机载电子设备硬件
设计保证指南

RTCA/DO-254

2000 年 4 月 19 日　　编制：SC-180

前言

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。

RTCA 股份公司是一个非盈利性机构，旨在推进航空科学技术和航空电子系统发展以便利大众。该组织的职能类似于联邦顾问委员会，致力于为现代航空业务提供协调一致的建议。RTCA 的目标包括但不局限于：

- 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。
- 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。
- 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。
- 协助开发相关的技术材料，使国际民航组织和国际电信联盟和其它感兴趣的国际组织可以在其基础上使用。

组织的建议通常用作政府和私人机构决定的基础，以及许多联邦航空管理技术标准指令的基础。

因为 RTCA 不是美国政府的一个官方机构，其建议不能被视为官方政府政策声明，除非在与该建议有关的任何事务方面有法令管辖权的美国政府组织或机构这样宣布。

概述

航空工业对负载电子硬件的开发和应用已经产生了对新的安全和鉴定方面的问题。作为响应，RTCA SC-180 和 EUROCAE WG-46 成立了。在本标准编写的较早阶段，WG-46 和 SC-180 同意成为一个联合委员会。该联合委员会被特许开发清楚一致的电子机载硬件设计保证指南，使其安全地实现其预期的功能。

电子机载硬件包括航线替代单元、电路板组件、特定用途的集成电路和可编程逻辑设备等等。本指南适用于当前的、更新的和扩展的技术。

本标准中的指南拟为飞机制造商和用于飞机系统的电子硬件项目的供应商所使用。指南中识别了硬件设计生命周期过程。描述了每个过程的目标和活动。本指南适用于通过系统安全评估确定的所有硬件设计保证级别。

在本指南开发过程中，委员会考虑到了其他工业文档，包括汽车工程师协会（SAE）航天推荐惯例（ARP）文档 ARP4754/EUROCAE ED-79，对高度集成的或复杂飞机系统的颁证考虑；SAE ARP4761，对民用机载系统和设备进行安全评估过程的指南和方法；以及 RTCA DO-178/EUROCAE ED-12，机载系统和设备颁证中对软件的考虑等等。

目录

插图

表格

1.0 引言

随着在许多安全要求严格的飞机功能中使用复杂电子硬件的日益增多，对于安全性和鉴定要求形成了新的挑战。这些挑战来源于关于所谓的飞机功能可能越来越容易受到硬件设计错误的不利影响的考虑，因为硬件的复杂性日益增大，这些错误越来越难以处理。为了应对这种逐渐增加的风险，有必要确保在设计和鉴定过程中以更加一致和可检验的方式来识别潜在的硬件设计错误。

随着机载电子硬件变得更加复杂，技术不断进步，以及应用经验和本文档所述程序的使用经验的增加，本文档将被修订和评审到与批准的 RTCA/EUROCAE 程序相互一致。

1.1 目的

编制本文档旨在通过提供设计保证指南来帮助组织进行机载电子硬件的开发，使其能够在特定的环境下安全地实现其预期功能。本指南应被等同地应用于当前的、新的和发展的技术。本文档的目的在于：

1. 定义硬件设计保证目标。
2. 描述这些目标的基础以助于确保对该指南的正确解释。
3. 提供对这些目标的描述，使开发手段符合本指南及其它指南。
4. 为设计保证活动提供指南，以满足设计保证目标。
5. 在新工艺技术可获得时，允许灵活选择所需要的工艺来满足本文档中包括改进项目的目标。

本文档推荐了实施活动来满足设计保证目标，而不是详细描述如何进行设计。

用于生成本指南文档的原理是一种自上而下的透视法，它基于电子硬件所实现的系统功能，而不是自下而上透视法，或仅基于用于实现该功能的特定硬

件部件的方法。在通过改进报告的系统和硬件设计决定，以及有效的验证过程来识别安全性设计错误时，自上而下的方法更为有效。例如，应在系统、组件、子组件、部件或硬件项目中既能实现硬件项目与其要求的符合性，又可满足验证目标的最高层级来进行验证。

1.2 范围

本文档提供了机载电子硬件的设计保证指南，其范围从概念设计到初始鉴定和后续的鉴定后产品改进，以确保持续的适航性。它是在显示与运输类飞机和设备鉴定要求的符合性的基础上进行编制的，但本文档的一部分也可以适用于其它设备。

文档中对系统生命周期和硬件设计生命周期之间的关系进行了描述，以助于对系统和硬件设计保证过程之间的相关性进行理解。系统生命周期的完整描述，包括系统安全性评估（SSA）和批准，以及飞机鉴定过程并未涉及。

鉴定问题只在与硬件设计生命周期相关的方面进行讨论。针对生产、试验和维持硬件项目的能力的问题，只在与硬件设计的适航性相关时才被提及。

本文档中的指南适用于，但不局限于下列硬件项目：

1. 航线可替换装置（LRU）。
2. 电路板组件。
3. 客户微编码部件，如特定用途的集成电路（ASIC）和可编程逻辑设备（PLD），包括任何相关的宏功能。
4. 集成技术部件，如混合电路和多芯片模块。
5. 商业货架产品（COTS）部件。

因为 COTS 部件供应商或许不一定遵循本文档描述的设计过程或提供必要的硬件设计生命周期数据，特别针对 COTS 部件的其它考虑包含在第 11 节中。

本文档并不试图定义固件。固件应归类为硬件或软件并由适用的过程来述及。本文档假定在系统定义期间，已经为硬件或软件分派了功能。RTCA DO-178/EUROCAE ED-12 提供了关于在软件执行中被分配的功能的指南。本文档提供了被分配给硬件的功能的指南。

注：这就使得在指定了系统时和分配了功能时，可以确定一种有效的实施方法和设计保证。在完成了分配时，所有相关方均应同意该机制的决定。

硬件项目设计和验证中使用的工具的评估和鉴定在第 11.4 节中进行了描述。

本文档并不提供关于组织结构或在这些结构中如何划分职责的指南。

环境鉴定准则也在本文档所及范围之外。

1.3 与其它文档的关系

除了适航性要求之外，存在着针对硬件的各种国家和国际标准。在一些国家，可能会要求与这些标准一致。然而，援引特定的国家或国际标准，或者推出一项建议使这些标准可用作对本文档的替代或补充，已经超出了本文档的范围。

在本文档中使用术语“标准”时，它应被解释为使用机载系统、机载设备、发动机或飞机制造商所使用的特定项目的标准。这些标准可以从制造商制定或引用的一般标准中引申出来。第 10.2 节中提供了关于标准的指南。

1.4 相关的文档

SAE ARP4754/EUROCAE ED-79《高度集成或复杂飞机系统的鉴定问题》，可作为高度集成或复杂飞机系统开发指南的来源。

SAE ARP4761《民用机载系统和设备实施安全性评估过程方法指南》，可作

为硬件设计保证过程中使用的安全性评估方法的来源。

RTCA DO-178/EUROCAE ED-14《机载设备的环境条件和测试程序》，可被设备设计者用作硬件项目鉴定的主要的环境测试标准。

1.5 如何使用本文档

本文档预期为国际航空团体所使用。为便于此应用，对特定国家的规程和程序的引用被减少了。代之以使用一般性的术语。例如，使用了术语“鉴定机构”来指以国家的名义给予批准的负责鉴定的机构或人员。在第二个国家或一些国家要进行批准或参与此鉴定时，可以使用本文档，因为在所涉及的国家之间对双边协议或谅解备忘录给予了承认。

本文档中的指南代表了航空团体的一致意见，是机载电子硬件设计保证的最佳工业实践的一个集合。纳入本文档中导出的过程，是为了生成能适用于完整的新硬件设计和后续更改的指南。对以前为其它过程开发的硬件的指南参见第 11.1 节。可以理解为，除了此处描述的之外，其它手段也可以为使用者获得和使用。

在用例子表明了如何应用本指南的场合，无论是图示的还是通过文字描述的，该例子都不能被解释为优选的方法。

第 11 节讨论了针对特定已知情况的其它考虑，在这些情况下，第 2 节到第 9 节的一些目标无法得到满足。这些考虑包括对先前开发的硬件的使用，COTS 部件的使用，产品维护经验，以及工具评估和鉴定。

附录 A 提供了针对必要的硬件设计生命周期数据的指南，这些数据基于所实施的硬件设计保证级别。

附录 B 包含了关于用于实现 A 级和 B 级功能的硬件的设计保证技术指南，该指南应作为第 2 节到第 11 节中指南的补充。根据使用者的自行判断，附录 B

可应用于设计保证级别为 C 级和 D 级的硬件。

本文档中使用的术语总汇包含于附录 C 中。附录 D 包含了一个本文档中使用的缩略词列表，并拼出了其完整的名称。

一个列表并不意味着任何时候其元素都是完备的，或所有元素都与任何特定产品相关。

本文档中使用了注释来提供解释性的材料，强调某个重点，或提醒对相关主题的注意，这些内容并未在文中完整描述。注释中并不包括指南。

当旨在提供指南时，使用了单词“应当（Should）”，而与可选的文本相联系时，使用了单词“可（May）”。

本文档中使用了术语“硬件项目”来描述作为本文档主题的电子硬件。

除非另外特别说明，在贯穿本文范围内假定使用了修饰词“硬件”。当使用术语“要求”时，即意味着硬件要求。一个系统或软件修饰词将会被特别说明，如系统要求。

注：各种工业咨询文档和航空要求文档中并不总是使用经过协调的术语。例如，联邦航空规定（FAR）第 21 条和联合航空要求（JAR）第 21 条使用的术语“产品”是指一架飞机、飞机发动机、螺旋桨。文档 SAE ARP4754/EUROCAE ED-79 所使用的术语“产品”是指作为对定义的要求集的响应而生成的硬件、软件、项目或系统。建议读者在术语使用中的这些和其它不同之处。本文档使用了术语总汇中的定义。

1.6 复杂性的考虑

尽管使用了各种级别的术语“复杂性”来描述电子设备，如简单、复杂、高度复杂等等，这些级别之间的不同点却未被严格地定义。此处复杂性的定义区别是基于通过已确定的手段实现可接受的鉴定覆盖率的可行性和难度级别来

确定的。

硬件应在集成电路、电路板和 LRU 级别按层级检查其复杂性，包括所涉及的不可检查的功能，例如在多用途设备中未使用的模式和在后续机器中潜在隐藏的状态。

只有在确定的测试的综合性组合和适于设计保证级别的分析能够确保在所有可预见的工作条件下能获得正确的功能性特性而没有任何异常动作的情况下，才能将一个硬件项识别为简单项。

当一个项目不能被划分为简单项时，它就应当被划为复杂项。一个完全由简单项构成的项目可能其本身是一个复杂项。包含一个设备，如一个 ASIC 或一个 PLD 的项目可以被视为简单项，如果它们满足本节中所描述的简单项的条件的话。

对于复杂项，所提出的提供设计保证的措施应在硬件设计生命周期的早期就征得鉴定机构的同意，以减少程序的风险。

对于一个简单的硬件项目，设计过程的扩充归档是不必要的。验证和构型管理的支持过程和归档工作需要完成，但不需要扩充归档。这样，在设计一个简单的硬件项目以符合本文档时就会减少过头的现象。该文档的主要影响是针对复杂硬件项目的设计。

1.7 可选择的方法和过程

除本文档所描述的内容之外的方法或过程可以用于提供硬件设计保证。这些方法和过程应基于其能力进行评估以满足适用的规定，可选择的方法或过程在投入使用前应经过鉴定机构批准。作为与适用的规定直接比较的代替，使用者可以在与本文档进行比较来对备选方法或过程进行评估时使用下列指南来减少程序风险。

关于评估可选方法或过程的考虑可能包括：

1. 在用于代替本文档所描述的过程时，符合第 2 节至第 9 节的目标中的一个或多个的过程应显示出等同的设计保证级别。
2. 应对所提出的可选方法或过程对符合硬件设计保证目标的影响进行评价。
3. 应对所提出的可选方法或过程对生命周期数据的影响进行评价。
4. 使用所提出的可选方法或过程的基本原理应通过证据证实该方法或过程将产生预期的结果。

1.8 文档概述

图 1-1 是对本文档中各节内容、它们的一些相互关系和与其它相关过程的关系的形象化概述。这里并未打算显示数据流，而是显示出哪一节与外部过程是相关的。

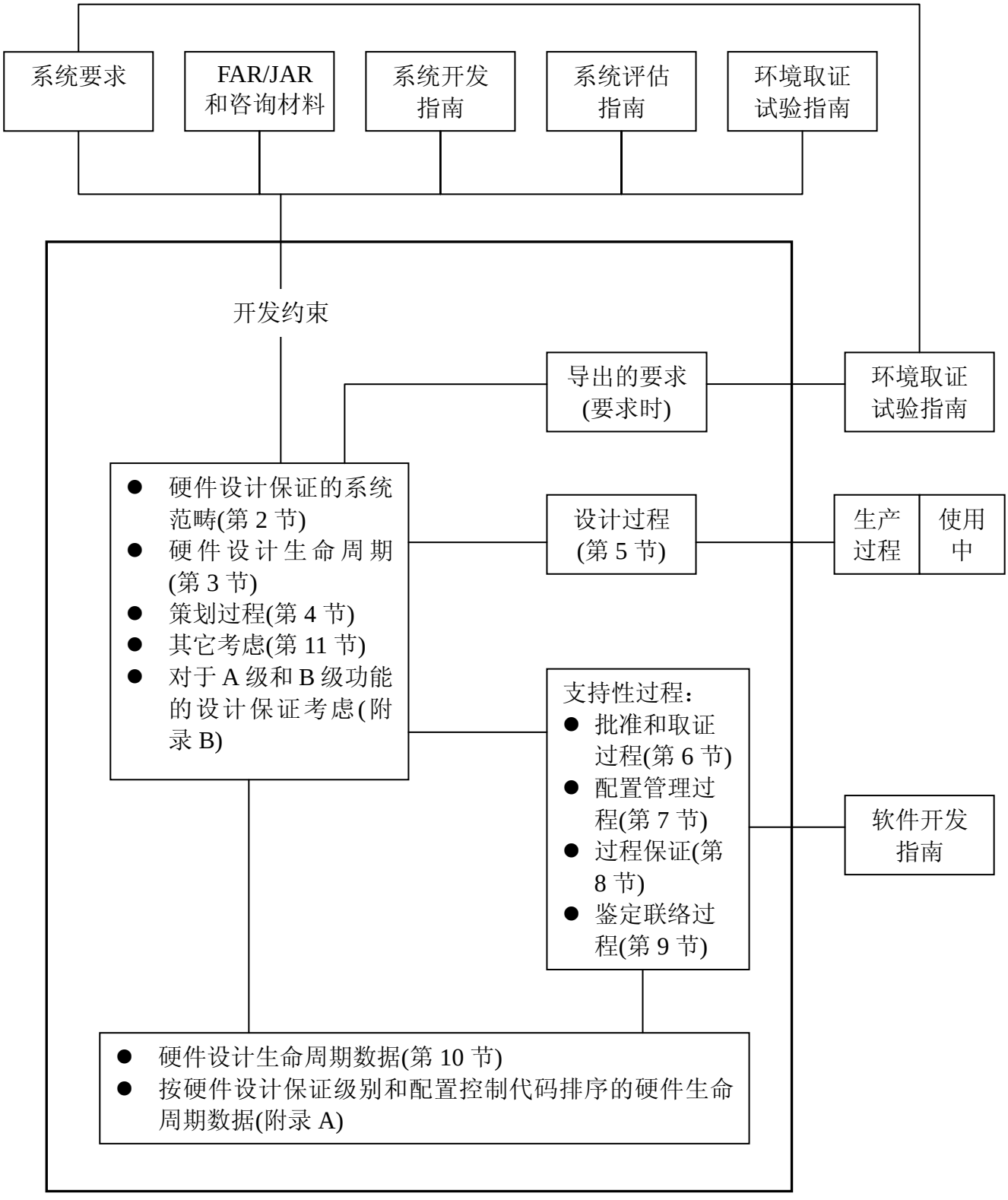
系统要求
FAR/JAR
和咨询材料
系统开发
指南
系统评估
指南
环境取证
试验指南
开发约束
导出的要求
(要求时)
环境取证
试验指南
硬件设计保证的系统范畴(第 2 节)
硬件设计生命周期(第 3 节)
策划过程(第 4 节)
其它考虑(第 11 节)
对于 A 级和 B 级功能的设计保证考虑(附录 B)
设计过程
(第 5 节)
生产
过程
使用
中
支持性过程:
批准和取证过程(第 6 节)
配置管理过程(第 7 节)
过程保证(第 8 节)
鉴定联络过程(第 9 节)
软件开发
指南
硬件设计生命周期数据(第 10 节)
按硬件设计保证级别和配置控制代码排序的硬件生命周期数据(附录 A)

图 1-1 文档概述

2.0 硬件设计保证的系统范围

硬件设计保证起始于系统功能被分配给硬件的系统级及对应的系统开发保证级别被赋值时。

单个系统功能可以分配给一个硬件项目，一个软件部件或硬件和软件的一个组合。从一个系统透视、一个软件透视和一个硬件透视中提出了与此功能相关的安全性要求来确定满足这些要求所需要的可靠性级别和保证级别。

图 2-1 示出了机载系统和设备的系统开发过程与安全性评估、硬件开发和软件开发过程的关系。

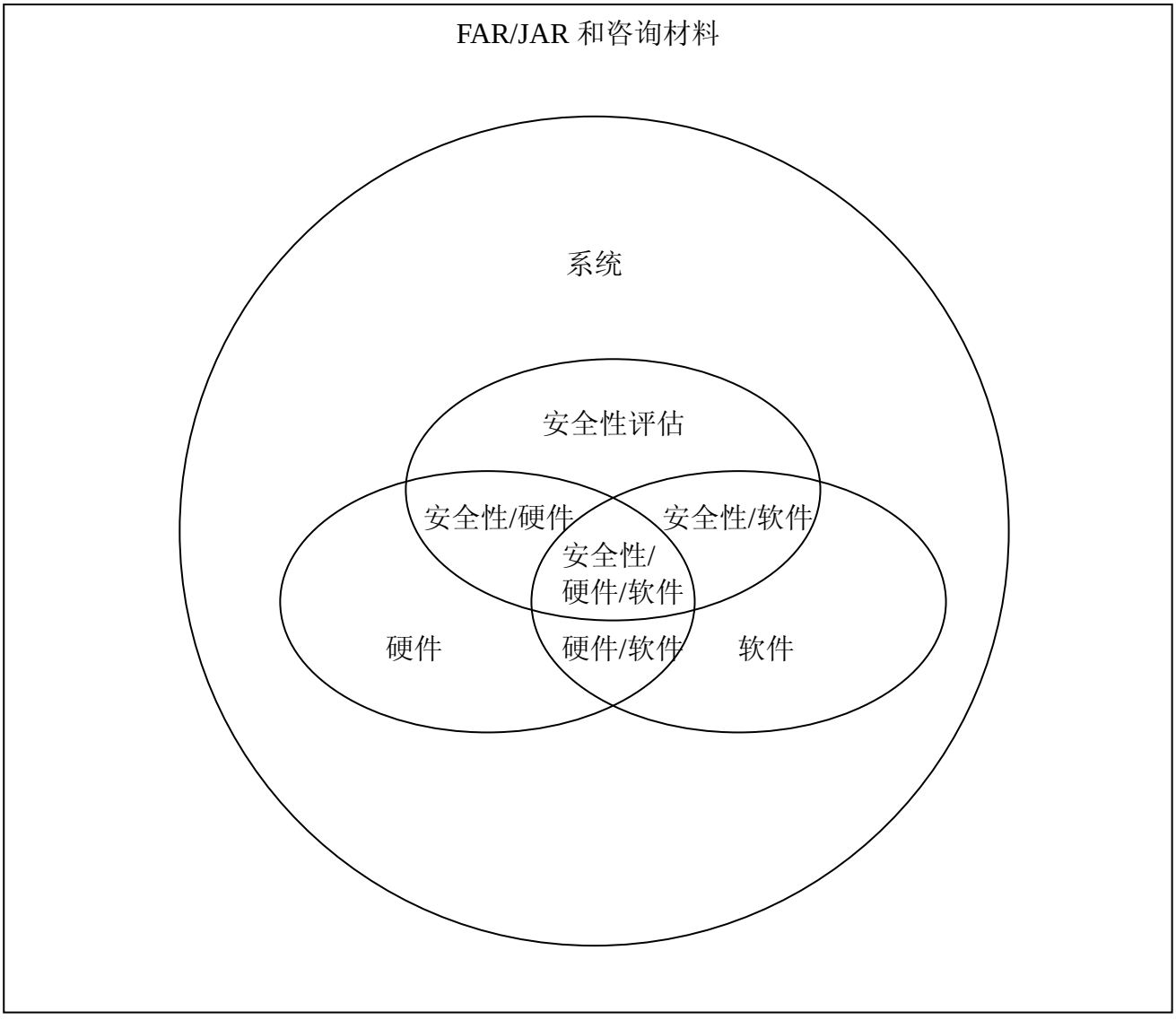

图 2-1 在机载系统、安全性评估、硬件和软件过程之间的关系

在图中有四个重叠的区域，安全性/硬件、安全性/软件、硬件/软件和安全性/硬件/软件。这些重叠示出了在这些过程之间的关系和相互作用，其中系统要求可能会导致在此范围内的要求和多个过程的设计保证指南。例如，一个包含安全性要求的硬件功能会牵涉到安全性评估过程和硬件设计生命周期过程。

