

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

**Guidelines for Communication, Navigation,
Surveillance and Air Traffic Management
(CNS/ATM)
Systems Software Integrity Assurance**

RTCA DO-278
March 5, 2002

Prepared by: SC-190
© 2002 RTCA, Inc.

Copies of this document may be obtained from

RTCA, Inc.

Telephone: 202-833-9333

Facsimile: 202-833-9434

Internet: www.rtca.org

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

FOREWORD

This report was prepared by Special Committee 190 (SC-190) and approved by the RTCA Program Management Committee (PMC) on March 5, 2002.

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 for now 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 to 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 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 announced by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

This page intentionally left blank.

Currently in preview, click buy full version

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	Purpose	1
1.2	Scope	1
1.3	Relationship to Other Documents	1
1.4	Document Overview	2
1.5	How to Use This Document	3
2	SYSTEM ASPECTS RELATING TO CNS/ATM SOFTWARE DEVELOPMENT	5
2.1	Assurance Levels	5
2.2	Additional System Considerations	6
2.2.1	Architectural Considerations	6
2.2.2	System Communication	6
2.2.3	Security	6
2.2.4	Adaptability	6
2.2.5	Cutover (Hot Swapping)	7
2.2.6	Post-Development Life Cycle	7
3	OBJECTIVES FOR CNS/ATM SYSTEMS	9
3.1	Software Planning Process Objectives (<u>Table A-1</u>)	11
3.1.1	Considerations in Applying <u>Table A-1</u> Objectives to CNS/ATM Systems	12
3.2	Software Development Process Objectives (<u>Table A-2</u>)	12
3.2.1	Considerations in Applying <u>Table A-2</u> Objectives to CNS/ATM Systems	14
3.3	Verification of Outputs of Software Requirements Process Objectives (<u>Table A-3</u>)	15
3.3.1	Considerations in Applying <u>Table A-3</u> Objectives to CNS/ATM Systems	15
3.4	Verification of Outputs of Software Design Process Objectives (<u>Table A-4</u>)	16
3.4.1	Considerations in Applying <u>Table A-4</u> Objectives to CNS/ATM Systems	18
3.5	Verification of Outputs of Software Coding and Integration Process Objectives (<u>Table A-5</u>)	19
3.5.1	Considerations in Applying <u>Table A-5</u> Objectives to CNS/ATM Systems	19
3.6	Testing of Outputs of Integration Process Objectives (<u>Table A-6</u>)	20
3.6.1	Considerations in Applying <u>Table A-6</u> Objectives to CNS/ATM Systems	20
3.7	Verification of Verification Process Results Objectives (<u>Table A-7</u>)	21
3.7.1	Considerations in Applying <u>Table A-7</u> Objectives to CNS/ATM	22
3.8	Software Configuration Management (SCM) Process Objectives (<u>Table A-8</u>)	23
3.8.1	Considerations in Applying <u>Table A-8</u> Objectives to CNS/ATM Systems	23
3.9	Software Quality Assurance (SQA) Process Objectives (<u>Table A-9</u>)	24
3.9.1	Considerations in Applying <u>Table A-9</u> Objectives to CNS/ATM	24
3.10	Software Approval Process Objectives (<u>Table A-10</u>)	25
3.10.1	Considerations in Applying <u>Table A-10</u> Objectives to CNS/ATM	25
4	ADDITIONAL CONSIDERATIONS FOR CNS/ATM SOFTWARE	27
4.1	Commercial Off-The-Shelf (COTS) Software	27

4.1.1	Introduction.....	27
4.1.2	Scope of COTS Section	27
4.1.3	SystemAspects Relating to COTS in CNS/ATM Systems	28
4.1.4	COTS Planning Process.....	28
4.1.4.1	COTS Planning Process Objectives	28
4.1.4.2	COTS Planning Process Activities	29
4.1.5	COTS Acquisition Process	30
4.1.5.1	COTS Acquisition Process Objectives.....	31
4.1.5.2	COTS Acquisition Process Activities	31
4.1.6	COTS Verification Process	32
4.1.6.1	COTS Verification Process Objectives.....	32
4.1.6.2	COTS Verification Process Activities	32
4.1.6.3	Use of Service Experience for Assurance credit of COTS Software	32
4.1.7	COTS Configuration Management Process	34
4.1.7.1	COTS Configuration Management Process Objectives.....	34
4.1.7.2	COTS Configuration Management Activities	34
4.1.8	COTS QualityAssurance.....	35
4.1.9	COTS Specific Objectives	35
4.2	Adaptation Data Process.....	36
4.2.1	Adaptation Data Process Objectives.....	37
4.2.2	Adaptation Data Process Activities	37
5	CNS/ATM-SPECIFIC LIFE CYCLE DATA	39
5.1	Plan for Software Aspects of Approval (PSAA).....	39
5.2	Adaptation Data.....	39
5.3	COTS Software Life Cycle Data.....	39
	MEMBERSHIP	41
	APPENDICES	
	APPENDIX A – ACRONYMS AND GLOSSARY OF TERMS.....	A-1
	APPENDIX B – BACKGROUND OF DOCUMENT DO-278/ED-109	B-1
	APPENDIX C – IMPROVEMENT SUGGESTION FORM.....	C-1

