

引用格式:陈茜,高扬,曲翕,等.可变冗余架构四余度飞管计算机技术研究[J].微电子学与计算机,2021,38(9):67-73.
[CHEN X, GAO Y, QU X, et al. Research on four redundancy flight control computer with variable redundancy architecture [J]. Microelectronics & Computer, 2021, 38(9): 67-73.]

可变冗余架构四余度飞管计算机技术研究

陈 茜,高 扬,曲 翕,吴 铭,樊光焘
(西安微电子技术研究所,陕西 西安 710054)

摘 要: 飞管计算机作为空天飞机关键电子产品,全程参与飞行器的飞行控制. 针对其强实时性、高可靠性、抗辐照、长寿命的特点,提出了一种结合自检测(BIT)技术、当班表决技术的可变冗余架构四余度计算机技术,可以通过故障检测、自恢复、当班权控制、多模表决等技术实现不同的冗余架构管理. 结合工程实践,从飞管计算机的系统架构出发,分析了两种四余度架构模式;通过自检测技术快速进行故障检测和定位,进而利用当班表决实现四余度的升降级管理与重构. 通过建立可靠性模型进行分析,四模并联模式 5 年(约 4.5 万小时)的可靠度高达 0.995. 该技术已成功应用于某天地往返飞行器.

关键词: 可变冗余架构;四余度;故障检测;自恢复;当班权控制

中图分类号: TP336 **文献标识码:** A **文章编号:** 1000-7180(2021)09-0067-07

Research on four redundancy flight control computer with variable redundancy architecture

CHEN Xi, GAO Yang, QU Xi, WU Ming, FAN Guangtao

(Xi'an Microelectronics Technology Institute, Xi'an 710054, China)

Abstract: As a key electronic product of space aircraft, flight control computer participates in the flight control of aircraft throughout the process, which has the characteristics of strong real-time performance, high reliability, radiation resistance and long life. A variable redundancy architecture four-redundancy computer technology is proposed, which combines the self-detection (BIT) technology and on-duty voting technology. It can realize different redundancy architecture management through fault detection, self-recovery, on-duty control, multi-mode voting and other technologies. Combined with the engineering practice, two four-redundancy architecture modes are analyzed from the system architecture of the flight control computer. Through the self-detection technology, the fault detection and location can be carried out quickly, and then the promotion and degradation management and reconstruction of the four-redundancy can be realized by the on-duty voting, and the reliability model can be established for the analysis. The reliability of four-mode parallel mode in 5 years (about 45,000 hours) is as high as 0.995. The technology has been successfully applied to a space shuttle.

Key words: variable redundancy; four redundancy; fault detection; self-recovery; on-duty control

1 引言

空天飞机既兼具飞机可反复升降、多次飞行、可地面维护的特征,又具有航天飞行器需要使用运载

工具发射、长期在轨飞行的特征. 要求其上的电子产品既要具有航空电子产品的高性能又要具有航天电子产品的高可靠、长寿命和抗空间辐射环境的能力. 提升空间计算机系统可靠性的主要途径之一,

是采用恰当的容错策略和系统架构,利用冗余资源屏蔽故障对系统的影响,重构系统,使系统正常工作^[1-5].

目前我国星舰载计算机产品系统架构基本采用两种冗余容错方式,即双机冷备、三机热备模式. 双机冷备只能容忍一余度故障,三机热备模式通过三机同步,三取二表决输出控制,其缺点是当发生一次故障后仍能继续工作,但再次故障就进入安全状态^[6-12].

本文提出了一种可变冗余架构四余度计算机技术,通过故障检测、自恢复、当班权控制、多模表决等技术实现不同的冗余架构管理,实现了两余度故障工作,三余度故障安全的高可靠性要求. 针对四余度不同架构建立了可靠性模型,推导了可靠度计算公式,并对不同架构可靠度进行了分析比较,分析结果表明,针对不同飞行阶段对可靠性的要求,可以采用不同的冗余架构.

2 体系架构

本文采用可变冗余架构四余度体系结构^[12],整个系统由四个完全相同的 CPU 处理器模块(CPUA1/CPUA2/CPUB1/CPUB2)和两个完全相同的智能 IO 模块(IOA、IOB)组成.

