doi:10.3969/j.issn.1671-637X.2016.03.016

机载高速互连网络适航审定要求分析

赵长啸[a], 阎 芳[a], 刘 锐[b], 王 鹏[a]
(中国民航大学,a.天津市民用航空器适航与维修重点实验室; b.安全科学与工程学院,天津 300300)

摘 要:机载网络互连技术由传统的以ARINC 429为代表的低速、单工总线向着高速、双向、网络化方向发展。互联体系结构的变化引入了新的安全性需求,现有的适航审定技术已无法对机载高速互连网络做出评判。分析了机载高速互连网络适航的审定要求,给出了机载高速互连网络在实际审定中的审定要素和评审要求。本研究可为我国解决机载高速互连网络的适航审定问题提供理论支撑。

关键词:机载网络;适航审定;安全性;体系结构
中图分类号:V243.1 **文献标志码**:A **文章编号**:1671-637X(2016)03-0067-05

Airworthiness Certification Requirements Analysis for High-Speed Airborne Network

ZHAO Chang-xiao[a], YAN Fang[a], LIU Rui[b], WANG Peng[a]
(Civil Aviation University of China, a. Civil Aircraft Airworthiness and Repair Key Laboratory of Tianjin; b. College of Safety Science and Engineering, Tianjin 300300, China)

Abstract: The airborne network interconnection technology is progressing from the low-speed, single-station bus, such as ARINC429, to high-speed, bidirectional, and networking way. The change of the network architecture introduces new safety requirements, and the existing airworthiness certification technology is unable to justify the airworthiness of the high-speed airborne network. In this paper, analysis is made to the airworthiness certification requirements of high-speed airborne interconnection network. The validation elements and review requests of the high-speed airborne interconnection network are given. This study can provide a theoretical basis for the authority to solve the certification problem of aircraft data network.

Key words: airborne interconnect network; airworthiness certification; safety; architecture

0 引言

航空电子网络互连技术又称机载网络技术,是航空电子综合化的关键支撑技术,是机载电子子系统、功能区之间的系统互连技术,是一个在航空工程领域苛刻的空间、时间限制条件下,对信息密集型航空电子子系统进行信息综合和功能综合的技术[1]。它是网络通信技术在航空领域的应用,本质上属于实时计算机网络技术。分立式航空电子系统基本上是各个子系统内部进行通信,子系统之间通信需求较少,往往通过加装点到点的互连电缆来完成少量的通信任务,如ARINC429[2];联合式航空电子系统要求子系统间共享显示输出和控制信息,低速总线网络MIL-STD-1553B[3]在这一应用背景下发展出来,能够满足各子系统之间的互连需求。航空电子系统的综合化和模块化使得航空电子子系统间需要进行大量的信息融合,高速数据总线(High-Speed Data Bus,HSDB)[4]采用光纤通道,提高了数据通信容量,用以满足处理部件之间以及系统之间的大量数据交换的需要。目前,综合模块化航空电子系统(Integrated Modular Avionics,IMA)[5]高度的信息综合特性,开放的系统结构,商用货架技术的应用都对航空电子网络提出了更高的要求,光纤通道(Fibre Channel,FC)网络和全双工交换式以太网(Avionics Full Duplex Switched Ethernet,AFDX)[6]被航空界采用,为IMA系统提供互连解决方案。

机载航电网络是航空电子系统的互连枢纽,航空电子系统在不同时代下的互连需求推动了机载航电网络

收稿日期:2015-04-30 **修回日期**:2015-05-11
基金项目:国家重点基础项目"九七三"计划(2014CB744902);中央高校基金(3122015C028)
作者简介:赵长啸(1989—),男,山东临清人,博士,讲师,研究方向为适航技术、机载网络和综合模块化航电。

的演变,逐渐从传统的低速总线向高速交换式网络方向演变。随着技术的进步和航空业对高性能航电系统的需求不断提高,机载高速度互连网络已成为新型航空器的必选系统,如AFDX网络已成功应用于波音787、空客A380以及我国的国产大飞机C919。机载高速互连网络作为飞机航电系统的重要组成部分关系着整机的飞行安全,也是局方适航审查中重点关注的部分,互连结构的变化和数据传输速率的提高,带来了信号完整性、电磁兼容、时钟漂移、故障增殖路径复杂等一系列新的安全性问题,现有的针对点对点总线的适航审定方法已无法解决机载高速互连网络带来的新问题。

