2018 年第 3 期　总 130 期
ISSN 1674-9804　CN 31-1614/V

DOI: 10.19416/j.cnki.1674-9804.2018.03.011

民机电传飞控系统故障检测与容错技术

Fault Detection and Fault-Tolerance Technology in Civil Aircraft Electrical Flight Control System

司马骏 / SIMA Jun
（上海飞机设计研究院，上海 201210）
（Shanghai Aircraft Design and Research Institute, Shanghai 201210, China）

摘　要：
现代民机广泛采用数字式电传飞控系统，它有利于飞机减重、飞行品质改善、飞机维护性改善等。民机电传飞控系统需满足严格的安全性与可用性要求，保证飞机取证与运营可靠性。故障检测与容错技术是实现高度安全可靠电传飞控系统的关键。该文阐述了已应用于现代民机的故障检测与容错技术，重点介绍了波音、空客公司故障检测与容错技术应用于民机设计的成功案例，对未来民机容错技术发展进行了探讨与展望。
关键词：电传飞控系统；故障检测；容错技术；余度设计
中图分类号：V227^{+}.83　　**文献标识码：**A　　**OSID：**

[**Abstract**] Electrical flight control system (EFCS) has been widely applied in modern civil aircraft and brings benefits such as weight saving, improvement of flying qualities and improved maintenance strategies. EFCS is designed to meet very stringent requirements in terms of safety and availability, in order to satisfy aircraft certification and airline reliability. Fault detection and fault-tolerance technology are the key to realize highly dependable EFCS. This paper deals with the industrial practices on fault detection and fault-tolerance for civil aircraft, especially the state of the art and experiences from Airbus and Boeing Company. Several detail examples of fault detection and fault-tolerance have been introduced. Finally, future trends and challenges for fault-tolerance technology are presented.
[**Keywords**] electrical flight control system; fault detection; fault-tolerance; redundancy design

0　引言

自 20 世纪 60 年代主动控制技术与随控布局设计思想提出以来，电传飞控系统（Electrical Flight Control System，以下简称 EFCS）开始随之发展，EFCS 使用数字式计算机与电信号通信，为飞机减重、飞行品质改善、飞机维护性改善等作出显著贡献。民机数字式 EFCS 最早应用于空客公司 A310（1982 年），仅用于控制扰流板、缝翼和襟翼。随后空客公司在 A320（1987 年）机型中首次应用了全权限 EFCS。波音公司在波音 777 机型上首次使用 EFCS，并于 1995 年成功取证[1]。中国首架按照国际标准设计的支线客机 ARJ 21 采用了 EFCS。EFCS 发展至今，大量先进的设计技术被不断提出并成功应用于民机研制中，以 A380 为代表的先进民机在故障检测与容错技术方面有了新的突破，但受限于计算机处理能力，一些复杂的非线性实时算法难以应用。

随着 EFCS 对飞机性能改善的要求不断提高，其系统架构的复杂性也随之增长，系统设计中需考虑的故障模式也成倍增多。EFCS 是关键的机载系统，需满足严格的安全性与可靠性要求，保证飞机取证与运营可靠。Federal Aviation Administration（简称 FAA）、European Aviation Safety Association（简称 EASA）、Civil Aviation Administration of China（简称 CAAC）适航规章（如 CCAR 25.1309（b））要求飞机系统设计需保证发生妨碍飞机继续安全飞行与着陆的失效状态概率是极不可能的（概率小于 10^{-9}/飞

行小时)。

故障检测与容错技术是实现高度安全可靠电传飞控系统的关键,系统容错能力是指在发生故障情况下,系统维持其正常功能或完成指定任务的能力[2]。现代民机容错系统设计主要是依赖于余度设计,如采用多套相互冗余的计算机、传感器、作动器,以保证系统发生一次故障或二次故障后仍能安全执行任务。故障检测主要通过冗余设备之间的交叉比较、一致性检查、信号表决等技术实现,实时监控系统的工作状态与故障状态。本文重点介绍容错系统设计中的余度技术与故障检测技术。

