

RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington, DC 20036-3816 USA

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

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 report 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.

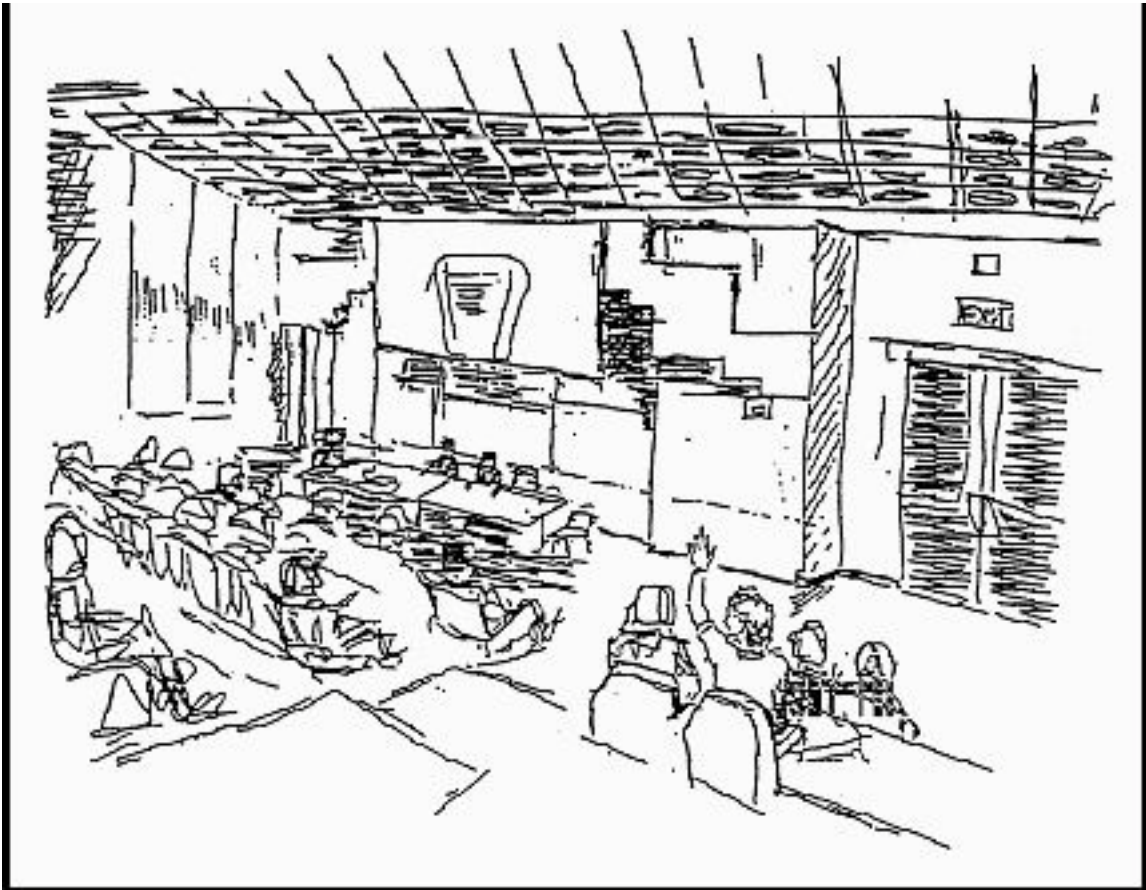


Illustration provided by Pat Neilan, UK CAA

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

TABLE OF CONTENTS

1.0	INTRODUCTION	1
1.1	Purpose	1
1.2	Scope	1
1.3	Relationship to Other Documents	2
1.4	How to Use This Document	2
1.5	Document Overview.....	5
2.0	SYSTEM ASPECTS RELATING TO SOFTWARE DEVELOPMENT.....	7
2.1	System Requirements Allocation to Software.....	7
2.2	Information Flow Between System and Software Life Cycle Processes	8
2.2.1	Information Flow from System Processes to Software Processes	10
2.2.2	Information Flow from Software Processes to System Processes	10
2.2.3	Information Flow between Software Processes and Hardware Processes.....	11
2.3	System Safety Assessment Process and Assurance Level.....	11
2.3.1	Relationship between Software Errors and Failure Conditions.....	12
2.3.2	Assurance Level Definitions	12
2.3.3	Assurance Level Definitions	14
2.3.4	Assurance Level Determination	15
2.4	Architectural Considerations	15
2.4.1	Partitioning	15
2.4.2	Multiple-Version Dissimilar Software	16
2.4.3	Safety Monitoring.....	17
2.5	Additional System Considerations	17
2.5.1	System Communication.....	17
2.5.2	Security.....	17
2.5.3	Adaptability	17
2.5.4	Cutover (Hot Swapping).....	17
2.5.5	Post-Development Life Cycle	18
2.6	Software Considerations in System Life Cycle Processes	18
2.6.1	Adaptation Data Items	18
2.6.2	User-Modifiable Software	19
2.6.3	Commercial-Off-The-Shelf Software.....	20
2.6.4	Option-Selectable Software.....	20
2.6.5	Field-Loadable Software	21
2.6.6	Software Considerations in System Verification.....	21
2.7	System Considerations in Software Life Cycle Processes	22
3.0	SOFTWARE LIFE CYCLE.....	23
3.1	Software Life Cycle Processes	23
3.2	Software Life Cycle Definition	23
3.3	Transition Criteria Between Processes	24
4.0	SOFTWARE PLANNING PROCESS	27
4.1	Software Planning Process Objectives	27
4.2	Software Planning Process Activities.....	27
4.3	Software Plans	28
4.4	Software Life Cycle Environment Planning.....	29
4.4.1	Software Development Environment	30
4.4.2	Language and Compiler Considerations.....	30
