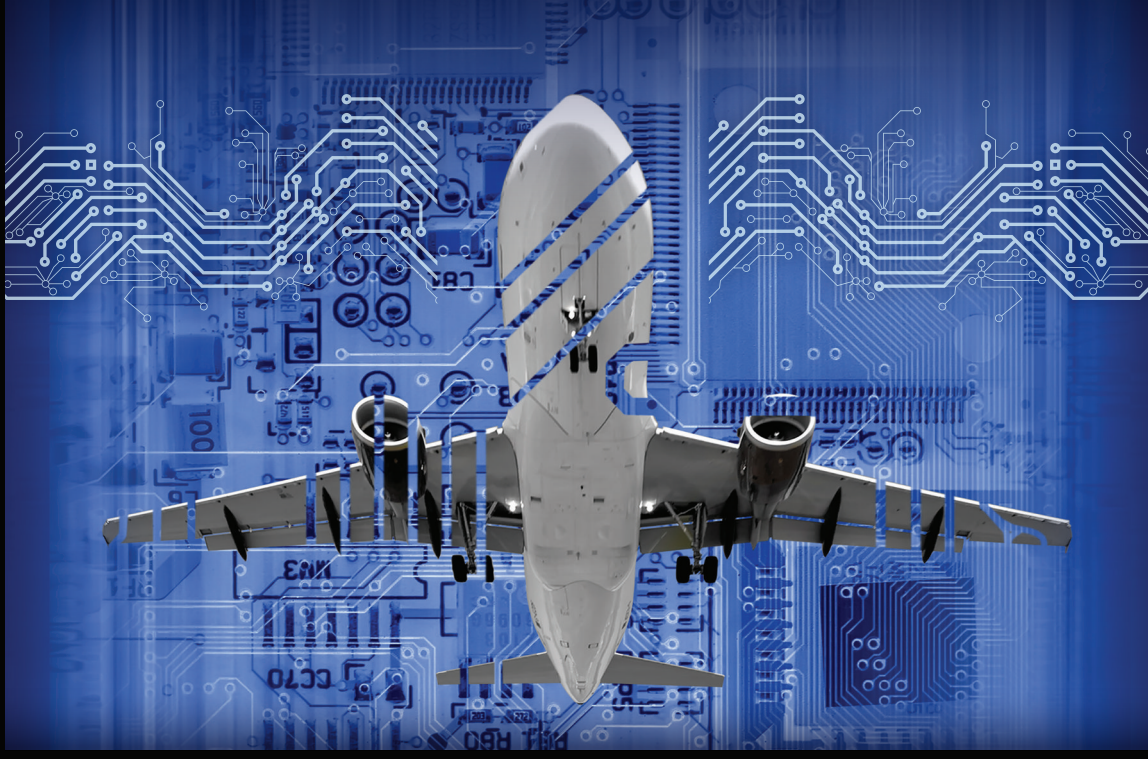

Airborne Electronic Hardware Design Assurance

A Practitioner's Guide to RTCA/DO-254

Randall Fulton • Roy Vandermolen

CRC Press
Taylor & Francis Group

Documents
Document Sharing Library
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Airborne Electronic Hardware Design Assurance

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Airborne Electronic Hardware Design Assurance

A Practitioner's Guide to RTCA/DO-254

Randall Fulton
SOFTWAIR ASSURANCE, INC.
REDWOOD CITY, CA

Roy Vandermolen
HARDWAIR ASSURANCE
BOUNTIFUL, UT

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2015 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20141024

International Standard Book Number-13: 978-1-4822-0606-7 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Contents

Preface ix
Acknowledgments xi
Authors xiii

Chapter 1 Introduction to RTCA/DO-254 1

Design Assurance Level 2
DO-254 and DO-178B 4
Overview of DO-254 7
What Does It Mean to Me? 13
References 15
Further Information 15

Chapter 2 Regulatory Background 17

Means of Compliance 21
Guidance Materials 25
Issue Papers 26
Orders 27
References 29

Chapter 3 Planning 31

Plan for Hardware Aspects of Certification 38
Tool Assessment and Qualification 46
Alternative Methods 47
Schedule 47
FAA Order 8110.105 Aspects 48
Hardware Design Plan 49
Hardware Validation Plan 52
Hardware Verification Plan 52
Hardware Configuration Management Plan 54
Hardware Process Assurance Plan 58
Hardware Standards 61
Validation and Verification Standards 64
Hardware Archive Standards 65
Submittals and Coordination 65
References 66

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Chapter 4 Requirements 67

Why Use Requirements? 69
Requirements Author 70
System Requirements 72
Types of Requirements for Electronic Hardware 74
Allocation and Decomposition 85
Timing and Performance Specifications 88
Writing Requirements 89
PLD Requirements 93
Electronic Hardware Requirements 97
Requirements Organization 101
Systems, Hardware, and Software 102

Chapter 5 Validation 107

Derived Requirements 107
Creating Derived Requirements 109
Validation Methods 111

Chapter 6 Philosophy 101—Design Assurance Through Design Practice 113

DATDP 116
Device Selection 117
Design Philosophy 119
Design Execution 127

Chapter 7 Verification 135

Functional Failure Path Analysis 136
Appendix B Additional Verification 141
Independence 147
Review 148
Analysis 151
Test 154
Test Case Selection Criteria 154
Test Cases and Requirements 163

Chapter 8 Process Assurance 171

Sampling 171
Conformity 172
Audits 173
Audits of Configuration Management 173
SOI Audit Dry Run 176
Inspections 176
Deviations 177
Sub-Tier Supplier Oversight 177

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Chapter 9 Configuration Management 179

Why Configuration Management? 180
Data Control Categories 182
Configuration Management Activities 182
Configuration Identification 183
Baselines 184
Baseline Traceability 184
Problem Reports 185
Change Control 190
Release 192
Retrieval 192
Data Retention 194
Protection against Unauthorized Changes 195
Media Selection, Refreshing, Duplication 195
References 196

Chapter 10 Additional Considerations 197

Previously Developed Hardware 197
Commercial Off-the-Shelf Components Usage 199
Product Service Experience 203
Tool Assessment and Qualification 205

Chapter 11 Summary 213

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Preface

This book was inspired by, and evolved from, the experience we gained while teaching the DO-254 class at RTCA in Washington, D.C. and at numerous companies throughout the United States and abroad. In some respects it is the logical extension of our DO-254 class, and in fact some of the material in this book shares common origins.

Most of this book, however, is a testimony of the lessons learned and wisdom gained from many years of first-hand experience in the design, verification, and approval of airborne electronics and software, including some of the very first projects in which DO-254 was applied, and also including the very first projects where DO-254 was applied at the LRU level. The early years of DO-254 were seminal to us for revealing not only the difficulties inherent in applying a comprehensive document like DO-254 to a very narrow target, but also for the labor pains endemic throughout the industry as it struggled to understand—let alone comply with—this new way of doing business. Pain is a hard but effective teacher, so by any measure those of us who experienced those years should be geniuses by now.

As we and the rest of the industry adjusted and eventually mastered both the document and its ramifications, we were able to discern the practices and techniques that complemented the processes in DO-254 and therefore worked best in this new environment. This book documents the practices and techniques that we have identified and witnessed as being compatible with the intent of DO-254, and which thus make the road to compliance and eventual approval as direct, efficient, and effective as possible. While most of the material in this book is written from the perspective of programmable logic devices (à la FAA Advisory Circular 20-152), all of it can easily be extended to encompass the rest of an electronic system in the way DO-254 was actually intended to be used.

That said, there is only so much that can be documented, let alone taught, in one book. The concepts and techniques that we introduce here are presented in their most basic and fundamental form; actually mastering the topic can only be accomplished through first-hand experience in developing an electronic system in a certification program. While this means that newcomers to the world of DO-254 compliance may experience the sometimes difficult initiation that was sustained by those who went before them, it is our fond desire that they will embrace the material in this book to minimize the cost—both literal and metaphorical—to its lowest possible level. After all, a wise person will learn from his own mistakes, but a wiser person will learn from other peoples' mistakes. This book is built upon the mistakes and successes of many people all over the world, so it offers the wiser person the means to learn from the mistakes of a distinguished club of professionals who had to learn their lessons through experience, hardship, and even trial and error. Through this book the reader

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

can access an enormous compendium of experiences without having to experience the associated travail first hand.

It is our desire, and our motivation for writing this book, to make that wisdom available to all of the developers of safety critical electronic hardware to minimize the needless repetition of the difficulty of those early years, and of course to make modern aircraft as safe and reliable as possible.

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Acknowledgments

This book is dedicated to all the engineers, managers, and personnel we encounter in the trainings, consulting, development programs, and compliance programs that we have and will participate in. We would like to express our utmost gratitude to all those people who have taken the time to help us further our understanding and application of design assurance in the realm of safety critical system and electronics development.

We also thank our partners, friends, and colleagues for their support in this effort.

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Authors

Randall Fulton is an FAA Consultant DER with over 36 years of Electrical Engineering experience emphasizing software and electronic hardware development and verification. Randall has a Bachelor of Science in Electrical Engineering from the Pennsylvania State University and earned his Federal Aviation Administration Designated Engineering Representative credentials in software and programmable logic devices while working at Boeing Commercial Aircraft. As a Designated Engineering Representative, Randall has had approval authority for programmable logic devices since 1997 and has worked numerous Part 23 and Part 25 certification programs with field programmable gate arrays, application-specific integrated circuits (ASIC), and software. Randall, along with Roy Vandermolen, taught the DO-254 practitioners course for RTCA in Washington, D.C. from 2006 to 2009. Randall has also taught the Airborne Electronic Hardware Job Functions class for the Federal Aviation Administration Academy in Oklahoma City. Randall works as a Consultant DER through his company SoftwAir Assurance, Inc.

Roy Vandermolen is an electronics design engineer with over 35 years of experience in electronics ranging from vacuum tubes to programmable logic devices, but has spent the majority of that time designing and verifying programmable logic devices and the circuit cards that employ them. Roy has a Bachelor of Science in Electrical Engineering from the Massachusetts Institute of Technology (MIT), and is currently a Staff Engineer and Certification Manager for electronic flight control systems at Moog Aircraft, and an airborne electronics hardware Outside Boeing Authorized Representative (OBAR) for Boeing Commercial Aircraft. Roy has worked in a variety of engineering environments including research laboratories, educational institutions, military R&D facilities, and commercial aircraft flight controls manufacturers. In his career at Moog Aircraft Roy has been involved in the design, verification, and certification of numerous Level A flight control systems. Roy, along with Randall Fulton, taught the DO-254 practitioners course for RTCA in Washington, D.C. from 2006 to 2009.

