文章编号:1671-4598(2021)03-0099-05 DOI:10.16526/j.cnki.11—4762/tp.2021.03.020 中图分类号:V19 文献标识码:A

机载机电管理系统通道故障逻辑设计

吴凌涵,杨雪巍,卢 毅,朱晓丹,邓 林
(中国航空工业集团 成都飞机设计研究所,成都 610041)

摘要:机载机电系统是保障飞机正常运行的重要系统,为了提高双通道机电管理系统的任务可靠性,对系统容错和重构管理技术进行研究,提出了一种适用于机载双通道机电管理系统的通道故障逻辑设计;该设计的特点在于以本通道自监控策略为核心,并结合它通道的辅助监控和强制切除能力,实现故障的准确定位和有效隔离,从而避免故障影响的进一步扩散,同时该设计还具备故障复位能力,进一步提高系统冗余度;从分析和仿真结果可以看出,该设计有效地提高了双通道机电管理系统的稳定性和任务可靠性,并且可以应用到更高余度通道的系统中,具有良好的应用前景。

关键词:双通道;机电管理系统;通道故障逻辑;系统容错;重构管理

Design of Channel—Failure—Logic for Airborne Electromechanical System

Wu Linghan, Yang Xuewei, Lu Yi, Zhu Xiaodan, Deng Lin
(AVIC Chengdu Aircraft Design and Research Institute, Chengdu 610041, China)

Abstract: Electromechanical system is an important system to ensure the normal operation of the aircraft. In order to improve the reliability of the double redundancy electromechanical management system, this paper studies on the techniques of system fault—tolerance and reconfiguration management, and present a design of Channel—Failure—Logic for airborne double redundancy electromechanical management system. The features of this design is it takes the self—monitoring strategy as the core, and combines the other channel's auxiliary monitoring and forced resection, to realize accurate location and effective isolation of failure, thereby avoiding the further diffusion of failure effect. Meanwhile, the design has the function of fault reset, which can improve the redundancy of the system. Analysis and simulation results show that, this design can effectively improve the stability and reliability of the double redundancy electromechanical management system, and it can be applied to higher redundancy system, thus it has a good application prospect.

Keywords: double redundancy; electromechanical management system; channel—failure—logic; system fault—tolerance; reconfiguration management

0 引言

飞机机电系统主要由燃油系统、环控系统、供电系统、液压系统、动力系统、应急动力系统、刹车系统等组成,是飞机的重要平台系统,用于保障飞机的正常运行[1-2]。

为了提高飞机可靠性、维修性和保障性,并为飞机减重、减体积[3],需对飞机机电系统的功能进行整合,并采用机电系统综合化设计技术[4],形成机载机电管理系统(utility—subsystem management system, UMS)。UMS通过整合资源提高了飞机机电系统综合化水平,但是系统故障失效时对飞机安全性的影响面也变得更大。因此为提高系统的可靠性和安全性[5],结合经济性等系列因素权衡,UMS一般会采用双通道的余度设计。对于双通道冗余设计,如果系统不能正确识别故障通道,会导致输出错误指令,反而会降低系统的可靠性和安全性,因此通道故障逻辑(channel failure logic, CFL)的设计显得尤为重要。

然而,现阶段双通道系统的通道故障逻辑设计仍是短板,通常存在以下问题:①各通道只监控自身状态[6-7],当故障状态下自监控失效时,可能出现本通道工作异常,但无法切除故障通道的情况,造成系统功能丧失;②对故障模式的考虑不够全面[8],对故障的隔离能力有限;③通常不具备故障复位的能力。因此本文对通道故障逻辑的容错和重构技术进行研究,提出了一种新型的通道故障逻辑设计,可以有效地识别和隔离故障通道,保证双余度系统的高可靠性运行。

1 双通道机电管理系统架构

双通道UMS的系统架构如图1所示,核心为机电管理计算机(utility—subsystem management computer, UMC)。两台UMC与相关组件协同工作,实现机电系统控制、故障监测及综合告警、数据送显,以及维护等功能。

两台UMC以完全对等的方式处理余度数据信息,运行机电监控和控制任务,信号以交叉数据链(cross channel data link, CCDL)互传的方式在2台UMC上形成完整的信号映射,实现数据共享。

机电各系统的状态信号,以双余度方式分别引入两台

收稿日期:2020-08-13; **修回日期**:2020-09-16。

作者简介:吴凌涵(1989-),女,成都人,硕士,工程师,主要从事机电系统综合设计方向的研究。

引用格式:吴凌涵,杨雪巍,卢 毅,等.机载机电管理系统通道故障逻辑设计[J].计算机测量与控制,2021,29(3):99-103.