1　容错系统设计

民机 EFCS 属于安全性级别很高的系统,系统设计要求发生任何导致飞机灾难级失效的故障必须是极不可能的(故障概率小于 10^{-9}/飞行小时),典型的灾难级故障包括舵面极偏(如方向舵或水平安定面)、舵面振荡超过飞机结构限制、单发失效后丧失舵面控制等[3]。波音、空客公司在民用飞机设计领域走在世界前沿,为保证民机 EFCS 符合严格的适航取证要求,其飞机设计需遵循一套完整可靠的设计流程与方法,如空客公司针对飞机容错设计提出了一套“黄金原则”[1]。

EFCS 设计目标为高度安全可靠的容错系统,系统设计应考虑以下因素:

1)严格的设计流程

系统设计应遵循严格的研制流程与行业规范,如 ARP 4754A 给出了复杂飞机系统的设计指南,软件设计应保证满足 DO-178 规范,硬件设计应满足 DO-254 规范。这些设计指南与行业规范并不考虑系统具体的功能设计,而是重点规定了系统、软硬件的研制过程,如研制计划、验证方法、构型管理、质量保证等。

2)安全性分析

安全性分析是基于系统架构评估系统功能失效的影响,并采用故障树的分析方法给出底层故障事件的发生概率与失效影响。系统安全性分析应评估对系统存在重大影响的故障事件,包括单点故障、潜在故障、LRU 故障组合等。安全性分析的结果会指导系统架构优化(如增加余度或监控器),从而保证系统的容错能力满足适航条款中的安全性要求。

3)余度设计

余度设计主要是采用多余度配置满足系统安全性与可用性要求,如配置多余度的飞控计算机(A330/A340 采用了 5 台,A380 采用了 6 台,波音 777 采用了3 台),为舵面分配不同的驱动源(A320/A340 布置了三套液压源、A380 布置了两套液压源与两套电源)[4-5]。余度设计还需考虑共因故障(如共模故障、发动机转子爆破等)的影响,关键的冗余设备需采用非相似设计方法,且冗余设备的功能设计应尽量独立,安装布置应适当隔离。

4)故障检测与重构

EFCS 故障检测主要是通过实时监控器与设备自检测(Built-In Test,简称 BIT)完成,需监控的系统状态包括驾驶舱操纵器件传感器位置、舵面作动器状态、计算机指令完整性等。当计算机探测到故障后,系统应具备自动的故障管理能力,重构系统硬件功能或软件功能。如对于采用双余度作动器配置的飞机舵面,当单个作动器故障后,系统可继续使用另一作动器执行舵面操纵功能。

2　余度设计

余度技术是指采用多套系统/设备执行同一项工作任务。民机余度设计主要依赖于硬件冗余,如采用多套计算机进行控制指令计算与监控,同一块舵面采用多套作动器进行控制等,互为冗余的设备具备同等的功能和任务执行能力。20 世纪 90 年代起,出现了大量关于解析余度的研究,与硬件余度不同,解析余度是一种基于模型的余度设计方法,通过在软件中构建与硬件具备相同输出的数学模型,对硬件输出的物理信号进行比较监控。

为了避免共模故障对关键冗余设备的影响,现代民机广泛采用了非相似的余度设计技术,即相互冗余的设备通过不同的研发团队以不同设计方法与工具实现相同的功能。此外,为了避免共因故障(如发动机转子爆破、区域性火灾)同时影响到多套互为冗余的设备,需考虑冗余设备之间的隔离。

2.1 硬件冗余

EFCS 的主要任务是执行飞行控制律计算,并驱动舵面按期望的指令运动。图 1 给出典型的 EFCS 控制回路原理图,飞控计算机会同时接收到驾驶员操纵输入和飞机状态(如大气数据、姿态角速率等)反馈,计算机执行控制律运算并向作动器发出控制指令,作动器从而驱动飞机舵面运动。现代民机设

