

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

Software Considerations in Airborne Systems and Equipment Certification

RTCA DO-178B
December 1, 1992

Prepared by: SC-167
© 1992 RTCA, Inc.

Copies of this document may be obtained from

RTCA, Inc.

Telephone: 202-333-9439

Facsimile: 202-333-4434

Internet: www.rtca.org

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

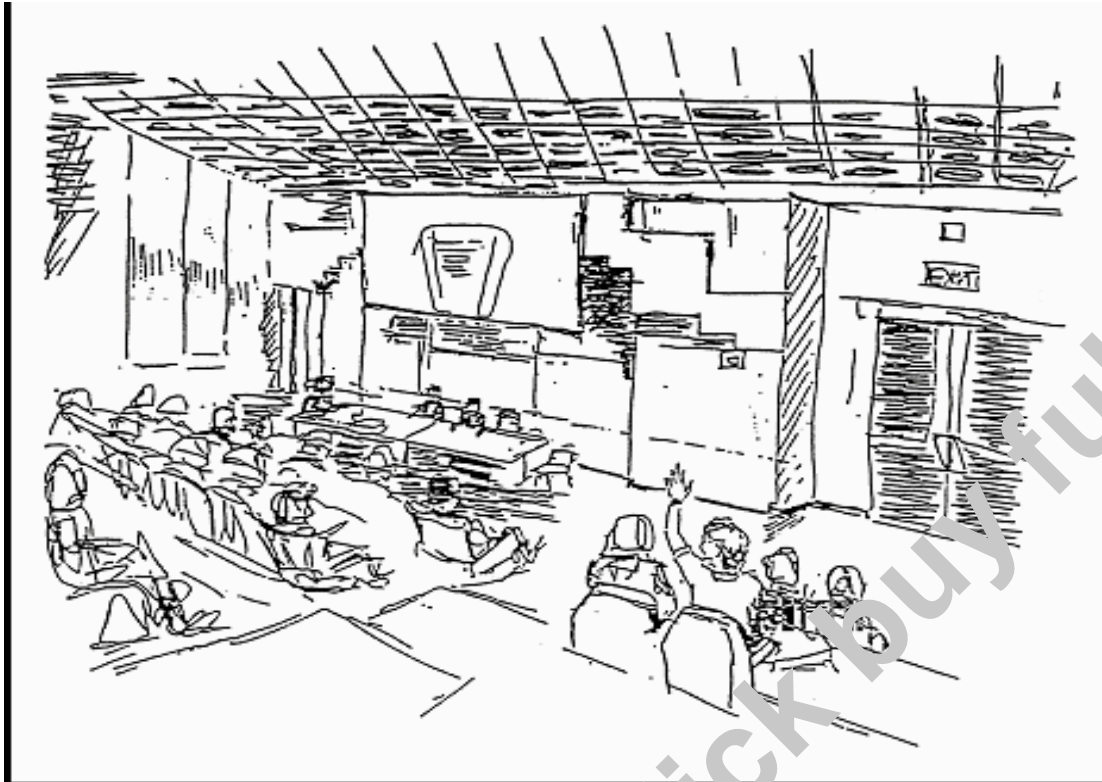
FOREWORD

This document was prepared by Special Committee 167 of RTCA, Inc. It was approved by RTCA, Inc. on December 1, 1992.

RTCA is an association of aeronautical organizations of the United States of America from both government and industry. Dedicated to the advancement of aeronautics, RTCA seeks sound technical solutions to problems involving the application of electronics and telecommunications to aeronautical operations. Its objective is the resolution of such problems by mutual agreement of its members and participating organizations.

The findings of RTCA are in the nature of recommendations to all organizations concerned. As 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 federal government organizations or agency having statutory jurisdiction over any matters to which the recommendations relate.

The development of these guidelines was jointly accomplished by RTCA SC 167 and the European Organisation for Civil Aviation Equipment (EUROCAE) WG-12 through a consensus process.