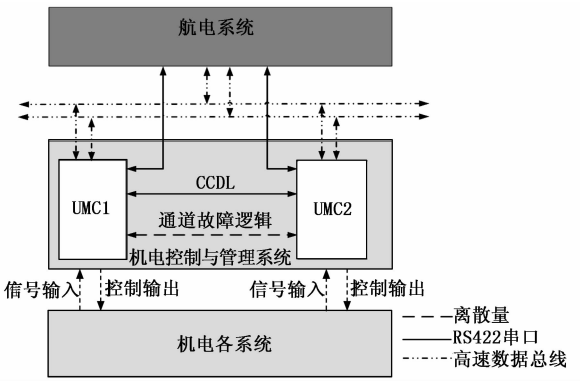

图 1 机电管理系统架构图

UMC，每台 UMC 会将自身采集的信号，和来自 CCDL 的它机采集信号进行比对，判断数据有效性，采信表决后的有效值，再进行系统控制律解算。

两台 UMC 的双余度任务运行方式，满足对机电各系统的监控和控制重要功能一次故障安全的要求。当一台 UMC 故障时，将自己的控制输出信号自锁，避免影响系统安全，此时对机电系统的监控和控制功能由另外一台 UMC 完成；当两台 UMC 均故障时，两台均将输出自锁，此时机电系统核心功能由座舱开关与电气控制盒实现，避免机电系统失控。

UMC 将故障信息和采集的机电系统重要参数，通过高速数据总线和 RS422 串口送航电系统进行处理[9]。飞机架构决定了两台 UMC 共用一个输出告警和显示通道，因此两台 UMC 以主、备方式运行和航电系统的通讯任务。通过故障通道逻辑保证在同一时刻，仅一台 UMC 能向总线发送数据。通道故障逻辑设计的关键是要避免双机都抢总线权，和双机都放权这两种情况。

2 通道故障逻辑设计

本文基于对通道故障逻辑设计关键要素的分析，提出一种新型的通道故障逻辑设计，该设计以本机自监控为主，它机监控和强制切除为辅，有效地实现故障定位和隔离。

2.1 故障定位和隔离

本文提出的通道故障逻辑设计架构如图 2 所示。

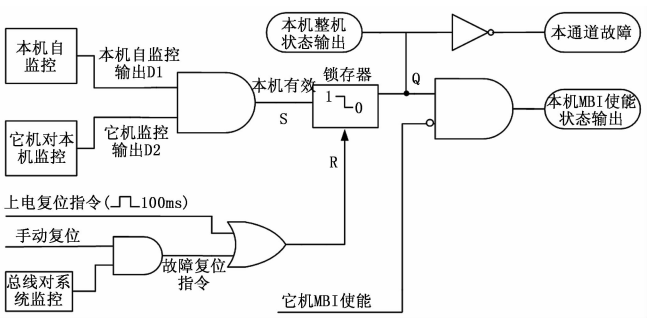

图 2 CFL 电路架构

本设计增强了通道故障监控的完备性，覆盖了以下 3 种情况：①当本机故障时，若本机自监控有效，可自身进行故障隔离；②当本机故障，且本机自监控失效时，可通过它机监控强行切除本通道，并改由它机接管系统；③当双机失效时，可通过总线对系统的监控，进行故障提醒和故障自动复位。

2.1.1 本机自监控

本机自监控电路如图 3 所示。

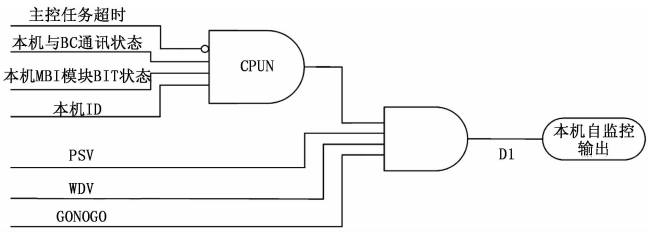

图 3 本机自监控示意图

本机自监控电路的输入包含了影响通道状态的所有关键要素，当所有输入均为正常状态时，本机自监控输出才为有效（正常）；一旦某个输入出现异常，可通过 CFL 正确定位到通道故障，并且可结合非易失存储器（non－volatile memory，NVM）中的故障记录信息，对故障原因进行排查。

