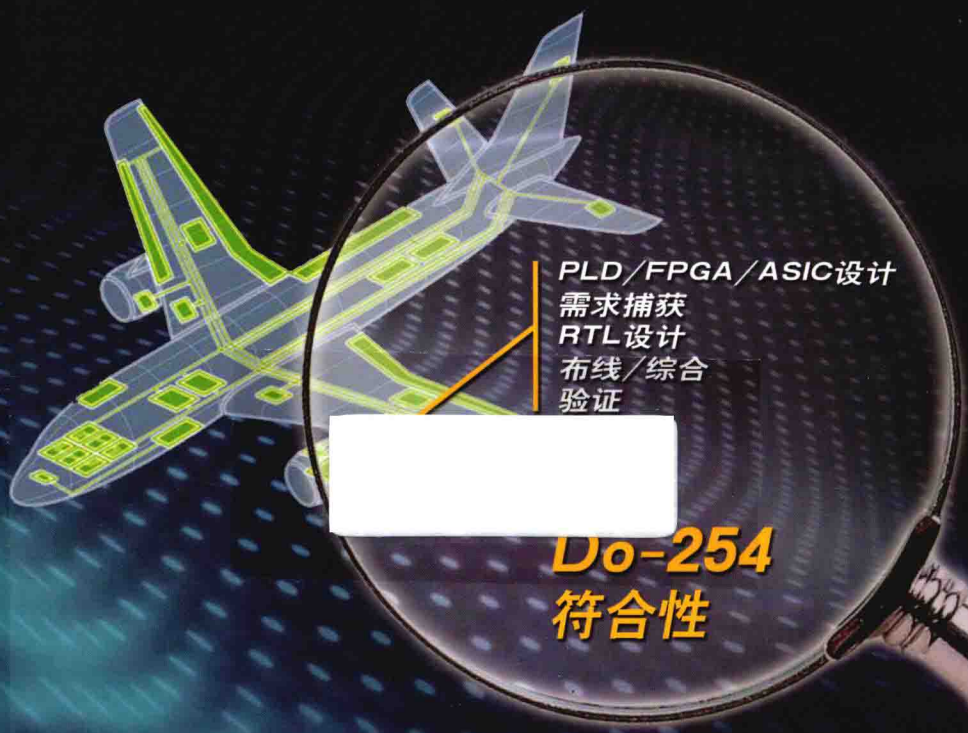
剖析 Do-254

万 波 编著



航空工业出版社

剖析 Do－254

万　波　编著

航空工业出版社
北　京

内 容 提 要

航空工业界对复杂电子硬件所造成的安全性影响日益关注，由此催生了本书的问世。本书系统地介绍了复杂电子硬件的开发流程、设计保证等级的确定、FAA 和 EASA 的 Do－254 审定流程，还介绍了硬件生命周期数据和高级验证方法，最后给出了中英文对应的 Do－254 文档编写示例。

本书适合从事航空机载设备硬件设计的工程师、质量保证工程师、构型管理工程师，以及系统工程师参考和阅读，可以提供硬件设计、适航流程方面的指导。

图书在版编目（CIP）数据

剖析 Do－254 / 万波编著. --北京 : 航空工业出版社，2016.1

ISBN 978－7－5165－0943－2

Ⅰ. ①剖… Ⅱ. ①万… Ⅲ. ①硬件—系统设计 Ⅳ. ①TP303

中国版本图书馆 CIP 数据核字（2015）第 292053 号

剖 析 Do－254

Pouxi Do－254

航空工业出版社出版发行

（北京市朝阳区北苑 2 号院 100012）

发行部电话：010－84936597 010－84936343

北京京华虎彩印刷有限公司印刷 全国各地新华书店经售

2016 年 1 月第 1 版 2016 年 1 月第 1 次印刷

开本：787×1092 1/16 印张：10.75 字数：279 千字

印数：1—1000 定价：36.00 元

前　言

航空工业界对复杂电子硬件所造成的安全性影响日益关注，由此催生了《Do－254 机载电子设备硬件设计保证指南》的问世。

与简单电子硬件不同，复杂电子硬件难以在元件外部，即引脚（Pin 脚）级对设计进行充分的验证。相反地，为了达到可以接受的验证覆盖率，复杂电子硬件往往要深入到元件的内部；必要时，还要采用一些特殊的验证方法，如元素分析等，以确保硬件实施能反映需求，没有非预期的行为。