Consensus n. Collective opinion or concord; general agreement or accord. [Latin, from *consentire*, to agree]

TABLE OF CONTENTS

		Page
1.0	INTRODUCTION.....	1
1.1	Purpose.....	1
1.2	Scope.....	1
1.3	Relationship to Other Documents	1
1.4	How to Use This Document.....	1
1.5	Document Overview.....	3
2.0	SYSTEM ASPECTS RELATING TO SOFTWARE DEVELOPMENT.....	5
2.1	Information Flow Between System and Software Life Cycle Processes	5
2.1.1	Information Flow from System Processes to Software Processes.....	6
2.1.2	Information Flow from Software Processes to System Processes.....	6
2.2	Failure Condition and Software Level.....	6
2.2.1	Failure Condition Categorization.....	7
2.2.2	Software Level Definitions.....	7
2.2.3	Software Level Determination.....	8
2.3	System Architectural Considerations.....	8
2.3.1	Partitioning.....	9
2.3.2	Multiple-Version Dissimilar Software	9
2.3.3	Safety Monitoring.....	9
2.4	System Considerations for User-Modifiable Software, Option-Selectable Software and Commercial Off-The-Shelf Software	10
2.5	System Design Consideration for Field-Loadable Software	10
2.6	System Requirement Considerations for Software Verification.....	11
2.7	Software Considerations in System Verification	11
3.0	SOFTWARE LIFE CYCLE.....	13
3.1	Software Life Cycle Processes	13
3.2	Software Life Cycle Definition	13
3.3	Transition Criteria Between Processes.....	14
4.0	SOFTWARE PLANNING PROCESS	15
4.1	Software Planning Process Objectives.....	15
4.2	Software Planning Process Activities.....	15
4.3	Software Plans.....	16
4.4	Software Life Cycle Environment Planning	16
4.4.1	Software Development Environment	17
4.4.2	Language and Compiler Consideration.....	17
4.4.3	Software Test Environment.....	18

	Page
4.5	Software Development Standards.....18
4.6	Review and Assurance of the Software Planning Process.....18
5.0	SOFTWARE DEVELOPMENT PROCESSES19
5.1	Software Requirements Process.....19
5.1.1	Software Requirements Process Objectives19
5.1.2	Software Requirements Process Activities19
5.2	Software Design Process20
5.2.1	Software Design Process Objectives20
5.2.2	Software Design Process Activities20
5.2.3	Designing for User-Modifiable Software21
5.3	Software Coding Process.....21
5.3.1	Software Coding Process Objectives.....21
5.3.2	Software Coding Process Activities22
5.4	Integration Process22
5.4.1	Integration Process Objectives22
5.4.2	Integration Process Activities22
5.4.3	Integration Considerations.....23
5.5	Traceability23
6.0	SOFTWARE VERIFICATION PROCESS25
6.1	Software Verification Process Objectives25
6.2	Software Verification Process Activities26
6.3	Software Reviews and Analyses26
6.3.1	Reviews and Analyses of the High-Level Requirements.....27
6.3.2	Reviews and Analyses of the Low-Level Requirements27
6.3.3	Reviews and Analyses of the Software Architecture.....28
6.3.4	Reviews and Analyses of the Source Code28
6.3.5	Reviews and Analyses of the Outputs of the Integration Process29
6.3.6	Reviews and Analyses of the Test Cases, Procedures and Results.....29
6.4	Software Testing Process29
6.4.1	Test Environment.....30
6.4.2	Requirements-Based Test Case Selection30
6.4.2.1	Normal Range Test Cases31
6.4.2.2	Robustness Test Cases31
6.4.3	Requirements-Based Testing Methods31
6.4.4	Test Coverage Analysis33
6.4.4.1	Requirements-Based Test Coverage Analysis33
6.4.4.2	Structural Coverage Analysis33
6.4.4.3	Structural Coverage Analysis Resolution.....33

