引用格式:田毅,赵长啸,史春蕾,等. COTS IP适航审定技术研究[J]. 电光与控制,2019,26(12):96-99,110. TIAN Y, ZHAO C X, SHI C L, et al. On COTS IP airworthiness certification technology[J]. Electronics Optics & Control, 2019, 26(12):96-99, 110.

COTS IP适航审定技术研究

田 毅, 赵长啸, 史春蕾, 王 鹏
(中国民航大学,天津 300300)

摘 要: 机载电子硬件承担的系统功能越来越多,基于成本考虑,使用COTS IP成为一种趋势,也为适航审定带来挑战。首先分析了COTS IP在机载电子硬件设计中的使用位置及带来的风险,研究了当前适航审查需求,然后依据局方文件和审定经验提出了建议的评估过程,并总结适航审查要素。研究成果有助于解决COTS IP的适航审定问题,为现有机载电子硬件设计保证方法提供参考。

关键词: 机载电子硬件; COTS IP; 适航审定
中图分类号: V37 **文献标志码**: A **doi**:10.3969/j.issn.1671-637X.2019.12.020

On COTS IP Airworthiness Certification Technology

TIAN Yi, ZHAO Chang-xiao, SHI Chun-lei, WANG Peng
(Civil Aviation University of China, Tianjin 300300, China)

Abstract: Airborne electronic hardware is assuming more and more system functions. Considering the cost, using COTS IP becomes a trend, which also brings challenges to airworthiness certification. The usage position and risk of COTS IP in airborne electronic hardware design are analyzed, and the current airworthiness certification requirements are studied. A suggested evaluation process is proposed based on the authority documents and certification experience, and the airworthiness certification elements are summarized. The research results are helpful to solve the airworthiness certification issues of COTS IP, and provide a reference for the existing airborne electronic hardware design assurance methods.

Key words: airborne electronic hardware; COTS IP; airworthiness certification

0 引言

随着航空电子技术的快速发展,机载电子硬件承担了越来越多的系统功能。为了缩短系统研制周期,在软硬件设计中采用商用货架产品(COTS)推进产品的标准化和模块化是一种趋势[1]。由于完全自定义的设计方法研制成本高、技术难度大,越来越难实现,因此,在可编程逻辑器件(PLD)和专用集成电路(ASIC)中使用COTS IP(Intellectual Property)是目前机载电子硬件研制过程中常见的设计方法。

美国联邦航空管理局(FAA)和欧洲航空安全局(EASA)在近年来分别发布审定指导材料[2-3],给出了COTS IP的适航要求。我国针对具体型号,以问题纪要的形式进行管理,但尚未发布统一的适航审定指导文件。C919飞机于2017年首飞,中国民航局在系统审查过程中发现,显示、监视等系统中采用了COTS IP来承担高安全等级系统功能,对高安全等级机载系统中COTS IP审定是审查面临的难点。本文针对机载电子硬件的适航审定关键问题,结合已有的审查经验,给出了建议的符合性方法和适航审定要素,为我国局方和工业方在COTS IP的适航审定方面提供理论支持。

收稿日期:2019-01-02 **修回日期**:2019-01-31
基金项目:民航安全能力建设资金(AADSA2018007)
作者简介:田 毅(1983—),男,陕西汉中人,硕士,副研究员,研究方向为飞行器适航技术。

1 COTS IP

COTS是由供应商面向多用户开发的部件、集成电路或子系统,其设计和配置由供应商或行业规范控制[4]。COTS部件可以包括电阻、电容、微处理器、未编程的现场可编程门阵列和可擦除可编程逻辑器件、其他集成电路类型及其可实现部件模块、印刷布线组件和完整的航线可更换单元(LRU)。

COTS IP是可进行功能设计的设计模块或功能模块,包括IP库以及用于设计和实现部分或完整的PLD,ASIC等可编程器件。COTS IP面向通用商业市场,可供客户根据需求进行二次开发,在汽车、航空、航天等

