SAFE SOFTWARE FOR SPACE APPLICATIONS: BUILDING ON THE DO-178 EXPERIENCE

Cheryl A. Dorsey
Digital Flight / Solutions
cadorsey@df-solutions.com

Presentation Outline

* DO-178 Overview
* What vs. How Standard
* System Safety Process (begins prior to software development)
* Software Tie to System Safety
* Requirements
* Traceability
* Standards
* Verification
* Quality Assurance
* Good Practices
* Conclusion

DO-178 Overview Presentation Context

* DO-178
  * International Standard for Assurance of Software Used in Civil Airborne Systems
  * Also used in other Mission Critical Industries
* Current Status
  * Latest Version is DO-178C (2012)
  * Same Overall Concept as DO-178B (fixes mistakes, adds tribal knowledge)
  * Four New Supplements (Tool Qualification, Formal Methods, OO, Model Based Development)
* Presentation Context
  * Relevance to Space Community
  * What v. How Standard
  * Strengths and Weaknesses
  * Best Practices

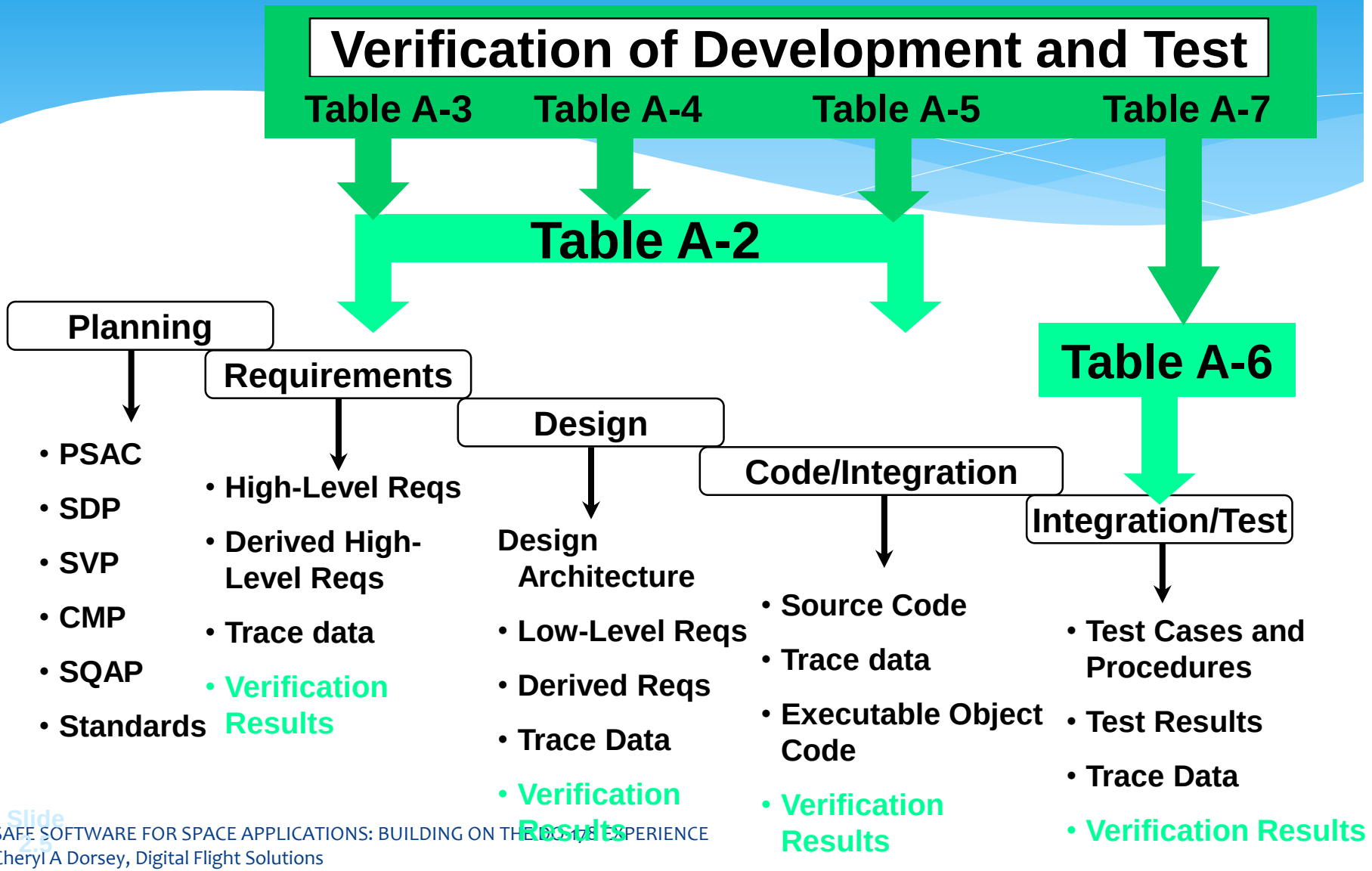
What vs. How Standard

* Objective Based Approach
* Qualitative
* Requires some "tribal knowledge"

