

Merging Safety and Assurance: The Process of Dual Certification for FAA and the Common Criteria

Jim Alves-Foss, Bob Rinker, Carol Taylor
University of Idaho
Center for Secure and Dependable Systems

<http://www.csds.uidaho.edu/~jimaf>

Comparison/Merger Goals

- Provide a mapping from FAA guidelines into Common Criteria (CC)
 - Detailed mapping of supporting sections of RTCA DO-178B into CC assurance criteria
 - Summary of “gaps” in the mapping
- Why compare and merge?
 - Vendors may wish to apply dual use embedded systems components/controllers
 - There may exist security related failure conditions of avionic components

Presentation Contents

- Introduction
 - DO-178B
 - FAA Failure Levels DO-178B
 - Common Criteria
 - Evaluation Assurance Levels EAL's
- High-Level Comparison DO-178B Processes to CC Classes
- Non-mapping CC Classes
- Considerations

Introduction to DO-178B

- Requirements for software development are divided into several main processes within DO-178B.
 - Software Planning
 - Software Development
 - Software Verification
 - Software Configuration Management
 - Software Quality Assurance.

Introduction to DO-178B

- Software Levels in DO-178B
 - DO-178B describes certification requirements relating to five software levels.
 - Certification only occurs at the system level –aircraft, engines or propellers.. However, components can be “approved” to meet predefined public requirements (TSO’s). A TSO may not guarantee that a component meets the integration requirements in the system.
 - The DO-178B “Plan for Software Aspects of Certification” is the document used by certifying authority to guide evaluation of rigor of software lifecycle.
 - Software level is correlated to the contribution of the software to the FAA failure conditions in aircraft. The five levels range from
 - Level A- the most failure critical to
 - Level E - no effect on aircraft safety.

FAA Failure Conditions

- **Level A (Catastrophic):** Failure conditions that prevent continued safe flight and landing.
- **Level B (Hazardous/Severe-Major):** Failure conditions which would reduce the capability of the aircraft or the capability of the flight crew to cope with adverse operating conditions to the extent that there would be:
 1. a large reduction in safety margins or functional capabilities
 2. physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or
 3. adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants

FAA Failure Conditions

- ***Level C (Major)***: Failure conditions which would reduce the capability of the aircraft or the capability of the flight crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or function capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.
- ***Level D (Minor)***: Failure conditions which would not significantly reduce aircraft safety, and which would involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins, or functional capabilities, a slight increase in crew workload, such as, routine flight plan changes, or some inconvenience to occupants.
- ***Level E (No Effect)***: Failure conditions which do not affect the operational capability of the aircraft or increase crew workload.

Introduction to DO-178B

- The differences between the requirements for certification at the various levels focus primarily on two issues:
 - Software engineering processes that generate data/documents required to prove compliance with development standards and processes managing that data including configuration control.
 - Independent vs. non-independent assessment of compliance with DO-178B requirements.

Introduction to DO-178B

- There are two control processes under which data can be classified:

- Control Category 1 (CC1) and
- Control Category 2 (CC2).

CC2 is a subset of CC1 requirements and is less stringent in terms of software life cycle data management.

Features of these control processes include requirements for baselines, traceability, change control, change review, unauthorized changes protection, release and data retention among others.

Introduction to DO-178B

- Second area of difference between failure levels concerns independent assessment of compliance with process requirements
- The three levels of assessment include:
 - Objective should be satisfied with independence.
 - Objective should be satisfied
 - Satisfaction of the objective is at applicant's discretion

Introduction to DO-178B

- Software Verification
 - This is a crucial aspect of DO-178B. It effectively boils down to two critical issues:
 - *Structural Coverage Testing*: Testing of the generated software (typically at the intermediate or object code level) must be complete. (ex. If (a | b | c) then s0 else s1) – 100% structural coverage
 - *Traceability*: Evidence is required for systematic processes that ensure each requirement has been incorporated and verified. Evidence must show all levels of requirements must be traceable up to all of their roots and each must be fully tested. Evidence must be reversible (tracing tests up to requirements) – 100% requirement coverage

Introduction to CC

- The Common Criteria (CC)
 - Provides a framework for developing a set of security requirements for products.
 - First part provides for functional requirements. These can be combined into a template for a class of products, a protection profile (PP). The PP must be consistent and complete.
 - Second part provides for assurance (discussed later)
 - Vendor will instantiate a PP, or a PP-like document called the security target (ST). Assurance maps processes, data and documentation to this target.

