http://myfj.cnjournals.com myfj_sadri@comac.cc (021)20866796

DOI: 10.19416/j.cnki.1674-9804.2021.01.021

简单用户微编码器件适航要求研究

周 红* 江玉峰

(中电科航空电子有限公司,成都 611731)

摘 要: 用户微编码器件的便捷性与高效性,使其在机载设备研制中被广泛应用。由于具有高度集成性和复杂性,难以通过传统方法对开发过程中产生的设计错误进行管理和评估,其使用会对飞机的安全性造成影响,因此通常采用研制保证方法表明用户微编码器件的适航符合性。但在实际项目中,用户微编码器件实现的功能可能较为简单,采用充分的确定性测试和分析相结合的方法足以表明其功能确定性,确保其在机载设备中的使用安全性。通过对现有适航咨询通告、工业标准及实践指南等资料的分析和研究,旨在梳理出简单用户微编码器件通过充分的确定性测试和分析相结合的方法表明适航符合性需满足的相关要求和关键要素,为机载设备制造商完成简单用户微编码器件的适航验证提供支持和帮助。

关键词: 用户微编码器件;简单;测试;分析;适航

中图分类号: V243 **文献标识码**: A **OSID**:

0 引言

随着民用飞机研制周期的大大缩短,机载设备研制节奏也随之加快。在短时间内研制出安全、可靠、功能强大且成本更低的机载设备,是制造商们的迫切愿望。用户微编码器件在电子硬件设计中的便捷性与高效性,使其在机载设备研制中广泛被使用。用户微编码器件高度集成且复杂,开发过程中产生的设计错误难以通过传统的测试分析方法进行管理和评估,而这些设计错误会对飞机功能的实现造成影响,进而影响飞机安全性。因此,各国局方普遍采用研制保证(又称“过程保证”)方法对其进行管理。但在实际项目使用中,用户微编码器件可能实现的功能较为简单,制造商希望采用工作量更少,成本更低的测试分析方法来表明其适航符合性。在缺乏明确要求的情况下,本文旨在通过对现有适航咨询通告、工业标准及实践指南的研究,梳理出通过测试分析方法表明简单用户微编码器件(以下简称“SEH”)符合性需满足的适航要求。

1 用户微编码器件

用户微编码器件的名称来源于美国联邦航空局(FAA)发布的咨询通告(AC 20-152),其定义为被封装成可在电路板或更高层级组件上安装使用的单一集成电路器件[1]。用户微编码器件是 20 世纪 70 年代发展起来的一种新型逻辑器件,其应用和发展不仅简化了电路设计,降低了成本,提高了系统的可靠性和保密性,还给数字系统设计带来了革命性变化。用户微编码器件发展至今,已形成多种型别,包括小规模集成的可编程只读存储器(PROM)、可编程阵列逻辑(PAL)和通用可编程阵列逻辑(GAL),以及大规模集成的复杂可编程逻辑器件(CPLD)和现场可编程门阵列(FPGA)。

2 国内外研究现状

为确保在民航领域的使用安全,美国联邦航空局(FAA)于 2008 年 7 月发布指令(Order 8110.105),对用户微编码器件的使用进行管理[2]。FAA 还将其分为简单和复杂两类,并指出简单类型有两

* 通信作者. E-mail: zhouh@cetca.net.cn

引用格式: 周红,江玉峰. 简单用户微编码器件适航要求研究[J]. 民用飞机设计与研究,2021(1):128-131. ZHOU H, JIANG Y F. Research on certification requirement of simple custom micro-coded component[J]. Civil Aircraft Design and Research, 2021(1):128-131(in Chinese).

