

RTCA, Inc.
1828 L Street, NW, Suite 805
Washington, D.C. 20036-5133 USA

**Final Report for Considerations of DO-178B
“Software Considerations in Airborne Systems
and Equipment Certification”**

RTCA/DO-248B
October 12, 2001

Prepared by: SC-190
© 2001, RTCA, Inc.

Copies of this document may be obtained from

RTCA, Inc.

Telephone: 202-833-9339

Facsimile: 202-833-9434

Internet: www.rtca.org

Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This document was prepared by RTCA Special Committee 190 (SC-190). It was approved by the RTCA Program Management Committee on October 12, 2001.

RTCA, Incorporated is a not-for-profit organization formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization functions as a Federal Advisory Committee and develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- Coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities.
- Analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency.
- Developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation.
- Assisting in developing the relevant technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other interested international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

1.0	<u>INTRODUCTION</u>	1
1.1	<u>Purpose</u>	1
1.2	<u>Document Overview</u>	2
2.0	<u>ERRATA</u>	3
2.1	<u>ERRATA #1: Name Correction in Appendix B</u>	3
2.2	<u>ERRATA #2: Typographical Correction in Section 2.3.2</u>	3
2.3	<u>ERRATA #3: Typographical Correction in Section 2.3.3c</u>	3
2.4	<u>ERRATA #4: Inconsistency Correction in Section 6.3.2c</u>	4
2.5	<u>ERRATA #5: Wording Improvement in Section 6.3.3f</u>	4
2.6	<u>ERRATA #6: Typographical Correction in Title of Section 6.4</u>	4
2.7	<u>ERRATA #7: Typographical Correction in Section 6.4</u>	5
2.8	<u>ERRATA #8: Typographical Correction in Figure 6-1 Title</u>	5
2.9	<u>ERRATA #9: Typographical Correction in Table 7-1</u>	6
2.10	<u>ERRATA #10: Typographical Correction in Section 8.3g</u>	7
2.11	<u>ERRATA #11: Typographical Correction in Table A-4</u>	8
2.12	<u>ERRATA #12: Typographical Correction in Table A-7</u>	10
3.0	<u>FREQUENTLY ASKED QUESTIONS (FAQ)</u>	13
3.1	<u>FAQ #1: Section 2.0 of DO-178B/ED-12B provides an introduction to the system aspects relating to software development and notes that guidelines were under development at the time of writing. Where are these system life cycle guidelines documented?</u>	13
3.2	<u>FAQ #2: Throughout DO-178B/ED-12B reference is made to the system safety assessment process. Where can guidelines for this process be found?</u>	13
3.3	<u>FAQ #3: What is meant by safety monitoring software experiencing transients in DO-178B/ED-12B Section 2.3.2, paragraph 3?</u>	14
3.4	<u>FAQ #4: Does DO-178B/ED-12B’s definition of commercial off-the-shelf (COTS) software include COTS software designed for option-selectable software?</u>	14
3.5	<u>FAQ #5: What are “end-to-end checks” in the context of field-loadable software?</u>	15
3.6	<u>FAQ #6: What are the design description and verification activity objectives for a Level D system and why are there apparent inconsistencies in the objectives to be satisfied in Annex A?</u>	16
3.7	<u>FAQ #7: How can compliance with DO-178B/ED-12B Section 5.2.3b be obtained?</u>	17