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

1 Introduction to RTCA/DO-254

RTCA DO-254 (also known as EUROCAE ED-80), *Design Assurance Guidance for Airborne Electronic Hardware*,[1] was prepared jointly by RTCA Special Committee 180 and EUROCAE Working Group 46, and was subsequently published by RTCA and EUROCAE in April 2000. These industry working groups were formed in the 1990s and took seven years to create DO-254.

DO-254 is not a technical manual, nor is it an engineering cookbook. It does not prescribe the design characteristics of electronic circuits or components, nor does it contain design standards. In fact, it contains virtually no technical information that an engineer can use to guide a circuit design. Instead, it provides guidance on the processes and methodologies that should be applied in the development and verification of electronic hardware to achieve an acceptable level of confidence that the end hardware functions correctly and will be in compliance with airworthiness requirements. While it can be argued that some aspects of a design can be influenced by the desire to facilitate the design and verification methodologies contained in DO-254, there are actually no design features that must or must not exist solely because of the need to comply with it.

The guidance in DO-254 represents industry consensus on the best practices that will ensure that electronic hardware is developed and verified in a way that is appropriate for its design assurance level (DAL)—often shortened to "Level"—and will ensure, to a realistic level, a safe and reliable product. The supporting processes defined in DO-254 (configuration management, process assurance, and validation/verification) are particularly effective in controlling the introduction of design errors as well as identifying errors that are inevitably introduced despite best efforts to the contrary. DO-254 describes the objectives for each phase of a typical electronic hardware development life cycle and describes the activities usually associated with the life cycle phase.

The genesis of DO-254 stems from concerns that as electronics technology rapidly evolved, enabling systems to become more complex and to host more functionality, proving that these systems were safe and reliable was becoming more and more difficult. Most of the electronic systems and programmable logic devices (PLDs) that are used on modern aircraft are well beyond our ability to prove safe through quantitative analysis, and in the absence of this avenue of design assurance, the only other viable means of establishing the necessary design assurance is to use structured and disciplined processes and methodologies during their development. The advantages of using this means are, first, that the processes and methodologies force designers to create a design in a logical and systematic (and therefore repeatable) manner, and second, they create a type of transparency in the design and its project by enforcing

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

a high level of documentation and traceability that, while inconvenient on the surface, has repeatedly proven its worth over the long-term life of a design. Like them or not, the best practices in DO-254 can, particularly in the long run, be a project's best friend.

The guidance in DO-254 was written to apply to all complex electronic hardware that performs safety-critical system functions. While DO-254 discusses PLDs, they are considered within the context of system and equipment development, and not necessarily as the only aspect of the system that should use the guidance in DO-254. When the Federal Aviation Administration (FAA) published its Advisory Circular (AC) 20-152,[2] which approved DO-254 as an acceptable (but not the only) means of satisfying the Federal Aviation Regulations (FARs) for PLDs, it essentially reduced the application of DO-254's guidance to a small subset of its original scope.

Narrowing the focus of DO-254 from the system level to the component level can be problematic due to the need to interpret and apply electronic system guidance to singular components within the system. Examples of potential problems include determining the scope of the life cycle data, determining how to interpret and apply DO-254 Table A-1 to PLD life cycle data, and sorting out which activities and aspects apply at the component level as opposed to the system level (such as acceptance tests, environmental tests, functional failure path analysis, and traceability to elements in the hardware implementation, none of which are entirely practical at the component level). There are also boundary issues that arise: much of DO-254's overall effectiveness relies upon implementing all of its guidance to all levels of a system, which creates a seamless interconnection and flow of processes and data between all levels of the system (line replaceable unit [LRU], sub-assemblies, circuit card assemblies [CCA], and component [typically a PLD]). When one level of the system is singled out for the isolated application of DO-254, it loses this flow to the other levels, creating a discontinuity in both processes and data that can, if not properly anticipated, potentially render much of the design assurance activities ineffective or meaningless. Applying DO-254 only at the PLD level can be made to work through judicious interpretation and tailoring, but in the end the document is most easily comprehended and most effectively applied according to the perspective for which it was conceived and written, and ultimately for which it was intended to be applied, in other words throughout the entire system.

DESIGN ASSURANCE LEVEL

DO-254 defines five levels for the design assurance of airborne electronic systems. These five design assurance levels are defined as levels A through E, where A is the most stringent and E is the least. These five levels correspond to the five classifications of failure conditions defined in the regulatory materials that govern the certification of airborne systems and equipment.

Table 1.1 identifies the five hazard classifications and maps them to their corresponding design assurance level, the required probability of failure per flight hour for equipment of each level, and a description of the hazard. The hazard classifications are described with respect to the effect that a failure of the system or equipment will have on the aircraft, its occupants, its safety margins, and the ability of

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

TABLE 1.1
Design Assurance Level and Hazard Classification

Failure Classification	Hardware Design Assurance Level	Probability of Failure per Flight Hour	Hazard Description
Catastrophic	Level A	10^{-9}	Prevents continued safe flight and landing.
Hazardous/ Severe-Major	Level B	10^{-7}	• Serious or fatal injuries to small number of occupants. • Reduces aircraft capabilities or crew's ability to deal with adverse operating conditions. • Higher crew workload. • Large reduction in safety margins.
Major	Level C	10^{-5}	• Possible injuries to occupants. • Reduces aircraft capabilities or crew's ability to deal with adverse operating conditions. • Increase in crew workload. • Significant reduction in safety margins.
Minor	Level D	10^{-3}	• Possible inconvenience to occupants. • Reduces aircraft capabilities or crew's ability to deal with adverse operating conditions. • Slight increase in crew workload. • Slight reduction in safety margins.
None	Level E	N/A	• No effect on operational capabilities. • No crew workload impact.

its crew to deal with adverse operating conditions. The most severe classification is *catastrophic* (level A), indicating that a failure of level A equipment will, for all practical purposes, result in a catastrophic hull loss of the aircraft. The least severe is *no effect*, indicating that a failure will affect neither the aircraft's operational capabilities nor the workload of its crew.

In DO-254 the design assurance level also determines the objectives of, and amount of rigor in, the development process, the type and quantities of artifacts from the development effort that must be preserved, the level of independence that must be maintained when conducting the development activities, and the amount and type of verification that must be performed on the design.

The guidance in the main body of DO-254 (chapters 1 through 11) is written for electronic hardware of design assurance level C. DO-254 accommodates the higher design assurance levels (A and B) through the application of its Appendix B, which contains additional verification-related activities that are intended to provide the

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

extra measure of assurance that is appropriate for equipment that requires per-hour failure probabilities less than 10^{-7}. Equipment with a design assurance level of C or D must comply with chapters 1 through 11 of DO-254, and levels A and B must comply with chapters 1 through 11 and Appendix B.

It is worth noting that the inherent failure probability of semiconductor components is typically no better than 10^{-5} to 10^{-6}. Or in other words, the inherent reliability limitations of semiconductor devices prevents the electronic hardware from achieving the failure probabilities required for level A or B systems, and therefore the development guidance in DO-254 will not by itself result in a design with the requisite level A or B reliability. The requisite reliability, however, can be achieved at the system level through the architectural mitigation techniques described in SAE ARP4754[3] or SAE ARP4754A,[4] even though the hardware itself is limited to the approximate failure rate for level C hardware.

Since the design process cannot create hardware that is able by itself to satisfy the requisite failure rate for level A or B systems, the only remaining avenue of design assurance for those higher levels is to employ additional verification-related techniques to ensure that every design error is detected and removed, thereby assuring that the hardware will achieve its maximum potential reliability. DO-254 Appendix B, which focuses on the verification-related techniques that ensure that every function in the design is fully identified and tested, is applied to level A and B hardware to ensure, as well as possible, that all design errors are detected and removed.

DO-254 AND DO-178B

DO-178B,[5] *Software Considerations in Airborne Systems and Equipment Certification*, was published and adopted years before electronic hardware was required to comply with DO-254. DO-178B's head start had two rather curious effects on electronic hardware development. First, there was a temptation for equipment manufacturers to move their system functionality from software to hardware because of the significant increase in time and effort (both perceived and actual) that DO-178B imposed on software development. The idea, of course, was that if equipment functionality could be moved to electronic hardware it would not have to be subjected to the expensive and difficult design assurance processes in DO-178B. The second effect is that the terminology, concepts, and processes from DO-178B became so well established in the airborne design assurance community that it still heavily influences how DO-254 is applied and implemented for hardware. While it may seem obvious that hardware and software are fundamentally different, and therefore should be treated differently for the purposes of design assurance, this seemingly elemental observation has at times been overwhelmed by the sheer inertia of DO-178B's influence.

So how do DO-254 and DO-178B (or DO-178C[6]) compare? And are the differences all that significant? Since both documents provide guidance on development processes, there are bound to be significant similarities in their content and philosophy. In fact, from the high level perspective they are quite similar in their approaches and fundamental concepts. The similarities can be summarized as follows:

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

- Their safety background and basis are the same.
- Both rely on process and design assurance.
- Both use life cycle phases to govern development.
- Both use the integral processes of process assurance (quality assurance for software), configuration management, and verification.
- Verification is requirements-based.
- Both include tool qualification.

So in a broad sense the two documents are very similar. However, when examining the details of their design assurance concepts and processes, a number of differences emerge, some of them dramatic enough that trying to apply DO-178 concepts to hardware development will not result in the desired design assurance. The differences between DO-254 and DO-178 (and to some extent between hardware and software) are embedded in the details, and are listed in **Table 1.2**.

