文章编号:1674-8190(2024)06-209-07

基于分布式系统构架的飞控系统容错设计研究

杨朝旭,杨林,万天才,张君
(航空工业成都飞机设计研究所,成都 610091)

摘 要: 传统的集中式飞控系统构架,与机电、任务等其他系统相互独立,难以满足现代战斗机系统综合设计的要求,而具备开放性和综合控制特征的分布式系统构架是技术发展的必然趋势。基于分布式系统架构的飞控系统容错设计展开研究,首先,介绍分布式飞控系统的典型系统架构及其容错设计的目标;其次,针对分布式系统的运行时序特点,开展基于时间的容错设计;最后,针对分布式系统的组成和体系构架特点,设计多级表决/监控面。通过对分布式系统的运行时序、组成和体系构架特征的分析,梳理分布式系统容错设计的关键切入点,阐述容错设计方案的解决思路和实施方式。经工程实践验证,结果表明:本文所研究的容错设计技术可保证飞控系统运行稳定可靠,有效提升了系统安全性。

关键词: 分布式系统;容错设计;表决/监控
中图分类号: V249.1; V448 **文献标识码:** A
DOI: 10.16615/j.cnki.1674-8190.2024.06.19

Study the fault-tolerant design of flight control system based on distributed systems architecture

YANG Zhaoxu, YANG Lin, WAN Tiancai, ZHANG Jun
(AVIC Chengdu Aircraft Design and Research Institute, Chengdu 610091, China)

Abstract: The traditional centralized flight control system architecture is independent of other systems such as electromechanical and mission systems, making it difficult to meet the requirements of modern fighter system comprehensive design. The distributed system architecture with openness and comprehensive control features is an inevitable trend in technological development. In this paper, the fault-tolerant design for flight control systems based on distributed system architecture is studied. Firstly, the typical system architecture of distributed flight control systems and the objectives of their fault-tolerant design are introduced. Secondly, based on the operational timing and working mode characteristics of the distributed system, a time-based fault-tolerant design is conducted. Finally, based on the composition and system architecture characteristics of the distributed system, a multi-level voting/monitoring surface is designed. By analyzing the running time sequence, composition and architecture characteristics of distributed system, the key entry points of fault-tolerant design of distributed system are sorted out, and the solutions and implementation methods of fault-tolerant design scheme are expounded. The engineering practice shows that the fault-tolerant design scheme studied in this paper can ensure the stable and reliable operation of flight control system and effectively improve the system security.

Key words: distributed system; fault-tolerant design; voter/monitor

收稿日期: 2024-05-09; **修回日期:** 2024-10-25

通信作者: 张君(1985-),男,硕士,研究员。E-mail: 995538876@qq.com

引用格式: 杨朝旭,杨林,万天才,等. 基于分布式系统构架的飞控系统容错设计研究[J]. 航空工程进展, 2024, 15(6): 209-215.
YANG Zhaoxu, YANG Lin, WAN Tiancai, et al. Study the fault-tolerant design of flight control system based on distributed systems architecture[J]. Advances in Aeronautical Science and Engineering, 2024, 15(6): 209-215. (in Chinese)

0 引 言

梳理当前主流战斗机的设计要求，系统综合无疑是其中极具分量的一条。综合意味着在设计过程中需要充分挖掘飞机潜能，对各机载系统资源进行统一的规划管理和使用，从而获得性能、重量、体积、成本、可靠性、维护性等方面的综合优势。以往三代机使用的集中式飞控系统构架，与机电、任务等其他系统相互独立，难以满足现代战斗机系统综合设计的要求，因此，具备开放性和综合控制特征的分布式系统构架是目前技术研究的必然选择[1-3]。

然而由于分布式系统涉及多个独立的子系统和节点，系统间的通信、协同工作以及故障隔离的复杂性大幅增加。与集中式系统不同，分布式系统需要针对各个节点的可靠性、数据一致性以及通信链路的稳定性进行全面考虑，且对于关系到飞行安全的飞控系统而言，稳定、可靠的容错设计是保证飞行任务顺利执行的基础。因此，基于分布式系统构架的飞控系统容错设计是衡量飞控系统成功研制与否的关键[4-5]。

