Engineering in Depth

NDIA Summit on Software Assurance
September 7-8, 2005
Arlington, VA

Ken Hong Fong
Chuck Johnson
OUSD(AT&L), Defense Systems
Systems Engineering/Enterprise Development
ekenneth.hongfong@osd.mil; (703) 695-0472
chuck.johnson.ctr@osd.mil; (703) 602-0851 X123

Mitch Komaroff
OASD(NII) Commercial Policy & Oversight
mitchell.komaroff@osd.mil
703-602-0980 x146

Wednesday, September 7th 0800 - 1700

- Opening remarks - NDIA
- DoD Software Assurance Efforts – OSD Tiger Team
- DHS Software Assurance Efforts – DHS Dir, Software Assurance
- **Overview: Engineering-in-Depth – OSD DS/Systems Engineering**
- Overview: Science and Technology
- **Afternoon: Structured Breakout Sessions**
  - Science and Technology for SwA
  - Industry Best Practices for SwA

Thursday, September 8, 0800-1500

- Industry Perspective – TBD
- Report out from Wednesday Breakout
- Structured Breakout Sessions
  - Engineering processes for SwA
  - Standards, metrics, models for SwA
- **Afternoon: Breakout Sessions Report Out**
- General Discussion and Way Ahead

Software Assurance (SwA) Definition

Software assurance (SwA) is the level of confidence that software is free of exploitable vulnerabilities, either intentionally or unintentionally designed as part of the software or inadvertently created.

SwA Systems Goals and Objectives

- Free of exploitable vulnerabilities
- Function reliably as intended
- Free of malicious functionality
- Cannot be used as conduits for attack
- Secure from IA exploitation
- Leverage commercial technologies for cost, schedule, performance
- Logistically supportable, economically maintainable and technically up-gradable
- Efficiently hardened against malicious intent
- Can operate in increasingly hostile environments

Notional Workshop Goals

- Engineering In Depth Strategy Review
  - EID Model
    - How do we make it more effective?
  - Who we've engaged and results to date
    - OMG Problem Statement
  - Desires and Expectations for NDIA engagement
    - Whitepapers
    - Who would provide them?
    - By when?
    - What are the mechanisms for continued engagement?
- Standards, Metrics & Models
  - Concepts for review
  - Formulation of way-ahead

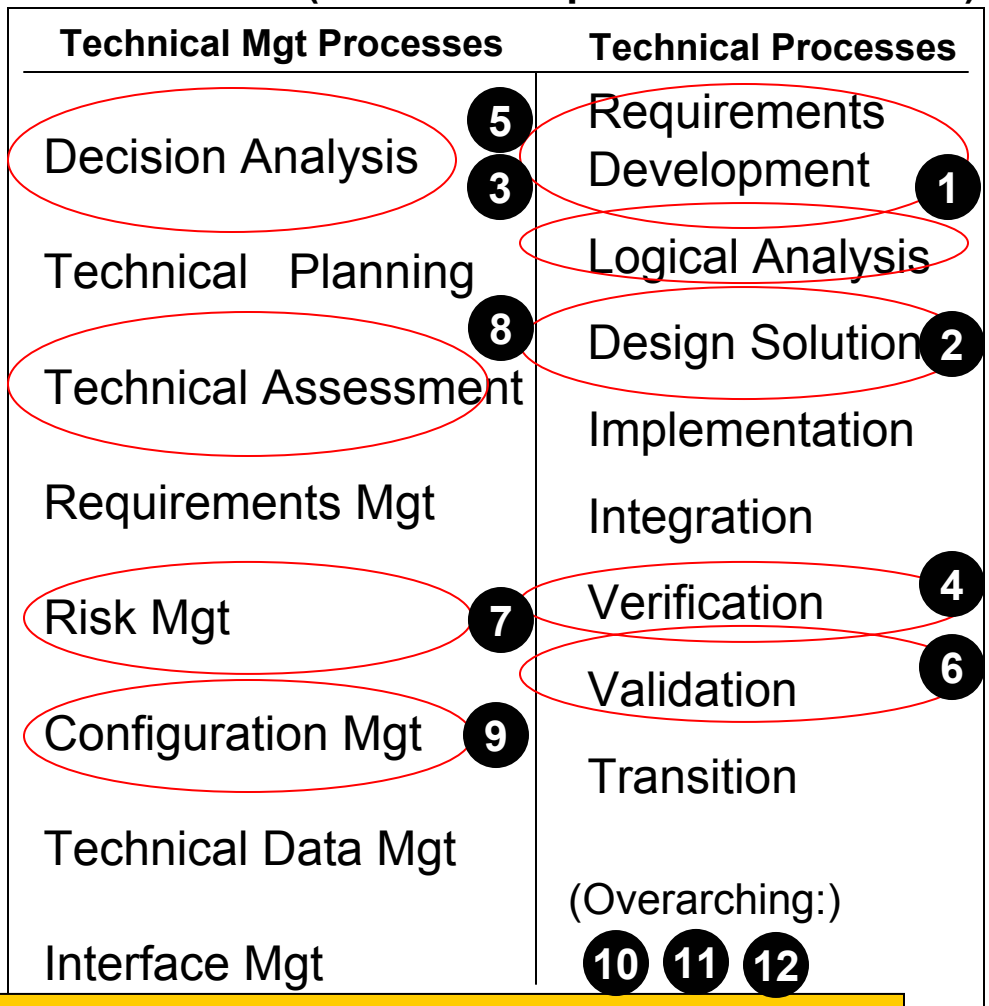
EID Core Members

- OSD
  - Ken Hong Fong, OUSD(AT&L) DS/SE AS
  - Chuck Johnson, CTR, OUSD(AT&L) DS/SE AS (Decisive Analytics)
  - David Wheeler, CTR, OASD(NII) (IDA)
- Department of the Army
  - Jim Linnehan, ASA(ALT)
- Department of the Navy
  - Brenda Zetterval, ASN(RDA) CHENG
  - Jim Dietz, CTR, ASN(RDA) Cheng (MITRE)
- Department of the Air Force
  - Ernesto Gonzalez, SAF AQR
- NSA
  - Janet Oren
  - Steve Lafontain
- MDA
  - Abe Bushra
  - Michael Smith
  - Margaret Powell