TABLE 1.2
Differences between DO-254 and DO-178B/C

Topic	DO-254 Hardware	DO-178B/C Software
Environmental tests	Required	Not applicable
Part wear out	Need to consider	N/A
White box testing	Test points and simulation	Can perform with emulator and/or symbolic debugger
Implementation	Hardware and components	Machine code within hardware components
Debugging	Device pin level	Assembler level
Robustness testing	Optional or project dependent	Required
Object oriented considerations	Not applicable	Ada95, C++, Java
Objectives for compliance	Defined in sections 4.1, 5.1.1, 5.2.1, 5.3.1, 5.4.1, 5.5.1, 6.1.1, 6.2.1, 7.1, 8.1	Annex A Tables
Applicability	LRU, CCA, PLD, any complex electronic hardware	Software only
Tool qualification	Tool qualification not required for elemental analysis tools	Tool qualification required for structural coverage analysis tools
Independence	Broad brush stroke approach in Appendix A	Specific objectives depending on software level

continued

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

TABLE 1.2 (continued)
Differences between DO-254 and DO-178B/C

Topic	DO-254 Hardware	DO-178B/C Software
Simulation	May need second independent simulation; difficult to use same test procedures in simulations and in-circuit hardware tests	Easy to use the same test cases on simulation and on target hardware
Coverage analysis	Elemental analysis not specific about coverage criteria definition	Modified Condition/Decision Coverage defined for Level A Decision coverage defined for Level B Statement coverage defined for Level C
Verification	Test coverage of requirements, coverage of elements for Levels A and B	Test coverage of high-level and low-level requirements, structural coverage and test coverage of data and control coupling
Definition of derived requirement	Design decision; may or may not have a parent requirement	Glossary—almost the same as DO-254 Usage in Section 5—no parent requirement
Simple	Exhaustive input testing and reduced documentation allowed	Not applicable
Design approach	For PLDs, hardware description language describes how the physical hardware in the PLD will be configured For other electronic hardware, graphical entry such as schematic diagrams	Procedural language that describes a sequence of steps
Processing	For PLDs, parallel simultaneous implementation of hardware design language (HDL); functionality is implemented concurrently	Instructions execute in sequence
Validation	Derived requirements are validated to ensure they are correct and complete	Not in the scope of software—derived requirements must be justified but are not validated
Means of application	Written for Level C with additional measures for Levels A and B	Written for Level A with reductions in objectives, activities, and artifacts for Levels B through D

While some of the differences may seem trivial or inconsequential, others are significant and can result in serious consequences if DO-178 is allowed to influence how DO-254 is applied to hardware. All of the differences should be carefully considered and understood to pre-empt any confusion or misunderstandings when applying DO-254. In general, software definitions, techniques, and processes should not be used with hardware.

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Perhaps the most insidious, confusing, and persistent of the differences is the definition of a derived requirement. DO-178B's long dominance of the design assurance field has resulted in a strong tendency, especially among people who have a software background or who are used to the language of DO-178B, to assume that the DO-254 definition is the same as the one found in DO-178B, or more commonly, that the DO-178B definition is universal and therefore applies to hardware as well as software. However, while the glossaries in both documents define a derived requirement as an additional requirement that results from the design process and which (may or) may not be directly traceable to a higher level requirement, Section 5.0 of DO-178B narrows the definition of a derived requirement to a requirement that does not directly trace to a higher level requirement. The definition in DO-178B Section 5.0 has superseded the glossary definition and has, again due to the long-time dominance of DO-178B, been treated as the more or less universal definition of a derived requirement. This is unfortunate from a number of perspectives, a significant one being that the processes (particularly the validation process) in DO-254 are designed to work with the DO-254 definition, and as will be described in more detail later, problems can arise if the DO-178B definition is indiscriminately used with the processes in DO-254.

OVERVIEW OF DO-254

The guidance in DO-254 covers a variety of topics including:

- Hardware standards
- Hardware design life cycle data
- Additional design assurance techniques for design assurance level (DAL) A and B functions
- Previously developed hardware
- Tool assessment and qualification
- Use of commercial off-the-shelf (COTS) components
- Product service experience
- Hardware safety assessment
- Design assurance strategy, including consideration for DAL A and B functions
- Planning process
- Requirements capture
- Conceptual design
- Detailed design
- Implementation
- Production transition
- Validation process
- Verification process including tests and reviews
- Configuration management
- Process assurance
- Certification liaison and proposed means of compliance

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

DO-254 ties together several key aspects of equipment development and compliance issues that would be otherwise difficult to achieve for complex and/or highly integrated devices and/or systems. These aspects are:

- Use of design assurance in lieu of quantitative analysis of failures
- Use of requirements to capture the aspects of aircraft functions performed by complex electronic hardware
- Use of review, analysis, and test to satisfy compliance to the FARs through verification

DO-254 contains eleven sections (or chapters) and four appendices. **Table 1.3** identifies the sections and appendices and summarizes their topic areas.

The sections of DO-254 and their relationships are shown in **Figure 1.1**.

Section 1 introduces DO-254 and describes its scope and applicability, and defines certain keywords such as "should," "may," and "hardware item." It is worth noting here that DO-254 does not define nor use the word "shall," which is commonly used to identify mandatory practices or requirements. This is appropriate given DO-254's role as *guidance* rather than requirements. Even AC 20-152 does not mandate compliance to DO-254 by stating that compliance to DO-254 is an acceptable, but not the only, means of complying with the FARs. Novices in the certification industry are quick to latch onto this point and object that DO-254 is just guidance, not requirements, and that the FAA does not make compliance to it mandatory. This is normally stated in the hope of sidestepping DO-254, but in realistic terms, any means of compliance other than DO-254 could be much more difficult and expensive to implement, even in the unlikely event that the certification authorities approve it.

DO-254 Section 1 also states that DO-254 does not attempt to define the nature or identity of "firmware," but does state that firmware should be classified as either hardware or software and then addressed appropriately through DO-254 or DO-178 as applicable. To persons who are inexperienced in the business of hardware description languages and PLD design, it is common for an HDL's resemblance to software to prompt them to try to classify it as such. However, those who are more experienced with firmware realize that HDLs, while similar to software code in appearance, are fundamentally different and have more in common with, and thus should be classified and treated as, hardware. Subjecting an HDL design to the software processes in DO-178B or DO-178C would present a host of problems, and for some processes would prove to be impractical if not impossible.

One aspect of DO-254 Section 1 that attracts a great deal of interest is the introduction of the concept of "simple" versus "complex" hardware, especially the last paragraph of Section 1.6, which states that simple hardware items do not need extensive documentation and can comply with DO-254 with reduced overhead. For virtually all equipment suppliers, the idea of simple hardware, and the reduced effort associated with it, is immensely attractive, and is immediately embraced as a possible means of avoiding full compliance to DO-254. This desire to avoid the cost and schedule impact of DO-254 is often so strong that equipment suppliers will go to great lengths to classify their hardware as simple even when it really is not. The fact that DO-254 does not provide a quantifiable definition of the "comprehensive

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

TABLE 1.3
Summary of Contents of DO-254

Section	Title	Topics
1	Introduction	Purpose/Scope, relationship to other documents, related documents, how to use DO-254, complexity, alternative methods, overview
2	System Aspects of Hardware Design Assurance	Information flow, system safety assessment processes, hardware safety assessment
3	Hardware Design Life Cycle	Life cycle processes, transition criteria
4	Planning Process	Planning process objectives and activities
5	Hardware Design Processes	Design process phases, objectives, and activities
6	Validation and Verification Process	Validation process, objectives, and activities Verification process, objectives, and activities Validation and verification methods
7	Configuration Management Process	Configuration management objectives and activities Data control categories
8	Process Assurance	Process assurance objectives and activities
9	Certification Liaison Process	Means of compliance and planning Substantiating compliance
10	Hardware Design Life Cycle Data	Plans, standards, design data, validation/verification data, acceptance test criteria, problem reports, configuration management (CM) records, process assurance records, Hardware Accomplishment Summary (HAS)
11	Additional Considerations	Previously developed hardware, COTS components, product service experience, tool assessment and qualification
Appendix A	Modulation of Hardware Life Cycle Data Based on Hardware Design Assurance Level	Life cycle data, independence
Appendix B	Design Assurance Considerations for Level A and B Functions	Functional failure path analysis (FFPA), architectural mitigation, product service experience, advanced verification methods
Appendix C	Glossary of Terms	Definitions of relevant terminology
Appendix D	Acronyms	Definitions of acronyms

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

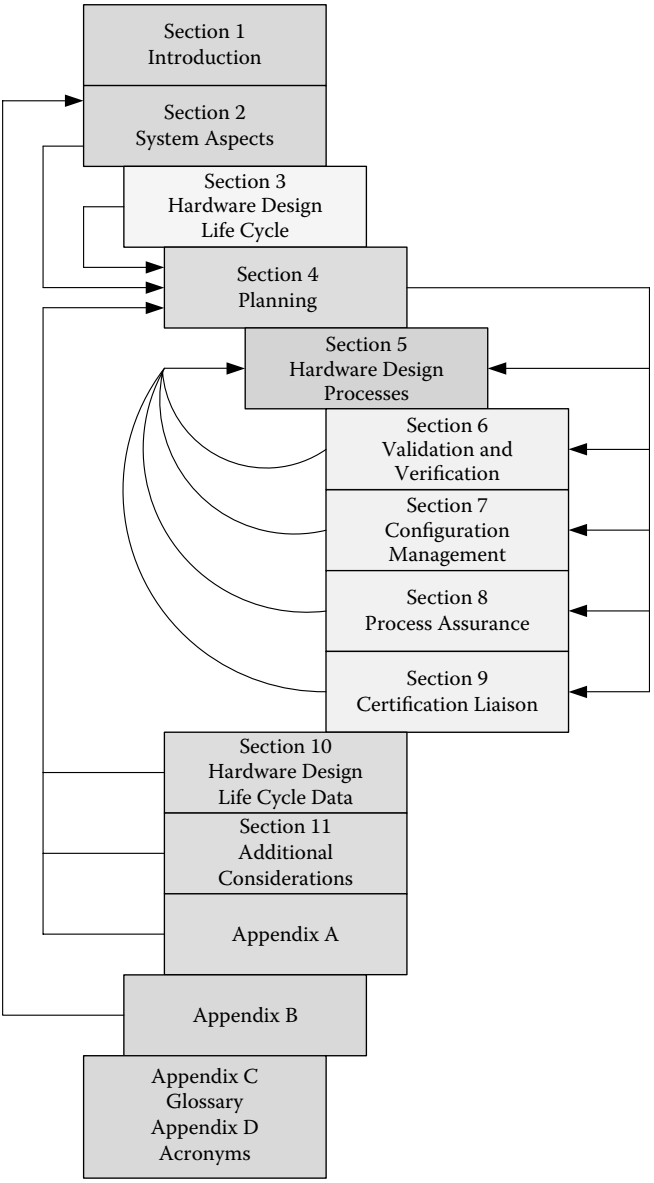

FIGURE 1.1 **(See Color Insert.)** Structure of DO-254

combination" of tests and analyses that must be performed on simple hardware just exacerbates the situation and provides the necessary ambiguity to inspire these efforts to thwart DO-254. However, FAA Order 8110.105[7] addresses the complexity issue and provides specific guidance on what constitutes the necessary comprehensive combination of tests for simple hardware, the result being that for anything other

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

than truly simple hardware, the simple hardware approach will be either impractical or more expensive than treating the hardware as complex and complying with all of DO-254. In fact, 8110.105's verification guidance for simple hardware can be used in reverse to provide guidance on the definition of a simple device: if it is realistic or even possible to comprehensively test a hardware item according to the guidance in 8110.105, then the hardware can be correctly classified as simple.