3.8	<u>FAQ #8:</u> Can multi-operational configurable software contain deactivated code?	17
3.9	<u>FAQ #9:</u> Do all high-level requirements require hardware/software integration testing? And, what does “<i>To verify the interrelationships between software requirements and components</i>” mean?	18
3.10	<u>FAQ #10:</u> Are baselines allowed to be changed? Section 7.2.2c states baselines should be protected from change, whereas Section 7.2.4c talks about changes to baselines.	19
3.11	<u>FAQ #11:</u> Is the "approved source" in Section 7.2.7a of DO-178B/ED-12B the previous approved product or is it the organization building the product?	19
3.12	<u>FAQ #12:</u> What are the definitions of Control Categories 1 and 2 (CC1 and CC2)?	19
3.13	<u>FAQ #13:</u> How is Table 7-1 used to understand Control Categories 1 and 2 (CC1 and CC2)?	20
3.14	<u>FAQ #14:</u> What do Control Categories 1 and 2 (CC1 and CC2) mean when applied to the objectives of Annex A?	20
3.15	<u>FAQ #15:</u> Is software certified as a stand-alone product?	21
3.16	<u>FAQ #16:</u> What is the highest software level (per DO-178B/ED-12B) that can be attained for previously developed software (PDS)?	21
3.17	<u>FAQ #17:</u> What are the issues related to changing previously developed software (PDS) versions from an earlier baseline?	21
3.18	<u>FAQ #18:</u> Since there is no specific guidance for handling changes to the aircraft’s operational environment, what part of DO-178B/ED-12B addresses this type of change?	22
3.19	<u>FAQ #19:</u> How does one determine if in-service problems indicate an inadequate process, and can one continue to pursue a service history means of compliance with some process inadequacies?	23
3.20	<u>FAQ #20:</u> What is the source of the glossary of terms in DO-178B/ED-12B and why do they appear to be different from other standard definitions?	23
3.21	<u>FAQ #21:</u> How is the second sentence of the definition of “patch” in DO-178B/ED-12B Annex B relevant to the definition itself?	24
3.22	<u>FAQ #22:</u> Can various industry process assessments such as the Software Engineering Institute (SEI) Capability Maturity Model (CMM), Software Process Improvement Capability Evaluation (SPICE), etc. be used for certification credit?	24
3.23	<u>FAQ #23:</u> Is software reliability addressed by DO-178B/ED-12B?	25
3.24	<u>FAQ #24:</u> What is the relationship between ARP4754/ED-79 and DO-178B/ED-12B?	25
3.25	<u>FAQ #25:</u> Can architectural means be used to reduce the software level needed for the incorporation of previously developed software (PDS) in a system?	26

3.26	<u>FAQ #26:</u> Does the fulfillment of “independence of multiple-version dissimilar software” (DO-178B/ED-12B Section 12.3.3.1) supercede the independence requirements as defined in Annex A of DO-178B/ED-12B?	27
3.27	<u>FAQ #27:</u> What is meant by “user-modifiable software”?	28
3.28	<u>FAQ #28:</u> What is the value of removing <i>dead code</i> or <i>unused variables</i> ?	29
3.29	<u>FAQ #29:</u> What does DO-178B/ED-12B Section 2.5b mean, when it addresses requirements related to a default mode, if one is provided to protect against software load errors?	29
3.30	<u>FAQ #30:</u> What does DO-178B/ED-12B Section 2.6a(2) mean regarding system safety requirements addressing system anomalous behavior?	30
3.31	<u>FAQ #31:</u> How does verification of product relate to “compiler acceptability”?	31
3.32	<u>FAQ #32:</u> What are defensive programming practices?	31
3.33	<u>FAQ #33:</u> Is it permissible to NOT meet the safety objectives by justifying any deviations from the design standards?	33
3.34	<u>FAQ #34:</u> What is the concept of independence as used in DO-178B/ED-12B?	34
3.35	<u>FAQ #35:</u> What are low-level requirements and how may they be tested?	34
3.36	<u>FAQ #36:</u> What is the exact definition or interpretation of derived requirements in DO-178B/ED-12B?	36
3.37	<u>FAQ #37:</u> What is meant by providing derived software requirements to the system safety assessment process?	36
3.38	<u>FAQ #38:</u> What is the difference between Integration Process and Integration Testing?	37
3.39	<u>FAQ #39:</u> What is the definition of an unbounded recursive algorithm in DO-178B/ED-12B Section 6.3.3d?	37
3.40	<u>FAQ #40:</u> What representation of the software is used to perform reviews and analyses of source code?	38
3.41	<u>FAQ #41:</u> Why is source code to object code traceability required for Level A software?	38
3.42	<u>FAQ #42:</u> Can structural coverage be demonstrated by analyzing the object code instead of the source code? Then, can a compiler be used to simplify the analysis?	38
3.43	<u>FAQ #43:</u> What is the intent of structural coverage analysis?	39
3.44	<u>FAQ #44:</u> Why is structural testing not DO-178B/ED-12B requirement?	40
3.45	<u>FAQ #45:</u> What is the relevance of the exception case stated in the last sentence of the definition of dead code?	40