Objectives and Reference

	Objective		SW Level				Output		Control Category by SW level			
	Description	Ref	A	B	C	D	Description	Ref	A	B	C	D
1	Test procedures are correct.	6.3.6 b	●	○	○		Verification Results	11.14	②	②	②	

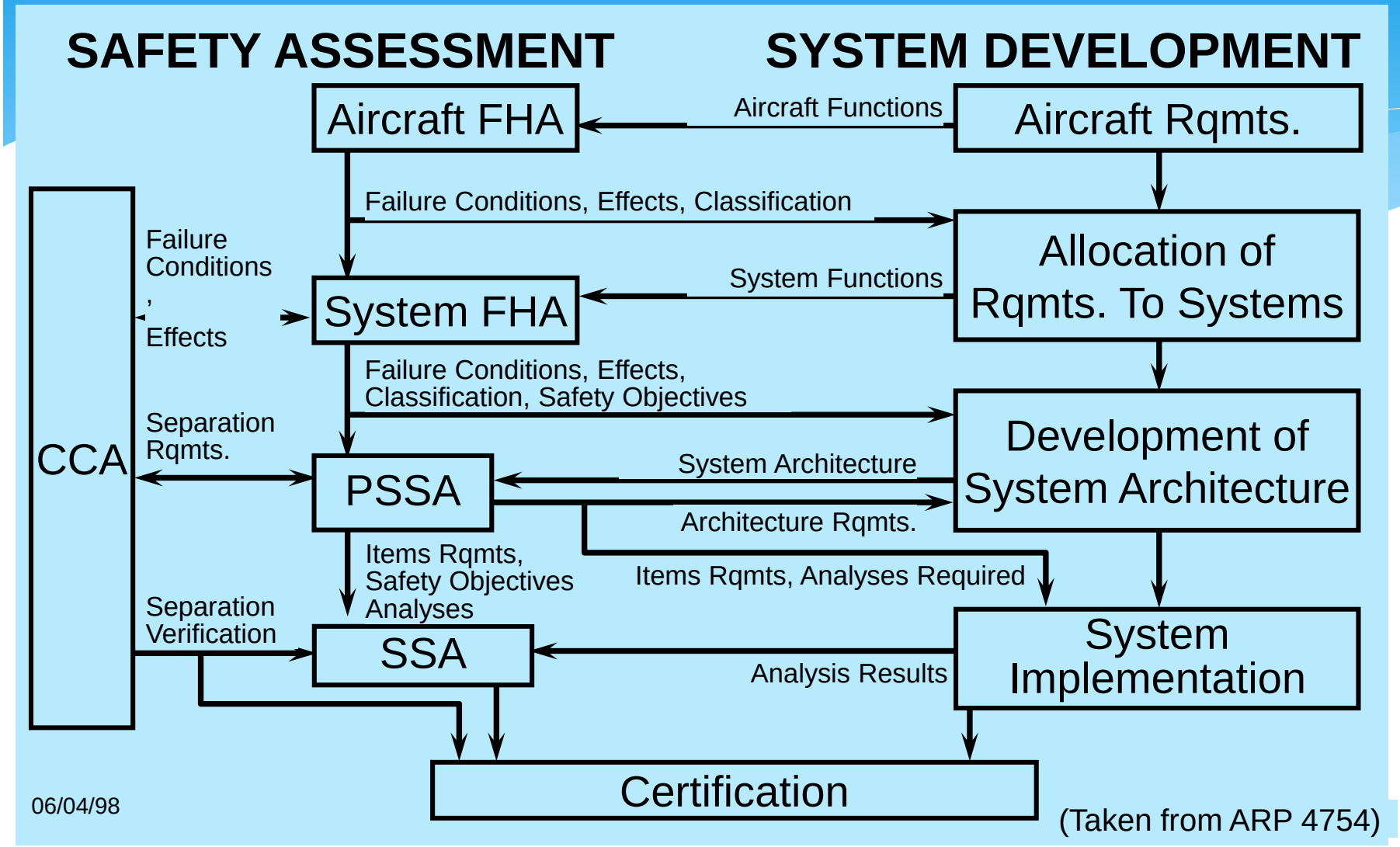
Four Annex Tables for Verification of Development and Test Processes