DO-254 Section 2 describes how the processes, activities, hardware, and other data from DO-254 interface to the overall certification process. Information flow between hardware and system, and between hardware and software, is briefly discussed. Section 2 also discusses the system safety process and identifies the design assurance levels and their characteristics, as well as hardware safety assessment considerations.

DO-254 Section 3 contains a very brief discussion of the hardware design life cycle and the transition criteria that govern the movement of the life cycle from one phase or process to the next. This section identifies the life cycle processes as being the planning process, the design process, and the supporting processes. The supporting processes are further identified as being validation, verification, configuration management, process assurance, and certification liaison.

DO-254 Section 4 describes the objectives and activities of the planning process, which is the first of the design life cycle processes. Six hardware management plans and four standards are defined for hardware development: the Plan for Hardware Aspects of Certification (PHAC), Hardware Design Plan (HDP), Hardware Validation Plan (HVP), Hardware Verification Plan (HVP), Hardware Configuration Management Plan (HCMP), Hardware Process Assurance Plan (HPAP), Requirements Standards, Hardware Design Standards, Validation and Verification Standards, and Hardware Archive Standards. **Table 1.4** lists these plans and standards, where in DO-254 their contents are described, and which of the DO-254 objectives are satisfied by them.

DO-254 Section 5 describes the objectives and activities of the hardware design process. This section describes a generic design process consisting of five phases: Requirements Capture, Conceptual Design, Detailed Design, Implementation, and Production Transition. An organization's design process does not have to be the same as this process, but it should be able to satisfy all of the Section 5 objectives.

DO-254 Sections 6 through 9 describe each of the supporting processes. The objectives and activities of the validation and verification processes are described in Section 6, configuration management in Section 7, process assurance in Section 8, and certification liaison in Section 9.

DO-254 Section 6 covers the objectives and activities of the validation and verification supporting processes. Validation is the process of ensuring that derived requirements are correct and complete, and verification is the process of ensuring that the final product meets its requirements.

DO-254 Section 7 addresses the objectives and activities of the configuration management supporting process. It includes configuration items, configuration identification, baselines, problem reporting, change control, and archiving.

DO-254 Section 8 is about the process assurance supporting process, and covers its objectives and activities such as process assurance reviews and audits.

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

TABLE 1.4
Hardware Management Plans

Plan	Content Described in DO-254 Section	Objective Satisfied
Plan for Hardware Aspects of Certification (PHAC)	10.1.1	4.1-1, 2, 3, 4
Hardware Design Plan	10.1.2	4.1-1, 2, 3, 4
Hardware Validation Plan	10.1.3	4.1-1, 2, 3, 4 6.1.1-1
Hardware Verification Plan	10.1.4	4.1-1, 2, 3, 4 6.2.1-1
Hardware Configuration Management Plan	10.1.5	4.1-1, 2, 3, 4 7.1-3
Hardware Process Assurance Plan	10.1.6	4.1-1, 2, 4 8.1-1, 2, 3
Requirements Standards	10.2.1	4.1-2
Hardware Design Standards	10.2.2	4.1-2
Validation and Verification Standards	10.2.3	4.1-2
Hardware Archive Standards	10.2.4	4.1-2; 5.5.1-1; 7.1-1, 2

DO-254 Section 9 discusses the certification liaison supporting process, including means of compliance, planning, and how to substantiate compliance.

DO-254 Section 10 describes the content of each type of hardware life cycle data, especially the hardware management plans (PHAC, HDP, HVP, HCMP, HPAP), standards, hardware design data, verification data, and the Hardware Accomplishment Summary.

DO-254 Section 11 includes the "Additional Considerations," or in other words everything that is left over. Its contents include previously developed hardware (PDH), COTS components, product service experience, and tool assessment and qualification.

DO-254 Appendix A includes a table of all hardware life cycle data items and correlates them to their hardware control category, which in turn defines which configuration management processes and methods must be used to manage them. It also includes a definition of independence.

DO-254 Appendix B contains various verification-related techniques that must be applied with level A and B hardware. The techniques include functional failure path analysis, architectural mitigation, product service experience, and advanced verification techniques (elemental analysis, safety-specific analysis, and formal methods).

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

WHAT DOES IT MEAN TO ME?

Among organizations that are getting into the business of DO-254 programs, two common questions are, "What do I have to do to comply with DO-254?" and "How much will DO-254 cost?"

Compliance is obviously the simpler question to answer, and the answer is to simply adopt (and adapt to) the industry best practices in DO-254. These are summarized as follows:

- Establish a structured design process that meets the objectives defined in DO-254
  - Well-defined phases with realistic entry and exit criteria
  - Built-in peer reviews
  - Do the front-end work (requirements, traceability, plans, analysis, research, etc.) conscientiously and at the proper time
  - Honor and observe the design process (do not ignore or bypass it, even during a crisis)
- Learn how to write well-formed requirements
  - Emphasize the use of functional requirements rather than design description (implementation) requirements
  - Write them early
  - Understand what a derived requirement is
  - Learn how to document validation and traceability data as part of requirements capture
- Establish high integrity validation and verification processes and methods, including:
  - An independent peer review process for levels A and B
  - Peer reviews of data and documents
  - Requirement reviews to validate derived requirements
  - Learn how to conduct requirements-based verification
  - Learn how to write effective and optimized test cases
  - Learn how to conduct robustness verification
  - Simulations—functional and post-layout timing (or static timing analysis)
  - Elemental analysis—code coverage
  - Hardware test—in the actual flight hardware
  - Acquire tools to support verification
- Establish a configuration management infrastructure, including:
  - Problem reporting
  - Document/data control
  - Document/data release
  - Backups/archives
  - Refresh of backup media
  - Retention of data for life of use of the equipment
  - Retention of tools and test equipment for life of use of the equipment

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

- Establish a component management process—be prepared for parts obsolescence
- Establish a process assurance role or department
  - Perform audits, review
  - Track deviations
  - Audit transition criteria
- Be prepared for audits of off-shore or subcontracted work
  - May need a sub-supplier management plan
  - May need on-site stage of involvement (SOI) audits
  - Close coordination with configuration management and control of data
  - Close coordination with process assurance
  - Technical oversight
- Interface with customer and/or airframer
  - Establish and interpret requirements
- Interface with certification authority
  - FAA and/or designee
  - SOI audits
- Organize vast amounts of data
- Write lots of documentation and reports
- Cultural changes
  - Use the CM system
  - Use change control
  - Comply with processes—no more informal engineering
  - Transparency
  - Accountability
- Learn new rules for component selection
  - Settle for less than the leading edge technology
  - Embrace more tried and true technology, tools, methods
  - New is ok, but may require more verification or justification

Obviously the list seems long, but for most companies, compliance might require adaptation (or not) but should never be impossible. Changing the engineering culture—if it is needed, since some companies have already discovered the benefits of using the best practices in DO-254—is often the hardest part of complying with DO-254, but with time it can be done.

The second question is somewhat dependent on the answer to the first one and is considerably harder to answer, mainly because there simply is not a good quantifiable answer to it. Some people try to attach a percentage escalation factor to a project, for example adding on 30 percent to a project's non-DO-254 cost to account for DO-254 compliance, but in reality the cost is going to be determined by a company's DO-254 "gap" (how much its existing processes fall short of DO-254) and how agreeable the company and its personnel are to changing their ways and learning new tricks, i.e., how willing they are to close that gap. A company whose processes are reasonably consistent with DO-254 can conceivably incur significant additional costs simply because its personnel resist DO-254 rather than embrace it. Likewise, a

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

company that has little or none of the DO-254 infrastructure can conceivably comply with DO-254 with minimal inconvenience and cost if the company and its people are open to learning and using the processes in it. The amount of discomfort and cost associated with DO-254 is almost entirely self-determined, and the lesson that "the most expensive path to DO-254 compliance is the one that tries to go around it" can be a difficult and expensive one to learn.

For convenience, references to DO-178B and DO-178C in this book will simply use DO-178 when the discussion applies equally to both versions of DO-178. The reference to DO-178B will be used when reference to the earlier version is intended. Similarly, references to SAE ARP4754 and SAE ARP4754A will use ARP4754 when the discussion applies equally to both versions of ARP4754.

REFERENCES

1. RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, RTCA Inc., Washington, D.C., 2000. This document is also known as EUROCAE ED-80.
2. Advisory Circular Number 20-152, RTCA, INC., DOCUMENT RTCA/DO-254, DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE, Federal Aviation Administration, June 2005.
3. SAE ARP4754, *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*, Warrendale, PA: SAE, 1996.
4. SAE ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*, Warrendale, PA: SAE, 2010.
5. RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA Inc., Washington, D.C., 1992. This document is also known as EUROCAE ED-12B.
6. RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA Inc., Washington, D.C., 2011. This document is also known as EUROCAE ED-12C.
7. Order 8110.105 CHG 1, *Simple and Complex Electronic Hardware Approval Guidance*, Federal Aviation Administration, dated September 23, 2009.

FURTHER INFORMATION

1. The Federal Aviation Administration Web page: www.faa.gov
2. The RTCA Web page: www.rtca.org
3. The SAE Web page: www.sae.org
4. EASA Web page: www.easa.europa.eu
5. FAA Regulatory and Guidance Library (RGL) Web page: rgl.faa.gov
6. CAST Position Papers Web page: www.faa.gov/aircraft/air_cert/design_approvals/air_software/cast/cast_papers/

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

2 Regulatory Background

In the United States, the Code of Federal Regulations (CFR)[1] is the codification of the rules published in the Federal Register by the departments and agencies of the federal government. The Code of Federal Regulations is divided into 50 titles that represent areas subject to federal regulation. The 50 subject matter titles contain one or more volumes that are updated annually. Each title is divided into chapters, and each chapter typically bears the name of the issuing agency. Each chapter is further subdivided into parts that cover specific regulatory areas. Large parts may be subdivided into subparts; parts are then organized in sections.