这种重叠显示了需要在过程之间具有协调的相互作用以确保该系统功能的保证要求得到满足。系统或软件保证过程的讨论超出了本文档的范围。然而，在协调硬件功能的设计保证时，使用者或许希望利用由系统或软件过程中的活动提供的保证。

这些关系和相互作用将在第 2.1.1 至第 2.1.3 节作进一步描述。

2.1 信息流

在生命周期过程之间的信息流示于图 2-2。下列章节描述了从系统开发过程到硬件设计生命周期过程、从硬件设计生命周期过程到系统开发过程，以及在硬件设计生命周期过程及其软件生命周期过程之间的信息流。

注：可以看出这些是迭代的过程，在贯穿硬件设计生命周期的各时段将出现变化。

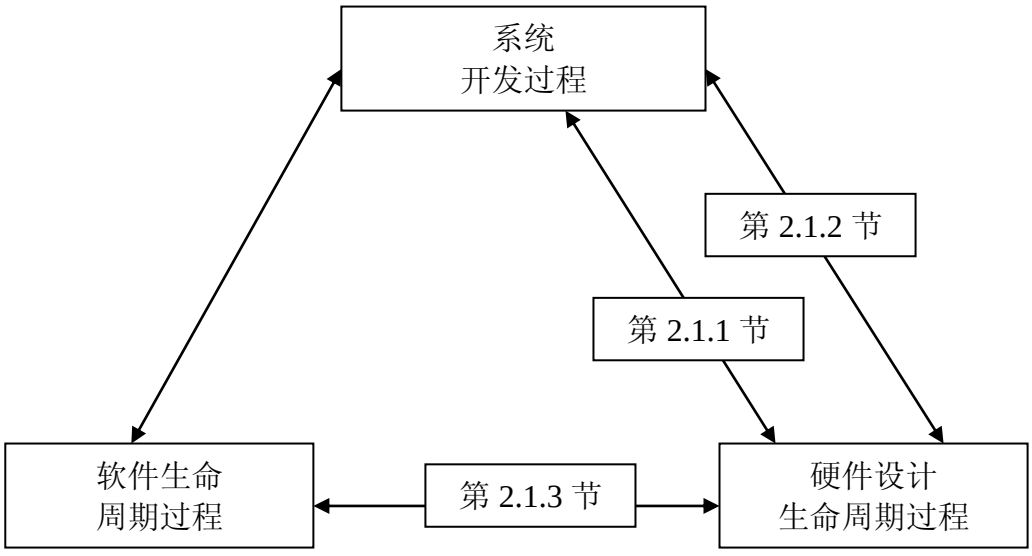

图 2-2 系统开发过程

2.1.1 从系统开发过程到硬件设计生命周期过程的信息流

该信息流可能包括：

1. 分配给硬件的设计和安全性要求。
2. 适用时，每项功能的设计保证级别，以及与其相关的要求和故障状态。
3. 对于硬件功能性故障，分配的几率和暴露于风险状态的次数。
4. 硬件/软件接口说明。
5. 对安全性战略和设计约束的要求，例如可测试性、设计方法和硬件结构。
6. 对要通过硬件级别验证来完成的系统验证活动要求。
7. 分配给硬件的安装、人类工程学和环境要求。
8. 可能对要求有影响的集成问题报告。这些可能作为活动，如系统验证、系统要求或 SSA 的生成等的结果而形成。

2.1.2 从硬件设计生命周期过程到系统开发过程的信息流

该信息流可能包括：

1. 要求的实施，如机械图纸、原理图和部件清单。
2. 可能对任何分配的要求有影响的硬件导出要求。
3. 实施结构，包括故障容许边界。
4. 在硬件设计生命周期中完成的任何要求的系统验证和批准活动的证据。
5. 产品安全性分析数据，如：
    a. 所标识的与 SSA 过程有关的硬件功能性故障的几率和失效比。
    b. 共模故障分析。
    c. 隔离边界和一般故障缓解战略。
    d. 与系统要求有关的潜在分析数据。例子有针对故障监控、故障检测间隔和无法检测的故障的硬件条款。

6. 对要通过系统级验证来完成的硬件验证活动的要求。

7. 使分析生效所必需的针对安装要求和环境条件的假定和分析方法。

8. 可能对系统、软件或分配的硬件要求有影响的问题或变更报告。

2.1.3 在硬件设计生命周期过程和软件生命周期过程之间的信息流

该信息流包括：

1. 硬件/软件集成所需要的导出要求，例如协议的定义、定时约束以及对硬件和软件之间接口的寻址程序。
2. 硬件和软件验证活动要求进行协调的例子。
3. 在硬件和软件之间识别出的不兼容性，它可以是报告和纠正措施体系的一部分。
4. 安全评估数据，它也应可被系统过程所获取。

2.2 系统安全评估过程

共有三种系统安全评估过程：功能性危害评估（FHA），初级系统安全性评估（PSSA）和 SSA。这些过程被用于建立适用于系统开发保证过程的系统安全目标，并确定达到安全性目标的系统功能。

SSA 过程应将安全性目标转换为系统和设备安全性要求。这些要求应包括基本安全性目标和关于系统和设备功能与结构的安全属性。SSA 过程和系统开发过程会将这些安全要求分配给硬件。

共有 5 个系统开发保证级别，A 级至 E 级，分别对应于 5 种失效状态级别：灾难性的、危害严重的、主要的、次要的和无影响的。表 2-1 将硬件设计保证级别与 5 种失效状态级别对应起来，并提供了硬件失效状态及其对应设计保证级别的定义。最初对于每种硬件功能的硬件设计保证级别是由 SSA 过程通过使用 FHA 识别潜在危害来确定的，然后 PSSA 过程将安全要求和相关的失效状态分

配给在硬件中实现的功能。

在整个硬件设计生命周期，在安全性、系统和硬件过程之间会有反复的反馈来确保所设计和制造的硬件满足被分配给该硬件的系统安全性、功能性和性能要求。

表 2-1 硬件设计保证级别定义及其与系统开发保证级别的关系

系统开发保证级别	失效状态分级	失效状态描述	硬件设计保证级别定义
A 级	灾难性的	失效状态将妨碍连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 级	危害严重的	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力的大幅降低，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 级	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力的明显降低，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 级	次要的	失效状态并不明显地减低飞机安全性，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力稍有降低，飞行人员工作负荷稍有增加，例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 级	无影响的	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，不需要使用本文档的其它指南，但这些指南可作为参考。

2.3 硬件安全评估

硬件安全性评估是与 SSA 过程一起进行的，并用于支持 SSA 过程。本安全性过程的目的是显示适用的系统和设备，包括硬件，已经满足适用的飞机鉴定要求的安全性要求。

已知安全性后，就可由系统过程将功能和性能要求分配给硬件，硬件的安全性评估确定了对于每个功能的硬件设计保证级别，并有助于确定所要采用的相应的设计保证策略。

2.3.1 硬件安全评估考虑

硬件项目的设计者可通过一个适当的设计保证策略来显示与分配给硬件的安全性要求的符合性和与硬件设计表征级别的符合性。

对于整个硬件项目可以应用单个设计保证级别和策略，而一个硬件项目也可以评估为具有不同的功能失效路径（FFP），以便适应设计保证级别或设计保证策略的组合。可以使用功能失效路径分析（FFPA）来判断某部分硬件项目的较低设计保证级别，或适应以不同的技术或产品服务历史实现的不同功能。

注：FFPA 在附录 B 第 2 节中进行了描述。尽管所叙述的内容是附录 B 的主题，该分析方法仍可用于任何设计保证级别。

如果某个硬件项目包含分别具有不同设计保证级别的功能，此时可以通过下列方法之一来处理：

- 确保整个项目为最高的设计保证级别。
- 如果可以保证其功能、接口和共享资源不会受到来自较低设计保证级别的功能的不利影响，则各硬件功能可以分别保障为由硬件安全性评估所定义的各自的硬件设计保证级别。共享资源的设计保证应为最高级别功能的设计保证级别。

关于安全性评估的指南包括：

1. 反复的硬件安全评估和设计应确定导出的硬件安全性要求，确保分配给硬件的系统安全性要求得到满足，并确保该导出要求得到满足。
2. 这些导出要求应包括对硬件结构、电路和部件的安全性要求，并防止出现异常动作，包括纳入特定的硬件结构和功能性安全属性，例如：
   a. 电路或部件冗余度。
   b. 在电路或部件之间进行隔离或电气绝缘。
   c. 在电路或部件之间的非相似性。
   d. 电路或部件的监控。
   e. 保护或重新配置机制。
   f. 对电路和部件随机失效和潜在失效允许的失效比和几率。
   g. 用途或安装的限制。
   h. 混乱的防止和管理及混乱的恢复。
3. 硬件设计保证过程和硬件安全性评估应共同确定特定的符合性措施和对于每个功能的设计保证级别，并确定已经达到的可接受的设计保证级别。

注：硬件的异常动作可能是由硬件项目中的随机失效或设计错误所导致的，或是由硬件的混乱导致的。

对于某个硬件项目功能，硬件设计者可以选择一个较高的硬件设计保证级别。例如在某安装位置硬件项目的复用就要求有较高级别的设计保证。

硬件安全性评估可以使用各种定性的和定量的评估方法。这些方法包括故障树分析（FTA），共模分析，失效模式和效果分析，以及适用于随机故障定量评估的统计学可靠性分析方法。

2.3.2 随机硬件故障的量化评估

基于硬件失效比、冗余度、隔离度和绝缘度、故障模式统计、概率分析、部件减定额、应力分析和制造过程控制的统计学故障评估和预见方法，已经被证明是可以接受的评估硬件随机故障的定量风险因素的手段。

2.3.3 硬件设计错误和混乱的量化评估

不同于硬件的随机故障，设计错误和一些类型的混乱都不能按统计学方法进行预见，它们会以共模故障的形式穿过冗余度边界。应适当选择要使用的冗余度管理技术和定量评估方法，使潜在的共模故障和混乱的影响在必要时得以排除或减轻。

尽管难以定量评估，来自设计错误和混乱的安全性风险仍可以通过定性的安全评估方法的实际应用来进行有效的评估。诸如故障树分析、共模分析和功能性故障模式与影响分析（F-FMEA）之类的分析技术基本上都是定性方法，可以用于识别硬件设计错误和混乱。更为特殊地，这些方法可以确定设计错误和混乱的潜在影响，有助于确定排除或减轻这种影响的手段。使用这些方法，硬件安全性评估可以有助于确定要使用的硬件设计保证策略，并可在硬件设计过程中反复使用以便定性的确定使用所选择的策略能够得到的保证。

2.3.4 硬件故障状态分类的设计保证考虑

随着系统故障状态严重程度的增加，确保相关故障状态被减轻所需要的硬件设计保证的程度也增加了。对于所有的设计保证级别，均应选用一种手段或策略来确保达到适当的设计保证级别。图 2-3 勾画出了用于选择适当的设计保证策略的决策过程。

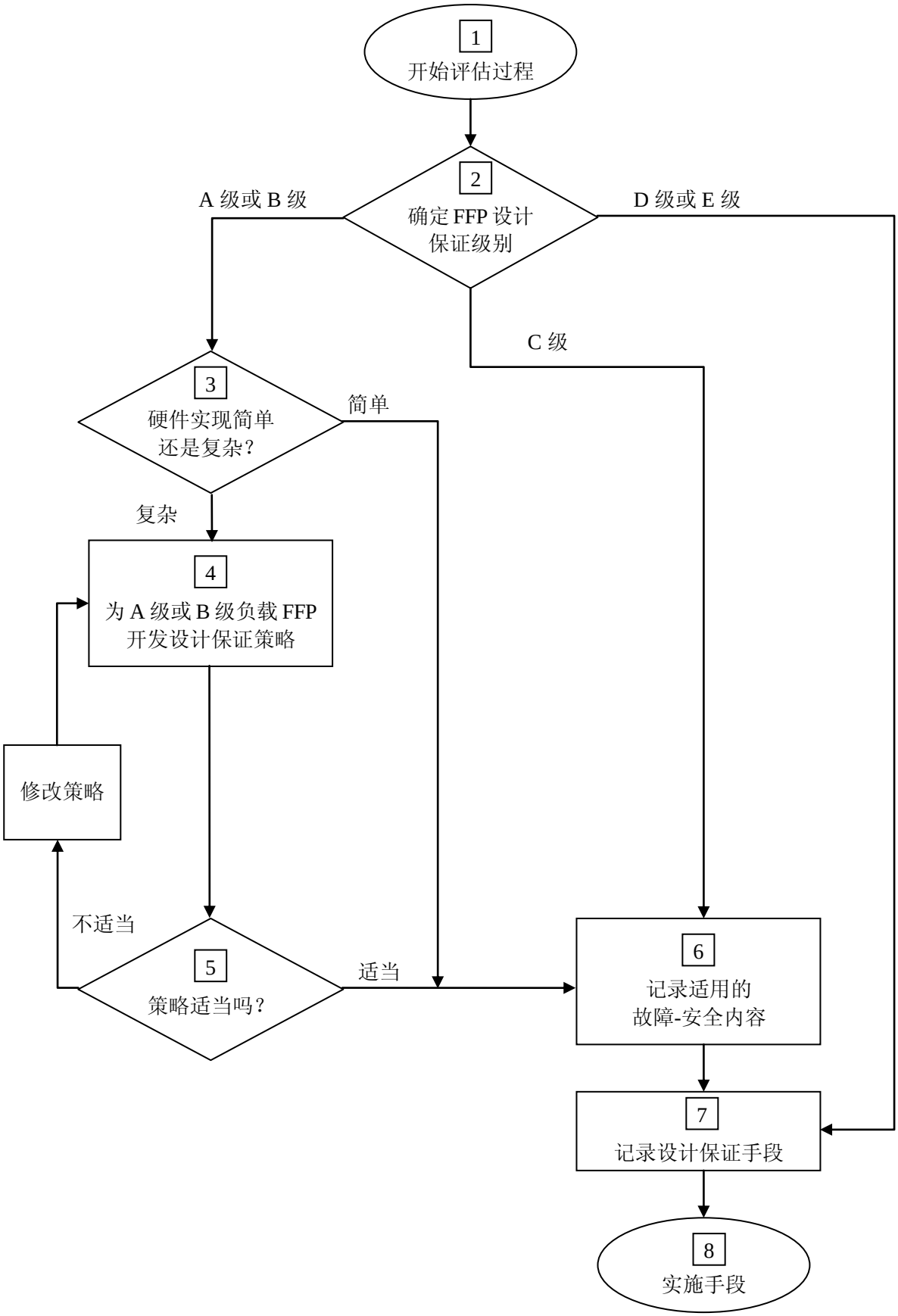

图 2-3 选择硬件设计保证策略的决策过程

指南包括：

1. 对于硬件中实现的 A 级或 B 级功能，对设计保证的考虑应识别出该硬件功能的潜在的异常动作和潜在的设计错误。
2. 在为每个被实现的硬件功能选用设计保证策略时，应使用图 2-3 中勾画的决策过程。
3. 除第 3 节至第 11 节提供的指南外，附录 B 中描述的策略应适用于 A 级和 B 级功能。
4. 设计保证策略应选择作为硬件结构和用途的函数，以及所选择的硬件实现技术的函数。

不同的技术、部件选择和部件用途提供了不同程度的硬件设计生命周期信息，以及不同程度的针对设计错误及其影响的固有保护。对于同一硬件项目内的不同功能路径，最适当的设计保证方法会是不同的。

图 2-3 的决定区和行动区中的号码是为参考在该图之后的编号项目，这些项目提供了关于决定或行动的进一步说明。

1. **开始评估过程。**对于所有设计保证级别，应当选择一种手段或策略来确保获得适当的设计保证级别。
2. **确定 FFP 设计保证级别**。对于每个被识别的硬件项目，确定并记录与该项目相关的 FFP 和设计保证级别。应使用常规的安全性评估技术来确定那些硬件电路在、那些硬件电路不在所识别的 A 级或 B 级 FFP 中。
3. **FFP 的硬件设计简单还是复杂**？对于 A 级或 B 级硬件设计保证 FFP，按第 1.6 节中所述来确定硬件是简单还是复杂。
4. **选择针对 A 级或 B 级复杂 FFP 的设计保证策略**。如果 FFP 是复杂的而且是 A 级或 B 级，则使用附录 B 中描述的其它策略来确定适当的设计保

证策略、对应的实施概念和减轻错误的方法。对于每个 A 级或 B 级 FFP，应使用先进的分析、产品服务经验或结构性调整来确定设计保证策略。如果所选择的手段并未提供对潜在故障和异常动作的全面减轻，则实施中的 A 级 FFP 可能要求不止一种手段。

5. **策略适当吗**？确定在设计保证策略中是否有缺陷，而如果在策略中存在缺陷或在可获得的数据中存在缺陷，应通过提出其它的设计保证、实施或结构性策略来修改策略以纠正该缺陷。

   当设计保证策略可以接受时，应记录对于每个 FFP 的设计保证过程，该策略也应识别鉴定机构参与的内容，例如里程碑计划、程序评审和监视行动。

6. **记录适用的故障-安全内容**。确定适当的故障-安全设计结构和硬件项目的特性，并完成一项分析来满足系统的获得性和完整性要求。记录故障-安全设计内容及相关的共模分析、概率分析、结构和其它特性。
7. **记录设计保证手段和策略**。记录并获取系统鉴定计划或硬件鉴定计划（PHAC）中鉴定机构对适用的设计保证手段和策略的批准。
8. **实施手段**。按照符合批准计划中所定义的适当的设计保证手段来实施硬件设计，并记录符合批准的计划和策略的证据。

3.0 硬件设计生命周期

本节描述了在第 4 节至第 9 节中讨论的硬件设计生命周期。本文档并未预先描述一个优选的生命周期模型，也未暗指针对执行机构的结构。硬件设计生命周期等同地适用于新系统或设备的开发及对现有系统或设备的改动。每个项目的生命周期应基于过程和由该项目的属性确定的活动的选择和安排，例如稳

定性要求、先前开发的硬件的使用，以及硬件设计保证级别。硬件设计生命周期过程可以是迭代的，意即，由于增量式开发和过程之间的反馈导致的进入、再进入和修改。

3.1 硬件设计生命周期过程

硬件设计生命周期过程是：

1. 第 4 节中描述的硬件计划过程，它定义和协调了对于某项目的硬件设计和支持性过程的行动。
2. 第 5 节中描述的硬件设计过程，它生成了设计数据和形成的硬件项目。这些过程是需求分析、概念设计、详细设计、实施和生产转移。
3. 第 6 节到第 9 节中描述的支持性过程产生了硬件设计生命周期数据，这些数据确保了硬件设计生命周期及其输出的正确性和控制，包括策划、设计、硬件安全性评估和支持性过程。这些过程一般是与策划和设计过程同步进行的。这些过程有批准、验证、构型管理、过程保证和鉴定联络等。