Engineering in Depth

- Top level definition:
  - An analytical approach of focusing SE to the issues of SwA
  - Like defense-in-depth seeks to implement multiple layers of strength, by building SwA into the product instead of adding it on
- Top level approach:
  - Work with industry to define SE enhancements
- Derive reasonable and cost effective enhancements
  - Insert agreed enhancements into DoD acquisition policies & guidance

SE Processes (Defense Acquisition Guidebook)



What Key SE processes can we enhance to achieve the best effects?

= potential EID SE process intersects

Engineering-in-Depth Mechanisms Defined

1. **Develop a common core set of tailorable SwA requirements & metrics**
2. **Develop an approach for performing operational SwA sensitivity analysis**
3. **Develop an approach for identifying SwA driven scenarios for use in Analyses of Alternatives (AOA) and hazard analyses**
4. **Develop candidate SwA test metrics for inputs to Test and Evaluation Master Plan (TEMP) SwA Annexes, to include applicable:**
5. **Define an approach for SwA applicable Modeling and Simulation (M&S)**
6. **Define a mechanism for selective technical "red-team" reviews of key software**
7. **Develop a common core set of SwA threats and vulnerabilities with probability and consequence metrics**
8. **Develop top-level Software and SwA Entry/Exit Criteria for SE Technical review(s)**
9. **Develop an enhanced SwA informed CM process to ensure full life cycle protection**
10. **Examine strategies for providing enhanced DoD SwA Standards leadership and management**
11. **Develop and implement education, training and certification avenues for acquisition participants**
12. **Define a continuous process improvement approach based upon evolving threat assessments through an engineering community sensitized to SwA**

Workshop Task: NDIA Problem Statement

- This workshop
  - Leverage NDIA strengths
  - Provide “Industry” input for how best to achieve EID elements
  - Honest look at 12 proposed EID elements to discuss whether to:
    - Add
    - Subtract
    - Amend
    - Replace
  - Call for white-papers in topics of interest
    - Government purpose rights required

Industry Discussions for Conducting SwA Sensitivity Analysis

- What functional statements in the SOW for vendors best enable optimal vendor solutions
  - How do we say it in such a way that you can respond most effectively?
- How do we execute this at different phases in the product lifecycle?
- How do we address n-tiered subcontracting, including COTS, where specific product mixes change significantly
- How do we measure and manage subsequent trade decisions through the product lifecycle

Industry Discussions for Conducting SwA Requirements

- What functional statements in OSD Guidance for SwA requirements best enable optimal vendor solutions
  - How do we say it in such a way that you can respond most effectively?
- What guidance in 5000 and DAG will allow developers to make credible trade decisions at different phases in the product lifecycle?
- What JCIDS and/or 6212, etc., language will provide effective guidance for deriving measurable, effective and system specific requirements for SwA
- How do we measure and manage subsequent trade decisions through the product lifecycle

Industry Discussions for Conducting SwA Test

- What functional statements in the SOW for vendors, OSD test guidance best enable optimal vendor solutions
  - How do we say it in such a way that you can respond most effectively?
- Where can we find, or who can we engage to get to overarching SwA test measures to guide DT, OT to ensure consistency across the department?
- What 5000/DAG, etc., guidance will best ensure that TEMP and TEPs provide sufficient guidance for devising/deriving test criteria for SwA
- What are effective, yet reasonable, exit criteria for SwA

Industry Discussions for ID and Assessment of SwA Hazards

- What functional statements in the SOW for vendors and in OSD guidance best enable optimal vendor solutions
  - How do we say it in such a way that you can respond most effectively?
- How do we get to an overarching set of SwA hazards that can be derived by developers?
- How do we address n-tiered subcontracting, including COTS, where specific product mixes change significantly
- How do we measure and manage subsequent trade decisions, including economic considerations, through the product lifecycle

Standards Metrics & Models for SwA Discussion

The SwA knowledge environment

- Standards – many IA/IT security focused standards but none directly focused on all of SwA
  - SwA per se, is new ground
- Guidance – much IA/IT assurance related guidance
  - FIPS pubs, IATF, Academic and industry literature
- Processes – many processes in DoD that support key SwA elements, but none directly address all of SwA
  - DITSCAP for system security C&A
  - NIAP/Common Criteria evaluation to search for unintentional vulnerabilities in COTS components
  - DoD IA to address IS security controls to protect and defend information confidentiality, integrity, availability, authentication and non-repudiation

SwA Way Ahead Ground Rules

- Should not duplicate or contradict, but leverage other policies, processes, practices, tools and metrics:
  - Supporting Standards
  - NIAP/ISO 15408 (Common Criteria);
  - DITSCAP C&A process;
  - DoD Information Assurance (IA);
  - CMM/CMMI/SSE-CMM;
  - Information System Security Engineering (ISSE); and
  - Information Assurance Technical Framework (IATF)
  - Trusted Software Development Methodology (TSDM)
  - Others…
- Barriers:
  - No agreement on what constitutes SwA
  - Other processes on fringe

Much past work around idea of Software Assurance, but what do we really know?

Back-ups

How Does Assurance Fit in the System and Software Life Cycles?