Title 14 of the CFR covers regulations for aeronautics and space. Within Title 14 there are six Chapters spread over five Volumes. The Volumes, Chapters, and Parts are organized as shown in **Table 2.1**.

Chapter one of Title 14 has three subchapters that define the contents of Part 1–59. The subchapters are as follows:

- Subchapter A—Definitions
  - Part 1 Definitions and Abbreviations
  - Part 3 General Requirements
- Subchapter B—Procedural Rules
  - Part 11 General Rulemaking Procedures
  - Part 13 Investigative and Enforcement Procedures
  - Part 14 Rules Implementing the Equal Access to Justice Act of 1980
  - Part 15 Administrative Claims Under Federal Tort Claims Act
  - Part 16 Rules of Practice for Federally Assisted Airport Enforcement Proceedings
  - Part 17 Procedures for Protests and Contract Disputes
- Subchapter C—Aircraft
  - Part 21 Certification Procedures for Products and Parts
  - Part 23 Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes
  - Part 25 Airworthiness Standards: Transport Category Airplanes
  - Part 26 Continued Airworthiness and Safety Improvements for Transport Category Airplanes
  - Part 27 Airworthiness Standards: Normal Category Rotorcraft
  - Part 29 Airworthiness Standards: Transport Category Rotorcraft
  - Part 31 Airworthiness Standards: Manned Free Balloons
  - Part 33 Airworthiness Standards: Aircraft Engines

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

TABLE 2.1
Title 14 Code of Federal Regulations

Title	Volume	Chapter	Part	Regulatory Entity
Title 14 Aeronautics and Space	1	I	1–59	Federal Aviation Administration, Department of Transportation
	2		60–109	
	3		110–199	
	4	II	200–399	Office of the Secretary, Department of Transportation (Aviation Proceedings)
		III	400–1199	Commercial Space Transportation, Federal Aviation Administration, Department of Transportation
	5	V	1200–1299	National Aeronautics and Space Administration
		VI	1300–1399	Air Transportation System Stabilization

- Part 34 Airworthiness Standards: Fuel Venting and Exhaust Emission Requirements for Turbine Engine Powered Airplanes
- Part 35 Airworthiness Standards: Propellers
- Part 36 Noise Standards: Aircraft Type and Airworthiness Certification
- Part 39 Airworthiness Directives
- Part 43 Maintenance, Preventive Maintenance, Rebuilding and Alteration
- Part 45 Identification and Registration Marking
- Part 47 Aircraft Registration
- Part 49 Recording of Registration Titles and Security Documents
- Part 50-59 [Reserved]

Figure 2.1 shows the structure of the Code of Federal Regulations, Title 14 for Aeronautics and Space, Part 21/23/25/27/29 for parts, aircraft, and engines, regulation 1301 for function and installation, and regulation 1309 for equipment, systems, and installation.

A particular regulation is referenced by Title, Part, Subchapter, and Subpart. The regulations pertaining to systems and equipment on Part 25 transport aircraft are referenced:

- 14 CFR 25.1301[2]
- 14 CFR 25.1309[3]

Federal Aviation Regulations have an amendment level to identify the date and identification of the most recent change to the regulation. In general, aircraft certification programs for new aircraft or changes to existing aircraft use the most recent amendment level of the regulations applicable to the program. In some instances

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

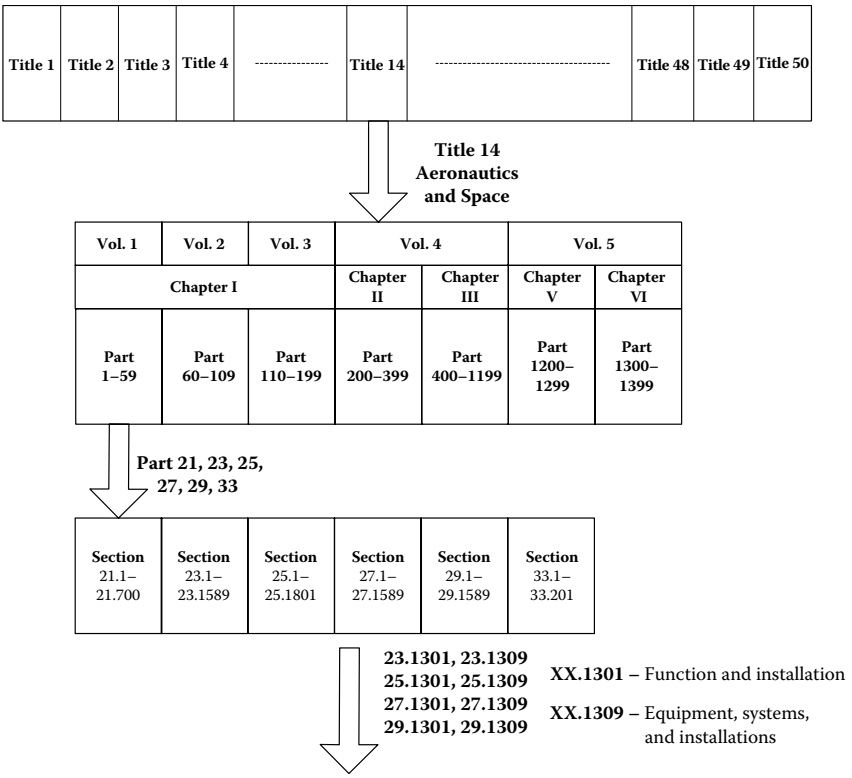

FIGURE 2.1 CFR Structure

programs such as aircraft derivative models or changes to an existing model aircraft can use the regulations and amendment level from original approval or certification basis.

The following paragraphs show the basic text of FARs 25.1301 and 25.1309. While other versions and amendments of this FAR exist, the point here is to show the basic intent of the text. Foreign certification authorities such as the European Aviation Safety Agency (EASA) use a set of Certification Specification (CS) that follow the numbering, and largely, the intent or same text, as the equivalent FAR.

The text of 14 CFR 25.1301 states:

Function and installation.

(a) Each item of installed equipment must—
  (1) Be of a kind and design appropriate to its intended function;
  (2) Be labeled as to its identification, function, or operating limitations, or any applicable combination of these factors;
  (3) Be installed according to limitations specified for that equipment; and
  (4) Function properly when installed.

[(b) EWIS must meet the requirements of subpart H of this part.]

Amendment 25-123, Effective 12/10/07

Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

The term EWIS refers to electrical wiring interconnection system for the wiring and connections to, and between, aircraft systems.

The text of 14 CFR 25.1309 states:

> Equipment, systems, and installations.
>
> (a) The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.
> (b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that—
> (1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and
> (2) The occurrence of any other failure condition which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.
> (c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards.
> (d) Compliance with the requirements of paragraph (b) of this section must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider—
> (1) Possible modes of failure, including malfunctions and damage from external sources.
> (2) The probability of multiple failures and undetected failures.
> (3) The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and
> (4) The crew warning cues, corrective action required, and the capability of detecting faults.
> [(e) In showing compliance with paragraphs (a) and (b) of this section with regard to the electrical system and equipment design and installation, critical environmental conditions must be considered. For electrical generation, distribution, and utilization equipment required by or used in complying with this chapter, except equipment covered by Technical Standard Orders containing environmental test procedures, the ability to provide continuous, safe service under foreseeable environmental conditions may be shown by environmental tests, design analysis, or reference to previous comparable service experience on other aircraft.]
> [(f) EWIS must be assessed in accordance with the requirements of Section 25.1709.]
>
> Amendment 25-123, Effective 12/10/07

The certification basis for a project or an aircraft program is the applicable airworthiness requirements as established in 14 CFR 21.17[4] (original certification) and 14 CFR 21.101[5] (change to a type certificate), as appropriate; special conditions; equivalent level of safety findings; requirements per 14 CFR 21.21(b)(2)[6]; and exemptions applicable to the product to be certificated. The certification basis specifies the applicable regulations and their respective amendment level at the time of application for a certificate. An application for type certification of a transport category

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

aircraft (Part 25) is effective for five years. An application for any other type certificate is effective for three years, unless an applicant shows at the time of application that their product requires a longer period of time for design, development, and testing, and the FAA approves a longer period. The applicant is the party that applies to the FAA for a type certification, supplemental type certificate, or an amended type certificate. A type certificate (TC) is the certification for a new type of aircraft. A supplemental type certificate (STC) is the certification for modification to existing aircraft. An amended type certificate (ATC) is FAA approval to modify an aircraft design from its original design. An amended type certificate approves not only the modification, but also how that modification affects the original design.

MEANS OF COMPLIANCE

The FAA publishes additional information that explains an acceptable method to comply with the certification basis and thus to the applicable regulations (FAR). These publications are known as Advisory Circulars (AC). The Advisory Circulars contain information known as a **means of compliance** (MoC) to a FAR. Advisory Circulars are identified by the regulation they are associated with. For example, AC 25.1309[7] explains a means of compliance to regulation 14 CFR 25.1309. Advisory Circulars may also contain explanations of regulations and other guidance materials, best practices, or information useful to the aviation industry. Advisory Circulars can also provide guidance, methods, procedures, and practices for complying with Federal Aviation Regulations and requirements.

The most commonly used means of compliance to a FAR are:

- Engineering evaluation
  - Compliance statement
  - Design review
  - Calculation/analysis
  - Safety assessment
- Tests
  - Laboratory test
  - Ground test on aircraft
  - Flight test
  - Simulation
- Inspection
  - Conformity inspection
  - Design inspection
- Equipment qualification

Engineering evaluation for demonstration of compliance to a regulation includes compliance statement, design review, calculation/analysis, and safety assessment. A compliance statement is a formal statement that a design complies with a regulation and may include compliance by similarity. A design review is used when compliance is based on a review of data, descriptions, or drawings. Calculation or analysis is used when compliance is demonstrated by an engineering analysis, calculation,

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

or report. Safety assessment is used when compliance is demonstrated by a safety analysis such as probability analysis.

