引用格式:刘利加,曹东,王余伟. 主从式双余度飞控计算机容错策略研究[J]. 电光与控制,2017,24(7):95-99. LIU L J, CAO D, WANG Y W. Fault tolerant strategy for master-slave dual redundancy flight control computer[J]. Electronics Optics & Control, 2017, 24(7):95-99.

主从式双余度飞控计算机容错策略研究

刘利加, 曹 东, 王余伟
(南京航空航天大学自动化学院,南京 211106)

摘 要: 针对样例主从式双余度飞控计算机体系架构,提出一种容错管理策略,设计了系统故障检测与诊断、系统资源管理、故障恢复等算法。在无人机半物理仿真平台下进行了容错策略算法测试,结果表明,该容错策略正确,算法功能和性能满足工程应用需求。

关键词: 飞行控制计算机; 双余度; 容错; 无人机
中图分类号: V249.1 **文献标志码**: A **doi**:10.3969/j.issn.1671-637X.2017.07.020

Fault Tolerant Strategy for Master-Slave Dual Redundancy Flight Control Computer

LIU Li-jia, CAO Dong, WANG Yu-wei
(College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

Abstract: Aiming at system architecture of the master-slave mode, dual redundancy flight control computer, a fault tolerant management strategy is proposed, and the algorithms are presented for system fault detection and diagnosis, system resource management, and fault recovery. The fault tolerant strategy algorithm is tested under the UAV semi-physical simulation platform. The results show that the strategy is correct, and the function and performance of the algorithm can meet the engineering application requirements.

Key words: flight control computer; dual redundancy; fault tolerance; UAV

0 引言

无人机是一种机上无人驾驶、可循环使用、能够进行自主或者半自主飞行、携带设备执行复杂任务并由动力驱动的航空器,无人机的多种优势使其在军用和民用领域得到广泛的应用。飞控系统是无人机的控制核心,而飞行控制计算机又是控制系统的最关键核心,综合调度与管理所有飞行控制系统的所有单元模块,完成飞行控制任务以及其他各项功能[1]。飞控计算机已经具有很高的可靠性,但若不考虑其故障失效状况,一旦其发生故障,必使无人机失控,造成灾难性损失。

无人机容错飞控系统要求系统体积小、重量轻、低功耗和低成本。在满足安全可靠性前提下降低成本,是设计无人机容错飞控计算机时需要重点考虑的因素之一。针对无人机容错飞控计算机的特点,提出一种基于FlexRay总线主从容错飞控计算机体系结构。FlexRay具有以下特点:1) 快速性,独立通道的传输速率可以达到10 Mbit/s;2) 确定性,采用时分多址机制,在确定的时间片内传输确定的消息,接收端可提前获知相应数据的传输时间;3) 灵活性,支持总线型、星型和混合型多种网络拓扑结构,可根据实际需要选择双通道或者单通道进行数据传输,两个通道的数据传输互不影响;4) 容错能力,FlexRay标准通信协议提供了用户可灵活配置的容错协议[2]。

在这种体系结构下研究各种引发系统故障的情况并给出相应的容错策略,最后在无人机半物理仿真环境下,通过故障注入的方法验证了容错策略的正确性[3]。

1 主从容错式双机飞控计算机结构

本文设计的主从容错式双机飞控计算机系统由主控节点、FlexRay总线和接口模块组成。系统结构见图1。

主控节点是核心控制单元,主要负责控制逻辑解算,以及容错策略的实现;FlexRay总线是提供主控节点与接口模块之间数据信息与控制信息交互、主控节点间数据比较以及状态监控的“通道”,是容错策略得以实现的基础;接口模块是主控节点与外围设备连接

收稿日期:2016-07-05 修回日期:2017-04-10
作者简介:刘利加(1990—),女,壮族,广西崇左人,硕士生,研究方向为飞行器控制。

的“桥梁”,提供数字量、模拟量以及串口通讯接口。外围设备根据自身的接口特性与接口板相连,外围设备包括传感器设备以及执行机构,外围设备相关物理量测量关系以及与接口模块的连接关系见表1。

