第 38 卷 第 11 期
2016 年 11 月

系统工程与电子技术
Systems Engineering and Electronics

Vol. 38 No. 11
November 2016

文章编号:1001-506X(2016)11-2586-12

网址:www.sys-ele.com

无人机容错飞行控制计算机体系结构研究

吕迅竑,姜 斌,陈 欣,齐瑞云

(南京航空航天大学自动化学院,江苏 南京 210016)

摘 要:高性能无人机对飞行控制计算机提出了高可靠性要求,使用余度容错飞控计算机是提高安全可靠性的重要途径之一。对容错飞控计算机安全可靠性、实时性、维护性等设计要求进行研究,分析了无人机容错飞控计算机的设计要求特点;阐述了典型军用、民用有人机以及无人机容错飞控计算机的体系结构及关键余度管理策略,总结了无人机容错飞控计算机体系结构特点及发展方向。根据上述研究结果,提出一种基于 FlexRay 总线的相似三模余分布式容错飞控计算机体系结构,FlexRay 总线既是单通道飞控计算机的内部总线,也是多通道飞控计算机的系统总线。该体系结构能够抑制拜占庭故障,满足无人机高可靠、低成本、扩展性强、维护性能好等要求。

关键词:无人机;容错计算机系统;飞行控制系统;体系结构设计;余度设计;三模冗余

中图分类号:TP 273,V 249 **文献标志码**:A **DOI**:10.3969/j.issn.1001-506X.2016.11.20

Research on architecture of fault tolerant flight control computer for UAVs

LÜ Xun-hong, JIANG Bin, CHEN Xin, QI Rui-yun

(*College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*)

Abstract: The flight control computer (FCC) of high performance unmanned aerial vehicles (UAVs) must meet the increased safety and reliability requirements, and redundancy and fault tolerance are essential elements to improve the reliability and availability. The flight control system requirements, such as safety, reliability, maintainability, and real-time response, are studied. Then, compared among civil and military aircraft and UAV, the architectures and redundancy management of typical fault-tolerant FCC systems are introduced. Next, the particularity and future developments of FCC for UAV are addressed, and a triple modular redundancy (TMR) FCC system for UAV is developed. The TMR is a distributed system based on the FlexRay bus, and FlexRay is not only the backplane bus for the single FCC but also the system bus for the TMR system. The TMR system is Byzantine resilience, and meets the highreliability flexibility, scalability and low cost requirements of UAVs.

Keywords: unmanned aerial vehicle (UAV); fault tolerant computer system; flight control system; architecture design; redundant design; triple modular redundancy (TMR)

0 引 言

随着无人机应用日益广泛、应用领域不断扩大,功能不断增强,研制生产和使用维护成本不断提高,对飞控计算机的可靠性要求也越来越高。余度技术是提高飞控计算机可靠性的重要手段之一,余度容错飞控计算机已经成功地运用于民航客机[1-3]、战斗机[4]等有人机中,将飞控系统的故障率降低为 $10^{-7}\sim10^{-10}$/飞行小时。然而,有人机的容错飞控计算机系统不能满足无人机体积、功耗、价格等要求,无法直接应用于无人机中。容错飞控计算机系统也在美国全球鹰[5-6]、以色列 B-Hunter[7] 等无人机上得到了成功的应用。随着微电子、电子、计算机、总线等技术的发展,电子设备集成化程度更高、功能更强大,而体积更小、重量更轻、功耗更小、价格更便宜。工业电子技术应用广泛,其发展速度通常远高于航空电子技术的发展,但其可靠性也较低。如何合理地将先进的工业产品运用于航空电子设备中,充分利用工业技术的进步提高产品性能,在满足高可靠性的同时降低成本,始终是科技工作者需要解决的问题。

本文在对容错飞控计算机安全可靠性、实时性、维护性等要求进行研究的基础上,分析了无人机容错飞控计算机的设计需求特点。对 20 世纪 70 年代以来的典型容错飞控计算机体系结构进行了研究,阐述了针对不同需求设计的系统的体系结构及关键余度管理算法,以及系统随电子、总线、计算机等科技进步的发展,并对发展趋势进行了总结。

收稿日期:2015-06-28;**修回日期**:2016-07-05;**网络优先出版日期**:2016-08-25。

网络优先出版地址:http://www.cnki.net/kcms/detail/11.2422.TN.20160825.1440.004.html

基金项目:国家自然科学基金(61428303,61374130,61374116)资助课题

这些分析和总结，期望能够为无人机，乃至有人机容错飞控计算机新项目设计所借鉴。

无人机容错飞控系统可靠性低于有人机，要求系统体积小、重量轻、低功耗、低成本，而低成本是无人机能够占领市场，成功应用的关键。针对无人机容错飞控计算机的特点，提出一种基于 FlexRay 总线的相似三模余(triple modular redundancy，TMR)分布式容错飞控计算机体系结构。FlexRay 是一种针对汽车内部高可靠网络通信开发的总线，2006 年成功应用于宝马 X5 中，2010 年成为 ISO 国际通用标准[8]。目前，FlexRay 总线控制器已经集成于某些型号微控制器中，在满足高可靠性的同时降低了总线使用成本，使之与 CAN 总线的使用成本相差不远。

FlexRay 总线在航空领域的应用还较少，本文将 FlexRay 总线应用于容错飞控计算机系统中，FlexRay 总线既是单通道飞控计算机的内部总线，也是 TMR 系统数据交互的系统总线。FlexRay 总线传输速度为 10Mbps，作为单通道内部总线时，实际起到背板总线的作用，分析表明能够满足实时性要求。

TMR 系统会引起拜占庭将军问题，本文利用 FlexRay 总线及余度管理算法消除拜占庭将军故障，提高了系统可靠性。由于使用了分布式结构，本文提出的容错飞控计算机系统具有扩展性强、结构简单灵活、维护成本低等优点；容错技术及工业成熟产品的应用，使系统同时满足无人机高可靠及低成本，高性价比要求。

1　容错飞行控制计算机设计要求

容错飞控计算机本质上是一种高可靠实时数据采集与处理系统，设计时须考虑安全可靠性、实时性、飞行认证、性价比、维护性等要求。

1.1　安全可靠性要求

可靠性要求是飞控计算机必须满足的要求之一，是决定容错飞控计算机结构的主要因素。美国军机Ⅰ、Ⅱ、Ⅳ类飞机电传飞控系统故障率小于 62.5×10^{-7}/飞行小时，Ⅲ类飞机为 0.745×10^{-7}/飞行小时[9]；商用运输机则为 1×10^{-9}/飞行小时。无人机没有统一标准，传统无人机使用的是无余度飞控计算机，根据目前的技术水平及可靠性试验水平，单通道故障率一般可以达到小于 1×10^{-3}/飞行小时～1×10^{-4}/飞行小时。美国全球鹰无人机整机安全可靠性要求为 200 次飞行失效不大于 1 次[5]，即飞机总的安全可靠性要求 $R_s=0.995$。全球鹰一次飞行任务的时间定义为 42 h[10]，设整机故障率为 λ，则

$$e^{-\lambda\cdot42}=R_s=0.995 \tag{1}$$

可得

$$\lambda\approx1.2\times10^{-4}/\text{飞行小时} \tag{2}$$

假设采用典型飞行控制系统安全因子 $A_{s(FCS)}=0.10$[9]，飞行控制系统故障率 λ_{FCS} 应小于 1.2×10^{-5}/飞行小时。

由此可见，民航客机飞控系统的故障率小于军用飞机大概 2 个数量级，军用飞机故障率则小于无人机故障率大约 2 个数量级。由于飞控系统由飞控计算机、传感器、执行机构组成，飞控计算机的故障率还应小于上述值。如国内某高空长航时无人机要求余度飞控计算机故障率不大于 7.3×10^{-6}/飞行小时[11]。

余度等级(容错能力准则)是另一影响容错飞控计算机结构的重要因素。国内商用运输机飞控系统余度等级最低要求为故障－工作/故障－工作/故障－工作(FO/FO/FO)[12]，FA-16 为 FO/FO，X-29A 为故障-工作/故障-安全(FO/FS)[9]。对于无人机而言，飞机坠毁只引起经济上的损失，因此一般要求较低，如国内某高空长航时无人机要求为 FS[11]。

1.2　实时性要求

实时性要求是飞控系统最根本的要求。在指定时间间隔(控制周期)内，飞控计算机必须完成对机载传感器信息的采集，解算控制律，输出控制指令；舵机则响应控制指令，控制舵面偏转至指定位置。如果实时性得不到满足，飞机有可能失控。比如，如果不能每 40～100 ms 内提供正确的控制指令，静不稳定战斗机将发散[13]。飞控系统的控制周期一般为 10～100 ms，如航天飞机的控制周期为 40 ms[14]。对于高超声速无人飞行器，控制周期需要达到 10 ms，而对中低速无人机，40 ms 控制周期可以满足其控制要求。