种可接受的符合性方法。一种是研制保证,即采用已计划并开展的系统性活动证明,用户微编码器件的开发错误已被识别和纠正,且满足适用的审定基础;另一种是测试分析,即通过充分的确定性测试和分析相结合的方法证明用户微编码器件的适航符合性。另外,FAA 除在指令中提出针对 SEH 的要求外,还额外发布支持文件(如 CAST Position paper)对要求进行详细说明[3]。欧洲航空安全局(EASA)和加拿大民用航空运输部(TCCA)则分别发布审查备忘录(CM-SWCEH-001 Issue 01 Revision 02)和电子硬件审查手册(CM E-02),提出针对 SEH 的管理要求。

目前,国内还未发布关于 SEH 的适航规章要求。但在实际审查时,审查方会针对具体项目中使用的 SEH 提出专门的审查要求。

3　国外要求分析和研究

本文仅讨论采用测试分析方法表明 SEH 适航符合性的通用要求,其它额外要求(如工具评估及鉴定、先前开发硬件等)不在考虑范围。

3.1 FAA 管理要求

审定计划(PHAC)需满足 DO-254 指南要求,还需包含 SEH 清单、器件实现功能、器件失效影响、建议符合性方法、器件研制保证等级(DAL)及输出数据等[4]。

确认方面,需识别和确认衍生需求,记录确认活动,并对记录进行合理构型管理[5]。A 和 B 级 SEH 的确认活动需具备独立性。验证方面,需验证 A 级和 B 级 SEH,在输入信号及内部状态所有可能的排列、组合和并发条件下,能够正常工作,不产生异常行为,并开展验证目标覆盖率及时序分析。验证 C 级 SEH,在输入信号所有可能的排列和组合条件下,能够正常工作,并验证状态机所有可能状态[6]。验证 D 级 SEH 满足硬件需求。

追溯性方面,A 级和 B 级 SEH,需建立硬件需求(直接分配的系统需求)、概念设计、详细设计及实现之间的追溯;建立硬件需求、概念设计、详细设计及实现与验证和确认结果的追溯。C 级和 D 级 SEH,建立需求与测试的追溯。构型管理方面,识别构型项,并开展变更控制及问题报告管理。建议提交数据包括 PHAC、硬件验证计划(HVEP)、硬件研制综述(HAS)及硬件构型索引(HCI)等。

3.2 EASA 管理要求

SEH 是通过符合其 DAL 要求的充分的确定性测试和分析,能够证明在所有预期条件下可正确实现功能,不存在异常行为的器件。

验证方面,需验证 A 级和 B 级 SEH,在器件内所有逻辑块(门或节点)输入状态的所有可能排列、组合及并发条件下,能够实现预期功能。验证 C 级 SEH,在器件管脚级输入的所有可能排列、组合及并发条件下,能够实现预期功能,并验证状态机所有状态。验证 D 级 SEH 满足硬件需求。所有 SEH,需完成需求验证,并开展验证覆盖率分析[7]。

对 SEH 进行合理构型控制。提交数据包括 PHAC、硬件开发计划(HDP)、硬件确认计划(HVAP)、HVEP、硬件构型管理计划(HCMP)、供应商管理计划(SMP)、HAS 及 HCI。

3.3 TCCA 管理要求

SEH 是通过确定性测试和分析的充分组合,能够证明在所有预期工作条件下,可正确实现功能,不存在异常行为的器件。

PHAC 需列出 SEH 清单,说明器件供应商、器件实现功能、器件 DAL 及建议符合性方法等[8]。

验证要求与 EASA 一致。追溯性方面,A 级和 B 级 SEH 需完成系统需求、硬件架构设计及硬件需求、概念设计、详细设计与实现的追溯。C 级和 D 级 SEH 完成硬件需求与测试用例的追溯。

构型管理要求与 EASA 要求一致。提交数据包括 HAS、顶层图纸及所有符合性报告。

3.4 DO-254 指南要求

SEH 是通过符合其 DAL 要求的确定性测试和分析的充分组合,能够证明在所有预期工作条件下,可正确实现功能,不存在异常行为的器件[9]。

验证和构型管理过程要求对 SEH 适用。

3.5 要求对比与分析

国外各方对 SEH 的要求汇总如表 1 所示。

表 1　SEH 要求汇总表

序号	要求类型	FAA 要求	EASA 要求	TCCA 要求	DO-254 要求
1	器件定义	√	√	√	√
2	审定计划	√	√	√	
3	确认要求	√			
4	验证要求	√	√	√	√
5	追溯性	√		√	
6	构型管理	√	√	√	√
7	提交数据	√	√	√	