Tests for demonstration of compliance to a regulation include laboratory tests, ground tests with an aircraft, flight tests with an aircraft, and simulation of aircraft functions. Laboratory test is used when compliance is demonstrated by testing in a lab. Ground test is used when compliance is demonstrated by aircraft testing conducted on the ground. Flight test is used when compliance is demonstrated with aircraft flight testing. Simulation is used when compliance is demonstrated by flight or computer model simulation or with the use of a representative mockup of the equipment.

Inspection for demonstration of compliance to a regulation includes conformity inspection and design inspection. Conformity inspection is used when compliance is demonstrated by a review of the equipment against its approved and released drawings. Design inspection is used when compliance is demonstrated by an inspection of the design as it is installed on the aircraft.

Equipment qualification is used when compliance is demonstrated by environmental qualification testing, such as RTCA/DO-160.[8]

The means of compliance allow the applicant to "show compliance" to a regulation. Once the compliance has been demonstrated, the regulatory authority or designee may then make a finding of compliance to the regulation.

Many of the methods for demonstrating compliance to the regulations are not well suited or practical for airborne electronic hardware, especially circuit cards or devices such as field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), or complex programmable logic devices (CPLDs). DO-254 was written to provide applicants and developers with suitable methods and techniques to show compliance to the FARs.

Figure 2.2 shows the Advisory Circulars for FARs pertaining to systems, equipment, and electronic parts.

AC 25.1309 includes several objectives based on fail-safe system design principles. When considering a system and its operation, failure objectives need to include:

- The failure of any single element, component, or connection during any one flight.
- Any single failure of an element, component, or connection should not prevent safe flight and landing.
- Catastrophic failures must be extremely improbable.
- Common cause analysis should be used to ensure that single failures do not adversely affect more than one channel in a redundant system (i.e., with multiple channels). These single failures do not adversely affect more than one system performing equivalent aircraft functions.

AC 25.1309 also includes techniques to assess failures and their impacts. These assessments are supported with qualitative and quantitative analysis. A functional hazard assessment (FHA) is a qualitative assessment to identify and classify failures. The FHA is used in early design stages to assess various system architectures and design for suitability. The FHA, as will be described later, is also used

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

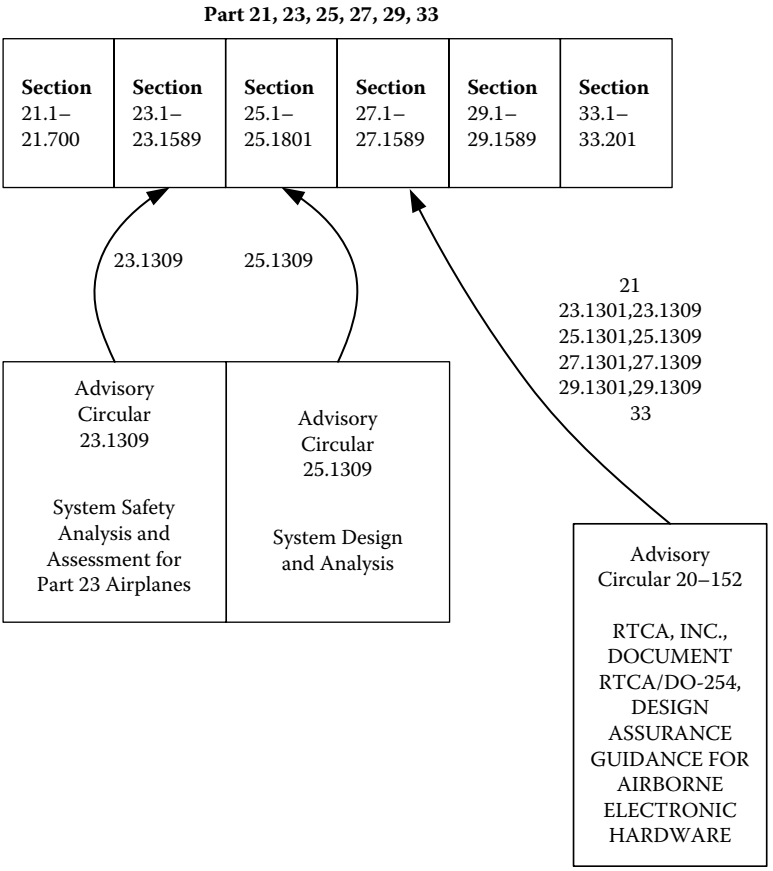

FIGURE 2.2 Advisory Circulars

to determine the DAL associated with a function and its electronic hardware. In Aerospace Recommended Practice (ARP) 4754A, the aircraft level function design assurance level is the FDAL, the software and/or airborne electronic hardware has the resultant item design assurance level (IDAL). A reliability or fault tree analysis is a quantitative assessment of failures to show that their probability is commensurate, i.e., inversely proportional, to their severity.

In accordance with AC 25.1309, catastrophic hazards must be shown to be extremely improbable. Analysis of catastrophic hazards should include qualitative and quantitative assessment. Failures classified as major hazards must be shown to be improbable. Analysis of major hazards includes qualitative and sometimes a quantitative assessment.

The AC goes on to define extremely improbable failures as those having a probability on the order of 1×10^{-9} or less, improbable failures as those having a probability on the order of less than 1×10^{-5} but greater than 1×10^{-9}, and probable failures as those having a probability on the order of greater than 1×10^{-5}.

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Updates to these categories added a hazardous/severe-major condition. Analysis of failures classified as hazardous/severe-major should include qualitative and quantitative assessment. Failures classified as hazardous/severe-major must be shown to have a probability on the order of less than 1×10^{-5} but greater than 1×10^{-7}.

As system or component complexity increases, the ability to perform qualitative and quantitative assessments of system or component failures becomes more and more difficult. The FARs for systems and equipment and the associated Advisory Circular came about in the era of electrical and mechanical systems with comparatively low complexity. As system and component complexity increased, the industry recognized the need to provide a means of compliance to the FARs that considered the increasing complexity.

In 1996, ARP4754 was written to address highly integrated electronic systems, especially those with significant functionality implemented in software. ARP4754 addresses development assurance for a system, where development assurance results in a system that satisfies its certification basis and from which errors have been detected and removed. Development assurance uses a development methodology with planned and systematic actions in conjunction with qualitative and quantitative assessments to ensure that the system is fail-safe and that any failures meet their probability of occurrence.

The 1996 version of ARP4754 references RTCA/DO-178B for software aspects and the document that would become DO-254 for complex electronic hardware aspects of the system development. RTCA/DO-254 was subsequently published in April 2000. The FAA published the Advisory Circular for complex custom microcoded components, AC 20-152, in June 2005. AC 20-152 defines DO-254 as a means of compliance to the FARs for complex electronic hardware. As stated in AC 20-152, "By following the guidance and procedures outlined in RTCA/DO-254, you have assurance that the hardware design performs its intended functions within the environment it was designed for, and the assurance of meeting all the applicable airworthiness requirements."[9] Notice that this language wraps back around to the FARs and the Advisory Circulars:

- FAR 25.1301 states that equipment must operate properly and FAR 25.1309 states that equipment must perform its intended function.
  - AC 20-152 states that if DO-254 is used, then there is assurance that complex electronic hardware will perform its intended function.
- FAR 25.1309 states that equipment must perform its intended function under all foreseeable operating conditions.
  - AC 20-152 states that if DO-254 is used, then there is assurance that complex electronic hardware will perform its intended function in the environment for which it was designed.
- AC 25.1309 states that qualitative and quantitative analysis should be used for catastrophic and hazardous/severe-major failure conditions. The AC also gives probabilities for all categories of failure conditions. AC 25.1309 is a means of compliance to FAR 25.1309.
  - AC 20-152 states that if DO-254 is used then there is assurance of meeting applicable airworthiness requirements.

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Advisory Circular 20-152, published in June 2005, addresses RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware for 14 CFR Parts 21, 23, 25, 27, 29, and 33. DO-254 can be used for compliance to Federal Aviation Regulations for:

- Products and Parts
- Normal, Utility, Acrobatic, and Commuter Category Airplanes
- Transport Category Airplanes
- Normal Category Rotorcraft
- Transport Category Rotorcraft
- Aircraft Engines

GUIDANCE MATERIALS

Guidance is information that explains how to comply with certification requirements and aviation regulations. FAA Advisory Circular 20-152 recognizes the guidance in DO-254 for complex custom micro-coded components with hardware design assurance levels of A, B, and C (i.e., the IDAL). The types of components covered by AC 20-152 include ASICs, PLDs, FPGAs, and similar components.

The guidance in DO-254 is applicable to line replaceable units (LRU), circuit cards or circuit boards, programmable logic devices including CPLDs, ASICs, and FPGAs, and COTS components. While DO-254 has a broad scope, AC 20-152 limits the scope to complex custom micro-coded components. The guidance in DO-254 represents industry consensus on design assurance for airborne electronic hardware. DO-254 also incorporates best practices for design assurance identified by the aviation and electronics industry.