领域均有广泛的应用。

1.1　COTS IP 的使用

文献[5]将 COTS IP 分为软 IP、固 IP 和硬 IP 3 类，其中：软 IP 通常是以硬件描述语言（HDL）文本形式提交的，可供寄存器传输级（RTL）设计、优化和功能验证，但其中不含任何具体的物理信息；固 IP 是可以与特定器件技术（如 PLD，FPGA，ASIC 等）映射的结构网表；硬 IP 是器件上固定的一部分，已完成了全部的设计过程，如概念设计、详细设计和硬件实现等，通常以完整的固定版图呈现。图 1 给出了 3 种 IP 在 FPGA，ASIC 典型设计流程中的使用位置。

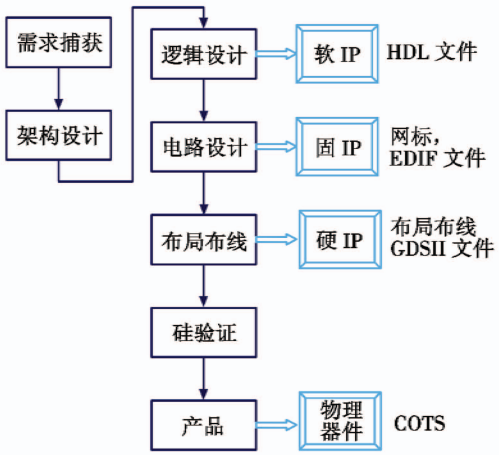

图 1　COTS IP 在典型设计流程中的使用位置

Fig. 1　Position of COTS IP within typical design flow

1.2　COTS IP 的风险

COTS IP 在提高系统设计效率的同时，也给系统适航审定工作带来了挑战。

首先，目前市场上可用的 COTS IP 可能不适用于民机产品。大多数 COTS IP 不是以航空设计标准开发的，可能存在的风险包括：文档、数据不完整或缺失，供应商验证不充分，质量缺陷等。由于 COTS IP 可能缺乏设计保证或服务经验不足，也增大了发生设计错误的概率。

其次，在 COTS IP 内部或在 COTS IP 的使用过程中产生的错误也会导致产品失效。主要的错误包括：COTS IP 设计和验证过程可能并不如宣称的那么严格；COTS IP 的预设使场景与 IP 用户目标使用场景不匹配；不完整或缺少关于 COTS IP 的详细使用描述；COTS IP 与其他硬件设计部分的不正确集成；集成人员缺乏 IP 功能的专业技能。

最后，COTS IP 用户完成集成开发直至器件物理实现时，由于用户对 COTS IP 的内部设计掌握得不完整，COTS IP 用户可能在完成 COTS IP 物理实现的同时引入设计错误。

1.3　COTS IP 适航审定文件体系

针对 COTS IP 的安全使用，局方和研究机构也开展了诸多探索。2000 年，美国航空无线电技术委员会发布《机载电子硬件设计保证指南》（DO-254）标准，探讨了电子部件的管理和采购。2005 年，FAA 发布 AC 20-152，正式认可了 DO-254 标准作为机载电子硬件的符合性方法，但认为标准中关于 COTS 使用的说明不适用于 COTS IP。随着局方认识的深入，FAA，EASA 分别发布审定指导材料，进一步明确了相关适航要求；我国局方针对 C919 型号，以问题纪要的形式给出相关要求。2014 年，国际组织“审定机构软件组”发布了 CAST-33 文件，探讨使用第三方 COTS IP 的可接受的符合性方法。