1.3　其他要求

任何容错系统都要求具备高性价比，在满足可靠性要求的前提下尽可能降低系统成本。使用商用货架(commercial-off-the-shelf，COTS)产品是降低航空电子产品成本的手段之一。航天飞机轨道飞行器及 F-8 容错飞控计算机使用的是 IBM AP-101 通用计算机，X-38 容错飞控系统大部分使用 COTS 产品。使用 COTS 可以降低开发、重新设计、集成、测试等成本；在系统的生存周期中，方便地进行产品的升级换代。

维护性设计也是容错飞控计算机体系结构设计所需要考虑的重要因素。民航客机要求延迟维修，使任何硬件故障都延迟到方便的时间和地点再进行维修，减少或者消除签派延时[3]。因此，民航客机需要更高的余度水平以实现延期维修，如波音 777 使用了三-三余度容错飞控计算机系统。

某些容错飞行控制系统还要满足认证要求。如商用运输机必须要获取相关部门颁发的适航证才能投入运营，而适航认证的费用非常高，因此，在设计时必须充分考虑系统的认证要求，如在现有已经通过适航认证系统的基础上进行改进，只需补充认证改进部分，从而降低认证成本。

此外，还应该考虑通用性要求，不同项目使用相同的硬件模块，减少设计、认证和维护成本；可扩展性要求，在已有项目基础上进行有限的扩展以在新的项目中使用，或在现有的基础上加入新的功能；以及体积、重量、功耗等要求。

1.4　无人机容错飞行控制计算机特点

综上所述，无人机容错飞控计算机的特点首先是安全可靠性要求较低，余度等级要求也较低。由于不涉及人的

生命安全，出现故障后，能保证无人机安全返航即可。

无人机的实时性要求则不低于有人机的要求。无人机飞控计算机必须完成轨迹控制功能，其要求的控制周期与无人机的性能相关。

无人机体积小，重量轻，机载设备安装空间有限，因此，对容错飞行控制计算机体积、重量、功耗等提出更严格的要求。

低成本是无人机能够推广应用，占领市场的前提。因此，在满足安全可靠性要求的前提下，降低成本，提高系统的市场竞争力是无人机容错飞控计算机设计的重点之一。工业电子产品应用广泛，发展速度快，价格低，航空电子产品属专用产品，可靠性高，发展速度较慢，价格昂贵，因此，应最大化使用高可靠 COTS 产品，充分利用新产品提高系统性能的同时降低成本。

2 容错飞行控制计算机体系结构分析

容错飞控计算机系统的研究与应用相对成熟，文献[13，15-19]阐述了各种飞控计算机体系结构的优缺点及应用范围。本节先简述航空器常用的主从热备份结构、多数表决结构。然后对这两种结构在军用，民用有人机、无人机中的典型应用进行分析，阐述其工作原理及关键余度管理算法。有人机可靠性、余度等级比无人机高，因此，容错飞控计算机余度水平也较高，一般无法直接应用于无人机中，但其结构体系及余度管理算法可提供有益的参考。最后说明容错飞控计算机系统随电子技术、计算机技术、网络技术等先进技术的发展，并分析、总结其发展趋势。

2.1 常用航空器容错飞行控制计算机体系结构

主从热备份飞控系统中，若干能够实现相同功能的飞控计算机同步运行，但只有一个主飞控计算机允许输出，控制舵面偏转，其他飞控计算机都为备份计算机；当主飞控计算机故障时，切换至备份计算机。双机主从热备份飞控系统如图 1 所示。

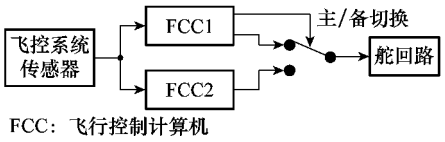

图 1 主从备份结构

Fig. 1 Dual standby architecture

故障检测技术是主从热备份结构最关键的技术，主飞控计算机的故障必须被及时、成功地检测并切换至备份计算机。常用的故障检测技术有机内自检测(built-in test，BIT)技术及自检测对比较监控技术[17]。BIT 技术很难达到 100%自检覆盖率，设计良好的电子设备自检覆盖率典型值为 95%。自检测对比较监控技术可实现更高的自检覆盖率。自检测对由两组实现相同功能的计算机组成，输入信号相同，控制律算法相同，对控制律解算的结果进行比较。假设两台飞控计算机同一时间出现相同故障并产生相同错误结果的可能性很小，则两台计算机结果相同表明系统无故障，否则，系统出现故障。如果两台计算机紧同步(时钟同步)运行，使用相同的输入信号，相同的软件，中间变量也保持相同的历史数据，则自检测对的输出结果是按位精确匹配的，也就是完全相同的，可以将自检测覆盖率提高至 100%。否则，两台飞控计算机输出只能大致匹配，需要阈值判别是否出现故障，这时自检测覆盖率为接近 100%。

一个自检测对只能检测出故障，要容忍 n 个故障，需要 $n+1$ 个自检测对，如容忍 1 个故障，需要 4 个通道计算机系统。由此可见，自检测对结构需要较多的冗余资源。

多模冗余表决结构运用的是故障掩盖技术，3 个或 3 个通道以上飞控计算机并列运行，对计算机的输出进行表决，表决算法有中值选择、多数表决算法等，其中多数表决算法最为常见。多数表决算法对所有通道输出进行比较，多数者为正确，少数者故障。和自检测对一样，多数表决算法对输出值的比较分为精确匹配和大致匹配 2 种方式。如果通道飞控计算机之间紧同步运行，则可实现精确匹配，否则，为大致匹配。

多模冗余系统需对表决面进行设置。除了对舵面指令进行多数表决，屏蔽飞控计算机故障外，通常也对冗余传感器数据进行表决，以屏蔽故障传感器对系统的影响。在传感器输出信号、飞控计算机输出信号设置表决面的 TMR 飞控系统结构如图 2 所示。

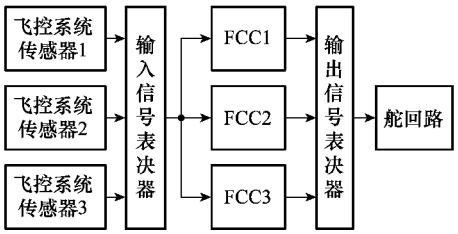

图 2 TMR 飞行控制系统结构

Fig. 2 Triple modular redundancy architecture

图 2 中的表决器可以是外加的硬件表决器，也可以由飞控计算机软件完成。如果使用软件表决器，则图 2 中冗余传感器与飞控计算机系统的连接有两种模式：一种是传感器 1、2、3 同时与计算机 1、2、3 连接，这种方案容错性能最好，但要求飞控计算机的资源为一台计算机的 3 倍。在一个系统中，飞控计算机所需的模拟量、开关量及串行接口的数量一般就已经相当可观[5]，如果所有的冗余传感器进行交叉连接则大大增加飞控计算机所需资源以及电缆的重量。另一种方法是传感器 1、2、3 分别与飞控计算机 1、2、3 连接，一个飞控计算机只采集一组传感器信息，飞控计算机之间进行交换数据并表决。这种方法容错能力较差，但计算机所需资源较少，也较常用。

需要在各通道之间交换数据的系统会引起拜占庭将军问题[20]。拜占庭将军问题的出现，是由于信息传输中出现了故障，导致两台计算机接收到的另一台计算机发送的数

据不一致，从而使单一故障在多模冗余系统中得不到一致的表决结果。虽然有些学者认为拜占庭故障出现的几率很小[19,21]，花很大的代价去解决一个出现可能性微乎其微的故障简直是舍本逐末，但是，对飞行控制系统这种高可靠控制系统，必须解决任何可能出现的故障，是否对出现可能性很小的故障进行解决，正是区分高可靠性系统和非高可靠性系统的标志。而且，之所以认为拜占庭故障出现可能性小，是因为受经验、测试条件及水平、能力等限制，在出现时拜占庭故障时，并未意识到出现的其实是拜占庭故障，实际上，拜占庭故障时可以检测到的[22]，因此，对在通道之间交换数据的多模冗余系统，必须解决拜占庭将军问题[17]。

舵面指令表决器可以设置在飞控计算机内部，表决后输出统一的指令，也可以由舵回路进行表决。用余度液压舵机进行舵面指令表决是一种常用的表决方法，相比而言，余度电动舵机用的较少。如果飞机本身有冗余的舵面，不仅可以通过容错控制[23-28]提高了系统的可靠性，更是可以降低系统对舵机可靠性的要求，提高飞控系统的性价比。