3.2 转移条件

在不同的开发阶段开发具有不同子项目的硬件的挑战要求有对设计过程提供合理控制的手段，以便管理在完成前一过程的全部元素之前启动下一过程的风险。转移条件，定义为用于评估从一个过程到另一个过程的运动的最少数据，可以在关键过程点使用。在策划过程的分析应确定转移条件的使用。没有必要在计划中定义的每组过程步骤之间建立转移条件。转移条件的选择应当识别出对安全性的影响。例如，在为鉴定目的而对某项功能进行验证之前，对该功能的要求需要加以记录，而且该功能的实现需要在构型管理之下。

转移条件应当记录在硬件计划中。转移条件的使用并未暗指任何特定的生

命周期模型，或阻止诸如快速模型和同步工程之类的开发策略。

4.0 策划过程

本节描述用于控制硬件项目开发的硬件策划过程。该过程产生了硬件计划，该计划可包含于一个或多个文档中。如果使用多个文档，则主要文档中应包含对支持性文档的适当引用。标准文档包含了特定的硬件设计生命周期过程，例如构型管理或过程保证都是可以接受的，只要它们满足针对适用的过程的策划目标。

4.1 策划过程目标

硬件策划过程的目的是定义一个手段，通过该手段可将功能性和适航性要求转化为具有可接受的保证证据的硬件项目，而且该项目将安全地实现其预期的功能。硬件策划过程的目标是：

1. 定义硬件设计生命周期过程。

注：活动、里程碑、输入、输出和组织职责可以包括在计划中。

2. 选择和定义标准。
3. 选择和定义硬件开发和验证环境。
4. 硬件设计保证目标的一致性手段，包括用第 2.3.4 节中的指南识别的策略，被推荐给鉴定机构。

注：新的和发展的技术、工具和过程会要求对策划过程的细节进行改动。因而灵活性是策划过程的一个关键元素。

4.2 策划过程活动

策划过程的指南包括：

1. 硬件设计生命周期过程，包括转移条件，适用时，还包括各过程之间

的相互关系，例如其程序化和反馈机制，都应当进行定义。

2. 推荐的设计方法应予以定义和解释。这包括对预期硬件设计和推荐的验证方法的考虑。
3. 硬件设计标准，如果有任何标准要用于该项目，包括与标准之间可接受的偏差，都应被识别出来。这些可以从一般性的质量标准到公司或程序的特定标准。

   注： 通过提供与从过去的开发中确定的经过证明的工程实践的一致性，标准可以帮助减少出现非预期的设计错误的几率。

   在对新设计和新技术应用新标准时，使用者和硬件开发者应明白其适用性可能是无效的。因为设计的约束、与系统要求的冲突或与新技术的不兼容性的原因，对这些标准的偏离将是必要的。策划过程就是对如果使用标准，哪些偏离可以接受进行评审的一个机会。
4. 应选择在硬件设计过程和支持性过程之间达到协调的方法，并对与系统软件和飞机鉴定相关的活动予以特别关注。

   注：协调可以采用日程表的形式，在日程表上显示出完成本文所述过程目标的事件的里程碑。
5. 每个硬件设计过程和相关的支持过程的活动应被定义下来。该定义应在使硬件设计过程和相关的支持性过程能被控制的阶段进行。
6. 应选择设计环境，包括将被用于开发、验证和控制硬件项目和生命周期数据的工具、程序、软件和硬件。
7. 对所建立的计划形成偏离的过程，如果偏离是必需的并且影响鉴定，就应当予以识别。

8. 要用于识别、管理和控制硬件、相关的基线和硬件设计生命周期数据的政策、程序、标准和方法应予以描述。
9. 当使用者打算对所有或部分的硬件设计生命周期使用转包商的话，硬件计划应识别用于确保设计保证目标得到满足的方法。
10. 用于硬件设计过程的过程保证的实施的政策和程序应予以描述。
11. 验证过程独立性、过程保证独立性和相关的机构职责应在 PHAC 中予以描述。
12. 应记录满足此指南目标的方法，并在过程的早期与鉴定机构进行沟通。这些方法应记录在 PHAC 中。

注：鼓励定期对这些方法的任何偏离进行协调，以便在有满足设计保证要求的适当证据时，所得到的鉴定数据的可接受性最大。

5.0 硬件设计过程

硬件设计过程将产生一个硬件项目，该项目满足从系统要求中分配给硬件的要求。本节描述了图 5-1 中所描述的 5 个主要过程。这些分别是需求分析、概念设计、详细设计、实施和生产转移。这些过程可以适用于硬件项目的任何层级，例如 LRU、电路板组件和 ASIC/PLD。下列各节描述了每个过程，其目标和相关的活动，应对这些进行识别以减少出现影响安全性的设计和实施错误的几率。重要的是应对这些过程的每一个进行策划，并在硬件设计计划中详细记录。

每个过程，以及在过程之间的相互作用都可以是反复的。对于每次反复，都应识别该变化对每个过程的效果，并就它对上次反复的结果的影响进行评估。

注 1：在整个设计过程里对过程的产物，如设计注释、设计评审注释和问题

报告等进行记录是很好的工程实践。

当前的做法提供了很多不同的手段，包括图形的、数学的、基于数据库或文本的，来表述要求和设计实施。这些表述的例子有图解、硬件说明语言（HDL）、状态图、逻辑表述和图形方法。

注 2：一些表述被用于特定的过程或过程的组合，例如需求分析、概念设计或详细设计，而一些被用于更有效地实施某个特定的实现技术。应提供支持设计保证级别的证据，无论是否使用了设计表述。

对于所使用的每个设计表述，都应考虑下列内容：

1. 无论是否使用表述或表述的组合，都必需遵循本文档的指南。
2. 设计表述应允许硬件项目被持续一致地被复制出来。
3. 设计表述中的微小变化可能对设计实施具有重大影响。应识别这些变化对设计保证的影响。
4. 在设计数据的基线被建立之后，设计表述环境或方法可能会发生变化。如果出现这种情况，则应对该变化对设计的复制造成的影响进行评估。

HDL 设计表述使用基于编码文本的技术，该技术类似于用于软件表述的技术。其相似性可能会误导人们试图直接对 HDL 或其它等同的硬件规范语言的设计表述使用软件验证方法。本文档的指南适用于对使用 HDL 表述的设计的保证。

注：在本文档中描述的结构化的过程适用于复杂的硬件设计，包括 ASIC 和 PLD 的设计。作为一个例子，下表中将典型的 ASIC/PLD 过程映射到本文档图 5-1 中所述的过程。

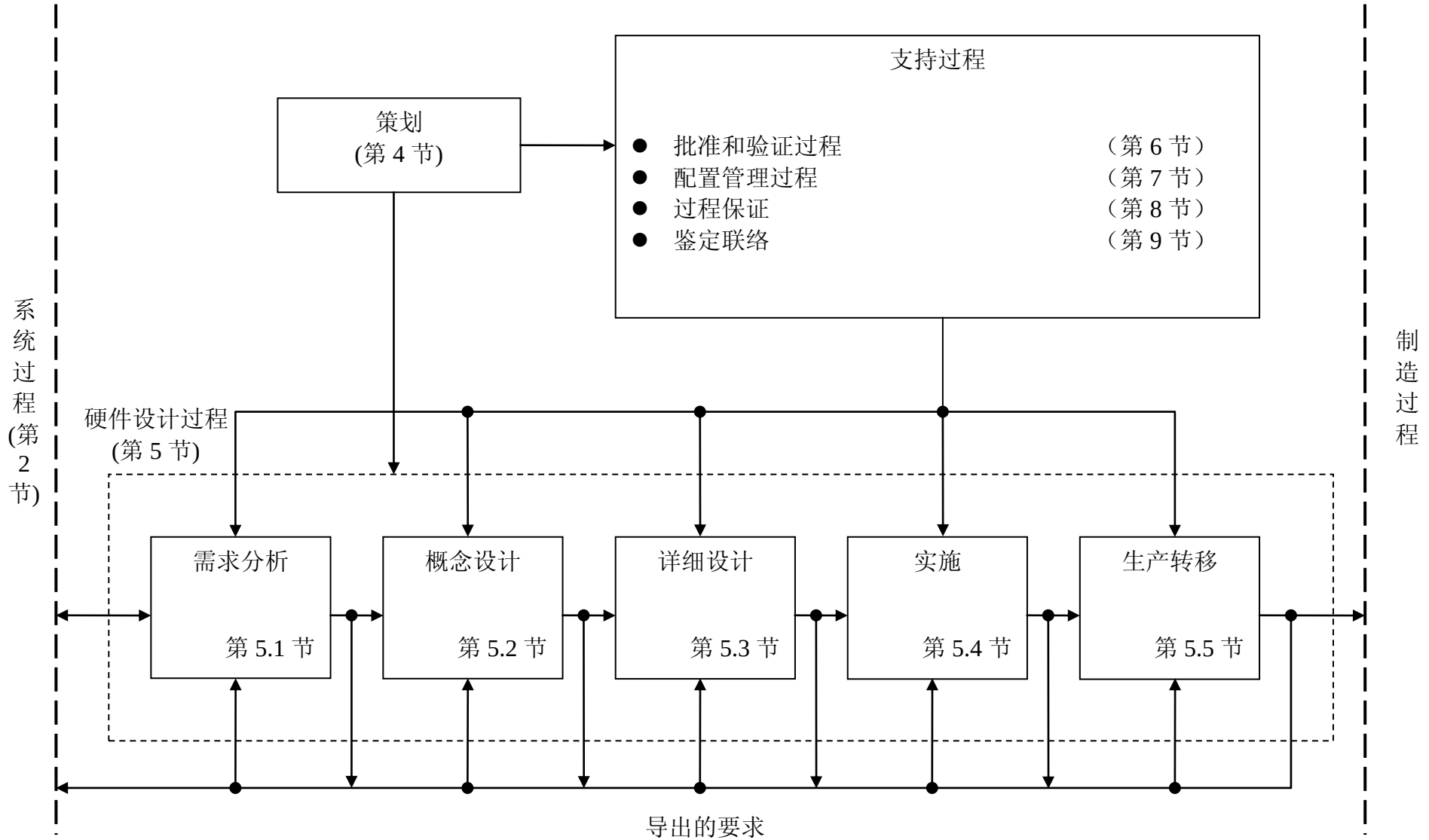

图 5-1 硬件设计生命周期

表 5-1 典型的 ASIC/PLD 过程映射

典型的 ASIC/PLD 过程	过程
部分高级策划	策划（第 4 节）
ASIC/PLD 构造决定	安全评估（第 2.3 节）
ASIC/PLD 需求分析	需求分析（第 5.1 节）
ASIC/PLD 初步设计，包括动作设计	概念设计（第 5.2 节）
ASIC/PLD 详细设计，包括综合、掩膜生成和保险文件	详细设计（第 5.3 节）
ASIC/PLD 制造，包括外部制造和试验，以及对可编程部件进行编程	实施（第 5.4 节）
ASIC/PLD 生产转移	生产转移（第 5.5 节）
ASIC/PLD 批准和验证，包括定时分析、动作仿真、门电平仿真和设计	批准和验证过程（第 5.5 节）
ASIC/PLD 构型管理，包括工具和部件数据库	构型管理过程（第 7 节）

5.1 需求分析过程

需求分析过程将识别和记录硬件项目的要求。这些要求包括由推荐的硬件项目结构强加的导出要求，如技术的选择、基本的和可选的功能、环境和性能要求，以及由系统安全性评估强加的要求。因为在设计期间一些其它的要求会变为已知，所以该过程可以是反复的。

5.1.1 需求分析目标

需求分析过程的目标是：

1. 识别、定义和记录要求。这些要求包括从 PSSA 中分配的要求和从硬件安全性评审中导出的要求。

   注：验证结果对硬件要求的溯源性在第 6 节中进行了识别。最理想的是在需求分析过程中建立这种溯源方法。

2. 所产生的导出要求将反馈给相应的过程。
3. 对要求的疏忽和错误将被提供给相应的过程以便得到解决。

5.1.2 需求分析活动

需求分析活动形成了一个反复的过程，它有助于确保要求与设计实现、系统要求和软件要求的符合性。

对需求分析活动的指南包括：

1. 应记录分配给硬件项目的系统要求。这些可能包括识别要求，如功能性和性能和结构的考虑，例如隔离、内建测试、可测试能力、外部接口、环境、测试和维护考虑、电源和物理特性等。
2. 应记录来自与硬件项目有关的 PSSA 的安全性要求。这些要求可能包括：
   a. 强加给要在硬件中实现的功能的设计保证级别。
   b. 对故障或失效的概率要求。
   c. 硬件结构和功能性安全属性，如第 2.3.1 节中所描述的属性，应选择用以满足功能性分配。
3. 应识别因为生产过程、标准、程序、技术、设计环境和设计指南所导致的设计约束。
4. 应确定实施所需要的导出要求。从硬件安全性评估中导出的具有安全性含义的要求应被唯一识别出来。

   注：导出的要求可以识别出状态，例如：

a. 从具有较低设计保证级别的功能接口处来看，确保更高级别设计保证的功能的特定约束可以抵抗低设计保证级别的功能异常。
b. 数据输入的范围考虑了典型的和全规格的数据值，以及数据字或控制寄存器的高和低状态位。
c. 加电复位或其它复位状态。
d. 电源电压和电流需求。
e. 与时间相关的功能特性，如滤波器、积分器和延时器。
f. 可能的状态机器转移，无论它们是否在预料之中。
g. 信号定时关系或在正常和最坏条件下的电器状态。
h. 信号噪声和交叉通讯。
i. 在异步逻辑电路中的伪信号(glitches)。
j. 控制未用功能的特定约束。

5. 导出要求应反馈给 SSA 过程，这样可对对系统要求的效应进行评估。
6. 要求数据应以定量形式记录下来，适用时应附上公差。这并不包括设计或验证方案的说明。
7. 在此过程中发现的要求疏忽或错误应提供给系统开发过程。
8. 要求，包括生成用以满足 PSSA 要求的内容，应溯源到下一个更高层级的要求。导出的要求也应识别出来，并且沿层级跟踪到尽可能远。

   注：对被分配的硬件安全性要求的系统级批准会在需求分析过程出现。导出的硬件要求的批准在第 6.1 节中进行描述。

5.2 概念设计过程

概念设计过程产生了一个高级的设计概念，可对该概念进行评估以确定所产生的设计实施满足要求的潜力。这可以用诸如功能框图、设计和结构说明、

电路卡组件概要和底板草图之类的项目来完成。

5.2.1 概念设计目标

概念设计目标为：

1. 硬件项目概念设计的开发与其要求一致。
2. 产生的导出要求被反馈给需求分析或其它适当的过程。
3. 对要求的疏忽和错误被提供给适当的过程以便得到解决。

5.2.2 概念设计活动

对概念设计活动的指南包括：

1. 对于硬件项目应生成一个高级说明。这将包括：
   a. 与安全性相关的结构性约束，包括识别设计错误和功能性、部件过应力、可靠性和鲁棒性（译注：即坚固性）缺陷所需要的约束。
   b. 任何对软件或其它系统部件的实施约束的识别。
2. 应识别主要部件。应确定它们对硬件安全性要求产生贡献的方式，包括未用功能的影响。
3. 导出的要求，包括接口定义，均应反馈给需求分析过程。
4. 对要求的疏忽和错误应反馈给适当的过程以便处理。
5. 要提供的可靠性、维护性和测试特性应予以识别。

   注：在相关方之间的协调一致是要满足概念设计目标。典型地，可用设计评审来完成这种协调。

5.3 详细设计过程

详细设计过程将产生详细设计数据，并使用硬件项目要求和概念设计数据作为详细设计的基础。

5.3.1 详细设计目标

详细设计过程的目标是：

1. 详细设计是从硬件项目要求和概念设计数据中进行开发的。
2. 导出的要求将被反馈给概念设计过程或其它适当的过程。
3. 对要求的疏忽或错误应提供给适当的过程以便得到解决。

5.3.2 详细设计过程活动

对详细设计活动的指南包括：

1. 用于硬件项目的详细设计数据应在要求和概念设计数据的基础上产生。这可包括组件和相互连接数据、部件数据、HDL、测试方法和硬件-软件接口数据。

   注：在详细设计过程中，验证方法被正式地用于便利在此过程中做出的技术决定。例如，诸如逻辑定时和参数变动之类的设计参数分析可以提供关于设计决定基于什么的信息。
2. 必要时应利用结构化设计技术。这些可能包括对适当的功能性建立安全监视器、在功能和安全性监视器之间的非相似性、排除设计错误对安全性的影响，以及容错设计。
3. 在必要时，应在设计中考虑测试特性以便对安全性要求进行验证。

   注：重要的是以适当的方式进行开发以使某些安全性特性不仅可在硬件设计生命周期进行验证，也可作为验收测试的一部分，并作为返回给服务测试的一个字段。
4. 应进行对未用功能的评估以识别其对安全性的潜在影响。对不利的影响应进行识别。
5. 如果未加处置会影响硬件项目安全性的对设计、安装或操作的约束应予以识别。

6. 在详细设计过程产生的导出要求应反馈给概念设计或其它适当的过程。
7. 在详细设计过程中发现的对要求的疏忽和错误应提供给适当的过程以便处理。

5.4 实施过程

实施过程使用了详细设计数据来产生硬件项目，该项目是测试活动的一项输入。

5.4.1 实施目标

实施过程的目标是：

1. 产生一个硬件项目，它将利用有代表性的制造过程来实现硬件详细设计。
2. 硬件项目实施、组装和安装数据是完备的。
3. 导出的要求被反馈给详细设计过程或其它适当的过程。
4. 对要求的疏忽和错误将被提供给适当的过程以便得到解决。

5.4.2 实施活动

对实施活动的指南包括：

1. 硬件项目应使用设计数据产生，可行时，使用拟用于生产产品的资源。这可包括采购、配套、制造、检验和测试。
2. 通过实施过程产生的导出要求应反馈给详细设计过程或其它适当的过程。
3. 在实施过程中发现的疏忽和错误应提供给适当的过程以便得到解决。

5.5 生产转移过程

在此过程中，应对制造数据、测试设施和一般资源进行检查，以确保生产的可获得性和适宜性。生产转移过程使用来自实施和验证过程的数据来将产品推入生产阶段。

5.5.1 生产转移目标

该过程的目标是：

1. 建立一个基线，它包括支持硬件项目的一致性复制所需要的所有设计和制造数据。
2. 对与安全性有关的制造要求进行了识别和记录，建立了制造控制。
3. 导出的要求被反馈给实施过程或其它适当的过程。
4. 错误和疏忽被提供给适当的过程以便得到解决。

5.5.2 生产转移活动

对生产转移活动的指南包括：

1. 制造数据应从配置的设计数据中准备。
2. 应对制造数据的完整性和与配置的设计数据的一致性进行检查。

   注：对制造文档的性质附加任何条件已超出了本文档的范围。
3. 在生产转移过程期间纳入的任何变动或改进均应进行评价，以确保它们与所有产品要求，尤其是安全性要求联系起来。任何未依从客户或鉴定要求的变动都应经过相关方的批准。
4. 对与安全性相关的制造要求应进行明确定义，使它们在生产过程中得到控制。
5. 应确定改进验收测试准则所要求的数据。
6. 被识别的疏忽或错误应提供给适当的过程以便得到解决。

5.6 验收试验

验收试验显示了所制造的、改动的或修理的产品的特性符合鉴定所依据的单元的关键属性。这些关键属性是用工程判断进行选择的，可作为产品能满足该装置开发要求的指标。

注 1：在制产品的构型控制并非由验收测试活动来完成的功能。本文档第 7 节中所述的构型管理计划应描述使用者如何计划完成此项活动。

本文档的范围的确包括了验收测试准则的确定，包括合格/不合格条件。生产活动，包括验收测试，应视为在本文档的范围之外。

注 2：验收测试并不打算验证对每个生产单元的所有要求。

子项目的测试可以用作验收测试的一部分。

验收测试准则应确保：

1. 识别了电气测试。
2. 必要时识别了环境屏蔽测试。
3. 验收测试提供了对满足安全性要求所需要的设计内容的覆盖。测试未包括的与项目或子项目有关的安全性应予以识别，并提供其它保证手段。这些手段包括分析、设计控制、统计过程控制或其它适当的手段。

