

Merging Safety and Assurance: The Process of Dual Certification for Software

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

Track 5 250-B High Integrity Software
Thursday 1:50-2:30

Keywords: Common Criteria, Software Development, FAA Certification

Abstract

This paper describes a process of dual certification for software that meets both FAA safety requirements and NIST/NSA security requirements. The commercial avionics industry depends on RTCA DO-178B, for software assurance while security products are evaluated according to the Common Criteria. The two sets of requirements from DO-178B and the Common Criteria are assessed for similarity of function with non-corresponding parts identified. Each certification process is outlined and a merged certification procedure is presented.

1 Introduction and Motivation

This document summarizes the similarities and differences between the certification processes required by the FAA, as embodied in RTCA document DO-178B, aimed at insuring flight safety, and by the NSA and NIST, as embodied in the Common Criteria requirements, aimed at insuring information security. At present, a system that needs to be certified for both purposes must be subjected to both processes. While the purposes for each certification are clearly different, many of the requirements and procedures are aimed at insuring that the final design and implementation meets certain quality standards. In many cases, these standards are similar, and by modifying or adding to the current procedure in each case, a single common process can be developed which will satisfy both certifications. Since each certification process can potentially be quite expensive, a common process should result in significant cost savings for those systems that must meet both standards.

Interest in computer aviation security has been an ongoing concern since the late 1990's [5]. With the recent terrorist events involving the World Trade Center in New York City, and the Pentagon in Washington, DC, it is probable that the FAA's mission to insure aircraft safety will become more and more intertwined with the need to protect sensitive data. Therefore, the need to merge safety requirements with information security has become more than just a cost-savings issue. This document compares and

contrasts the two processes, and proposes a merged process, which can be used to satisfy both certifications.

This paper is geared toward two separate audiences, those familiar with the FAA certification process, who now must become familiar with the security requirements specified in the Common Criteria, and security people who are familiar with the Common Criteria requirements, who are now interested in safety requirements. The two defining documents have been written for different purposes, from different communities with divergent backgrounds. Each document obtains a part of its context from the group experience of the rest of the community; and therefore each document makes assumptions, uses language, and builds upon unwritten rules and definitions that are not familiar to the other community. This makes the documents somewhat difficult to compare.

The first step in trying to merge the processes required by the FAA and NIST/NSA involved doing a comparison of the requirements of each document. The result of this effort was a mapping of the procedures specified in each document to one another [1]. Once the mapping was complete, it was relatively straightforward to determine which procedures were common to both processes, and which were unique to one or the other. This allowed us to propose a new, combined procedure that satisfies both certification authorities.

2 History of DO-178B and the Common Criteria

2.1 History and Summary of DO-178B

The use of software in avionics systems dates back to the 1970's. Engineers recognized that software allowed for easier modification or extension of hardware components [4] (Figure 1). Yet, certification of systems became more complex since the system now had to withstand both software design errors and hardware component failures. Traditional safety assessment methods based on predictable failure rates were no longer valid. Additional methods were necessary to assure that avionics software systems achieved the same level of assurance as hardware based systems. This need led to the creation of DO-178 in 1980 by the Radio Technical Commission for Avionics, now RTCA, Inc. [4]. RTCA is a not for profit corporation formed to advance the art and science of aviation and aviation electronic systems for public benefit [Reynolds]. In Europe, a parallel effort known as ED-35, was proposed by the European Organization for Civil Aviation Equipment (EUROCAE). In an effort to avoid duplication, both groups decided to combine efforts and produce a *common certification criteria* for software development. Thus, RTCA produced DO-178 and the EUROCAE published ED-12 which had identical content. Both documents went through several revisions with the production of DO-178A and ED-12A in 1985 [4]. Following the release of these documents, the aviation industry and certification authorities worldwide used DO-178A/ED-12A to determine the acceptability of systems and equipment containing software. Experiences with both DO-178A/ED-12A along with rapid advances in software technology led to the publication of DO-178B/ED-12B in 1989. A final version

of the document was approved by RTCA in 1992 [9]. This is the document currently in use today and is the version referred to in this paper.