该设计的关键输入包含以下内容。

1）处理器有效（central－processing－unit valid，CPUV）：

CFL 对影响系统运行的关键状态进行了监控，包含主控任务、航电处理任务以及机位信息。

UMC 通过定时器对自身软件的主控任务进行监控，若主控任务超时，则认为任务监控故障，会触发 CFL 报故，并将故障记入 NVM。另外，两台 UMC 需正确识别自己的机位，以保证系统工作的时序性和确定性。

若 UMC 的航电处理任务出现异常，也会触发 CFL 报故。因为总线通讯任务的失效，可能会造成总线不能正确从该通道获取数据，需要 CFL 切换通道，由另外一台 UMC 将双机的重要信息发送到航电系统。航电处理任务的监控分为两方面，一方面若总线接口板（max bus interface，MBI）硬件 BIT 故障，会引发报故，另一方面，UMC 自身会对总线通讯状态进行监控，若连续多拍未收到总线数据，或连续多拍数据发送失败，会引发报告航电处理任务异常，触发 CFL 报故。

2）电源监控有效（power supply valid，PSV）：

由电源模块对二、三次电源进行监控，并将监控到的电源信号值送往 CFL 进行处理，CFL 将该信号与期望值进行比对，若差值在容差范围内，则认为正常，否则认为电源故障，触发 CFL 报故并将故障记入 NVM。

3）看门狗有效（watchdog valid，WDV）：

若软件关键任务不及时喂狗，会触发看门狗叫。该设

计的输入包含了表征关键任务运行状态的看门狗故障。

4）加载表征信号（GONOGO）：

本设计引入了用于表征 UMC 的处理器（central－processing－unit，CPU）是否已完成加载的 GONOGO 信号。该信号通过下拉电阻接地，UMC 在上电复位的过程中，该信号保持为无效，UMC 完成复位后信号为有效。将 GONOGO 作为 CFL 的输入，可保证 UMC 在逻辑加载过程中，置自身整机状态无效，不抢占总线权，不参与对它机监控。

2.1.2　它机对本机监控

它机对本机监控的架构如图 4 所示。本通道故障时，为防止本机不能正确识别自身状态，造成故障隔离失效，需要通过它机的监控结果进行故障隔离。

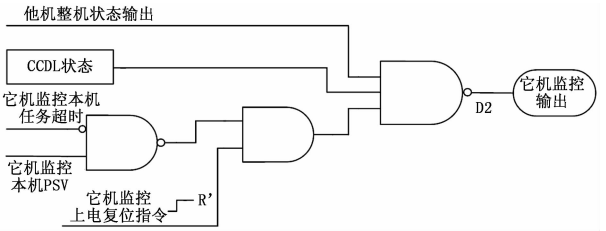

图 4　它机对本机的监控示意图

它机监控是作为本机监控的备份使用，当它机监控到本通道故障时，可以强行切除本通道。为了避免它机误切除本通道的情况，它机监控的设计应该更为谨慎。因此本设计中，在它机自身整机工作正常的情况下，它机监控才有效，一旦它机整机状态输出异常，会直接关闭对本机的监控。它机通过 CCDL 获取本机的任务运行情况和 PSV 状态来进行监控，因此该设计是在监控到双机之间的 CCDL 传输通道正常的情况下，才采信收到的状态值，保证监控信息的有效性。

产品刚上电时，“它机监控上电复位指令”为无效，不参与对对方的监控；当产品进入正常工作模式后，再自身触发出复位指令，才开始监控对方。通过复位指令，避免了 UMC 上电复位期间，误切除对方通道的情况。

2.1.3　总线对系统监控

两台 UMC 与航电的总线通信采用热备份的余度方式。航电总线会周期查询 UMC 在线情况，UMC 也周期回复状态。当 UMC 故障时，通过 CFL 的本机自监控或它机监控，切换故障通道，由另一台 UMC 完成与航电系统的总线通讯，并向航电上报通道故障告警。