计中为了保证飞机控制安全性与可用性的高指标要求，会对控制回路中关键的传感器、计算机、作动器采用多余度硬件配置，同时还需相应配置多套电源或液压源保证系统正常工作。

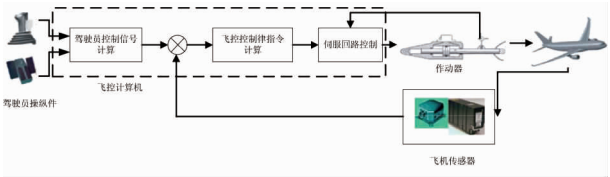

图 1　电传飞控系统控制原理图

图 2 给出了空客 A340 各操纵舵面上作动器的余度配置图，对于非关键的控制舵面如扰流板，每个舵面仅配置一个作动器；对于关键的控制舵面如副翼、升降舵、方向舵和水平安定面，每块舵面配置了两个或三个作动器用于舵面控制。A340 飞机配置了 3 套液压源用于驱动作动器运动，每个作动器都对应了一套液压源驱动，图 2 中 H1、H2、H3 分别代表了三套独立的液压源。此外，A340 飞机配置了 5 台飞控计算机，每个作动器都对应了一台或两台飞控计算机控制。图 2 中 P1、P2、P3 代表三台主计算机，S1、S2 代表两台次级计算机。多余度硬件配置的目标是当组成系统某部分设备出现故障后，系统可通过冗余信号的比较监控探测到故障源，并进行故障重构，保证系统仍能继续安全执行任务。

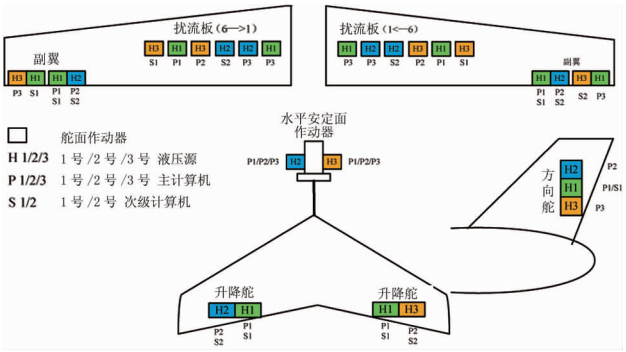

图 2　A340 舵面余度配置

2.2 解析冗余

传统的故障检测是基于冗余的硬件传感器进行交叉检查，而解析冗余是一种基于模型的设计方法，通过构建与真实硬件传感器功能相当的数学模型，实时计算期望的输出信号，并与真实传感器的物理信号进行比较监控，以检测系统故障。相比于基于硬件冗余的故障检测方法，解析冗余对系统故障的覆盖率更广，且不依赖于额外的硬件来实现故障检测，有利于飞机减重、硬件维护等。由于解析冗余通常依赖于实时、非线性的数学算法，如非线性滤波、矩阵转换等，解析冗余应用对计算机的运算处理能力提出了很大的挑战，合理简化数学模型以适应计算机处理能力是解析冗余工程应用的关键。

现代民机设计中仍然主要采用硬件冗余，解析冗余技术应用相对较少，以空客 A380 为代表的先进民机 EFCS 设计中已经成功应用了解析冗余技术。A380 由于在舵面上使用了新型电动舵机（Electro-Hydraulic Actuator，简称 EHA），传统的基于硬件冗余的故障检测方法不能完全覆盖 EHA 的各类故障源，使用解析冗余的方法不但可以减少硬件设计，同时也能保证覆盖 EHA 各类故障源[3]。图 3 给出了解析冗余在 A380 上的应用案例，A380 使用解析冗余方法执行舵面振荡故障的检测。飞控计算机输出控制律指令驱动相应作动器及舵面运动，同时计算机中构建了作动器与舵面运动模型，模型根据控制律指令实时运算并输出舵面期望的运动位置，飞控计算机中对模型输出的期望位置与舵面传感器反馈的实际位置进行比较监控，当舵面出现超过监控器容忍范围的振荡运动后，则系统会进行故障重构，切断故障作动器使用正常的作动器驱动舵面继续正常运动。

