

RTCA, Inc.
1140 Connecticut Avenue, NW, Suite 1020
Washington, D.C. 20036-4001 USA

**Design Assurance Guidance
For Airborne Electronic Hardware**

RTCA/DO-254
April 19, 2000

Prepared by: SC-180
© 2000, 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 180 (SC-180). It was approved by the RTCA Program Management Committee on April 19, 2000.

RTCA SC-180 and the European Organization for Civil Aviation Equipment (EUROCAE) WG-46 jointly accomplished the development of this guidance through the consensus process.

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.

EXECUTIVE SUMMARY

The development and use of complex electronic hardware by the aviation industry has created new safety and certification concerns. In response, RTCA SC-180 and EUROCAE WG-46 were formed. WG-46 and SC-180 agreed to become a joint committee early in the development of this document. This joint committee was chartered to develop clear and consistent design assurance guidance for electronic airborne hardware such that it safely performs its intended functions.

Electronic airborne hardware includes line replaceable units, circuit board assemblies, application specific integrated circuits, programmable logic devices, etc. This guidance is applicable to current, new, and emerging technologies.

The guidance in this document is intended to be used by aircraft manufacturers and suppliers of electronic hardware items for use in aircraft systems. The hardware design life cycle processes are identified. Objectives and activities for each process are described. The guidance is applicable to all hardware design assurance levels as determined by the system safety assessment.

In the development of this document, the committee considered other industry documents including Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) document ARP4754/EUROCAE ED-79, Certification Considerations for Highly Integrated or Complex Aircraft Systems; SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment; and RTCA DO-178/EUROCAE ED-12, Software Considerations in Airborne Systems and Equipment Certification.

TABLE OF CONTENTS

FOREWORD.....	i
EXECUTIVE SUMMARY.....	ii
1.0 INTRODUCTION.....	1
1.1 Purpose	1
1.2 Scope	2
1.3 Relationship to Other Documents.....	2
1.4 Related Documents	3
1.5 How to Use This Document.....	3
1.6 Complexity Considerations	5
1.7 Alternative Methods or Processes	5
1.8 Document Overview.....	6
2.0 SYSTEM ASPECTS OF HARDWARE DESIGN ASSURANCE	9
2.1 Information Flow	10
2.1.1 Information Flow from System Development Process to Hardware Design Life Cycle Process	11
2.1.2 Information Flow from Hardware Design Life Cycle Process to System Development Process	11
2.1.3 Information Flow between Hardware Design Life Cycle Process and Software Life Cycle Process	12
2.2 System Safety Assessment Processes	12
2.3 Hardware Safety Assessment	15
2.3.1 Hardware Safety Assessment Considerations.....	15
2.3.2 Quantitative Assessment of Random Hardware Faults.....	16
2.3.3 Qualitative Assessment of Hardware Design Errors and Upsets.....	16
2.3.4 Design Assurance Considerations for Hardware Failure Condition Classification ...	17
3.0 HARDWARE DESIGN LIFE CYCLE	21
3.1 Hardware Design Life Cycle Processes.....	21
3.2 Transition Criteria	21
4.0 PLANNING PROCESS.....	23
4.1 Planning Process Objectives.....	23
4.2 Planning Process Activities	23
5.0 HARDWARE DESIGN PROCESSES	27
5.1 Requirements Capture Process.....	29
5.1.1 Requirements Capture Objectives.....	29
5.1.2 Requirements Capture Activities.....	30
5.2 Conceptual Design Process.....	31
5.2.1 Conceptual Design Objectives	32
5.2.2 Conceptual Design Activities.....	32
5.3 Detailed Design Process	32
5.3.1 Detailed Design Objectives	32
5.3.2 Detailed Design Process Activities	33
5.4 Implementation Process	33

5.4.1	Implementation Objectives	34
5.4.2	Implementation Activities	34
5.5	Production Transition Process	34
5.5.1	Production Transition Objectives.....	34
5.5.2	Production Transition Activities	35
5.6	Acceptance Test	35
5.7	Series Production.....	36
6.0	VALIDATION AND VERIFICATION PROCESS.....	37
6.1	Validation process	37
6.1.1	Validation Process Objectives	38
6.1.2	Validation Process Activities	38
6.2	Verification Process	39
6.2.1	Verification Process Objectives.....	39
6.2.2	Verification Process Activities.....	40
6.3	Validation and Verification Methods	40
6.3.1	Test.....	41
6.3.2	Analysis.....	41
6.3.3	Reviews.....	42
6.3.3.1	Requirements Review.....	43
6.3.3.2	Design Review.....	44
7.0	CONFIGURATION MANAGEMENT PROCESS	47
7.1	Configuration Management Objectives.....	47
7.2	Configuration Management Activities.....	47
7.2.1	Configuration Identification.....	47
7.2.2	Baseline Establishment.....	48
7.2.3	Problem Reporting, Tracking and Corrective Action.....	48
7.2.4	Change Control	49
7.2.5	Release, Archive and Retrieve	50
7.3	Data Control Categories.....	51
8.0	PROCESS ASSURANCE.....	53
8.1	Process Assurance Objectives	53
8.2	Process Assurance Activities	53
9.0	CERTIFICATION LIAISON PROCESS.....	55
9.1	Means of Compliance and Planning	55
9.2	Compliance Substantiation.....	56
10.0	HARDWARE DESIGN LIFE CYCLE DATA	57
10.1	Hardware Plans	58
10.1.1	Plan for Hardware Aspects of Certification.....	58
10.1.2	Hardware Design Plan.....	59
10.1.3	Hardware Validation Plan.....	60
10.1.4	Hardware Verification Plan.....	60
10.1.5	Hardware Configuration Management Plan.....	61
10.1.6	Hardware Process Assurance Plan	61
10.2	Hardware Design Standards and Guidance.....	62
10.2.1	Requirements Standards.....	62