四个 CPU 模块之间通过表决逻辑实现对外控制权的选择,采用 20 ms 任务周期进行同步,采用 LVDS 接口 1 发 3 收工作模式交互数据,CPU 模块与智能 IO 模块之间同样采用 LVDS 接口交互数据,CPU 模块采用 1 发 2 收模式,智能 IO 模块采用 1 发 4 收模式.

两个智能 IO 模块互为冷/热备份,智能 IO 模块供电由当班 CPU 模块控制,IO 模块输出使能由当班 IO 模块确定.

飞管计算机系统框图如图 1 所示.

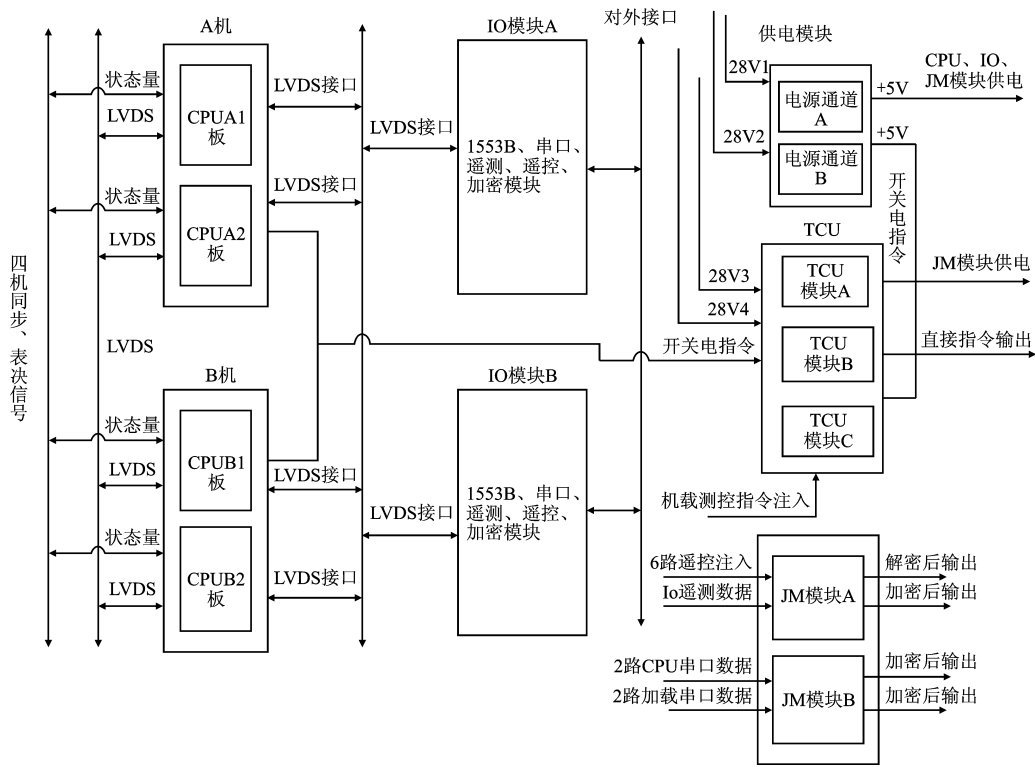


图 1 系统框图

3 冗余架构模式

四余度体系结构可以细分为四模并联模式和四模表决模式.

3.1 四模并联模式

飞管计算机采用四余度四处理器体系结构,任

意一机均可作为当班机,角色的确定与切换由硬件和飞控软件联合实现. 当其中一机发生瞬态故障时,通过单机看门狗狗咬复位或者四机中任意三机三取二表决对第四机进行关电重启,实现自主恢复运行. 当其中一机发生永久故障时系统降级重构. 两个智能 IO 模块互为冷/热备份,智能 IO 模块供电由当

班 CPU 模块控制,IO 模块输出使能由当班 IO 模块确定。

正常情况下,四个完全相同的处理器模块 CPUA1、CPUA2、CPUB1、CPUB2 均工作正常,飞管计算机工作在四机模式, {CPU (A1、A2、B1、B2)}。当其中一机发生瞬态故障时,自主恢复运行,系统仍工作在四机模式,其中一机当班,另外三机监控。

四机模式下,当其中一机发生永久故障时系统降级为三机模式,可组合成 4 种三机工作模式 {CPU(A1、A2、B1)}、{CPU(A1、A2、B2)}、{CPU(A1、B1、B2)}、{CPU(A2、B1、B2)}。三机模式下,当其中一机发生瞬态故障时,单机自主恢复运行,系统仍工作在三机模式,其中一机当班,另外两机监控。