多模冗余表决技术可以和自检测对技术相结合，构成诸如三-二冗余、四-二冗余容错飞控计算机系统。

2.2　军用飞机容错飞行控制计算机体系结构

军用飞机容错飞控计算机一般为相似三余度或相似四余度[9]，早期很多军机有非相似模拟或机械备份，在数字容错飞控计算机的可靠性得到充分验证之后，拆除了备份系统。

F-8 是最早使用无机械备份数字电传操控系统(digital fly-by-wire，DFBW)的战斗机。F-8 余度等级为 FO/FS，使用了三余度相似飞控计算机[29-31]，飞控系统结构如图 3 所示。飞控系统传感器也为三余度，单通道飞控计算机只采集一组传感器信息；通过串行口进行通道间传感器数据交换。对传感器输入数据、离散量输入数据及舵面指令进行表决，传感器数据用典型的中值选择器，离散量输入数据则使用多数表决器。舵面指令表决由三余度液压舵机完成，3 个飞控计算机通道输出的模拟量舵面指令同时送到 3 个硬件中值选择器，完成中值选择后输出至 3 个电子伺服单元以驱动余度液压舵机。

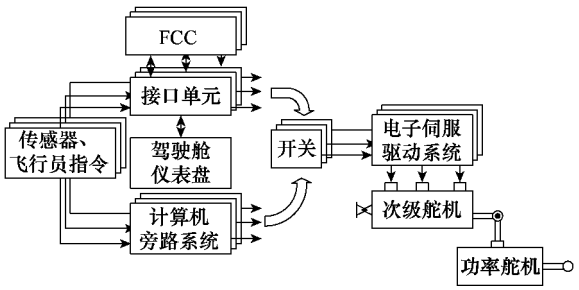

图 3　F-8 DFBW 结构

Fig. 3　Digital fly-by-wire system of F-8

3 个通道飞控计算机使用附加的离散量进行同步。每台计算机输出两个同步离散量，同时接收来自另两台飞控计算机输出的两个共 4 个同步离散量信号。使用两个离散量以识别离散量本身的故障。同步周期为 20 ms，每次于 10～50 μs 内完成，以使 3 个通道计算机同时采集传感器数据以进行内环控制律解算。除内环控制以外其他控制的控制周期为 80 ms。由于采用紧同步方式，输出指令用位精确匹配方法进行表决，且不对输出指令进行同步。

航天飞机容错飞控系统余度等级为 FO/FO/FS，其 DFBW 以 F-8 为基础，由四余度飞控计算机及一台非相似备份计算机组成[14,32-33]。备份计算机硬件与其他计算机相同，都为 IBM AP101B 计算机，但装载了简化的软件版本，在容错计算机出现第二次故障之后，由备份计算机接管，执行应急返航任务。

由于航天飞机全长 37.24 m，三角形后掠机翼的最大翼展 23.97 m，使得电缆重量占据了航空电子系统总重量的大部分，为此，采用了如图 4 所示共 28 路串行数据总线实现整个机载电子系统的数据与指令的传输，完成导航与制导、飞行控制、发动机控制、显示、系统管理、地面数据交互等功能。数据总线采用主从方式进行数据传输，飞控计算机为总线控制者，所有的数据传输都需要飞控计算机先发送相应指令。关键飞行控制总线有 8 路，其中 4 路为传感器数据采集总线，4 路为液压舵机控制总线。将传感器分成 4 组，4 个通道飞控计算机通过 4 路串行口与所有 4 组传感器相连：1 个通道计算机只能控制 1 路串行口的传输，请求该组传感器发送测量数据，但能同时接收所有 4 路总线的数据。因此，4 个通道飞控计算机拥有相同的传感器数据。每个通道飞控计算机通过 1 路串行口控制 1 个伺服放大单元，而伺服放大单元的输出控制四余度液压舵机的 1 个伺服阀。舵面控制指令表决由液压舵机完成。

航天飞机使用 3 个离散量完成同步操作，3 个离散量组成 1 个 3 位的同步码，用以标明同步操作、定时器及 I/O 中断，或标明故障的飞控计算机/传感器组。同步每 40 ms 进行一次，每次于 20 μs 完成。和 F-8 一样，输出指令用位精确匹配方法进行表决。

F-8 DFBW 于 1972～1973 年试飞，航天飞机于 1977 年进行自由飞首飞试验。由于当时还未形成拜占庭将军问题的系统理论，上述容错飞行控制系统未涉及拜占庭将军问题的解决。

X-38 容错飞控系统如图 5 所示，使用了基于德雷珀实验室(Draper laboratory)拜占庭故障恢复并行处理技术的四模余容错飞控计算机系统[34-35]，可以容忍 1 个拜占庭故障。4 个通道飞控计算机分别通过 4 路 MIL-STD-1553 总线与 4 组传感器、4 组电动执行机构连接，每个通道只采集 1 组传感器信息，控制 1 组执行机构；各通道飞控计算机之间则用 Network Element 光纤网互联，实现各通道间的数据交换。

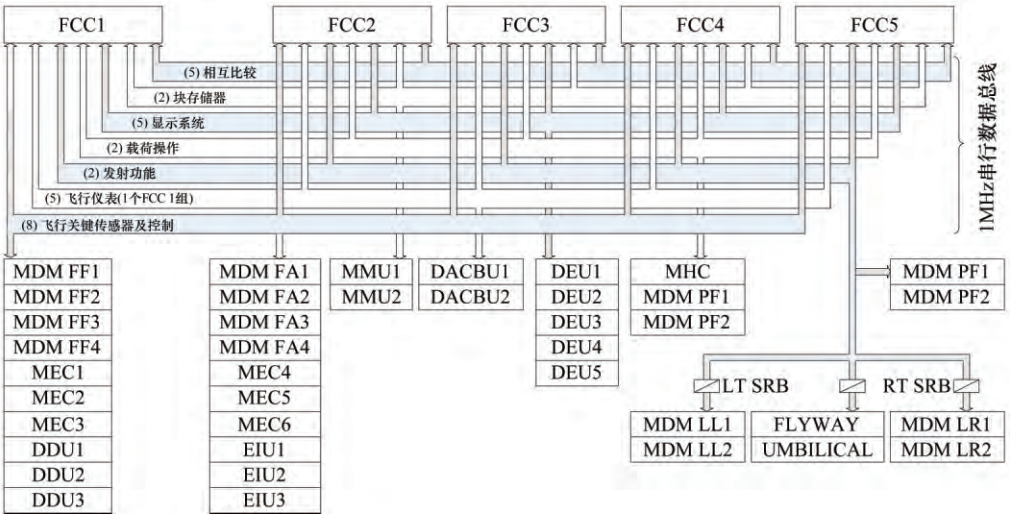

图 4 航天飞机飞行控制计算机系统接口示意图

Fig. 4 Digital processing system of space shuttle

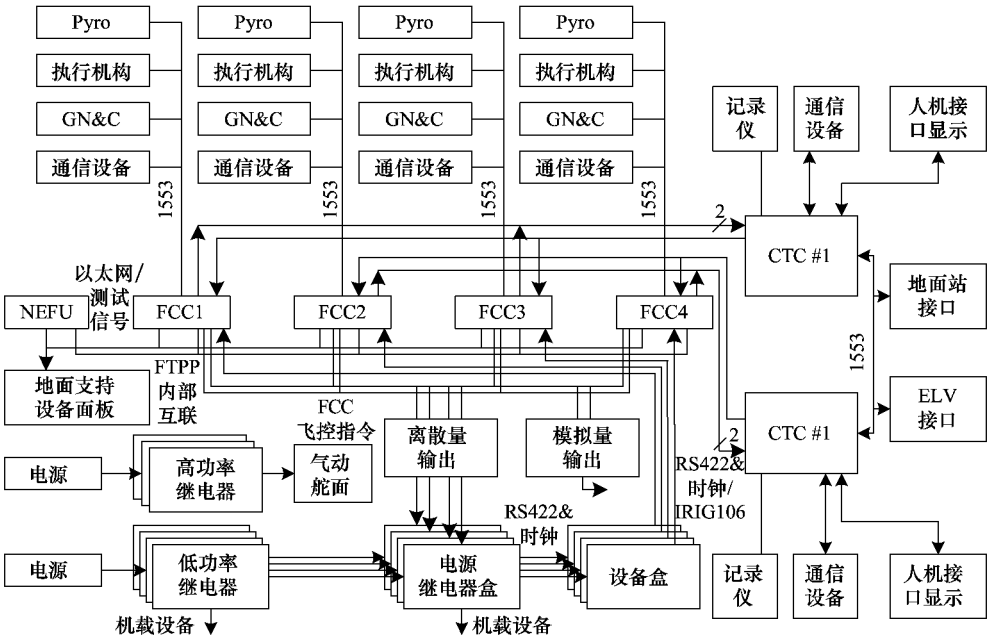

图 5 X-38 飞行控制系统结构

Fig. 5 X-38 avionics architecture

各通道飞控计算机每 20 ms 同步一次，严格按照预定时间节拍交换输入数据，比较控制律解算结果，发送表决后的控制指令。为了抑制拜占庭故障，保证传感器数据的一致性，飞控计算机之间执行两轮数据交换：第一轮飞控计算机交换自己采集到的传感器数据，第二轮交换第一轮中接收到的其他通道采集到的传感器数据。之后，对传感器数据进行故障检测与表决；解算控制律，得到舵面控制指令。最后，对舵面控制指令进行交换及表决，输出相同的表决结果。