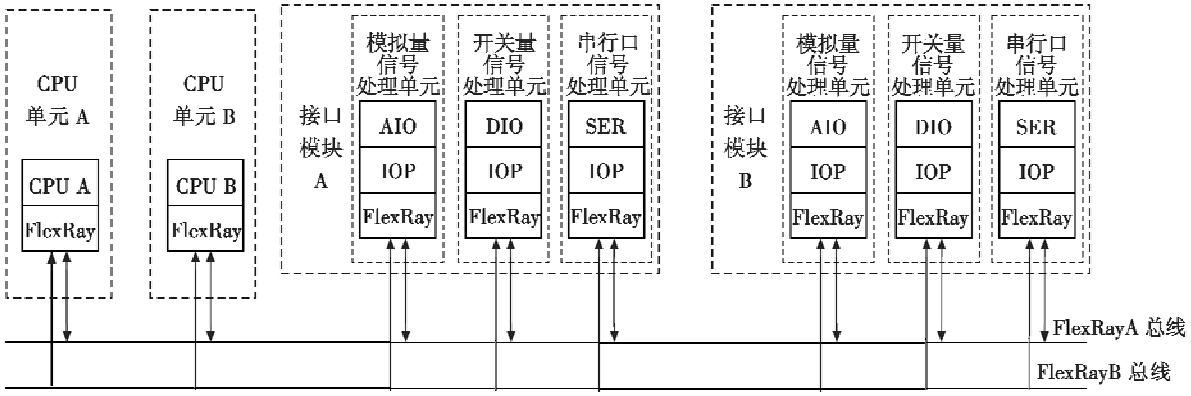

图1 系统结构图

Fig. 1 System structure diagram

表1 外围设备冗余信息一览表

Table 1 Redundant information list of peripheral equipment

物理量	接口模块A连接设备	接口模块B连接设备
姿态角	惯导	航姿
角速率	惯导	航姿
位置	惯导	GPS
高度	大气机	无线电高度表、GPS
速度	惯导	GPS
航迹航向	惯导	航姿
执行机构	左副翼、左升降舵、左方向舵	右副翼、右升降舵、右方向舵

从表1中可看出,所有物理量均具有冗余特性。体现在对于每一个传感器所测量的相关物理量,都可通过不同的传感器设备测量得出,即实现了传感器信息的冗余。当一路传感器信息出现故障时,可切换到其冗余信号设备。执行机构有左右升降舵、左右副翼以及左右方向舵。从控制逻辑的角度出发,采用舵面故障重构技术解决气动舵面故障后的安全控制[4]。结合外围设备的冗余特性以及接口模块自身的冗余特性,在接口设计中需对其进行合理分配,以充分发挥系统的容错性能。如表1所示,当整个接口模块均发生故障时可实现分配,采用另一接口模块仍能完成规定的任务。

因此,本文飞控计算机系统具有对传感器子系统、飞行控制计算机子系统和执行机构子系统的监控能力。若飞行控制计算机出现故障,通过飞行控制计算机系统的自检测(或互检测)能报告故障,并能将无效信号切除,将故障隔离。

这种架构体现了主从容错的设计思想,每个模块都具有其冗余备份。无故障情况下,主模块正常工作。当主模块发生故障时,备份模块可进行替换。主控节点工作状态如下。

1)两节点均正常工作,则其中一个为主节点,另一个为从节点。主节点具有总线输入输出控制权,从节点只从总线接收数据,而不对总线发送数据。

2)当主节点故障时,从节点接管总线输入输出控制权,主节点进行恢复操作。当主节点故障恢复时,向从节点发送恢复请求信号,从机通过总线向主节点发送恢复数据。主节点状态恢复完成后自动变为从节点身份。当故障不可恢复时,将其永久隔离,系统降级为单机模式,并停止双机容错相关操作。