LIST OF TABLES

<u>TABLE 2-1</u>	CNS/ATM TO AIRBORNE LEVEL ASSOCIATION.....	6
<u>TABLE A-1</u>	SOFTWARE PLANNING PROCESS	11
<u>TABLE A-2</u>	SOFTWARE PLANNING PROCESS	13
<u>TABLE A-3</u>	SOFTWARE PLANNING PROCESS	15
<u>TABLE A-4</u>	VERIFICATION OF OUTPUTS OF SOFTWARE REQUIREMENTS PRCESS.....	16
<u>TABLE A-5</u>	VERIFICATIONOF OUTPUTSOF SOFTWARE CODING AND INTEGRATION PROCESS	19
<u>TABLE A-6</u>	TESTING OF OUTPUTS OF INTEGRATION PROCESS	20
<u>TABLE A-7</u>	VERIFICATION OF VERIFICATION PROCESS RESULTS	21
<u>TABLE A-8</u>	SOFTWARE CONFIGURATION MANAGEMENT PROCESS	23
<u>TABLE A-9</u>	SOFTWARE QUALITY ASSURANCE PROCESS	24
<u>TABLE A-10</u>	SOFTWARE APPROVAL PROCESS	25
<u>TABLE 4-1</u>	COTS PLANNING PROCESS OBJECTIVES.....	35
<u>TABLE 4-2</u>	COTS ACQUISITION PROCESS OBJECTIVES	36
<u>TABLE 4-3</u>	COTS CONFIGURATION MANAGEMENT PROCESS OBJECTIVE.....	36

LIST OF FIGURES

<u>FIGURE 4-1</u>	REQUIREMENTS INTERSECTION	30
-------------------	---------------------------------	----

This page intentionally left blank.

Currently in preview, click buy full version

1 DO-278/ED-109 INTRODUCTION

The implementation of Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) systems has resulted in increased interdependence of systems providing Air Traffic Services (ATS) and systems onboard aircraft. CNS/ATM systems include ground, airborne, and space-based systems. In order for these systems to perform their intended function while providing an acceptable level of safety, there is a need to define consistent and/or equivalent means of providing integrity assurance for the software in these systems.

1.1 Purpose

This document provides guidelines for the assurance of software contained in non-airborne CNS/ATM systems. DO-178B/ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, defines a set of objectives that are recommended to establish assurance that airborne software has the integrity needed to use in a safety-related application. These objectives have been reviewed, and in some cases, modified for application to non-airborne CNS/ATM systems. This document is intended to be an interpretive guide for the application of DO-178B/ED-12B guidance to non-airborne CNS/ATM systems.

1.2 Scope

This guidance applies to software contained in CNS/ATM systems used in ground or space-based applications shown by a system safety assessment process to affect the safety of aircraft occupants or airframe in its operational environment. The assurance of software resident within the airframe boundaries, including CNS/ATM-related equipment, is addressed by DO-178B/ED-12B.

A description of the safety assessment process is not included in this document. Information on such assessments is available from other industry sources and in related regulatory guidance. Likewise, a complete description of the system life cycle processes, including system validation, as well as CNS/ATM systems approval, is not intended. This guidance is not intended to be a development standard nor a process document.

It should be noted that additional objectives and evidence may be needed for certain elements of CNS/ATM systems for reasons that are beyond the scope of this document (e.g., additional requirements due to the difficulty in servicing satellite systems).

1.3 Relationship to Other Documents

This document is intended to be used in conjunction with DO-178B/ED-12B and related explanatory material found in DO-248B/ED-94B, *Final Report for Clarification of DO-178B/ED-12B 'Software Considerations in Airborne Systems and Equipment Certification'*. Using DO-178B/ED-12B as a basis for this document is intentional and is intended to produce an equivalent level of assurance for the integrity of software in both non-air-