X-38 虽然于 2002 年由于经费问题被终止，但之前进行了 8 次高空投放试验，验证了飞控系统设计的正确性。

2.3 民航客机容错飞行控制计算机体系结构

民航客机容错飞控计算机要求的可靠性很高，同时还要考虑延迟维修等要求，典型的有波音 777 及空客 A340 的飞控系统，其飞控计算机系统可靠性达到故障率小于 10^{-10}/飞行小时。

空客 A340 容错飞控计算机系统[1,3]用的是主从备份结构，由 3 台主飞控计算机(FCPC)、2 台从飞控计算机(FCSC)组成。3 台 FCPC 和 2 台 FCSC 互为备份，其中任何 1 台飞控计算机都能独立完成 A340 的飞行控制，因此，

可以容忍最多 4 台飞控计算机故障。正常情况下，所有飞控计算机同时工作，分别独立控制某个舵面，对于这个舵面而言，这台飞控计算机处于运行状态，其他计算机处于备份状态。A340 使用分离的舵面提供控制面气动冗余：2 个升降舵、4 个副翼舵及 12 个扰流板。

FCPC 和 FCSC 都有舵机驱动功能，因此，飞控计算机输出信号直接与舵机连接，同一时刻只有一台飞控计算机允许输出某个舵机的控制信号。

FCPC 和 FCSC 使用了如图 6 所示自检测对结构，其内部有 2 个支路计算机，一个支路为控制支路，另一个为监控支路。每台飞控计算机输出信号的连接/断开由继电器进行控制。对 2 个支路运算结果进行比较，如果超出预定的阈值，并且持续了指定的时间间隔，则判断该通道故障并断开该通道的输出，通过开关量信号指示备份计算机接管控制，控制权限在多台备份计算机之间变更的顺序是固定的。

FCPC 和 FCSC 采用了非相似余度技术，FCPC 和 FCSC 分别使用了不同的处理器；FCSC 使用手工编写代码，FCPC 则用同一自动编程工具的不同的编译器生成了控制支路和监控支路软件代码。

FCPC 和 FCSC 之间没有复杂的信息交互，也不需要复杂的余度管理算法，结构相对简单。

波音 777 FBW 采用分布式结构[2-3,36-37]，飞控系统结构框图如图 7 所示。三-三余度容错飞控计算机系统由 3 个完全相同的主飞控计算机（primary flight computer，PFC）组成，通过 3 组物理及电气上都隔离的 ARINC629 飞行控制总线与传感器、舵机控制器（ACE）及其他机载设备连接。PFC 通过 ARINC629 总线读取传感器数据并进行表决，解算出舵面指令，表决后通过飞行控制总线发送至 ACE。PFC、ACE 及飞行控制总线被分成左、中、右 3 组，每个 PFC 可以同时从 3 组总线接收数据，但只能向同组总线发送数据。

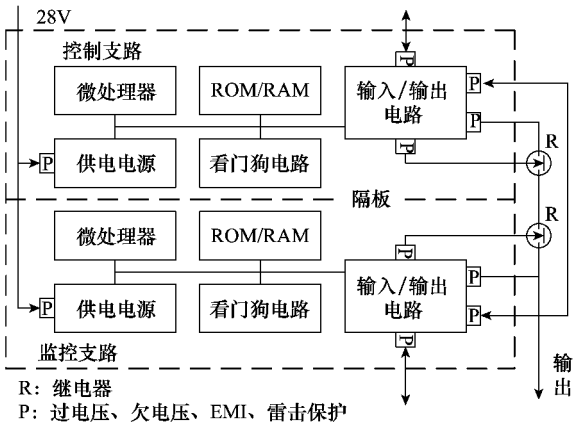

图 6　空客 A340 飞行控制计算机结构

Fig. 6　Flight control computer of Airbus A340

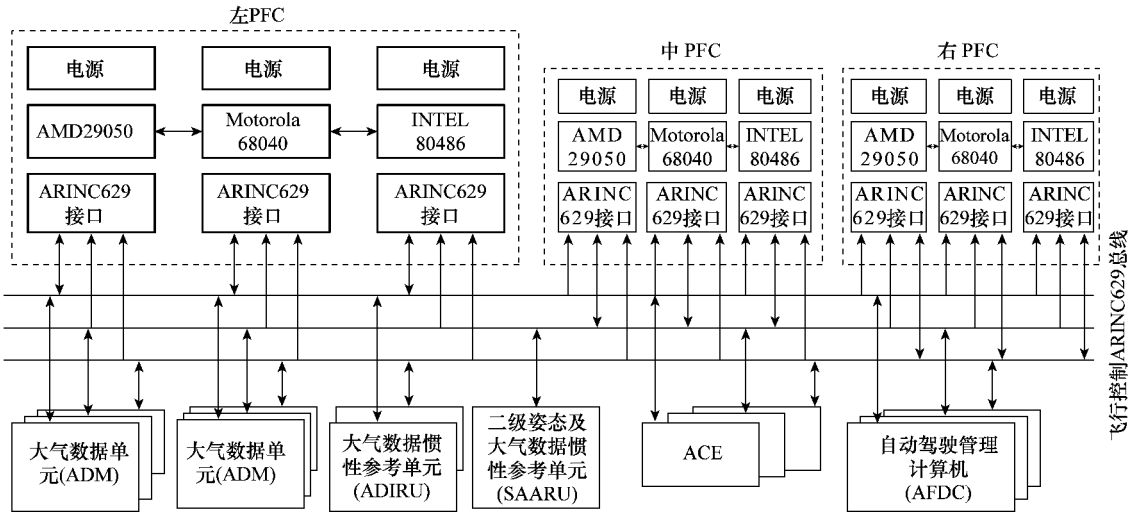

图 7　波音 777 飞行控制系统结构

Fig. 7　Primary flight computer architecture of Being 777

为了抑制共模故障，PFC 使用了非相似余度技术。每个 PFC 中有 3 个支路计算机，分别使用 3 种不同类型的 CPU 及外围接口电路，软件编译器也不同，由此克服相同硬件、编译器导致的共模故障。3 个支路分别执行指令运算、监控及备份功能。所有支路都有发送舵面指令的能力，但只有指令运算支路有发送舵面指令的权限。在系统上电时，3 个 PFC 中不同类型的计算机执行指令运算功能，如果指令运算支路故障，则切换至备份支路，PFC 继续工作。如果再出现故障，则切断该 PFC 输出。因此，在出现 6 个故障之后，切断所有的 PFC 输出，系统切换至直接控制模式。

指令运算、监控及备份支路用另一 ARINC629 内部总线实现帧同步、数据同步以及信息交换。在内部总线上发送同步帧，同步帧由一个帧标识符和一个数据字组成，20μs 内可完成数据传输，实现支路间的同步。数据同步帧则由帧标识符及若干数据字组成，以使 3 个支路使用相同的数据进行控制律解算。

ARINC629 飞行控制总线及 ARINC629 内部数据总线实现 PFC 通道之间、通道内部支路之间的监控。

3 个 PFC 及 ARINC629 飞行控制总线异步运行[38]，PFC 解算控制律的起始时间、解算时间都不一致，为此，对 3 个 PFC 的离散量输出进行统一，对舵面指令进行均衡。控制律解算结果通过 ARINC629 飞行控制总线在 3 个 PFC 内交叉传输。舵面指令通过 PFC 内的硬件中值选择器进行表决后再通过 ARINC629 总线发送给同组的 ACE。

PFC 提供了拜占庭将军问题的解决方案，所有连接到飞行控制总线的系统必须满足指定 ARINC629 总线需求；通过通道之间监控、输出指令中值表决等余度管理算法从根本上消除系统功能及信息不对称。

2.4 无人机容错飞行控制计算机体系结构

无人机安全可靠性要求较低，常规无人机使用无余度飞控系统，而高性能的无人机如长航时无人机、装载了昂贵任务设备的无人机等则需要装载高可靠容错飞控系统。

全球鹰无人机机载电子系统[5-6]如图 8 所示，关键飞控系统传感器、飞控计算机为双余度，舵机则无余度。全球鹰将所有的控制舵面都分离成内侧和外侧两组，提供了气动冗余。分析表明，在一个或多个舵机故障时，飞机仍然可控。双余度飞控计算机(IMMC)通过 MIL-STD-1553 总线与 INS/GPS 集成系统、敌我识别器(IFF)、防御系统、通信系统等连接；通过集成接口单元(IIU)与其他接口机载设备相连，如模拟量接口的电动舵机、大气数据计算机、无线电高度表等；开关量接口的电气系统；串行接口的差分 GPS、双余度发动机控制器、除冰器等。此外，飞行关键传感器如光纤陀螺、导航计算机同时与两台 IMMC 直接连接。