4.4.3	Software Test Environment.....	31
4.5	Software Development Standards	31

4.6	Review of the Software Planning Process	32
5.0	SOFTWARE DEVELOPMENT PROCESSES	33
5.1	Software Requirements Process	34
5.1.1	Software Requirements Process Objectives	34
5.1.2	Software Requirements Process Activities	34
5.2	Software Design Process	35
5.2.1	Software Design Process Objectives	35
5.2.2	Software Design Process Activities.....	35
5.2.3	Designing for User-Modifiable Software	36
5.2.4	Designing for Deactivated Code.....	36
5.3	Software Coding Process.....	37
5.3.1	Software Coding Process Objectives.....	37
5.3.2	Software Coding Process Activities	37
5.4	Integration Process	37
5.4.1	Integration Process Objectives	38
5.4.2	Integration Process Activities.....	38
5.5	Software Development Process Traceability.....	39
6.0	SOFTWARE VERIFICATION PROCESS	41
6.1	Purpose of Software Verification	41
6.2	Overview of Software Verification Process Activities.....	42
6.3	Software Reviews and Analyses	43
6.3.1	Reviews and Analyses of High-Level Requirements	43
6.3.2	Reviews and Analyses of Low-Level Requirements.....	44
6.3.3	Reviews and Analyses of Software Architecture	44
6.3.4	Reviews and Analyses of Source Code	45
6.3.5	Reviews and Analyses of the Outputs of the Integration Process	46
6.4	Software Testing.....	46
6.4.1	Test Environment	48
6.4.2	Requirements-Based Test Selection	48
6.4.2.1	Normal Range Test Cases	48
6.4.2.2	Robustness Test Cases	49
6.4.3	Requirements-Based Testing Methods.....	49
6.4.4	Test Coverage Analysis	51
6.4.4.1	Requirements-Based Test Coverage Analysis	51
6.4.4.2	Structural Coverage Analysis.....	52
6.4.4.3	Structural Coverage Analysis Resolution	52
6.4.5	Reviews and Analyses of Test Cases, Procedures, and Results	53
6.5	Software Verification Process Traceability.....	53
6.6	Verification of Adaptation Data Items	54
7.0	SOFTWARE CONFIGURATION MANAGEMENT PROCESS	55
7.1	Software Configuration Management Process Objectives	55
7.2	Software Configuration Management Process Activities.....	56
7.2.1	Configuration Identification	56
7.2.2	Baselines and Traceability.....	57
7.2.3	Problem Reporting, Tracking, and Corrective Action.....	57
7.2.4	Change Control.....	58
7.2.5	Change Review.....	58
7.2.6	Configuration Status Accounting	58
7.2.7	Archive, Retrieval, and Release	59
7.3	Data Control Categories	59
7.4	Software Load Control	60