Guidance in DO-254 covers a variety of topics including:

- Hardware standards
- Hardware design life cycle data
- Additional design assurance techniques for design assurance (IDAL) A and B functions
- Previously developed hardware
- Tool assessment and qualification
- Use of COTS components
- Product service experience
- Hardware safety assessment
- Design assurance strategy, including consideration for design assurance (IDAL) A and B functions
- Planning process
- Requirements capture
- Conceptual design
- Detailed design
- Implementation
- Production transition
- Validation process

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

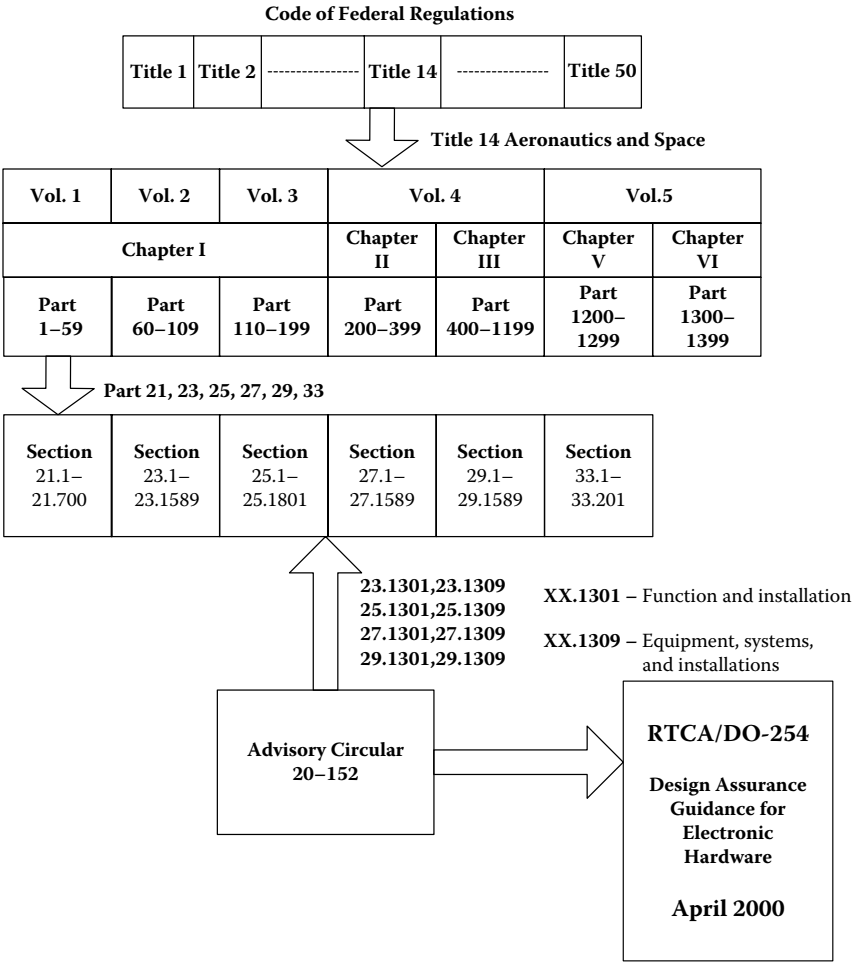

FIGURE 2.3 DO-254 Relationship to CFR

- Verification process including tests and reviews
- Configuration management
- Process assurance
- Certification liaison and proposed means of compliance

The path to DO-254 from the Code of Federal Regulations is shown in **Figure 2.3**.

ISSUE PAPERS

The Federal Aviation Administration (FAA) uses Issue Papers to provide a structured means of accomplishing the necessary steps in the type certification and type validation processes. Type certification includes projects for type certificates, amended type certificates, type design changes, supplemental type certificates, and

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

amended supplemental type certificates. Issue Papers provide a means for describing and tracking the resolution of significant technical, regulatory, and administrative issues that occur during a project. The Issue Paper process establishes a formal communication for significant issues between the applicant, a foreign civil aviation authority if applicable, and the FAA.

For type certification projects, Issue Papers are useful tools for keeping an unbiased uniform certification approach between applicants. Issue Papers also form a valuable reference for future type certification programs and for development of regulatory changes. By describing significant or precedent setting technical decisions and the rationales employed, Issue Papers can become reference material.

The Issue Paper process is documented in FAA Order 8110.112[10] titled Standardized Procedures for Usage of Issue Papers and Development of Equivalent Levels of Safety Memorandums. The FAA maintains a Transport Airplane Issues List for issues applicable to international validation and domestic certification projects on the FAA Web site.

The list identifies the subject "Assurance of Simple and Complex Electronic Hardware" for inclusion in certification programs. The description states that a means of compliance Issue Paper may be needed for most aircraft programs and modification projects for airborne systems containing electronic hardware components.

Current FAA certification programs use an Issue Paper to cover topics relevant to airborne electronic hardware. Contents of these Issue Papers are proprietary to the applicant. Foreign certification authorities have similar processes; e.g., EASA has a similar process that uses certification review items (CRI).

ORDERS

The FAA uses Orders to provide information to the managers and staff of the FAA Aircraft Certification Service, including designated engineering representatives (DER), and organizations associated with the certification process described in Title 14 of the Code of Federal Regulations. Order 8110.105 applies to PLDs and is titled *Simple and Complex Electronic Hardware Approval Guidance*.

Order 8110.105 supplements RTCA/DO-254 and gives guidance for approving both simple and complex custom micro-coded components. Topics covered, and the associated paragraphs in 8110.105, are:

- Reviews and FAA involvement
  - Chapter 2: How to review simple electronic hardware (SEH) and complex electronic hardware (CEH)
  - Chapter 3: How much FAA involvement should apply to hardware projects
- Topics for SEH and CEH
  - Chapter 4–2: Modifiable components
  - Chapter 4–3: Certification plan
  - Chapter 4–4: Validation processes
  - Chapter 4–5: Configuration management
  - Chapter 4–6: Assessing and qualifying tools

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

    - Chapter 4–7: Approving hardware changes in legacy systems using RTCA/DO-254
    - Chapter 4–8: Acknowledging compliance to RTCA/DO-254 for TSO approvals that don't reference RTCA/DO-254
    - Chapter 4–9: COTS intellectual property
- Topics for SEH
    - Chapter 5–2: Verification processes
    - Chapter 5–3: Traceability
- Topics for CEH
    - Chapter 6–2: Verification processes
    - Chapter 6–3: Traceability

Chapter 2 of Order 8110.105 describes reviews as part of the certification liaison process. Reviews may be conducted on-site, at the applicant or supplier's facility, or may be conducted as a desk review. The four reviews, known as SOI reviews, are as follows:

- SOI #1—Hardware planning review
- SOI #2—Hardware design review
- SOI #3—Hardware validation and verification review
- SOI #4—Final review

SOI #1 is conducted when most of the plans and standards are complete and reviewed. SOI #2 is typically conducted when at least 50 percent of the hardware design data (requirements, design, and implementation) is complete and has been reviewed. SOI #3 is typically conducted when at least 50 percent of the hardware validation and verification data is complete and has been reviewed. SOI #4 occurs after the final hardware build and verification are complete, a hardware conformity review is done, and the application(s) is ready for formal system approval.

The depth and extent of FAA involvement in a project, including determination of when and where to conduct the SOI reviews, is determined by the hardware design assurance level and a score based on relevant criteria. Level A and B hardware require high or medium FAA involvement, Level C hardware requires medium or low FAA involvement, and Level D hardware requires low FAA involvement. The score derived from relevant criteria can range from 0 to 207. A score of less than 80 results in high FAA involvement for Level A and B, medium FAA involvement for Level C, and low FAA involvement for Level D hardware. A score of between 80 and 130 results in high FAA involvement for Level A, medium FAA involvement for Level B and C, and low FAA involvement for Level D hardware. A score of greater than 130 results in medium FAA involvement for Level A and B, and low FAA involvement for Level C and D hardware. The FAA involvement could be direct participation by an FAA engineer from an Aircraft Certification Office (ACO) or by a DER assigned and delegated for the project. Compliance organizations can use Authorized Representatives (AR) or Unit Members (UM) as the designated authority to perform oversight and reviews.

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Stage of Involvement audits use the content of the Airborne Electronic Hardware Review Job Aid[11] as a reference tool during the reviews. While the Job Aid is not intended to be used as a checklist, it often does serve as the official checklist during a review. Either way, it would behoove applicants and developers to be familiar with the Job Aid questions. The Job Aid questions can form the basis for project review forms or can be used to conduct internal dry run reviews before a formal FAA review is held.

The Job Aid also includes a description of tasks to be performed before, during, and after a hardware review in Part 2; a list of activities and questions to be considered during a review in Part 3; and an approach to the Findings and Observations to DO-254 objectives in Part 4.

REFERENCES

1. Code of Federal Regulations, United States Government Printing Office, electronic version available at: http://www.ecfr.gov
2. Code of Federal Regulations, Title 14: Aeronautics and Space, PART 25—AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES, Subpart F—Equipment, 25.1301 Function and installation.
3. Code of Federal Regulations, Title 14: Aeronautics and Space, Part 25—AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES, Subpart F—Equipment, 25.1309 Equipment, systems, and installations.
4. Code of Federal Regulations, Title 14: Aeronautics and Space, PART 21—CERTIFICATION PROCEDURES FOR PRODUCTS AND PARTS, Subpart B—Type Certificates, 21.17 Designation of applicable regulations.
5. Code of Federal Regulations, Title 14: Aeronautics and Space, PART 21—CERTIFICATION PROCEDURES FOR PRODUCTS AND PARTS, Subpart D—Changes to Type Certificates, 21.101 Designation of applicable regulations.
6. Code of Federal Regulations, Title 14: Aeronautics and Space, PART 21—CERTIFICATION PROCEDURES FOR PRODUCTS AND PARTS, Subpart B—Type Certificates, 21.21 Issue of type certificate: normal, utility, acrobatic, commuter, and transport category aircraft; manned free balloons; special classes of aircraft; aircraft engines; propellers.
7. Advisory Circular, AC 25.1309-1A—System Design and Analysis, Federal Aviation Administration, June 1988.
8. RTCA DO-160F, ENVIRONMENTAL CONDITIONS AND TEST PROCEDURES FOR AIRBORNE EQUIPMENT, RTCA Inc., Washington, D.C., 2000.
9. Advisory Circular Number 20-152, RTCA, INC., DOCUMENT RTCA/DO-254, DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE, Federal Aviation Administration, June 2005, p. 1.
10. Order 8110.112, *Standardized Procedures for Usage of Issue Papers and Development of Equivalent Levels of Safety Memorandums*, Federal Aviation Administration, June 2010.
11. *Conducting Airborne Electronic Hardware Reviews Job Aid*, Aircraft Certification Service, Federal Aviation Administration, February 2008.

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

3 Planning

DO-254 development takes place within the context of ARP4754 processes. The certification aspects of airborne electronic hardware are encapsulated by the development of the system in which the electronic hardware is used. Similarly, the system development is performed within the context of a certification program for an aircraft, a modification or update to an aircraft, or in the case of a technical standard order (TSO), the TSO approval process.

Figure 3.1 shows the airborne electronic hardware within a system and the system within the aircraft program concept.

The system and safety processes start before, or along with, the DO-254 planning processes. The system process outputs that factor into planning include:

- System description
- Hardware description

The safety process outputs that factor into planning include:

- Top-level hazards from the functional hazard assessment that are the drivers for the design assurance level.
- Preliminary system safety assessment that establishes the function design assurance level at the aircraft level and the item design assurance level for the hardware.
- Functional failure path analysis that establishes which failures the hardware participates in and the corresponding classification for the hazard associated with the failure.