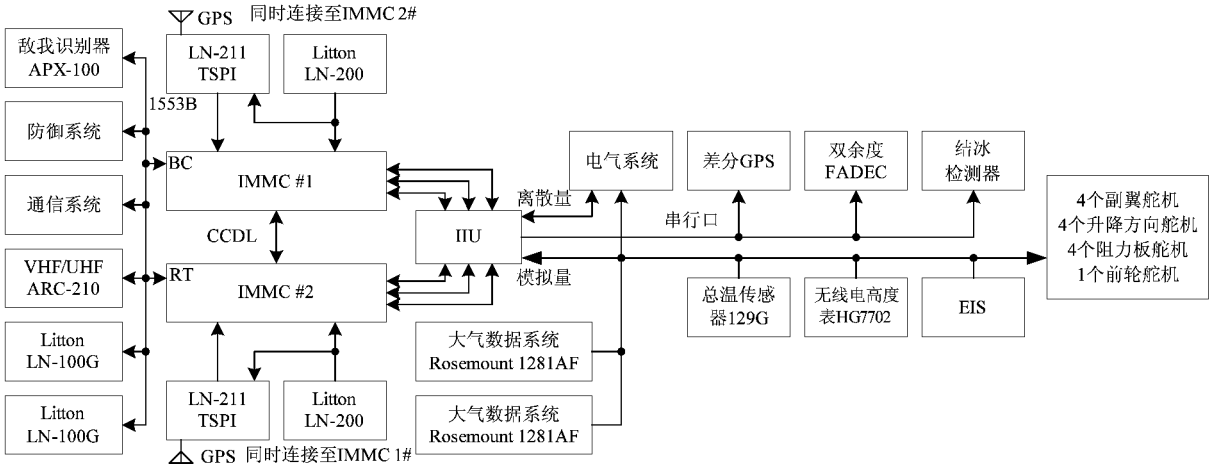

图 8 全球鹰电子系统架构

Fig. 8 Global Hawk avionics architecture

IMMC 之间使用 CCDL(cross channel data link)进行连接，交换采集的传感器数据及其他数据。对传感器数据进行合理性检查、比较监控、求均值等操作，IMMC 用相同的传感器数据进行控制律解算，以获取一致的舵面控制指令。

双余度 IMMC 并非工作于主从备份方式，系统无故障时，2 台 IMMC 同时工作，分别控制内侧舵面和外侧舵面。IMMC 使用了 VME64 背板具有 90% 以上自检覆盖率的 COTS 计算机，当一个 IMMC 通过自检测判断自身故障后，由另一个 IMMC 控制所有的舵面。

以色列飞机工业公司(IAI)的 B-Hunter 无人机[7]容错飞控计算机系统(DCPA)为主备结构，由相似双余度飞控计算机(AVC-1 与 AVC-2)组成，AVC-1 为主计算机，AVC-2 为从计算机，CCDL 用 RS422 串行接口实现。所有的输入信号同时与 AVC-1、AVC-2 连接，AVC-1 与 AVC-2 的大多数输出信号也连接在一起，但只有主飞控计算机能够输出控制信号。飞控计算机提供周期自检测功能，如果 AVC-1 故障，则 AVC-2 成为主计算机，接管全机的控制。

IAI 的鹰无人机(Eagle UAV)容错飞控系统如图 9 所示[39]，容错飞控计算机系统为主备相似三余度结构，3 台飞控计算机(AVC-1、AVC-2 和 AVC-3)分别工作于主/备状态，AVC-1 为主计算机，其他为备用计算机；多数表决器实现飞控计算机表决和监控功能。所有的输入信号同时与 3 台飞控计算机相连，关键飞控系统传感器为三余度，用多数表决器对传感器数据进行表决。鹰无人机用分离舵面提供气动冗余，消除舵面单点故障，降低了舵机的安全可靠性要求。

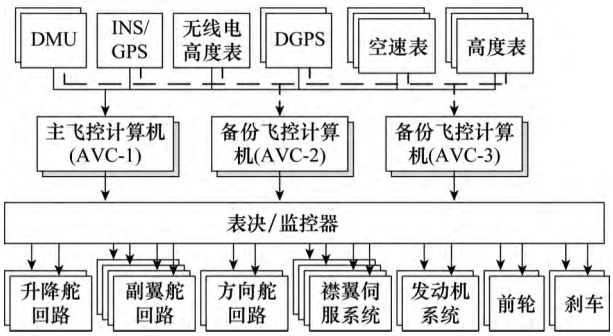

图 9 鹰无人机飞行控制系统架构

Fig. 9 Flight control system of Eagle UAV

2.5 无人机容错飞行控制计算机体系结构特点及发展方向

综上所述，主从热备份结构和多数表决结构在容错飞控计算机系统中都得到了成功的应用。

主从热备份结构的优点是主、从飞控计算机之间不需要进行复杂的数据交换，余度管理算法较简单，缺点是故障检测需要一定的时间，用 BIT 很难实现 100％的自检覆盖率。利用自检测对进行故障检测，如 A340 飞控计算机系统，在紧耦合的情况下，假设两台计算机不会同时出现相同的故障，则自检覆盖率可达到 100％，但自检测对使系统硬件数量加倍。随着电子技术的发展，元器件的功能越来越强，体积越来越小、功耗越来越低，由于较多冗余资源带来的负面影响越来越小，自检测对结构得到越来越广泛的应用。

多数表决结构的优点是用多数表决算法掩盖故障，对计算机的 BIT 能力没有特殊要求。缺点是多数表决系统需要计算机之间同步运行、互相交换数据；需要设置软件或硬件表决器对数据进行表决；此外，还应考虑拜占庭将军问题的解决。因此，余度管理算法相对复杂。

虽然随着电子、信息、计算机、网络等技术的发展，容错飞控计算机总体架构仍然以主从热备份结构、多数表决结构及两种结构的结合为主，但组成这些结构的计算机系统，以及整个机载电子系统，随着科技的进步一直在发展。

机载电子系统向分布式系统发展[40-41]。机载电子系统最初为联合式系统，每个子系统完成独立的功能，子系统由独立的计算机组成，有独立的 CPU、存贮器、I/O 处理单元；子系统之间用最少的线连接。联合式系统结构的优点是一个子系统故障不会蔓延至其他系统；通用性强，一个系统稍微进行修改即可在另一系统中使用；可以使用 COTS 组成系统等，缺点是造成计算、存贮等资源的浪费，增加了整个系统的体积、重量、功耗，且不便于子系统之间通信。为了克服联合式结构的缺点，系统向集成式结构发展，由一台计算机实现多个子系统的功能，如将舵机控制器功能集成到飞控计算机中。集成式结构的缺点是随着集成度越来越高，集成式结构系统的管理越来越复杂；子系统软件之间紧密耦合，降低了软件可靠性，增加了软件测试的难度；一般需要开发专用设备，无法使用 COTS 产品；最严重缺点的是子系统的故障有可能会蔓延至整个系统。随着嵌入式计算机技术的发展，计算机集成度提高，功耗降低，联合式结构又重新得到广泛应用，各子系统之间用串行总线连接在一起，形成分布式系统结构。分布式系统可以减少开发时间，降低成本，增强系统可扩展性，增加系统灵活性，降低了系统的复杂性，提高了维修性。

系统总线是分布式系统的基础，因此，分布式系统的结构、性能与总线的传输协议、拓扑结构、可靠性、传输速率等息息相关，随总线技术的发展而发展。文献[22]、文献[42]对几种有望使用于分布式航空电子系统的总线进行了研究，分析表明，对于强实时分布式控制系统，基于时间触发(time-triggered protocol，TTP)的总线协议优于基于事件触发的总线协议。分布式航空电子系统是高可靠强实时控制系统，运用于该系统的总线不仅要满足带宽要求，通信可预测、低等待时间及低的不稳定性，还要求在任何时候，特别是系统存在故障的情况下，系统节点仍可定时访问总线、系统通信仍可预测。基于事件触发的总线如 CAN 总线，以太网等，需要在高层通信协议中解决上述问题才可以运用于实时分布式控制系统中，如文献[43]提出了一种基于 CAN 总线分布式无人机飞控计算机结构，CPU 模块通过 2 路 CAN 总线与模拟量、开关量、串行口接口模块相连。CAN 总线在系统中为主从结构，CPU 模块为主节点，是所有总线传输的发起者，其他接口模块在接收到 CPU 模块发送的指定数据帧后方可发送数据。TTP 总线静态分配整个系统的通信带宽，每个节点在指定的时间发送数据，总线上的设备在任何时候都清楚是谁在发送数据，不需要在发送的数据帧中附加源地址和目标地址信息，这不仅增加了有效数据通信的带宽，还消除了故障节点发送信息给错误的接收节点，或伪装成别的设备发送数据的可能性。此外，在没有通信保护措施情况下，要容忍 n 个拜占庭故障，需要 $3n+1$ 台计算机，如 X-38 容错飞控计算机系统，用 4 台飞控计算机容忍 1 个拜占庭故障。而对于签名信息(signed message)传输，则只需要 $2n+1$ 台计算机[20]。每个节点在总线架构层处理时序故障，在应用层处理数值故障，且总线架构层和应用层彼此独立的情况下，如果通信系统能够提供合适的全局时钟，则 $2n+1$ 台计算机可容忍 n 个拜占庭故障。