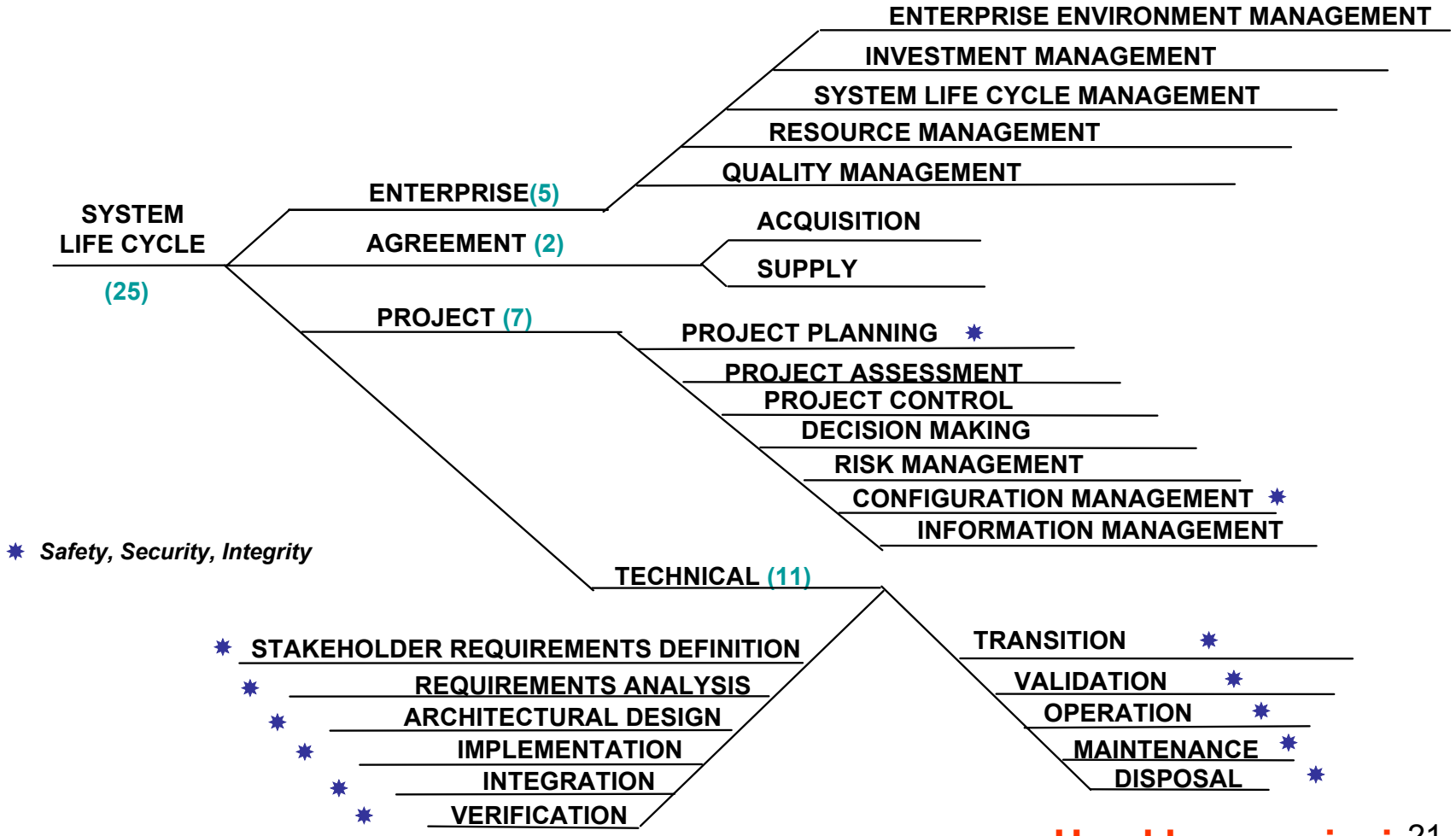
Used by permission

Life Cycle Process Framework Standards

- System Life Cycle
  - **ISO/IEC 15288**, *Systems engineering — System life cycle processes*
- Software Life Cycle
  - **ISO/IEC 12207**, *Standard for Information Technology —Software life cycle processes*
  - **IEEE/EIA 12207.0**, *Industry Implementation of International Standard ISO/IEC12207:1995 — (ISO/IEC 12207) Standard for Information Technology —Software life cycle processes*
    - **IEEE/EIA 12207.1**, *Industry Implementation of International Standard ISO/IEC12207:1995 — (ISO/IEC 12207) Standard for Information Technology —Software life cycle processes – Life Cycle Data*
    - **IEEE/EIA 12207.2**, *Industry Implementation of International Standard ISO/IEC12207:1995 — (ISO/IEC 12207) Standard for Information Technology —Software life cycle processes – Implementation considerations*