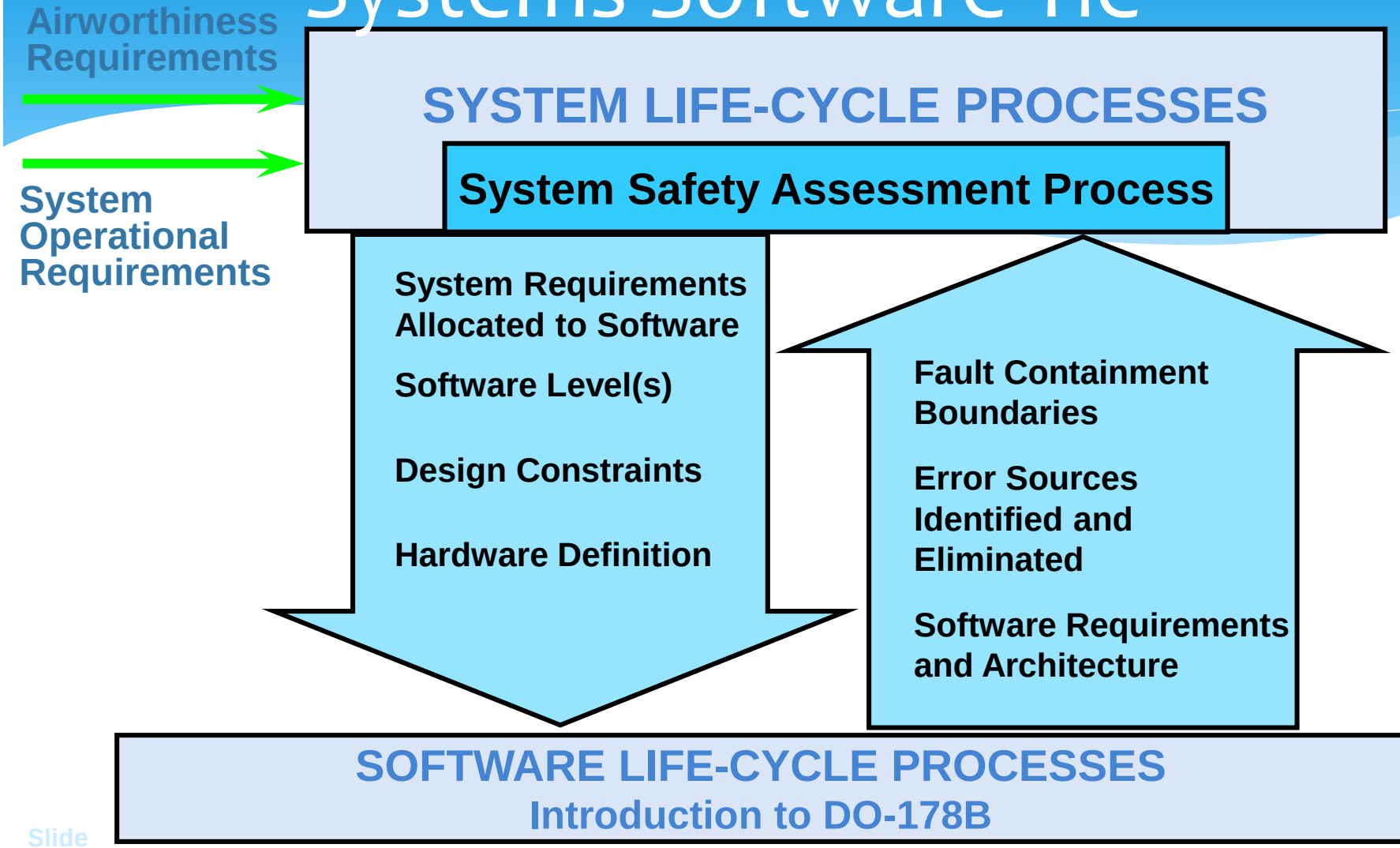
An Example of What Taken From Annex A Table 3

* DO-178 attributes of requirements:
  * High level requirements conform to system requirements
  * High level requirements are accurate and consistent
  * High level requirements are compatible with target computer
  * High Level Requirements are Verifiable
  * High level requirements conform to standards
  * High level requirements are traceable to system requirements
  * Algorithms are accurate