电子硬件开发过程的严格程度与其失效所造成的影响成正比，失效影响越严重，则开发过程要求越严格。因此，要正确理解 Do－254，首先需要理解的概念是设计保证等级。为此，本书在第 1 章对 Do－254 提出的背景做了说明之后，在第 2 章详述了如何按照 ARP 4754A 的建议来划分硬件的设计保证等级。

Do－254 是航空工业界的通用指南，在具体实施时，不同的适航当局会根据需要对其进行删减和补充。本书的第 3 章和第 4 章分别介绍了 FAA 和 EASA 的硬件评审过程。

本书第 5 章阐述了在硬件生命周期过程中所产生的相关数据，其中包括硬件计划、硬件设计标准和指南、硬件设计数据、硬件确认和验证数据、接收测试准则、问题报告、构型管理记录、过程保证记录，以及硬件完结综述等方面的内容。

第 6 章介绍了功能失效路径分析（FFPA），以及 A 级和 B 级功能所用到的一些高级验证方法，包括元素分析、特定安全分析和形式化方法。

本书最后一章以某飞机集成断路器板为例，介绍了硬件合格审定计划与硬件开发计划的文档编写示例，为初次应用 Do－254 的读者提供了参考。示例文档以中英文双语的形式给出，因为民用飞机要进入国际市场，要获得 FAA 和 EASA 的适航证，因此需要提供英文版的技术文档。

我国大型民用飞机的研制尚处于起步阶段，目前市场上关于 Do－254 的书籍不多。中航工业上海航空电器有限公司作为国内唯一一家 C919 大型民用客机的系统级供应商，愿将自身积累的适航经验与业界分享，争取早日将我国建设成民用航空强国，这也是撰写此书的初衷。

本书写就于上海航空电器有限公司工作期间，要特别感谢公司董事长、总经理蒲毅，副总经理周鹏程，公司领导王潇、刘季仲、李章进，以及乔中奇、解亚梅、乔臻臻等同事对本书出版工作的大力支持。同时，还要感谢航空工业出版社王少雄主任对本书所提出的有益建议。没有大家的热心帮助，也不会有本书的问世。

万　波

2015 年 11 月 22 日

目　录

第1章　Do－254概述

1.1　中国民用航空局、FAA与EASA

经过型号合格审定、获得型号合格证（type certificate，TC）是民用航空器进入民航运营市场的先决条件。型号合格证TC是由适航认证机构（或适航审定当局，简称适航当局）根据民用航空器产品和零件合格审定的规定，对民用航空器颁发的证明该航空器处于安全可用状态的证件。中国的适航认证机构是中国民用航空局，美国和欧洲的适航认证机构分别是FAA和EASA。

中国民用航空局（Civil Aviation Administration of China，CAAC）是中华人民共和国国务院主管民用航空事业的由部委管理的国家局，归交通运输部管理。其前身为中国民用航空总局，在1987年以前曾承担中国民航的运营职能；2008年3月，由国务院直属机构改制为部委管理的国家局，同时更名为中国民用航空局。

中国民用航空局发布的中国民用航空规章（CCAR）25部《运输类飞机适航标准》，是我国民用航空政府部门在借鉴航空发达国家，特别是美国联邦航空条例（FAR）中的相关规章（FAR 25）的基础上，制定和发布的用于民用飞机适航认证的法规，它是颁发和更改运输类飞机型号合格证TC的适航标准。自1985年12月31日发布以来，已先后于1990年8月8日、1995年12月18日和2001年5月14日进行三次修订。现行有效的版本为CCAR－25－R3，即第三号修正案。