Used by permission

Assurance in the ISO/IEC 15288 System Life Cycle Process Framework



Used by permission

ISO/IEC 15288 – System Assurance Objectives

Stakeholder Requirements Definition Process

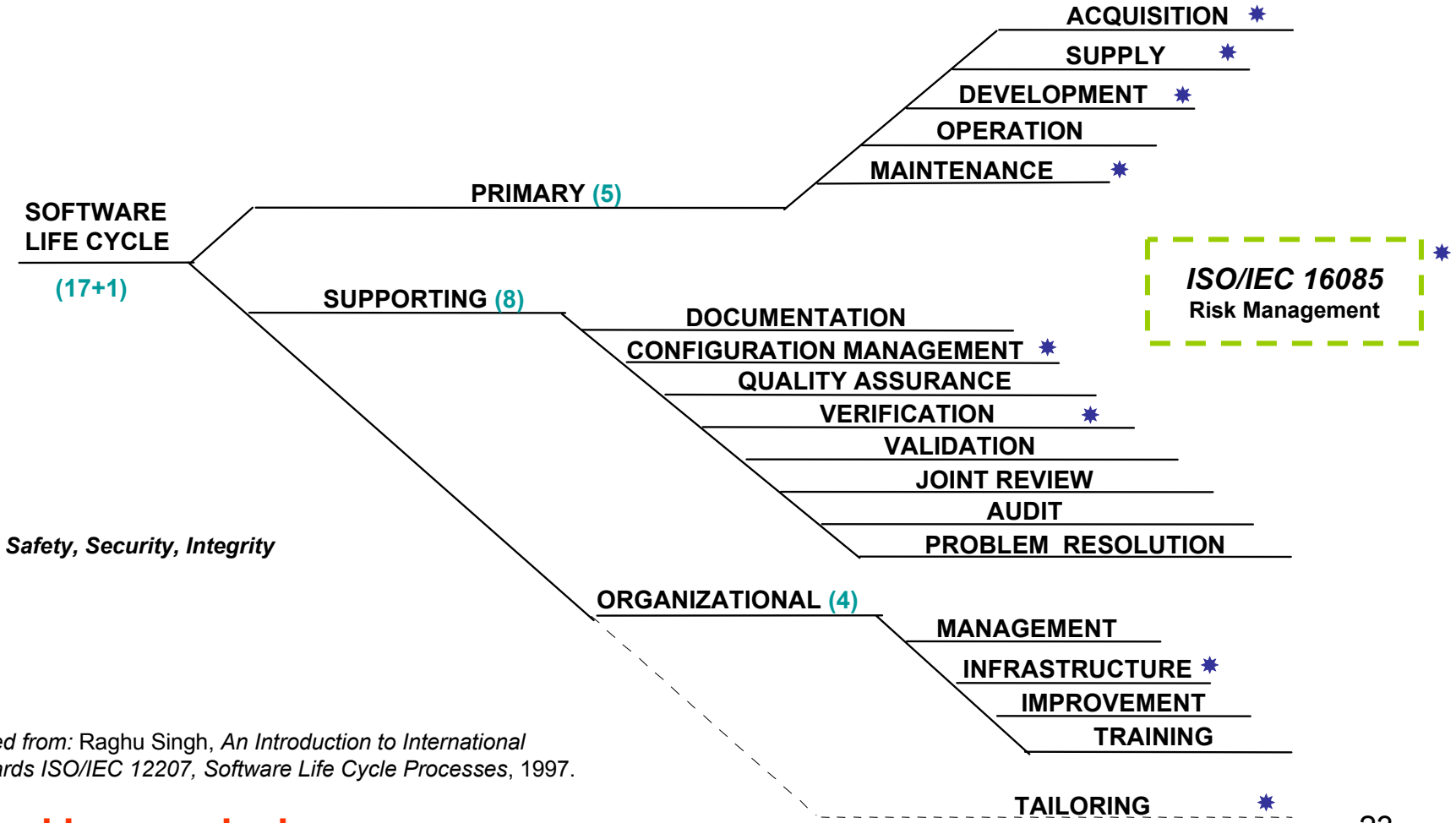
- ***Specify*** health, ***safety, security***, environment and other ***stakeholder requirements and functions*** that relate to ***critical qualities; Identify safety and security risk.***

Requirements Analysis Process

- ***Specify system requirements and functions*** that relate to critical qualities, such as health, ***safety, security***, reliability, availability and supportability.

Used by permission

Assurance in the IEEE/EIA 12207 Software Life Cycle Process Framework



Adapted from: Raghu Singh, *An Introduction to International Standards ISO/IEC 12207, Software Life Cycle Processes*, 1997.

