RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington, D.C. 20036

Supporting Information for DO-178C and DO-278A

RTCA DO-248C
December 13, 2011

Prepared by: SC-205

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 205 (SC-205) and EUROCAE Working Group 71 (WG-71) and approved by the RTCA Program Management Committee (PMC) on December 13, 2011.

RTCA, Incorporated is a not-for-profit corporation 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; and

- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate 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 the 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 INTRODUCTION 1

1.1 Purpose 1

1.2 Document Overview 2

1.3 How to Use This Document 2

2.0 ERRATA 3

3.0 FREQUENTLY ASKED QUESTIONS (FAQ) 5

3.1 FAQ #1: Section 2 of DO-178B 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? 5

3.2 FAQ #2: Throughout DO-178B reference is made to the system safety assessment process. Where can guidelines for this process be found? 5

3.3 FAQ #3: What is meant by safety monitoring software experiencing transients in DO-178B Section 2.3.2, paragraph 3? 5

3.4 FAQ #4: Does DO-178C/DO-278A's definition of commercial off-the-shelf (COTS) software include COTS software designed for option-selectable software? 5

3.5 FAQ #5: What are "end-to-end checks" in the context of field-loadable software? 6

3.6 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? 6

3.7 FAQ #7: How can compliance with DO-178C/DO-278A section 5.2.3, Designing for User-Modifiable Software, be obtained? 7

3.8 FAQ #8: Can option-selectable software contain deactivated code? 7

3.9 FAQ #9: Do all high-level requirements require hardware/software integration testing? And, what does "*To verify the interrelationships between software requirements and components*" mean? 8

3.10 FAQ #10: Are baselines allowed to be changed? Section 7.2.2.c states baselines should be protected from change, whereas section 7.2.4.c talks about changes to baselines. 8

3.11 FAQ #11: Is the "approved source" in section 7.2.7.a of DO-178B the previous approved product or is it the organization building the product? 8

3.12 FAQ #12: What are the definitions of Control Categories 1 and 2 (CC1 and CC2)? 8

3.13 FAQ #13: How is Table 7-1 in section 7.3 used to understand Control Categories 1 and 2 (CC1 and CC2)? 9

3.14 FAQ #14: What do Control Categories 1 and 2 (CC1 and CC2) mean when applied to the objectives of Annex A? 9

3.15 FAQ #15: Is software certified as a stand-alone product? 9

3.16 FAQ #16: What is the highest software level (per DO-178C) or assurance level (per DO-278A) that can be attained for previously developed software (PDS)? 10
3.17 FAQ #17: What are the issues related to changing previously developed software (PDS) versions from an earlier baseline? 10
3.18 FAQ #18: Since there is no specific guidance for handling changes to the aircraft's operational environment, what part of DO-178C addresses this type of change? 11
3.19 FAQ #19: 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? 11
3.20 FAQ #20: What is the source of the glossary of terms in DO-178C, DO-278A, and the Supplements, and why do they appear to be different from other standard definitions? 12
3.21 FAQ #21: How is the second sentence of the definition of "patch" in DO-178C/DO-278A Annex B relevant to the definition itself? 12
3.22 FAQ #22: Can various industry process assessments such as the Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI), Software Process Improvement Capability Evaluation (SPICE), etc. be used for certification credit? 13
3.23 FAQ #23: Is software reliability addressed by DO-178C/DO-278A? 13
3.24 FAQ #24: What is the relationship between ARP4754A/ED-79A and DO-178C? 14
3.25 FAQ #25: Can architectural means be used to reduce the software level/assurance level needed for the incorporation of previously developed software (PDS) in a system? 15
3.26 FAQ #26: Does the fulfillment of "independence of multiple-version dissimilar software" (DO-178B section 12.3.3.1) supersede the independence requirements as defined in Annex A of DO-178B? 16
3.27 FAQ #27: What is meant by "user-modifiable software"? 16
3.28 FAQ #28: What is the value of removing *dead code* or *unused variables*? 16
3.29 FAQ #29: What does DO-178C section 2.5.5.b (DO-278A section 2.6.5.b) mean when it addresses requirements related to a default mode, if one is provided to protect against software load errors? 16
3.30 FAQ #30: What does DO-178B section 2.6a(2) mean regarding system safety requirements addressing system anomalous behavior? 16
3.31 FAQ #31: How does verification of product relate to "compiler acceptability"? 16
3.32 FAQ #32: What are defensive programming practices? 17
3.33 FAQ #33: Is it permissible to NOT meet the safety objectives by justifying any deviations from the design standards? 19
3.34 FAQ #34: What is the concept of independence as used in DO-178B? 19
3.35 FAQ #35: What are low-level requirements and how may they be tested? 19
3.36 FAQ #36: What is the definition or interpretation of derived requirements in DO-178C/DO-278A? 20