5.7 系列产品

该过程不在本文档的范围之内，但对影响设计保证的要素进行了简要描述以使生命周期完整。

该过程在符合生产数据和要求的常规基础上复制了硬件项目。

具体考虑包括：

1. 生产过程或设计变化的管理提供了该改变不会对现有安全性或鉴定或对要求的符合性造成不利影响的保证。

   注：除了由文档主体提出的指南外，第 11.1.1 节包括了“对先前开发的硬件的改动”，在涉及到部件过时时，参考第 11.2 节。
2. 与变动有关的所有文档的升级符合经过批准的构型管理计划。

6.0 批准和验证过程

本节描述了批准过程和验证过程。批准过程保证了硬件项目导出要求相对于分配给硬件项目的系统要求是正确的和完整的。验证过程则保证了硬件项目实施满足所有的硬件要求，包括导出的要求。

6.1 批准过程

此处讨论的批准过程拟用于通过主观和客观过程组合的使用，确保导出的要求相对于分配给硬件项目的系统要求而言是正确的和完整的。批准可以在硬件项目可获得之前或之后进行，然而，典型情况下批准是在贯穿于设计生命周期的整个阶段进行的。

注 1：经验表明对要求的开发和批准可以识别在开发周期早期的细微错误或疏忽，并且减少后续重新设计或不适当的硬件特性出现的机会。

此处讨论的批准过程并不打算批准从系统要求中分配的要求，因为这些要求的批准被假定作为系统过程的一部分出现。此外，并非所有的硬件项目导出要求都需要批准。

对系统安全性或分配给系统的其它部分的功能性要求有影响的设计决定应划为导出要求，并应被批准。另外，设计决定和约束后续设计任务的假定都应作为导出要求进行批准。

需要批准的导出要求应根据分配给硬件项目的系统要求进行批准。未溯源至更高层级要求的导出要求应根据它们被从中导出的设计决定来进行批准。

注 2：包括独立电源的设计决定可导致指导该电源设计的要求的偏离，该独立电源用于完成特定功能的电路。这些导出要求可包括基于故障条件的安全性要求，这些故障条件可能是由从该电源处接收能量的电路所支持的功能的故障或失效所导致的。这些要求应予以批准。

成为导出要求的设计决定的另一个例子是对外围设备的存储器地址分配。通常没有针对该分配的要求基础，然而，一旦进行了分配，则它们将约束后续设计任务，使其符合这些分配，以便使设计正确工作。该导出要求可以勿须批准。

6.1.1 批准过程目标

对导出的硬件要求的审批过程的目标是：

1. 硬件项目将按其验证的导出要求应是正确的和完整的。
2. 导出要求对安全性的影响应进行评价。
3. 疏忽和错误应被反馈给适当的过程以便解决。

6.1.2 批准过程活动

硬件批准目标可通过诸如评审、仿真、原型化、模型化、分析、服务经验、工程评估或测试的开发和执行等活动的组合来满足。

评审过程活动的指南包括：

1. 应识别需要进行批准的导出的硬件要求。
2. 对于第 1 项中识别的每一个要求，应按如下所述识别和满足批准完成准则：
    a. 每个要求都在一些层级通过评审、分析或测试进行了批准。
    b. 每个要求的评审、分析或测试对于批准该要求，尤其是对于安全性而言，都是适当的。
    c. 与每个要求的批准相关的评审、分析或测试结果都是正确的，而且对在实际结果和预期结果之间的差异进行了解释。当预期结果未预先定义，如对于评审和分析时的情况时，批准活动的结果应符合要求，尤其是安全性要求。

注：批准完成准则可基于要求、安全性考虑、工作模式或实施。

3. 应就导出的要求对安全性的影响进行评价。
4. 应就导出的硬件要求相对于分配给该硬件项目的系统要求的完整性进行评价。就此过程的目的而言，当所有被定义的特性均是必要的，而所有必要的特性均被定义时，这一组要求就是完整的。
5. 应就导出的硬件要求相对于分配给该硬件项目的系统要求的正确性进行评价。就本文档的目的而言，当要求的定义明确且在定义的特性中没有错误时，该要求就是正确的。
6. 应建立在导出的硬件要求和批准活动与结果之间的溯源性。
7. 要求的疏忽和错误应反馈给适当的过程以便处理。

6.2 验证过程

验证过程为硬件项目实施满足要求提供了保证。验证包括按验证计划中的定义进行的评审、分析和测试。验证过程应包括对结果的评估。

注 1：硬件设计的安全性内容采用了要通过硬件实现来满足的安全性要求的形式。

本节为应用于硬件设计的验证过程提供了指南。验证过程可以按硬件验证计划中的定义在任何设计层级应用。对于安全性要求，最好是将验证过程应用于设计过程的不同阶段，以增加设计错误以高置信度被消除的几率。一些设计保证级别要求按附录 A 中所述的独立性满足验证过程的目标。

此处并未述及软件验证、软件/硬件集成验证和系统集成验证过程。然而，在这些过程中，硬件要求的验证是一个有效的硬件验证方法。

对已验证的构型的改变可通过相似性、分析、新设计的测试或通过重复初始验证的一部分来重新验证。

注 2：推荐进行在记录的验证过程之外的非正式测试。然而其程序和结果的维护并不一定在构型管理控制之下，但它在检测和消除设计过程早期的设计错误方面却是非常有效的。只有在这种测试被正式化以后，验证的信誉度才能够被认可。

6.2.1 验证过程目标

验证过程的目标是：

1. 为硬件实施过程满足要求提供证据。
2. 在硬件要求、实施和验证程序与结果之间建立溯源性。
3. 识别可以实施，且与该硬件功能的硬件设计保证级别一致的验收测试准则。
4. 将疏忽和错误反馈给适当的过程以便处理。

6.2.2 验证过程活动

验证过程目标可以通过方法，诸如评审、分析和测试的开发与实施等的组合来满足。验证计划列出了应用来显示与要求的符合性的验证活动。

验证活动包括：

1. 应识别需要有验证活动的要求。并不需要在每个层级上对要求进行验证，要求可以在较高的层级上验证。
2. 对验证方法，如测试、仿真、原型化、分析和评估等应进行选择和执行。
3. 应建立在要求、实施和验证程序与结果之间的溯源性。溯源性应与该硬件所完成的功能的设计保证级别一致。除非因安全性考虑而特别要求，一般不要求到详细的部件，如晶体管、电容器或门电路的溯源性。
4. 应进行验证覆盖分析来确定该验证过程是完整的，包括：
   a. 每个要求都在一些层级通过评审、分析或测试进行了验证。

b. 每个要求的评审、分析或测试对于验证该要求，尤其是对于安全性而言，都是适当的。

c. 与每个要求的验证相关的评审、分析或测试结果都是正确的，而且对在实际结果和预期结果之间的差异进行了解释。当预期结果未预先定义，如对于评审和分析时的情况时，验证活动的结果应符合要求，尤其是安全性要求。

5. 验证活动的结果应予以记录。

6. 应将疏忽和错误反馈到适当的过程以便处理。

6.3 批准和验证方法

本节描述了适用于批准和验证过程的一些方法。

6.3.1 测试

测试是一种确认硬件项目正确地响应某个激励或一组激励的方法。测试的例子包括对硬件项目的功能性测试、系统测试、系统批准测试和飞机测试。

测试可以使用手动、自动或特制测试设备来进行。在验证过程中，测试也可以利用内部硬件项目测试能力，如内建测试的优点。

当无法通过在其预期工作环境下对硬件项目进行激励来验证特定的要求时，应提供其它验证手段，并对该手段进行证明。

测试可以在各个硬件设计过程中进行。为鉴定信誉度而进行的测试要求有一个构型项目。系统集成或软件/硬件集成测试结果也可以用于测试信誉度。

对测试的指南包括：

1. 应识别每个通过测试进行批准或验证的要求。环境符合性测试要求是这些要求的一部分。

2. 应为每个测试定义测试激励、顺序和测试条件，如项目的环境温度和所

用的电压。

3. 在测试执行前应定义合格/不合格条件和记录结果的方法。

4. 应记录测试设备的完整识别和每台设备的校准日期。

5. 应记录被测试的硬件项目的构型一致性。

6. 应记录和保存测试结果。

7. 测试失败应反馈个适当的过程以便处理。

6.3.2 分析

分析是用于特定硬件项目特性的评价以证实某个特定要求得到满足的一种详细的、可重复的、分析性的方法。分析的例子是应力分析、设计边界分析、共模失效分析、最坏情况分析和测试覆盖率分析。服务经验可以为各种分析提供数据。

注：随着硬件设计复杂性的增加，最好是利用计算机化的工具，如仿真等来验证设计的要求和实施。

分析可以包括对硬件项目功能的功能、性能、溯源性和安全推断及其与在机载系统或设备中的其它功能之间的关系的仔细检查。单独的分析或分析与其它验证方法的组合为某个要求被正确满足提供了证据。分析应基于由设计过程、服务经验或其它可获得的数据库提供的数据。

对于电路操作的可视化或对于高级别的功能操作而言，仿真都是一种重要的设计分析工具。仿真可用于分析生产变动在硬件参数中的影响，而这种影响很难用其它验证手段来分析，这样就为减少因这些变化而导致的影响安全性的设计错误建立了信心。因为结果取决于所使用的模型和场景，所以在没有其有效性的支持证据时，仿真结果不能单独地用于鉴定信誉度的目的。

分析的例子包括：

1. **热效应分析。**热效应分析验证了当暴露于工作温度环境时，设计实施满足要求。
2. **应力分析。**应力分析验证了部件满足在要求的工作范围满足额定值减少的条件。
3. **可靠性分析。**可靠性分析确定了设计实施是否满足产品的可靠性要求。
4. **设计边界分析。**设计边界分析验证了设计实施满足了其给出了部件可变性的功能要求。
5. **相似性分析。**相似性分析将特性和使用情况与先前鉴定过的系统的特性和使用情况进行比较。
6. **仿真分析。**仿真分析将仿真结果和预期结果进行比较。

6.3.3 评审

评审是用于计划、要求、设计数据、设计概念或设计实施的评价的一种定性的方法。

评审应按相关计划中所述在整个硬件设计生命周期进行。在批准和验证计划中，应对用于鉴定信誉度的所有评审进行识别。

对评审的指南包括：

1. 参与者应具有完成评审所需要的知识。
2. 硬件评审结果可用于允许或否决在硬件设计生命周期过程活动之间的转移。
3. 评审的结果应予以记录，包括做出的决定和要采取的行动的处置。

6.3.3.1 要求评审

要求评审是一种确保要求的可接受性的一种方法。要求评审可在同一评审中同时从批准和验证过程中提出目标。

在初始要求评审后出现的要求变换应接受与最初所用的评审过程相同或等同的评审过程。该评审的目的并非对分配给该硬件项目的系统要求进行批准。

对要求评审的指南包括：

1. 每个要求都应是明确的、可验证的，并对其层级而言足够详细和完整地描述，且不能与其它要求相冲突。
2. 导出的要求应与它们从中导出的系统要求或要求一致。
3. 要求应与 SSA 一致。
4. 导出的安全性要求应加以定义并反馈给 SSA。
5. 要求应与相关的硬件设计标准兼容。
6. 要求应与可获得的技术的能力和局限兼容。
7. 部件的要求，如性能、温度范围、额定值减少和屏蔽等，应符合安全性和可靠性要求。
8. 应涉及测试、维护和制造硬件项目的能力。
9. 应定义软件/硬件接口要求。
10. 要求应能根据计划中定义的准则向上溯源至下一层级。
11. 导出的要求应记录不会在较高层级验证的实施的约束。
12. 疏忽和错误应反馈给适当的过程以便处理。

注 1：下列问题有助于评估要求的完整性：

a. 考虑了上一层级的所有要求吗？

b. 考虑了适用的标准和指南吗？

c. 所有硬件功能和接口都覆盖了吗？

d. 结构完整覆盖了吗？

e. 对要求充分验证的所有硬件实施进行了规定吗？

f. 安全评估中所有禁止的动作特性都被覆盖了吗？

g. 工作环境被适当地规定了吗？

h. 考虑了假定和约束吗？

i. 该实施能够避免现有类似硬件中的任何已知问题吗？

注 2：下列问题有助于评估要求的正确性：

a. 要求符合上一层级的要求吗？

b. 要求符合分配给该硬件项目的系统要求吗？

c. 要求的陈述有矛盾之处吗？

d. 要求明确吗？

e. 要求可实现吗？

f. 要求可验证吗？

g. 功能模式已经定义了吗？

h. 要求与安全评估一致吗？

i. 鉴定和约束被正确地识别为导出要求了吗？

6.3.3.2 设计评审

设计评审是确定设计数据和实施满足要求的一种方法。设计评审应按计划中所定义在硬件设计生命周期内多次进行。其例子包括概念设计、详细设计和实施评审。对于跨越多个硬件项目级别的多层次设计，如 ASIC 和电路板组件而言，当要最大程度地保证正确设计时，应考虑进行设计评审。

对设计评审的指南包括：

1. 所有的要求都应被涉及，导出要求和设计数据应被正确地定义。
2. 环境要求应被涉及。
3. 安全性和可靠性要求应被涉及。

4. 应明确识别设计数据中的安全性内容。

5. 设计应能被实施、测试和维护。

6. 对新的制造技术应进行评价。

7. 应满足在计划中识别的部件选择准则。

8. 设计应能向要求溯源。

9. 疏忽和错误应反馈个适当的过程以便处理。

7.0 构型管理过程

构型管理过程拟用于提供完全一致地复制构型项目、必要时重新生成信息和在需要改动时对一个受控型式中的构型项目进行修改的能力。本节描述了硬件构型管理的目标和支持这些目标的活动。

7.1 构型管理目标

构型管理过程的目标是：

1. 构型项目被唯一地识别和记录。

2. 确保构型项目的一致和准确复制。

3. 提供识别和跟踪对构型项目的更改的一种受控的方法。

7.2 构型管理活动

对构型管理活动的指南包括：

1. 构型项目应被唯一地识别、记录和控制。这可能包括但不局限于硬件、硬件的设计表述、用于鉴定信誉度和基线的工具或其它数据项目。

2. 应建立基线。

3. 问题应被唯一地识别、跟踪和报告。

4. 应保持对更改的控制和更改的溯源性。这要求在计划中识别的生命周期

数据应是可靠的和可调用的。

5. 构型项目的归档、调用和发布应加以控制。

有多种方法可用于满足构型管理目标和活动，而下列段落提供了对可作为一个可接受的方法使用的活动的指南。

7.2.1 构型识别

构型识别活动的目的是明确地标记每个构型项目，这样就建立了对构型项目进行控制和引用的基础。

其指南包括：

1. 应对数据项目建立构型识别。
2. 应对每个构型项目、构型项目的每个独立控制的部件和构型项目的组合建立构型识别，这种组合可组装成一个与由鉴定机构同意的计划一致的产品。

   注：对部件，如 ASIC、成形的 PLD、印刷电路板和黑盒进行识别的详细程度是由构型管理计划来确定的。
3. 在它们用于基线中之前，应对 COTS 部件和先前开发的硬件项目建立构型识别。
4. 在构型项目用于新的基线、被其它数据项引用或用于产品制造之前，应对每个构型项目建立构型识别。

7.2.2 基线建立

基线建立的目的是为将来的活动定义一个基础，并允许在构型项目之间进行引用和溯源性控制。

指南包括：

1. 应对用于鉴定信誉度的构型项目建立基线。

注：可以建立中间基线以助于控制硬件活动。

2. 一旦基线被建立，它就应到受更改控制程序约束。
3. 在从一个已建立的基线中开发一个导出基线时，应遵循更改控制指南。
4. 如果在开发一个新基线中，要寻求与前一基线的设计相关的活动或数据的鉴定信誉度，则该新基线应能从其导出处溯源至前一基线。

   注：基线可以是一个构型项目，一个以前鉴定过的硬件项目或一个 COTS 部件。

7.2.3 问题报告、跟踪和纠正措施

问题报告、跟踪和纠正措施的目的是记录问题并保证纠正处置和解决。问题可能包括与计划和标准的不符合，生命周期过程输出的欠缺，产品的异常动作，以及工具和技术过程的缺陷。问题的报告应不迟于可获得鉴定信誉度的基线的建立。

指南包括：

1. 问题报告应覆盖每一个报告的问题。
2. 问题报告应识别受影响的构型项目的构型。
3. 要求采取纠正措施的问题报告应启动更改控制活动。
4. 所有关闭的问题报告应包括一个所采取的用于管理问题报告的措施的说明，包括实施纠正措施所需要的数据项更改的完成。
5. 并非所有问题报告都必须关闭才能获得鉴定，然而，应对所有问题报告进行评价，而且确定具有安全性或鉴定影响的报告应予以关闭。
6. 问题报告系统应跟踪问题报告的状态，包括它们的批准和处置。

7.2.4 更改控制

更改控制活动的目的是确保更改的记录、评价、解决和批准。更改控制应

按照构型管理计划进行实施，并在不迟于可获得鉴定信誉度的基线的建立之前实施。

指南包括：

1. 更改控制应通过提供对未授权更改的防止来保留构型项目的完整性。
2. 更改控制应确保更改经过评估并确定构型的等同性是否需要更新。
3. 在更改控制下对构型项目的更改应予以记录、批准和跟踪。批准机构在构型管理计划中进行了定义。

   注 1：问题报告与更改控制有关，因为对所报告的问题的解决可能会导致对构型项目的更改。

   注 2：一般认为更改控制的早期实施有助于过程活动的控制和管理。
4. 更改控制应确保更改的溯源性，并掌握做出更改的理由。
5. 更改控制应确保更改的影响经过评估，以确定更改对过程输出的影响，并确保输出数据已被更新。

   注 1：过程的一些或所有活动可能需要从其输出收到影响的点开始重复进行。
6. 更改控制应确保为受到影响的过程提供反馈。

   注 2：应当了解对制造工具、技术过程或外部部件的更改可能会影响到设计。

7.2.5 发布、归档和调用

发布活动的目的是将数据项置于构型管理控制之下，以确保在其它活动中只有经过授权的数据才被使用。归档的目的是确保与产品有关的数据项在需要时可调出进行复制、重新生成、重新测试或修改产品。

指南包括：

1. 构型项目应在用于制造之前进行识别和发布，而且应建立对其发布的授权。
2. 与产品相关的数据项应能从一个已经批准的来源，如开发机构或公司调出。

   注：更改控制数据和问题报告是数据项的一部分。
3. 应有数据保留程序来满足适航性要求和允许更改。
4. 应建立程序来确保存储的数据的完整性，直至鉴定机构所要求的时间。
   a. 确保没有进行未经授权的更改。
   b. 选择存储介质。
   c. 维持存储数据的可获得性。例如，以与介质的存储寿命兼容的频率对存档数据进行刷新。
   d. 确保不会发生可导致存档数据出现不可恢复的损失的事件。例如，以物理隔离的归档方式存储两份拷贝。

7.3 数据控制类别

与数据项目的构型管理相关的两个类别被定义为：硬件控制类别 1（HC1）和硬件控制类别 2（HC2）。规定两种类别可使对某些数据项的构型控制严格程度有所减低。HC1 要求完成所有的构型管理活动，而 HC2 限制就少一些。划为 HC2 的数据项预期不会进行增量更改，但将由新数据代替。

表 7-1 定义了要在 HC1 和 HC2 控制下进行的构型管理活动。例如，表 7-1 显示出在附录 A 表 A-1 中识别为 HC2 的数据项需要调出，但不需要发布。另外，表 7-1 还示出了任何 HC1 数据都会有一个基线。

附录 A 对作为硬件设计保证级别的某个功能的每个数据项的控制类别进行了识别。例如，在表 A-1 中，HC1 适用于针对所有保证级别的硬件要求，而 HC2

适用于针对所有保证级别的硬件评审和分析结果。

表 7-1 与 HC1 和 HC2 相关联的构型管理过程活动

参考	构型管理活动	HC1	HC2
7.2.1	构型识别	X	X
7.2.2(1),(2),(3)	基线	X	
7.2.2(4) ①	基线溯源性	X	X
7.2.3	问题报告	X	
7.2.4(1),(2)	更改控制－完整性和识别	X	X
7.2.4(3),(4),(5),(6)	更改控制－记录、批准和溯源性	X	
7.2.5(1)	发布	X	
7.2.5(2)	调出	X	X
7.2.5(3)	数据保留	X	X
7.2.5(4a)	防止未授权更改	X	X
7.2.5(4b),(4c),(4d)	介质选择，刷新，复制	X	