美国联邦航空局（Federal Aviation Administration，FAA）隶属于美国交通部，负责制定美国民用航空的法规并全面监管美国民用航空领域。其前身是成立于1926年的美国商务部航空司，1958年11月单独成立美国联邦航空局，1967年划归美国运输部管理。

FAA建立了以美国联邦航空条例（Federal Aviation Regulation，FAR）为基础的适航标准体系，其中涵盖了运输类、特技类和通勤类飞机的适航标准、载人自由气球的适航标准，以及航空发动机和螺旋桨的适航标准。

在美国联邦航空条例之下，FAA还颁布了咨询通告（Advisory Circular，AC）作为对规章所要求的符合性方法的建议性和解释性材料。尽管FAA一再申明，咨询通告中介绍的符合性方法并不是强制性的或者唯一的，但一般而言，型号合格证TC申请人都采用咨询通告中介绍的符合性方法来表明对适航标准的符合性，因为采用其他的符合性方法往往意味着需要局方认可且成本更高等问题。以运输类飞机为例，为了表明对运输类飞机适航标准的符合性，FAA制定了约90份咨询通告，涵盖飞行性能、结构强度、动力装置、飞机系统和持续适航等多个专业。比如，针对Do－254的咨询公告AC 20－152、《Do－254机载电子设备硬件设计保证指南》，是FAA在机载电子硬件合格审定过程中的重要法律性文件。

对于机载设备，FAA还颁布了技术标准规定（Technical Standard Order，TSO），引用

工业界标准作为飞机材料、零部件和机载设备的适航标准。它是由适航当局针对部分航空产品新使用的材料、零部件和机载设备等项目而制定的最低性能标准和附加要求。

FAA 建立了以美国联邦航空条例（FAR）、咨询通告（AC）和技术标准规定（TSO）为基础的适航标准体系。联邦航空条例作为国家层面的航空立法，赋予适航标准以法律的地位；咨询通告作为 FAA 的法律文件，是对规章的解释，其中引用了工业界的各种标准；TSO 作为 FAA 的法律文件，是针对新材料、零部件和机载设备的适航标准。

欧洲的适航当局是欧洲航空安全局（European Aviation Safety Agency，EASA）。第二次世界大战以后，世界航空业有了长足的发展，尤其是美国，几乎一度垄断了西方国家全部大型商用客、货机市场。到了 20 世纪 70 年代初，欧洲国家也不甘示弱，决定通过整合欧洲的技术和资源，联合设计、制造大型商用飞机，同美国分享庞大的世界航空业市场。随后，欧洲成立了联合航空局（Joint Aviation Authority，JAA），其主要职责就是制定和完善欧洲联合航空要求（Joint Aviation Requirements，JAR），其内容涉及飞机的设计和制造、飞机的运营和维修，还有相关的管理和技术程序。欧盟成立以后，该组织被欧洲航空安全局（EASA）所取代。

2003 年 9 月，EASA 通过了 1702/2003 的实施规则——产品审定部分，它包括一个实施法规，即 21 部和相关的审定规范（certification specification，CS）（如 CS－23、CS－25、CS－E 等）。同年 11 月，又通过了 2042/2003 的实施规则——维护部分，它包括 4 个实施法规——M 部（适航）、145 部（维修机构）、66 部（放行人员）、147 部（维修培训机构）和相关 AMC（局方接受的符合性方法）和 GM（指导材料）。EASA 今后还会将法规范围扩大到飞机营运人的运行规范和飞行员执照等方面。

