RTCA DO-178B (EUROCAE ED-12B)

Ankit Singh
(Bachelor of Engineering, Computer Science)
University of Applied Sciences - Frankfurt am Main, Germany
Email: ankitsingh.05@gmail.com

***Abstract*—This paper is intended for the people who are completely unaware of DO-178B/ED-12B document. The purpose of this paper is to explore certifications and standards for development of aviation softwares. The difference between creating aviation software and other software can be summarized in one simple phrase: "RTCA DO-178B" [10]. This paper will give some overview on the history of DO-178 as well as also give brief introduction to the future version DO-178C documents. The development and verification process using document RTCA DO-178B/ED-12B are very well covered in this paper [1] [1]. The paper will examine the Software Capability Maturity Model (SW-CMM) and DO-178B by considering the basic concepts of each standard, keys to successful integration of the standards, and benefits of integrating the two standards [3].**

CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

DO-178B/ED-12B 'Software Considerations in Airborne Systems and Equipment Certification' is a mature document and is an international standard relating to the safety and airworthiness of software for avionics. DO-178B is officially recognized as a *de facto* international standard by the International Organization for Standardization (ISO). There were two previous revisions DO-178 and D-178A which were done in the span of 20 years. [1] [5]

A. History of DO-178B [9]

Earlier, the softwares were considered as the easy and flexible way to enhance the functionality of mechanical and analog electrical systems. But very soon, it was realized that the usual approach to seek the safety and reliability will not work for Safety critical systems. There was a great need for finding design errors which came out in the form of first DO-178 certification document.

1) DO-178: DO-178 provided the software certification using "best practices", but it was written at a conceptual level. The rules were developed by trial and error over time. The concept was first introduced by DO-178 that describes the software verification requirements which were dependent on the safety criticality of the software. The software applications were divided into three categories: critical, essential, and nonessential. DO-178 also established the relationship between the software certification process and the other relevant Federal Aviation Regulations (FARs), such as the Type Certification Approval, the Technical Standard Order (TSO) Authorization, and the Supplemental Type Certification.

[1]DO-178B and ED-12B are copyrighted documents of RTCA and EUROCAE, respectively. In this paper, DO- 178B shall be used to refer to both the English version and the European equivalent. This convention was adopted solely as a means for brevity.

2) DO-178A: The first version DO-178 introduced the concept of software certification. The attempt to apply it quickly leads to the need of revision. A special committee 152 of RTCA was responsible for the revision of DO-178A which was published in 1985. DO-178A turned out to be very different from DO-178. The features such as systematic and structured detail, software development and verification processes were missing in DO-178. It introduced the concept of software applications Levels 1, 2 and 3 corresponding to the criticality safety categories of software applications i.e critical, essential and nonessential. For example, if adequate partitioning of the design could be shown, some of the software of a critical application would only need a Level 2 or 3 certification effort, rather than Level 1, because of its lesser role in the overall functioning of the critical application. As with DO-178, attempting to apply DO-178A led to many new problems. Interpretation of certification requirements differed from one FAA region to another. There were some misinterpretation of DO-178's intent which led to disqualification of entire software development cycle as it was not following the traditional waterfall-like processes. And there was an overall lack of understanding of the purpose of the certification requirements by the industry.

II. DO-178B

This chapter is going to give insight of the main topic DO-178B certification document. The DO-178/ED-12 document and all its revisions were sponsored by RTCA and EUROCAE. DO-178B consists of 12 sections, 2 annexes and 3 appendices as shown in the Figure 1 [1]. In short description of the