① 与新基线一起使用的 HC2 数据的识别并不意味着数据重新划为 HC1。

8.0 过程保证

过程保证确保了生命周期过程目标得到满足，活动按计划中所述完成，或其偏离已被列出。本节描述了过程保证的目标和支持这些目标的活动。并未打算强加特定的组织结构。

为了客观地评估生命周期过程，识别偏离和确保纠正措施得到执行，过程保证活动应独立的完成。

8.1 过程保证目标

过程保证的目标是确保：

1. 生命周期过程符合批准的计划。
2. 所产生的硬件设计生命周期数据符合批准的计划。
3. 用于符合性评估的硬件项目被正确地建立，符合相关的生命周期数据。

8.2 过程保证活动

对过程保证活动的指南包括：

1. 应确保在本文档计划过程章节所述的、符合 PHAC 的硬件计划的可获得性。
2. 应确保评审的组织符合批准的计划，所产生的行动项目的跟踪得以关闭。
3. 应确保对硬件计划和标准的偏离进行检测、记录、评价、批准、跟踪和处理。
4. 应确保符合批准的计划的硬件生命周期过程的转移准则得到满足。

   注：审计是完成上面的第 1 项至第 4 项所述活动的一个有效方法。
5. 应进行一次检查来确保硬件项目的建造符合其设计数据。

   注：这种活动的一个例子是首件检验。
6. 应产生过程保证活动的记录，包括设计活动完成的评估的证据。
7. 适用时，使用者应确保转包商使用的过程符合硬件计划。

9.0 鉴定联络过程

鉴定联络过程的目的是在贯穿整个硬件设计生命周期的过程中，在申请者和鉴定机构之间建立通讯和理解，以有助于鉴定过程。鉴定联络过程应按第 4 节，硬件计划过程和第 10.1.1 节，PHAC 中所述来进行。附录 A 的表 A-1 给出了这一过程的输出的总结。另外，联络活动可能包括为及时批准而进行的设计

方法演示、关于与鉴定基础的符合性的手段的协商、设计方法的批准、数据批准的手段、以及任何要求的鉴定机构评审和测试的见证。

在项目结束时，所遵循的设计过程的总结，所产生的输出和硬件项目的状态都应在第 10.9 节的硬件完成总结中进行描述。

9.1 符合性和策划的手段

申请者提出针对硬件符合性的手段。OHAC 定义了提出的符合性手段。指南包括：

1. PHAC、硬件验证计划和其它要求的数据应在设计更改对项目的影响最小时及时提交给鉴定机构进行评审。
2. 鉴定机构识别的与鉴定的硬件部分的计划有关的问题应得到解决。
3. 应获得鉴定机构对 PHAC 的同意。
4. 在计划中所述的设计和鉴定周期与鉴定机构的联络应予继续，由鉴定机构提出的问题应以及时的方式进行解决。

在某些项目中，鉴定联络不是由设备制造商提供的，而是由机架或其它客户提供的，设备制造商仅为一个支持性角色。这种关系应在 PHAC 中进行定义，并且与鉴定机构的联系应通过鉴定申请者来进行。鉴定申请者有责任确保数据被提供给鉴定机构。

当从一个转包商处采购一些嵌入在设备中的硬件项目时，鉴定计划应识别哪些数据预期来自转包商，而哪些数据由申请者生成。

申请者将 PHAC 和验证计划及其它相关的计划包含于顶级鉴定计划中是可以接受的。

9.2 符合性的证实

申请者提供硬件设计生命周期过程满足硬件计划的证据。鉴定机构评审可

能在申请者所在地或申请者的供应商所在地进行。申请者应安排这些评审并使硬件生命周期数据可在需要时获得。

申请者应：

1. 解决作为其评审的结果由鉴定机构提出的问题。
2. 向鉴定机构提交第 10.9 节所述硬件完成总结和第 10.3.2.2.1 节所述的顶级图纸。
3. 对于鉴定机构要求的其它数据或符合性证据，申请者应进行提交或使其可获得。

10.0 硬件设计生命周期数据

本节描述了将在硬件设计生命周期中产生的、用于提供设计保证和与鉴定要求的符合性的证据的硬件生命周期数据项目。鉴定机构需要用作设计保证证据的生命周期数据的范围、数量和详细程度将随一些因素而变化。这些因素包括适用的鉴定机构对机载系统的要求、被分配的设计保证级别、硬件的复杂性和服务经验。设计保证证据的细节应在 PHAC 中予以识别和记录，并征得鉴定机构的同意。

第 11 节中的其它考虑和附录 B 中对于 A 级和 B 级功能的设计保证考虑会导致产生额外的生命周期数据。

附录 A 从硬件设计保证级别方面指出了要选择的硬件设计生命周期数据、验证独立性的程度和第 7 节中定义的适用的数据控制种类。

1. 硬件设计生命周期数据特性应是：

   a. **明确。**信息/数据按照只允许一种解释的方式填写。

   b. 完整。信息/数据包括必要的和相关的要求及说明性材料、有标记的

图，以及定义的术语和计量单位。

c. **可验证。**信息/数据可以通过某人和某个工具来检查其正确性。

d. **一致。**信息/数据没有冲突之处。

e. **可更改。**信息/数据是结构化的，可以在保持其结构的前提下完整地、一致地和正确地进行更改。

f. **可溯源。**可以确定信息/数据的来源。

本节的描述并非暗指一种特定的数据打包方法和硬件生命周期数据在此包内的形式和组织。例如，所有的计划、标准和程序都可以在一个文档或多个文档中进行描述。

2. 数据打包方法、形式和组织应在 PHAC 中提出并在项目的早期获得鉴定机构的同意。
3. 协调一致的信息和数据应在机载系统或设备的整个服务生命周期内可调用和可获得。

10.1 硬件计划

硬件计划描述了用于硬件鉴定、设计、批准、验证、过程评估和构型控制的过程、程序、方法和标准。

10.1.1 硬件鉴定计划（PHAC）

PHAC 定义了要用于达到本文档的目标和获取鉴定机构对包含硬件项目的系统的鉴定批准的过程、程序、方法和标准。PHAC 一旦获得批准，就表示在鉴定申请者和鉴定机构之间，就要进行的过程和活动及要产生结果证据以满足硬件鉴定要求等达成了一致。PHAC 可以是其它计划，例如机载系统鉴定计划的一部分。

PHAC 应包括：

1. **系统概述**。本节提供了该硬件项目要用于其中的机载系统的一个概述，包括系统功能说明，系统失效条件，系统结构，分配给硬件项目和软件的功能描述，以及对现有系统文档的引用。
2. **硬件概述**。本节描述了硬件功能、硬件项目、结构、要使用的新技术以及任何失效保护、容错、冗余和要使用的分区技术等。
3. **鉴定考虑**。本节描述了鉴定的基础、建议的符合性措施和硬件项目每个功能的硬件设计保证级别。它也提供了对基于硬件的安全性评估及其在机载系统内的用途进行的硬件设计保证级别分配的说明，包括如第 2.3.4 节中所述的潜在硬件失效条件的说明。适用时，也应包括 FFPA 的概述或完成一个 FFPA 并应用其结果的计划。
4. **硬件设计生命周期**。本节描述了要使用的程序、方法和标准及要完成以满足硬件设计保证目标的过程和活动。它描述了活动，活动的组合和排序，过程和活动之间的关系，转移条件，职责，工具的使用，以及提供反馈的手段，硬件过程之间及硬件过程和系统与软件过程之间的相互作用。本节或许会引用使用的计划、政策、标准、程序及与这些计划和用于该项目的标准的偏离。
5. **硬件设计生命周期数据**。本节描述或参考了要开发和提交的数据，或可作为与本文档的目标和计划的符合性的证据而获得的数据。
6. **其它考虑**。本节描述了其它的考虑。这些考虑包括第 11 节所述的先前开发的硬件的使用，包括对要再利用的适用数据的引用，COTS 使用，产品服务经验和工具评估与批准，或附录 B 中所述的对 A 级或 B 级功能的设计保证考虑。
7. **可选的方法**。本节描述了任何可选择用于该项目的方法，这些方法或者

未在本文档中描述，或者将以不同于本文档中所描述的方式应用。关于为何该可选方法是可接受的理由也应提供。

8. **鉴定日程**。本节识别了主要的项目里程碑和将硬件设计生命周期数据提交给鉴定机构的日期。

10.1.2 硬件设计计划

硬件设计计划描述了该硬件项目设计要使用的程序、方法和标准及要进行的过程和活动。该计划可包含于 PHAC 中，并可引用设计方针和要应用的标准。

硬件设计计划应包括：

1. **硬件设计生命周期。**对设计方针和要应用的标准的引用，以及要用于达到该硬件设计保证级别的设计目标而完成的硬件设计生命周期过程和活动的说明。
2. **硬件产品说明。**对要达到的硬件规范、可选的用途、计划的服务寿命和升级考虑的识别。
3. **硬件设计方法。**对用于该硬件项目的需求分析和规范方法、概念设计方法、详细设计方法、综合技术、实施方法和生产转移方法的说明。当对附录 B 第 3.1 节中所述的对 A 级或 B 级功能的结构化缓解已经有所考虑但在编写本计划时尚未落实时，应说明其决定将如何被引入设计过程。
4. **硬件设计环境。**对要使用的设计工具的说明。
5. **硬件项目数据。**对要产生的硬件项目设计数据的说明，或对先前开发的硬件项目的规范、文件、图号和部件号的引用。
6. **其它考虑。**对计划的过程技术选项、使用和组装选项、产品包装和硬件安装选项的描述。

10.1.3 硬件批准计划

批准计划描述了要应用的程序、方法和标准及为硬件项目导出要求的批准达到本文档的批准目标而进行的过程和活动。本计划可包含于 PHAC 中，并可引用要应用的批准标准。

批准计划应包括：

1. **批准方法**。对要使用的批准程序、标准和方法的说明和引用。方法可包括分析、评审和测试。
2. **批准数据**。将作为硬件批准过程的结果而产生的证据的识别和说明。
3. **批准环境**。对要用于实施批准过程和活动的分析和测试设备及批准工具的识别和说明。

10.1.4 硬件验证计划

验证计划描述了要应用的程序、方法和标准及为硬件项目的验证达到本文档的验证目标而进行的过程和活动。本计划可包含于 PHAC 中，并可引用要应用的验证方针和标准。

验证计划应包括：

1. **验证方法。**对要使用的验证方针、程序、标准和方法的说明，它们将被用于提供硬件项目，包括 CITS 和未使用的功能的完整性的客观证据。方法可以包括分析、评审和测试。当使用了附录 B 第 3.3 节中所述的先进分析方法时，还包括对适用的 FFP 的方法和适用的验证完成准则的详细说明。
2. **验证数据。**要作为硬件验证过程的结果而产生的证据的识别和说明。
3. **验证的独立性。**用于保证对有独立性要求的目标的验证独立性的措施的说明。

4. **验证环境。**对要用于实施验证过程和活动的分析和测试设备及验证工具的识别和说明。
5. **机构职责。**对负责实施验证过程的机构的识别。

10.1.5 硬件构型管理计划

硬件构型管理计划描述了要用于满足本文档的构型管理目标的方针、程序、标准和方法。

硬件构型管理计划应包括：

1. **硬件构型管理方法。**对用于识别、管理和控制硬件及其生命周期数据的方针、程序、标准和方法的描述与引用。
2. **硬件基线。**对用于建立设计和产品基线和提供基线溯源性的方法和程序的描述。
3. **问题报告和处理。**对用于记录、跟踪和处理问题报告的方法和程序的描述。
4. **更改控制。**对用于识别、控制和跟踪对受控数据项目的更改的方法、程序和过程的描述。
5. **存储和调出。**对硬件设计生命周期数据的发放、归档和调出的程序的描述。该描述应包括归档的内容、格式和介质标准、规则、方法和条件。
6. **环境控制。**对用于识别和控制用于开发和验证该硬件的工具的程序和方法的描述。
7. **构型管理工具。**对用于构型管理过程和活动的工具和资源的描述。

10.1.6 硬件过程保证计划

硬件过程保证计划描述了要应用的程序、方法和标准，以及要为达到本文档的过程保证目标而进行的过程和活动。

硬件过程保证计划应包括：

1. **过程控制。**对用于硬件设计过程的过程保证的实施的方针和程序的描述。
2. **机构职责。**对负责实施过程保证的机构的识别。
3. **符合性。**对用于确定过程和产品符合性的方针、程序和准则的描述。
4. **过程保证活动。**对为显示过程对计划和标准的符合性而进行的过程保证评审和审计的描述。
5. **偏离。**对用于检测、记录、评价、处理和批准对计划和标准的偏离的方法的描述。

10.2 硬件设计标准和指南

硬件设计标准和指南可定义用于硬件设计、批准、验证、保证和控制过程的规则、程序、方法和准则，它们被用于评估硬件设计结果的可接受性和质量。标准可能是不要求的，但是，如果使用者在项目中引用了标准，则它就变成了该项目的鉴定基础和计划的一部分。与计划一样，这些标准和指南可以打包为一个文档或多个文档。工具可用于强制推行标准。

10.2.1 要求标准

在需求分析过程可以用要求标准来定义用于开发该要求的规则、程序、方法、指南和准则。要求标准可以包括用于开发和规定要求的方法和准则、用于批准要求的方法和准则、用于表述要求的标记、对要求规范工具的使用指南和用于为系统设计过程提供导出要求的手段。

10.2.2 硬件设计标准

在概念设计过程和详细设计过程可用硬件设计标准来定义用于开发和规定硬件设计的规则、程序、方法、指南和准则。

硬件设计标准可包括：

1. 硬件设计表述方法和标记。

2. 设计规范和命名惯例。

3. 设计方法指南。

4. 硬件设计工具使用指南。

5. 电子部件选择指南。

6. 关于评估设计选项的指南。

7. 关于评估失效保护和容错设计构建的指南。

8. 对用于向要求过程提供反馈和澄清要求的措施的描述。

10.2.3 批准和验证标准

在批准和验证过程可用硬件批准和验证标准来定义用于批准和验证硬件设计和实施的规则、程序、方法、指南和准则。

10.2.4 硬件归档标准

硬件归档标准可用来定义用于保存和归档产品数据和开发与维护程序和项目档案的程序、方法和准则。硬件归档标准可包含归档的内容、格式和介质标准、规则、方法和准则。

10.3 硬件设计数据

硬件设计数据是定义该硬件项目的规范、文档和图纸。

10.3.1 硬件要求

该要求规定了被开发的硬件项目的功能、性能、安全性、质量、可维护行和可靠性要求。

这些要求应包括：

1. 分配给该硬件的系统设计和安全性要求。

2. 对适用于该硬件的标准的识别。

3. 硬件的功能和性能要求，包括导出要求和对正常使用的应力极限。
4. 硬件的可靠性和质量要求，包括与失效比、暴露次数和设计约束有关的要求。
5. 在整个硬件项目服务生命周期的硬件维护和修理要求。
6. 硬件可制造性和组装要求。
7. 硬件可测试性要求。
8. 硬件存储和处置要求。
9. 安装要求。

10.3.2 硬件设计表述数据

硬件设计表述数据提供了硬件项目的一个定义，它由用于创建该硬件项目的一组图纸、文档和规范组成。下列段落定义了一些典型的硬件设计数据及其内容。对于某个指定硬件设计而言，所生成的数据、图纸和文档的类型将根据尺寸、复杂性和硬件项目所包含的部件数而变化。

10.3.2.1 概念设计数据

概念设计数据是描述硬件项目的结构和功能设计的数据，它可能包括：

1. 一个高级别的描述，如方框图和 HDL 定义，它勾画出了主要功能，并显示出了这些功能之间的信息流。
2. 描述了硬件项目布局的机械结构，例如显示了外包装、印刷电路板布局、连接器的选择和位置及主要连线的图纸或草图。
3. 从适航性的观点来看较为重要的其它结构特性和分区。这可能包括诸如 EMI、照明、震动或振动保护、主要部件中未使用的功能以及人机接口，如人体工程学因素、照明特性和显示分辨率等项目。
4. 顶级硬件项目功能描述。

5. 硬件项目功能结构。

6. 初步的硬件安全性评估数据。

10.3.2.2 详细设计数据

详细设计数据描述了按其要求实施硬件项目所必要的数据。取决于硬件项目的层级，这些数据可能包括顶级图、装配图、相互连接数据、部件数据、HDL硬件描述、可靠性数据、测试方法论数据、所选部件中未用功能的清单和为保证它们不会危及硬件项目的安全性所采取的措施、安装控制数据和硬件/软件接口数据。一些特定的数据将在下面描述。

注：除了其它适用的鉴定要求所要求的详细设计数据之外，诸如技术标准指令、其它详细设计数据项目的内容和可获得性应由使用者在 PHAC 中向鉴定机构进行说明。

10.3.2.2.1 顶级图

顶级图唯一地识别了硬件项目，并识别了所有组件、子组件、部件和定义该部件项目的相关文档。

10.3.2.2.2 组件图

组件图包括了组装该硬件项目、组件或子组件所需要的其它详细信息。

一个组件图可能包括：

1. 硬件项目在硬件组件中的位置和方位。

2. 对确保正确和无故障装配而使用的组装指令序列或方法的识别。

3. 用于识别标志、标签、后续操作中使用的参考版次的位置。

10.3.2.2.3 安装控制图

安装控制图确保了将硬件项目正确地安装到系统中，或将硬件项目正确地安装到其它硬件项目中。对于某些低级的硬件项目，用于下一个更高级别硬件

项目或组件的组件图可作为安装控制图使用。

安装控制图可能包括：

1. 尺寸。

2. 间隙要求。

3. 冷却和安装信息。

4. 关于重量、重心和保证安全和正确安装所需要的其它参数的信息。

10.3.2.2.4　硬件/软件接口数据

由要求规范确定的硬件性能可能取决于硬件与软件的构型、硬件与软件的校准，或取决于硬件和软件之间的相互作用。

与硬件和软件之间的接口有关的数据可能包括：

1. 存储器地址。

2. 数据可以装入的存储器地址字段的分配。

3. 定时和顺序信息。

4. 硬件/软件接口的操作所需要的其它信息。

10.4　批准和验证数据

批准和验证数据是硬件设计结果及硬件项目本身的完整性和正确性的证据。它提供了保证，证明硬件按其要求和设计进行开发、正确地生产、达到了设计目标。数据包括用于硬件评审、分析和测试的程序和结果。对于附录 B 中所述的 A 级和 B 级功能，可能还需要超出本节所述范围的其它数据。

10.4.1　溯源性数据

硬件溯源性建立了在要求、详细设计、实施和验证数据之间的相关性，有利于硬件项目的构型控制、更改和验证。

硬件溯源性数据应包括：

1. 在分配给硬件的系统要求和要求之间的相关性。
2. 在要求和硬件详细设计数据之间的相关性。
3. 在硬件详细设计数据和在建硬件项目或组件之间的相关性。
4. 在要求，包括导出的硬件要求和详细设计数据与验证程序和结果之间的相关性。
5. 溯源性分析的结果。

10.4.2 评审和分析程序

硬件评审和分析程序定义了用于实施评审和分析的过程和准则。

硬件评审和分析程序应包括：

1. 评审和分析的目的。
2. 参与评审的机构。
3. 评审或分析准则。
4. 关于进行评审或分析的详细说明。
5. 评审或分析的可接受性和完成准则。

10.4.3 评审和分析结果

硬件评审和分析结果是评审和分析已经按批准的程序和准则完成的证据。

硬件评审和分析结果应包括：

1. 对评审或分析程序的识别。
2. 对评审或分析的数据项的识别。
3. 参与评审或分析的人员。
4. 评审或分析结果。
5. 作为评审或分析结果而生成的纠正措施，例如一个问题报告或措施项目列表。