3.46	<u>FAQ #46:</u> What is the meaning of Section 7.2.2g in ED-12B/DO-178B, when it states that a baseline or configuration item should be traceable either to the output it identifies or to the process with which it is associated?	41
3.47	<u>FAQ #47:</u> What is meant by the term “certification credit”?	41
3.48	<u>FAQ #48:</u> In addition to Sections 9 and 10 of DO-178B/ED-12B, which provide a high-level overview of the certification liaison and certification processes, where can further guidance on the approval process for software be found?	42
3.49	<u>FAQ #49:</u> Where can current certification authority guidance regarding issues not covered in DO-178B/ED-12B or expanding upon issues in DO-178B/ED-12B be found?	43
3.50	<u>FAQ #50:</u> What data items are deliverable to the certification authority to support software approval and product certification?	43
3.51	<u>FAQ #51:</u> What is meant by the term “type design,” as used in Section 9.4 of DO-178B/ED-12B?	44
3.52	<u>FAQ #52:</u> Why do the certification authorities not approve an organization’s process once, rather than approve each product submitted as part of a certification application?	44
3.53	<u>FAQ #53:</u> Do the data items need to be prepared and packaged as specified in Section 11 of DO-178B/ED-12B?	45
3.54	<u>FAQ #54:</u> Is the documentation required in DO-178B/ED-12B Section 11 excessive, especially for small projects?	45
3.55	<u>FAQ #55:</u> What are the control category considerations when determining how to package the data items discussed in Section 11 of DO-178B/ED-12B?	45
3.56	<u>FAQ #56:</u> How are redundancies inherent in the software verification documents eliminated?	46
3.57	<u>FAQ #57:</u> Is it necessary to mention all the additional considerations in the Plan for Software Aspects of Certification (PSAC) or is it sufficient to mention only the applicable additional considerations?	46
3.58	<u>FAQ #58:</u> How do you implement re-verification?	47
3.59	<u>FAQ #59:</u> What type of non-flight software is covered by DO-178B/ED-12B?	47
3.60	<u>FAQ #60:</u> Is a complete set of plans required for modifications of a system?	48
3.61	<u>FAQ #61:</u> What constitutes a development tool and when should it be qualified?	49
3.62	<u>FAQ #62:</u> What are the requirements for flight test analysis software and ground-based test software?	49
3.63	<u>FAQ #63:</u> For exhaustive input testing, the applicant should provide an analysis which confirms the isolation of the inputs to the software. What does it mean to confirm the isolation?	50

3.64	<u>FAQ #64:</u> Is it sufficient to use different linker or loader to produce dissimilar versions for avionics software?	50
3.65	<u>FAQ #65:</u> In DO-178B/ED-12B Sections 12.3.3.4 (Tool Qualification for Multiple-Version Dissimilar software) and 12.3.3.5 (Multiple Simulators and Verification) what is meant by “ <i>equivalent software verification process activities</i> ”?	51
3.66	<u>FAQ #66:</u> What is the difference between certification, approval, and qualification?.....	51
3.67	<u>FAQ #67:</u> What are data coupling and control coupling and how are they verified?.....	52
3.68	<u>FAQ #68:</u> The third sentence of the third paragraph of Section 3.2 of DO-178B/ED-12B states that “ <i>Component X illustrates the use of previously developed software used in a certified aircraft or engine.</i> ” Is it necessary, for a reused component to have been used in the context of a previous certified aircraft or engine?.....	53
3.69	<u>FAQ #69:</u> What is the rationale to have software design process feedback to the planning process in Section 5.2.2f of DO-178B/ED-12B, where feedback to the system life cycle process and software requirements process seems adequate?	53
3.70	<u>FAQ #70:</u> What is the purpose of the second sentence in DO-178B/ED-12B Section 5.4.3a?	54
3.71	<u>FAQ #71:</u> What is the purpose of traceability, how much is required, and how is it documented? For example, is a matrix required or are other methods acceptable?.....	54
3.72	<u>FAQ #72:</u> What happens if an error indicates a weakness in the development process itself?	56
3.73	<u>FAQ #73:</u> Are timing measurements during testing sufficient or is a rigorous demonstration of worst-case timing necessary?.....	56
3.74	<u>FAQ #74:</u> What is the difference between the development and life cycle objectives stated in DO-178B/ED-12B for Level A versus Level B software, and how does that relate to safety?	57
3.75	<u>FAQ #75:</u> Can sampling be used for some verification activities (such as coding rules on source code)?	58
3.76	<u>FAQ #76:</u> Can problem reports and verification activities performed on a software configuration item be referenced in previously approved products without repeating this effort for each product that uses this software configuration item?.....	59
4.0	DISCUSSION PAPERS (DP)	61
4.1	<u>DP #1:</u> Verification Tool Selection Considerations	61
4.2	<u>DP #2:</u> The Relationship of DO-178B/ED-12B to the Code of Federal Regulations (CFRs) and Joint Aviation Requirements (JARs).....	63
4.3	<u>DP #3:</u> The Differences Between DO-178A/ED-12A and DO-178B/ED-12B Guidance for Meeting the Objective of Structural Coverage.....	64