	Page
7.0	SOFTWARE CONFIGURATION MANAGEMENT PROCESS.....35
7.1	Software Configuration Management Process Objectives35
7.2	Software Configuration Management Process Activities35
7.2.1	Configuration Identification.....35
7.2.2	Baselines and Traceability.....36
7.2.3	Problem Reporting, Tracking and Corrective Action.....36
7.2.4	Change Control37
7.2.5	Change Review37
7.2.6	Configuration Status Accounting.....37
7.2.7	Archive, Retrieval and Release.....38
7.2.8	Software Load Control.....38
7.2.9	Software Life Cycle Environment Control.....39
7.3	Data Control Categories39
8.0	SOFTWARE QUALITY ASSURANCE PROCESS..... 41
8.1	Software Quality Assurance Process Objectives41
8.2	Software Quality Assurance Process Activities41
8.3	Software Conformity Review.....42
9.0	CERTIFICATION LIAISON PROCESS43
9.1	Means of Compliance and Planning43
9.2	Compliance Substantiation.....43
9.3	Minimum Software Life Cycle Data That Is Submitted to Certification Authority.....43
9.4	Software Life Cycle Data Related to Type Design.....44
10.0	OVERVIEW OF AIRCRAFT AND ENGINE CERTIFICATION45
10.1	Certification Basis45
10.2	Software Aspects of Certification.....45
10.3	Compliance Determination45
11.0	SOFTWARE LIFE CYCLE DATA47
11.1	Plan for Software Aspects of Certification.....48
11.2	Software Development Plan.....48
11.3	Software Verification Plan49
11.4	Software Configuration Management Plan50
11.5	Software Quality Assurance Plan.....51
11.6	Software Requirements Standards.....51
11.7	Software Design Standards.....51
11.8	Software Code Standards52
11.9	Software Requirements Data52
11.10	Design Description52
11.11	Source Code53

	Page
11.12 Executable Object Code	53
11.13 Software Verification Cases and Procedures	53
11.14 Software Verification Results	53
11.15 Software Life Cycle Environment Configuration Index.....	53
11.16 Software Configuration Index.....	53
11.17 Problem Reports	54
11.18 Software Configuration Management Records.....	55
11.19 Software Quality Assurance Records.....	55
11.20 Software Accomplishment Summary	55
12.0 ADDITIONAL CONSIDERATIONS	57
12.1 Use of Previously Developed Software	57
12.1.1 Modifications to Previously Developed Software	57
12.1.2 Change of Aircraft Installation	57
12.1.3 Change of Application or Development Environment	57
12.1.4 Upgrading A Development Base	58
12.1.5 Software Configuration Management Considerations	59
12.1.6 Software Quality Assurance Considerations.....	59
12.2 Tool Qualification.....	59
12.2.1 Qualification Criteria for Software Development Tools	60
12.2.2 Qualification Criteria for Software Verification Tools	61
12.2.3 Tool Qualification Data	61
12.2.3.1 Tool Qualification Plan	61
12.2.3.2 Tool Operational Requirements	61
12.2.4 Tool Qualification Agreement	62
12.3 Alternative Methods	62
12.3.1 Formal Methods.....	62
12.3.2 Exhaustive Input Testing.....	63
12.3.3 Considerations for Multiple-Version Dissimilar Software Verification	63
12.3.3.1 Independence of Multiple-Version Dissimilar Software	64
12.3.3.2 Multiple Processor-Related Verification	64
12.3.3.3 Multiple-Version Source Code Verification	65
12.3.3.4 Tool Qualification for Multiple-Version Dissimilar Software	65
12.3.3.5 Multiple Simulators and Verification.....	65
12.3.4 Software Reliability Models	65
12.3.5 Product Service History	65
ANNEX A PROCESS OBJECTIVES AND OUTPUTS BY SOFTWARE LEVEL.....	67
ANNEX B ACRONYMS AND GLOSSARY OF TERMS	79
Acronyms	79

	Page
Glossary	80
APPENDIX A BACKGROUND OF DOCUMENT DO-178.....	A-1
1.0 Prior Document Version History	
2.0 RTCA / EUROCAE Committee Activities in the Production of This Document	
3.0 Summary Of Differences between DO-178B and DO-178A	
APPENDIX B COMMITTEE MEMBERSHIP	B-1
APPENDIX C INDEX OF TERMS.....	C-1
APPENDIX D IMPROVEMENT SUGGESTION FORM	D-1