6. 评审或分析结论，对于评审而言，包括对评审项目的一个定性的分析，对于分析而言，包括对分析项目的定量分析和分析数据。

10.4.4 测试程序

硬件测试程序定义了执行用于硬件项目验证的功能性和环境符合性测试的方法、环境和说明。

硬件测试程序应包括：

1. 测试的目的。
2. 硬件测试设置的识别，以及每个硬件测试所要求的软件和测试设备设置说明。
3. 执行测试程序的详细说明。
4. 测试输入数据。
5. 预期的结果，例如合格/不合格条件和测试所覆盖的要求。

10.4.5 测试结果

硬件测试结果是一种客观证据，证明作为对硬件项目验证的支持，测试已经按批准的程序完成。

硬件测试结果应包括：

1. 对测试程序的识别。
2. 对测试项目的识别。
3. 进行测试的实际结果。
4. 执行和见证测试的人员的识别。适用时，还包括进行测试的日期。
5. 可通过分析或评审给出的结果的解释，以及实际实现的测试覆盖。

10.5 硬件验收测试准则

该数据提供了准则和评估数据，该测试和相关的测试结果能够保证某项目

被正确地制造或维修。

该准则应包括：

1. 要测试的关键特性。
2. 每个关键特性的合格/不合格条件。
3. 任何测试约束。
4. 关键特性和合格/不合格条件的证实。
5. 满足安全性要求所必须的设计范围覆盖。
6. 显示测试准则已根据实际测试程序和相关的测试结果被适当地实施的评估数据。

10.6 问题报告

问题报告是识别和记录对硬件设计问题、过程与硬件计划和标准的不符合和硬件生命周期数据的不足的处理的手段。

问题报告应包括：

1. 构型项目和从中观察到问题的过程活动的识别。
2. 要修改的构型项目的识别或要修改的过程的说明。
3. 使问题能被理解和处理的问题描述。
4. 解决所报告的问题所采取的纠正措施的说明。

10.7 硬件构型管理记录

构型管理过程活动的结果被记录在构型管理记录中。这些结果可能包括构型识别清单、基线或电子记录、更改历史报告、问题报告总结、工具识别数据、归档记录和发放记录。

10.8 硬件过程保证记录

过程保证过程活动的结果被记录在过程保证记录中。这些结果可能包括评

审或审计报告、会议记录、授权的过程偏离记录或符合性评审记录。

10.9 硬件完成总结

硬件完成总结是显示与 PHAC 的符合性和向鉴定机构表明本文档对该硬件项目的目标已经得到实现的主要数据项。该总结应与系统完成总结组合在一起。如 PHAC 中所列，硬件完成总结应包括下列信息：

1. 系统概述。
2. 硬件概述。
3. 鉴定考虑。
4. 硬件设计生命周期描述。
5. 硬件设计生命周期数据。
6. 先前开发的硬件。
7. 其它考虑。
8. 可选的方法。

对与经过批准的 PHAC 的差异应进行识别。另外，应提及下列四项：

1. **硬件识别**。本节通过部件号和版次识别硬件构型和硬件项目。
2. **更改历史。**适用时，本节包括对硬件更改的一个总结，说明由于影响安全的故障而进行的更改，并识别自上次鉴定以来硬件设计生命周期过程所进行的改动。
3. **硬件状态。**本节包含在鉴定时尚未解决的问题报告的一个总结，包括对功能限制的说明。
4. **符合性说明。**本节包括对与本文档的符合性的说明，以及用于显示与硬件计划中规定的准则的符合性的方法的总结。本节也列出了其它的规则和对硬件计划、程序和本文档的偏离。

注：PHAC 中所包括的数据并不一定需要在硬件完成总结中加以重复，然而这样做可以加速鉴定过程。

11.0 其它考虑

本节提供了关于设计保证的其它考虑的指南，这些考虑并未在先前章节中被覆盖。这些附加的考虑可由使用者自由决定使用，以满足第 2 至第 9 节的一些目标。任何附加考虑的使用都应征得鉴定机构的同意。

11.1 先前开发的硬件的使用

本节讨论了与先前开发的硬件的使用相关的问题。其指南包括对硬件、飞机安装、应用环境或设计环境进行改动和对设计基线进行升级的评估。第 11.2 节中给出了对 COTS 部件使用的指南，即一个特别的先前开发硬件的案例。对于先前开发硬件的每次使用也应涉及构型管理和过程保证考虑。

使用先前开发硬件的打算应在 PHAC 中声明。

11.1.1 对先前开发硬件的改动

本节讨论了对先前开发硬件的改动。改动可从要求改变、错误的检测、硬件或技术增强或采购困难中产生。

对提出的改动的分析活动包括：

1. 对系统安全性评估过程输出的评审。
2. 如果硬件设计保证级别增加，需要应用第 11.1.4 节中的指南。
3. 对于改变的影响，包括可能导致对超出改动部分的区域进行重新验证的改动的后果应进行分析。该区域可以通过信号流分析、功能分析、定时分析、溯源性分析或其它适当手段来确定。

11.1.2 飞机安装的改变

本节讨论了在硬件在飞机上的新安装位置的使用，该硬件先前曾被授予某个硬件设计保证级别和一个特定的鉴定基础。当在新的飞机安装位置上使用先前开发的硬件时，应使用下列指南：

1. 系统安全性评估过程对新的飞机安装位置进行评估，并确定硬件设计保证级别和鉴定基础。如果与先前的安装位置相比，这些情况对于新的安装位置而言是相同的或更不严格的，则不要求进行其它的工作。
2. 如果对于新的安装位置要求有功能性改动，则应满足第 11.1.1 节的指南，“对先前开发硬件的改动”。
3. 如果先前的设计活动并未产生要求证明新安装位置的安全性目标的输出，则应满足第 11.1.4 节的指南，“对设计基线进行升级”。

11.1.3 应用或设计环境的改变

先前开发的硬件的使用可能涉及到一个新的设计环境，或与不同于初始应用时所用的其它软件或硬件的集成。

新的设计环境可能会增加或减少在硬件设计生命周期过程中的某些活动。指南包括：

1. 如果新的设计环境使用了硬件设计工具，则第 11.4 节的指南，“工具的评估和批准”是适用的。
2. 在先前开发的硬件与不同的接口硬件一起使用时，应进行硬件接口的验证。
3. 当先前开发的硬件使用了不同的软件时，应提出对硬件/软件接口进行重新鉴定的需要。

11.1.4 对设计基线进行升级

下列指南适用于其源于前次应用的生命周期数据被认为不足以适应与新应

用相关的安全性目标的硬件项目。本指南拟帮助使用者就以前在较低硬件设计保证级别上开发的硬件获得鉴定机构的同意。

对设计基线进行升级的指南包括：

1. 在利用先前开发的生命周期数据时，本文档的目标应予以满足。
2. 硬件鉴定内容应基于由系统安全性评估过程确定的故障条件和硬件设计保证级别。应对先前应用的改变所造成的影响进行分析，以确定不足的区域。
3. 对源自先前开发的生命周期数据应进行评价，以确保对于计划在要求的硬件设计保证级别实施功能升级的硬件，验证过程目标得到满足。
4. 可以使用逆向工程来重新生成目前不足或丢失的硬件生命周期数据，以满足本文档的设计保证目标。
5. 如果在对设计基线进行升级的过程中，计划使用产品服务经验来满足本文的实际保证目标，则应选择第 11.3 节中的指南，“产品服务经验”。
6. 使用者应在 PHAC 中规定实现与本文档的符合性的策略。

11.1.5 其它的构型管理考虑

除了第 7 节中的指南之外，对先前开发的硬件的新应用的构型管理过程还应包括：

1. 从先前应用的硬件产品和生命周期数据到新应用的溯源性。
2. 可以管理来自同一项目的不同应用的更改请求的更改控制过程。

11.2 商业货柜产品（COTS）部件的使用

COTS 部件在硬件设计中广泛使用，典型情况下，无法得到 COTS 部件的设计数据进行评审。鉴定过程并未特别针对各个部件、模块或子组件，因为这些是作为被鉴定的特定飞机功能的一部分被覆盖的。因而，COTS 部件将通过总体

设计过程，包括本文档中定义的支持过程进行验证。电子部件管理过程与设计过程一起使用，提供了 COTS 部件使用的基础。

11.2.1 对于 COTS 部件的电子部件管理

对于 COTS 部件的电子部件管理是一个与硬件的设计和开发相关的重要的支持过程。电子部件管理过程适用于 COTS 电子部件。尽管该过程同时具有商务和技术内容，但本节只处理技术内容，因为它影响到鉴定。

鉴定可通过建立下述原则来获得：

1. 部件制造商应出示高质量部件的生产的跟踪记录。
2. 部件制造商建立了质量控制程序。
3. 由服务经验支持该部件的成功使用。
4. 部件已经由制造商证实合格或通过建立了部件可靠性的其它测试手段证实合格。
5. 部件制造商具有部件质量水平的控制权或通过其它部件测试手段予以保证。
6. 部件已在预期应用的技术适宜性的基础上进行了选择，例如部件温度范围、额定功率或电压，或已经用其它测试或其它手段建立了这些选择。
7. 对部件的性能和可靠性进行了连续监测，关于需要改进的意见被反馈给部件制造商。

11.2.2 COTS 部件采购

COTS 部件采购保证并非本文档预期讨论的内容，但在对硬件设计保证有明显影响时，对采购事项的反馈应加以管理并由使用者予以解决。

主要关系的内容包括：

1. 本文档所要求的 COTS 部件设计保证数据的实际可获得性。

2. 取决于生产批次的部件参数的变化未被识别，甚至未被鲁棒测试（译注：即坚固性测试）所识别。

3. 电子部件技术发展的内容。

4. COTS 部件已变得无法采购。

11.3 产品服务经验

服务经验可以用于证实先前开发硬件和 COTS 部件的设计保证。服务经验与从部件的任何先前或当前应用中采集的数据有关。源自非机载应用的数据并不被排除。

注：某个服务中的项目的广泛和成功应用可提供信心，表明该项目的设计是成熟的，没有错误，而且该项目的制造质量是可以证明的。

11.3.1 产品服务经验数据可接受性条件

当服务经验数据用于设计保证时，服务经验数据的相关性和可接受性就取决于下列各项之一项或多项：

1. 硬件项目的使用在应用、功能、工作环境和设计保证级别方面的相似性。

2. 设计保证数据基于所提出的硬件项目配置的程度。

3. 在服务期间被评估的设计错误被消除、缓解或分析并确定对所用配置没有安全性影响的程度。

4. 工作中的实际失效比。

注：在某个应用的部件的设计保证依赖于服务经验数据时，PHAC 应特别列出这些内容。

11.3.2 产品服务经验数据的评估

为满足上述条件，使用者应：

1. 根据工程分析对先前应用。安装和环境与目标应用的相关性进行评估。

注：用于确定使用的适宜性和使用的局限性的数据可从规范、数据册、应用说明、服务通告、用户通讯和勘误表中获得。这些信息来源也可能描述了与该硬件项目有关的功能，所以预期机载用途可与先前的使用相互关联。

2. 评估预期应用对安全性评估过程的影响，包括由该数据识别的设计错误的效果可能的缓解。
3. 对关于设计错误及其对安全性评估过程的影响的任何统计数据进行评估。如果无法获得统计结果，可以使用定性评估。
4. 对可获得的问题报告进行评估。问题报告会显示出服务经验已经导致产生了当前配置中可获得的改进。已经识别但未修复的问题或仍需要通过结构化手段或通过完成附加的验证来缓解。应建立问题报告和硬件项目或产品要求变化之间的关系。

注：对于电子部件而言，实际的服务应用可以增大错误被检测和消除的几率。

11.3.3 产品服务经验评估数据

用于证实针对所建议的应用的设计保证的服务经验评估数据应包括：

1. 部件及其在机载系统中的预期功能的识别。识别设计保证级别，或对于用于 A 级和 B 级功能的部件而言，针对该部件的其它保证手段的说明，例如要应用的结构化手段和附加的或先进的验证策略。
2. 对服务经验数据收集和评估过程的说明，包括确定数据的充分性和有效性的准则。
3. 服务经验数据，包括被考虑的详细的服务信息、更改历史、用于分析服务经验数据的假定和分析结果的概述。

4. 服务经验数据相对于预期用途和要求的设计保证级别的充分性的理由。

11.4 工具评估和批准

工具，包括硬件和软件，通常在硬件设计和验证期间使用。当设计工具被用于生成硬件项目或硬件设计时，工具中的错误会将一个错误引入硬件项目中。当用验证工具来验证硬件项目时，工具中的错误会导致该工具不能检测出硬件项目或硬件设计中的错误。在使用工具之前，应进行一次工具评估。该评估的结果，必要时工具的批准应被加以记录和维护。

工具评估和批准的目的是要确保该工具能在其使用的可接受的置信水平上完成特定的设计或验证活动。

11.4.1 工具评估和批准过程

工具评估对工具在设计生命周期过程中的角色进行了评估，可能包括了要取决于工具的角色和硬件功能的设计保证级别来完成的批准活动。该评估指南作为一个流程图的形式呈现，适用于使用时要满足目标或用于生成满足这些目标的数据项目的设计工具和验证工具。该流程图将带领使用者对某些种类的工具做出有限制的评价和对其它工具进行批准。

工具评估和批准过程适用于单个工具或一组工具。工具通常具有超出针对特定项目的特定设计或验证活动所需的能力。只需要对用于特定硬件生命周期活动的工具功能进行评估，而勿需评估整个工具。

应该认识到工具通常是集成的并在不同的生命周期阶段被共享。如果同一工具既用于设计阶段又用于验证阶段，则该工具或许需要作为设计工具进行评估，除非可以在这两种功能之间建立起隔离和保护。

注 1：如果某指定工具的评估表明它的一些功能被用于设计而另一些功能被用于验证，就值得分别列出其功能并对每组工具功能进行评估。

注 2：该评估活动较多或更多地关注于工具的应用。

图 11-1 的流程图指明了工具评估的考虑和活动，并为需要进行工具批准的情况提供了指南。决策框和活动框中的号码对应于图后的编号项（译注：译文中将其移至本段后），这些编号项提供了关于决策和活动的进一步说明。

1. **识别工具**。包括名称，来源、版次号及其基于的主机环境。工具的更新应予以记录和跟踪。

   注：在对工具进行更新时，应就工具更新对现有结果和对硬件的剩余生命周期的潜在影响进行评估。

2. **识别工具支持的过程**。识别工具所支持的设计或验证过程，工具的任何相关的限制和产生的用于硬件设计生命周期的输出。如果已知工具存在某些问题，应提供对该工具使用的可接受性的说明，并陈述理由。

3. **工具数据被独立评估吗**？一个独立的评估可通过独立的手段验证工具输出的正确性。如果工具输出被独立地进行了评估，则没有必要再作进一步的评估。

   注：由工具整体或部分生成的设计工具输出的独立评估可通过在该项目，例如部件、网表（Netlist）或组件上完成的验证活动来建立。在此情况下，终结项目的完整性并不只是取决于设计工具输出的正确性。

   验证工具输出的独立评估或许包括工具输出的一次人工评审或包括与能完成与被评估的工具所能完成的相同验证活动的另一工具进行的比较。

   使用者也可以提出进行独立评估的其它方法。

4. **工具是 A 级、B 级或 C 级设计工具或是 A 级或 B 级验证工具**？如果工

具用于 D 级功能，作为针对 C 级功能的验证工具，或用于评估验证测试的完成情况，例如用于附录 B 第 3.3.1.1.2 节中描述的元件分析中，则没有必要作进一步评估。如果工具用作实现 A 级、B 级或 C 级功能的硬件的设计工具，或用作实现 A 级或 B 级功能的硬件的验证工具，则需要作进一步的评估。

5. **工具有相关历史吗？**当可以显示出工具以前被使用过并且已发现产生了可以接受的结果时，就不需要再作进一步评估。在其理由中应包括对先前的工具使用与建议的工具使用之间的关系的讨论。

   注：只要可获得数据来证实工具历史的关系和可信性，工具的历史便可基于机载或非机载应用。

6. **为工具批准建立基线和问题报告。**为工具构型管理建立基线和工具报告以便为工具批准做好准备。
7. **基本的工具批准。**建立和执行一个计划，用分析和测试来确认工具产生了对其预期应用的正确的输出。工具的用户指南或工具功能的其它说明及其使用可用于生成要求。
8. **工具的类型和级别。**被考虑的工具是一个 A 级或 B 级硬件设计工具还是一个 C 级硬件设计工具，或是一个 A 级或 B 级硬件验证工具？
9. **设计工具批准。**用本文附录 B 中所述的策略，RTCA DO-178B / EUROCAE ED-12B 中对软件开发工具的工具批准指南或其它可为鉴定机构所接受的手段来对 A 级或 B 级设计工具进行批准。该活动与工具开发之间的独立性也应建立起来。

   注：因为工具使用的环境、所牵涉的技术、工具的实施和生命周期数据的可视性和其它因素的变动性，在此并未提供用于 A 级或 B 级设计

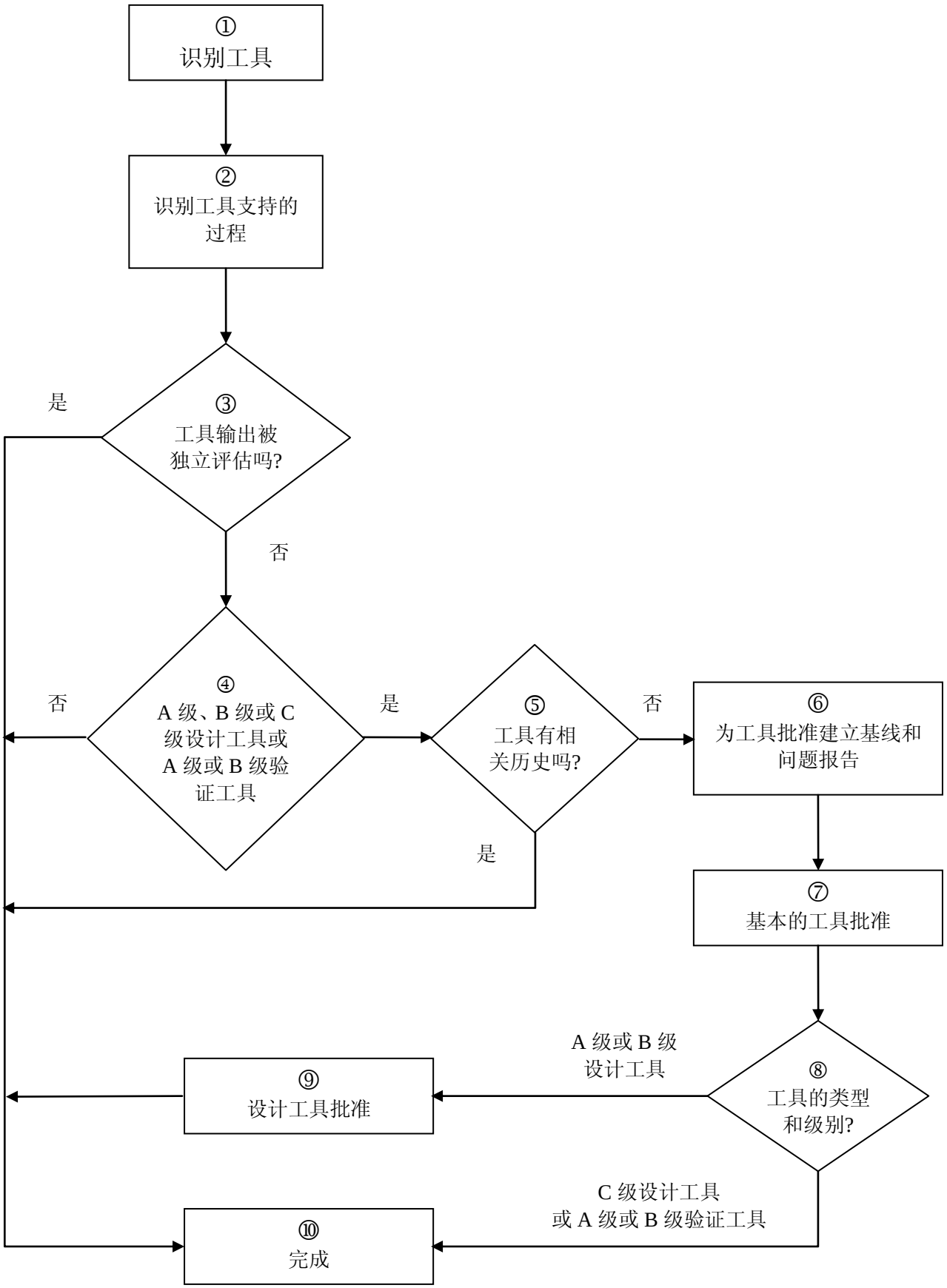

图 11-1　设计和验证工具评估与批准

工具批准的特定指南。不提倡使用未对工具输出进行独立评估或未建立相关历史的设计工具，因为对于拟使用的工具而言，这样做可能是具有与硬件开发相同挑战性的事情。

10.**完成。**记录工具评估、做出评估决定的理由，必要时记录工具批准数据。根据需要提供对安装指南、用户手册和工具批准数据的特定引用以支持工具分配和批准。

11.4.2 工具评估和批准数据

工具评估和批准数据应包括：

1. 识别工具、工具支持的过程，必要时识别下列项目：
   a. 按图 11-1 第 3 项进行的独立评估的理论基础和结果。
   b. 按图 11-1 第 4 项进行的工具指定。
   c. 用于满足图 11-1 第 5 项的工具的历史。在其理由中应包括对先前工具用途与建议的工具用途之间关系的讨论。
2. 要用于工具批准的明确的配置定义，符合图 11-1 中的第 6 项，如果与实际用于设计或验证最终硬件项目的工具配置不同，还应有经过测试的配置的适用性的说明。
3. 工具批准的详情，包括测试中使用的要求、测试程序、预期的结果、用于解释和补充测试结果的分析程序，以及如何建立独立性。
4. 批准设计工具的计划，包括适用的程序，以及计划中所识别的任何活动的结果。
5. 已知工具勘误表的处置，包括变通（Workarounds），适用时，将生成作为工具批准结果的问题报告。

