doi:10.3969/j.issn.1671-637X.2017.02.013

非相似双余度机载告警计算机系统设计与实现

李晓君[1], 郝玉锴[2]
(1.中航工业第一飞机设计研究院,西安 710089; 2.中航工业西安航空计算技术研究所,西安 710065)

摘 要:为了抑制计算机系统软件和硬件可能发生的共模故障,在余度技术的基础上,分析了非相似余度技术及其采用的余度结构和余度数量。分别从硬件架构设计、软件架构设计及热备份切换逻辑等方面详细论述了一种非相似双余度告警计算机的设计和实现方法,并且使用故障树模型分析方法在实验数据的基础上对该系统的可靠性进行了分析和计算。结果表明,采用非相似双余度技术可以有效地抑制系统的软件和硬件可能发生的共模故障,将机载告警计算机系统的可靠性提高到0.999 97。

关键词:机载电子设备;非相似余度;机载告警计算机;共模故障;可靠性
中图分类号:O213.2 **文献标志码**:A **文章编号**:1671-637X(2017)02-0060-04

Design and Realization of Dissimilar Dual Redundant Airborne Warning Computer System

LI Xiao-jun[1], HAO Yu-kai[2]
(1. The First Aircraft Institute, AVIC, Xi'an 710089, China;
2. Xi'an Aeronautic Computing Technique Research Institute, AVIC, Xi'an 710065, China)

Abstract: In order to effectively suppress the possible common mode failure of computer system software and hardware, analysis is made to dissimilar redundant technology and its redundant architecture and the number of redundancy based on the redundancy technology. The design and implementation of a dissimilar dual redundant alarm computer are discussed from such aspects of the hardware/software architecture design, hot-standby switching logic and so on. The fault tree analysis method is used for analyzing and calculating the reliability of the system based on the experimental data. The results show that: The use of dissimilar dual redundant technology can effectively suppress the common mode failures of software and hardware system, and improve the reliability of the airborne warning computer system to 0.999 97.

Key words: airborne electronic equipment; dissimilar redundant; airborne warning computer; common mode failure; reliability

0 引言

对于一些关键的计算机系统,为了满足安全性和可靠性的要求,通常采用余度技术,即使用能够执行相同给定功能的两个或两个以上的部件、分系统或通道,采用能够监测故障并完成自动转换或自动切除的监控装置[1-2]。余度技术的实质是利用余度资源来换取整个系统任务可靠性的提高[3]。

余度技术通常可分为相似余度技术和非相似余度技术两种。采用相似余度技术的计算机系统,尽管对于提高系统硬件的可靠性十分有效,但由于各分系统均在相同的指令控制下,运行相同的程序,并时刻处于相同的工作状态,导致通道间的耦合十分紧密,可能会出现两个或多个部件由于某种共同的原因而同时故障的情况,即所谓的共模故障,严重影响余度系统的安全,使系统的可靠性降低几个数量级,成为系统失效的主要根源[4-5]。所以,余度通道耦合越紧密,受共模故障影响使整个系统崩溃的可能性就越大[6]。因此,为了有效地抑制软件和硬件可能的共模故障,本文讨论采

收稿日期:2016-07-15 **修回日期**:2016-08-10
基金项目:国家科技重大专项基金(2012ZX01041-006);航空科学基金(2013ZC31003);工信部民机专项基金(MJ-S-2012-05)
作者简介:李晓君(1983—),男,陕西西安人,硕士,工程师,研究方向为飞机座舱仪表。

用非相似余度技术设计机载告警计算机系统。

1　非相似余度技术

非相似余度技术即软硬件非相似设计技术，指在相同的技术规范条件下，由不同的软硬件设计人员，使用不同的软硬件设计，采用不同生产厂家的元器件，包括不同的控制监控功能，运用不同的算法和编程语言进行开发，组成余度通道系统，产生和监控信号[7-8]。该技术的基础是硬件和软件的独立设计，这样各个余度之间所出现的故障也是独立的，可以达到避免共模故障的目的[9-10]。