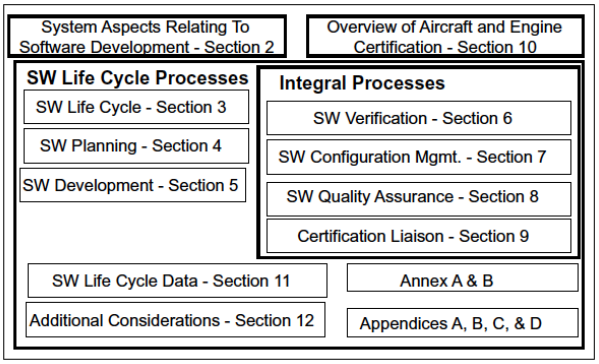

Figure 1. DO-178B Document Structure

components in the Figure 1 are as follows

- Section 2 and 10 provide a feedback to the overall certification process.
- Software life cycle processes given in Sections 3,4 and 5 are supported by Integral Processes detailed in Sections 6, 7, 8 and 9.
- Section 11 provides details on the life cycle data and Section 12 gives guidance to any additional considerations.
- Annex A provides a leveling of objectives. Annex B provides the document's glossary.
- Appendices A, B, C, and D provide additional material including a brief history of the document, the index, a list of contributors, and a process improvement form respectively.
- The 12 sections of DO-178B describe processes and activities for the most stringent level of software given in Table II.

Failure Condition	Software Level	Description
Catastrophic	A	Software that could cause or contribute to the failure of the system resulting in the loss of ability to continue safe flight and landing.
Hazardous	B	Software that could cause or contribute to the failure of the system resulting in a hazardous or severe failure condition
Major	C	Software that could cause or contribute to the failure of the system resulting in a major failure condition
Minor	D	Software that could cause or contribute to the failure of the system resulting in a Minor failure condition
No Effect	E	Software that could cause or contribute to the failure of the system resulting in no effect on the System

Table I
SOFTWARE LEVELS FOR DO-178B

Annex A provides a level by level tabulation of the objectives for lower levels of software. If an applicant adopts DO-178B for certification purpose, Annex A may be used as a checklist to achieve these objectives. The FAA's position is that if an applicant provides evidence to satisfy the objectives, then the software is DO-178B compliant. Accordingly, the FAA's checklists for performing audits of DO-178B developments are based on Annex A tables. The example is given in Figure 2

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Low-level requirements comply with high-level requirements.	6.3.2a	I	I	m		Software Verification Results	11.14	2	2	2	

Figure 2. Example Objective of Annex A

A. Software-System relationship

The software is considered as a part of the system. DO-178B specifies the information flow between system processes and software processes. The focus of the information flow from the system process to the software process is to keep track of requirements allocated to software, particularly those requirements that contribute to the system safety. The safety of the system (DO 254 [12]) is out of scope of this paper but it is important to understand how to apply DO-178B.

B. Software Life-Cycle Processes

The data exchange between the software and systems development processes is defined as the part of the software life-cycle processes in DO-178B. This includes the planning process, the software development processes (requirements,

design, code and integration), and the integral processes (verification, configuration management, software quality assurance, and certification liaison).

1) Software Planning Process: DO-178B defines five types of planning document for a software development. They are

- Plan for Software Aspects of Certification (PSAC)
- Software Development Plan
- Software Verification Plan
- Software Configuration Management Plan
- Software Quality Assurance Plan

These plans should include consideration of methods, languages, standards, and tools to be used during the development. A review of the planning process should have enough details to assure that the plans, proposed development environment, and development standards (requirements, design, and code) comply with DO-178B.

2) Software Development Process: The process include requirements, design and integration. The system's detailed functionality requirement is developed at various levels.

C. Integral Processes

Four processes are defined as integral in DO-178B which mean that they can be overlaid and extended throughout the software life cycle. They are as follows:

1) Software Verification: Verification is the most important in DO-178B which accounts to over two thirds of the total. Verification is a technical assessment of the results of both the software development processes and the software verification process. DO-178B defines verification as:

- Reviews provide qualitative assessment of a process or product. The most common types of reviews are requirements reviews, design reviews and test procedure reviews. DO-178B does not describe how these review are to be conducted or what means are to be considered as effective reviews.
- Analyses provide repeatable evidence of correctness and are often algorithmic or procedural in nature. Common types of analyses used include timing, stack, data flow, and control flow analyses. Race conditions and memory leakage should be checked as part of the timing and stack analysis. Data and control coupling analysis should include a minimum basic check for set/use and may extend to a full model of the system's behavior.
- Testing objective is met by maintaining a constant focus on requirements in a cost effective manner. The requirement-based test approach represents one of the most fundamental shifts from earlier versions of the document. A structural coverage analysis is performed to determine the extent to which the requirements-based test exercised the code. The tests should be written for both normal range and abnormal inputs (for robustness) as part of test generation process.
  - Level D: Software verification requires test coverage of high-level requirement only. No structural coverage is required.
  - Level C: Low-level requirement testing is required.
  - Level B: Decision coverage is required.
  - Level A: Code requires Modified Condition Decision Coverage (MCDC). Structural coverage analysis may be performed on source code only to the extent that the source code can be shown to map directly to object code. The reason for this rule is that some compilers may introduce code or structure that is different from source code.