1.2 RTCA 与 EUROCAE 组织

适航当局是政府性的组织，它借助法律的手段确保有关航空安全的政策法规得到实施。在这些政府性组织外，还有一些民间非营利性组织，他们在制定航空标准、促进航空安全方面也扮演着重要的角色。其中，比较有代表性的是 RTCA 和 EUROCAE。

RTCA 是英文 Radio Technical Commission for Aeronautics 的缩写，中文翻译为航空无线电委员会。它成立于 1935 年，主要针对航空领域内的通信导航监视和空中交通管理系统的问题，提出相关建议。RTCA 主要履行美国联邦咨询委员会的职责，由 RTCA 提出的建议被美国联邦航空局 FAA 用作制定政策、项目和管理决定的依据，也被一些私人公司用作制定发展、投资和其他商业决定的依据。

RTCA 的主要目标有：

（1）以适当的方式整合航空系统用户和供应商的技术要求，使其有助于政府和工业部门能满足双方的目标和责任；

（2）对不断追求日益增长的安全性、系统容量和效率的航空业务所面对的系统技术问题进行分析，并提供解决方案；

（3）在相关技术的应用方面开发协调一致的标准来满足用户和供应商的要求，包括用于支持航空的电子系统和设备的最低工作性能标准的开发；

（4）协助开发相关的技术材料，使国际民航组织、国际电信联盟和其他感兴趣的国

际组织可以在其基础上使用。

RTCA通过制定标准和专业指南，推动了新型飞机机载设备在效率和安全方面的认证，拓展了这些技术的市场，RTCA的成果是由相应专业志愿人员组成的特别委员会研究出来的，它以特别委员会会议的方式，向公众发布将要研究的问题，同时接受任何有兴趣的专业志愿人员参与该问题的特别委员会的具体工作。

自成立以来，已陆续有270多个来自美国和世界的政府机构、企业和学术组织申请成为RTCA组织的会员，这些会员几乎涵盖了整个航空领域。

欧洲民用航空设备组织EUROCAE（European Organization for Civil Aviation Equipment）是由欧洲及其他地区的航空利益相关方组成的非营利组织，包括制造商（飞机、机载设备、空管系统和地面设备）、服务供应商、国家和国际航空当局和用户（航空公司、机场和运营人）。EUROCAE已经发布了许多针对航空界的性能指标和文件，这些指标和文件被大量引用，作为欧洲TSO（Technical Standard Order，技术标准规定）和其他航空规章的符合性方法。

在制定航空标准和专业指南方面，RTCA和EUROCAE有过多次合作。同一个专业指南，可能是二者联合制定的，只不过在指南发布时，他们采用了不同的编号。比如，针对机载软件的专业指南《机载系统和设备的软件考虑》，RTCA的发布编号为Do-178，而EUROCAE的编号为ED-12。同样，针对机载硬件的专业指南《机载电子设备硬件设计保证指南》，RTCA的发布编号为Do-254，而EUROCAE的编号为ED-80。

1.3 Do-254标准提出的背景

当机载设备的硬件设计中包含PLD（可编程逻辑器件）、FPGA（现场可编程门阵列）、ASIC（专用集成电路）等复杂的用户微编程元件时，在开发过程中会使用类似软件编程语言的硬件描述语言，如超高速集成电路硬件描述语言（very high speed integrated circuit hardware description language，VHDL）。借助硬件描述语言，可以在不改变硬件电路的情况下，通过修改硬件逻辑描述，达到改变硬件设计的目的。因而，它给硬件设计带来了很大的灵活性。

如图1-1所示，要实现一个与门，除了用传统的硬件与门器件来实现外，我们还可以采用可编程逻辑器件，通过VHDL编程的方式，来实现一个与门。

```
LIBRARY IEEE;
USE IEEE.Std_Logic_1164.ALL;          ——库、程序包的说明调用
--------------------------------------------------------------------------------
ENTITY DigiLogic IS
PORT
(in1: IN Std_logic;
 in2: IN Std_logic;
 out1: OUT Std_logic);                ——定义端口，2输入、1输出
 END;
--------------------------------------------------------------------------------
ARCHITECTURE Behavior OF DigiLogic IS
BEGIN
process(in1,in2)
BEGIN
Out1<=in1 and in2;                    ——定义与门
END process;
END;
```