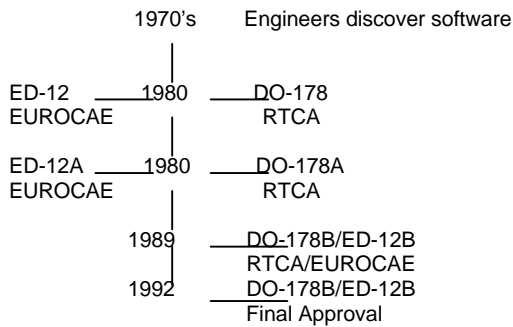


Figure 1. Time line of DO-178B development

DO-178B is divided into several main sections, each of which covers a life cycle process [9]. These processes include: Software Planning, Software Development, Software Verification, Software Configuration Management and Software Quality Assurance. While it is beyond the scope of this paper to describe the individual processes, further details can be found in a technical report titled, *Executive Summary, Towards Common Criteria Certification for DO-178B Compliant Airborne Software Systems* [1] and by direct reference to DO-178B [9].

An important part of avionics software development is determining the safety risk posed by the embedded software. DO-178B presents five software levels relating to potential failure in aircraft. The five levels range from Level A, the most failure critical, through Level E, which has no effect on aircraft safety. The levels are described as follows:

Level A is the most critical failure level and a software failure here would result in a catastrophic failure condition for an aircraft.

Level B would cause or contribute to hazardous/severe major failure condition for an aircraft.

Level C would cause or contribute to major failure condition for an aircraft.

Level D would cause or contribute to minor failure condition for an aircraft.

Level E would have no effect on an aircraft.

Further details on these failure levels can be found in DO-178B [9].

2.2 History and Summary of the Common Criteria

In the early 1980's, the National Security Agency (NSA) developed the Trusted Computer System Evaluation Criteria (TCSEC or Orange Book). TCSEC was used to evaluate IT security products. At the same time, other countries developed evaluation criteria based on TCSEC. In 1990, work began in the International Standards Organization (ISO) began development an international standard evaluation criteria for general use [14]. In 1993, seven organizations representing all of North America and Europe pooled criteria to join their separate efforts into a single set named the Common Criteria (Common Criteria) project. The countries currently involved in the Common Criteria project include: Canada, France, Germany, The Netherlands, the United Kingdom, and the United States [6]. The security organizations representing the United States are the National Institute of Standards and Technology (NIST) and the NSA. Version 1 of the Common Criteria was completed in 1996. Public review of the document was also conducted. Based on the results of trial use, public review and interaction with ISO, the Common Criteria Version 2 was revised from Version 1 and sent out in 1998 for use. A slightly modified version was approved as a draft for an ISO standard, 15408 in 1998. The Common Criteria Version 2.1 became the ISO standard, 15408 in December 1999 [14]. Version 2.1 of the Common Criteria is the most current version and is the document currently reviewed in this paper.

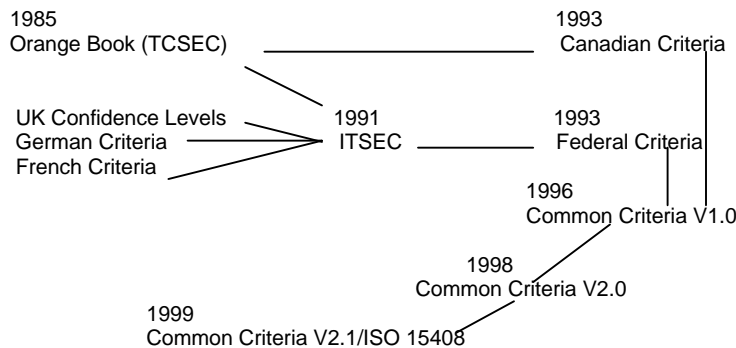


Figure 2. History of the Common Criteria

The Common Criteria forms the basis for the National Information Assurance Partnership (NIAP), a joint activity of NIST and NSA to establish an IT product security evaluation program supported by accredited, independent testing laboratories. The goals of NIAP are to establish cost-effective evaluation of security-capable IT products and promote the wide availability of tested products to federal agencies and others [14].