三代机电传飞控系统普遍采用了集中式的体系结构，系统以飞控计算机为核心，通过硬线与各成品进行连接，飞控计算机要同时承担数据采集、处理，信号余度管理，控制律计算和操纵面伺服控制等功能[6-8]。最早使用数字电传飞控系统的是美国F-16战斗机，其具备多重冗余设计，主计算机和备份计算机分开运行，确保主计算机全部故障时，系统能够自动切换到备份计算机。我国自主研制的“枭龙”战斗机的飞控系统也采用了集中式体系架构，以多余度数字主计算机和备份计算机为核心，通过硬线分别与前端多余度传感器和后端执行机构相连，各余度相互独立，当数字主计算机全部故障后可自动转入备份计算机。虽然集中式体系架构的结构简单、逻辑清晰，但上述任意一个功能的失效，往往会造成整个控制余度的损失，极大地影响了飞控系统的任务可靠性。

随着机载系统研发水平、技术的全面提高，为了充分发挥飞机及其机载系统的潜力，提高飞机性能、减轻重量、节约成本、提高可靠性和维护性，国外现代先进战斗机的飞控系统研发中逐步开始采用分布式体系构架，其典型结构特点为：

1）以主计算机为中心，所有与飞行控制相关的系统均在主计算机中进行功能综合；

2）三代机飞控计算机中负责采集、处理信号和执行伺服控制的功能模块被拆分出主计算机，就近安装在传感器和被控制操纵面附近，形成二级控制子系统；

3）通过高可靠性、高速的系统总线，将主计算机与各二级控制子系统连接起来，形成分布式结构。

20世纪末，F-22战斗机的飞控系统研制中就曾有限地采用了分布式系统构架，如飞控计算机通过1553总线与大气数据系统、全权限数字发动机控制器进行连接，构成了局部的分布式系统构架。但是，受当时的技术水平和开发经验等方面的限制，飞控系统中使用的关键传感器和控制部件，仍然通过硬线与飞控计算机连接[9]。此后十年，分布式系统构架技术逐步成熟，最终在X-32演示验证机和F-35战斗机的飞控系统研制中得以应用，并获得充分验证[10]。空客A320的飞控计算机中包括了2台升降舵副翼计算机、3台扰流板升降舵计算机、2台飞行增稳计算机以及2台襟翼计算机，不同计算机承担相对应的功能，从而提高可靠性[11]。波音B777客机将飞控计算机单元尽可能分离，同时将每一个飞控计算机设计成非相似结构，从而进一步提高系统的可靠性[12]。分布式架构保证了其构成系统具有更高的可靠性。

但与此同时，分布式系统的开发技术跨度大、难度高，尤其是在关系到飞行安全的飞控系统中采用分布式系统构架，需要解决系统构架设计、系统容错和高可靠系统总线研制等关键技术问题。因此，本文针对分布式架构的飞控系统容错设计展开研究，首先介绍容错设计的目标，其次给出基于时间的飞控系统容错设计，最后阐述分布式系统表决/监控面设计，并对现有研究情况进行总结。

1 容错设计的目标

飞控系统容错设计的主要目标是：确保在飞行中由于飞控系统故障导致的飞机灾难性事故的

概率符合飞控系统标准中的安全性要求,即小于等于10^{-7}/fh,并使故障导致的瞬态满足飞行品质规范的要求,同时,需产生合理的飞控系统综合告警信息,通报飞行员进行处置[13-14]。

当前主流战斗机飞控系统结构的演化示意图如图1~图3所示。

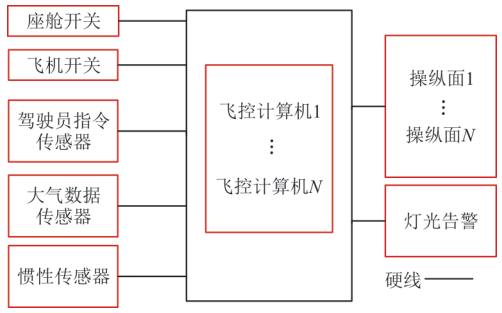

图1　传统集中式飞控系统结构示意图[15]