在设计和应用中，采用非相似余度方法应结合实际情况，如研制费用、重量、体积、安装位置等要素，在保证设备有较高的可靠性前提下，采用合理的余度技术，确定系统余度结构和余度数。对于多余度、多通道系统，保证各通道数据之间的同步，选择合理的监控算法、表决机制和更有效的余度策略是设计的关键。

1.1　余度结构

余度计算机系统常见的余度结构有两种类型。

1）冗余并列型。

每一时刻有多重分系统同时并列工作，且各系统多为表决型系统，将计算和交叉比较监控后的结果送至多数表决器[11]，按照规定的表决法则进行表决，决定输出。

2）备份转换型。

每一时刻只有一个分系统或部分分系统（主控系统）正常工作，处于备份状态的分系统不工作，当主控系统通过自检测、监控装置发现故障时，立刻用一个备份的分系统替代，即使用多重备份分系统相继运行的方式来维持系统的正常工作。

备份系统可分为冷备份系统和热备份系统。冷备份系统在其他时间不通电或不运行，只有在进行转换时才启动工作；热备份系统一直都处于通电不带载或不与机械传动系统啮合的同步随动状态，当主控系统失效后，备份系统立刻切换到工作状态，保证系统能够正常工作。

1.2　余度数

余度数是指同时工作或作为备份的分系统个数，主要由系统的可靠性、功耗、体积等因素确定[12-13]。余度数目增加，系统开销相应增多，包括增加相应的检测、判断隔离及转换装置，由于它们受串联结构可靠性影响，反而使系统的可靠性降低，成为系统可靠性的瓶颈。

1.3　余度技术

常见的非相似余度设计所使用的余度技术包括：1）看门狗部件备份技术；2）模拟备份技术；3）连续的动态重构复位技术。

2　告警计算机系统设计

告警计算机是飞机的重要组成部分之一，其功能是采集和处理飞机传感器、机载设备提供的关于飞机飞行状态和设备本身的告警信号，当有告警发生时，告警计算机驱动显示器、音频或告警灯来实现主动实时的报警，以帮助飞行员做出各种有利于飞行安全及人身安全的决定。

2.1　硬件架构

告警计算机硬件采用双平台设计方式，分别为 A 平台和 B 平台。两平台采用不同类型的处理器组成两个非相似硬件通道，A 平台为 TI 的 DSP 处理器，B 平台为 Freescale 的 PowerPC 处理器。

A，B 平台采用热备份转换运行方式，其中，A 平台为主控平台，B 平台为热备份工作平台。计算机工作后，两平台同步执行相同功能的程序，包括数据采集、处理、驱动等，以保证在 A 平台发生故障时 B 平台无缝接替其工作，实现正常告警功能。

A，B 平台各包含 4 个模块，即处理器（DSP/PowerPC）模块、电源模块、总线接口/处理模块和离散接口/处理模块，其中，处理器模块和对应的总线接口/处理模块及离散接口/处理模块统称为处理单元，两平台共用告警信息采集模块和输出模块，告警计算机硬件架构如图 1 所示。

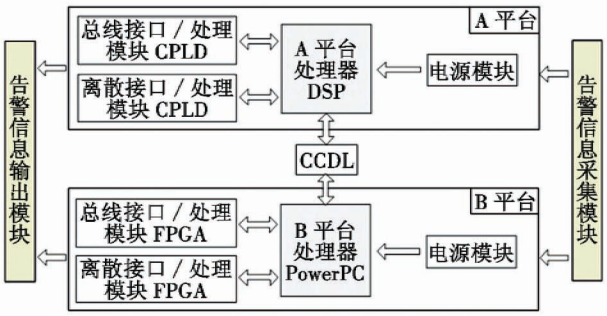


图 1　告警计算机硬件架构图

Fig. 1　Architecture of warning computer hardware

A，B 平台采用不同架构的处理器，因而在指令这一级上避免了相同机器指令的共模故障，其次由于两个处理器的主频、芯片、结构也不同，从而保证硬件系统中的共模故障率达到最小限度。