7.5	Software Life Cycle Environment Control.....	61
8.0	SOFTWARE QUALITY ASSURANCE PROCESS	63
8.1	Software Quality Assurance Process Objectives	63
8.2	Software Quality Assurance Process Activities	63
8.3	Software Conformity Review	64
9.0	APPROVAL LIAISON PROCESS	67
9.1	Means of Compliance and Planning.....	67
9.2	Compliance Substantiation.....	67
9.3	Minimum Software Life Cycle Data Submitted to Approval Authority	68
9.4	Software Life Cycle Data Related to the Approval Process.....	68
10.0	OVERVIEW OF CNS/ATM SYSTEM APPROVAL PROCESS	69
10.1	Approval Basis	69
10.2	Software Aspects of Approval.....	69
10.3	Compliance Determination.....	69
11.0	SOFTWARE LIFE CYCLE DATA.....	71
11.1	Plan for Software Aspects of Approval.....	72
11.2	Software Development Plan	73
11.3	Software Verification Plan	73
11.4	Software Configuration Management Plan	74
11.5	Software Quality Assurance Plan.....	75
11.6	Software Requirements Standards.....	76
11.7	Software Design Standards.....	76
11.8	Software Code Standards	77
11.9	Software Requirements Data.....	77
11.10	Design Description	78
11.11	Source Code	78
11.12	Executable Object Code	79
11.13	Software Verification Cases and Procedures.....	79
11.14	Software Verification Results.....	79
11.15	Software Life Cycle Environment Configuration Index	79
11.16	Software Configuration Index	80
11.17	Problem Reports	80
11.18	Software Configuration Management Records	81
11.19	Software Quality Assurance Records.....	81
11.20	Software Accomplishment Summary.....	81
11.21	Trace Data	82
11.22	Adaptation Data Item File	83
12.0	ADDITIONAL CONSIDERATIONS.....	85
12.1	Use of Previously Developed Software.....	85
12.1.1	Modifications to Previously Developed Software.....	85
12.1.2	Reuse of Previously Approved Software in a CNS/ATM System	86
12.1.3	Change of Application or Development Environment	86
12.1.4	Upgrading a Development Baseline	87
12.1.5	Software Configuration Management Considerations.....	88
12.1.6	Software Quality Assurance Considerations	88
12.2	Tool Qualification	88
12.2.1	Determining if Tool Qualification is Needed	88
12.2.2	Determining the Tool Qualification Level	89
12.2.3	Tool Qualification Process	89
12.3	Alternative Methods.....	90

12.3.1	Exhaustive Input Testing	90
12.3.2	Considerations for Multiple-Version Dissimilar Software Verification.....	90
12.3.2.1	Independence of Multiple-Version Dissimilar Software	92
12.3.2.2	Multiple Processor-Related Verification	92
12.3.2.3	Multiple-Version Source Code Verification	92
12.3.2.4	Tool Qualification for Multiple-Version Dissimilar Software.....	92
12.3.2.5	Multiple Simulators and Verification	93
12.3.3	Software Reliability Models.....	93
12.3.4	Service Experience	93
12.3.4.1	Relevance of Service Experience.....	94
12.3.4.2	Sufficiency of Accumulated Service Experience.....	95
12.3.4.3	Collection, Reporting, and Analysis of Problems Found During Service Experience...	95
12.3.4.4	Service Experience Information to be Included in the Plan for Software Aspects of Approval.....	97
12.4	Commercial Off-The-Shelf Software	98
12.4.1	Introduction	98
12.4.1.1	Purpose.....	98
12.4.1.2	Scope.....	98
12.4.1.3	Overview of Approach.....	99
12.4.2	System Aspects of COTS Software.....	100
12.4.2.1	The COTS Software Integrity Assurance Case.....	100
12.4.3	COTS Software Planning Process	101
12.4.3.1	COTS Software Planning Process Objectives.....	101
12.4.3.2	COTS Software Planning Process Activities	101
12.4.4	COTS Software Acquisition Process.....	102
12.4.4.1	COTS Software Acquisition Process Objectives	104
12.4.4.2	COTS Software Acquisition Process Activities.....	104
12.4.5	COTS Software Verification Process	105
12.4.5.1	COTS Software Verification Process Objectives	105
12.4.5.2	COTS Software Verification Process Activities	106
12.4.6	COTS Software Configuration Management Process	106
12.4.6.1	COTS Software Configuration Management Process Objectives.....	106
12.4.6.2	COTS Software Configuration Management Process Activities	107
12.4.7	COTS Software Quality Assurance Process.....	107
12.4.8	Software Life Cycle Data	107
12.4.8.1	COTS Software Integrity Assurance Case.....	108
12.4.9	Changes to COTS from an Earlier Baseline.....	108
12.4.10	Additional Process Objectives and Outputs by Assurance Level for COTS Software....	109
12.4.11	Alternative Methods for Providing Assurance of COTS Software	113
12.4.11.1	Definitions for Alternative Methods of COTS Software Assurance Strategies.....	113
12.4.11.2	Applicability of Alternative Methods to Objectives	116
ANNEX A	PROCESS OBJECTIVES AND OUTPUTS BY ASSURANCE LEVEL.....	125
ANNEX B	- ACRONYMS AND GLOSSARY OF TERMS.....	137
APPENDIX A	– BACKGROUND OF DO-278/ED-109 DOCUMENT	A-1
APPENDIX B	– COMMITTEE MEMBERSHIP	B-1