图1-1 用VHDL语言实现与门

当硬件设计需要更改时，比如，原有的与门，现在由于某种原因，需要更改为或门。当采用可编程逻辑器件时，不用另外选择一个或门器件，只需要将 VHDL 程序更新一下，重新灌装到可编程逻辑器件即可。如图 1－2 所示，要更改这个设计，只需要在原有 VHDL 程序基础上，更改一句描述语言就可以达到目的。

```
LIBRARY IEEE;
USE IEEE.Std_Logic_1164.ALL;          ——库、程序包的说明调用
--------------------------------------------------------------------------------
ENTITY DigiLogic IS
PORT
(in1: IN Std_logic;
 in2: IN Std_logic;
 out1: OUT Std_logic);                ——定义端口，2输入、1输出
 END;
--------------------------------------------------------------------------------
ARCHITECTURE Behavior OF DigiLogic IS
BEGIN
process(in1,in2)
BEGIN
Out1<=in1 or in2;                     ——定义或门
END process;
END;
```

图 1－2　用 VHDL 语言实现或门

也就是将

Out1 <= in1 and in2

改为

Out1 <= in1 or in2

这样，我们就实现了在不改变硬件电路的情况下，实现硬件设计原理的更改。可编程逻辑器件的应用，为硬件设计带来了很大的灵活性。

然而，硬件描述语言也带来了一个新的问题，即在逻辑设计中可能会产生潜在的缺陷或错误，从而导致部件和系统的故障。在图 1－1 和图 1－2 的例子中，因为 VHDL 程序简单，因而容易发现问题和定位潜在错误（Do－254 将其称为简单电子硬件）。在实现比较复杂的逻辑时，VHDL 的代码长度将不是 15 行，而可能达到 1500 行。在这种情况下，潜在问题就不容易发现和定位。

随着可编程逻辑器件的技术日益发展，它们越来越多地被应用到机载设备中。若在设计中存在着潜在的错误，不仅会影响任务的可靠性，还会对飞机安全构成威胁。

《Do－254 机载电子设备硬件设计保证指南》（简称 Do－254）正是为解决这一类问题而提出的一个行业指南。

在 Do－254 的执行总结（executive summary）中有这样一段话："航空工业界对复杂电子硬件（CEH）的开发和使用已经带来了新的安全性和认证方面的担忧。作为响应，RTCA SC－180 和 EUROCAE WG－46 工作组成立了。WG－46 和 SC－180 同意，在编制本文档的早期成立一个联合委员会。该联合委员会经过特许，来开发清晰的、前后连贯的机载电子硬件的设计保证指南，以便它能安全地履行其预期的功能。"

从这里我们可以看出，尽管 Do－254 并不仅仅针对复杂电子硬件，制定 Do－254 标

准的初衷是为了解决复杂电子硬件，如内嵌复杂控制逻辑的PLD、FPGA、ASIC等，对航空安全所带来的担忧。

实际上，Do-254的适用范围很广泛，在Do-254的1.2节中，有这样的描述：

本指南适用于，但不限于以下硬件单元：

(1) 航线可更换单元（LRU）；

(2) 印制电路板（PCB）组件；

(3) 用户微编程元件，如ASIC、PLD，包括任何相关的宏函数；

(4) 集成技术元件，如混合和多芯片模块；

(5) 商用货架元件。

1.4 Do-254与ED-80

在RTCA出版的Do-254标准前言中写道："本标准是由RTCA第180专门委员会（SC-180）编制的，2000年4月19日经RTCA程序管理委员会批准，RTCA SC-180和欧洲民用航空设备组织（EUROCAE）WG-46工作组通过一致的过程联合完成了本指南的开发。"