在硬件故障检测方面，为了有效地进行故障隔离定位，采用自检测、周期检测及看门狗技术来检测本通道内部硬件系统，包括处理器、存储器、输入输出模块等的有效性。

在余度管理方面，A，B 平台通过交叉通道数据链路（Cross Channel Data Link，CCDL）实现数据交互，CCDL

链路由 I/O 接口和 RS-422 通道组成。

1）8 个直连 I/O 接口，分为两组，4 输入 4 输出，A，B 平台分别通过 4 个 I/O 接口主动向对方发送自身前一个周期时间内的工作状态及本周期时间内的健康状态。约定前 2 位表示自身工作状态，后 2 位表示自身健康状态，标识各自平台自检测结果，其中，“01”表示不工作或不健康，“10”表示工作或健康。

2）2 个交叉的 I/O 接口，主要在维护模式的状态下使用。

3）1 路 RS-422 通道，用于交互各自平台自检数据及故障等级。当 A/B 平台中的某一个主控平台出现故障时，通过 CCDL 交互数据，选择健康状态良好的平台作为输出，当 A/B 平台的自检测都出现故障时，需要进一步判断两平台各自的故障严重程度，然后将故障程度低的作为主控平台，对外输出。

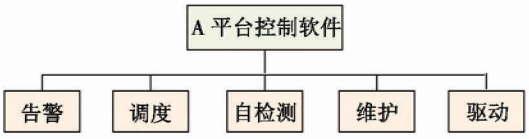
为了便于量化的比较，余度系统设定如下故障等级：0 为无故障；1 为维护接口故障（包括 RS-232，RS-422 和 CAN）；2 为任意一个 ARINC429 总线接口故障，每增加一个 ARINC429 总线接口故障，则等级加 1；3 为任意一个离散量输入输出接口故障，每增加一个离散接口故障，则等级加 2；10 为 CPU 故障。

当发生故障时，余度系统处理故障的逻辑为：故障等级大于等于 2，将影响正常工作，需要通过 CCDL 交互后确定当前主控平台；如果双机都出现故障等级大于等于 2 的故障，则根据故障等级设定主控平台，故障等级低的为主控平台，关闭故障等级高的另一个平台；如果故障等级相同，原主控平台转为单平台运行，关闭备份平台。

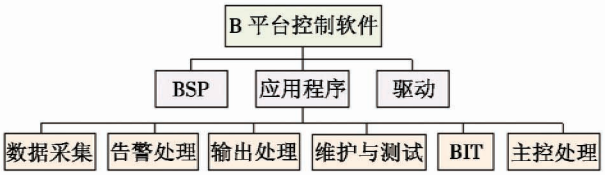
2.2 软件架构

为提高软件可靠性，对软件中安全性要求较高的关键部分进行差异性设计，并在设计中和不同的开发设计小组保持交流和沟通，减少由于设计要求不明确而产生的错误。

告警计算机 A 平台、B 平台控制软件采用不同的软件架构设计，如图 2 所示，其中，A 平台为单线程软件架构，B 平台为多线程软件架构，各平台对告警信息的处理和告警列表的生成采用不同的编程语言实现，避免由于编译和链接时发生错误而引起软件共模故障，语言的不同又带来了系统平台的非相似性，完全独立的相异性设计，可以使得软件的共模故障率大大降低。