附录 A 基于硬件设计保证级别的硬件生命周期数据的调整

本附录提供了关于基于硬件设计保证级别的硬件生命周期数据调整的指南。并提供了关于验证过程的独立性要求的指南。

附录 A-1 识别了对于每种数据元素的数据交付分级和构型管理数据控制种类。参见表 7.1。共定义了两种数据交付分级类型：

1. 提交。该数据项应被提交给鉴定机构。

2. 不可获得。对该数据项不作要求。

所有 A 级和 B 级功能的验证都应是独立的，C 级和更低级别的功能不要求进行独立的验证。只有在将设计与要求进行验证的设计层级才有独立性要求。独立性的一个等同措施，即识别共模故障的内容，应是可以接受的。

独立性是识别潜在的共模错误的手段，可在设计者验证处于开发状态的项目是按设计工作，而不是按要求工作时出现。为了识别这一问题，确保验证过程与显示设计要求已经得到满足相互一致的职责应由独立于设计者的一个人、一个过程或一个工具来完成。有许多建立独立性的措施，验证计划应识别用于特定验证活动的特定措施。

一些可接收的措施包括：

1. 要求或设计由另一人进行评审。

2. 测试实例或程序由另一人进行开发。

3. 测试实例或程序由设计者开发并由另一人进行评审。

4. 由设计者进行的分析由另一人或一个评审小组来进行评审。

5. 进行一次由设计者确认试验结果的不同的试验，例如在飞行试验期间独立开发并在目标硬件项目上进行的试验可确认硬件项目试验或软件

验证试验，由设计者来确认试验结果。

6. 用一个工具来验证试验或分析结果。

注1. 通常验证试验是自动化的，只要求用一个命令来执行。独立性的含义并不在于要求设计者以外的某人来执行已经独立地评价或开发过的测试。其结果仍需要进行独立评审来确认遵循了适当的程序，而且其结果验证了要求已得到满足。

注2. 要实现独立性并不需要组织机构的独立。

表 A-1 中加圈的号码对应于在该表之后（译注：译文将其移至此段后）的注释。

① 必须提交的数据是由“提交”栏中的 S 符号来表示的。用于检定的 HC1 和 HC2 数据勿需提交但应可获取。参见第 7.3 节。

② 此处所列的目标仅供参考。并非所有目标都适用于所有保证级别。

③ 如果该数据用于检定，则在表中示出了其可获得性。该数据并非总是用于检定，也可能不要求提供。

④ 这可以通过对 C 级和 D 级鉴定联络过程来非正式地完成。文档可以是会议记录和/或演示材料的形式。

⑤ 如果使用者在提交的数据项目中参考了这一数据项，则它应是可获得的。

⑥ 只需要有从要求到试验的溯源性数据。

⑦ 不需要测试范围覆盖导出的或更低层级的要求。

表 A-1 **按硬件设计保证级别和硬件控制种类排序的硬件生命周期数据**

数据章节	硬件生命周期数据 ①	目标 ②	提交	A 级	B 级	C 级	D 级
10.1	硬件计划						
10.1.1	硬件鉴定计划	4.1(1,2,3,4)	S	HC1	HC1	HC1	HC1
10.1.2	硬件设计计划	4.1(1,2,3,4)		HC2	HC2	HC2	NA
10.1.3	硬件批准计划 ③④	4.1(1,2,3,4);6.1.1(1)		HC2	HC2	HC2	NA
10.1.4	硬件验证计划	4.1(1,2,3,4);6.2.1(1)	S	HC2	HC2	HC2	HC2
10.1.5	硬件构型管理计划	4.1(1,2,3,4);7.1(3)		HC1	HC1	HC2	HC2
10.1.6	硬件过程保证计划	4.1(1,2,4);8.1(1,2,3)		HC2	HC2	NA	NA
10.2	硬件设计标准						
10.2.1	要求标准 ③	4.1(2)		HC2	HC2	NA	NA
10.2.2	硬件设计标准 ③	4.1(2)		HC2	HC2	NA	NA
10.2.3	批准和验证标准 ③	4.1(2)		HC2	HC2	NA	NA
10.2.4	硬件归档标准 ③	4.1(2);5.5.1(1); 7.1(1,2)		HC2	HC2	NA	NA
10.3	硬件设计数据 ③						
10.3.1	硬件要求	5.1.1(1,2);5.2.1(2); 5.3.1(2);5.4.1(3); 5.5.1(1,2,3); 6.1.1(1,2);6.2.1(1)		HC1	HC1	HC1	HC1
10.3.2	硬件设计表述数据						
10.3.2.1	概念设计数据 ③	5.2.1(1)		HC2	HC2	NA	NA
10.3.2.2	详细设计数据	5.3.1(1);5.4.1(2)		⑤	⑤	⑤	⑤
10.3.2.2.1	顶级图纸	5.3.1(1);5.4.1(2); 5.5.1(1)	S	HC1	HC1	HC1	HC1
10.3.2.2.2	装配图纸	5.3.1(1);5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.3	安装控制图纸	5.4.1(2);5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.4	硬件/软件接口数据 ③	5.3.1(1);5.5.1(1)		HC1	HC1	HC1	HC1
10.4	批准和验证数据						
10.4.1	硬件溯源性数据	6.1.1(1);6.2.1(1,2)		HC2	HC2	HC2 ⑥	HC2 ⑥
10.4.2	硬件评审和分析程序 ③	6.1.1(1,2);6.2.1(1)		HC1	HC1	NA	NA
10.4.3	硬件评审和分析结果 ③	6.1.1(1,2);6.2.1(1)		HC2	HC2	HC2	HC2
10.4.4	硬件测试程序 ③	6.1.1(1,2);6.2.1(1)		HC1	HC1	HC2	HC2 ⑦
10.4.5	硬件测试结果 ③	6.1.1(1,2);6.2.1(1)		HC2	HC2	HC2	HC2 ⑦
10.5	硬件验收试验准则	5.5.1(3);6.2.1(3)		HC2	HC2	HC2	HC2
10.6	问题报告	5.1.1(3);5.2.1(3); 5.3.1(3);5.4.1(4); 5.5.1(4);6.1.1(3);		HC2	HC2	HC2	HC2

数据章节	硬件生命周期数据 ①	目标 ②	提交	A 级	B 级	C 级	D 级
		6.2.1(4);7.1(3)					
10.7	硬件构型管理记录	5.5.1(1);7.1(1,2,3)		HC2	HC2	HC2	HC2
10.8	硬件过程保证记录	7.1(2);8.1(1,2,3)		HC2	HC2	HC2	NA
10.9	硬件完成情况总结	8.1(1,2,3)	S	HC1	HC1	HC1	HC1

附录 B　对 A 级和 B 级功能的设计保证考虑

1.0　引言

实现 A 级和 B 级功能的硬件设计者做出的设计决定可能或影响安全性。随着设计保证级别的增加，验证所给出的设计满足其安全要求的手段可能会要求使用设计保证方法的重叠、分层组合。选择这些方法中的一个或多个方法，或建议使用另外一种能提供设计保证的方法，都取决于使用者。

本附录为设计者提供了关于如何完成和使用一个 FFPA 来开发一个设计保证策略的指南，以及关于可用于设计保证的某些特定方法的指南。

2.0　功能型故障路径分析

FFPA 是一种结构化的、自顶向下的、迭代的分析。它识别了实现功能的设计中的特定部分，也就是说，识别了与每个路径相关的组件、部件和原件。对相关的故障模式和效果应进行分析，以确定硬件结构和实施符合安全性要求。FFPA 也可识别实现了 A 级和 B 级功能的设计的组件、部件和原件。

FFPA 始于 PSSA，后者用来识别系统级别的 FFP，这些 FFP 可以被分解到或分配给硬件 FFP。

FFPA 的目标是识别每个 FFP，使：

1. 实现 A 级和 B 级功能的硬件可通过本附录中描述的适当的设计保证方法或可被鉴定机构接受的其它先进方法来识别。
2. 对于实现 C 级或更低级别功能的硬件而言，本附录的考虑是可选的。亦即，这些功能只用本文档第 3 节至第 11 节中的指南来保证。

   注：对于用不同技术实现的或提供不同程度设计可视性的功能的 FFP 进行识别通常是有用的，因为总体的硬件项目设计保证可以通过使用多

种设计保证方法来实现。对于每个 FFP，分解的层级可以是不同的。

分解是用常规的自顶而下的安全评估技术来完成，例如故障树分析等等。这种分解可以用对每个逐级分解的 F-FMEA、依赖性图和共模分析来补充。取决于设计保证策略，对每个系统级 FFP 的分解层级可以不同，对应的执行概念和故障抑制方法将被推荐给被设计的硬件。分解的过程从：

系统级 FFP 到硬件级 FFP；

硬件级 FFP 到电路级 FFP；

电路级 FFP 到部件级 FFP；

部件级 FFP 到元件级 FFP。

2.1 功能型故障路径分析方法

FFPA 应按下列方法来进行：

1. 对于 A 级和 B 级功能，应识别该功能及其设计保证级别，该级别基于针对该功能的硬件要求和系统的 FHA。功能可以形成为一个子功能的集合，每个子功能都具有对应的一组导出要求和相关的设计保证级别。必要时这些子功能可以再作进一步分解。
2. 对于每个 A 级和 B 级功能，确定实现该功能和其子功能的手段，并分析其设计保证选项。可获得的或预期可获得的用于功能或功能的实现的保证数据应是完整的，并能为设计保证策略或所选的策略所接受。如果可获得的或预期可获得的保证数据是完整的、正确的和可接受的，则没有必要再做进一步分解。
3. 对于非 A 级和 B 级的 FFP，应使用一种 F-FMEA、共模分析或依赖性图来对它们与 A 级或 B 级 FFP 的相互关系进行评价，以确保 A 级和 B 级

FFP 不受非 A 级或 B 级 FFP 的不利影响。

这一评估过程是反复进行的。如果对于一个 FFP，没有可接受的设计保证方法，就应重复进行分解和评价过程，或改变结构或硬件功能的实现，直至确定了一种可接受的设计保证方法，提供了或能提供对于 A 级和 B 级 FFP 的可接受的保证数据。

用于硬件设计保证的 FFPA 的结果和选择的方法应与本文档第 2.1 节所述飞机系统过程进行协调。这些结果被用于检查和确认飞机级别的假设，特别是与类似硬件项目的多重交叉系统应用相关的假设仍然是有效的。

2.2 功能型故障路径分析数据

FFPA 数据应：

1. 识别已经从系统级别分派给硬件的异常动作和功能故障。
2. 识别 FFP，其异常动作或功能故障的效果以及设计等级中的分解级别，对于该级别已经进行了分析，且可接受的保证数据的类型和位置均应可获得。
3. 描述 FFP 之间的关系以确定其独立性和与其它 FFP 和部件的相互独立性。这种关系可以用定性的 FTA 或其它自顶而下分析、共模分析、F-FMEA 或依赖性图来进行描述。该关系描述应识别那些相互关联的路径和部件及其相互依赖性。
4. 在 FFP 和硬件要求与导出要求之间进行跟踪。

3.0 对于 A 级和 B 级功能的设计保证方法

本文档的目的并不在于通过使用任何当前的或将来的方法来限制设计保证的实施。本文中讨论的方法可以用于满足第 4 节到第 6 节中所述过程的一个或多个目标。

3.1 结构性缓解

结构化的设计特征，如不同的实施、冗余、监视器、隔离、分区和命令/授权限制，都可以特定地用来减轻或容忍硬件设计和实施错误的不利影响。作为PSSA 的一部分，诸如定性的故障树分析和共模分析之类的活动都可以为确定减轻或容忍硬件故障、失效和设计与实施错误的影响所需要的结构属性的范围提供保证。更特别地，对于附录 B 第 2 节中所述的硬件，该方法应与 FFPA 方法结合使用，并应采用共模分析过程来确定特定减轻策略包含硬件设计和实施错误的适用性。例如，冗余通常主要有助于随机故障或混乱的区域，而若其共模内容已被识别的话，冗余也可以有效地用于减轻设计和实施错误。

3.1.1 结构性缓解方法

结构性缓解是通过首先识别与推荐的硬件实施相关的 FFP，然后分析设计选项来识别和提出设计特征和减轻这些 FFP 影响的策略来完成的。提出的结果对于减轻 FFP 的所有相关影响的总体效果应予以评价和识别。结构性缓解策略的引入也引入了一些导出的要求，其实施应按此要求进行验证。特别地，结构性特征应防止所识别的 FFP 的一些或所有不利影响，并应就其它故障路径的引入进行评估，然后这些路径应通过进一步的结构性缓解，或通过本附录中描述的另一种设计保证策略来进行识别。

3.1.2 结构性缓解解决方案

安全性评估过程确定了结构性缓解的可接受性。FFPA 应首先识别所有为增加可信度而使用结构性缓解的 A 级和 B 级硬件 FFP，并应识别要使用的方法，确定该结构性缓解的基本原理。在可能涉及更复杂或更简单的结构性缓解策略的集合的总体结构方法的条件下，适宜性是通过对支持该结构性缓解的每个功能进行评估来确定的。

共模分析应识别在要求、实施、制造和维护中可能破坏该缓解的潜在的共模错误。设计者也应考虑的形成结构性缓解功能的硬件的潜在随机故障，这些故障可能会导致无法获得缓解。支持缓解的功能的可获得概率应与失去缓解的结果相当，其结果会导致安全性边界的降低。

总体方法应确保实现和维持正确的工作和在必要的功能之间的可接受的独立性。应对需要消除、隔离或限制残留共模效应的任何特殊安保需求进行识别，并以附加结构性缓解或本附录中所述其它设计保证策略的形式将其纳入。

当结构性定义完备时，被确定为未经缓解或未足够缓解的 A 级和 B 级 FFP 中的硬件功能应用本附录中的另一设计保证方法来重新识别。例如，当其分析用于识别和提供对适用的电路和部件的未缓解部分的验证覆盖时，各个电路和部件的部分结构性缓解可与特定安全性分析方法联系使用。

3.1.3 结构性缓解数据

用于保护硬件中的 A 级和 B 级 FFP 的结构性缓解措施文档，应以安全性评估数据、安全性要求数据和溯源性数据的形式提供。安全性评估数据应基于对硬件 FFP 和共模失效分析的评估，该分析特定地识别硬件设计的结构性缓解内容。

结构性缓解数据应包括：

1. 将通过结构化措施进行保护的 A 级和 B 级硬件 FFP 的识别。
2. 结构化方法的说明和关于由该方法提供的覆盖的批准的理论基础。
3. 适用于该结构的共模边界和共模分析内容的理论基础。
4. 未缓解的和未适当缓解的 A 级和 B 级 FFP 的识别，这些 FFP 要由其它设计保证方法来处理。
5. 关于功能型操作和结构化缓解机制所需要的设计属性的要求。

6. 包括软件，例如软件分区、安全性监视器和不同的软件的用于满足安全性要求的缓解机制。这些机制和安全性软件要求应提供给系统过程和软件开发过程。
7. 完成适当的结构性缓解的对任何硬件的常规失效比数据和潜在故障曝光评估数据。
8. 将安全性要求与适用的安全性评估数据和适用的设计验证数据相联系的溯源性数据。

3.2 产品服务经验

第 11.3 节提供了如何评估产品服务经验数据用于机载硬件的适用性的基本指南。对于使用先前开发硬件作为设计的一部分的 A 级和 B 级功能，有必要提供额外的设计保证。这种保证可以按下列方式提供：

3.2.1 产品服务经验方法

在完成了第 11.3 节所述的评估之后，应根据任何适用的服务经验对由所考虑的硬件来实施的 FFP 进行分析。使用者或设计者应识别服务经验数据并确定服务经验数据显示出硬件的再利用功能在先前的硬件使用期间已经试用够了。

3.2.2 产品服务经验解决方案

当完成了服务经验数据分析时，对已确定未试用、试用不够或在服务操作中未获得服务经验的 A 级和 B 级 FFP 中的硬件功能，应利用其它设计保证方法或通过对能用于试用该功能的其它验证方法的识别来进行处理。

3.2.3 产品服务经验数据

用于保护硬件中的 A 级和 B 级 FFP 的产品服务经验数据应包括：

1. 第 11.3.2 节中的产品服务经验评估数据。
2. 对通过服务经验和关于服务经验数据充分的理由提供了设计保证的 FFP

的识别。

3. 对服务经验数据不充分的 FFP 的识别和测试环境、测试程序、用于完成对该 FFP 的设计保证的分析和结果的识别。
4. 对 FFP 和服务经验未明示的工作条件的识别，它将要求使用其它的结构性缓解或先进验证方法。
5. 第 10.4.1 节中所述的溯源性数据显示出在服务经验数据和提供了每个 FFP 的设计保证覆盖的验证之间的明确关系。

3.3 先进验证方法

通过诸如元件分析、形式方法、特定安全性验证方法或其它使用者提出的、鉴定机构接受的先进验证方法的使用，可以实现额外的设计保证置信水平并提供证据。

选进的设计保证验证方法使用了附录 B 第 2 节中所提出的 FFPA 方法并延伸了其范围。FFPA 方法被渐进地在设备级、电路级和部件级使用以确定 A 级和 B 级 FFP 的硬件实现。然后来自 FFPA 的数据又用于确定适用于那些 A 级和 B 级 FFP 中所包含的硬件电路、部件和原件的设计保证手段。

这三种方法总结于下并在后续章节中进行描述。

1. **元件分析。**要素分析从一个自底向上的透视中提供了对硬件验证完整性的度量。在 FFP 中的每个功能型元件都被加以识别，并用满足第 6.1 节验证目标的验证试验案例进行了验证。该分析可能也识别了需要由其它适当手段来处理的相关区域。
2. **特定安全性分析**。该策略关注于找出和纠正从一个系统安全性透视中会对硬件输出产生不利影响的设计错误。硬件输入空间和输出空间的适用的安全性敏感部分被通过分析加以确定。对硬件输入空间的敏感部分加

以刺激，然后对输出空间进行观察，不仅观察安全性敏感的预期功能要求验证，也观察其异常动作。输出空间观察的方法预先通过分析进行了识别，该分析是利用传统的安全分析技术来完成的。