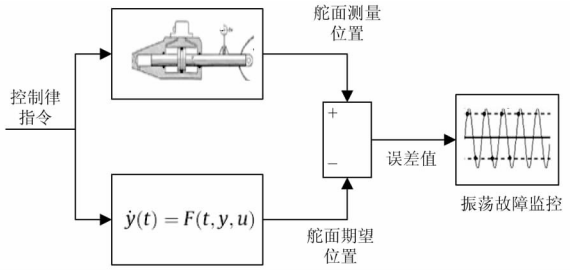

图 3　A380 解析冗余应用实例

2.3 非相似冗余

适航条款要求单点故障不能导致灾难级失效状态，EFCS 设计中需避免关键部件如飞控计算机存在共模故障（单点故障），以满足适航条款要求。现代飞机 EFCS 关键部件特别是飞控计算机广泛采用非相似冗余设计方法，从而避免冗余部件之间存在共模故障，典型的共模故障包括需求解释错误、硬件电路故障、软件编码错误、生产瑕疵等。非相似设计是为了保证互为冗余的关键部件之间的独立性，开展非相似冗余设计主要依赖于不同的研发团队进行底层需求开发，并采用非相似的工具方法实现具有相

同功能的软硬件。

以空客、波音为代表的民机先进 EFCS 中,关键冗余部件都采用了非相似设计。空客的主要机型都设计了两种类型的飞控计算机:主计算机和次级计算机。两种计算机采用了不同的硬件设计和软件设计,次级计算机相对主计算机设计更简单,飞控系统使用两种计算机进行故障重构。波音公司主要机型中通常采用三台主计算机,每台主计算机由三个非相似的处理器执行计算。非相似设计同样应用于多余度的作动器中,A380 中使用两种类型的作动器:传统的液压作动器和新型的电动作动器。

2.4 余度隔离

除了共模故障外,EFCS 设计中还需考虑共因因素(如发动机转子爆破、鸟撞、区域性风险、闪电环境、结构损坏等)对冗余设备的影响,冗余设备需进行隔离,包括功能隔离和安装隔离。

功能隔离要求执行相同功能的冗余设备之间尽量使用不同的信号源、电源、液压源等。以图 2 给出的 A340 配置升降舵控制为例,两块升降舵配置了 4 个作动器,4 个作动器由 3 套独立的液压源供压和两台主计算机进行控制,同一块升降舵舵面上的作动器分别使用了不同的液压源和计算机指令。当任意一个作动器失效或计算机失效后,两块升降舵舵面都仍然保证可控。

安装隔离要求冗余设备的物理安装位置应在飞机各个区域合理布置,如飞控计算机应布置在不同的电子设备舱,液压管路、电源线路、信号总线等应布置在不同的机身区域。当发生如发动机转子爆破时,转子碰撞区域不会同时影响到所有冗余的管路、线缆或设备,从而保证飞机仍然安全可控。

3　故障检测与重构

3.1 故障检测

EFCS 故障检测主要通过实时监控器与设备自检测(BIT)完成。BIT 通常包括 PBIT(上电自检测,设备上电自动执行)和 IBIT(启动自检测,通过外部激励执行)。现代民机电传飞控系统监控器类型主要包括:

1)冗余传感器的监控与表决

EFCS 常用的冗余传感器包括驾驶员指令传感器、速率陀螺和加速度传感器、大气数据传感器、迎角传感器和舵面位置传感器。冗余传感器信号的监控通常需设计两个参数:监控门限与故障确认时间。当冗余信号误差值大于监控门限,且持续时间超过故障确认时间后,监控器则标记相应的信号为故障信号。监控器设计应具备足够的鲁棒性与安全性,避免由于门限值过小导致虚警,也要避免由于门限值过大导致低于门限的错误信号对飞机控制产生安全性影响。此外,解析冗余技术已应用于先进机型,但应用范围有限,图 3 给出了 A380 使用解析冗余执行作动器振荡故障监控的实例。