三机模式下,当其中一机发生永久故障时系统降级为双机模式,可组合成 6 种双机工作模式 {CPU(A1、A2)}、{CPU(A1、B1)}、{CPU(A1、B2)}、{CPU(A2、B1)}、{CPU(A2、B2)}、{CPU(B1、B2)}。双机模式下,当其中一机发生瞬态故障时,自主恢复运行,系统仍工作在双机模式。其中一机当班,另外一机监控。

双机模式下,当其中一机发生永久故障时系统降级为单机模式,可组合成 4 种单机工作模式 CPUA1、CPUA2、CPUB1、CPUB2。四模并联模式工作状态迁移如图 2 所示。

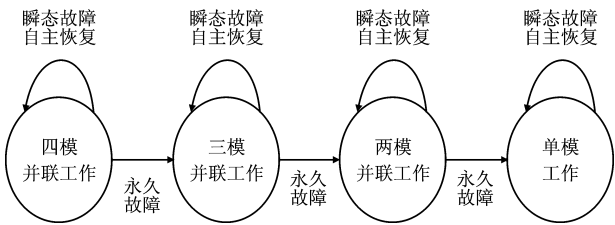


图 2 四模并联模式工作状态迁移图

3.2 四模表决模式

正常情况下,四个完全相同的处理器模块 CPUA1、CPUA2、CPUB1、CPUB2 均工作正常,系统采用四取三模式工作。

当其中一机发生瞬态故障时,自主恢复运行,系统仍工作在四取三模式。

当其中一机发生永久故障时,系统采用三取二模式(TMR)工作,当其中一机发生瞬态故障时,自主恢复运行,系统仍工作在三取二模式。

当其中两机发生永久故障时,系统仍能正常输

出,当其中三机发生永久故障时,系统失效。四模表决模式工作状态迁移如图 3 所示。

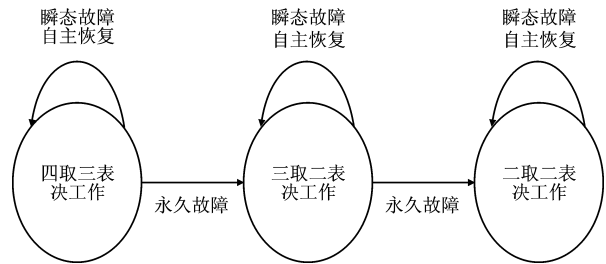


图 3 四模表决模式工作状态迁移图

4 自检测功能 BIT(Built-in test)

飞管计算机要实现四模的升降级管理与重构,就需要快速进行故障检测和定位,及时剔除故障模块。采用自检测(BIT)技术,用来完成自身的硬件功能正确性测试、故障检测、故障定位和故障隔离,并给出测试、诊断咨询指示报告。BIT 作为飞管计算机设计的一个组成部分,通过软件及硬件激励或监控电路,用飞管计算机本机的元器件和电路执行 BIT。当 BIT 运行时,不需外加任何激励或测试设备。BIT 的可靠性考虑飞管计算机整机或 SRU 级的可靠性。BIT 电路的故障率不超过所检测项目或功能故障率的 10%。BIT 包括如下内容:加电 BIT(PUBIT);飞行中 BIT(IFBIT);维护 BIT(MBIT)。

BIT 数据可根据需要实时下传。

(1)加电 BIT(PUPBIT)

飞管计算机在地面上电启动期间,将自动进行上电机内自检测 PUPBIT。上电机内自检测内容如下:

CPU 检测:寄存器 EDAC 造错测试、Cache EDAC 测试、寄存器常规测试、Cache 测试;

程序存储器(PROM/EEPROM、FLASH):通过计算校验和进行测试;

数据存储器:部分数据存储器进行读写测试,检测读写功能是否正常;

多机通讯测试:通过 CPU 处理器之间及 CPU 处理器与 IO 之间的通讯链路互发消息,进行确认;

心跳检测:上电通过 FPGA 自身的检测模块,对本机及其它单机心跳功能进行检测,将记录在非易失存储器中。

(2)飞行中的 BIT(IFBIT)