当两台 UMC 均故障，或通道切换出现异常时，UMC 无法给航电回复自身状态。航电未收到 UMC 回复的状态时，一方面在座舱指示 UMC 不在线告警；另一方面通过硬线触发 UMC 复位电路，进行 CFL 自动复位。

2.2　CFL 复位功能

该设计具备 CFL 上电复位和故障复位功能。UMC 完成上电加载后，会自动产生“CFL 上电复位信号”，CFL 上电复位信号与机位进行了关联，A 机的 CFL 上电复位信号早于 B 机，从而保证 A、B 机同时上电时，由 A 机占取总线权；当双机上电不同步时，则由先上电的产品占取总线权。

工作过程中发生通道故障时，正常情况下 CFL 电路能自动定位和切除故障通道，并上报通道故障的提示。飞行员或机务人员，可根据当前实际工况进行判断，决定是否手动按压故障复位开关。收到“故障复位指令”后，若该通道故障已消除，则可清除本通道故障的指示，但不会抢占它通道总线权。若两台 UMC 均故障或通道切换出现异常时，航电系统会通过硬线触发 UMC 的 CFL 电路自动复位。

复位功能通过锁存器实现，图 2 中锁存器的功能如表 1 所示，具体设计原理见章节 3.3。

表 1　锁存器功能

本机有效(S)	复位(R)	输出
1	0	保持
0	0	0
0	1	0
1	1	1

2.3　安全态的保证

该设计能够保证 CPU 上电复位阶段和通道故障时，系统都处于安全态。

CPU 上电复位阶段通过 GONOGO 信号置本通道故障为存在；上电或工作过程中通道异常时，可通过自监控或它机监控置本通道故障为存在。一旦通道故障存在，MBI 使能状态输出为不使能状态，可保证不占取总线权。

另外，软件初始化时会将输出置于安全态；工作过程中检测到通道故障时，UMC 软件会将通道输出锁定为无效状态，切断输出控制信号，避免对系统安全造成影响。

2.4　上电自检测

CFL 上电时，会对自身状态进行自检测，保证 CFL 电路自身正常。若自检测失败，则向航电系统报出 CFL 失效故障，并将检测结果记录在 NVM 中。

3　通道故障逻辑工作原理

CFL 主要应用于两个工作场景：①上电初始化阶段，通过 CFL 保证系统初态的稳定性；②工作过程中，若通道故障时，通过 CFL 正确定位和切除故障通道。

CFL 同时存在于 A 机和 B 机中，下面结合图 2～4，从 A 机的角度对通道故障逻辑的工作原理进行介绍。

3.1　上电复位阶段

A 机上电复位过程中，通过 GONOGO 信号保证本机自监控输出结果 D1 为无效，因此本机有效性 S 无效，此时 CFL 复位信号 R 无效，A 机本通道故障为存在，MBI 使能输出为不占权。A 机不会抢占总线权，并锁住本机控制输出，不参与对它机故障的判断。通过 CFL 保证了 UMC 在

上电或复位过程中不影响系统的正常运行。

若 A 机成功完成复位，则本机自监控输出结果 D1 有效，此时包含以下两种情况：

1）B 机复位不成功或 B 机在复位中，则 B 机不参与对 A 机故障的判断，此时 S 有效，A 机自动进行 CFL 上电复位后，A 机 MBI 使能输出为占权，A 机本通道故障为不存在；

2）B 机复位成功，并监控到 A 机工作正常，此时 S 有效，A 机保持 MBI 使能输出为占权，A 机本通道故障为不存在。

若 A 机复位不成功，此时包含以下两种情况：

1）B 机复位成功并监控到 A 机工作异常，它机对本机监控 D2 无效，因此本机有效性 S 为无效，A 机 MBI 使能输出为放权，A 机本通道故障存在，B 机通过 CFL 占取总线权和系统控制权；

2）B 机复位不成功，总线检测到双机故障，给出故障提示，并进行 CFL 自动复位。

3.2 工作过程中

A 机上电复位成功后占取总线权，然而工作过程中 A 机出现故障，此时包含以下 3 种情况：

1）A 机自监控到自身故障，本机自监控输出结果 D1 无效，本机有效性 S 为无效，A 机 MBI 使能输出为放权，A 机本通道故障存在，由 B 机接管；

2）A 机丧失自监控能力，B 机监控到 A 机工作异常，它机对本机监控 D2 无效，本机有效性 S 为无效，A 机 MBI 使能输出为放权，A 机本通道故障存在，由 B 机接管；