系统总线按照某种总线拓扑结构(总线型连接、星形连接、点对点连接等)实现分布式系统各子系统之间的互联。最先使用串行总线进行子系统互联的是航天飞机，如前所述，整个系统共使用了 28 路点对点串行总线。随着总线技术的发展，军用航空总线 MIL-STD-1553 总线、商用航空总线 ARINC629 总线等航空专用总线提供了多种网络拓扑结构，简化了机载电子设备的连接，如 X-38 部分使用主从结构的 MIL-STD-1553 总线，部分使用 Network Element 光纤网；波音 777 中的 PFC 则通过 ARINC629 总线以总线型拓扑结构与其他设备连接。总线技术的进步使容错飞控系统的连接关系越来越简单，连接线越来越少，从而降低了机载电缆重量，提高了飞行器的有效载荷能力。

总线的传输速率是衡量总线性能的重要标准之一，传输速率越高，能够传输的数据越多，此外，还使多通道飞控计算机之间通过串行总线进行同步成为可能。F-8、航天飞机使用离散量进行同步，这种同步方式简单明了，速度快，到目前还有借鉴作用。缺点是占用离散量资源，且需要的离散量数量随通道的增加而增加，通用性差。波音 777PFC 则使用 ARINC629 总线实现同步，简化了系统设计。

航空总线有很高的容错能力，但应用范围窄，发展缓慢，价格昂贵，比如 MIL-STD-1553 总线，第一个版本发布于 1978 年，最后修改版本发布于 1996 年，传输速率为 1Mbps，只支持主从拓扑结构，目前没有升级版本发布。而工业总线应用范围广，发展迅速，价格低，因此，FlexRay，TTCAN 等工业总线都是有可能使用于航空系统的总线[42]。FlexRay 是一种基于时间触发，高可靠的车载总线，实际上，车载总线的可靠性要求和机载总线的可靠性要求相差不远[22]，虽然一辆汽车的故障率要求远低于一架飞机的故障率要求，但由于数量众多，运行时间长，所以

可靠性要求也非常高。此外，车载电子设备运行的温度、振动、电磁等环境与机载设备有相似之处，其与发动机、刹车等相关的电子设备也与驾驶员、乘客的生命相关，要求具备高安全可靠性。汽车电子产品使用广泛，发展速度远高于航空电子产品。因此，近年来有将汽车电子技术运用于航空电子领域的趋势。

工业总线的使用降低了系统的成本，航空电子系统的其他设备也应尽量使用 COTS，进一步提高系统性价比。直接使用 COTS 计算机，如航天飞机，是一种提高认证效率、方便系统升级的方法。但对于无人机而言，体积、重量、功耗的限制使得诸如 VME64、CPCI 总线的货架产品不一定能满足要求，且一般满足机载设备可靠性要求的 COTS 计算机在国内价格不菲。因此，使用通用总线、COTS 集成芯片及电路等是无人机飞控系统提高性价比的常用方法。

此外，传统机载计算机为集中式结构，计算机由若干板卡组成，核心 CPU 板通过并行总线访问其他板卡，如模拟量板、串行口板等，如全球鹰 IMMC 计算机[6]。由于并行总线至少有几十根数据总线及地址总线，因此，需要进行加固、抗震等处理，以确保并行总线连接的可靠性。近年来，分布式飞控计算机开始得到应用。文献[43-44]设计了以 CAN/FlexRay 总线为系统内部总线的飞控计算机，CPU 板通过冗余的内部串行总线与模拟量板、串行口板、开关量板等进行通信交互。由于 CAN/FlexRay 总线传输需要的信号线数量少，可以通过对串行总线本身冗余配置、连接线冗余配置、连接器多根芯连接同一信号等方法实现总线的可靠连接，不需要进行特殊加固、抗震处理，从而降低成本。此外，系统内部总线使用串行总线还有体积小，扩展性好，维护方便，一个功能板的故障不会扩展至整个系统等优点，是无人机飞控计算机发展方向之一。

3 基于 FlexRay 总线无人机容错飞行控制计算机体系结构

本文研究了一种以 FlexRay 总线为系统内部总线的分布式容错飞控计算机体系结构，满足无人机高可靠性及高性价比要求。

FlexRay 总线针对车载网络通信进行开发，2006 年成功应用于宝马 X5 中，2010 年成为 ISO 国际通用标准。经过多年的发展，已经相当成熟，一些微控制器如飞思卡尔的 MPC56XX 系列，MPC57XX 系列等内嵌 FlexRay 总线控制器，降低了总线使用成本。FlexRay 总线在航空领域的运用还较少，文献[44]研究了基于 FlexRay 的单通道分布式飞控计算机，本文在此基础上，研究一种基于 FlexRay 总线的分布式相似三余度容错飞控计算机系统。

3.1 FlexRay 总线分布式容错飞行控制计算机体系结构及关键余度管理算法

基于 FlexRay 的分布式容错飞控计算机系统如图 10 所示，由完全相同的 3 个通道飞控计算机及 4 组冗余 FlexRay 总线组成。假设 3 组飞控系统传感器分别与 3 个通道飞控计算机中的 1 个通道连接，无人机具有冗余气动舵面，因而使用无余度舵机，舵面指令通过通用串行总线(UART)发送至舵机控制器。舵机控制器同时接收 3 个通道飞控计算机指令，进行多数表决后输出。由于本节主要进行容错飞控计算机体系结构的研究，因此在图中未标明传感器与执行机构的连接关系。

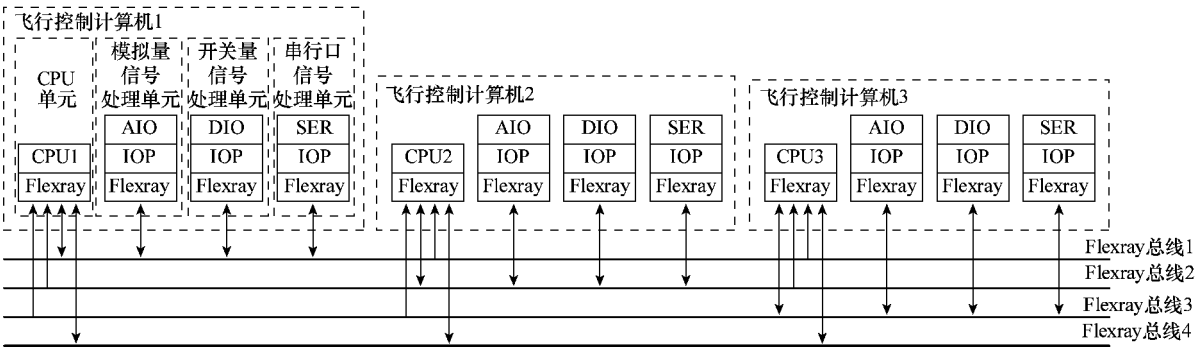

图 10 FlexRay 总线分布式容错飞行控制计算机体系结构

Fig. 10 The architecture of FlexRay-based distributed triple modular redundancy flight control computers

单通道飞控计算机的主要功能单元有 CPU 单元、模拟量信号处理单元(AIO)、开关量信号处理单元(DIO)及串行口信号处理单元(SER)。AIO、DIO 及 SER 由一块或多块功能板组成，每块功能板上都有微处理器(IOP)，通过 FlexRay 总线发送采集的机载设备的信息；接收 CPU 单元指令并输出。FlexRay 总线取代了传统并行总线实现计算机内部各功能模块的连接。每个通道飞控计算机都有单独的 1 路 FlexRay 内部总线，每个功能模块都可以向该总线发送/接收数据；同时，该总线也是容错飞控计算机系统的系统总线，其他通道飞控计算机可以接收该通道的数据，但不可以向该通道发送数据。如 FlexRay 总线 1 为飞控计算机 1 的内部总线，飞控计算机 1 的各个功能模块可以通过 FlexRay 总线 1 发送/接收数据，飞控计算机 2、3 可以接收 FlexRay 总线 1 数据，但不能向 FlexRay 总线 1 发送数据，以此类推。FlexRay 总线 4 为系统备份总线，不作为任何飞控计算机的内部总线。