The Common Criteria organizes assurance requirements into *classes* which identifies the general topic covered by that class. Each class then contains subtopics called *families*, which in turn have *components* that specify the individual requirements. The assurance classes that we have included in the comparison are:

ACM - Configuration Management
ADO – Delivery and Operation
ADV- Development
AGD – Guidance Documents
ALC – Life Cycle Support
ATE – Tests
AVA – Vulnerability Assessment

Security requirements for software and systems will vary depending on the purpose of the system. The Common Criteria thus offers prepackaged levels of assurance, termed Evaluation Assurance Levels (EALs). The EALs range from EAL1, the lowest level of assurance to EAL7, the highest security assurance level. A detailed comparison of the different EALs is presented in our *Executive Summary* report [13] and can also be found in Common Criteria - Part3 [7].

EAL1 up through EAL4 introduces increasing rigor but without the introduction of specialized security engineering techniques [6]. EAL4 is the highest level for COTS systems. Above EAL4, increasing application of specialized security engineering is required. Products that meet requirements above EAL4 will have been designed with security in mind. Each EAL level requires increasing effort on the part of the manufacturer to produce additional evidence of compliance with security requirements. This effort is directly related to the cost of producing the product [6].

The Common Criteria model is founded on modularity and reuse. As such, there is the concept of a Protection Profile (PP) which is an implementation independent statement of security needs for a set of IT security products that “could” be built [6]. The PP is intended to be a re-usable definition of security requirements that are known to be useful to the security of a specific product. For example, a PP can be developed for Smart Cards or Firewalls. A PP is tied to a specific EAL level and should be developed by user communities, developers, or other parties interested in defining a common set of requirements [6]. More information on Protection Profiles can be found in the Common Criteria Users Guide [6] or in the Common Criteria – Part 1 [7].

A Security Target (ST) is a statement of security claims for a particular IT security product or system. An ST parallels the structure of a PP but contains product specific detailed information. The ST contains specifications which defines the specific measures taken in the product or system to meet security requirements [7].

The IT product to be evaluated is called a Target of Evaluation (TOE). The product’s security characteristics are described in an accompanying ST which may be linked to a PP for that particular type of product. Evaluation consists of rigorous analysis and testing performed by an accredited, independent laboratory. The scope of the evaluation is set by the EAL associated with the product [6].

3 Certification Using DO-178B and the Common Criteria

3.2 Steps to Merging Certification

Developing a merged certification process required several steps. We needed to identify the overlap between the two processes and insure that all of the requirements for both DO-178B and the Common Criteria were included. The steps for creating a combined process are as follows:

- Map DO-178B requirements to Common Criteria assurance requirements
- Document non-mapping requirements on the Common Criteria side.
Assume all DO-178B requirements will be completed.
- Examine separately the FAA and Common Criteria certification processes
- Outline a merged certification process

3.2 Mapping DO-178B and Common Criteria Requirements

In generating a high-level map between DO-178B and Common Criteria assurance requirements, we made the assumption that all DO-178B requirements would be completed. We then needed to identify Common Criteria assurance classes that would not map to any DO-178B processes and require separate inclusion in a final merged process. The following mapping shows a rough correspondence between the Common Criteria assurance classes and the DO-178B software processes.