飞行中 BIT 用于系统硬件状态自监控。测试结果记录在非易失存储器(NVM)中。根据需要 BIT

检测数据传送到地面数据处理站。

①心跳检测:FPGA 心跳检测模块在飞行过程,可以对本机及其它备份模块心跳信号进行检测,作为当班权的表决的条件之一,同时也作为本机及该项功能是否正常的依据;

②飞控周期检测:FPGA 中的检测模块对本机及其它单机的飞控周期信号进行检测,作为当班机的飞控信号的表决的依据,同时也作为本模块是否正常的依据;

③GPS 秒脉冲信号检测:FPGA 中的检测模块对输入的 3 路 GPS 秒脉冲信号进行检测,作为外部校时的依据,同时也是作为本模块是否正常的依据;

④指令回采检测:FPGA 中的检测模块对外输出的指令进行回采,作为本模块功能是否正常的依据;

⑤遥测串口回采检测:FPGA 中的检测模块对外输出的串口遥测数据进行回采,作为本模块功能是否正常的依据;

⑥其它单机电源及运行状态检测:在运行过程中,通过 AD 采集及状态量采集,对其它单机的供电及运行状态进行检测,作为其它单机电源及运行状态是否正常的依据;

⑦28V 指令母线检测:通过专用电路,对外部输入的 28V 指令母线供电电压进行检测,如果异常,则产生中断,方便系统冗余容错及降级,同时作为本机 28V 指令母线检测功能是否正常的依据。

(3)维护 BIT(MBIT)

维护 BIT 用于本系统维护时的功能测试或在故障修复后,进行系统功能综合测试验证。

MBIT 支持维护人员隔离在 PBIT 期间或在飞行中被检测到的故障,以及 PBIT 检测不能覆盖的故障. MBIT 提供将故障尽可能隔离到外场可更换部件 LRU 的能力. MBIT 使用地面 MBIT 测试设备进行故障检测、隔离和显示。

5 当班机状态表决逻辑

飞管计算机通过上电、运行阶段进行全方位的自检,快速检测和定位故障,进而通过当班策略表决,实现系统冗余重构。飞管计算机四机中只有一机是当班机,当班权(MC)由以下信号控制:

(1)机器号

$D[2:0] = 000$ 为 A1 机, 001 为 A2 机, 011 为 B1 机, 111 为 B2 机;

(2)心跳信号

心跳信号的产生:每个 CPU 处理器模块在每个飞控周期,通过向一个硬件端口写“AAAA”,FPGA 自动输出周期为 20ms 心跳信号,并输出到其它三个 CPU 模块,心跳信号采用两路并联方式输出。本机同时接收其它三个 CPU 模块输入的心跳信号,接收的并联心跳信号通过硬件或逻辑(即任何一路心跳信号有效则认为发送心跳信号的单机心跳正常),来判定发送心跳信号的单机是否正常工作。

心跳信号的检测:在 FPGA 中可以对本机心跳信号进行自动检测,也可对其它 CPU 模块心跳信号进行自动检测,以单机为例进行说明。

心跳信号使能:飞控软件向本机心跳检测使能写‘1’,允许检测本机心跳,写‘0’不允许检测本机心跳;向其它机心跳检测使能位写‘1’,允许检测其它 CPU 模块心跳,写‘0’不允许检测其它 CPU 模块心跳。

当软件置允许检测心跳后,心跳检测模块自动对本机和其它 CPU 模块的心跳信号进行检测,如果 FPGA 在一个飞控周期没有检测到心跳变化,则认为该 CPU 模块心跳异常,置该模块心跳异常标识,反之置心跳正常标志。飞控软件可通过端口读到本机和其它 CPU 模块心跳硬件检测结果。

(3)禁止其它机当班信号

本机 FPGA 检测到其它任何一个 CPU 模块心跳异常,自动输出禁止其它机当班信号。

(4)FV 健康状态信号

当本机心跳监测模式开启时,如果监测到本机心跳状态异常,则将本机的 FV 健康状态置为无效。另外 FV 可以由 CPU 进行配置,CPU 向端口写 $0x5555$ 代表 FV 的设置为有效,写 $0xAAAA$ 代表 FV 的设置为无效。

其逻辑示意图如图 4 所示。

当班权表决策略:

(1)任意一机均可作为当班机,角色的确定与切换由硬件和飞控软件联合实现。

(2)本机复位后,硬件自动设置本机 MC 状态为无效状态,本机输出的禁止其它机当班信号为无效状态。

(3)本机 FV 健康状态信号无效,则本机无法当班。

禁止当班信号来源于其它三机,采取 3 取 2 表决控制,当其他三机对本机的禁止当班信号有两机有效时,则本机被禁止当班。

当本机心跳正常、本机没有被禁止当班时,本机

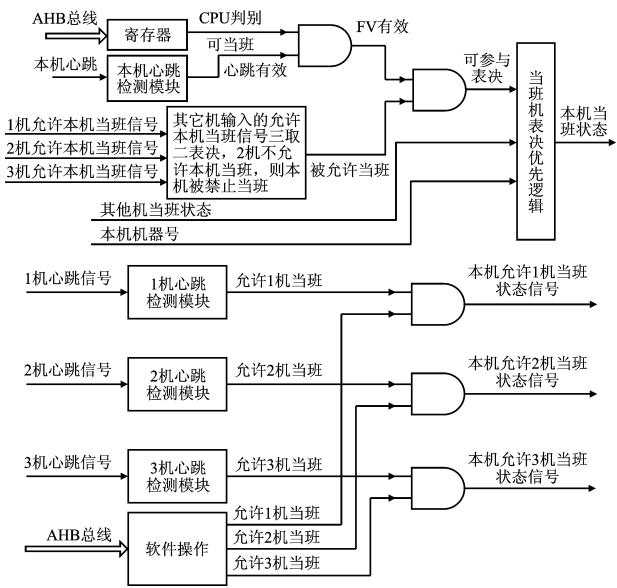


图 4 当班机状态表决逻辑

方可按照优先链的逻辑来当班,即:当班优先链为 A1→B1→A2→B2. 当比本机优先权高的单机均未当班时,本机方能当班.

6 冗余架构可靠性分析

飞管计算机使用的四余度体系结构,由四个完全相同的 CPU 处理器模块组成. 每一模块所有器件总的失效率为 λ , 固定时间可靠度为 $R = \exp(-\lambda t)$. 根据可靠性分析计算方法,对两种四余度体系结构的可靠性进行了比较分析.

6.1 四模并联模式可靠度

n 模并联系统可靠度为:

$$R(t) = 1 - \prod_{i=1}^n (1 - R)$$
 (1)

根据式(1) 计算四模并联系统可靠度为:

$$R(t) = 1 - (1 - R)^4$$
 (2)

将式(2) 化简得:

$$R(t) = 4R - 6R^2 + 4R^3 - R^4$$
 (3)

6.2 四模表决模式可靠度

根据可靠性理论, n 个单元内,有 i 个单元正常、 $(n - i)$ 个单元故障的概率是 $R^i(1 - R)^{n-i}$, 则 n 中取 k , 表决系统的可靠度为:

$$R(t) = \sum_{i=k}^n \binom{n}{i} R^i (1 - R)^{n-i}$$
 (4)

组合公式 $\binom{n}{i}$ 表示 n 个单元中取 i 个成功单元有多少种取法,其值为:

$$\binom{n}{i} = \frac{n!}{i!(n - i)!}$$
 (5)

根据式(4) 计算,四模表决系统的可靠度为:

$$R(t) = \sum_{i=2}^4 \binom{4}{i} R^i (1 - R)^{4-i}$$
$$= \binom{4}{2} R^2 (1 - R)^2 + \binom{4}{3} R^3 (1 - R) + \binom{4}{4} R^4$$
 (6)

将式(5) 带入式(6) 化简得:

$$R(t) = 6R^2 - 8R^3 + 3R^4$$
 (7)

6.3 两种四余度可靠度比较分析

根据设计,飞管计算机单模失效率 $\lambda = 6.538\ 090 \times 10^{-6}/\text{h}$, 根据公式(3) 计算出四模并联模式可靠度随时间变化值(最长工作时间按 5 年计算)如表 1 所示,变化曲线如图 5 曲线 1 所示.