2)飞控计算机指令完整性监控

飞控计算机的主要任务是执行控制律运算并输出作动器控制指令,飞控计算机指令完整性需要满足错误概率小于 10^{-9} 要求。民机飞控计算机广泛采用非相似的 COM/MON(指令通道/监控通道)架构,COM 与 MON 通道采用非相似设计,使用不同处理器或编程语言实现。此外,COM 与 MON 两个通道相互独立执行特定的任务,COM 通道主要执行包括控制律的各项功能运算,MON 通道主要执行系统监控功能,COM 与 MON 会同时运算控制律指令并进行比较监控。仅当 COM 与 MON 通道运算的控制律指令一致时,飞控计算机输出有效的作动器控制指令。

3)单个传感器有效性监控

飞控计算机执行冗余传感器比较监控之前,会对单个传感器的有效性进行检查,如传感器输出信号是否在有效范围内、设备供电是否正常、线路是否正常等。仅当单个传感器信号标记为有效时才会进入下一层级的冗余传感器比较监控。

4)总线信号完整性监控

民机 EFCS 内部设备之间的通信、与交联系统的通信通常采用不同的总线信号,如 ARINC629、ARINC429 总线等。为了保证总线信号发送和传输过程中的完整性,飞控计算机通常会采用 CRC(Cyclic Redundancy Check)校验、信号刷新率检查等方式进行监控。

图 4 给出了应用于 EFCS 的 3 余度大气数据与惯导设备(Air Data Inertial Reference Units,简称 ADIRU)监控与表决方法。ADIRU 将飞机空速管、速率陀螺等传感器信号转换为数字信号发送给飞控计算机,每台飞控计算机同时接收到 3 个 ADIRU 发出的飞机参数(如校正空速、飞机角速率、飞机加速度),并对所有 3 余度的飞机参数进行比较监控和表决,表决后生成唯一的飞机参数用于控制律计算。典型的 3 余度信号监控与表决方法如下:

1）单个信号有效性检查：检查 3 个信号源均是有效（如检查总线数据包的 CRC、信号数值的有效范围），无效的信号不参与比较监控与表决；

2）比较监控：从 3 个信号中按数值大小选择中值信号，将剩余的两个信号与中值信号进行差值比较，任意一个信号与中值信号的误差值大于监控门限且持续时间超过故障确认时间后，则标记该信号失效，失效信号不参与表决；

3）表决计算：常用的表决计算为均值算法，即使用通过比较监控的有效信号求平均值。表决后的信号用于控制律计算。

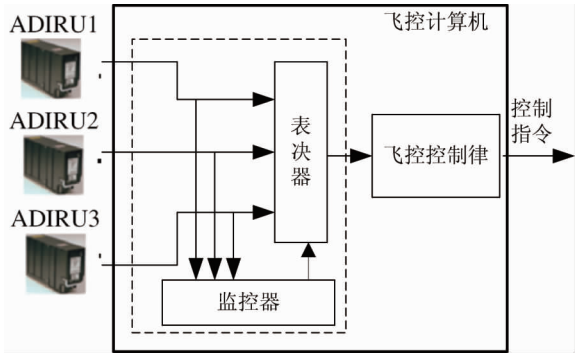

图 4　冗余传感器监控与表决

3.2 故障重构

故障检测是系统重构的前提，系统检测到故障后，会自动进行故障管理与重构，故障重构能力也是系统容错能力的重要体现。电传飞控系统故障重构可分为两个层级的重构：硬件重构和控制律重构。

