# ISO/IEC/IEEE 15026
# Systems and Software Assurance


Paul R. Croll
CSC
pcroll@csc.com

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

*Chair, IEEE Software and Systems Engineering Standards Committee*

*Chair, U.S. Technical Advisory Group for ISO/IEC JTC1/SC7*

# Topics

- Assurance Defined
- The Assurance Problem Space
- DoD-Related Guidance For Systems Assurance
- ISO/IEC/IEEE15026 in the System and Software Life Cycles
- ISO/IEC/IEEE 15026, System and Software Assurance
- The ISO/IEC/IEEE 15026 Assurance Case
- Current Status

# Assurance Defined

*From ISO/IEC DTR 15026-1, Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary, January 2009*

- Assurance

  Grounds for justified confidence that a claim has been or will be achieved

  Assurance case

  Representation of a claim or claims, and the support for these claim

# The 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 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 problem**

# DoD-Related Guidance For Systems Assurance

- ***National Defense Industrial Association Guidebook on Engineering for System Assurance***
  - Intended to supplement the knowledge of systems (and software) engineers who have responsibility for systems for which there are assurance concerns
    - General Guidance mapped to ISO/IEC 15288, System Life Cycle Processes
    - DoD Specific Guidance
      - Anti-Tamper
      - DAG Lifecycle Framework
      - Technology Development Phase
      - System Development & Demonstration Phase
      - Production, Deployment, Operations, & Support Phases
      - Supporting Processes
      - Periodic Reports
      - Supplier Assurance
      - Mappings
    - Correspondence with Existing Documentation, Policies, and Standards
      - Executive Policy, Services Standards, NIST/NSA (NIAP) Standards, GEIA, AIA, IEEE, ISO Standards, Best Practice (e.g., DHS/DOD SwABOK)

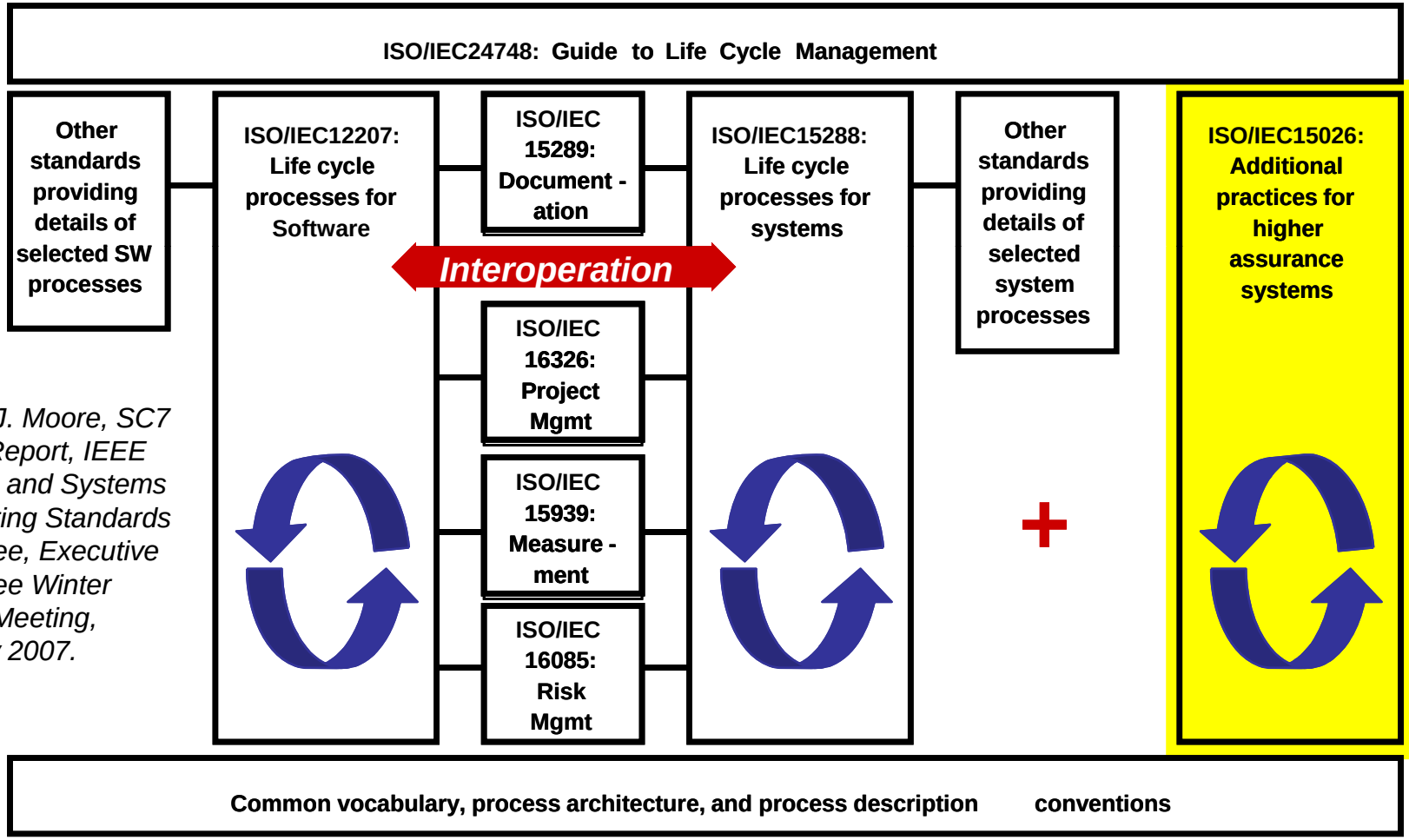
# NDIA/DoD System Assurance Guidebook – Mapped To ISO/IEC/IEEE 15288