如图 2 所示，COTS IP 的适航审定文件体系主要包括局方文件、局方或组织的指导文件，以及具体工程设计、产品描述、IP 管理相关的行业文件。

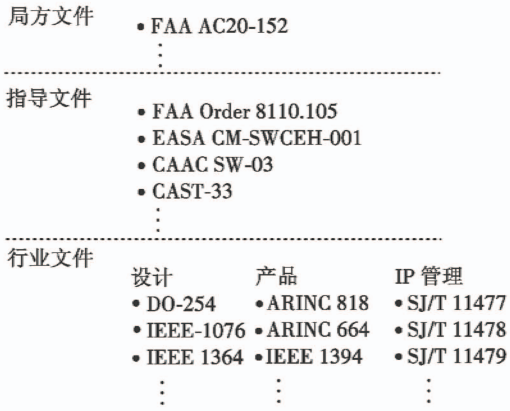

图 2　COTS IP 适航审定文件体系

Fig. 2　Airworthiness certification documentations for COTS IP

2　适航审定需求

早期取证型号中 COTS IP 使用量不大，通常局方建议对于软 IP 和适用的固 IP 直接符合 DO-254，对于不能符合 DO-254 的固 IP 以及硬 IP 按照普通 COTS 器件处理。经过多年实际审定实践，形成了以下审定要求。

1）申请人必须展示使用的 COTS IP 与适用的适航要求、指令、政策以及为其工程而制定的方针相符合。

2）根据 COTS IP 的复杂度和 IP 文件的可用性，申请人为了表明系统或设备的符合性，可能需要补充做大量相应工作，例如仅网表文件或 COTS 处理器（软或硬）核可能难以获得文档来证明符合性。

3）将 COTS IP 应用于那些安装在机载系统或设备上的硬件时应当满足适用的功能和相关安全性要求。申请人采取的方法包括架构缓解、部件验证、试验、分析以及 COTS IP 的其他生命周期数据分析。所有这

些都需要证实 COTS IP 预期的功能,展示其不会发生异常行为。

4) 可以采用下列方法来表明符合性:

① 从已知关于 COTS IP 功能和设计的信息中反向工程(又称逆向工程)所要求的生命周期数据;

② 申请人全面地进行 COTS IP 测试与分析,以便能够获得详细的关于功能以及在边界或失效状态情况下工作的信息,包括对任何不使用的或在特定应用中激活的 COTS IP 中的功能进行测试与分析,对于高安全等级,参考使用高级验证方法[4];

③ 在器件、板卡、LRU 或系统级别上的架构缓解将探测或缓解非预期操作,包括缓解不用的或在特定的应用中激活 COTS IP 中的任何功能;

④ 为了获得审定置信,申请人应当使用已证明过的证据来支持产品服务历史的使用。

3 COTS IP 评估过程

COTS IP 通常是由申请人以外的商业机构开发的,其开发过程可能没有使用严格的设计保证方法。申请人应该证明使用 COTS IP 符合适用于该硬件的适航要求、法规、政策和指南。文献[6]提到目前国际航空业通常采用 DO-254 作为机载电子硬件的符合性方法。文献[2]指出,DO-254 第 11.2 节说明了 COTS 使用,针对的是实际 COTS 部件,虽然很有价值,但没有充分说明在机载系统或设备中使用 COTS IP 的方法,不适于如 FPGA 编程的 IP。因此,为了保证 COTS IP 的使用安全可靠,文献[7]提到在机载应用时需要对其进行全面且有效的适航符合性验证。

为了满足适航要求,在开展 COTS IP 评估前,首先假设已经有了基本的需求和概念设计,并且 COTS IP 已经借鉴文献[8]类似的 IP 评价方法开展了质量评价。

依照局方指导材料和 DO-254 的生命周期过程,图 3 给出了描述 COTS IP 评估过程的建议。

流程中步骤如下所述。

1) 判断是否采用了合适的 IP 方案。在开展 COTS IP 评估前,首先确认拟使用的 COTS IP 是可获取的,具备一定的质量,有一定的数据支撑,并且能够满足相关的设计需求。将适航符合性工作完全寄托于不可控的供应商将给整个项目带来风险。