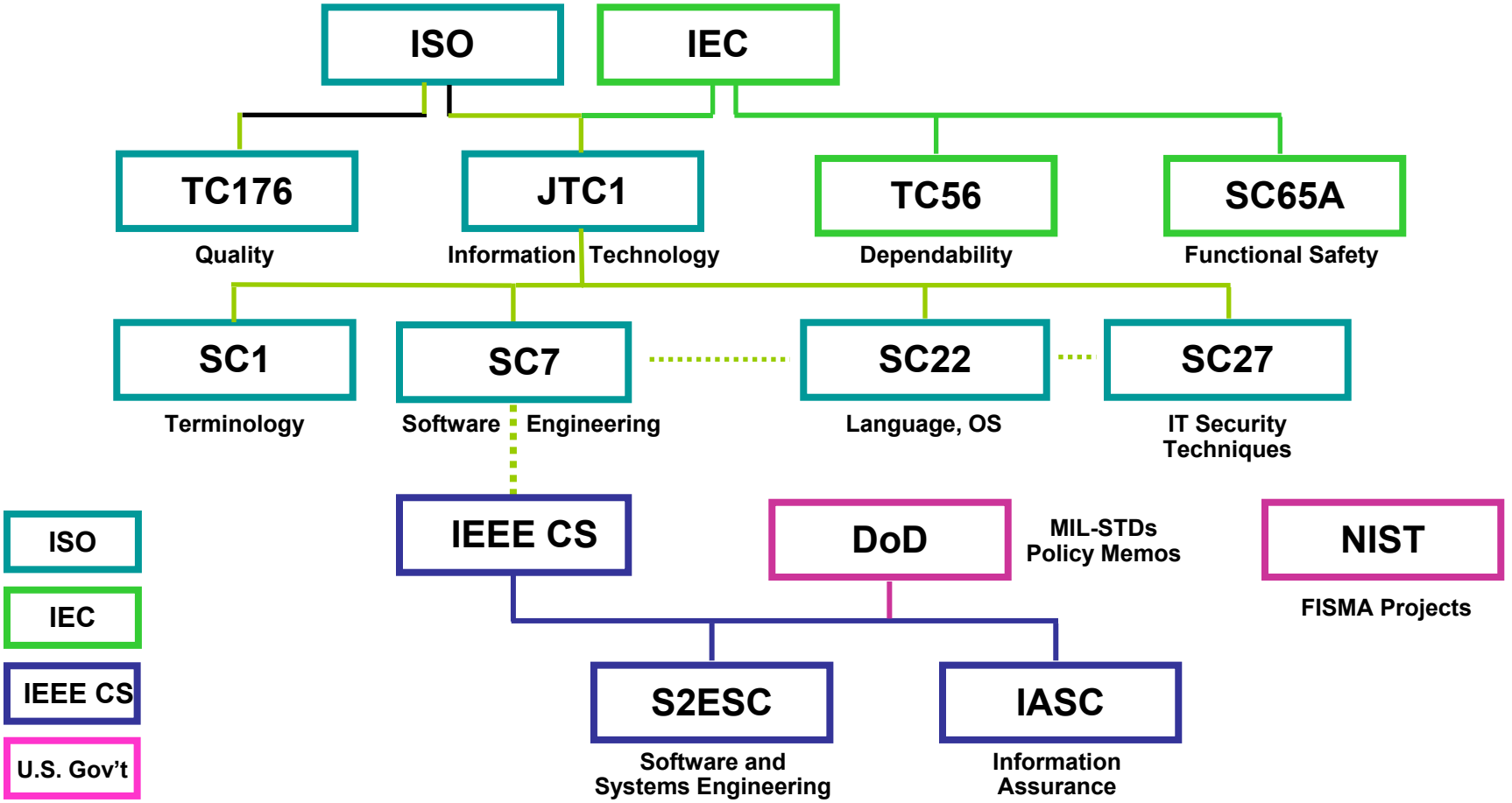
Used by permission

IEEE/EIA 12207 – Software Assurance Objectives

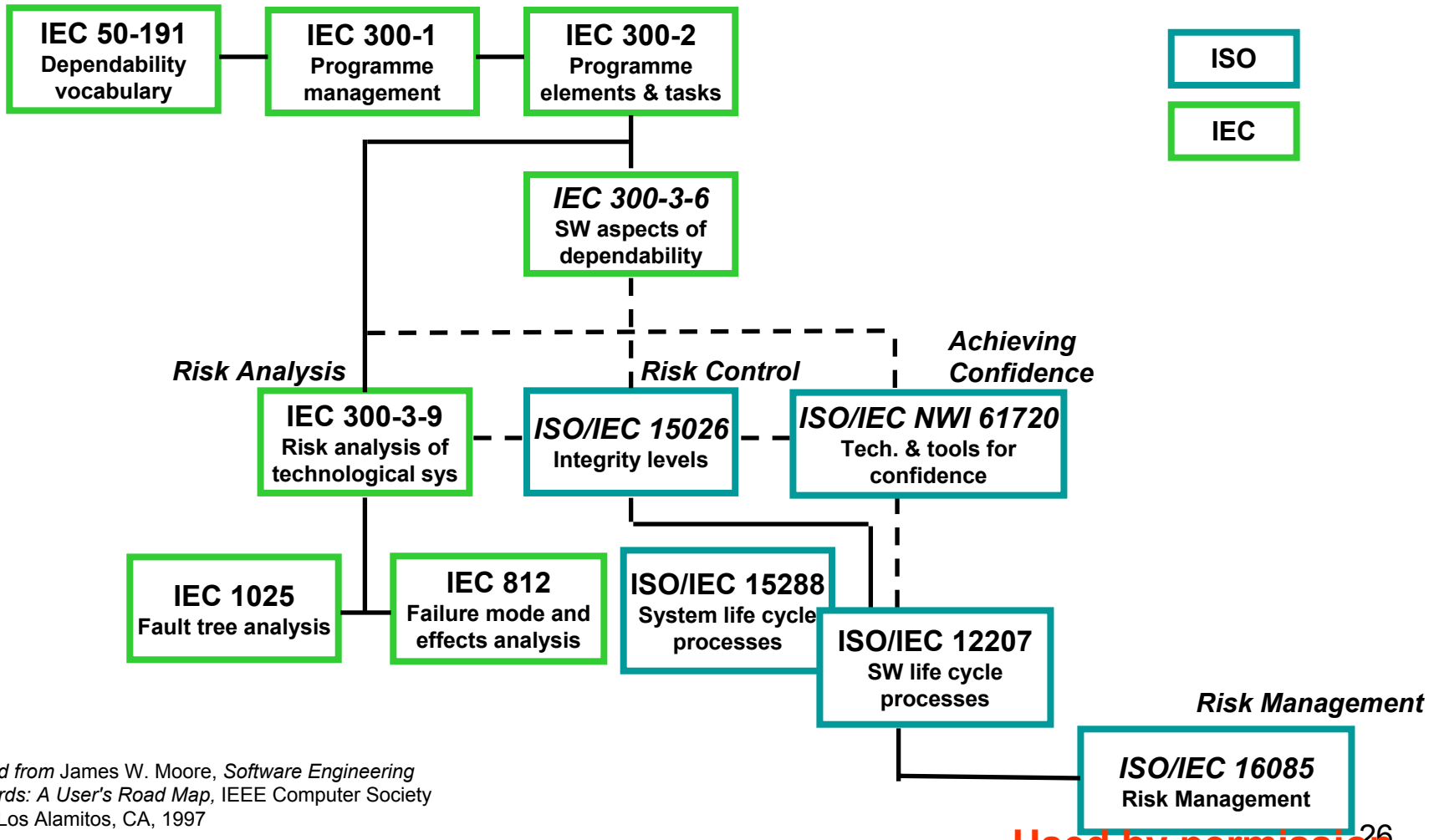
Development Process

- The developer shall ***establish and document software requirements***, including quality characteristics specifications ***such as safety specifications***, including those related to methods of operation and maintenance, environmental influences, and personnel injury; ***and security specifications***, including those related to compromise of sensitive information