3)当从节点故障时,工作方式类似2)所述,不同的是主节点始终掌握总线控制权。

由于双处理机系统具有极高的可靠性,两节点均发生故障的概率极小[5],所以这种状态本文暂不考虑,即认为系统至少有一个正常工作的节点。

2 容错策略设计与实现

结合系统的硬件体系结构,本文通过设计交叉通讯传输、故障检测与诊断、系统资源管理和故障恢复等策略实现系统容错功能。

2.1 交叉通讯传输

由系统结构图可知,交叉通讯链路采用FlexRay总线,其中,FlexRayA为主运行总线,FlexRayB为从运行总线。正常情况下采用FlexRayA总线通讯,当FlexRayA总线故障时采用FlexRayB总线。通过Flexray总线主控节点间传递系统全局状态信息以及任务运行信息以实现容错策略,主控节点与接口设备则通过该总线实现对I/O资源的管理和控制。其中,系统状态信息包括主节点编号、从节点编号、节点状态、节点平均无故障时间(MTBF)、节点负载和节点外设状态信息等,任务运行状态包括任务CPU使用率、堆栈状态和输入输出参数等,这些信息以数据包的形式在总线中传输。总线负责整个系统的数据流传输,因此

需要对其通讯状态进行检测，通讯状态检测可通过下文的心跳检测机制实现。

2.2　故障检测与诊断

双机飞行控制系统中快速准确的故障检测是一个非常重要的指标，对提高系统可靠性具有重要意义。本文中故障检测主要分为自检测和互检测两部分。

2.2.1　自检测

自检测是指处理机对自身状态进行检测，自检测主要基于软硬件实现。在实际工作过程中，飞控计算机容易受到外界电磁环境的干扰，造成软件中某些重要标志位发生变化，导致任务调度异常或程序失控[6]，因此必须对系统自身运行状态进行实时监测。自检测分为上电初始化检测，以及周期性检测。上电初始化检测只进行一次，主要对 CPU 功能模块进行自检测，周期性检测包括中断响应自检测、串口自检测、定时器自检测、离散量自检测、数字量自检测和 RAM 自检测等。

2.2.2　互检测

针对自检测技术不能及时地获取对方状态信息出现故障检测盲区的问题，采用互检测技术[7]，通过数据交叉通讯链路，相互检测对方运行状态，可为当前系统运行状态提供判断依据。应用互检测技术的必要性体现在当主控节点本身出现故障时无法对自身状态进行判断，此时必须由对方主控节点来判定。

互检测包括任务运行状态检测及心跳检测[8]。

任务运行状态检测主要基于应用级软件实现。在飞控计算机中，任务是双机飞控计算机中运行程序存在的主要形式，可视为一个独立的执行进程，每个进程完成一项特定的飞行控制任务。在任务运行期间，特别是对于一些数据计算性质的飞行控制任务，例如控制律解算任务，在解算过程中可能会发生非法指令、地址错误、浮点溢出、除零错误等，造成数值运算结果错误。导致任务运行出错，引发系统异常。

任务状态检测的原理是利用交叉通讯链路的硬件基础，两节点运行相同的任务程序，通过在运行期间的对比实现检错。若比对结果不一致，则进行相应的错误处理。

整个任务状态检测的算法如图 2 所示。

1）在需要检测的任务处调用检测接口函数，启动检测程序。

2）开始检测处理流程，主从控制节点处理流程如表 2 所示。

3）错误处理进程接收到从节点返回比对结果信息。若比对结果不一致，则认为该任务出错，并重启该任务重新计算。若在规定的时间范围内重启次数超过阈值，则判定该任务永久失效，需通过任务接管机制转移至对方节点运行。