目前,我国局方尚未颁布针对机载高速互连网络的适航审定指导文件。C919飞机已进入结构总装阶段,并预计2016年首飞,对其机载网络互连系统的审定问题将是我国局方目前面临的一个重大技术难题。本文针对机载高速互连网络的适航审定问题,结合已有的审定经验,从审定文件体系、审定要求以及适航审定要素等方面开展研究,为我国局方和工业方在机载高速互连网络的适航审定方面提供理论支持。

1 IMA系统研制、适航审定文件体系

针对机载高速互连网络的发展,世界各国的适航当局也纷纷寻求相应的审定方法解决方案,基于航空总线技术的发展情况,2003年2月国际组织Certification Authorities Software Team发布了CAST文档CAST-16《数据总线评估准则》,提出了适用于数据总线制造商、飞机型号申请人和审查局方的关于航空数据总线的评估准则要求。2006年,美国联邦航空管理局(FAA)根据CAST-16的内容,发布了咨询通告AC 20-156《航空数据总线保证》,用于对航空器及航空发动机制造商和设计者在设计使用航空数据总线时进行约束和指导;FAA AC25.1701-1《运输类飞机电气布线互连系统合格审定》将数据总线的传输线路当作一种EWIS部件,但未对其进行特别分析。

机载高速互连网络的适航审定文件体系主要包括局方文件、国际组织指导文件和具体总线协议的行业标准,如图1所示。

局方文件	指导文件	行业标准
FAA AC20-156	CAST-16	ARINC664
Aviation Databus Assurance	Databus Evaluation Criteria.position paper	ARINC818
		ISO11898
		…

图1 机载高速互连网络适航审定文件体系

Fig. 1 Airworthiness certification documentation for aircraft databus network

1.1 局方文件

FAA AC20-156是美国适航当局于2006年颁布的,针对高速、双向数据总线的适航审定的指导性文件,其发布依据为国际组织Certification Authorities Software Team发布的CAST-16文档。此咨询通告适用于采用高度综合复杂数据总线技术的型号审定或大改。

此AC为航空器和发动机审定申请人提供了一种数据总线技术研制、选择、集成的符合性方法,并获取符合相关要求的批准,其中涵盖了安全性、数据完整性、数据总线性能、软件和硬件保证、电磁兼容、验证和确认、构型管理、保障性等8个方面,申请人必须确定适用于所申请总线的方面,并严格执行。

1.2 行业标准

咨询通告对适航审定中需关注的问题给出了指导,实际民机设计中所使用的总线技术需依据具体的协议,当前民机中大规模应用的高速、双向总线协议包括以下几点。

1) ARINC664——AFDX,该协议基于商业以太网标准,采用目前已被广泛接受的IEEE802.3/IP/UDP协议,并增加了特殊的功能来保证带宽和服务质量,是专用于航空电子网络互连的"确定性网络",目前已应用于空客A380、波音B787和商飞C919。

2) ARINC818[7]——航空电子数字视频总线,是航电系统中针对高带宽、低延迟、非压缩数字视频传输制定的一种视频接口标准,该标准基于FC-AV(ANSI INCITS 356-2002)协议制定,映射于光纤通道(Fibre Channel),提供了在FC上实现标准化高速视频系统的手段,目前已应用于A400M和波音787等机型。

3) ISO 11898[8]——CAN(Controller Area Network)总线即控制器局域网是目前国际上应用最广泛的现场总线之一。CAN总线能有效支持分布式控制节点,配置灵活,价格相对低廉,适合作为飞机系统传感器和激励器进行数据采集和控制的通信总线,目前已在波音787飞机的控制面板中应用。

2 机载高速互连网络审定需求

根据FAA AC20-156,局方在对机载高速互连网络的审定过程中,需关注8个方面的问题,如图2所示。

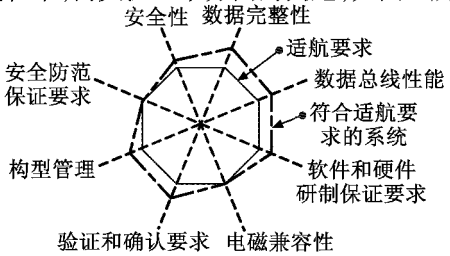

图2 机载高速互连网络适航审定要求

Fig. 2 Airworthiness certification requirement for aircraft databus network

实际总线网络只有全部符合这8项要求才能通过适航审定，取得相应适航证件。

2.1 安全性要求

航空器或航空发动机项目的申请人必须首先确定数据总线的设计对航空器或航空发动机的安全运行会有怎样的影响。申请人数据总线的设计和功能必须遵守CCAR §25.1301和§25.1309，§33.28，§33.75以及相关的咨询通告和管理程序。当数据总线安装到飞机或航空发动机上时，对其安全性的评估必须包括以下几点。