Common Criteria Assurance Class

DO-178B Process

ACM Configuration Management	—————>	Software Configuration Management
ADO Deliver and Operation	—————>	<i>(No Correspondence)</i>
ADV Development	—————>	Software Development Process
AGD Guidance Documents	—————>	<i>(No Correspondence)</i>
ALC Life Cycle Support	—————>	Software Planning Process
ATE Tests	—————>	Software Verification Process
AVE Vulnerability Assessment	—————>	<i>(No Correspondence)</i>
<i>(No Correspondence)</i>	—————>	Software Quality Assurance

Three Common Criteria assurance classes did not map to any of the DO-178B processes [1]. These classes were AGD – Guidance Documents, ADO- Delivery and Operation and AVA-Vulnerability Assessment classes. Guidance Documents refer to documents specifically related to the security aspects of administration and operation of software. DO-178B does not address documentation relating to just the security aspects of system operation or for that matter any specific operation. 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. Vulnerability

Assessment deals specifically with covert channel analysis, deliberate misuse and other security function assessments that are absent in DO-178B.

3.3 FAA DO-178B Certification for Software

The FAA certification process begins outside the software development environment. Since software is not certified separately, it must be considered within the larger context of a certifiable component or aircraft. FAA certification typically involves either a Type Certification (TC) for an aircraft, engine or propeller or Technical Standard Order (TSO) which is a certification for a part used on an aircraft.

The only avionics regulations that references software is AC 20-115B which directly references DO-178B as a way of meeting regulation requirements [4]. Since software is not certified separately, it must be considered within the context of a system safety process. The software process and its relationship to other processes involved in the overall avionics system development is shown in Figure 1. The expectation of DO-178B is that there are outside safety and system processes that interface with software development. The interaction begins with a system process that identifies a set of system requirements. These requirements are passed to the system safety assessment process. This process sets the system development assurance level from the five possible levels, A through E [9]. This assurance level is passed back to the system process, which in turn sets the software criticality level, system requirements and safety related requirements, and passes these down to the software process.

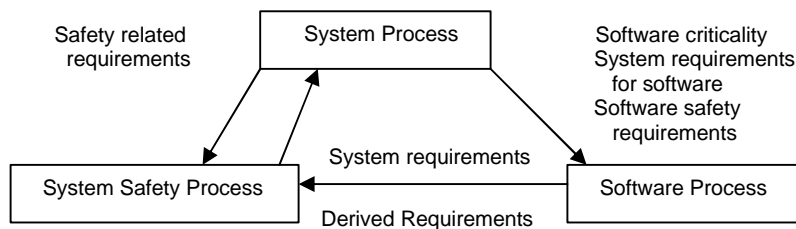


Figure 3. FAA Certification Overview

While not mandated, other documents are often used in the safety process. These documents include SAE ARP-4754 [11], SAE ARP-4761[12], MIL-STD-882D[3], and RTCA DO-254[10].

Certification approval involves the Designated Engineering Representative (DER) as the official representative of the FAA and the FAA. The DER's also function as the on-site safety officers and establish appropriate engineering processes to ensure FAA certification requirements are met [4]. Once software development is complete, assuming completion of the component or system in which the software is to be embedded, the DER either approves the component or recommends the component or system for approval to the FAA. The FAA has the final approval for all aircraft and aircraft systems and evaluates the evidence presented for certification [4].

3.2 NSA/NIST Common Criteria Certification

For a Common Criteria certification of a software component or system, the first step is to determine the EAL level for the product to be evaluated. The EAL level determines the effort and cost of Common Criteria certification [6]. EAL1 to EAL4 introduces increasing rigor without introducing specialized engineering techniques. From EAL5 to EAL7, products will have been designed with extra security considerations specifically for meeting these EAL requirements [6]. Once the EAL level has been determined, the next step is to identify a Protection Profile that could meet a given product's security requirements. If a PP is close but doesn't match exactly, it could be adapted to meet the product's requirements. If a PP doesn't yet exist, the product can still be developed by deciding on an EAL level and following security functional requirements from Common Criteria-Part 2 and assurance requirements from Common Criteria-Part 3 [6].