2) 判断 IP 是否采用了结构化方法。如果 COTS IP 是依照结构化方法设计的,那么应该评审 COTS IP 的设计生命周期过程和产生的数据,以便判别结构化方法和相关数据是否能够表明满足 DO-254 的目标。

3) IP 设计生命周期数据评审。应评审 IP 设计生命周期过程和相关数据,数据应当是可提交或可审查的。COTS IP 数据应当与 DO-254 定义的对应等级的数据相匹配。

4) 判断所有数据是否已经生成并可用。在生命周期审查完成后,申请人应评估为满足 DO-254 目标所需的所有必要数据是否可用。

5) "反向工程"缺失的生命周期数据。如果没有采用结构化方法,或者没有足够的可用数据,那么应该根据指定的 DAL,参考审定机构软件组(CAST)推荐的《审定项目中的反向工程》[9]执行反向工程活动以满足 DO-254 目标。虽然知识产权不是适航审查的关注点,但对于实际生产产品的申请人,需要在反向工程之前,对相关 COTS IP 的专利情况做出调查和分析,了解其专利布局情况、专利保护范围,明确侵权风险。

6) 判断生命周期数据是否充分。申请人应确保反向工程得到的生命周期数据满足 DO-254 目标,并将结果记录在审定数据包中。如果数据不能完全满足,可以选择服务历史数据来进一步提供置信。

7) 判断服务历史数据是否充分。在 DO-254 第 11.3 节讨论了服务历史的概念。如果 IP 具有相关的服务历史,则可以用来获得一些附加的审定置信,并弥补在所需数据的反向工程期间出现的任何缺漏。数据相关性证明以及数据获取来源这两个问题是审查中的关注点。

8) 服务历史数据记录。如果采纳了服务历史方法,那么相关的证据应该被整理和归档。

9) 实施架构缓解。检查架构缓解技术对于减轻保证级别上的任何缺陷是否必要,并检查其实现。申请人应始终考虑使用架构缓解技术作为其他方法的补充。在实施架构缓解时可能引发生命周期过程的设计迭代。

10) 判断是否满足设计保证目标。检查 COTS IP 相关数据对于设计保证目标的满足情况。如果满足,可进一步开展后续 COTS IP 集成、验证等工作;如果不满足,需要返回到概念设计阶段进一步考虑硬件架构或 COTS IP 的选型。

在开发 ARINC429-RS232 的 A 级数据转换电路时已实践了该评估过程。首先,选择了有一定质量保证并且 HDL 可见的软 IP;然后,依据需求设计电路架构,并评估该软 IP 适用性;接着,采用反向工程的方法补充缺失的生命周期数据,并进行集成;最后,对设计进行验证,并采用元素分析法对整个模块进行分析。