Fig. 1　Traditional centralized flight control system(FCS) architecture diagram[15]

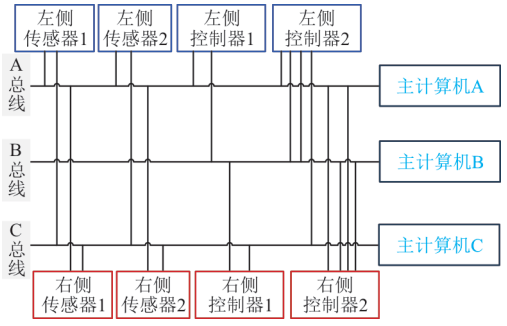

图2　有限分布式飞控系统结构示意图[15]

Fig. 2　Semi-distributed FCS architecture diagram[15]

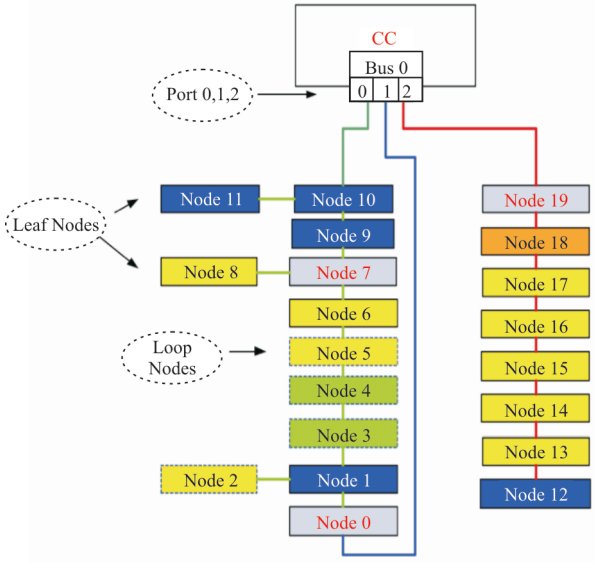

图3　分布式飞控系统结构示意图[15]

Fig. 3　Distributed FCS architecture diagram[15]

对集中式飞控系统而言,容错设计主要围绕各余度飞控计算机完成。每个余度的飞控计算机在采集信号的同时即可判断信号的采集是否有效,随后对交叉通道传输后的信号进行表决监控,剔除故障的信号,获得正确的表决值用于控制律计算并输出控制指令;飞控计算机的伺服控制功能将控制指令转换为伺服指令,用于驱动操纵面运动,操纵面运动中产生的异常也由飞控计算机监控并处理。纵观整个流程,飞控计算机直接参与了系统从输入到输出全过程的状态监控和管理,是系统容错设计的核心。

与集中式系统不同,分布式系统中存在多个智能部件,以信号采集为例,主计算机不再通过硬线直接采集所用的信号,而是通过前端专用的二级控制器完成信号的采集,并通过系统总线将信号的采集结果发给主计算机。因此,在容错设计中,除了传统的信号余度管理外,还需要对二级控制器的工作状态、总线的通讯状态、主计算机自身的工作状态进行考虑。由此可见,在分布式系统中,主计算机只是系统容错设计的一个中心,完整的系统容错设计已被分解到了系统的每一级控制器中,每一个环节都会对整个系统的容错结果产生影响。

因此,在保证飞控系统可靠性的基础上,如何根据分布式系统的组成、运行时序特征等进行合理的容错设计,是分布式飞控系统设计的关键技术。

典型四余度分布式飞控系统架构如图4所示,其各部分的主要功能如下:

1) 主计算机:采用四余度配置,主要完成系统级的余度管理、控制律计算等功能;

2) 系统总线:采用四余度配置,用于系统内各成品之间,以及与其他系统之间进行数字信息传递。对于传感器采集、操纵面控制单元等重要成品,采用如图3所示“环状”结构进行连接,可容忍总线1次物理连接故障;