1）数据总线架构和实现。例如，可参考SAE ARP 4754A《民用航空器和系统研制指南》和SAE ARP4761《关于民用机载系统和设备的安全性评估过程实施的指南和方法》。

2）数据总线的可用性和可靠性应满足安全性要求。

3）数据总线架构和实现中的分区、保护要求。

4）故障检测、报告与管理方面的特点，例如使用冗余特性、节点丧失的检测、支持探明影子节点以及支持并联节点。

5）数据总线设计包括故障抑制、故障容限以及监控，使其不受主机系统内硬件和软件失效的影响。

6）共因（包括共模）和级联失效，对每架航空器，申请人必须进行共因故障分析以证明故障不在自己的数据总线故障分析范围内，共因分析包括区域安全分析、特殊风险分析和共模分析。

2.2 数据完整性要求

在各个LRU、节点、交换机、模块或其他实体之间传输的数据都必须保持精确并满足由数据总线所保障的航空器功能的数据完整性要求。通过数据总线架构中的错误探测、结果修正来确保数据完整性，评定数据总线系统包括下列方面：

1）预期数据传输每个字节的最大误码率；

2）为满足安全性、可用性和完整性要求，数据总线提供检测失效和错误的方法以及恢复方法；

3）数据总线负载分析，以保证能满足数据完整性要求；

4）缓冲上溢和下溢限制，以保证能满足数据完整性要求；

5）如适用，数据总线能够重新配置节点、数据总线架构以及网络（包括软硬件）以实现数据总线完整性要求；

6）实施双向错误检测，以解决数据总线完整性问题。

2.3 数据总线性能要求

申请人必须评估数据总线下列性能项：

1）数据总线的运行速度和信息顺序（时序和优先级）能保障操作上的安全性和完整性要求；

2）系统的协同工作能力，包括数据总线或网络的拓扑、部件间连接协议以及其他方面；

3）每束数据总线长度、短（截）线长度、电缆接头规格和限制；

4）数据总线的带宽容量；

5）数据总线容量的实际规范；

6）数据延迟和效率；

7）系统失效管理（包括失效/故障报告）以及在数据总线内部的失效影响。

2.4 软件和硬件研制保证要求

不管申请人提出的总线架构如何（同步或异步，单向或双向），机载系统、设备或发动机必须满足适用的软件和硬件的设计与研制保证指南。

每台复杂电子设备都必须满足有关的硬件设计保证要求。这些复杂电子设备的硬件设计保证必须满足由安全性评估所确定的失效状态类别和硬件设计保证等级。为确保符合硬件设计保证，要遵照咨询通告AC 20-152，RTCA文件RTCA/DO-254，或其他可接受的符合性方法。

为确保在数据总线架构内部工作的软件符合设计和研制保证，必须按AC20-115C，RTCA文件RTCA/DO-178C或其他可接受的符合性方法来开发软件，使之符合相应的设计保证等级。此外，还需要考虑DO-178C的补充文件，包括DO-330《软件工具鉴定考虑》、DO-331《基于模型的开发和验证》、DO-332《面向对象技术及相关技术》和DO-333《形式化验证》。

如果申请人使用工具来开发或检查数据总线的软件或硬件，需要对工具进行鉴定。鉴定研制软件和硬件的工具指南可以对应查阅RTCA/DO-178C，RTCA/DO-330和RTCA/DO-254。

2.5 电磁兼容性要求

为保证数据总线能良好工作，必须表明数据总线具有电磁兼容性。

数据总线以及总线部件电磁发射和电磁敏感性有潜在的较大差异。当数据总线要设计、选择或定型安装到飞机上时，需要考虑电磁发射和电磁敏感性的影响问题。当把存在电磁噪声的数据总线安装遍及航空器后，将难以再进行调整。

