redwine (ed.), Secure *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software*, *Draft 1.1*. U.S. Department of Homeland Security, September 25 2006.

Software Assurance in Acquisition: Mitigating Risks to the Enterprise, Draft 1.0. U.S. Department of Homeland Security, March 2007.

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