Next, the manufacturer prepares a Security Target (ST) which contains product specific details for meeting security requirements (See Section 2.2). The product is built including the security functional requirements specified in the security target. The manufacturer then submits the product, the ST, and accompanying documentation to an accredited testing laboratory for evaluation [6]. The lab evaluates the product against the ST. If it passes evaluation, it is submitted to an evaluation authority for validation of the results. In the US, the evaluation authority is NIST and the NSA. Validation of a product results in the awarding of a Common Criteria certification and the product is added to an official validated products list [14].

4 Mapping DO-178B to the Common Criteria Certification

4.1 Pre-development Certification Decisions

Before examining the overlap between the DO-178B and Common Criteria requirements, several steps related to both certifications need to be completed. For a FAA certification, the overall system design process for the certifiable component or aircraft must establish the system requirements, safety related requirements and set the software criticality level. This occurs outside of the DO-178B process and must occur before software development begins. Certification under the Common Criteria requires that the product manufacturer first decide on the appropriate EAL level for their product. The EAL level then defines the process that must be followed for certification. If available, a PP is used to assist the manufacturer in identifying security requirements and assurance components for the product. If no PP is available, then the manufacturer must put together the security requirements and assurance components for that level of EAL given the nature of the software product.

For dual certification, all the above steps must be completed before the software developed. Of particular importance is determination of DO-178B software criticality and Common Criteria EAL level since both steps define the documentation and development effort required to meet certification. For example, configuration management issues are

important in both DO-178B and Common Criteria requirements as are traceability and correspondence between high and low-level requirements. The requirements related to these activities will vary depending on software criticality and EAL assurance level.

The next phase in joint certification is to develop the software using both DO-178B and either a product specific PP or a derived set of security requirements and assurance components according to a defined EAL level. Specific areas of overlap between DO-178B development and Common Criteria assurance classes will be covered in the next section.

4.3 Mapping Certification Requirements

In mapping FAA software development requirements presented in DO-178B to the Common Criteria requirements, we have identified three broad areas of correspondence. These three areas relate to generic software lifecycle development phases with no assumption of a formal software model and include: Software Planning, Software Development, and Software Test and Assurance. Each of these areas will be discussed in detail regarding the areas of correspondence between the FAA and NIST/NSA certifications. Different EAL levels will be discussed where relevant and for DO-178B certification, software criticality level A will be assumed.

Software Planning is the first stage in the development life cycle and includes activities such as creating software plans, setting up the configuration management system and defining project life support activities. Support of these and other life cycle activities requires that the documentation process be established to create life cycle data needed for later certification. One of our assumptions in merging DO-178B and Common Criteria requirements is that there is considerable overlap between these two processes. Consequently, documentation generated for DO-178B certification can serve a dual purpose in assisting with Common Criteria certification.

The first area of correspondence under Software Planning deals with software configuration management (Table 1). Both DO-178B and Common Criteria require software configuration management to be used throughout the software development process. DO-178B discusses similar types of activities as the Common Criteria. Common activities for both areas include identification of each configuration item plus its version ID, authorized life cycle change control and establishment of data controls. Differences exist in the type of CM management system required by the Common Criteria and in some additional requirements for authorization of change control. Requirements can be met for both DO-178B and Common Criteria by automating or partially automating the configuration management system. The Common Criteria requires partial CM automation for EAL levels 4 and 5 and total automation for levels 6 and 7. DO-178B discusses change control and suggests that the CM system record changes to items plus provides protection against unauthorized changes. However, the Common Criteria makes the stronger statement that the CM system shall provide measures such that only authorized changes are made to the configuration items.

Under the category of Software Planning, the second area of correspondence between DO-178B and the Common Criteria is Software Planning. For DO-178B, this section is called Software Planning and for the Common Criteria the matching assurance class is ALC-Life Cycle Support (Table 1). Correspondence between these two areas is fairly weak in that one out of the three families correspond to the Software Planning activities of DO-178B. The ALC-Tat – Tools and Techniques maps to several DO-178B planning activities. EAL4-7 incorporates the ALC-Tat components while lower level EAL's do not require this assurance family at all. The other families under ALC, ALC-DVS-Development Security and ALC-LCD-Life Cycle definition have no corresponding DO-178B activities and would need to be added to the development of a dual certified software product. ALC-DVS concerns the physical security of the development environment and ALC-LCD outlines the use of an approved life cycle software development model.