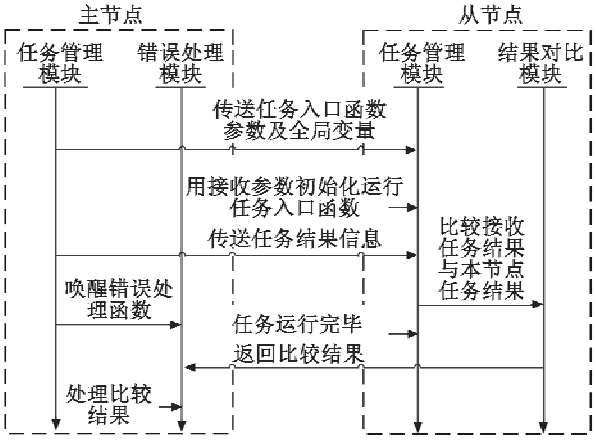

图 2　任务状态检测

Fig. 2　Task state detection

表 2　主从节点检测处理流程

Table 2　Master and slave node detection and processing flow

主节点	从节点
1）将任务入口函数的全局变量及输入参数传送至从节点。	1）接收主节点的任务入口函数的全局变量及输入参数。
2）执行任务入口函数。	2）利用接收的参数和全局变量，运行任务入口函数。
3）将运行完毕时的结果状态信息通过消息通信模块传送至从节点。	3）接收主节点的结果状态信息并传送到消息通信模块进行处理。
4）等待比对结果返回，激活错误处理进程。	4）进行结果状态比对并返回主节点错误处理进程。

只有在节点正常运行的情况下，任务状态检测结果才是可靠的。但是在节点失效的情况下，其检测结果将无意义。因此有必要建立心跳检测机制判别节点失效的情况。心跳检测是指通过双机数据交叉传输链路，主节点和备用节点周期性地互发节点监控信息。

两个节点之间互相建立对方的心跳计数器，在收到首个对方节点的节点心跳信号后开始计数。每收到一次对方心跳信号则对计数器清零，否则计数器累加。当累加数值超过某个阈值，引起一次失效报错。考虑到节点未发送节点监控信息不一定是节点失效的情况，还有可能是总线通信模块发生故障。这时先切换到备用总线，主节点再向从节点发送状态询问信号，若这时主节点还未收到反馈信号则判定为节点失效，否则判定为总线故障。

2.3　系统资源管理

2.3.1　主控节点主从控制权管理

每个节点在系统状态信息表中都有平均故障间隔时间（MTBF）记录，数据初值为 0。该信息用来作为主备竞争的依据。系统上电后，根据非易失性存储器中

的故障记录对节点状态进行评估,得出 MTBF。MTBF 值较大的节点竞选主节点成功,另一节点为备份节点。当两节点的 MTBF 值相等时,选择逻辑标号为"A"的节点为主节点。主节点每收到一次节点监控信息,MTBF 值增加一个时间周期,当节点失效重启时将 MTBF 重置为0,这样在主节点失效恢复后,其控制权将由备份节点接管。

2.3.2 I/O 资源管理

I/O 资源管理策略是在系统初始化时,将所有连接至各节点的外围设备情况登记于系统状态信息表内,该表存在于两 CPU 节点的非易失性存储器中,通过主节点周期性自检测对其进行定时刷新。当检测到外设发生故障时,主节点将其在系统状态信息表内的状态标记为失效,而将其备件状态标记为启动。通过总线广播 I/O 检测结果,将输入输出接口切换到标记启动的 I/O 资源,实现对系统 I/O 资源的管理。

2.3.3 任务管理

任务管理体现在任务接管机制的实现,任务接管是指正常节点将故障节点的任务在本节点中重新运行以得到正确结果的过程。下面2种情况需要进行任务接管:1) 由于某节点某硬件出现了故障,经过多次检测任务仍为故障状态,为了使任务正常运行,需要正常节点对其进行接管,从而得到正确的执行结果;2)整个节点发生了永久性故障,节点上所有任务失效,需将控制权整体转换到正常的节点。任务接管只需在主节点任务发生故障时,备用节点将对应任务启动即可,无需过程数据的大量迁移。

2.4 故障恢复

在系统出现故障时,首先通过故障检测与诊断技术对故障进行定位,对故障单元进行重组,实现对故障的屏蔽。当故障为永久性,将故障模块进行永久隔离。当瞬时性故障排除之后,恢复操作可使故障恢复节点重新加入正常工作队列[9]。

主控节点的工作状态与飞行阶段有关,具有记忆效应,因此在心跳恢复后必须恢复当前的工作状态。工作状态恢复的核心问题是将正常节点的内存数据与机器状态复制到故障节点上,使其能够恢复到与正常节点相同的状态。为了有效地利用系统任务的空闲时间,并能够提供较强的系统扩展能力,本文将恢复数据分成适当的数据小包,结合不同状态恢复的需要,制定一套具有扩展能力的恢复命令包协议,在此基础上研究一种节点级故障恢复机制。