Figure 3.2 shows the relationship between system and safety ARP4754 processes and electronic hardware DO-254 processes. The Formal Test phase included in Figure 3.2 is not mandated by DO-254.

The aircraft or TSO certification program will determine the certification basis for the program. The certification basis is the applicable Federal Aviation Regulations and their respective amendment level and any project specific FAA Issue Papers. The certification basis is typically defined in the system level certification plan. The certification basis for airborne electronic hardware will have the same certification basis as the equipment in which it is used. Certification programs conducted in concert with foreign certification agencies may have additional issues levied to meet the requirements of other countries. The outputs of the aircraft, system, and safety processes become inputs for the formulation of the project-specific Plan for Hardware

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

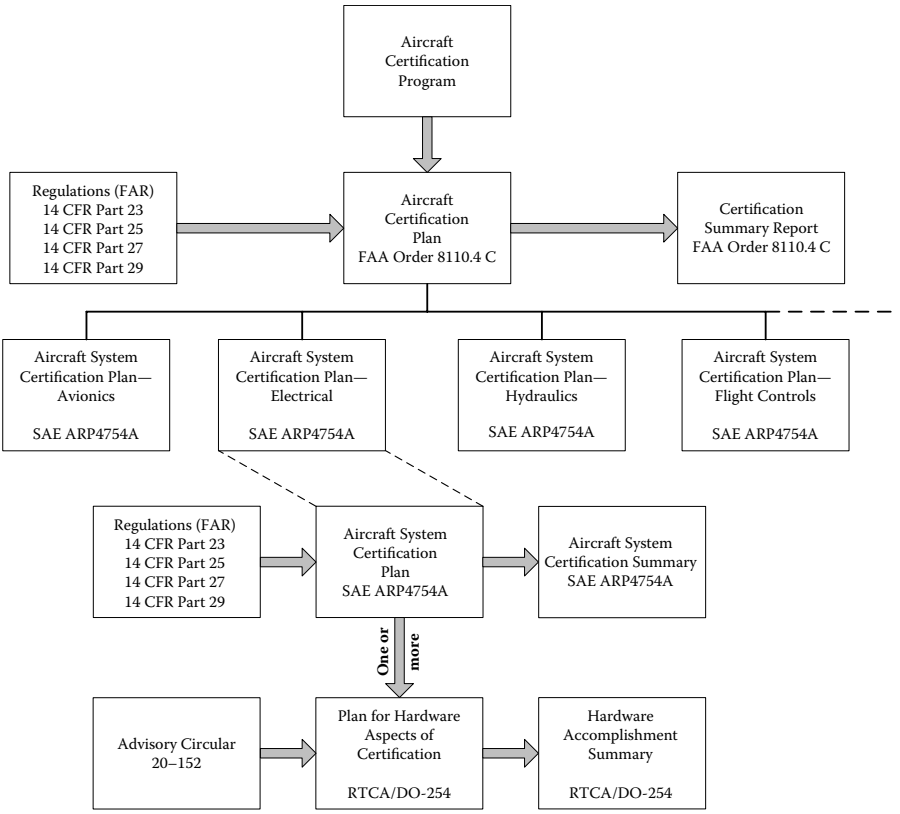

FIGURE 3.1 Electronic Hardware Development Context

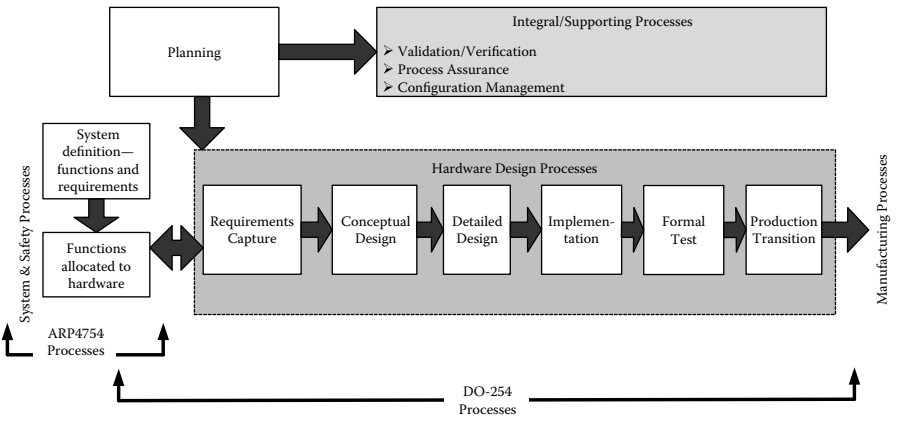

FIGURE 3.2 ARP4754 and DO-254 Processes

AVA Documents Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

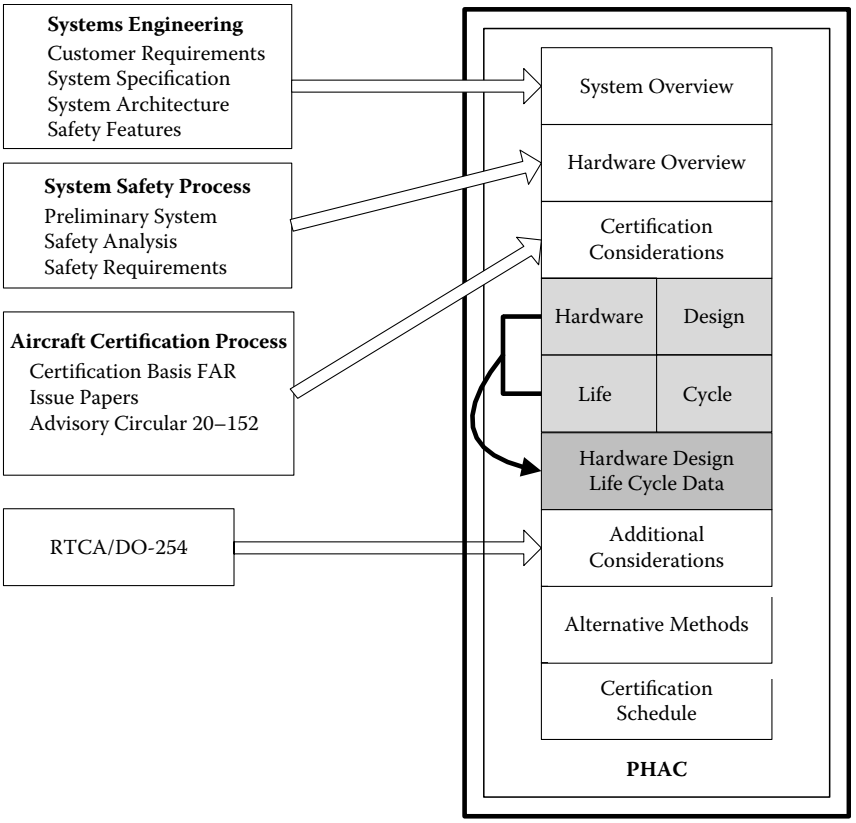

FIGURE 3.3 Inputs to Plan for Hardware Aspects of Certification

Aspects of Certification, or PHAC. The aircraft and system process outputs and PHAC inputs are depicted in **Figure 3.3**.

Project planning begins with a combination of several aspects—the idea for the design, gathering the processes and tools to accomplish the design, establishing the resources and organization to accomplish the tasks, evaluating customer-specific requirements, and evaluating project-specific aspects including the certification basis.

Planning considers hardware development from conception all the way through development and into production. Planning also includes production aspects after the design is complete to account for parts obsolescence or parts change. Planning should be a horizon-to-horizon vision of the project to ensure that all phases correctly describe the processes, methodologies, and tools used.

The planning can include a trade study or design trade-off that evaluates whether a particular design or implementation technology can be realized. Planning an FPGA design with a device that has been used in other programs and that uses the same design and verification tools will have less planning or preparation than embarking on a project that uses multiple intellectual cores developed on an FPGA, converts the design into an ASIC for production, and uses new verification tools and techniques.

AVA Documents
Document Sharing Hub
Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254

Planning is performed for projects that encompass the full development life cycle, such as new equipment for a new aircraft, and also for projects that incorporate changes into existing designs.

There are several approaches companies can use for hardware management plans and standards. One approach is to create a common set of hardware management plans and hardware standards. The common set of plans and standards describe a consistent set of processes and procedures followed for AEH or PLD development. The plans and standards state which activities are used and which data is produced for each design assurance level. The Plan for Hardware Aspects of Certification is then created for each project. The PHAC describes the project-specific system, hardware, life cycle data, schedule, and design and verification tools. Any other aspects of the project that are unique are also described in the PHAC. In addition, the PHAC would take into account project-specific FAA Issue Papers and any applicable topics from foreign certification agencies.

Another approach is for organizations to create hardware management plans and standards that are specific to each project. The plans and standards are created or updated for each project. The Plan for Hardware Aspects of Certification is also created for each specific project. The PHAC describes the project-specific system, hardware, life cycle data, schedule, and design and verification tools. Any other aspects of the project that are unique are also described in the PHAC. In addition, the PHAC would take into account project-specific FAA Issue Papers and any applicable topics from foreign certification agencies.

A third approach is for organizations to create hardware management plans and standards specific to a technology. This could be the case for the differences in life cycles required for the development of an FPGA versus the development of an ASIC. The Plan for Hardware Aspects of Certification is then created for each specific project. The PHAC describes the project-specific system, hardware, life cycle data, schedule, and design and verification tools. Any other aspects of the project that are unique are also described in the PHAC. In addition, the PHAC would take into account project-specific FAA Issue Papers and any applicable topics from foreign certification agencies.

A fourth approach is for organizations to create hardware management plans and standards that are specific to development approaches. In this case the plans would focus on the unique requirements that are specific to different development approaches, such as new product development, modifications to previously developed hardware, reuse of previously developed hardware, etc. As with other approaches the PHAC would be specific to the project, and would describe the system, hardware, life cycle data, schedule, processes, and tools that are unique to each development approach, as well as the project-specific Issue Papers and topics from foreign certification agencies.

Planning also takes into account the groups, organizations, and even companies involved in the development of airborne electronic hardware. Using the tools, processes, procedures, and personnel of an experienced DO-254 team that is located within one facility of a company is quite different from planning for spreading the life cycle and activities across different groups, different companies, and groups located in different countries, or outsourcing some of the life cycle activities. Planning may need to consider protection of proprietary data that goes outside a company or even

AVA Documents
Document Sharing Hub

Full document details: Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254