表 1 四模并联模式可靠度

序号	工作时间/hour	可靠度
1	5 000	0.999 998 930 045 687
2	10 000	0.999 983 955 628 155
3	15 000	0.999 923 848 243 075
4	20 000	0.999 774 273 953 121
5	25 000	0.999 482 961 240 143
6	30 000	0.998 993 754 489 043
7	35 000	0.998 249 744 740 439
8	40 000	0.997 195 640 053 383
9	45 000	0.995 779 512 699 610
10	50 000	0.993 954 038 897 864

根据公式(7) 计算出四模表决模式可靠度随时间变化值(最长工作时间按 5 年计算)如表 2 所示,变化曲线如图 5 曲线 2 所示^[13].

表 2 四模表决模式可靠度

序号	工作时间/hour	可靠度
1	5 000	0.999 870 138 710 897
2	10 000	0.999 034 100 251 627
3	15 000	0.996 967 686 995 556
4	20 000	0.993 310 931 632 355
5	25 000	0.987 835 910 840 431
6	30 000	0.980 419 802 300 64
7	35 000	0.971 022 410 208 223
8	40 000	0.959 667 492 448 404
9	45 000	0.946 427 316 109 594
10	50 000	0.931 409 948 914 436

根据以上计算结果和变化曲线比对可以看出,四模并联模式在 5 年后(约 4.5 万小时)的可靠度高为 0.995,四模表决模式在 5 年后(约 4.5 万小时)的可靠度高为 0.946,显然四模并联模式的可靠性

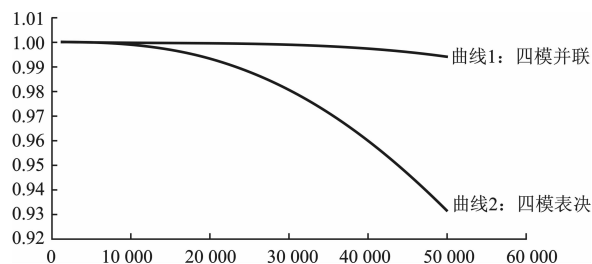


图5 两种架构的系统可靠度变化曲线

高于四模表决模式,但是四模表决模式可以通过多模表决产生输出控制信号,避免误输出。因此要根据系统在轨工作时间,输出控制信号的重要程度,选择不同的系统架构,确保系统在轨长期稳定可靠运行。

7 结束语

本文针对空天飞机对数据、控制管理的强实时性、综合性、高可靠性要求,提出了一种结合自检检测(BIT)技术、当班表决技术的可变冗余架构四余度计算机技术。通过故障检测、自恢复、当班权控制、多模表决等技术实现不同的冗余架构管理。针对四余度不同架构进行了可靠性分析比较,分析结果表明,两种可变冗余架构模式均具有较高的可靠度。可根据系统在轨工作时间,输出控制信号的重要程度,选择不同的系统架构,确保系统在轨长期稳定可靠运行。

参考文献:

- [1] 徐斌,王贞松,陈冰冰,等. 适用于空间环境下的FPGA容错与重构体系[J]. 计算机工程, 2007, 33(3): 231-233. DOI: 10.3969/j.issn.1000-3428.2007.03.084.
- XU B, WANG Z S, CHEN B B, et al. Architecture for fault-tolerance and reconfiguration of FPGA in aerospace[J]. Computer Engineering, 2007, 33(3): 231-233. DOI: 10.3969/j.issn.1000-3428.2007.03.084.
- [2] JACOBS A, CIESLEWSKI G, GEORGE A D, et al. Reconfigurable fault tolerance: a comprehensive framework for reliable and adaptive FPGA-based space computing[J]. ACM Transactions on Reconfigurable Technology and Systems, 2012, 5(4): 21. DOI: 10.1145/2392616.2392619.
- [3] 刘洪刚,谢廷峰,丁伟程,等. 液体火箭发动机实时故障检测与报警原型系统的设计与实现[J]. 火箭推进, 2005, 31(4): 21-25. DOI: 10.3969/j.issn.1672-9374.2005.04.004.