通过 COTS IP 的评估并反向了缺失数据,再进行模块设计时,能够使得整个设计有效地满足 DO-254 标准生命周期过程的目标,符合适航要求,证明该评估过

程切实有效。

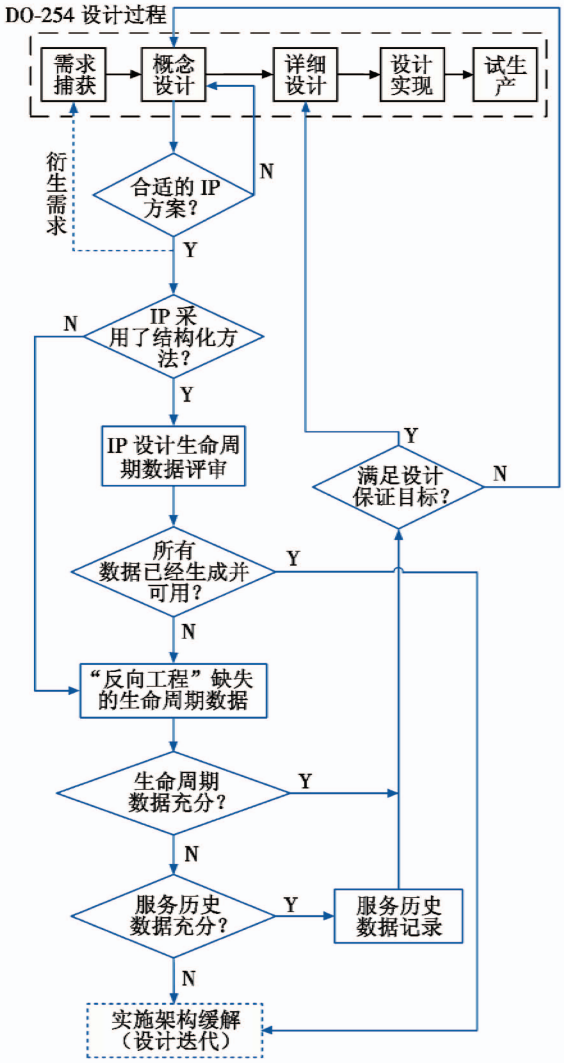

图 3　COTS IP 评估过程流程图

Fig. 3　Flow chart of COTS IP assessment process

4　COTS IP 审查要素

COTP IP 的审定过程涉及器件的选取、数据的评估、硬件设计保证方法的确定、确认、验证、高级验证方法等各方面，本文对各部分的审定关注点进行了归纳。

1）COTS IP 的选取。IP 在技术上应当适合于实现预期功能，并与目标机载电子硬件的设计保证等级相称；IP 供应商可以提供足够的信息，便于全面了解 IP 的功能、架构、运行模式和配置，并创建 COTS IP 的物理实现；提供的数据和文件应该满足一定的质量要求。

2）COTS IP 数据评估。应评估 COTS IP 供应商和在硬件中集成 COTS IP 所需的所有信息。COTS IP 应当是按照可信和可靠的过程进行验证的；提供可供借鉴的已知错误和限制。如适用，应评估产品服务历史数据。

3）确定硬件设计保证方法。申请人应在合格审定计划中说明使用 COTS IP 的硬件设计保证方法，重点关注 COTS IP 类型、格式，功能描述，为实现安全性目标而确定的设计保证方法，与设计集成和在硬件开发过程中的使用有关的过程，设计或验证工具的评估与鉴定。

4）确认。硬件需求应该包含与 COTS IP 支持功能相关的需求。分配的需求应与验证策略相称，包括：COTS IP 使用功能（包括参数、配置、选项）；未使用功能的停用或禁用；正确控制和使用 COTS IP；对于 A/B 级的 COTS IP，应保证确认的独立性。

5）验证。应在计划文件中说明验证策略，包括：COTS IP 本身的验证；在申请人完成如综合、布局布线设计步骤之后，对 COTS IP 进行验证；验证硬件集成的 COTS IP 功能。申请人应确保 COTS IP 作为整个硬件验证过程的一部分来验证，对于 A/B 级的 COTS IP，应保证验证的独立性。

6）高级验证方法。当开发 A/B 级机载电子硬件时，可以参考 DO-254 附录 B，选择元素分析法或安全特质分析法增加设计保证的置信并提供设计保证证明。

5　结束语

本文分析了 COTS IP 在民航机载产品中使用的风险，梳理了在审查 COTS IP 时适用的适航文件以及适航审定需求，给出了建议的符合性方法以及审查要素。建议申请人在表明符合性时，综合考虑使用反向工程、充分的测试与分析（如元素分析或安全特质分析）、架构缓解、产品服务历史等方法来表明符合性。

参 考 文 献

[1] 赵长啸，阎芳，张帆，等. 综合模块化航电系统可重用软件组件的适航审定要求分析[J]. 电光与控制，2016, 23(9):63-67.

[2] FAA Order 8110.105A. Simple and complex electronic hardware approval guidance[R]. Washington:FAA, 2008.