4.4	<u>DP #4: Service History Use – Rationale for DO-178B/ED-12B, Section 12.3.5a through k</u>	66
4.5	<u>DP #5: Application of Potential Alternative Methods of Compliance for Previously Developed Software (PDS)</u>	70
4.6	<u>DP #6: Transition Criteria</u>	81
4.7	<u>DP #7: Definition of Commonly Used Verification Terms</u>	84
4.8	<u>DP #8: Structural Coverage and Safety Objectives</u>	85
4.9	<u>DP #9: Certification With Known Software Problems</u>	86
4.10	<u>DP #10: Considerations Addressed When Deciding to Use Previously Developed Software (PDS)</u>	88
4.11	<u>DP #11: Qualification of a Tool Using Service History</u>	91
4.12	<u>DP #12: Object Code to Source Code Traceability Issues</u>	97
4.13	<u>DP #13: Definitions of Statement Coverage, Decision Coverage, and Modified Condition/Decision Coverage (MC/DC)</u>	98
4.14	<u>DP #14: Partitioning Aspects in DO-178B/ED-12B</u>	105
4.15	<u>DP #15: Relationship Between Regression Testing and Hardware Changes</u>	109
APPENDIX A – ACRONYMS		A-1
APPENDIX B – COMMITTEE MEMBERSHIP		B-1
APPENDIX C – INDEX OF KEYWORDS		C-1
APPENDIX D – CORRELATION BETWEEN DO-178B/ED-12B AND FINAL REPORT PRODUCTS		D-1
APPENDIX E – SC-190/WG-52 TERMS OF REFERENCE		E-1
APPENDIX F – REFERENCES		F-1

1.0 **INTRODUCTION**

DO-178B/ED-12B, “Software Considerations in Airborne Systems and Equipment Certification,” was published December 1, 1992, to provide recommendations for the production of software for airborne systems and equipment that performs its intended function with a level of confidence in safety that complies with airworthiness requirements. Since the date of publication, the aviation community has gained experience using DO-178B/ED-12B and has raised a number of questions regarding the document’s content and application.

In order to address the questions of both the industry and certification authorities, RTCA Special Committee 190 (SC-190) and the European Organisation for Civil Aviation Equipment (EUROCAE) Working Group 52 (WG-52) was formed in 1996. This document represents the third and final report of the SC-190/WG-52 joint committee. It contains the same errata, frequently asked questions, and discussion papers from the second annual report (DO-248A/ED-94A). Additionally, documents approved by the SC-190/WG-52 through September 22, 2000 are included. This report contains all of the SC-190/WG-52 committee’s work on clarification of DO-178B/ED-12B.

1.1 **Purpose**

The purpose of this document is to provide clarification of the guidance material in DO-178B/ED-12B. The clarification material may accomplish any or all of the following purposes:

- Resolution of content errors in DO-178B/ED-12B.
- Clarification of a specific section or topic of DO-178B/ED-12B.
- Resolution of an inconsistency between DO-178B/ED-12B and any other relevant civil aviation standards.

In order to accomplish these clarification purposes, the following products have been generated and are included in this annual report:

- **Errata**: The purpose of Errata is to provide a means of correcting errors in DO-178B/ED-12B (e.g., typographical errors). Errata contain no new or additional guidance material.
- **Frequently Asked Question (FAQ)**: The purpose of a FAQ is to provide short and concise responses to questions that are frequently asked by industry concerning the material of DO-178B/ED-12B. These questions are frequently posed to certification authorities or others who provide interpretation of DO-178B/ED-12B. A FAQ contains no new or additional guidance material.
- **Discussion Paper (DP)**: The purpose of a Discussion Paper is to provide clarification for certain sections of DO-178B/ED-12B in cases where the clarification requires more than a short answer to a question. A DP contains no new or additional guidance material.