- LIU H G, XIE T F, DING W C, et al. Design and realization of primitive real-time fault detection and alarm system for liquid propellant rocket engines[J]. Journal of Rocket Propulsion, 2005, 31(4): 21-25. DOI: 10.3969/j.issn.1672-9374.2005.04.004.
- [4] YANG C H, DECONINCK G. A fault-tolerant reservation-based strategy for scheduling aperiodic tasks in multiprocessor systems[C]//Proceedings 10th Euro-micro Workshop on Parallel, Distributed and Network-based Processing. Canary Islands: IEEE, 2002.
- [5] YANG C H, DECONINCK G. Fault-tolerant scheduling of periodic and aperiodic tasks in multiprocessor systems[C]//Proceedings of the IASTED-ISMM International Conference on Parallel and Distributed Computing and Systems. Calgary: ACTA Press, 2001: 535-542.
- [6] 陈超. 三机二冗余的实时嵌入式容错系统研究[J]. 航天控制, 2008, 26(6): 82-85. DOI: 10.16804/j.cnki.issn1006-3242.2008.06.018.
- CHEN C. Research on real-time fault-tolerant embedded system for two redundancy with three subsystem[J]. Aerospace Control, 2008, 26(6): 82-85. DOI: 10.16804/j.cnki.issn1006-3242.2008.06.018.
- [7] 曲翕,黄慧敏,张宁,等. 基于多冗余可重构的上面级箭载计算机技术[J]. 计算机工程, 2016, 42(9): 21-25. DOI: 10.3969/j.issn.1000-3428.2016.09.004.
- QU X, HUANG H M, ZHANG N, et al. Upper stage rocket computer technology based on multi-redundancy and reconfigurable[J]. Computer Engineering, 2016, 42(9): 21-25. DOI: 10.3969/j.issn.1000-3428.2016.09.004.
- [8] 程俊强,杨菊平. 多余度飞控计算机通道故障逻辑技术研究[J]. 现代电子技术, 2014, 37(10): 43-46. DOI: 10.3969/j.issn.1004-373X.2014.10.012.
- CHENG J Q, YANG J P. Research of channel fault logic technology for multi-redundancy flight control computer[J]. Modern Electronics Technique, 2014, 37(10): 43-46. DOI: 10.3969/j.issn.1004-373X.2014.10.012.
- [9] 韩伟,臧红伟,谢克嘉. 四余度容错计算机系统结构及其可靠性分析[J]. 计算机工程与科学, 2003, 25(1): 98-100. DOI: 10.3969/j.issn.1007-130X.2003.01.027.
- HAN W, ZANG H W, XIE K J. Quad-redundant fault-tolerant computer architecture and reliability analysis[J]. Computer Engineering & Science, 2003, 25(1): 98-100. DOI: 10.3969/j.issn.1007-130X.

2003. 01. 027.
- [10] 李洪波, 车明. 完全自校验四余度容错系统设计[J]. 微处理机, 2008, 29(3): 165-167. DOI: 10. 3969/j. issn. 1002-2279. 2008. 03. 054.
- LI H B, CHE M. Totally self-checking QMR fault-tolerant systems design[J]. Microprocessors, 2008, 29(3): 165-167. DOI: 10. 3969/j. issn. 1002-2279. 2008. 03. 054.
- [11] 张鹏利. 四余度飞控计算机系统余度管理的设计[J]. 航空计算技术, 1997(3): 58-61.
- ZHANG P L. Design of redundancy management of four redundancy flight control computer system[J]. Aeronautical Computer Technique, 1997(3): 58-61.
- [12] 王桂花. 非相似平台管理计算机的余度管理技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2015.
- WANG G H. Research on redundancy management technique of dissimilar platform management computer [D]. Harbin: Harbin Institute of Technology, 2015.
- [13] 马秀娟, 张秀珍, 曹喜滨, 等. 容错星载计算机系统

结构设计[J]. 微处理机, 2003(2): 47-49. DOI: 10. 3969/j. issn. 1002-2279. 2003. 02. 016.

MA X J, ZHANG X Z, CAO X B, et al. Design of fault-tolerant on-board computer system construction [J]. Microprocessors, 2003(2): 47-49. DOI: 10. 3969/j. issn. 1002-2279. 2003. 02. 016.

作者简介:

陈茜女, (1986-), 硕士研究生, 高级工程师. 研究方向为飞行器计算机系统技术. E-mail: chenxi_1015@126. com.

高扬男, (1990-), 硕士研究生, 工程师. 研究方向为星船载计算机 FPGA 技术.

曲翕男, (1963-), 研究员. 研究方向为星船箭载计算机系统技术.

吴铭男, (1974-), 研究员. 研究方向为星船箭载计算机技术.

樊光焘男, (1994-), 硕士研究生, 工程师. 研究方向为星船箭载计算机技术.