节点级故障恢复算法流程:1) 故障节点进入恢复状态后,等待恢复命令包;2) 收到一个恢复命令包后,故障节点按照协议对命令包进行校验,如果两个节点命令包均不正确,回送通信故障应答字后,转到1),等待新的恢复命令包;3) 如果收到恢复结束命令包,转到5),否则转到4);4) 解析恢复命令包的类型字,根据恢复命令转移表调用相应的子程序,恢复相应的机器状态或内存数据区,然后转到1),继续等待新的恢复命令包;5) 退出恢复状态。节点级故障恢复算法流程如图3所示。

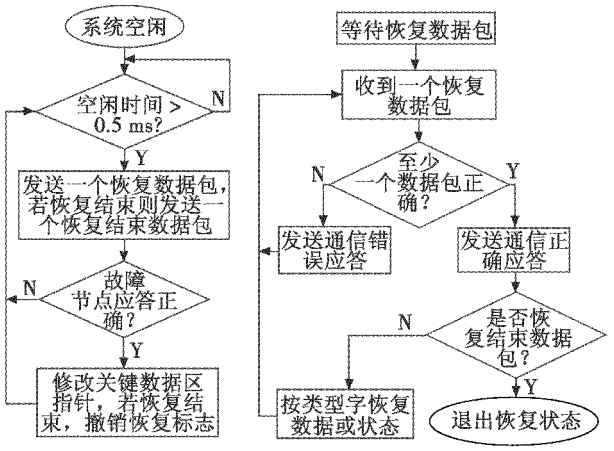

图3 节点级故障恢复算法

Fig. 3 Node-level failure recovery algorithm

3 实验验证

为了验证本文设计的容错策略的可行性,需要对其进行半物理仿真实验,通过故障注入软件向目标系统人为施加典型故障,以激发系统容错机制,并对仿真验证结果进行分析。

样例主从容错式飞控计算机系统的半物理仿真环境由样例主从容错式飞控计算机、飞行仿真计算机、遥控遥测软件以及故障注入计算机构成。半实物仿真结构图如图4所示。通过故障注入计算机可设置相应的故障模型参数,以串口通讯的方式对目标系统实施有效的故障注入,并通过系统反馈参数对系统状态进行分析得出故障注入结果。

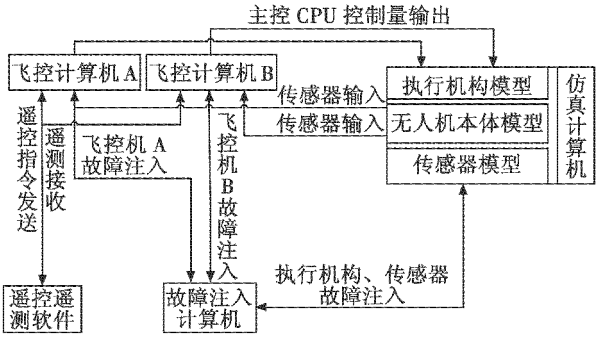

图4 半实物仿真结构图

Fig. 4 Structure of hardware-in-the-loop simulation

利用故障注入软件通过串口发送指令模拟故障,

故障位置、故障模拟方式和系统响应如表 3 所示。

表 3　故障注入报告

Table 3　Fault injection report

故障位置	故障模拟方式	系统响应
AHRS	数值拉偏	航姿告警切换备份源
DGPS	数值拉偏	差分 GPS 告警
无线电高度表	数值拉偏	告警切换至备份
大气数据系统	数值拉偏	告警切换至备份
GPS	数值拉偏	GPS 告警
执行机构	数值拉偏	执行机构系统告警
软件复位	停止喂狗	对故障机进行恢复
主控节点 A	掉电	切换至主控 B
主控节点 B	掉电	切换至主控 A