The next broad area to be mapped is Software Development, which includes activities directly related to development of the software. Table 1 shows the rough correspondence between families in the ADV-Development class and the DO-178B software development sub-processes.

While these two sets of certification requirements match in terms of activities, the scope of the software development differs between DO-178B and the Common Criteria. The Common Criteria only focuses on activities related to security functionality while DO-178B encompasses the process of development for the entire product. Specifically, ADV-FSP-Functional Specification, ADL-HLD-High Level Design, ADV-IMP-Implementation, ADV-LLD-Low Level Design, and ADL-SPM-Security Policy Model all show some correspondence with DO-178B activities. Depending on the chosen EAL level, components from each of the above families will need to be incorporated into the DO-178B software development process. Two families had no match to any DO-178B activities and included ADV-INT-TSF-Internals and ADV-RCR Correspondence Demo. ADV-TSF addresses the internal structure of the security functionality of the product. The ADV-RCR family addresses modularity requirements and security policy issues. Components from these two families will need to be added to the DO-178B development process to meet Common Criteria certification.

The final area of software development to be mapped between the Common Criteria and DO-178B is termed Software Test and Assurance. Both DO-178B and the Common Criteria require extensive test, analysis and review of the adequacy and completeness of software requirements and their implementation. The Common Criteria class that covers test is ATE – Tests while the DO-178B section dealing with test and assurance is titled, Software Verification (Table 1). For the ATE assurance class, there appears to be many areas of overlap with DO-178B. Within ATE, the test procedures relate strictly to security functionality. For a merged test process, adding security tests to the test requirements for DO-178B appears to be feasible.

Table 1. Cross-reference between Common Criteria class components and DO-178B processes (for EAL5)