在输入传感器数据及舵面指令输出端设置表决面。IOP 采集输入的模拟量、开关量、串行口数据，通过 FlexRay

总线发送给本通道飞控计算机 CPU 单元的同时，其他通道的 CPU 单元同时接收该通道的数据，从而实现第 1 轮输入数据的交叉传输。之后，CPU 板发送自己接收到的其他通道的输入数据，进行第 2 轮输入数据交叉传输，通过 2 轮数据交叉传输消除信息传输的不对称性，抑制拜占庭故障。

在此基础上，3 个通道飞控计算机利用相同的传感器数据进行多数表决，采用同一多数表决算法及相同的阈值，表决出相同的输入数据以进行控制律解算。对控制律解算的舵面指令及关键中间变量进行 2 轮交叉传输并进行表决。表决后的舵面指令通过串行口信号处理单元输出至舵机控制器。

由于飞控计算机采用了分布式结构，使得监控可以在较低层次的功能模块间进行。对控制律解算得出的舵面指令及其他输出指令进行多数表决即可判别 CPU 单元是否故障；CPU 单元同时接收 3 个通道的输入数据，进行多数表决同样可以判别某个功能单元故障。在 FlexRay 总线启动之后，AIO、DIO 及 SER 在指定的时隙内发送指定数据，而与 CPU 单元是否正常工作无关，这使得在某个通道的 CPU 单元故障的情况下，其他无故障功能单元的数据仍可利用。比如，飞控计算机通道 1 的 CPU 单元故障，其 AIO 采集的数据仍可以被飞控计算机通道 2、3 利用以进行多数表决，提高了系统的容错能力。

3.2　FlexRay 总线实时性分析与验证

综上所述，FlexRay 总线为系统核心，既是飞控计算机内部总线，也是容错飞控计算机的系统总线，FlexRay 总线的传输速率为 10Mbps，总线实时性至关重要。

以样例无人机飞控计算机[45]为例分析 FlexRay 总线实时性。将 CPU 单元发送给其他单元的数据称为下行数据，其他单元发送给 CPU 单元的为上行数据。单通道飞控计算机 SER 采集惯性导航传感器(ADU)、大气数据计算机(ADC)、无线电高度表(ALT)、速度及加速度传感器(DMU)等飞控系统传感器共 117 个字节(Byte)上行数据；发动机控制器(ECU)23 个字节上行数据，8 个字节下行数据；测控设备、任务管理计算机、地面检测设备等共 224 字节上行数据，160 字节下行数据；模拟量处理单元上行数据 64 个字节、下行数据为 32 个字节，为舵机控制器指令信号、舵机位置指示信号及备份模拟量输入/输出信号；开关量处理单元上行数据、下行数据各为 20 个字节。选飞行控制周期为 10 ms，10 ms 的控制周期可以满足绝大多数无人机飞控系统的控制要求。

FlexRay 总线将总线带宽按通信周期进行静态分配，每个通信周期都包含静态段、动态段、符号窗、网络空闲段，选择通信周期与控制周期一致，为 10 ms，只用针对时间触发的静态段进行数据的传输。

FlexRay 数据帧包括帧头、数据段、帧尾 3 部分，帧头占用 5 个字节，帧尾占用 3 个字节，数据段长度可以在 0～254 字节间选择。如果数据段短，则总线的有效数据传输效率低，如果数据段太长，很多数据帧无法填满，则同样会降低总线有效传输效率。根据样例无人机的特点，选择数据段长度为 32 个字节。由此，一个数据帧共 40 个字节，在 10 Mbps 传输速率下，需要的可靠传输时间不大于 50 μs，因此，将一个静态时隙设置为 50 μs。

样例单通道无人机飞控计算机一次数据传输需要 13 帧串行口上行数据，6 帧串行口下行数据，2 帧模拟量上行数据，1 帧下行数据，开关量上行数据及下行数据各 1 帧，此外，1 帧状态检测下行数据，3 帧检测上行数据，共 28 帧数据，传输时间为 1.4 ms。

由于 3 个通道飞控计算机都拥有自己的一组 FlexRay 内部数据总线，3 个通道飞控计算机同时接收上行数据，在自己的内部总线上同时发送下行数据，因此，额外需要的数据传输为进行第 2 轮交叉传输的飞控系统传感器输入数据及与控制律切换相关的开关量数据，以及需要进行 2 轮交叉传输及表决的与控制律积分运算相关的中间变量及控制指令。在样例无人机中，飞控系统传感器数据共 117 个字节数据，关键开关量数据 1 个字节；中间变量以及控制指令共 320 个字节。因此，额外的数据传输为第 2 轮交叉传输输入信号 8 帧数据(2 个通道共 236 个字节)，中间变量以及控制指令共 30 帧数据(1 个通道 10 帧数据，共 3 个通道)。38 帧数据的传输时间小于 2 ms，因此，FlexRay 总线传输时间小于 3.5 ms，可以满足 10 ms 控制周期的要求。

在图 10 结构的计算机通信系统中进行实时性验证，CPU 使用 MPC5644A，IOP 使用 C8051F120，由于 3 个通道的 FlexRay 总线逻辑相同，因此这里只对其中一路总线信号进行说明。用安捷伦 DSO-X 2012A 示波器记录的 FlexRay 总线波形如图 11 所示。在时间段 1 传输单通道 19 帧上行数据(串行口 13 帧、模拟量 2 帧、开关量 1 帧、检测 3 帧)后，在时间段 2 对飞控系统传感器数据及关键开关量进行第 2 轮交叉传输的 8 帧数据进行传输。在时间段 3 进行中间变量及控制指令的 30 帧数据进行传输；在时间段 4 输出 9 帧下行数据(串行口 6 帧、模拟量 1 帧、开关量 1 帧、状态检测 1 帧)。由图可见，数据帧传输时间和理论分析时间吻合，数据帧传输及应用程序处理时间小于 7 ms，可以满足实时性要求。

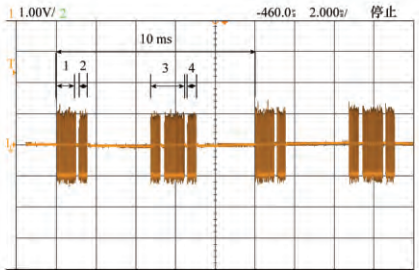

图 11　FlexRay 总线波形图

Fig. 11　Bandwidth utilization of FlexRay

4　结　论

(1) 容错飞控计算机设计要求有可靠性要求、余度等

级要求、实时性要求、认证要求、维护性要求、通用性要求、性价比要求、重量,体积及功耗要求等。无人机容错飞控计算机可靠性要求较有人机低,余度等级要求一般为 FS。因此,最大化使用高可靠 COTS 产品,充分利用新产品提高系统性能的同时降低成本,提高市场竞争力是无人机容错飞行计算机设计的重点之一。

(2) 对典型军用,民用有人机、无人机容错飞控计算机体系结构进行研究,阐述了针对不同需求设计的系统的体系结构及关键余度管理算法。这些系统可被新项目设计所借鉴。

(3) 机载电子系统向分布式系统发展,分布式系统的核心是系统总线。基于 TTP 协议的总线比基于事件触发的总线更适合于在飞控系统等硬实时控制系统中使用。航空专用总线可靠性高,但应用范围小,发展缓慢,价格昂贵。FlexRay 总线是一种高可靠车载专用总线,其运行的温度、振动、电磁等环境与机载设备有相似之处,应用广泛,价格低,是一种适合于在航空领域使用的总线。

(4) 提出一种基于 FlexRay 总线的分布式相似 TMR 容错飞控计算机体系结构,并给出了关键余度管理算法。FlexRay 总线既是单通道飞控计算机的内部总线,实现计算机背板总线的功能,也是多通道数据交互的系统总线。该系统能够满足无人机高可靠、低成本,高性价比、维护性好、扩展性强等要求。

参考文献:

[1] Briere D, Traverse P. AIRBUS A320/A330/A340 electrical flight controls-a family of fault-tolerant systems[C]// *Proc. of the 23rd IEEE International Symposium on Fault-Tolerant Computing*, 1993: 616-623.

[2] Aplin J D. Primary flight computers for the Boeing 777[J]. *Microprocessors and Microsystems*, 1997, 20(8): 473-478.

[3] Chen Z J, Qin X D, Gao J Y. Dissimilar redundant flight control computer system[J]. *Acta Aeronautica et Astronautica Sinica*, 2005, 26(3): 320-327. (陈宗基,秦旭东,高金源. 非相似余度飞控计算机[J]. 航空学报, 2005, 26(3): 320-327.)

[4] Ammons E. F-16 flight control system redundancy concepts[C]// *Proc. of the Guidance and Control Conference*, 1979.

[5] Loegering G, Evans D. The evolution of the global hawk and MALD avionics systems[C]// *Proc. of the 18th IEEE Digital Avionics Systems Conference*, 1999: 1-8.

[6] Loegering G. Global Hawk in a network centric environment[C]// *Proc. of the 3rd AIAA Unmanned Unlimited Technical Conference, Workshop and Exhibit*, 2004: 1-6.