通过对各方要求的分析和总结,可看出:

1) SEH 要求可分类为器件定义、审定计划、确认、验证、追溯性、构型管理和提交数据;

2) 器件定义、审定计划、验证、构型管理及提交数据方面,各方都提出要求且基本一致;

3) FAA 和 TCCA 立场一致的提出追溯性要求;

4) 仅 FAA 提出确认要求。

TCCA 的 SEH 定义与其他方不同,缺少关键词 DAL。由于所实现功能存在不同 DAL 要求,且对 SEH 的测试和分析也应充分考虑 DAL 差异,因此在 SEH 定义中增加 DAL 约束是有必要的。

追溯活动建立了系统需求、硬件需求、硬件设计、硬件实现与硬件确认和验证之间的联系,对确保需求分配、实现及验证的正确性和完整性有重要意义[10]。

硬件需求的正确性与完整性是保证项目成功的基础。硬件需求包含系统分配的需求和衍生需求,衍生需求可能会对安全性造成影响。EASA 在审查备忘录第 8.4.1 节要求对所有硬件需求进行确认,而 FAA 在指令第 4.4 节仅要求对衍生需求进行确认。另外,DO-254 指南第 6.1 节指出确认过程是确保衍生需求正确性和完整性所不可或缺的。因此,在考虑系统分配到硬件的需求由系统进行确认的情况下,增加衍生需求的确认工作是合理的。

4　适航要求考虑

通过上述分析和研究,建议从如下几个方面考虑针对 SEH 的管理。

1) SEH 器件定义

通过采用符合其 DAL 要求的充分确定性测试和分析相结合的方法,能够证明在所有预期的工作条件下可正确实现其功能,而不存在其它异常行为的器件。

2) 审定计划

PHAC 除需包含 DO-254 指南第 10.1.1 节内容外,还需包含 SEH 清单、器件实现功能、器件 DAL 要求、建议的符合性方法、提交数据及器件使用经验说明(按需)等。

3) 确认要求

识别和确认衍生需求,并根据 DO-254 指南第 6.1.2 节准则检查确认活动完整性;记录确认活动,并根据 DAL 及 DO-254 指南附录 A 要求对确认活动记录进行管理;捕获异常和边界条件下,期望 A 级和 B 级 SEH 的输出为需求;A 级和 B 级 SEH 的确认活动需满足独立性。

4) 验证要求

建议的验证要求为:

(1) A 级和 B 级 SEH,在器件内所有逻辑块(门或节点)输入状态的所有可能排列、组合和并发条件下,能够实现预期功能[11];完成需求验证,并开展验证目标覆盖率分析;开展时序分析,并考虑最好和最坏时序条件、潜在时钟偏移、温度变化、输入信号建立时间与保持时间等问题。

(2) C 级 SEH,在器件管脚级输入信号所有可能排列、组合和并发条件下,能够实现预期功能,且完成状态机所有可能状态验证;完成需求验证,并开展验证目标覆盖率分析;开展时序分析,要求与 A 级和 B 级一致。

(3) D 级和 E 级 SEH,验证硬件实现满足硬件需求,且覆盖所有需求;

(4) 采用分区设计或者其它手段来证明器件为简单时,需开展分区完整性的验证;

(5) 开展验证规程和验证用例评审,确保规程与用例适用于追溯的需求,且需求被正确和完整的覆盖。

5) 追溯性

(1) A 级和 B 级 SEH,需建立系统需求、硬件需求、硬件设计与硬件实现之间的追溯;建立硬件需求、设计及实现与硬件验证及确认结果之间的追溯;

(2) C 级、D 级和 E 级 SEH,建立硬件需求与硬件确认和验证结果之间的追溯。

6) 构型管理

识别构型项,按照 DO-254 指南开展变更控制及问题报告管理。每次审查前,需建立审查基线,关闭必要的问题报告。对已批准设计进行变更时,需证明从批准基线开始即开展构型项的变更控制及问题报告的管理。