以高度源故障为例，系统初始采用无线电高度表，当注入无线电高度表故障时，高度源切换到 GPS。故障注入后高度响应曲线如图 5 所示。

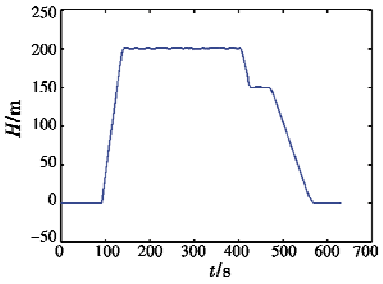

图 5　高度响应曲线

Fig. 5　Height response curve

系统能够按照设计对故障进行正确的处理。当传感器设备故障，切换到备用的传感器数据源；当软件发生异常，进行相应的任务容错处理输出正确的执行结果；当主控节点发生故障，进行相应的控制权转换，使正常节点及时进行接管，任务切换时间仅为 0.2 ms；当节点故障可恢复，正常节点利用系统空闲时间对其进行工作状态恢复，并在时限范围内恢复到正常的工作状态。

4　结束语

容错策略的设计在保证了系统可用性的基础上提高了系统可靠性，切换时不需任务整体迁移，从而减少了切换时间，在故障恢复过程中充分利用系统空闲时间对节点工作状态进行恢复，不产生多余的时间开销，保证了任务的无缝接管和不间断运行。

参 考 文 献

[1] 洪春霞，陈欣，郭鸿昌. 基于 Linux 的无人机故障注入软件研究[J]. 计算机测量与控制，2009，17(6)：1218-1220.

[2] SIEH V, TSCHACHE O, BALBACH F. Verify：evaluation of reliability using VHDL-Models with embedded fault descriptions[C]//The 27th IEEE International Symposium on Fault-Tolerant Computing, Seattle, 1997：32-36.

[3] 张登峰，王执铨，孙金生. 控制系统故障诊断的理论与技术[J]. 数据采集与处理，2002，17(3)：293-299.

[4] ELHADEF M, DAS S, NAYAK A. System-level fault diagnosis using comparison models：an artificial-immune-systems-based approach[J]. Journal of Networks, 2006, 1(5)：43-53.

[5] 王迪爽，肖前贵，杨柳庆. 无人机双余度 MPC5554 飞控计算机[J]. 电光与控制，2013，20(9)：79-83.

[6] 潘计辉，张盛兵，张小林，等. 三余度机载计算机设计与实现[J]. 西北工业大学学报，2013，31(5)：798-802.

[7] YIN Y, LIU B. A method of test case automatic generation for embedded software[C]//International Conference on Information Engineering and Computer Science, IEEE, 2009：1-5.

[8] CHESSA S, SANTI P. Comparison-based system-level fault diagnosis in Ad Hoc networks[C]//Proceedings of the IEEE Symposium on Reliable Distributed Systems, 2001：257-266.

[9] YU S Y, MCCLUSKEY E J. On-line testing and recovery in TMR systems for real-time applications[C]//Test Conference Proceedings, International, IEEE, 2001：240-249.

（上接第 89 页）

[4] 邱晓波，窦丽华，单东升，等. 光电跟踪系统自抗扰伺服控制器的设计[J]. 光学精密工程，2010，18(1)：220-226.

[5] 黄勇，刘杰. 高能激光武器的杀伤机理及主要特性分析[J]. 光学与光电技术，2004，2(5)：20-23.

[6] 秦帅，张斌，李彬郎. 模糊自抗扰控制在永磁同步电机调速系统的应用[J]. 计算机测量与控制，2014(10)：3199-3202.

[7] 孙丽娜，宋悦铭，戴明. 采用复合控制提高机载光电平台的数引跟踪精度[J]. 光学精密工程，2008，16(2)：265-269.

[8] 刘倩，谭文，李东海. 一种多变量自抗扰控制结构的设计研究[J]. 华北电力大学学报：自然科学版，2014，41(6)：97-103.

[9] 臧斌. 直线伺服系统的基于参数优化自抗扰控制研究[D]. 沈阳：沈阳工业大学，2013.

[10] 段慧达. 一类不确定高阶非线性系统的级联自抗扰控制策略研[D]. 长春：吉林大学，2012.

[11] 周宏，谭文. 线性自抗扰控制的抗饱和补偿措施[J]. 控制理论与应用，2014，31(11)：1457-1463.