从这里我们可以看出，《Do-254机载电子设备硬件设计保证指南》是由RTCA和EUROCAE共同制定的。只不过EUROCAE在标准出版的时候，将这个标准的编号改为ED-80。

因此，RTCA出版的Do-254和EUROCAE出版的ED-80实际上是同一个标准。在本书的叙述中，将把二者等同看待。它们之间的关系可以用图1-3简明地表示出来。

图1-3 RTCA出版的Do-254与EUROCAE出版的ED-80之间等价

在对标准的引用方面，FAA在其相关文献中基本上只提到RTCA/Do-254，不提ED-80。而相反，EASA在其相关文献中，则采用ED-80/Do-254的方式，表示两个标准是等同的。

1.5 硬件设计保证等级

Do-254的适用范围与硬件的设计保证等级（design assurance level，DAL）息息相关，不同的硬件设计保证等级对应于不同程度的硬件生命周期数据（hardware life-cycle data，HLCD）。硬件设计保证等级越高，对过程控制要求越严格，需要提供的硬件生命周期数据就越完备，反之，则越简略。

根据硬件失效对飞机安全性所造成的影响，Do-254中共定义了5种硬件设计保证等级DAL，即A、B、C、D、E，如表1-1所示。

Do-254针对不同的设计保证等级，提出了不同的生命周期数据要求，如表1-1所

示，对于设计保证等级为 E 的硬件，Do－254 不适用。也就是说，《Do－254 机载电子设备硬件设计保证指南》仅适用于设计保证等级为 A、B、C、D 的硬件。

表 1－1　硬件设计保证等级与系统设计保证等级之间的关系

系统设计保证等级	失效状态等级	失效状态描述	硬件设计保证等级定义
A	灾难性的	失效状态将妨碍持续的安全飞行和着陆	A：硬件功能，其失效或异常动作，如硬件安全性评估所示，将导致系统功能失效，从而导致飞机处于灾难性的失效状态
B	危害的	失效状态会降低飞机的能力或飞行人员应付不利工作条件的能力到这样的程度：飞行边界或功能性能的大幅降低，身体痛苦或更高的工作负荷使得不能依靠飞行人员来准确地和完备地完成其任务，或对乘员产生不利影响，包括对这些乘员中的少数人造成严重的或特别致命的伤害	B：硬件功能，其失效或异常动作，如硬件安全性评估所示，将导致系统功能失效，从而使飞机处于危害严重的失效状态
C	主要的	失效状态会降低飞机的能力或飞行人员应付不利工作条件的能力到这样的程度：飞行边界或功能性能的明显降低，飞行人员工作负荷明显增加，或使飞行人员工作效率降低，或使乘员感觉不适，甚至可能对这些乘员造成伤害	C：硬件功能，其失效或异常动作，如硬件安全性评估所示，将导致系统功能失效，从而使飞机处于程度较重的失效状态
D	次要的	失效状态并不明显地降低飞机安全性，可能会导致飞行人员采取一些行动，而这些行动在其能力范围内。次要的失效状态包括：安全边界或功能性能稍有降低，飞行人员工作负荷稍有增加，如正常的飞行计划被改变，或对乘员造成一些不便	D：硬件功能，其失效或异常动作，如硬件安全性评估所示，将导致系统功能失效，从而使飞机处于程度较轻的失效状态
E	无影响	不影响飞机的工作能力或增加飞行人员工作负荷的失效状态	E：硬件功能，其失效或异常动作，如硬件安全性评估所示，将导致某个系统功能失效，但对飞机工作能力或飞行人员工作负荷无影响，对于定义为 E 级的功能，不需要使用 Do－254 作为指南，但这些指南可作为参考