Standards Organizations Supporting Assurance



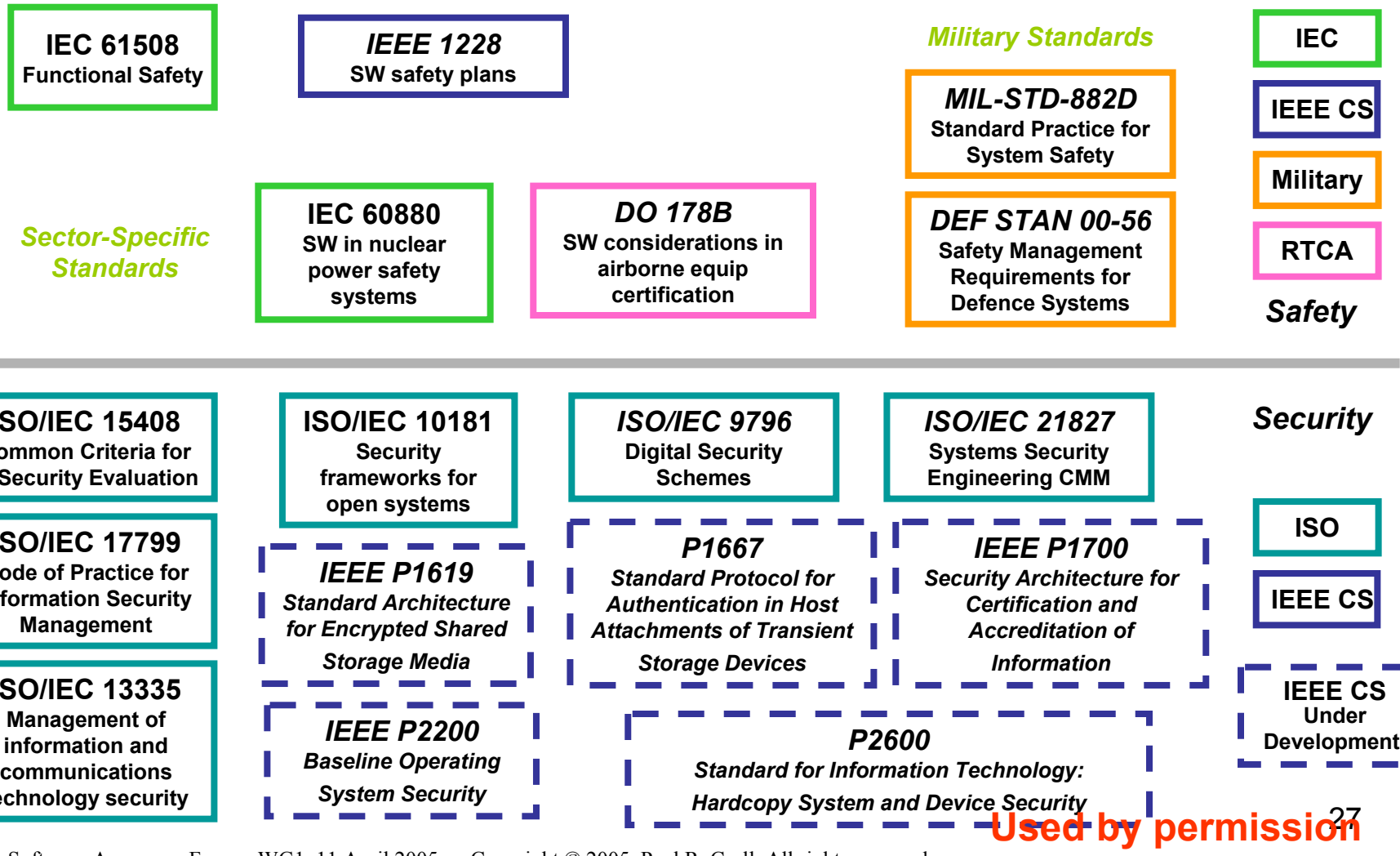
Dependability Standards



Adapted from James W. Moore, *Software Engineering Standards: A User's Road Map,* IEEE Computer Society Press, Los Alamitos, CA, 1997