3.37 FAQ #37: What is meant by providing derived software requirements to the system processes, including the system safety assessment process? 20
3.38 FAQ #38: What is the difference between Integration Process and Integration Testing? 21
3.39 FAQ #39: What is the definition of an unbounded recursive algorithm in DO-178C/DO-278A section 6.3.3.d? 21
3.40 FAQ #40: What representation of the software is used to perform reviews and analyses of Source Code? 21
3.41 FAQ #41: Why is Source Code to object code traceability required for Level A software? 22
3.42 FAQ #42: What needs to be considered when performing structural coverage at the object code level? 22
3.43 FAQ #43: What is the intent of structural coverage analysis? 23
3.44 FAQ #44: Why is structural testing not a DO-178C/DO-278A requirement? 24
3.45 FAQ #45: What is the relevance of the exception case stated in the definition of dead code? 24
3.46 FAQ #46: What is the meaning of section 7.2.2.g in DO-178C/DO-278A, when it states that a baseline or configuration item should be traceable either to the output it identifies or to the processes with which it is associated? 25
3.47 FAQ #47: What is meant by the term "verification credit" or "approval credit"? 25
3.48 FAQ #48: In addition to sections 9 and 10 of DO-178C, 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? 26
3.49 FAQ #49: Where can current certification authority guidance regarding issues not covered in DO-178B or expanding upon issues in DO-178B be found? 27
3.50 FAQ #50: What data items are deliverable to the certification/approval authority to support software approval and product certification/approval? 27
3.51 FAQ #51: What is meant by the term "type design," as used in section 9.4 of DO-178B? 27
3.52 FAQ #52: Why do the certification/approval authorities not approve an organization's process once, rather than approve each product submitted as part of a certification/approval application? 27
3.53 FAQ #53: Do the data items need to be prepared and packaged as specified in section 11 of DO-178B? 28
3.54 FAQ #54: Is the documentation required in DO-178C/DO-278A section 11 excessive, especially for small projects? 28
3.55 FAQ #55: What are the control category considerations when determining how to package the data items discussed in section 11 of DO-178C/DO-278A? 28
3.56 FAQ #56: How are redundancies inherent in the software verification documents eliminated? 29

3.57 FAQ #57: Is it necessary to mention all the additional considerations in the Plan for Software Aspects of Certification (PSAC) or Plan for Software Aspects of Approval (PSAA) or is it sufficient to mention only the applicable additional considerations? 29

3.58 FAQ #58: How do you implement re-verification? 29

3.59 FAQ #59: What type of non-flight software is covered by DO-178C? 30

3.60 FAQ #60: Is a complete set of plans required for modifications of a system? 30

3.61 FAQ #61: What constitutes a development tool and when should it be qualified? 31

3.62 FAQ #62: What are the requirements for flight test analysis software and ground-based test software? 31

3.63 FAQ #63: 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? 32

3.64 FAQ #64: Is it sufficient to use different linker or loader to produce dissimilar versions for avionics software? 32

3.65 FAQ #65: What is meant by "*equivalent software verification process activity*" in DO-178C/DO-278A sections 12.3.2.4 (Tool Qualification for Multiple-Version Dissimilar Software) and 12.3.2.5 (Multiple Simulators and Verification)? 33

3.66 FAQ #66: What is the difference between certification, approval, and qualification? 33

3.67 FAQ #67: What is analysis of data coupling and control coupling? 33

3.68 FAQ #68: The third sentence of the third paragraph of section 3.2 of DO-178C states that "*Component X illustrates the use of previously developed software used in a certified product.*" (The equivalent sentence in DO-278A states that "*Component X illustrates the use of previously developed software used in an approved system.*") Is it necessary, for a reused component to have been used in the context of a previously certified product or an approved system? 35

3.69 FAQ #69: What is the rationale to have software design process feedback to the planning process in section 5.2.2.g of DO-178C/DO-278A, where feedback to the system life cycle process and software requirements process seems adequate? 35