- 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

# ISO/IEC/IEEE 15026 in the System and Software Life Cycles



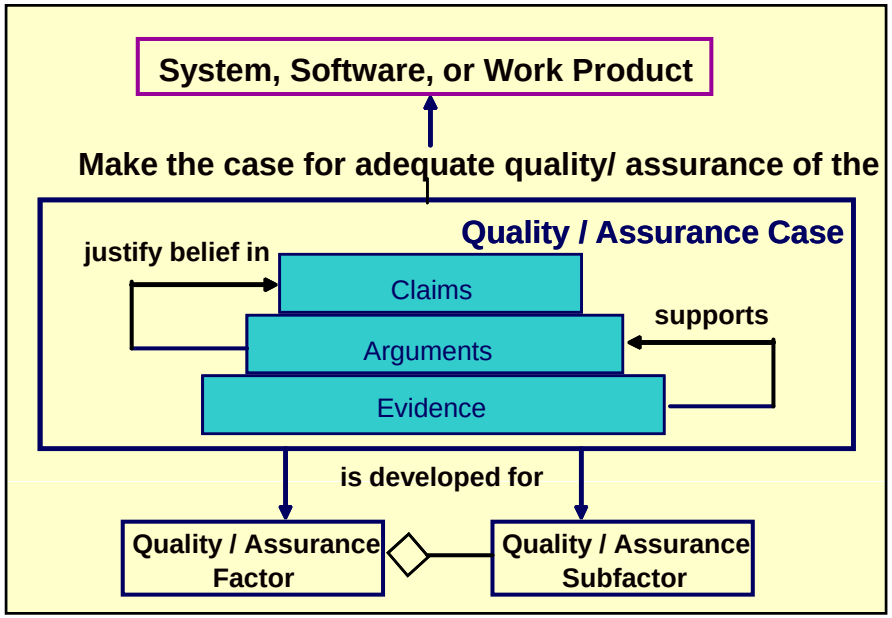

*Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.*

# ISO/IEC/IEEE 15026, System and Software Assurance

- A four-part standard
  - 15026-1: Concepts and vocabulary
    - Initially a Technical Report
  - 15026-2: Assurance case
    - Includes requirements on the assurance case content and the life cycle of the assurance case itself as well as an informative clause on planning for the assurance case itself
  - 15026-3: System integrity levels (a revision of the 1998 standard)
    - Relates integrity levels to the assurance case and includes related requirements for their use with and without an assurance case
  - 15026-4: Assurance in the life cycle
    - Addresses concurrent development and maintenance of the product and the assurance case including project planning for assurance considerations

# The ISO/IEC/IEEE 15026 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

***Attributes***

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

# Current Status

- 15026-1: Concepts and vocabulary
  - In DTR (Draft Technical Report) ballot
- 15026-2: Assurance case
  - CD 2 (Committee Draft) approved, but is being re-balloted
- 15026-3: System integrity levels (a revision of the 1998 standard)
  - Working Draft in progress
- 15026-4: Assurance in the life cycle
  - Working Draft in progress

# For More Information . . .

Paul R. Croll
CSC
17021 Combs Drive
King George, VA  22485

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