3. **形式方法**。形式方法对规范、设计和计算机系统的验证利用了源自形式逻辑和离散数学的技术。这些技术可用于证明在硬件设计生命周期的各个过程中使用的推理分析。

使用者也可以选择除本节所述方法之外的其它先进验证方法。

3.3.1 元件分析

元件分析可用于表明 FFP 是通过相关的验证测试案例进行验证的。元件分析提供了信心和证据，表明设计错误已通过将 FFP 的复杂实现分解为在设计者生成该元件的级别的元件的方法进行了排除。该分析方法提供了对支持验证覆盖率和完整性的确定的验证过程的一个度量，在详细设计为可视并在构型控制之下的场合最为适用。这可以是 ASIC 或 PLD 中的案例，其中功能在相同的设计保证级别予以识别，或不同设计保证级别的功能被隔离或分开。适用的电路或部件的每个功能元件都被加以识别，并用满足第 6.1 节验证目标的验证程序对其预期功能正确性进行了验证。元件分析通常适用于整个部件或一个组件，而与其中实施的变动的 FFP 的数目无关，但如果可为隔离、独立性或不同 FFP 的分离提供一个理论基础，也适用于一个部件或组件的一部分。

注：当对在一个 PLD 中实现的某个功能进行一次元件分析时，编程的内容和 PLD 特性的应用也应包括其中，而未编程的部件可以用另一方法，如先前的服务经验等来进行处理。

该分析识别了需要通过适当手段来处理的关注区域。没有这种分析的验证过程可能使某些电路的测试不够充分。从历史经验来看，这种不充分性是由于

缺乏基于要求的测试程序、不清晰或不完整的硬件要求、未使用的电路、初始化电路和程序库功能导致的。这种分析检查了所关心的 FFP 中元件的验证，并确定了与每个元件相关的验证覆盖是否完整。对每个元件的验证覆盖不完整的结论表明需要有其它的验证或适当的活动。

使用者应提出在设计层级的哪一级对元件进行定义，以及如何对它们进行验证覆盖分析。

3.3.1.1 元件分析方法

考虑到硬件设计保证级别、硬件技术和实施的硬件的详情的可视性，元件分析方法将从定义一组将用于分析的准则开始。

其准则应包括：

1. 在硬件设计的适当级别对元件的识别和定义。

2. 对每个元件均应验证的验证覆盖。

然后这些准则将被用于验证活动的分析以确定所计划的验证是否满足验证覆盖完整性准则。如果未满足该准则，则每个被检查的元件应通过给出一组适当的激励，并在试验中被监测的信号上产生相应的可被观察的效果来进行检查。

注：随着本过程检查了针对硬件本身的测试，它也可以检查测试程序的不足。然后对测试不足的识别可提供额外的信心和证据，表明测试是充分的，而且新的或改进的测试案例可以找出硬件中的错误。

3.3.1.1.1 选择元件分析准则

要使用的元件分析准则应取决于硬件元件类型和复杂性，以及元件的可识别的功能操作，在逐个案例的基础上进行选择。该分析可显示出所有低级的原始单元块，如计数器、寄存器、多路复用器、累加器、运算放大器和滤波器都经过了适当的测试，所有的相连原始单元块组合都经过了测试，并满足了验证

覆盖准则。测试程序的分析准则应在对元件及其与其它硬件元件的组合的功能操作进行评估的基础上进行导出，以便实现下一个更高层级的硬件功能。

注 1：例如，如果一个元件是用作延时器的模 n 计数器，则其测试程序可以使用适当的同级选择的输入数据来验证是否在被选通时计数、在被关闭时停止计数、以正确的速率计数、计数到 n 后在规定的时间翻转。没有必要显示出测试程序对组合形成该计数器的各个门电路或触发器进行了测试。

作为将相连的原始单元块用作一个元件的例子，一个算术逻辑单元（ALU）可以由诸如寄存器、累加器和控制逻辑构成。可以模拟该 ALU 来显示组合形成该 ALU 的原始单元块，但在元件分析中使用的验证程序应使用适当的同级输入数据来显示该 ALU 实现了其功能。

不需要在低于硬件设计者规定的设计级别上对元件进行定义。只有在设计明确规定门电路作为组合逻辑或状态机控制时，门电路级分析才是适当的。

注 2：在低于设计者规定的级别，例如在门电路级或晶体管级进行分析是不必要的，因为它类似于在组件语言或二进制图像级别进行软件分析。这些较低的抽象级别是通过对在硬件上进行的验证测试、或成功评估的布局后仿真进行元件分析来隐含地处理的，必要时随验证工具按第 11.4 节进行评定。

ASIC 或 PLD 可能包含专利程序库功能，它不会提供其内部设计的可视性，因而不会允许进行人工分析。程序库功能可以作为元件分析中的 COTS 元件对待，其 COTS 硬件内容按第 11.2 节和附录 B 第 2.2 节之定义进行处理。对程序库功能应用的验证应表明它是与其规范或由程序库制造商提供的说明一致的，而且测试应在允许观察到测试结果的环境中进行。

注 3：其目的并非反对使用设计程序库，提倡创建新功能，而是鼓励通过设计程序库的实际使用来减少在硬件中进一步引入错误的机会。

对于从 HDL 的高级别描述中进行合成的 ASIC 或 PLD，其分析准则可以基于代表硬件的高级别特性语言代码。然而，由于从 HDL 表述中合成的实施可能包括并行逻辑结构和非顺序暂态内容，其综合输出应包含于分析完成决定之中。对合成器也应进行评估。

3.3.1.1.2 完成元件分析

元件分析应使用在下列测试环境的一个或多个中完成的以要求为基础的验证测试：

1. 实现功能路径的电路安装在目标组件中的测试。
2. 在独立的原型上进行的测试。这种测试典型地用于 ASIC 或 PLD。
3. 制造验收测试。

   注：因为制造测试通常并非基于要求，制造验收测试可局限于它们在元件分析中的应用。
4. 布局后仿真，典型地用于已经过评估的 ASIC 或 PLD，必要时，可用作第 11.4 节中所述的验证工具。

元件分析自身可通过使用仿真来测试所达到的完整性来进行，只要被分析的测试程序可以与所用的元件分析准则相联系，而且用于满足第 6 节目标的硬件功能验证。如果分析的测试程序是从一个硬件或独立原型的电路内测试导出的，并且用仿真来进行检查，则测试激励和预期的结果可以对仿真器进行翻译，只要作为元件分析的一部分，对翻译过程进行了精度检查。用于进行元件分析的仿真器应表明能够正确地确定在实施中所包括的每一类型的元件是否满足分析准则。

3.3.1.2 元件分析结果解决方案

元件分析可以揭示硬件元件未经验证，表明需要进行其它的验证过程活动，又或许需要移除未测试的元件或减少由结构化手段导致的任何异常动作。未经测试的硬件元件可以是下列结果：

1. **验证测试案例或程序不足**：如果测试案例未按照附录 B 第 3.3.1.1 节中的准则对硬件项中的元件进行测试，就会出现这种不足。如果在功能性要求中有注意事项而硬件项目并未适当设计以产生可重复的响应，也会出现这种不足。在此情况下，测试程序和案例应进行增补或改动。此外，应就验证其各要求的测试能力进行评审。
2. **要求不充分**。应对要求进行修改或识别其它导出的要求。然后应开发针对新的或修订过的要求的附加验证测试，并予以执行和分析。
3. **未使用的功能**。硬件项目可能包含在其目标电路应用中未使用的功能，例如在程序库功能中未使用的子功能或仅用于元件级验收测试的测试结构。这种功能必须表明与其它使用了的功能实施了隔离，或表明不存在对安全性有不利影响的潜在异常动作。这可以通过显示未用元件在硬件中或在安装时已被彻底去除功能来实现。如果未使用的功能要在将来的一些应用中使用，则只要这种功能被识别为未经充分验证，就可在那时对元件分析缺陷进行再评估。
4. **无安全性后果的元件**。元件的异常动作的后果可以通过不会对飞机或其乘员造成不利安全影响的分析来限定和显示。这些项目应通过记录限定了元件异常动作后果的分析来解决。

3.3.1.3 元件分析生命周期数据输出

元件分析生命周期数据输出应：

1. 识别要通过元件分析来处理的 FFP，提出在哪一设计层级对元件进行定义，以及如何对其验证充分性进行分析，哪些是验证覆盖完成准则的一部分。这应包括在 PHAC 或硬件验证计划中。
2. 描述分析方法并识别在分析中处理的 FFP，以及完成分析的设计层级。
3. 确保第 10.4.1 节中所述的溯源性数据表明了验证程序与元件分析中的元件之间的明确关系。
4. 识别作为元件分析结果被增加的或修改的验证测试案例和要求。
5. 说明由元件分析处理的 FFP 所达到的验证完整性级别，包括对验证测试或要求的修改未解决的分析差异的识别，以及可接受性的理论基础。

3.3.2 特定安全性分析

在应用时，特定安全性分析方法通过对选择的电路和部件进行更深入的分析来扩展了硬件 FFPA 的概念。扩展的 FFPA 被用于导出和批准关于电路和部件的内部操作的特定安全性要求。然后这些导出的安全性要求又通过下面所述的验证测试来处理。

特定安全性分析是基于潜在的设计错误只会在特定的输入响应使其暴露时才能影响硬件项目的输出的概念。因而为了适当地激励和暴露所关心的安全性错误，安全操作是必要条件的输入案例的子集应予以识别，然后在验证测试中应包括来自该子集的相应的等同级别。在这些测试案例执行期间，将对项目输出是否不存在会导致不安全输出状态的特定异常动作进行评价。特定安全性分析被用于限定在验证测试案例中要施加的输入条件集，所以就不必处理潜在的无限的输入测试案例集。

注：该实施或也限制了输入集和条件，因而实施中允许超出测试限制的输入是不可能的，或是出现概率充分小的。

特定安全性分析方法也可用于确定适于部分结构性缓解的电路和部件功能中未缓解的部分。在此情况下，附加的特定安全性分析会是有用的，而且确定需要何种附加设计保证的有效方法是完成安全性覆盖所需要的。

特定安全性分析方法可等同地适用于 COTS 硬件或客户定制电路和部件，应为它能够使用关于这些电路和部件的用户指南数据而不是详细的内部设计数据。通过对用户指南数据与 FFPA 方法的更详细的应用进行组合，特定安全性分析就能够成功地确定电路和部件使用与相关的内部 FFP 的安全性敏感部分，对于这一部分有必要强调去除设计错误。然后该信息又可用于成功地导出电路和部件验证测试，而完成这些测试时，可使这些从系统安全性角度可对硬件产生不利影响的电路和部件设计错误在验证过程得以暴露和纠正、缓解或为其提供相关工作。

3.3.2.1 特定安全性分析方法

一旦选择了要用设计保证的特定安全性分析方法来处理的电路和部件，就应进行一个附加的 FFPA 来更详细地检查项目。这种分析更特定地确定了哪个电路和部件功能对已经识别的使用这些电路和部件的 A 级和 B 级功能做出贡献。这是通过逐个案例地在其功能边界检查每个适用的电路和部件来完成，其中考虑到了完成所识别的 A 级和 B 级 FFP 中包含的更高级别硬件功能的该电路或部件的实际功能应用。

注：在电路和部件用户指南数据中可以获得足够的信息，用户可以成功地使用该电路或部件的功能来完成更高级别的硬件功能。如果可以获得关于电路或部件内部功能的足够信息，进行这种评估也是非常适宜的。如果不能获得足够信息，就不能进行这种评估，可以使用其它方法来代替或与此方法结合使用。

在根据电路和部件的实际用途对其相关的安全性敏感功能进行了识别之后，下一步便是更为详细的功能分析。该分析应确定这些电路和部件功能的特定安全性敏感和未缓解属性，这些属性将通过特定安全性验证条件进行更为详细的处理。这些验证条件可以通过使用 F-FMEA 技术来导出和批准，以确定安全性敏感的特定功能属性，并进一步确定这些功能中会对电路或部件中的 A 级和 B 级 FFP 做出贡献的功能的异常动作。

通过上述特定安全性分析活动得到的导出验证条件可与下列指南结合使用，以完成用于 A 级和 B 级 FFP 中所含电路和部件验证的特性安全性分析准则。指南包括：

1. 识别该功能的相关输入空间。根据所识别的安全性敏感功能属性和异常动作来确定相关的输出空间合格/不合格条件，并选择将为相关的输入空间提供必要覆盖的等同类别。
2. 识别相关的可观察检测手段，以及用于所考虑的每个功能的输入空间激励措施。

   注：可以使用特殊工具或工具特性来确保观测能力和测试能力。
3. 规定对潜在错误来源进行验证和确保相互独立性的测试环境。

   注：元件级的功能应在可行的最高集成级别进行测试。在最高集成级别进行测试通常可提供对错误来源，如混乱、相互独立性和潜在的交叉功能性相互作用等的最佳覆盖。

测试应按等同级别来选择。测试应列出关键的逻辑决定，包括算术、定时、状态转移和实时属性等。

3.3.2.2 特定安全性分析解决方案

特定安全性验证完成准则应通过完成对所有适用的电路和部件的特定安全

性分析来建立。该分析或验证本身发现的任何缺陷都应通过下列方法之一予以解决：

1. 改变设计来纠正错误。
2. 增加结构性缓解，它将通过将其从相关的 FFP 中去除来解决该错误。
3. 增加适当的测试。

3.3.2.3 特定安全性分析数据

当应用于 A 级和 B 级 FFP 中的电路和部件时，特定安全性分析的文档应以安全性评估数据、安全性要求数据、验证程序和结果以及溯源性数据的形式提供。验证程序应能溯源至安全性要求，以及特定安全性分析。特定安全性分析数据应包括：

1. 要通过特定安全性分析方法来处理的电路和部件的识别。
2. 每个电路和部件所在的 A 级和 B 级 FFP 的识别。
3. 对适用于电路和部件的部分结构性缓解的识别，其设计保证的完成将通过特定安全性分析方法来实现。
4. 对于每个适用的电路和部件，安全性敏感功能的识别。
5. 对于每个识别的安全性敏感功能，所关心的安全性敏感属性和异常动作的识别。
6. 列出适用的电路、部件、内部功能、功能属性和异常动作的验证条件。
7. 列出要验证的输入依赖性和输出空间动作的验证条件。
8. 验证程序和结果。
9. 将验证程序和硬件安全性验证条件与特定安全性硬件分析数据相联系的溯源性数据。

3.3 形式方法

术语形式方法是指在计算机系统的规范、设计和构造中使用了形式逻辑和离散数学。

注：本节中的材料是从 1997 年 5 月出版，编号为 NASA-GB-001-97 的《用于软件和计算机系统验证的形式方法规范和分析指南》第 II 卷《实用指南》中导出的。其中可找到形式方法应用的更为详细的内容，并有工作实例。

形式方法的应用落入了两个较宽的范围，描述性的和演绎性的方法。描述性的方法利用了形式规范语言，它提供了对于要求和其它设计内容的清晰的、豪不含糊的描述。演绎性方法依赖于要求明确列举所有假想和推理步骤的规则。此外，每个推理步骤必须是少量允许的推理规则的一个例子。大多数严格的形式方法应用这些技术来证实用于证明要求或其它复杂和严格系统的设计和实现的内容的推理。形式方法的目的是在评价论据时减少对人的直觉和判断的依赖性。亦即，演绎性的形式方法较少了某个论据对于*计算*的可接受性，从原理上说，该计算可通过一个工具来检查，所以它用可重复的动作代替了评审过程的固有主观性。

有几个区域要应用形式方法来提供设计过程中的额外保证。尽管在整个设计过程中形式方法都是适用的，然而增加设计保证可以通过有目标的应用来获得。下面所列指出了其中一些可能性：

1. 形式方法可以应用于开发生命周期的不同阶段。一般地，在生命周期的较早阶段特别是在需求分析和高级别设计阶段应用形式方法是最有效的。
2. 形式方法可以应用于整个设计，也可以特别针对特定的部件。FFPA 用来确定哪个 FFP 要用形式方法来分析。处理复杂并发通讯的协议和实现

容错功能的硬件也可以用形式方法进行有效的分析。

3. 形式方法可以应用于验证系统功能性，也可以用于建立特定的属性。尽管传统上形式方法与“顶级正确性”相联系，即确保某部件满足其功能性规范，它们也可以只应用于最重要的属性。通常，更为重要的是确认某个设计并未显示出某些预料之外的特性，而不是证明其功能齐全。

典型情况下，形式方法的实际应用要求有工具支持。所用的工具应加以评估，必要时应符合第 11.4 节所述要求。

3.3.3.1 形式方法的方法论

形式方法的应用通过用形式语言来表述要求开始。要求规范用作一个重要的描述性功能。它为使用明确的标记来对系统的动作和特性进行记录、通讯和模型化奠定了基础。此外，要求规范还用作计算或形式化预计系统动作的基础。要被分析的部件的形式模型是用形式语言构建的。该模型使用选定的形式逻辑的规则按照要求的形式语句进行分析。模型的特性是通过要完成的形式分析的类型来确定的。

在部件模型中的详细程度是由所选形式方法技术的目标来确定的。一些方法被加以裁剪以发现会逃避测试的设计错误，而其它方法则致力于确保不存在某些类型的设计错误。

1. **错误检测。**用于错误检测的最普通的形式技术即所谓的模型检查。此处要求被表述为在可决定的暂态逻辑中的公式。部件的模型是适当设计的一个抽象状态机，它保留了要测试的属性。证明程序是自动完成的。失败的证明试图表明在模型化的部件中存在设计错误。失败证明的结果是输入激励产生的后果，它特定地表明了部件并不满足所描述的要求。
2. **错误排除。**旨在防止错误的形式方法一般基于具有支持性证明理论的表

示性规范语言。随着表述性的增加，可以表述更复杂的要求，可以构建更详细的部件模型。然而，证明程序或许只是部分自动化的。对于部件模型而言适当的详细级别或许是一个可合成的 HDL 描述。在某些情况下，可以对仿真和形式分析使用同一个模型。一个完备的证明是部件根据所述的要求对于所分析的输入空间而言在逻辑上正确的证据。

3.3.3.2 形式方法解决方案

共有三种可能的演绎性形式分析结果：

1. 如果证明成功，验证活动就是完整的。设计保证的级别取决于所用模型的重现性。例如，如果硬件项目的模型对应于详细设计，则该证明应保证其功能正确性等同于详尽测试的结果。
2. 在某些情况下，失败的证明产生了一个明显的计数器例子，亦即，它识别了一个特别表明设计如何不满足所述要求的测试场景。这可表明在设计或要求中存在缺陷。这样的缺陷可以通过纠正设计、修改显示出并非实际可实现的条件的要求或使用另一方法来解决。所有的计数器例子都应如此识别，以便于得到解决。对设计或要求的更改需要反馈至适当的过程。
    a. 在设计或要求已经加以修改以列出由失败的证明企图识别的缺陷后，应再次尝试该证明以确认该修改成功地处理了所识别的问题。应重复该循环直至实现了成功的证明。
    b. 在考虑某个计数器例子不进行要求或设计改动而只让工具识别一个计数器例子，即已被解决的计数器例子的情况下，应对该过程进行适当修改，使它能够识别所有其它的计数器例子。
3. 最难以解决的情况是不能产生证明而且不能识别计数器例子。一个可能

的选择是修改设计以便简化验证效果。另一种选择是，验证活动可以用在该证明所处理的案例和其要求需要通过其它手段进行处理的案例之间的清晰描述来分解。对设计和导出要求的改变应反馈至 FFPA。

3.3.3.3 形式方法数据

在实行方法应用期间产生的数据包括：

1. 要被使用的特定形式方法和欲对其应用形式方法的部件或 FFP 的描述。
2. 对要求的形式化描述。
3. 部件的形式模型。
4. 证明，或足以生成证明的详细的脚本，它将部件的模型与要求的形式化描述关联起来，并将相关性纳入溯源性数据中。
5. 所用的工具的识别和工具评估结果。
6. 验证测试案例和作为分析结果被添加或修改的要求的识别。
7. 分析所处理的 FFP 达到的验证完整性级别描述。包括对验证测试案例或要求进行改动未能解决的分析差异的列表，以及该差异的可接受性的理论基础。