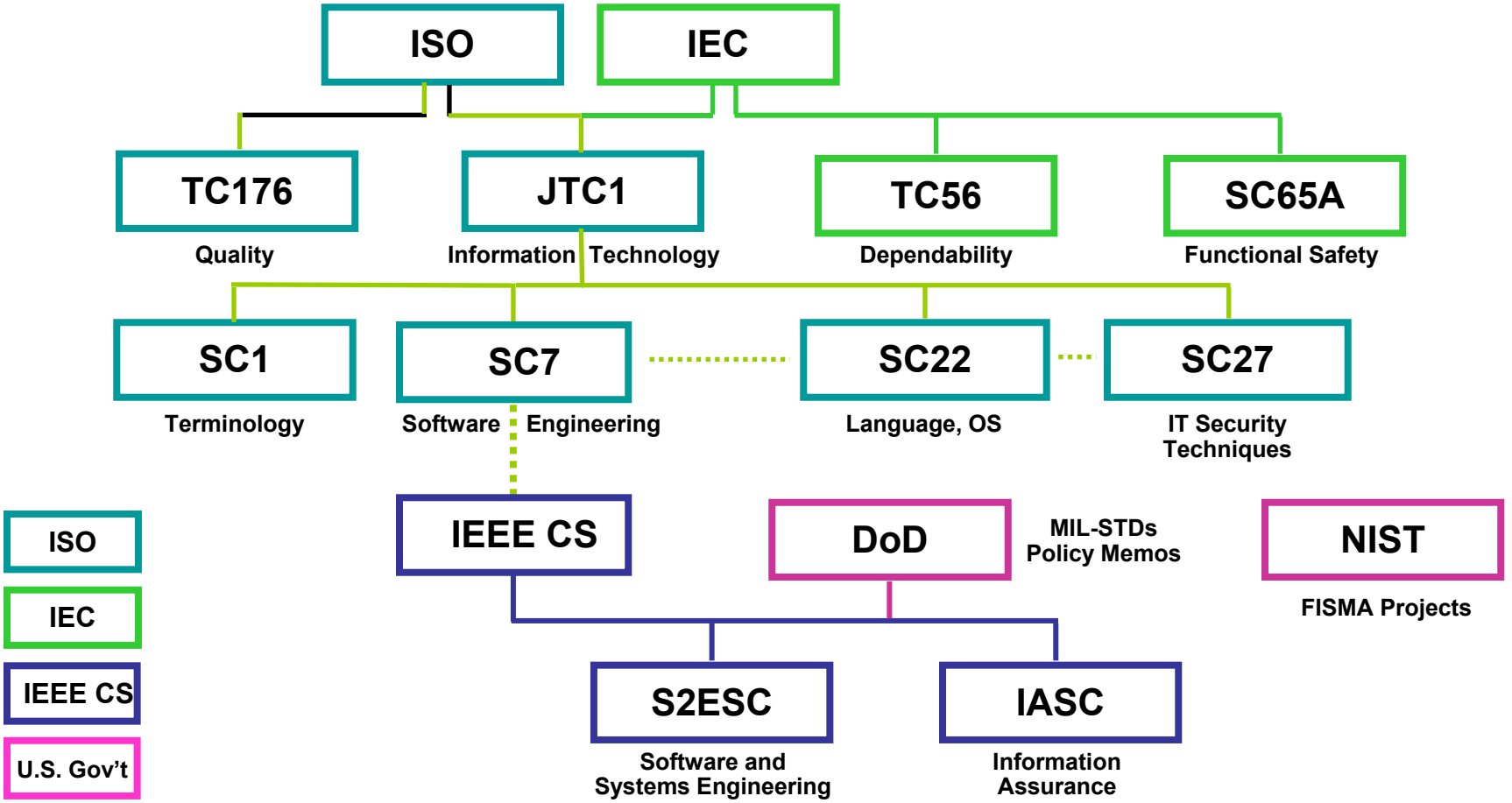
Used by permission

Safety and Security Standar



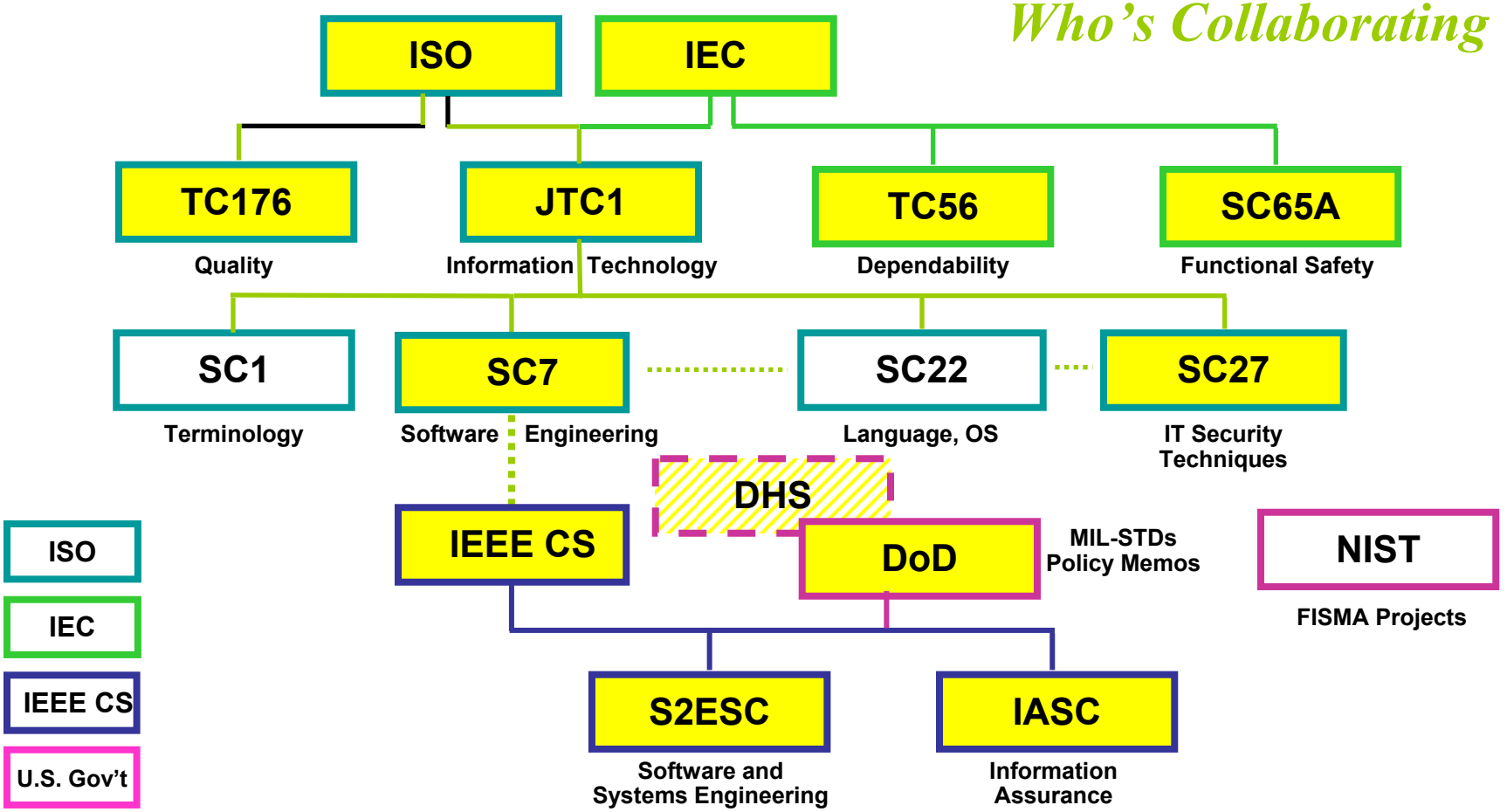
Used by permission

Harmonization Efforts Impacting Systems and Software Assurance



Used by permission

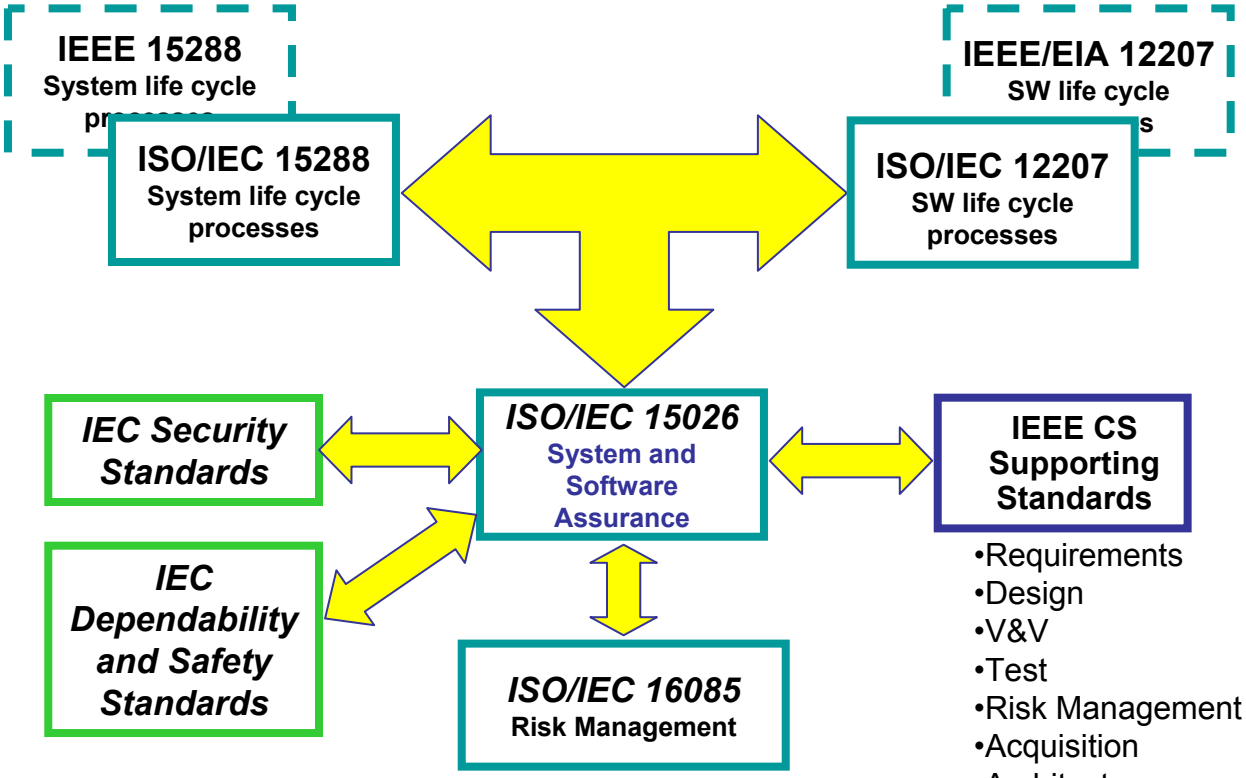
Harmonization Efforts Impacting Systems and Software Assurance



Used by permission

Harmonization Efforts Impacting Systems and Software Assurance

What's Being Harmonized



- Requirements
- Design
- V&V
- Test
- Risk Management
- Acquisition
- Architecture
-
-

Used by permission

A Closer Look at Three Standards Development Organizations Working Closely With the Homeland Security and Defense Communities

Used by permission

ISO/IEC JTC1/SC7 WG9 – System and Software Assurance

- Terms of Reference

  Development of standards and technical reports for system and software assurance. System and software assurance addresses management of risk and assurance of safety, security, and dependability within the context of system and software life cycles

- Liaisons: IEC TC56, SC65A, JTC1/SC27
- Convener: Paul Croll, CSC

Used by permission

IEEE Software and Systems Engineering Standards Committee (S2ESC)

- Terms of Reference:

  Standardization of processes, products, resources, notations, methods, nomenclatures, and techniques for the engineering of software and systems dependent on software

- Liaisons: ISO/IEC/JTC1/SC7, DoD, DOE, DHS, NASA, NRC, SEI, ASQ, IEEE IASC
- Chair, Paul Croll, CSC

Used by permission

IEEE Information Assurance Standards Committee (IASC)