3) 飞行员控制装置及信号采集单元:采用四余度配置,提供飞行员对飞控系统的驾驶杆、脚蹬和开关的操作指令;

4) 传感器单元:提供飞控系统所需的传感器参数,如大气数据、惯性运动参数等;

5) 操纵面控制单元:采用四余度配置,根据主计算机控制指令,完成飞控系统主操纵面的驱动;

6）辅助控制单元：采用两余度配置，根据主计算机指令，完成飞控系统辅助操纵面等监控和驱动。

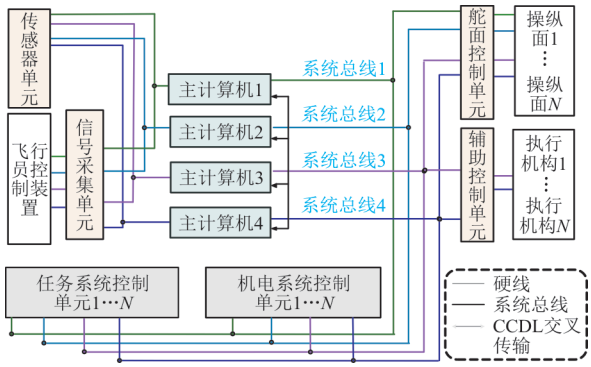

图4 分布式飞控系统结构示意图

Fig. 4 Typical distributed FCS architecture diagram

2 基于时间的容错设计

根据分布式系统的运行时序和工作模式特点，进行基于时间的容错设计，包括：

1）同步机制，飞控系统为多余度系统，各余度间要求同步，需对采用分布式架构的飞控系统同步状态进行管理并通报全系统使用；

2）运行时序，分布式系统中一、二级等控制器并存，采用不同的运行周期，需对系统中各成品运行时序的差异进行设计；

3）模式管理，分布式系统中一、二级等控制器的复杂度各不相同，响应速度存在差异，需对系统中各成品的工作模式差异进行设计。

2.1 同步机制管理

分布式飞控系统的同步主要分为两部分进行，分别是各余度主计算机之间的同步和系统各余度分支之间的同步。

主计算机之间的同步通过专用硬线实现，由飞控系统机载软件每个周期对本余度主计算机与其他余度主计算机的同步状态进行“双握手”监控。

主计算机完成各自的同步后，会通过自身控制的系统总线，由总线上的专用消息包向总线上的其余二级控制器通报本余度分支的同步信息，总线上的二级控制器将根据总线上的同步信息，完成本周期的操作。

由于存在主计算机和系统总线两个异步的时钟源，需要对周期性同步的优先级进行设定。正常工作期间，由主计算机上的应用软件控制本余度分支的周期性同步；若主计算机故障（软件无法正常运行），则由系统总线自动接管本余度分支的周期性同步，确保在主计算机故障的情况下，对应余度分支的二级控制器不受影响。

2.2 运行时序管理

分布式飞控系统架构下运行的多个控制器均具有独立的时钟，控制器之间通过系统总线进行数据交互，根据系统组成和架构特征，时序设计采用以一级控制器为基准、系统总线为载体、二级控制器同步匹配的策略。一方面确保对时间敏感的飞控系统时间延迟最小（不超过一个小帧），另一方面确保各控制器之间数据交互的高度确定性，为系统总线监控和余度管理奠定基础。

系统总线的数据传输时序与主计算机的系统功能调度时序需要进行匹配性设计，以避免竞争和冲突：

1）时序匹配设计，基于各二级控制器的运行时序和传输延迟，统筹考虑主计算机小帧分区任务调用时序和总线传输的时序分配，既要保证任务调度在分配的时间周期段能够执行完毕，又要保证任务的调度与总线数据的收发匹配；