ACM – Configuration Management ACM_Aut CM Automation ACM_CAP Advanced support ACM_SCP Development Tools	<table border="0"> <tr> <th colspan="2">Software Configuration Management</th> </tr> <tr> <th>Activities</th> <th>Data Control Processes</th> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td>X</td> <td></td> </tr> </table>	Software Configuration Management		Activities	Data Control Processes	X		X		X		Life Cycle Data Sect. 11.4 Sect. 11.18 Sect. 11.4, 11.18																									
Software Configuration Management																																					
Activities	Data Control Processes																																				
X																																					
X																																					
X																																					
ADO – Delivery and Operation ADO_Del Prevention Modification ADO_IGS Installation and Start-up	(No correspondence with DO-178B Areas) (No correspondence with DO-178B Areas)																																				
ADV – Development ADV_FSP Functional Specification ADV_HLD High Level Design ADV_IMP Implementation of TSF ADV_INT Minimization Complexity ADV_LLD Low Level Design ADV_RCR Correspondence Demo ADV_SPM Security Policy Model	<table border="0"> <tr> <th colspan="5">Software Development Process</th> </tr> <tr> <th>Requirements</th> <th>Design</th> <th>Code</th> <th>Integrate</th> <th>Trace</th> </tr> <tr> <td>X</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>X</td> <td></td> <td>X</td> <td></td> </tr> <tr> <td></td> <td></td> <td>X</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td>X</td> <td></td> </tr> <tr> <td>X</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Software Development Process					Requirements	Design	Code	Integrate	Trace	X						X		X				X						X		X					Life Cycle Data Sect. 11.6, 11.9, 11.14 Sect. 11.7, 11.10, 11.14 Sect. 11.14, 11.11 Sect. 11.7, 11.10 Sect. 11.14 Sect 11.9, 11.14
Software Development Process																																					
Requirements	Design	Code	Integrate	Trace																																	
X																																					
	X		X																																		
		X																																			
			X																																		
X																																					
AGD – Guidance Documents AGD_ADM Administrative AGD_USR User	(No Correspondence with DO-178B Areas) (No Correspondence with DO-178B Areas)																																				
ALC – Life Cycle Support ALC_DVS Sufficiency Security ALC_LCD Measurable Model ALC_TAT Compliance Standards	<table border="0"> <tr> <th colspan="3">Software Planning</th> <th>Review</th> </tr> <tr> <th>Activ.</th> <th>Plans</th> <th>Life/Cycle/Env.</th> <th>Stand Plans</th> </tr> <tr> <td></td> <td></td> <td>X</td> <td>X</td> </tr> <tr> <td></td> <td></td> <td></td> <td>X</td> </tr> </table>	Software Planning			Review	Activ.	Plans	Life/Cycle/Env.	Stand Plans			X	X				X	Life Cycle Data Sect. 11.2																			
Software Planning			Review																																		
Activ.	Plans	Life/Cycle/Env.	Stand Plans																																		
		X	X																																		
			X																																		
ATE – Tests ATE_Cov Coverage ATE_DPT Impement. Represent. ATE_FUN Functional Testing ATE_IND Independent Testing	<table border="0"> <tr> <th colspan="3">Software Verification Process</th> </tr> <tr> <th>Activities</th> <th>Review and Analysis</th> <th>Testing</th> </tr> <tr> <td></td> <td>X</td> <td>X</td> </tr> <tr> <td></td> <td>X</td> <td>X</td> </tr> <tr> <td></td> <td></td> <td>X</td> </tr> <tr> <td></td> <td></td> <td>X</td> </tr> </table>	Software Verification Process			Activities	Review and Analysis	Testing		X	X		X	X			X			X	Life Cycle Data Sect. 11.3, 11.13, 11.14																	
Software Verification Process																																					
Activities	Review and Analysis	Testing																																			
	X	X																																			
	X	X																																			
		X																																			
		X																																			
AVA – Vulnerability Assessment AVA_CC Covert Channel AVA_MSU Insecure States AVA_SOF Functional Eval AVA_VLA Highly Resistant	(No Correspondence with DO-178B Areas) (No Correspondence with DO-178B Areas) (No Correspondence with DO-178B Areas) (No Correspondence with DO-178B Areas) (No Correspondence with DO-178B Areas)																																				

4.4 Non-mapping Common Criteria Classes

Three classes of the Common Criteria dealing more specifically with security issues did not map to any of the DO-178B certification requirements. These included the AGD–Guidance Documents, ADO-Delivery and Operation and AVA-Vulnerability Assessment Common Criteria 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 or for that matter any specific operation. 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. There is no corresponding activity in DO-178B. Vulnerability Assessment deals specifically with covert channel analysis, deliberate misuse and other security function assessments that are completely absent in DO-178B. Components from these classes will need to be added to comply with certification under both agencies.

5 Conclusion

The development of software intended for commercial aircraft, requires certification through the FAA. Currently, DO-178B is the recommended process document followed for software development while DO-254 is the equivalent document for electronic hardware. FAA certification is primarily concerned with safety and stresses production of software/hardware that meets their standard for safe plane operation. In contrast to the FAA, NIST/NSA certification using the Common Criteria stresses system security. The intent of a Common Criteria certification is to create IT products that meet an agreed upon level of assurance that the product won't succumb to security flaws.

This paper has focused on the feasibility of merging two certification processes in the interest of saving resources and avoiding duplication of effort. In mapping the actual development steps needed for dual certification, there is a great deal of overlap between DO-178B and the Common Criteria requirements. For some DO-178B requirements, simply incorporating security considerations or following a more rigid methodology is enough to meet both DO-178B and Common Criteria requirements. Other Common Criteria requirements missing from DO-178B will need to be added to the development process in order to meet both FAA and NIST/NSA certification.