Introduction to CC

- The CC organizes assurance requirements into *classes* which identifies the general topic covered by that class.
 - *ACM* – *Configuration Management*
 - *ADO* – *Delivery and Operation*
 - *ADV* – *Development*
 - *AGD* – *Guidance Documents*
 - *ALC* – *Life Cycle Support*
 - *ATE* – *Tests*
 - *AVA* – *Vulnerability Assessment*

Introduction to CC - EALS

- Security requirements for software and systems can vary depending on the purpose of the system.
- CC offers different levels of assurance - Evaluation Assurance Levels (EALS).
 - EALS range from EAL1 - the lowest level of assurance to EAL7 - the highest security assurance level.

Introduction to CC - EALS

- EALS are predefined assurance packages that define a consistent set of assurance requirements.
- EALS form an ordered set that is the predefined assurance scale of the CC.
- EALS are hierarchically ordered in that each EAL represents more assurance than all lower EALS.
- An increase in assurance is achieved by substituting a higher assurance component from the same family or adding a component from other families.

Introduction to CC - EALS

- **EAL1 – functionally tested**
- **EAL2 – structurally tested**
- **EAL3 – methodically tested and checked**
- **EAL4 – methodically designed, tested and reviewed**
- **EAL5 – semi formally designed and tested**
- **EAL6 – semi formally verified design and tested**
- **EAL7 – formally verified design and tested**

Introduction to CC - EALS

- *EAL2* represents an increase in security over EAL1 by requiring developer testing, a vulnerability analysis and independent testing based upon a more detailed target of evaluation (TOE) specification.
- *EAL3* is an increase in assurance over EAL2 by requiring more complete testing coverage of the security functions and mechanisms and/or procedures that provide some confirmation that the TOE will not be tampered with during development.

Introduction to CC - EALS

- *EAL4* is an increase in assurance over EAL3 because it requires more design description, a subset of the implementation and improved mechanisms that provide confidence that the TOE will not be tampered with during development or delivery.
- *EAL5* offers increased assurance over EAL4 in that a semiformal design description is required over the entire implementation, more structured architecture, covert channel analysis, and improved mechanisms and or procedures that provide confidence that the TOE will not be tampered with during development.

Introduction to CC - EALS

- *EAL6* offers increased assurance over EAL5 by requiring semiformal design descriptions, a structured representation of the implementation which is more analyzable, system covert channel identification and improved configuration management and development environment controls
- *EAL7* offers more assurance than EAL6 by requiring comprehensive analysis using formal representations and formal correspondence plus comprehensive testing.

High-Level Comparison - DO-178B Processes to CC Classes

<u>CC Assurance Class</u>	<u>DO-178B Area</u>
• ACM Configuration Management	Software Configuration Management
• ADO Deliver and Operation	<i>(No Correspondence) – elsewhere</i>
• ADV Development	Software Development Process
• AGD Guidance Documents	<i>(No Correspondence) - elsewhere</i>
• ALC Life Cycle Support	Software Planning Process
• ATE Tests	Software Verification Process
• AVE Vulnerability Assessment	<i>(No Correspondence) – testing?</i>

Non-mapping CC Classes

- Several CC classes dealing only with security issues could not be mapped to any DO-178B processes.
- These include
 - *AGD* – *Guidance Documents*
 - *ADO* – *Delivery and Operation*
 - *AVA* – *Vulnerability Assessment CC*

Non-mapping CC Classes

- **Guidance documents** refer to documents specifically related to the security aspects of administration and operation of the software.
 - DO-178B does not address documentation relating to just the security aspects of system operation. Nor does it address user or management documentation directly. This is typically the function of the integration requirements for the system.

Non-mapping CC-classes

- **The Delivery and Operation** class seeks to insure that the software was delivered without interference or tampering and that the software is installed and initially started securely and correctly.
 - Again, no corresponding DO-178B process components addressed the security aspects of tampering and initial start-up. This is typically a requirement of integration; although FAA looks at safety, not necessarily security.