LIST OF FIGURES AND TABLES

FIGURES

FIGURE 1-1 DOCUMENT OVERVIEW	3
FIGURE 2-1 SYSTEM SAFETY-RELATED INFORMATION FLOW BETWEEN SYSTEM AND SOFTWARE LIFE CYCLE PROCESSES	5
FIGURE 3-1 EXAMPLE OF A SOFTWARE PROJECT USING FOUR DIFFERENT DEVELOPMENT SEQUENCES	14
FIGURE 6-1 SOFTWARE TESTING PROCESS	30

TABLES

TABLE 7-1 SCM PROCESS OBJECTIVES ASSOCIATED WITH CC1 AND CC2 DATA	39
TABLE A-1 SOFTWARE PLANNING PROCESS	68
TABLE A-2 SOFTWARE DEVELOPMENT PROCESSES	69
TABLE A-3 VERIFICATION OF OUTPUTS OF SOFTWARE REQUIREMENTS PROCESS	70
TABLE A-4 VERIFICATION OF OUTPUTS OF SOFTWARE DESIGN PROCESS	71
TABLE A-5 VERIFICATION OF OUTPUTS OF SOFTWARE CODING & INTEGRATION PROCESSES.....	72
TABLE A-6 TESTING OF OUTPUTS OF INTEGRATION PROCESS	73
TABLE A-7 VERIFICATION OF VERIFICATION PROCESS RESULTS	74
TABLE A-8 SOFTWARE CONFIGURATION MANAGEMENT PROCESS	75
TABLE A-9 SOFTWARE QUALITY ASSURANCE PROCESS	76
TABLE A-10 CERTIFICATION LIAISON PROCESS.....	77

THIS PAGE INTENTIONALLY LEFT BLANK

Currently in preview, click buy full version

1 INTRODUCTION

The rapid increase in the use of software in airborne systems and equipment used on aircraft and engines in the early 1980s resulted in a need for industry-accepted guidance for satisfying airworthiness requirements. DO-178, "Software Considerations in Airborne Systems and Equipment Certification," was written to satisfy this need.

This document, now revised in the light of experience, provides the aviation community with guidance for determining, in a consistent manner and with an acceptable level of confidence, that the software aspects of airborne systems and equipment comply with airworthiness requirements. As software use increases, technology evolves and experience is gained in the application of this document, this document will be reviewed and revised. Appendix A contains a history of this document.

1.1 Purpose

The purpose of this document is to provide guidelines 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. These guidelines are in the form of:

- Objectives for software life cycle processes.
- Descriptions of activities and design considerations for achieving those objectives
- Descriptions of the evidence that indicate that the objectives have been satisfied.

1.2 Scope

This document discusses those aspects of airworthiness certification that pertain to the production of software for airborne systems and equipment used on aircraft or engines. In discussing those aspects, the system life cycle and its relationship with the software life cycle is described to aid in the understanding of the certification process. A complete description of the system life cycle processes, including the system safety assessment and validation processes, or aircraft and engine certification process is not intended.

Since certification issues are discussed only in relation to the software life cycle, the operational aspects of the resulting software are not discussed. For example, the certification aspects of user-modifiable data are beyond the scope of this document.

This document does not provide guidelines concerning the structure of the applicant's organization, the relationships between the applicant and its suppliers, or how the responsibilities are divided. Personnel qualification criteria are also beyond the scope of this document.

1.3 Relationship to Other Documents

In addition to the airworthiness requirements, various national and international standards for software are available. In some communities, compliance with these standards may be required. However, it is outside the scope of this document to invoke specific national or international standards, or to propose a means by which these standards might be used as an alternative or supplement to this document

Where this document uses the term "standards," it should be interpreted to mean the use of project specific standards as applied by the airborne system, airborne equipment, engine, or aircraft manufacturer. Such standards may be derived from general standards produced or adopted by the manufacturer for its activities.

1.4 How to Use This Document

These points need to be noted when using this document:

- Explanatory text is included to aid the reader in understanding the topic under discussion. For example, section 2 provides information necessary to understand the interaction