a A 平台



b B 平台

图 2 控制软件架构图

Fig. 2 Architecture of control software

A，B 平台非相似双余度热备份逻辑设计基于各平台的 BIT 结果，由 BIT 结果判断出处于输出状态的工作平台，故障检测判断及热备份判断流程如图 3 所示。

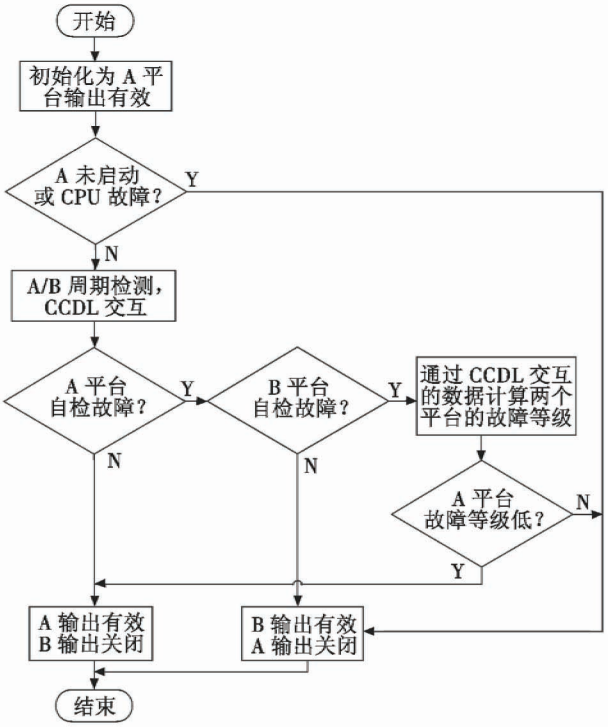


图 3 A，B 平台故障检测判断及热备份判断流程图

Fig. 3 Flow chart of A，B platform fault detection and hot standby judgement

依据图 3 所述流程，通过向 A，B 平台中的 CPLD/FPGA 写入固定的值，实现两平台的输出使能控制，保证正常工作的平台向外发送数据，故障平台输出被关闭。

告警计算机由于采用了非相似余度的处理器，A，B 平台的指令系统、执行算法及编译效率都不相同，导致各平台对同一告警信号输入的处理和告警列表生成时间不同步，而对于告警计算机而言，其设计的目的是保证不会因为余度调度而造成告警数据丢失，因此在实际设计中，利用 A，B 两平台采集周期和处理周期的时间差抵消两平台之间的不同步，保证输出结果的一致性，并在软件设计上保证当 A 平台检测到故障时，它已将本周期内采集到的告警信息形成列表发送出去，再切换到 B 平台，保证告警计算机正常工作。

3 可靠性分析

告警计算机通过非相似设计，使得各个余度之间所出现的故障也是独立的，从而达到避免共模故障、提高计算机安全性和可靠性的目的。

对计算机系统可靠性的分析有很多方法和模型[14-15]，如故障树模型、马尔可夫模型等，本文采用故障树分析法，以“告警计算机失效”为顶事件，进行自顶而下的故障分析，告警计算机故障树模型如图 4 所示。

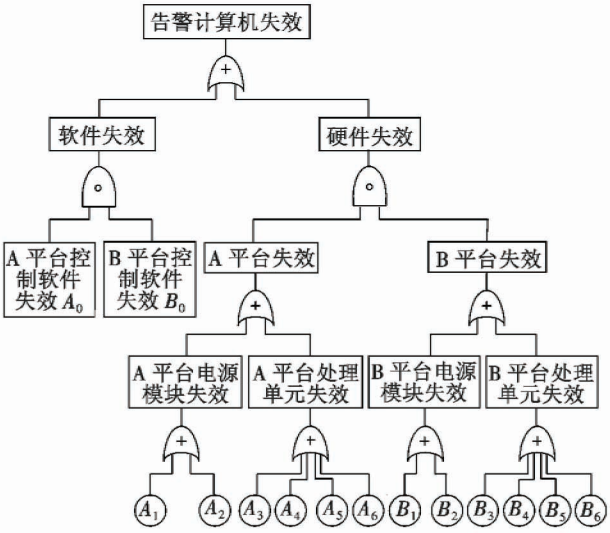


图 4　告警计算机故障树模型

Fig. 4　Warning computer fault tree model

各事件描述如下：A_0/B_0 为控制软件失效；A_1/B_1 为不能提供二次供电输出；A_2/B_2 为二次供电性能下降；A_3/B_3 为离散输入或输出数据错误；A_4/B_4 为总线接收或发送数据错误；A_5/B_5 为处理器计算性能下降或失效；A_6/B_6 为不能进行交互通信或通信错误。