Non-mapping CC Classes

- **AVA-Vulnerability Assessment**
 - Vulnerability Assessment deals specifically with covert channel analysis, deliberate misuse and other security function assessments that are absent in DO-178B.
 - DO-178B requires structural coverage testing and traceability; avoiding inclusion of unspecified “features”. Does fault tree analysis encompass security vulnerability analysis?
 - Specific security requirements can be added to the product specification, therefore requiring verification.

Considerations ...

- Certain considerations in Mapping CC to DO-178B need to be addressed ...
 - Differences exist between the intended purposes of the two documents which are important to the final outcome of merging requirements from both documents.
 - DO-178B is intended to certify that software used in aircraft is developed with "best known" practices and does not contribute to aircraft safety hazards.
 - Emphasis in DO-178B
 - outlining general policies and procedures to produce safe software in terms of airworthiness requirements
 - produce documentation to substantiate that the development requirements have been met.

Considerations ...

- Consequently, language and content is high-level and abstract
 - A lot of compliance decisions are left up to the developer
- CC higher EALs require more formalism in product requirements, development and analysis.
 - This formalism is not required by DO-178B, but can be added to specific product requirements
 - CC does not explicitly require 100% structural coverage testing only of security functions (ATE_COV), but this would be a bonus to support CC verification.

Considerations ...

CC

- The Common Criteria (CC) is intended to specify security requirements that a system, hardware or software, must satisfy in order to achieve a specific level of assurance.
 - The CC only deals with security functionality of systems and does not address overall development issues except where they affect security.
 - CC can be considered guidelines for a subset of the system.

Considerations ...

Emphasis in CC

- The CC is a much more detailed document in terms of specifying **how** compliance is achieved for an intended product.
 - Each component of each assurance class has specific action elements and evidence of compliance for both developers and evaluators.
 - DO-178B is not nearly as prescriptive. Good practices, and experience with certification authorities are the guidelines.

Considerations ...

- Merging CC security requirements into DO-178B will need to address these differences in detail so that none of the CC functionality is lost.
- Integrating security functionality into the FAA certification process needs to be addressed for the total system being evaluated, not just the software that will be integrated into the aircraft since the CC's scope encompasses entire systems. This involves other FAA regulations.

Considerations ...

- Consequently, a mapping between DO-178B and the CC will only constitute part of the process for achieving certification by the FAA for a high safety level system and by NSA/NIST for a high-level assurance system.

In conclusion...

- the mapping and integration of CC requirements will need to be extended beyond DO-178B to satisfy CC certification
 - Ex. DO-254 is digital hardware equivalent of DO-178B.

Comparison Summary

ACM-Configuration Management	Software Configuration Mng.		Lifecycle Data
	Activities	Data Control	
ACM_AUT	X		Sect. 11.4
ACM_CAP	X		Sect. 11.18
ACM_SCP	X		Sect. 11.4, 11.18
ADO – Delivery and Operation ADO_DEL ADO_IGS	<i>No correspondence with DO-178B</i>		

Comparison Summary

ADV – Development	Soft. Development Process	Life cycle data
	Rqmt. Design Code Integ. Trc.	
ADV_FSP	X	Sect. 11.6, 11.9, 11.14 Sect. 11.7, 11.10, 11.14
ADV_HLD	X X	Sect. 11.14, 11.11
ADV_IMP	X	
ADV_INT		Sect. 11.7 11.10
ADV_LLD	X	Sect. 11.14
ADV_RCR		Sect. 11.9, 11.14
ADV_SPM	X	
AGD – Guidance Documents AGD_ADM AGD_USR	<i>No direct DO-178B correspondence</i>	

Comparison Summary

ALC – Life Cycle Support	Software Planning	Rev	Life Cycle Data
	Activ. Plans. LC/Env	Stand	Plans
ALC_DVS			
ALC_LCD			
ALC_TAT	X	X	X
			Sect. 11.2
ATE – Tests	Software Verification Process		Life Cycle Data
	Activities	Reviews	Testing
ATE_COV		X	X
ATE_DPT		X	X
ATE_FUN			X
ATE_IND			X
			Sect. 11.3, 11.13, 11.14
AVA – Vulnerability Assessment			
AVA_CCA	<i>No direct DO-178B correspondence</i>		
AVA_MSU			
AVA_SOF			
AVA_VLA			