3.70 FAQ #70: What is the purpose of the second sentence in DO-178C/DO-278A section 5.2.4.b? 36

3.71 FAQ #71: 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? 36

3.72 FAQ #72: What happens if an error indicates a weakness in the development process itself? 36

3.73 FAQ #73: Are timing measurements during testing sufficient or is a rigorous demonstration of worst-case timing necessary? 37

3.74 FAQ #74: What is the difference between the development and life cycle objectives stated in DO-178C for Level A versus Level B software, and how does that relate to safety? Similarly, what is the difference in DO-278A for AL1 versus AL2 software? 38

3.75 FAQ #75: Can sampling be used for some verification activities (such as coding rules on Source Code)? 39

3.76 FAQ #76: 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? 40

3.77 FAQ #77: The Software Requirements Data are described by DO-178C/DO-278A section 11.9. What is meant in step 11.9.g: "*Failure detection and safety monitoring requirements*"? 40

3.78 FAQ #78: For software requirements expressed by logic equations, how many normal range test cases are necessary to verify the variable usage and the Boolean operators? 41

3.79 FAQ #79: Can an applicant for aircraft, engine, or propeller certification take credit for DO-178C compliance found under an earlier approval (that is, Technical Standard Order (TSO) or European Technical Standard Order (ETSO))? 41

3.80 FAQ #80: What needs to be considered when using inlining? 42

3.81 FAQ #81: What aspects should be considered when there is only one level of requirements (or if high-level requirements and low-level requirements are merged)? 43

3.82 FAQ #82: If pseudocode is used as part of the low-level requirements, what issues need to be addressed? 44

3.83 FAQ #83: Should compiler errata be considered? 46

3.84 FAQ #84: How can all Level D (AL 5) objectives be met if low-level requirements and Source Code are not required? 46

4.0 DISCUSSION PAPERS (DP) 49

4.1 DP #1: Verification Tool Selection Considerations 49

4.2 DP #2: The Relationship of DO-178B/ED-12B to the Code of Federal Regulations (CFRs) and Joint Aviation Requirements (JARs) 49

4.3 DP #3: The Differences Between DO-178A and DO-178B Guidance for Meeting the Objective of Structural Coverage 49

4.4 DP #4: Service History Rationale for DO-178C 49

4.5 DP #5: Application of Potential Alternative Methods of Compliance for Previously Developed Software (PDS) 55

4.6 DP #6: Transition Criteria 67

4.7 DP #7: Definition of Commonly Used Verification Terms 70

4.8 DP #8: Structural Coverage and Safety Objectives 70

4.9 DP #9: Assessment and Classification of Open Software Problems 71

4.10 DP #10: Considerations Addressed When Deciding to Use Previously Developed Software (PDS) 76

4.11 DP #11: Qualification of a Tool Using Service History 79
4.12 DP #12: Object Code to Source Code Traceability Issues..... 79
4.13 DP #13: Discussion of Statement Coverage, Decision Coverage, and Modified Condition/Decision Coverage (MC/DC) 81
4.14 DP #14: Partitioning Aspects in DO-178C/DO-278A..... 88
4.15 DP #15: Relationship Between Regression Testing and Hardware Changes ... 92
4.16 DP #16: Cache Management 94
4.17 DP #17: Usage of Floating-Point Arithmetic..... 96
4.18 DP #18: Service Experience Rationale for DO-278A 97
4.19 DP #19: Independence in DO-178C/DO-278A 103
4.20 DP #20: Parameter Data Items and Adaptation Data Items 109
4.21 DP #21: Clarification on Single Event Upset (SEU) as It Relates to Software 118

5.0 RATIONALE FOR DO-178C/DO-278A 125
5.1 Introduction..... 125
5.2 Rationale for DO-178C/DO-278A Section 2: SYSTEM ASPECTS RELATING TO SOFTWARE DEVELOPMENT 126
5.3 Rationale for DO-178C/DO-278A Section 3: SOFTWARE LIFE CYCLE.... 126
5.4 Rationale for DO-178C/DO-278A Section 4: SOFTWARE PLANNING PROCESS 126
5.5 Rationale for DO-178C/DO-278A Section 5: SOFTWARE DEVELOPMENT PROCESSES 127
5.6 Rationale for DO-178C/DO-278A Section 6: SOFTWARE VERIFICATION PROCESS 128
5.7 Rationale for DO-178C/DO-278A Section 7: SOFTWARE CONFIGURATION MANAGEMENT PROCESS..... 130
5.8 Rationale for DO-178C/DO-278A Section 8: SOFTWARE QUALITY ASSURANCE PROCESS 130
5.9 Rationale for DO-178C/DO-278A Section 9: CERTIFICATION/APPROVAL LIAISON PROCESS 131
5.10 Rationale for DO-178C/DO-278A Section 10: OVERVIEW OF CERTIFICATION (CNS/ATM SYSTEM APPROVAL) PROCESS 131
5.11 Rationale for DO-178C/DO-278A Section 11: SOFTWARE LIFE CYCLE DATA 131
5.12 Rationale for DO-178C/DO-278A Section 12: ADDITIONAL CONSIDERATIONS..... 131
5.13 Rationale for TOOL QUALIFICATION DOCUMENT AND DO-178C/DO-278A SUPPLEMENTS..... 132