- Terms of Reference:

  Information Technologies and their inter-dependencies that affect/effect timely delivery of information subject to well-known quality of service requirements: authentication/ authorization, confidentiality, data integrity, and non-repudiation (auditing)
- Liaisons: (Planned) IEEE SSSC, IEEE S2ESC, Defense Standardization Program, Department of Homeland Security, NIAP, NIST, NSA
- Chair: Jack Cole, ARL

Used by permission

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

For IEEE Standards:

http://computer.org/standards/sesc/
http://ieeeia.org/iasc/
http://computer.org/cspress/CATALOG/st01110.htm

For ISO/IEC Standards:

http://saturne.info.uqam.ca/Labo_Recherche/Lrgl/sc7/

Used by permission

Systems Engineering Challenge - Metrics

- Key part of Systems Engineering is ensuring requirements are right
- Requirements must be sufficient, valid, well formed, measurable and ultimately testable
- Good requirements are essential for designing and producing fully suitable and effective systems
  - Requirements → Performance Specifications → System Specifications → Allocated Baseline
- Good requirements are essential for devising valid and sufficient test and acceptance criteria
  - Ensures end performance meets user needs and expectations
- Goal: a Software Assurance Key Performance Parameter/s (KPP)

KPP Definition

"Those minimum attributes or characteristics considered most essential for an effective…capability."

-- Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3170

Discussions