System Safety Process



Systems Software Tie



Taken from DO-178B

Safety Tie To Software

* DO-178 References System and Safety Standard (ARP4754)
  * Section 2 of DO-178 - Informative Section (no objectives)
  * Safety is really a systems property in civil airborne
* DO-178b "Safety" Processes
  * Assumes "safe" requirements as an entry point
  * Extensive Verification (assures requirements are met)
  * Safety Review of Derived Requirements (may not be enough)
* Best Practices
  * Safety Review of All Requirements (criticality)

Requirements

* Use of non-standard requirements terminology
  * High level requirements vs. Low level requirements
  * Derived requirements definition and understanding
* Leads to problematic non-standard practices
  * Combined low and high level requirements
  * Derived requirements not tagged as derived
* Pseudo-code as low-level requirements
  * Implementation not requirements/testability
  * Maintenance issue after original development

Requirements

* Best practices for requirements
  * Assure clear criteria is established for DO-178 requirement review
  * Independently develop requirements based tests in parallel to assure the requirements are testable
  * Provide clear definition and criteria for derived requirements

Traceability

* Traceability is a clear strength of DO-178
  * One way trace upward to system requirements allocated to sw
  * Two way trace between high level requirements and low level requirements
  * Two way trace between low-level and code
  * Trace between tests and requirements
* Forward trace assures all requirements are implemented
* Backward trace assures nothing but requirements implemented (no unintended function on the aircraft)

Traceability

* Review of requirements traceability
  * After each phase during verification
  * Again during requirements coverage analysis (requirement completely tested (normal and robust), structure covered
* Best practices
  * Clear guidance (review criteria) for tracing
  * Nothing but the requirements are implemented (unless derived)
  * Independent trace review in each direction and compare the results for high criticality

Standards

* Three development standards
  * Requirements, Design, Code
* Standards in DO-178 do not assure good practices
  * Often minimal and add little toward design assurance
* Best practice
  * Use a strong standard like (MISRA or a subset of it) for DAL A and B
  * Although not required by DO-178, use a testing standard to assure all requirements are fully tested (normal and robustly) with observable results (you don't want to find problems at the certification reviews)

Verification

* Reviews
  * Requirements review
  * Design Review (low level requirements and architecture)
  * Code Review
  * Test Review
* Testing
  * Normal and robustness
  * Structural Coverage of the code via requirements based testing
  * MCDC (catastrophic), Decision (hazardous), statement (major)

Verification

* Analyses
  * Data Coupling
  * Control Coupling
  * Requirements Coverage
  * Stack Depth
  * Memory Margin
  * Worst Case Timing
* Analyses lack clear guidance and objectives, therefore often do not meet the intent

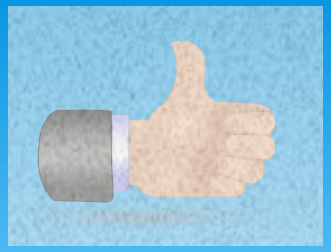
Verification

* Verification is a strength of DO-178
* DO-178 is an assurance standard and verification intensive (measuring stick put over development).
* When done correctly, assurance is gained through a series of reviews, analysis and tests
* DO-178 could benefit in clearer guidance with respect to:
  * Review criteria
  * Clear objective criteria for each analysis
  * Strong criteria for robustness testing commensurate with safety classification

Quality Assurance

* DO-178 Quality Assurance is really process assurance
  * Main concept - say what you do (planning), do what you say (follow the plans), prove it (records)
  * If Quality is not built into the process, than quality is not assured
  * Quality is often not involved at key points as prescribed by DO-178 transition criteria (between each life cycle phase)
  * Quality assurance often does not review the CM of development and verification artifacts
  * To work QA should be fully engaged throughout
* DO-178 does require dated records for each QA activity (check the checker)

Good Practices in the Airborne Community



* Required four certification reviews called SOIs
  * Planning, development, verification, final
* Support for reviews found in FAA Order 8110.49
* Good news FAA Software Job Aid provides a more detailed set of evaluation criteria at the SOI audits to mitigate weaknesses of DO-178
* Bad news is many companies do not know of this or use it during their development.

Conclusions

* Strength of DO-178 is when understood and implemented correctly provides an excellent mechanism to assure software is bug free
* To be effective it requires good knowledge of software engineering and process
* Strength and weakness is that it is not prescriptive
  * Not tied to any specific lifecycle or methodology
  * Requires a key knowledge of “good” SW Engineering processes and implementation
* Could benefit by clear examples and more “How” guidance

Conclusions (con't)

* Needs a stronger tie to systems and safety
  * architectural mitigations (e.g. monitors) are implemented correctly and tested robustly
  * Stronger tie, with feedback to systems and safety when requirements are not understood, missing, or too weak to implement
* ECSS has a safety process built in to the software process (this would benefit DO-178)