7) 提交数据

提交数据包括 PHAC、HVEP、HVAP、HAS、HCI 及其它符合性报告。与审查方达成一致后,如下数据可不提交,但需备查,如系统需求、硬件需求、HDL 代码、硬件评审和分析规程、硬件评审和分析结果、硬件测试规程、硬件测试结果、问题报告及硬件构型管理记录等。

5　结论

本文主要描述了民用航空机载设备中用户微编码器件的使用背景,介绍了用户微编码器件的主要特

性及发展情况,阐述了国内外主流局方对于 SEH 的管理要求,并通过对国外采用的 SEH 管理要求的分析和研究,梳理出适用于具体项目研制的 SEH 管理要求及关键要素,为民用航空机载设备适航验证过程中采用充分的确定性测试和分析相结合的方法表明简单用户微编码器件的适航符合性提供一定的指导和帮助。

参考文献:

[1] FAA. Design assurance guidance for airborne electronic hardware:RTCA DO-254[S]. U.S.:FAA,2005.

[2] FAA. Simple and complex electronic hardware approval guidance:Order 8110.105A[S]. U.S.:FAA, 2017.

[3] 田莉蓉. 机载电子产品适航工程方法[M]. 北京:航空工业出版社,2016:14-65.

[4] Certification Authorities Software Team(CAST). Clarifications on the use of RTCA Document DO-254 and EUROCAE Document ED-80, Design Assurance guidance for Airborne Electronic Hardware:Position Paper CAST-27[R]. [S.l.: s.n.],2006.

[5] Certification Authorities Software Team(CAST). Technical clarification identified for RTCA document DO-254 and EUROCAE document ED-80:Position Paper CAST-31[R]. [S.l.: s.n.],2012.

[6] Certification Authorities Software Team(CAST). Simple electronic hardware and RTCA document DO-254 and EUROCAE document ED-80,design assurance guidance for airborne electronic hardware:Position Paper CAST-30[R]. [S.l.: s.n.],2007.

[7] EASA. Certification memorandum development assurance of airborne electronic hardware:CM-SWCEH-001 Issue 01 Revision 02 [S]. [S.l.: s.n.],2018.

[8] TCCA. RDIMS 9956600,CME-02 Electronic hardware aspects of certification[S]. [S.l.: s.n.],2011.

[9] RTCA. Design assurance guidance for airborne electronic hardware:RTCA/DO-254[S]. [S.l.: s.n.],2000.

[10] FULTON R, VANDERMOLEN R. Airborne electronic hardware design assurance[M]. Boca Raton:Taylor & Francis Group,LLC,2015,107-163.

[11] 王鹏,田毅. DO-254 标准在机载电子硬件审定中的应用[J]. 中国民航大学学报,2010,28(5):18-24.

作者简介

周　红　本科,工程师。研究方向:系统/硬件设计及适航验证。E-mail: zhouh@cetca.net.cn

江玉峰　本科,高级工程师。研究方向:系统安全性评估及适航验证。E-mail: jiangyf@cetca.net

Research on certification requirement of simple custom micro-coded component

ZHOU Hong*　JIANG Yufeng

(CETC Avionics Company Limited, Chengdu 611731, China)

Abstract: Custom micro-coded components are widely used in the development of airborne equipment because of its convenience and high efficiency. Due to its high integration and complexity, it is difficult to manage and evaluate the design errors in the development process by traditional methods, and the components use will affect the safety of aircraft. Therefore, the design assurance method is usually adopted to demonstrate the airworthiness compliance of the custom micro-coded component to certification requirements. However, in practical projects, the function implemented by the custom micro-coded component may be relatively simple. The component functionality visibility can be shown by comprehensive combination of deterministic testing and analysis, and safety of component use in airborne equipment can be assured. Based on analysis and research of current advisory circular, industry standards and practical guidelines, the goal is to sort out the relevant requirements of the custom micro-coded component and key elements should be fulfilled to show compliance by comprehensive combination of deterministic testing and analysis to support and help airborne equipment manufacturers apply for airworthiness certification of simple custom micro-coded component.

Keywords: custom micro-coded component; simple; test; analysis; airworthiness

* Corresponding author. E-mail: zhouh@cetca.net.cn