2) Software Configuration Management: The clear definition of what is to be verified will be more reasonable for the various outputs of the verification in DO-178B. This definition or configuration is the design of the DO-178B objectives for configuration management. The six objectives in this are uniquely defined to meet all software levels which are as follows.

- What is to be configured?
- How baselines and traceability are established?
- How problem reports are dealt with?
- How the software is archived and loaded? and
- How the development environment is controlled?

DO-178B defines two control categories (CC1 and CC2) for data items produced throughout the development.

3) Software Quality Assurance: Software quality assurance (SQA) objectives provide oversight of the entire DO-178B process and require independence at all levels. SQA guarantees detection of plans and standards, deviated during development process are recorded, evaluated, tracked and resolved.

4) Certification Liaison Process: As mentioned earlier, the issues should be identified early for the certification process. DO-178B outlines twenty data items to be produced in a compliant process where three of these are specific to it and must be provided to the certifying authority. They are

- Plan for Software Aspects of Certification (PSAC)
- Software Configuration Index
- Software Accomplishment Summary

Other data items are requested by the certification authority if necessary.

D. Previously Developed Software

PDS is software that falls in one of the following categories:

- Commercial off-the-shelf software (COTS)
- Airborne software developed to other standards (e.g., MIL-STD-498)
- Airborne software that predates DO-178B (e.g., developed to the original DO-178 or DO-178A)
- Airborne software previously developed at a lower software level.

The use of one or more of these types of software should be planned for and discussed in the PSAC. The gap analysis need to be performed to determine where the objectives of DO-178B are not met.

III. Future Revision DO-178C/ED-12C

This chapter explores the new revision of the bible of the safety-critical software DO-178C/ED-12C which is expected to get published at the quarter of 2011. The author of [8] wrote "The new standard will allow credit for modern technologies

such as formal methods, object-oriented programming (OOP) languages, and model-based development, actions long sought by developers and vendors. Credit means that when a certain technology is used, some other certification requirements are reduced". DO-178C has been crafted specifically to handle the "sheer escalation in the amount of software" required by modern aircraft avionics, Hillary says [8]. This new version includes:

- Formal Methods: Mathematical based techniques used for specification, development and verification of a software/avionics software. Formal methods can be used to "prove that software is an accurate representation of the mathematical expressions," Hillary says [8].
- Object Oriented Programming: Languages like C++ and Ada are popular because they are at a higher level of abstraction than other languages which lead to promote re-use and promise more efficient development.
- Model-Based development which model systems at very high-level, domain-specific languages, are often used to automatically generate source code directly from the model.

"There will be a grandfather clause, so that everything that's been previously certified will be allowed to continue flying, as long as it hasn't been changed," says Vance Hilderman, co-founder and advisor at HighRely, a software services and certification tool supplier in Phoenix. DO-178C also will provide "some very nice criteria" to prove that new automated verification tools, such as formal methods tools and model verification tools, have been properly qualified and can be trusted, Hilderman continues [8].

IV. SW-CMM AND DO-178B

This section will give brief idea on the benefits of integrating the two standards. The software Capability Maturity Model (SW-CMM) became an important process for software standard throughout the 1990s. The SW-CMM was developed at Carnegie Mellon by the Software Engineering Institute. But SW-CMM was not sufficient without considering systems engineering and the acquisition life cycle. This motivated the development of the Systems Engineering Capability Maturity Model (SE-CMM) and the Systems Acquisition Capability Maturity Model (SA-CMM). These SW-CMM, SE-CMM, and SA-CMM became a foundation for a number of the other Capability Maturity Models like FAA which released the Integrated Capability Maturity Model (known as FAA-iCMM) to meet the software, systems and acquisition needs of the FAA for acquiring software. SW-CMM is a software process maturity framework which provides a roadmap for continuous process improvement based on good software engineering practices. These qualities motivate many avionics developers to implement the SW-CMM and vendors are required to meet specific SW-CMM levels prior to awarding contract. Avionics project for civil aviation must meet the regulations of the FAA to receive certification or authorization. RTCA DO-178B is recognized by FAA's Advisory Circular 20-115B for software aspects of certification as acceptable certification for the evaluation of software in airborne systems. There were some concerns regarding integration of SW-CMM and DO-178B together which author addressed in his paper [3]. The questions are:

- Are DO-178B/ED-12B and SW-CMM compatible?
- Can SW-CMM be used instead of DO- 178B/ED-12B?
- How can a company apply both SW- CMM and DO-178B/ED-12B?

For the purpose of SW-CMM, a "software process can be defined as a set of activities, methods, practices, and transformations that people use to develop and maintain software and associated products (e.g., project plans, design documents, code, test cases, and user manuals)" (Paulk, 3) [4] [3]. The maturity levels 1 to 5 indicated the overall effectiveness of the company's software engineering practices. The five levels are described in (page 8-9 [4] page 2 [3]). The key process areas of five levels for SW-CMM are given below in the Figure 3

Maturity Levels	Key Process Areas
5 – Optimizing (focus on continuous improvement)	• Process Change Management • Technology Innovation • Defect Prevention
4 – Managed (focus on product & process quality)	• Quality Management • Process Measurement & Analysis
3 – Defined (focus on engineering process)	• Peer Reviews • Intergroup Coordination • Software Product Engineering • Integrated Software Management • Training Program • Organization Process Definition • Organization Process Focus
2 – Repeatable (focus on project management)	• Software Configuration Management • Software Quality Assurance • Software Sub-contract Management • Software Project Tracking & Oversight • Software Project Planning • Software Requirements Management
1 – Initial (focus on individual)	• None

Figure 3. Key Process Area for SW-CMM

A. Comparison of SW-CMM and DO-178B/ED-12B

Both SW-CMM and DO-178B are assurance standards but, their primary focus is bit different. The SW-CMM looks at development processes along with their management and refinement which make sure that software meets its expected quality and ensure that development is within the cost and schedule. The DO-178B solely focuses on design assurance. The objective of required assurance is identified by its criticality levels A to E. The management cost and schedule is out of scope of FAA certification authorities who are concerned solely in the design aspects of software development. Due to the distinct features of both the standards, avionics company apply for both SW-CMM and DO-178B. This has led to the question: "Can SW-CMM be used as a substitute for DO-178B/ED-12B?" (i.e., can SW-CMM be considered an

alternate means of compliance to DO-178B/ED-12B?). While there are many similarities between DO- 178B/ED-12B and SW-CMM, there are also a number of significant differences that make it clear that SW-CMM is not an acceptable alternate means of compliance to DO- 178B/ED-12B - especially for the more safety critical systems, justified by Leanna in article [3]. The software companies which have SW-CMM level 2 or higher are nearly eligible to apply for DO-178B. So, together SW-CMM and DO-178B create a quality software process. Successful application of SW-CMM on certification projects may lead to cost savings, schedule reductions, and higher confidence from the FAA. So, we can **conclude** that *SW-CMM and DO-178B must be applied simultaneously.*

V. Conclusion

DO-178B is a guidance document only and focuses on software processes and objectives to comply with these processes. The DO-178B solely focuses on design assurance where the required assurance is defined on the basis of the criticality levels A to E. The benefits of DO-178B include: verifiable software quality, higher reliability, consistency, greater reusability, lower lifecycle costs, decreased maintenance cost, faster hardware integration, and greater portability. The DO-178B cannot be applied at the end of the project. It is very hard to apply reverse engineering to make software accommodated completely to DO-178B. The standard should be applied from the start or beginning of the development process. There are some issues with DO-178B that [13]:

- It is sometimes misunderstood as software development standard rather than an assurance standard.
- There is not a clear criteria for acceptance of software reuse, new techniques like object-oriented technology and automated tools (This issue is covered in DO-178C).
- DO-178B does not assure that the system requirements are correct.
- Phases like installation, maintenance and operation are not discussed in DO-178B.