2）低延迟设计，优先传输飞行控制所需参数，确保主计算机使用当前最新的数据进行控制律计算，一旦运算完成，立即将控制指令通过总线传输给各二级控制器；

3）总线固定偏移设计，系统总线数据包设置了固定的发送偏移，保证系统总线数据包的发送相对于每个周期时钟基准点的时序确定性；

4）总线负载均衡设计，对分布式系统总线的负载进行综合设计，确保各条总线上的负载能力相当。

分布式飞控系统传输延迟示意图和综合运行时序调度示意图如图5～图6所示。

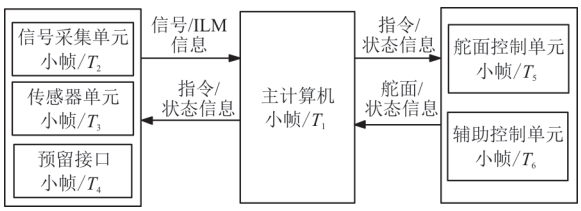

图5 分布式飞控系统传输延迟示示意图

Fig. 5 Distributed FCS transmission delay diagram

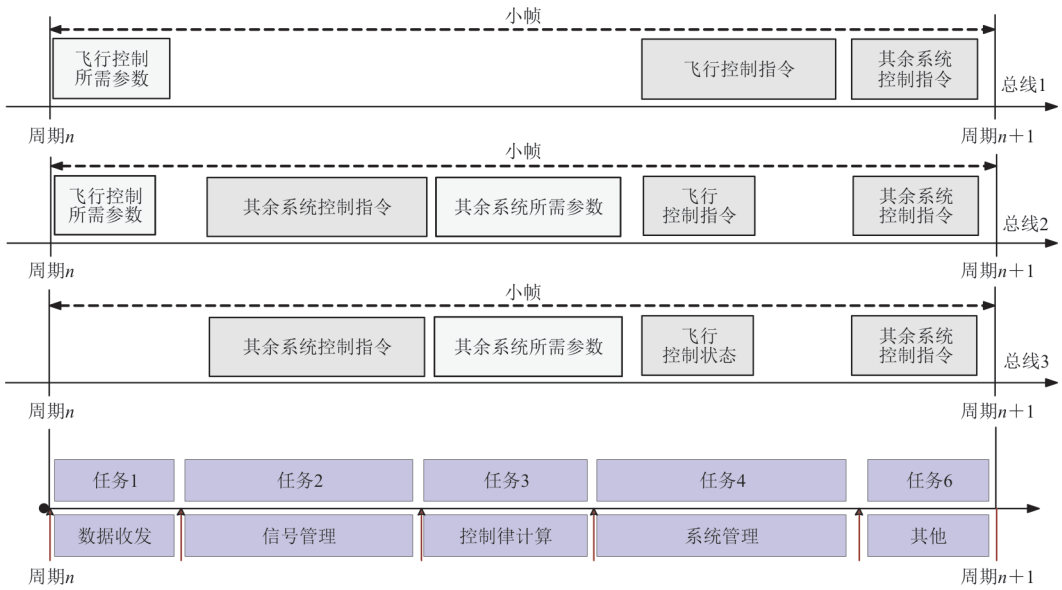

图 6　分布式飞控系统运行时序意图

Fig. 6　Distributed FCS typical operation diagram

3　分布式系统表决/监控面设计

根据分布式系统的组成和体系构架特点,飞控系统设置四级表决/监控面,检测不同层级的信号或部件故障,并从系统中剔除。一级/二级表决监控在主计算机中实现,三级/四级表决监控在二级控制器中实现,如图 7 所示。

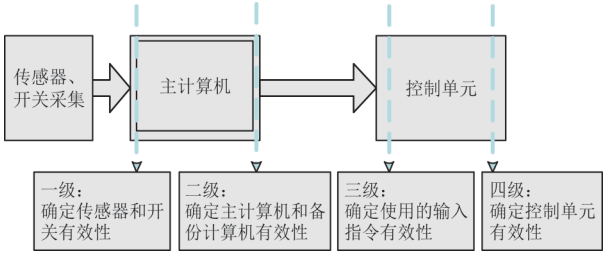

图 7　分布式系统表决/监控面设置

Fig. 7　Distributed FCS voting/monitor set diagram

3.1　一级表决/监控

第一级表决/监控的目的是消除前端输入信号故障对控制律计算的影响,防止故障蔓延。由主计算机对各类余度输入信号进行输入表决监控,以及时剔除故障的余度信号,为控制律计算提供正确的输入,并将各类信号的可用性通报控制律,确保其可根据获取的信息对飞机控制进行优化或重构,使信号损失对飞机安全性、性能的影响降至最低。主要包括下述内容:

1) 系统总线监控,检查总线数据传输及负载内容的有效性,包括:心跳字监控、软件奇偶校验和特定的状态字信息等;

2) 控制器状态监控,检查控制器余度有效性、工作状态是否正常、信号状态是否有效,剔除控制器异常或信号无效的余度;

3) 信号表决监控,根据飞控传感器和开关的余度配置及特点,对系统使用的多余度模拟和离散信号(如驾驶杆指令、三轴角速率/过载、轮载等信号)进行多数表决监控,并将有效的信号送控制律使用。

对总线监控异常、控制器工作异常的部件或信号,系统直接丢弃不予采用;对多余度信号,通过一致性比较监控,隔离错误通道,再采用多数表决方式计算正确的输入信号供控制律使用。

3.2　二级表决/监控

第二级表决/监控的目的是检测和隔离主计算机的故障。对各通道主计算机的输出指令进行比较监控,并获取通道的运行状态,采用通道故障逻辑监控各通道主计算机的 CPU 状态正确性,且通过离散输出将判断结果传输到各通道。同时,将主计算机的有效状态通过硬件在总线网络中进行广播,供二级控制器使用。主计算机中的二级表决监控算法示意图如图 8 所示。

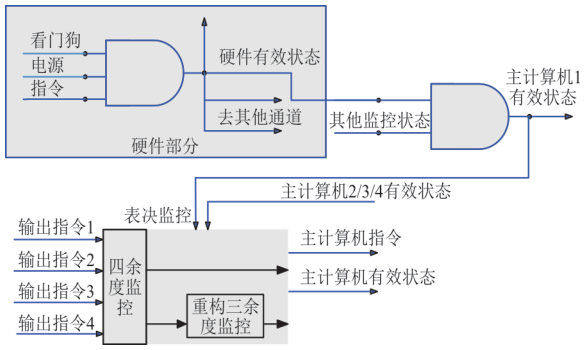

图 8 主计算机中的二级表决监控算法示意图

Fig. 8 Channel fail logic voting/monitor method diagram

与传统的输出表决/监控算法不同，此监控器的指令不直接对操纵面的伺服控制回路产生影响。在本级的算法中，对主计算机的有效性进行判断后，由二级控制器按三级表决/监控算法具体确定使用哪一个主计算机的指令。

3.3 三级表决/监控

第三级表决/监控主要在各二级控制器中进行，主要目的是确定二级控制器选择正确的主计算机输入指令，基本选择逻辑示意图如图 9 所示。二级控制器的表决/监控主要包括：输入信号监控、总线输入数据的监控、主计算机输入指令监控和控制指令选择。

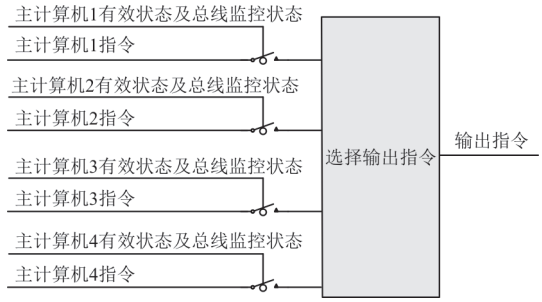

图 9 二级控制器的指令选择逻辑示意图

Fig. 9 Remote controller command select logic

输入信号监控是各二级控制器对自身产生的模拟和离散信号的监控，主要采用多余度的表决监控算法。

总线输入数据的监控主要针对本通道接收的主计算机数据包的正确性进行，监控内容包括总线数据负载的心跳和校验结果等。

3.4 四级表决/监控

与集中式控制方式相比，采用分布式系统构架后，二级控制器执行了部分原本由飞控计算机执行的功能，因此，在二级控制器中执行的第四级表决/监控主要原自集中式构架中飞控计算机的部分功能。