当系统丧失有限余度的传感器或作动器后，系统具备能力继续使用剩余的传感器或作动器继续执行任务，系统主要控制功能不受影响。图 5 给出了系统硬件重构的示例，同一块升降舵舵面上配置了两个液压作动器，两个作动器分别使用两台计算机 P1、P2 控制，且使用不同的液压源驱动。正常状态下，两个作动器为主-备（Active-Standby）工作状态，P1 控制的为主动作动器，P2 控制的备用作动器。当主作动器故障、主作动器液压源 H1 故障、P1 计算机任意一个发生故障后，P1 控制的作动器会被切断变为失效状态，不能继续执行升降舵控制。P2 计算机探测到 P1 控制作动器失效后，会设置 P2 控制的作动器为主动状态，控制升降舵运动，从而保证升降舵控制功能不受影响。多余度硬件配置保证了系统的重构能力与可靠性。

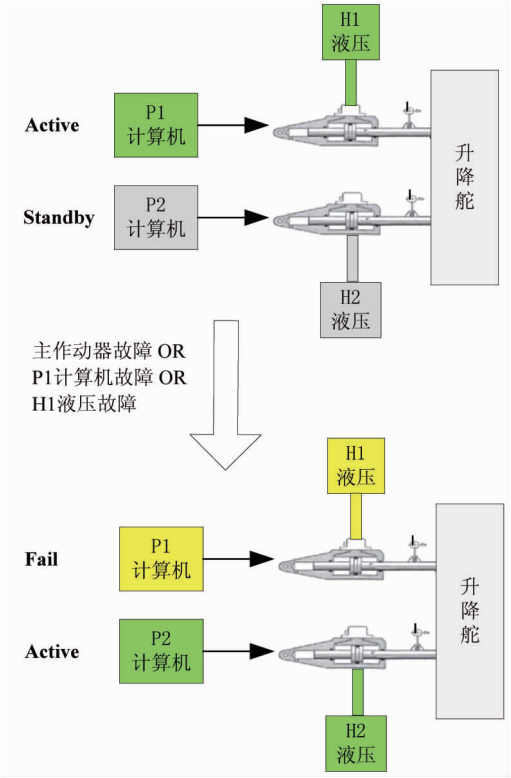

图 5　系统硬件重构实例

EFCS 控制律具备控制增稳、包线保护、失速告警等功能，执行完整控制律计算需要获取如校正空速、迎角、角速率等飞机参数。现代民机控制律设计通常包括多套控制律，图 6 给出了控制律重构的示意图。正常状态下，系统可执行三轴控制、包线保护等完整的控制功能，定义为“正常控制律”；当系统出现特定故障，如丧失迎角信号和校正空速信号后，系统会降级为“次级控制律”，次级控制律仍然保证飞机三轴控制能力，但包线保护等控制功能将不具备；当系统出现更为严酷的故障，如多台主计算机全

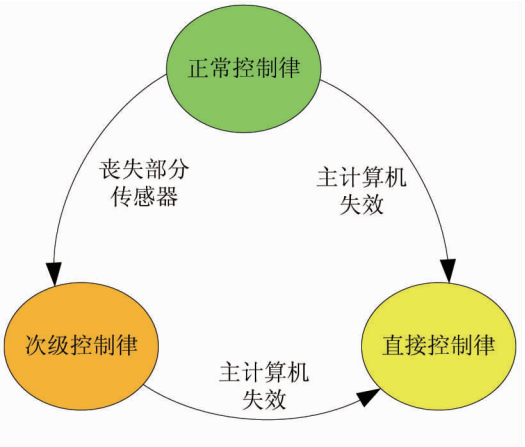

图 6　控制律重构示意图

部丧失,系统会降级为“直接控制律”,直接控制律通过架构简单的次级计算机执行,提供基本的舵面控制,控制品质较差。

4　容错技术发展方向

民机 EFCS 研制是一项复杂的系统工程,涉及到大量设备与交联系统的集成设计。数十年来 EFCS 发展表明,改进系统故障检测与容错技术能有效地帮助改善飞机控制品质、飞机结构设计(结构减重)、飞机运营成本(如飞机维护)等。国外学者研究了许多先进的容错方法,如飞行参数预计、基于模型的故障检测(如解析冗余)等[6],这些方法不依赖于额外的传感器硬件,而是通过软件算法构建虚拟的传感器,用于系统故障检测与重构。此外,软件相比于硬件更加容易控制与监控。