在评定数据总线的电磁兼容性时，要考虑全部数据总线系统，包括终端、硬件和安装。为了表明电磁发

射和敏感性的问题,不应把 RTCA/DO-160G 评估仅限于检测单台设备。

电磁发射同数据总线设计规范中的脉冲上升时间和恢复时间、数据总线速度和数据总线拓扑结构有关。数据总线拓扑结构也包括使用对称差模信号和变压器耦合连接,因此数据脉冲的形状(脉冲前缘和后缘)非常重要。数据总线的相互连接会大大影响电磁发射及敏感性。但是,屏蔽终端处装有优质接头、屏蔽双绞线比非屏蔽线具有更好的电磁特性。申请人应该指出并消除电磁敏感性的影响,该影响在采用冗余实现时会造成共模失效。

2.6 验证和确认要求

1) 确认航空器或航空发动机项目的数据总线需求。

2) 按照数据总线支持的每项关键功能相应的保证等级来评估数据总线是否符合 RTCA/DO-160G 的要求。通常,验证工作在航空器装配过程中已经完成,所以电磁兼容和闪电鉴定是数据总线技术尤为关注的。电磁试验和确认可以随数据总线的架构而有所变化。

3) 如2.4 节所述,按 RTCA/DO-178C 和 RTCA/DO-254 对数据总线完成相应的验证。

4) 完成数据总线集成功能试验,以确保其满足预期的功能。

5) 验证和确认数据总线的运行、架构及性能要求。一种可接受的方法是使用一架飞机或数据总线模拟器,该模拟器要能实现被试验系统所允许的最大吞吐率。

6) 如果支持降级模式运行能力,在降级模式测试数据总线以确保可以接受的性能。

7) 如果申请人使用测试台来验证数据总线的性能,还必须完成配线可接受性测试,通过记录测试方法或程序以确定线束的铺设是正确的。在飞机上初始装配时,以及以后的维修工作都必须使用这些程序。当安装获得批准后要进行更改时,需要进行更改影响分析,以确定配线可接受性测试或程序是否需重新执行。

2.7 构型管理要求

由于新的数据总线技术不断出现,具体到每架飞机的数据总线构型可能是唯一的,又由于这些唯一性,更改数据总线的构型可能对数据总线的信息交换、数据冲突率及可靠性造成负面影响。因此,就数据总线安装而言,制造商必须为数据总线规定一个构型管理方法。这些安装还要求维修人员和安装人员在保持和重新规定该数据总线构型的适航性时,使用制造商批准的数据总线构型和工具。申请人在开发数据总线时,要考虑下列系统构型管理项目。

1) 当航空器或航空发动机设计中集成了数据总线后,应考虑整个系统,保证有若干构型管理机制会负责数据总线更改后的持续运行安全和构型管理。在合格审定要求和使用中的维修工作中必须保证能够添加额外的数据总线节点和应用。

2) 必须在合格审定期间,从设计到生产、维修,依靠申请人自己规定的标准和文档程序来建立和保持对数据总线的构型管理。构型管理应该考虑每种安装的数据总线和选件,同时为了更改以前已批准的构型,应注意可能还需要额外的 CAAC 合格审定。

3) 制订可用的规范标准文件。申请人最少需要编写数据总线物理和逻辑规范。物理规范要求例如传输介质、接头、终端、最大节点数目以及驱动距离。逻辑规范例如信息包的定义。

4) 提供支持研制和运行数据总线的文件,例如,接口定义文件、用户指南及安装人员指南。

5) 未来总线扩展的策略、计划或进程,以及潜在变化都将影响系统的完好性和安全性。

2.8 安全防范保证要求

当代许多数据总线都提出了潜在的安全风险问题,这在传统网络系统里是常见的。访问安全和数据保护是申请人应该面对的两个方面。

1) 访问安全。当机载系统通过数据总线或网络与外部世界相联系时,很容易受到潜在的恶意攻击,例如软件病毒,应评估每束数据总线是否会遇到这种潜在的风险。针对这一风险采取相应的安全技术和控制方法,从而防止侵入机载软件。

2) 信息和数据保护。使用网络或现代数据总线时,申请人必须保护在机载系统里使用和存储的关键信息。

3 机载高速数据总线网络审定要素和评审要求

在实际取证过程中,机载高速数据总线网络的审定过程涉及对网络的物理层、数据链路层、网络层、传输层以及应用层各方面,本文以检查单的形式对各部分的审定关注点进行了归纳,如表1 所示。

表 1　机载高速数据总线网络适航评审要素及审定要求

Table 1　Airworthiness review and assessment requirements for aircraft databus network