10.2.2	Hardware Design Standards.....	62
10.2.3	Validation and Verification Standards.....	63
10.2.4	Hardware Archive Standards	63
10.3	Hardware Design Data.....	63
10.3.1	Hardware Requirements.....	63
10.3.2	Hardware Design Representation Data.....	63
10.3.2.1	Conceptual Design Data.....	64
10.3.2.2	Detailed Design Data	64
10.3.2.2.1	Top-Level Drawing.....	64
10.3.2.2.2	Assembly Drawings	64
10.3.2.2.3	Installation Control Drawings	65
10.3.2.2.4	Hardware/Software Interface Data	65
10.4	Validation and Verification Data.....	65
10.4.1	Traceability Data.....	66
10.4.2	Review and Analysis Procedures.....	66
10.4.3	Review and Analysis Results.....	66
10.4.4	Test Procedures.....	67
10.4.5	Test Results.....	67
10.5	Hardware Acceptance Test Criteria	67
10.6	Problem Reports.....	68
10.7	Hardware Configuration Management Records	68
10.8	Hardware Process Assurance Records.....	68
10.9	Hardware Accomplishment Summary.....	68
11.0	ADDITIONAL CONSIDERATIONS.....	71
11.1	Use of Previously Developed Hardware	71
11.1.1	Modifications to Previously Developed Hardware.....	71
11.1.2	Change of Aircraft Installation.....	71
11.1.3	Change of Application or Design Environment.....	72
11.1.4	Upgrading a Design Baseline.....	72
11.1.5	Additional Configuration Management Considerations	73
11.2	Commercial-Off-The-Shelf (COTS) Components Usage.....	73
11.2.1	Electronic Component Management for COTS Components.....	73
11.2.2	COTS Component Procurement	74
11.3	Product Service Experience	74
11.3.1	Product Service Experience Data Acceptability Criteria	74
11.3.2	Assessment of Product Service Experience Data	75
11.3.3	Product Service Experience Assessment Data	75
11.4	Tool Assessment and Qualification	76
11.4.1	Tool Assessment and Qualification Process.....	76
11.4.2	Tool Assessment and Qualification Data	79
MEMBERSHIP	81
APPENDIX A.....	MODULATION OF HARDWARE LIFE CYCLE DATA BASED ON HARDWARE DESIGN ASSURANCE LEVEL	
APPENDIX B.....	DESIGN ASSURANCE CONSIDERATIONS FOR LEVEL A AND B FUNCTIONS	

APPENDIX C.....GLOSSARY OF TERMS

APPENDIX D.....ACRONYMS

Currently in preview, click buy full version

FIGURES

Figure 1-1	Document Overview.....	7
Figure 2-1	Relationships Among Airborne Systems, Safety Assessment, Hardware and Software Processes	9
Figure 2-2	System Development Processes	10
Figure 2-3	Decision Making Process for Selecting the Hardware Design Assurance Strategy.....	18
Figure 5-1	Hardware Design Life Cycle.....	28
Figure 11-1	Design and Verification Tool Assessment and Qualification.....	77

TABLES

Table 2-1	Hardware Design Assurance Level Definitions and their Relationships to Systems Development Assurance Level.....	14
Table 5-1	Typical ASIC/PLD Process Mapping	29
Table 7-1	Configuration Management Process Activities Associated with HC1 and HC2	51
Table A-1	Hardware Life Cycle Data by Hardware Design Assurance Level and Hardware Control Category.....	1

This Page Intentionally Left Blank

1.0 INTRODUCTION

The use of increasingly complex electronic hardware for more of the safety critical aircraft functions generates new safety and certification challenges. These challenges arise from a concern that said aircraft functions may be increasingly vulnerable to the adverse effects of hardware design errors that may be increasingly difficult to manage due to the increasing complexity of the hardware. To counteract this perceived escalation of risk it has become necessary to ensure that the potential for hardware design errors is addressed in a more consistent and verifiable manner during both the design and certification processes.

As airborne electronic hardware becomes more complex, technology evolves and experience is gained in the application and use of the procedures described in this document, this document will be revised and reviewed consistent with approved RTCA/EUROCAE procedures.

1.1 Purpose

This document has been prepared to assist organizations by providing design assurance guidance for the development of airborne electronic hardware such that it safely performs its intended function, in its specified environments. This guidance should be equally applicable to current, new, and evolving technologies. The purposes of this document are to:

1. Define hardware design assurance objectives.
2. Describe the basis for these objectives to help ensure correct interpretation of the guidance.
3. Provide descriptions of the objectives to allow the development of means of compliance with this and other guidance.
4. Provide guidance for design assurance activities to meet the design assurance objectives.
5. Allow flexibility in choice of processes necessary to meet the objectives of this document including improvements, as new process technologies become available.

This document recommends the activities that should be performed in order to meet design assurance objectives, rather than detailing how a design should be implemented.

The philosophy used to generate this guidance document is one of a top-down perspective based on the system functions being performed by electronic hardware and not a bottom-up perspective or one based solely on the specific hardware components used to implement the function. A top-down approach is more effective at addressing safety design errors by facilitating informed system and hardware design decisions, and efficient and effective verification processes. For example, verification should be performed at the highest hierarchical level of the system, assembly, and subassembly, component or hardware item at which compliance of the hardware item to its requirements can be achieved and the verification objectives satisfied.