APPENDIX A – ACRONYMS A-1

APPENDIX B – COMMITTEE MEMBERSHIP B-1

APPENDIX C – INDEX OF KEYWORDS C-1

APPENDIX D – CORRELATION BETWEEN DO-178C, DO-278A, AND DO-248C D-1

TABLE OF FIGURES

FIGURE 4-1 PDS RELATIONSHIP TO PSAC/PSAA 58
FIGURE 4-2 INDEPENDENCE AND VERIFICATION OBJECTIVES ILLUSTRATED 106
FIGURE 4-3 PARAMETER DATA ITEM RELATIONSHIP WITH EXECUTABLE OBJECT CODE 110
FIGURE 4-4 PDI VIEW IN DO-178C AND DO-278A 111
FIGURE 4-5 EXAMPLE OF PDI HIGH-LEVEL REQUIREMENT 112
FIGURE 4-6 EXAMPLE OF PDI HIGH-LEVEL REQUIREMENTS 113
FIGURE 4-7 EXAMPLE OF HIGH-LEVEL REQUIREMENT DEFINING PDI VALUES 113
FIGURE 4-8 VERIFICATION OF PDI FILE 116

TABLE OF TABLES

TABLE 4-1 TRUTH TABLE FOR DECISION (A OR (B AND C)) 85
TABLE 4-2 TRUTH TABLE FOR DECISIONS (A || (B && C)) 86
TABLE 4-3 TRUTH TABLE FOR ((A || B) && C) 87
TABLE 4-4 TRUTH TABLE FOR ((A < 3) OR (A > 8)) 87
TABLE 4-5 INDEPENDENCE INTERPRETATION FOR VERIFICATION OBJECTIVES 107
TABLE 4-6 DATA TYPE ATTRIBUTES 114

This Page Intentionally Left Blank

1.0 INTRODUCTION

DO-178C, "Software Considerations in Airborne Systems and Equipment Certification," provides 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. DO-278A, "Software Integrity Assurance Considerations for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems," provides similar guidance for the CNS/ATM ground-based community. DO-178C and DO-278A are based on DO-178B; therefore, many of the questions that were raised by the aviation community against DO-178B are also relevant to DO-178C and DO-278A.

This document addresses the questions of both the industry and authorities. It contains frequently asked questions (FAQs), discussion papers (DPs), and rationale. Many of the FAQs and DPs are based on DO-248B; however, some have been modified to address changes from DO-178B to DO-178C and to make applicable to DO-278A. Additionally, some new FAQs and DPs have been added to provide additional clarification on DO-178C and/or DO-278A. The errata against DO-178B (which were in section 2 of DO-248B) have been deleted, since they have been incorporated into DO-178C and are no longer relevant. The rationale for DO-178C and DO-278A objectives has also been added to DO-248C.

Note: Prior to using this document, it is recommended that the reader consider section 1.3, "How to Use This Document".

1.1 Purpose

This document provides clarification of the guidance material in DO-178C and DO-278A. In order to accomplish this clarification the following products have been generated:

- Frequently Asked Question (FAQ) – Section 3: 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-178C and/or DO-278A. These questions are frequently posed to certification authorities or others who provide interpretation of DO-178C and/or DO-278A. A FAQ contains no new guidance material. A FAQ is typically no longer than two pages.

- Discussion Paper (DP) – Section 4: The purpose of a Discussion Paper is to provide clarification for certain sections of DO-178C and/or DO-278A in cases where the clarification requires more than a short answer to a question. A DP contains no new guidance material.

- Rationale – Section 5: The purpose of the rationale is to document some items considered when developing DO-178B and then DO-178C and DO-278A. The rationale is only intended to be background information to aid the reader's understanding of DO-178C and DO-278A — especially of those sections and objectives that industry feedback has shown might benefit from additional clarification. The rationale contains no guidance material.