[3] CM-SWCEH-001. Development assurance of airborne electronic hardware[R]. Koln:EASA, 2018.

[4] RTCA SC-180, EUROCAE WG-46. Design assurance guidance for airborne electronic hardware: RTCA DO-254-2000[S]. Washington DC:RTCA Inc., 2000.

[5] Certification Authorities Software Team (CAST) Position Paper CAST-33. Compliance to RTCA DO-254/EUROCAE ED-80, “Design assurance guidance for airborne electronic hardware”, for COTS intellectual property used

（下转第 110 页）

time delay processes[J]. International Journal of Control, 2016, 89(3):579-593.

[4] OZYETKIN M M. A simple tuning method of fractional order $PI^{\lambda}PD^{\mu}$ controllers for time delay systems[J]. ISA Transactions, 2018, 74:1-11.

[5] DAS S, PAN I, DAS S, et al. Improved model reduction and tuning of fractional order $PI^{\lambda}D^{\mu}$ controllers for analytical rule extraction with genetic programming[J]. ISA Transactions, 2012, 51(2):237-261.

[6] GAO Z, CAI X W, ZHAI L R, et al. Stabilization criterion of fractional-order PD^{μ} controllers for interval fractional-order plants with one fractional-order term[C]//The 35th Chinese Control Conference, 2016:10424-10430.

[7] GAO Z. Robust stabilization criterion of fractional-order controllers for interval fractional-order plants[J]. Automatica, 2015, 61(C):9-17.

[8] 薛定宇. 控制系统计算机辅助设计——MATLAB 语言与应用[M]. 3 版. 北京:清华大学出版社,2012:121-133.

[9] WANG Y G, SHAO H H. PID auto-tuner based on sensitivity specification[J]. Chemical Engineering Research and Design, 2000, 78(2):312-316.

[10] 戚志东,卞慧娟,冷博阳,等. 基于序列二次规划法的新型分数阶 PI^{λ}-PD^{μ} 控制器设计[J]. 控制与决策, 2016, 31(12): 2275-2279.

[11] 周铁军,王昕,王振雷. 基于最大灵敏度指标的分数阶 PID 参数最优整定方法[J]. 控制工程,2014,21(6):1001-1005.

[12] 李大字,刘浪,靳其兵. 基于最大灵敏度的加热系统分数阶内模控制[J]. 控制与决策,2015,30(10):1899-1902.

[13] 赵志诚,李明杰,刘志远,等. 复杂系统的分数阶内模控制器设计[J]. 控制与决策,2015,30(3):531-535.

[14] 邓立为,宋申民,庞慧. 控制系统的分数阶建模及分数阶 $PI^{\lambda}D^{\mu}$ 控制器设计[J]. 电机与控制学报,2014,18(3):85-92.

[15] 林青松,肖培智,宋晓娜. 基于模型降阶的最优分数阶 PID 控制器设计[J]. 计算机测量与控制,2014,22(8):2482-2484.

[16] 王惠芳,赵志诚,张井岗. 一种高阶系统的分数阶 IMC-ID^{μ} 控制器设计[J]. 山东大学学报:工学版,2014,44(6):77-82.

(上接第 99 页)

in programmable logic devices and application specific integrated circuits[R/OL]. [2019-01-02]. https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/cast/cast_papers/media/cast-33.pdf.

[6] 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):17-20,24.

[7] 金志威. 机载 IP 软核的适航符合性验证方法研究[D]. 天津:中国民航大学,2013.

[8] 中华人民共和国工业和信息化部. IP 核质量评测:SJ/T 11478-2014[S]. 北京:中国标准出版社,2014.

[9] Certification Authorities Software Team (CAST) Position Paper CAST-18. Reverse engineering in certification projects[R/OL]. [2019-01-02]. https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/cast/cast_papers/media/cast-18.pdf.