3）B 机工作异常，总线检测到双机故障，给出故障提示，并进行 CFL 自动复位。

A 机工作异常后，可通过自监控或它机监控，保证 A 机放权。此时打开了对 B 机总线接口的锁定，若 B 机工作正常，可以接管总线权。

A 机故障后，若收到故障复位指令，此时包含以下两种情况：

1）A 机未恢复正常，本机有效性 S 为无效，此时进行 CFL 故障复位，A 机本通道故障保持为存在；

2）A 机恢复正常，本机有效性 S 为有效，此时进行 CFL 故障复位，A 机本通道故障为不存在，可解除对 A 机控制输出的锁定。

不管 A 机是否恢复正常，此时 B 机已经占取总线，A 机收到的它机 MBI 使能为占权，因此 A 机 MBI 使能输出保持为放权，不会抢占总线权。

3.3 锁存器设计

根据锁存器功能需求，写出锁存器的真值表，如表 2 所示。

根据真值表，可写出逻辑表达式：

$$Q' = SR + SQ = S(R+Q) \qquad (1)$$

表 2 锁存器真值表

本机有效(S)	复位(R)	Q(上周期输出)	Q'(本周期输出)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	1	0	1
1	1	1	1
1	0	0	0
1	0	1	1

其逻辑图如图 5 所示。

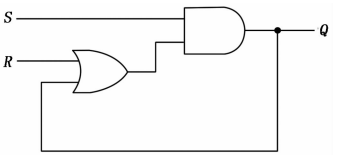

图 5 锁存器设计原理图

4 仿真验证

前面主要从 A 机的角度对 CFL 的工作原理进行了介绍，下面通过 Simulink 搭建仿真模型[10]，对 A 机和 B 机协同工作的真实场景进行模拟，仿真架构如图 6 所示，其中图 2～4 所示的通道故障逻辑电路封装于仿真模块内。

4.1 上电中发生故障

模拟 A 机上电过程中发生故障的情况，仿真结果如图 7 所示。

从图 7 看出，时刻①，A 机 CFL 上电复位，同时注入 A 机故障，A 机检测到自身故障，将 A 机通道故障状态保持为故障态，MBI 使能状态保持为放权。时刻②，B 机 CFL 上电复位成功后，B 机通道故障切换为正常态，B 机监测到 A 机未占权，B 机 MBI 使能状态切换为占权。时刻③，故障注入结束，A 机通道故障状态保持为故障态，MBI 使能为放权。时刻④，进行 A 机故障复位，A 机通道故障状态切换为正常态，B 机已占权，A 机 MBI 使能状态保持为放权。

仿真结果证明该设计可以在上电复位阶段通过本机监控实现故障定位和隔离；并具备故障通道复位功能。

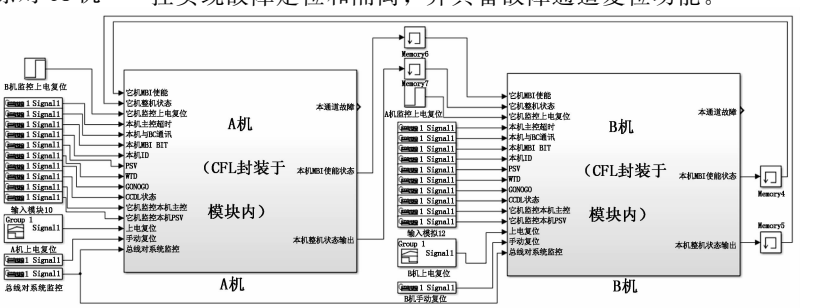

图 6 仿真架构图

图 7　上电中发生故障的仿真结果

4.2　工作中发生故障

模拟 A 机和 B 机均正常上电，A 机取得输出权，工作过程中 A 机发生故障，然后进行故障复位操作。仿真结果如图 8 所示。

图 8　工作中发生故障的仿真结果

从图 8 看出，时刻①，A 机 CFL 上电复位成功后，A 机通道故障状态从复位前的故障态切换为正常态，MBI 使能状态切换为占权。时刻②，B 机 CFL 上电复位成功后，B 机从复位前的故障态切换为正常态，此时 A 机已占权，B 机 MBI 使能状态保持为放权。时刻③，注入 A 机故障，A 机通道故障状态切换为故障态，MBI 使能状态切换为放权，B 机抢占总线权。时刻④，故障注入结束，A 机通道故障状态保持为故障态，MBI 使能为放权。时刻⑤，进行 A 机故障复位，A 机通道故障状态切换为正常态，此时 B 机已占权，A 机 MBI 使能状态保持为放权。