Some of the major issues mentioned above are taken into consideration in the new revision DO-178C of DO-178 document. Inclusion of object oriented programming languages like C++ and Ada facilitate a high degree of automation of the verification and test techniques. The Formal Methods allow to look on the parts or the whole code and enable the software verification process to begin earlier which reduces the development risk. And the Model-based development tools are used for modeling a system of high level which allows it to automatically generate the source code directly from the model. As DO-178B solely focuses on design assurance, SW-CMM must be considered for applying simultaneously as SW-CMM also focuses on Management and refinement of the processes. The integration of SW-CMM on certification projects will be benefited with cost savings and schedule control. Like every thing is having its own advantages and disadvantages, DO-178B also has its own. But with careful consideration of its content with solid engineering judgement and successful integration of other good standards like SW-CMM/FAA-iCMM simultaneously should result in better and safer airborne software.

VI. Appendix

A. Glossary

RTCA: Radio Technical Commission for Aeronautics, Inc. (www.rtca.org). It plays an important role in defining guidelines for various aviation practices.
EUROCAE: European Organization for Civil Aviation Equipment.
FAA: The Federal Aviation Administration - is an agency of the United States Department of Transportation with authority to regulate and oversee all aspects of civil aviation in the U.S. (National Airworthiness Authority).
SW-CMM: Software Capability Maturity Model - Using knowledge acquired from software process assessments and extensive feedback from both industry and government, an improved version of the process maturity framework has been produced called the Capability Maturity Model for Software
COTS: Commercial off the shelf - is software, which is commercially available and intended for the public market.
MIL-STD-498: Military-Standard-498 - A United States military standard whose purpose was to "establish uniform requirements for software development and documentation."
ISO: International Organization for Standardization- is an international-standard-setting body composed of representatives from various national standards organizations.

Acknowledgements

I would like to specially thank Prof. Dr. Matthias Wagner and my fellow colleagues for continuously supporting and being continuously a source of motivation for me.

References

[1] RTCA DO-178B/EUROCAE ED-12B, Thomas K. Ferrel and Uma D. Ferrel, Ferrell and Associates Consulting
[2] The Certification of Systems containing Software Developed using RTCA-178B, Carolyn Salmon and Clive Lee, Ref: ASSC/12/0013, June 2006.
[3] USING THE SOFTWARE CAPABILITY MATURITY MODEL FOR CERTIFICATION PROJECTS (1998), Leanna K. Rierson, Federal Aviation Administration, Washington, D.C.
[4] Capability Maturity ModelSM for Software, Version 1.1, February 1993, Mark C. Paulk, Bill Curtis, Mary Beth Chrissis, Charles V. Weber
[5] IPL Testing Tools and RTCA/DO-178B, IPL Information Processing Ltd.
[6] Software Development under DO-178B, John Joseph Chilenski, Associate Technical Fellow Airborne Software Engineering Boeing Commercial Airplanes, January 2002
[7] DO-178B and Safety-Critical Software, Technical Overview, Joseph Wlad Product Marketing Manager Wind River Alameda, CA.
[8] DO 178C Nears Finish Available: http://www.militaryaerospace.com/index/display/avi-article-display/7404622510/articles/avionics-intelligence/features-and-analysis/2010/9/do-178c-nears_finish.html. Last access on:12/5/2010
[9] DO-178B and DO-178C Available: http://www.t-vec.com/wiki/index.php?title=DO-178B_and_DO-178C/. Last access on:12/5/2010
[10] Birds Project, Introduction to DO-178B (or DO-254) Available: http://www.sandroid.org/birdsproject/4dummies.html. Last access on:12/5/2010
[11] SQS company, Avionics Available: http://www.sqs-uk.com/avionics2.php. Last access on:12/6/2010
[12] Certification Authorities Software Team (CAST) Position Paper CAST-27 CLARIFICATIONS ON THE USE OF RTCA DOCUMENT DO-254 AND EUROCAE DOCUMENT ED-80, DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE COMPLETED June 2006(Rev 0)
[13] Airborne Software Concerns in Civil Aviation Certification, Benedito Sakugawa, Edson Cury and Edgar Toshiro Yano, Brazil