二级控制器需要对自身的数字器件、电源、关键电路、所控制的执行机构进行监控，以确定本通道是否参加对操纵面的控制。

以操纵面控制单元为例，简要说明四级表决/监控的具体实现，如图 10 所示。对二级控制器的工作状态监控主要采取下述措施：

1）输出指令监控，采用多余度比较监控算法；

2）CPU 运行状态监控，包括电源、看门狗等；

3）伺服作动系统监控，包括控制模型比较监控、驱动电流监控和液压系统压力状态监控等。

当检测出某通道输出指令错误、CPU 故障或伺服作动系统故障时，及时切除该通道对操纵面的驱动控制。若所有控制通道均故障，可对主操纵面采用主动回中、辅助操纵面采用锁定当前位置的安全策略，控制律根据操纵面故障情况进行重构，以降低操纵面丧失对飞行控制的影响。

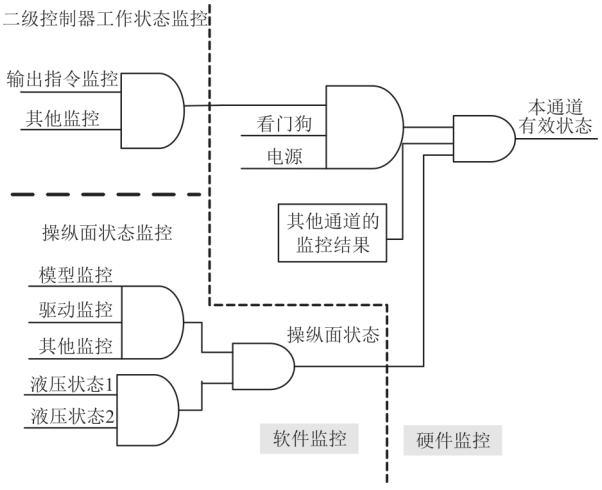

图 10 二级控制器的输出表决监控算法示意图

Fig. 10 Remote controller channel fail logic diagram

4 结 论

1）本文所研究的飞控系统容错设计技术已应用于相关型号研制，并取得了良好的工程效果。与集中式系统不同，分布式系统中存在多个智能部件，通过表决监控面的合理设置并在各一级、二级控制器中合理分配监控功能，一方面避免了集中式系统中单一故障导致整个系统丧失一个通道

的缺陷,另一方面降低了主计算机、二级控制器、系统总线数据参数异常、故障后对系统运行的不利影响。

2) 集中式系统的同步主要通过飞控计算机实现,一旦飞控计算机失步,则可能导致对应控制通道失步。分布式系统通过系统总线管理系统各余度间的时序同步,主计算机完成同步后,通过自身的系统总线向二级控制器通报本余度分支的同步信息,一旦主计算机发生故障,系统总线将通过专用处理逻辑自动按照小帧等时完成系统同步信息发布,降低了主计算机故障的影响。

3) 系统总线用于系统内各成品之间,以及飞控系统与其他系统之间进行数字信息传递,是飞行安全的重要保障。根据总线的运行/传输特征、各控制器的运行特征,设置专用的软、硬件监控措施,确保通信正确,提高了飞控系统的安全性和可靠性。

参 考 文 献

[1] 史国荣. 民机飞控系统数字总线应用分析[J]. 现代导航, 2016, 7(2): 107-112.
SHI Guorong. Analysis of digital bus of civil flight control system[J]. Modern Navigation, 2016, 7(2): 107-112. (in Chinese)

[2] 沈磊. 大型民用飞机新型飞控作动系统浅析[J]. 中国制造业信息化, 2012, 41(23): 67-71.
SHEN Lei. Analyses on large civil aircraft flight control actuator system[J]. Manufacture Information Engineering of China, 2012, 41(23): 67-71. (in Chinese)