LIST OF FIGURES

Figure 1-1 Document Overview	5
Figure 2-1 Information Flow Between System and Software Life Cycle Processes	9
Figure 2-2 Sequence of Events for Software Error Leading to a Failure Condition.....	12
Figure 3-1 Example of a Software Project Using Four Different Development Sequences	24
Figure 6-1 Software Testing Activities.....	47
Figure 12-1 Requirements Intersection.....	103

LIST OF TABLES

Table 2-1 Example Failure Condition Category Descriptions.....	13
Table 2-2 CNS/ATM to Airborne Level Association.....	14
Table 7-1 SCM Process Activities Associated with CC1 and CC2 Data.....	60
Table 12-1 Tool Qualification Level Determination	89
Table 12-2 COTS Software Planning Objectives	110
Table 12-3 COTS Software Acquisition Process Objectives.....	111
Table 12-4 COTS Software Verification Process Objectives	112
Table 12-5 COTS Software Configuration Management Process Objectives	112
Table A-1 Software Planning Process	126
Table A-2 Software Development Processes.....	127
Table A-3 Verification of Outputs of Software Requirements Process.....	128
Table A-4 Verification of Outputs of Software Design Process.....	129
Table A-5 Verification of Outputs of Software Coding and Integration Processes.....	130
Table A-6 Testing of Outputs of Integration Process	131
Table A-7 Verification of Verification Process Results	132
Table A-8 Software Configuration Mangement Process.....	133
Table A-9 Software Quality Assurance Process	134
Table A-10 Software Approval Process.....	135

This Page Intentionally Left Blank

1.0 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 can include ground, airborne, and space-based elements. 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 (SW) in these systems. DO-278, “Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems,” was written to satisfy the non-airborne (that is, ground and space) aspects of this need. Appendix A provides the background of this document.

1.1 Purpose

The purpose of this document is to provide guidance for the production of non-airborne software for CNS/ATM systems and equipment that performs its intended function with a level of confidence in safety that complies with approval requirements. This guidance includes:

- Objectives for software life cycle processes.
- Activities that provide a means for satisfying those objectives.
- Descriptions of the evidence in the form of software life cycle data that indicate that the objectives have been satisfied.
- Variations in the objectives, independence, software life cycle data, and control categories by assurance level (AL).
- Additional considerations (for example, previously developed software) that are applicable to certain applications.
- Definition of terms provided in the glossary.

In addition to guidance, supporting information is provided to assist the reader’s understanding.

1.2 Scope

This document discusses those aspects of approval that pertain to the production of software for CNS/ATM systems. 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 approval process. A complete description of the system life cycle processes, including the system safety assessment and validation processes, or the approval process is not intended.

The guidance contained in this document does not define or imply the level of involvement of an approval authority in an approval process. To understand approval authority involvement, the applicant should refer to applicable regulations and guidance material issued by the relevant approval authority.