Do－254 是一个通用的指南，不同的适航当局根据需要，对它的适用性做了进一步界定。如 1.6 节所述，对于 FAA 而言，这个界定的主要依据有 3 点：一是硬件设计保证等级，二是机载设备硬件是简单还是复杂，三是采用商用货架元件的情况。而对于 EASA 而言，界定标准比较复杂，Do－254 的适用范围相对 FAA 而言更宽。本书的第 3 章和第 4 章将会针对这个问题展开讨论。

因此，在应用 Do－254 来指导硬件开发设计流程之前，首先要确定的是硬件的设计

保证等级。硬件设计保证等级的界定是本书第2章所要探讨的主题。

这里还要说明的是，CAAC目前还没有发布关于Do-254是否适用的明确咨询公告，诚如中航工业系统公司发布的《〈RTCA/Do-254机载电子设备硬件设计保证指南〉实施指导意见》一书中所说："CAAC虽没有明确的咨询通告确认Do-254的有效性，但在ARJ21的研制中对设备供应商提出了通过Do-254来证明其符合性的要求。"因此，本书在介绍Do-254的应用时，主要以FAA（第3章）和EASA（第4章）为基础。可以预见，将来CAAC在发布Do-254的咨询公告时，也会参照FAA和EASA的做法。

1.6 Do-254的适用范围

Do-254是RTCA推荐的一个硬件设计保证指南，不同的适航当局在民用飞机适航取证的过程中，对Do-254的适用性做出了说明。这里首先要指出的是，并不是所有的机载设备硬件都需要采用Do-254标准来证明其符合性。

在FAA发布的咨询公告AC 20-152中有相关的说明，若硬件设计保证等级是D，制造商可以参照Do-254标准，也可以采用他们自己的设计保证规范。如果制造商决定采用Do-254标准，FAA不需要审核他们的硬件生命周期数据。

也就是说，当硬件设计保证等级为D时，FAA不会介入制造商的硬件开发设计流程。虽然FAA没有明确说明——在这里，它为自己保留了采用Do-254的余地——我们在实际操作时，只要设计保证等级为D，就可以不必采用Do-254标准。

AC 20-152中还说明，若硬件的设计保证等级为A、B或C，且里面包含了用户可编程元件，如ASIC、PLD和FPGA时，则Do-254适用于FAA的适航认证。需要注意的是，这里FAA并没有明确说明不含有用户可编程元件的硬件不必采用Do-254开发流程。但在适航认证过程中，若所有的硬件单元都是简单电子硬件（simple electronic hardware，SEH），则制造商可以提出免除Do-254适用性的申请，只要适航当局认可，则可以在硬件开发时，不参照Do-254建议的流程。诚如AC 20-152的备注里说明的那样："我们并不想应用RTCA/Do-254到任何类型的电子硬件。"

关于商用货架（commercial-off-the-shelf，COTS）微处理器，AC 20-152指出，考虑到获得COTS微处理器生命周期数据的困难，FAA并不要求制造商采用Do-254标准。他们可以采用替代的方法来确保COTS元件执行预期的功能和满足适航的要求。

除了咨询公告AC 20-152，FAA还发布了联邦指令Order 8110.105 Chg1，即《简单和复杂硬件认证指南》，其中详细说明了FAA对硬件适航认证的要求，本书的第3章将对这部分内容做详细的介绍。

与FAA不同，欧洲航空安全局EASA在Do-254的适用性上，有不同的规定。在EASA的认证备忘录（CM）EASA CM-SWCEH-001，即《机载设备硬件设计保证》中，列出了EASA与FAA在Do-254的适用性上所采取的不同态度。这些不同之处主要体现在：

（1）EASA认证备忘录的8.5节中，关于简单ASIC/PLD的定义与FAA不同。

（2）EASA新增了一些FAA并没有述及的认证考虑，其中包括：

①第6章单粒子效应指南；

②第7章设备和电路板组件的电子硬件设计保证指南；