[3] 占正勇, 刘林. 分布式电传飞行控制系统结构发展及分析[J]. 飞行力学, 2009, 27(6): 1-4,9.
ZHAN Zhengyong, LIU Lin. Architecture analysis and development of distributed FBW flight control system [J]. Flight Dynamics, 2009, 27(6): 1-4,9. (in Chinese)

[4] 徐艳玲, 崔玉伟, 罗川. 新一代分布式飞行器管理系统技术研究进展[C]// 第37届中国控制会议论文集. 武汉: 中国自动化学会, 2018: 10088-10092.
XU Yanling, CUI Yuwei, LUO Chuan. Research advancement for the new generation of distributed vehicle management system[C]// Proceedings of the 37th Chinese Control Conference. Wuhan: Chinese Association of Automation, 2018: 10088-10092. (in Chinese)

[5] HARRIS J J. F-35 flight control law design, development and verification[C]// 2018 Aviation Technology, Integration, and Operations Conference. Atlanta, Georgia: AIAA, 2018: 3516-3523.

[6] 路红飞. 三余度飞行控制计算机容错技术研究[D]. 南京: 南京航空航天大学, 2020.
LU Hongfei. Research on computer fault-tolerant technology of three-redundancy flight control[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2020. (in Chinese)

[7] 解文涛, 王锐. 基于分级容错技术的高完整计算机系统设计[J]. 电光与控制, 2019, 26(10): 106-110.
XIE Wentao, WANG Rui. High-integrity computer system design based on hierarchical fault-tolerant technology [J]. Electronics Optics & Control, 2019, 26(10): 106-110. (in Chinese)

[8] 柳孔明, 徐宏哲, 黄俊. 三余度飞控计算机架构及其可靠性研究[J]. 现代电子技术, 2012, 35(6): 102-106.
LIU Kongming, XU Hongzhe, HUANG Jun. Research on architecture of triple-redundant flight control computer and its reliability[J]. Modern Electronics Technique, 2012, 35(6): 102-106. (in Chinese)

[9] NATALE L, BERDUGO A. 1 overview of F-22 upgraded instrumentation system [C] // International Telemetering Conference 2007. Las Vegas, NV: International Foundation for Telemetering, 2007: 1-6.

[10] ROBBINS D, BOBALIK J, DE STENA D, et al. F-35 subsystems design, development & verification[C]// 2018 Aviation Technology, Integration, and Operations Conference. Atlanta, Georgia: AIAA, 2018: 1-15.

[11] BRIERE D, TRAVERSE P. AIRBUS A320/A330/A340 electrical flight controls-a family of fault-tolerant systems [C] // FTCS-23 the Twenty-Third International Symposium on Fault-Tolerant Computing. Toulouse, France: IEEE, 1993: 616-623.

[12] UZUNCAOVA E, AYALA M A. Boeing 777 flight control system[R]. Monterrey, Californi: Naval Postgraduate School, 2013.

[13] CULLEY D E, THOMAS G L, ARETSKIN-HARITON E. A network scheduling model for distributed control simulation[C]// 52nd AIAA/SAE/ASEE Joint Propulsion Conference. Salt Lake City, UT: AIAA, 2016: 4652-4667.

[14] 王兴坚, 杨新宇, 王少萍. 大型民机操纵系统容错控制技术综述[J]. 机械工程学报, 2024, 60(4): 50-65.
WANG Xingjian, YANG Xinyu, WANG Shaoping. Review of fault-tolerant control for flight control system[J]. Journal of Mechanical Engineering, 2024, 60(4): 50-65. (in Chinese)

[15] 吴文海, 高阳, 汪节. 飞行控制系统的发展历程、现状与趋势[J]. 飞行力学, 2018, 36(4): 1-5,10.
WU Wenhai, GAO Yang, WANG Jie. Development course, status and trend of flight control system[J]. Flight Dynamics, 2018, 36(4): 1-5,10. (in Chinese)

(编辑:马文静)