Individual manufacturers typically have a development process that already meets a given set of certification requirements. Existing processes include extensive requirement checklists and allocating requirements among development team members. A manufacturer of products intended for the commercial avionics market already has an FAA compliant development environment that includes DER supervision. Adding Common Criteria security requirements, with the exception of the EAL 7 assurance class, to this type of an environment will not require substantial change in the development

effort. This will most likely be the typical case of adding Common Criteria compliance to FAA products. We believe it is less likely that Common Criteria products will now be required to meet FAA certification. This latter case will require extensive revision of the development environment since satisfying FAA safety requirements is not trivial and requires the presence of an on-site DER.

The actual process of obtaining the certifications cannot be merged and differs widely between the two agencies. Software or electronic hardware is not separately certified by the FAA but is incorporated into a certification effort for a component, an engine or an entire aircraft. As previously stated, there is an on-site DER who acts as a FAA representative and either performs the certification him/herself or recommends certification to the FAA. A great deal of the certification effort is dictated by the DER who is responsible for ensuring the use of safe engineering practices throughout the development effort. Common Criteria certification requires that the product evaluation be done by an accredited testing laboratory. Depending on the EAL level, evaluation can be costly. Product manufacturers seeking Common Criteria certification can also engage the help of Common Criteria consultants to assist with the certification effort.

Overall, dual certification appears to be possible and can achieve a certain economy of effort. Adding security on top of safety will benefit both the civil aviation industry and the general public in that there will be assurance that planes will fly safe and be more resistant to security related failure.

6 References

- [1] Advisory Circular No: 20-115B, AIR-100, January 11th, 1993.
- [2] Alves-Foss, J., C. Taylor, and B. Rinker. "Towards Common Criteria Certification for DO-178B Compliant Airborne Software Systems", 2002, <http://www.csds.uidaho.edu/~jimaf>.
- [3] DOD, MIL-STD-882D, Standard Practice for System Safety, Feb. 10, 2000.
- [4] Johnson, L. A. "DO-178B, Software considerations in airborne systems and equipment certification", <http://www.stsc.hill.af.mil/CrossTalk/1998/oct/schad.asp>, 1998.
- [5] Neumann, P.G. "Computer security in aviation: vulnerabilities, threats and risks", International Conf. on Aviation Safety and Security in the 21st Century, 13-15th January, 1997, White House Commission on Safety and Security and George Washington Univ., 1997.
- [6] NIST. Common Criteria User Guide. 1999. <http://csrc.nist.gov/cc/>, 1999.
- [7] NIST. Common Criteria for Information Security Evaluation. Parts 1, 2, 3. 1999. <http://csrc.nist.gov/cc/ccv20/ccv2list.htm>, NIST, 1999.

- [8] Reynolds, B. "The Role of DO-178B in meeting safety assurance objectives for airborne software". IEEE Midwest Solutions Conference, 2001.
- [9] RTCA. DO-178B/ED-12B. Software Considerations in Airborne Systems and Equipment Certification. RTCA, 1992.
- [10] RTCA. DO-254. Assurance Guidance for Airborne Electronic Hardware. RTCA, 2000.
- [11] SAE. ARP-4754, Certification Considerations for Highly Integrated or Complex Aircraft Systems, Systems Integration Req. Task Group, AS-IC, ASD, SAE, 1996.
- [12] SAE. ARP-4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, S-18 Committee, SAE, March 29, 1996.
- [13] Taylor, C. and J. Alves-Foss, B. Rinker. "Executive Summary Towards Common Criteria Certification for DO-178B Compliant Airborne Software Systems", 2002, [http:// www.csds.uidaho.edu/~jimaf](http://www.csds.uidaho.edu/~jimaf).
- [14] Troy, E. F. "Common Criteria: Launching the International Standard", http://csrc.nist.gov/cc/info/cc_bulletin.htm, NIST, 1998.