仿真结果证明该设计在上电复位成功之前，可以保证通道输出为故障状态；在工作中发生故障后，能通过本机或它机监控实现故障定位和隔离，并进行总线权的切换；并且具备故障通道复位功能。

5　结束语

本文对通道故障逻辑的原理和设计要素进行了分析，开创性地提出了一种适用于机载双通道 UMS 的新型通道故障逻辑设计。分析和仿真结果表明，该设计能够正确定位故障通道，并有效进行故障隔离，切除故障通道；可在上电复位阶段和通道故障时，保证系统工作在安全态。该设计在不降低安全边界的情况下，极大地提升了高层级安全系统的双余度架构的容错能力和任务可靠性，保障机电管理系统正确地实现机电系统控制、故障监测及综合告警等功能，可为后续的改进提供重要的参考依据。本文的设计理念可推广到其他分布式机电综合系统的设计与应用中，具有广阔的应用前景。

参考文献：

[1] 孙　沛，陈　奎. 机载分布式机电系统的容错和重构 [J]. 测控技术，2014，33 (3)：80－85.

[2] 尚利宏，阮俊波，张　锐，等. 机载 UMS 分布式容错计算机系统设计 [J]. 北京航空航天大学学报，2001，27 (4)，396－399.

[3] 聂同攀，梁　伟. 基于模型的飞机机电综合管理系统设计应用研究 [J]. 航空科学技术，2017，28 (6)：74－78.

[4] 张晓艳，王铁勇. 基于机载机电控制与管理计算机 (UMC) 容错技术的研究 [J]. 微电子学与计算机 2008，25 (12)：125－127.

[5] 陈　福，王山虎，段海军，等. 飞机机电核心处理机余度管理技术研究 [J]. 信息通信，2016 (10)：29－30.

[6] 徐　杰，张　蕾，张　弛，等. 双余度机载计算机余度管理及其实现方法研究 [J]. 信息通信，2016 (3)：85－86.

[7] 闫　稳. 机载供电系统双余度控制器的容错控制 [J]. 航空计算技术，2010，40 (4)：86－88.

[8] 张　辉. 飞控双余度联合控制机制研究 [J]. 信息通信，2017 (8)：34－35.

[9] 周前柏，赵　刚，李爱军. 1394b 总线在机电综合管理系统设计中的应用 [J]. 设计与研发，2017 (13)：34－35.

[10] 黄新阳，董延军，胡佳林，等. 飞机供电系统容错供电 MATLAB 仿真 [J]. 测控技术，2015 (34)：63－66.

(上接第 98 页)

[5] 成　勋，周　铁，孙　侃，等. 基于小波去噪振动加速度信号处理及时频域积分方法研究 [J]. 电力与能源，2019，40 (6)：633－637.

[6] 张　朵，彭瑞元. 一种飞机振动测试系统设计 [J]. 中国科技信息，2019 (5)：31－32.

[7] Jin T，Liu Z，Sun S，et al. Theoretical and experimental investigation of a stiffness－controllable suspension for railway vehicles to avoid resonance [J]. International Journal of Mechanical Sciences，2020，187.

[8] 王昌林，付艳丽，刘琳琳. 振动测试技术在内燃机结构设计中的应用 [J]. 内燃机与配件，2019 (12)：171－172.

[9] 唐　源. 基于 LXI 总线的高速高精度数据采集器的研制 [J]. 电子技术与软件工程，2020 (20)：78－79.

[10] 杨建业，范小虎，常　伟，等. 基于 LXI 总线的液浮陀螺稳定平台自动化测试系统设计与实现 [J]. 计算机测量与控制，2019，27 (9)：8－12.