序号	协议层次	适航评审要素及审定要求
1	物理层	1）判断网络规范和可用的组件是否满足最新版本 DO-160 关于航空环境的要求以及其他强制环境要求。 2）比特误码率应当在最坏的应用环境下获得。 3）确保数据网络选用的电气部件可以获得硬件故障率(永久和暂时)以及其他相关性能数据,以便于航空电子设计人员进行必要的 FMEA 和故障树的计算。协议应当定义得足够完善,以便确定任意或所有组件的故障对协议的影响。 4）有足够的保护措施防止电气故障传播。 5）数据网络应当有相应的措施或设计规则来保证它可以和任何规模的网络可靠地协同工作,应当明确设定最大尺寸。
2	数据链路层	1）无论出现任何故障,MAC 子层协议必须提供一定的信息传递时间边界。 2）电磁兼容性测试(如 DO-160 19-22 章)在实际的数据线编码(如曼彻斯特码、8h/10b 编码)、最坏情况下的网络数据量、信息大小、位(bit)率、脉冲宽度和消息的重复传输速率下完成。 3）信息格式必须确保在客户端只接收完整的、正确同步的,在限定时间内恢复的消息。 4）在消息传递时数据链路层必须使用错误检测机制保证没有未被发现的错误。
3	网络层,传输层	1）在网络部件失效的场景下,应有相应机制确保正确的转发、路由或转换。 2）中级阶段(如中继器、网关、路由器、交换机)必须保证足够的可用性和完整性,此外相对于其他重复的中间阶段有足够的逻辑和物理独立性以确保正确的操作。 3）网络拓扑结构和组件配置数据必须与应用程序的容错能力和性能要求相当。应考虑表的生成、装载、操作过程中的错误、运行时对环境的影响(如辐射的影响)和维护活动。 4）组件和网络的集成、启动和恢复必须在有限的时间内进行,要求考虑可靠性要求、环境和部署的制约、与不同的系统和应用程序间的交互(如应用级时序影响和电源架构影响)。 5）如果同步是必需的,同步机制应当证明在所有定义的运行场景下都能够工作正常。 6）任何诊断、检测、或系统级协议机制必须证明故障假设正确,并考虑诊断活动的影响。 7）客户端不能对网络操作产生不利影响。 8）应当确认各种机制可以在所有故障情况下正常工作。
4	应用层	1）主机的应用程序接口(包括网关)协议必须按照所支持的服务类别提供承诺的优先级、延迟以及阻止信息丢失的措施。 2）任何应用层冗余的支持必须完全符合冗余管理机制的要求。 3）如果要求网络提供健壮性分区保证,应确定怎么证实要求的分区。 4）如果提供时钟标记和时钟中断服务,应当充分评估其可靠性和健壮性。

4　结论

本文首先分析了现有的针对机载高速互连网络系统的研制及审定文件体系,梳理了各适用文件的内容及关注点。根据适航审定要求,对 FAA 咨询通告中关注的 8 个方面进行了分析总结,最后从实际机载网络审查的技术角度给出了针对总线协议各层次的审定要素和评审要求。本文的研究对我国工业方和局方开展机载高速互连网络的设计和适航审查工作具有一定的理论支持作用。

参考文献

[1] 熊华钢,王中华. 先进航空电子综合技术[M]. 北京:国防工业出版社,2009. (XIONG H G, WANG Z H. Advanced integrated avionics technology [M]. Beijing: National Defense Industry Press, 2009.)

[2] ZHI M D, JUN Z. Design and application of the communication-card of the bus ARINC429 based on HS3282[J]. Computer Automated Measurement & Control, 2004(5): 76-79.

[3] BURTON P I. Field bus based on MIL-STD-1553B: proposal to ISA-SP-50[J]. ERA Technology Ltd. ISA/SP50-1988-148, 1988: 1-125.

[4] ZHANG H N, WANG S H, DIAO X X, et al. Test case generating for integrated modular avionics software health monitoring[J]. Applied Mechanics and Materials, 2014, 494: 873-880.

[5] SINGH G, PATRICK A, RAJPOOT L. A clustering based intrusion detection system for storage area network[J]. International Journal of Computer Applications, 2014, 88: 975-979.

[6] GUTIERREZ J J, PALENCIA J C, HARBOUR M G. Holistic schedulability analysis for multipacket messages in AFDX networks[J]. Real-Time Systems, 2013, 50(2): 230-269.

[7] BISSON K. Arinc-818 testing for avionics applications[C]// Autotestcon, 2007 IEEE, Baltimore, MD. 2007: 321-326.

[8] LAWRENZ. W. CAN system engineering[M]. Berlin: Springer, 2013.