[7] Defense Technical Information Center. The B-Hunter UAV system[EB/OL]. [2015-06-22]. http:// www. dtic. mil/dtic/tr/fulltext/u2/p010763. pdf.

[8] Wu B X, Guo Y H, Cao Y, et al. *The development examples for the automotive bus of FlexRay*[M]. Beijing: Publish House of Electronics Industry, 2012:1-6. (吴宝新,郭永红,曹毅,等. 汽车 FlexRay 总线系统开发实战[M]. 北京:电子工业出版社, 2012: 1-6.)

[9] Yao Y P, Li P Q. *Reliability and redundancy technology*[M]. Beijing: Aviation Industry Press, 7-10, 180-183. (姚一平, 李沛琼. 可靠性及余度技术[M]. 北京: 航空工业出版社, 1991: 7-10,180-183.)

[10] Loegering G. On the wings of a Hawk-a UAV navigation system takes flight[J]. *GPS World*, 2000, 11(4):34-45.

[11] Liu X X. Research on redundancy techniques for flight control computer of high altitude, long endurance UAV[D]. Xi'an: Northwestern Polytechnical University, 2004. (刘小雄. 高空长航时无人机飞行控制计算机系统冗余设计技术研究[D]. 西安:西北工业大学, 2004.)

[12] Qin X D, Chen Z J, Li W Q. Research on dissimilar redundant flight control computers of large civil aircraft[J]. *Acta Aeronautica et Astronautica Sinica*,2008,29(3):686-694. (秦旭东,陈宗基, 李卫琪. 大型民机的非相似余度飞控计算机研究[J]. 航空学报, 2008,29(3): 686-694.)

[13] Lala J H, Harper R E. Architectural principles for safety-critical real-time applications[J]. *Proceedings of the IEEE*, 1994, 82(1): 25-40.

[14] Minott G M, Peller J B, Cox K J. Space Shuttle digital flight control system, NASA-N76-31146[R]. NASA, 1976.

[15] Rice J W, McCorkle R D. Digital flight control reliability-Effects of redundancy level, architecture and redundancy management technique[C]// *Proc. of the AIAA Guidance and Control Conference*, 1979.

[16] Yount L J. Digital flight-critical systems for commercial transports, AIAA-A85-17806[R]. Reston: AIAA, 1985.

[17] Hammett R. Design by extrapolation: an evaluation of fault tolerant avionics[J]. *IEEE Aerospace and Electronic Systems Magazine*, 2002, 17(4): 17-25.

[18] Black R, Fletcher M. Next generation space avionics: layered system implementation[J]. *IEEE Aerospace and Electronic Systems Magazine*, 2005, 20(12): 9-14.

[19] Smith T J, Yelverton J N. Processor architectures for fault tolerant avionic systems[C]// *Proc. of the 10th IEEE/AIAA Digital Avionics Systems Conference*, 1991: 213-219.

[20] Lamport L, Shostak R, Pease M. The Byzantine generals problem[J]. *ACM Trans. on Programming Languages and Systems*, 1982, 4(3): 382-401.

[21] McGough J G. The Byzantine generals problem in flight control systems, AIAA-90-5210[R]. Reston: AIAA, 1990.

[22] Rushby J. Bus architectures for safety-critical embedded systems[C]// *Proc. of the Embedded Software*, 2001: 306-323.

[23] Lv X, Jiang B, Qi R, et al. Survey on nonlinear reconfigurable flight control[J]. *Journal of Systems Engineering and Electronics*, 2013, 24(6): 971-983.

[24] Jiang B, Yang H. Survey of the active fault-tolerant control for flight control system[J]. *Systems Engineering and Electronics*, 2007, 29(12): 2106-2110. (姜斌, 杨浩. 飞控系统主动容错控制技术综述[J]. 系统工程与电子技术, 2007, 29(12): 2106-2110.)

[25] Shen Q, Jiang B, Cocquempot V. Adaptive fuzzy observer-based active fault-tolerant dynamic surface control for a class of

nonlinear systems with actuator faults[J]. *IEEE Trans. on Fuzzy Systems*, 2014, 22(2): 338-349.

[26] Gayaka S, Yao B. Output feedback based adaptive robust fault-tolerant control for a class of uncertain nonlinear systems[J]. *Journal of Systems Engineering and Electronics*, 2011, 22(1): 38-51.

[27] He J, Qi R, Jiang B, et al. Adaptive output feedback fault-tolerant control design for hypersonic flight vehicles[J]. *Journal of the Franklin Institute*, 2015, 352(5): 1811-1835.

[28] Qi R, Huang Y, Jiang B, et al. Adaptive backstepping control for hypersonic vehicle with uncertain parameters and actuator failures[J]. *Proceedings IMechE: Part I-Journal of Systems and Control Engineering*, 2013, 227(1): 51-61.

[29] Szalai K J, Felleman P G, Gera J, et al. Design and test experience with a triply redundant digital fly-by-wire control system, AIAA-76-1911[R]. Reston: AIAA, 1976.

[30] Deets D A, Szalai K J. Design and flight experience with a digital fly-by-wire control system using Apollo guidance system hardware on an F-8 aircraft, AIAA-72-881[R]. Reston: AIAA, 1972.

[31] Szalai K J, Larson R R, Glover R D. Flight experience with flight control redundancy management[R]. Advisory Group for Aerospace Research and Development LS, 1980.

[32] Hanaway J F, Moorehead R W. Space shuttle avionics system, NASA-SP-504[R]. NASA, 1989.

[33] Blair-Smith H. Space shuttle fault tolerance: Analog and digital teamwork[C]// *Proc. of the 28th IEEE/AIAA Digital Avionics Systems Conference*, 2009: 6. B. 1-1-6. B. 1-11.

[34] Kouba C, Buscher D, Busa J. The X-38 spacecraft fault-tolerant avionics system, JSC-CN-8132[R]. NASA, 2003.

[35] Rice L E P, Cheng A M K. Timing analysis of the X-38 space station crew return vehicle avionics[C]// *Proc. of the 5th IEEE Real-Time Technology and Applications Symposium*, 1999: 255-264.

[36] Yeh Y C. Design considerations in Boeing 777 fly-by-wire computers[C]// *Proc. of the 3rd IEEE International High-Assurance Systems Engineering Symposium*, 1998: 64-72.

[37] Yeh Y C. Safety critical avionics for the 777 primary flight controls system[C]// *Proc. of the 20th IEEE Digital Avionics Systems Conference*, 2001: 1C2/1-1C2/11.

[38] Hammond R A, Newman D S, Yeh Y C. On fly-by-wire control system and statistical analysis of system performance[J]. *Simulation*, 1989, 53(4): 159-167.

[39] Goshen-Meskin D. Presentation of the eagle UAV system[R]. Israel Aircraft Industries, Ltd., MALAT Division, Military Aircraft Group, 2005.

[40] Hammett R. Flight-critical distributed systems: design considerations[J]. *IEEE Aerospace and Electronic Systems Magazine*, 2003, 18(6): 30-36.

[41] Alstrom K, Torin J. Future architecture for flight control systems[C]// *Proc. of the 20th IEEE Digital Avionics System Conference*, 2001: 1B5/1-1B5/10.

[42] Gwaltney D A, Briscoe J M. Comparison of communication architectures for spacecraft modular avionics systems, TM-2006-214431[R]. NASA, 2006.

[43] Zhang Z A, Chen X, Lü X H. Design of a distributed flight control computer for UAV[J]. *Computer Systems & Applications*, 2010, 19(8): 16-19. (**张增安, 陈欣, 吕迅竑. 一种用于无人机的分布式飞行控制系统设计[J]. 计算机系统应用**, 2010, 19(8): 16-19.)

[44] Zhang Y, Chen X, Lü X H. Flight control computer communication system based on FlexRay bus[J]. *Machine Design and Manufacturing Engineering*, 2013, 42(3): 53-56. (**章勇, 陈欣, 吕迅竑. 基于** FlexRay **网络的飞行控制计算机总线通信系统[J]. 机械设计与制造工程**, 2013, 42(3): 53-56.)

[45] Zhang Y. Design and research on FlexRay bus communication for flight control computer[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2013. (**章勇. 基于** FlexRay **飞行控制计算机总线设计与研究[D]. 南京:南京航空航天大学**, 2013.)

作者简介:

吕迅竑(1973-),**女,博士研究生,助理研究员,主要研究方向为容错控制、导航制导与控制。**

E-mail:lvxh@nuaa.edu.cn

姜　斌(1966-),**男,教授,博士,主要研究方向为故障诊断、容错控制。**

E-mail:binjiang@nuaa.edu.cn

陈　欣(1960-),**男,研究员,博士,主要研究方向为导航制导与控制。**

E-mail:chenxin@nuaa.edu.cn

齐瑞云(1982-),**女,教授,博士,主要研究方向为故障诊断、容错控制。**

E-mail:ruiyun.qi@nuaa.edu.cn