以解析冗余为代表的先进方法对飞控计算机的实时运算能力要求很高,空客 A340、A380 等机型虽然已经在个别监控器设计中应用了解析冗余技术,但都是采用简化建模与开环计算方法,牺牲了模型计算精度。如何在未来民机设计中广泛应用这些先进的容错技术需要解决以下问题:

1)在保证算法性能足够的前提下,尽量优化或简化算法,降低对飞控计算机处理能力的要求,以及减少对变量参数的要求,使算法更加接近工程应用;

2)现代民机使用的计算机处理能力相比于行业水平偏低,使用性能更高的计算机是未来的应用方向,但前提是先进计算机在工业领域已经广泛应用且证明具备很强的鲁棒性和可靠性。

5　结论

本文介绍了国外先进民机 EFCS 容错技术的成功经验,详细阐述了国外民机在余度设计、故障检测等方面的发展与应用。大型民用客机研制是高度复杂的系统工程,以波音、空客为代表的国外民机工业经过几十年的发展积累了成熟研制流程与方法,国内民机事业刚刚步入正轨,借鉴和学习国外先进技术与经验有助于推动国内民机的快速发展。

参考文献:

[1] GOUPIL P. AIRBUS state of the art and practices on FDI and FTC in flight control system [J]. Control Engineering Practice,2011,19 (6) :524-539.

[2] SGHAIRI M,BONNEVAL A D, CROUZET Y, et al. Challenges in building fault-tolerant flight control system for a civil aircraft [J]. IAENG International Journal of Computer Science, 2008,35 (4) :16-36.

[3] GOUPIL P. Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy [J]. Control Engineering Practice, 2010, 18 (9) :1110-1119.

[4] YEH Y C. Design considerations in Boeing 777 fly-by-wire computers [C]// IEEE International Symposium on High-assurance Systems Engineering. [S. l.]: IEEE Computer Society, 1998:64.

[5] BRIÈRE D, TRAVERSE P. AIRBUS A320/A330/A340 electrical flight controls-A family of fault-tolerant systems [C]// IEEE International Symposium on Fault-tolerant Computing. Toulouse:IEEE,1993: 616-623.

[6] GOUPIL P, BOADA-BAUXELL J, MARCOS A, et al. AIRBUS efforts towards advanced real-time fault diagnosis and fault tolerant control [C]//IFAC 19th World Congress. Cape Town: The International Federation of Automatic Control,2014: 3471-3476.

[7] YEH Y C. Dependability of the 777 primary flight control system [J]. Proc Dependable Computing for Critical Applications USA, 1998:3-17.

[8] VANEK B,SZABÓZ, EDELMAYER A,BOKOR J. Fault detection of electrical flight control system actuators using parameter dependent estimation [C]// IFAC 8th Symposium on Fault Detection. Mexico: The International Federation of Automatic Control,2012: 1358-1363.

[9] SAE International Aerospace Recommended Practice. Guidelines for development of civil aircraft and systems :SAE ARP4754A[S]. America: The Engineering Society For Advancing Mobility Land Sea Air and Space, 2010.

[10] SAE International Aerospace Recommended Practice. Guidelines and methods for the safety assessment process on airborne systems and equipments: SAE ARP4761[S]. America: The Engineering Society For Advancing Mobility Land Sea Air and Space, 1996.

[11] 中国民用航空总局. 中国民用航空规章第 25 部:运输类飞机适航标准[S]. 中国:中国民用航空局,2011.

[12] 吴森堂,费玉华. 飞行控制系统[M]. 北京:北京航空航天大学出版社,2013.

[13] 王占林,安敬军,裘丽华,等. 飞行容错控制系统中的关键技术[J]. 宇航学报,1995(1):64-68.

作者简介

司马骏　男,硕士,助理工程师。主要研究方向:飞行控制系统设计。E-mail: simajun@comac.cc