在系统综合阶段，对告警计算机系统出现错误的情况进行统计和记录，根据统计记录和实验数据，可以得到各事件失效率，如表 1 所示。

表 1　各事件失效率

Table 1　Fault rate of each event　$\times 10^{-6}\,h^{-1}$

事件	A_0	A_1	A_2	A_3	A_4	A_5	A_6
失效率	500	5.495	15.41	27.28	12.254	7.173	0.034
事件	B_0	B_1	B_2	B_3	B_4	B_5	B_6
失效率	1200	7.588	18.238	35.849	13.461	23.521	0.051

当软件和硬件有任一路失效时，判定告警计算机失效，告警计算机失效的割集为 $\phi = (A_0 \cdot B_0) + \{[(A_1 + A_2) + (A_3 + A_4 + A_5 + A_6)] \cdot [(B_1 + B_2) + (B_3 + B_4 + B_5 + B_6)]\}$。

由故障树模型可知，事件 $A_0/B_0 \sim A_6/B_6$ 相互独立，已知其发生概率，使用容斥原理即可得到“告警计算机失效”事件发生的概率，进而得到告警计算机的任务可靠性 $P = 1/\phi$。在该设计中，利用此方法得到非相似双余度告警计算机的任务可靠性为 0.999 97，满足使用需求。

4 结束语

非相似余度技术在硬件和软件上均有效抑制了共模故障，极大地提高了系统的可靠性。本文分析了非相似余度技术，采用非相似双余度的方法对机载告警计算机系统的软硬件分别进行设计和实现，并且使用故障树模型分析方法在实验数据的基础上对该系统的可靠性进行了分析和计算。结果表明，非相似双余度技术有效地抑制了系统的软件和硬件共模故障，提高了其可靠性，满足系统的使用需求，目前该系统已在某飞机上成功应用。

参 考 文 献

[1] 臧红伟，韩炜. 非相似余度计算机系统及其可靠性分析[J]. 航空计算技术，2003，33(1)：112-114.

[2] 陶想林，陆熊，殷斌. 基于 PowerPC 和 X86 的二余度非相似飞控计算机系统设计与实现[J]. 现代电子技术，2014，37(20)：91-94.

[3] DUCARD G J J. Fault-tolerant flight control and guidance systems: practical methods for small unmanned aerial vehicles[M]. Berlin: Springer, 2009: 89-90.

[4] 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.

[5] O'CONNOR P D T. 实用可靠性工程[M]. 4 版. 李莉，王胜开，陆汝玉，等译. 北京：电子工业出版社，2005：158-168.

[6] 杨伟. 容错飞行控制系统[M]. 西安：西北工业大学出版社，2007：192-200.

[7] 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.

[8] 杨菊平，董摇妍，程俊强. 民机飞控计算机余度设计及可靠性分析[J]. 计算机技术与发展，2014, 24(6)：211-214.

[9] 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.

[10] 殷斌，陆熊，陶想林. 非相似三余度飞控计算机设计和可靠性分析[J]. 测控技术，2015, 34(5)：53-56.

[11] 臧红伟，韩炜，高德远. 非相似余度计算机系统及其可靠性分析[J]. 哈尔滨工业大学学报，2008，40(3)：492-494.

[12] HUANG C Y, LYU M R. A unified scheme of some nonhomogenous poisson process models for software reliability estimation[J]. IEEE Transactions on Software Engineering, 2003, 29(3): 261-269.

（下转第 74 页）

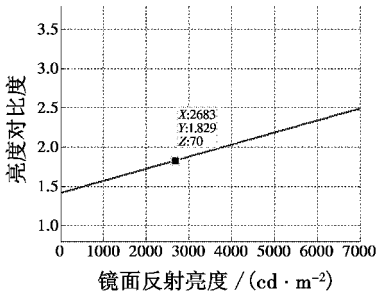


图7 亮度对比度与镜面反射亮度值的关系图

(P_{PJND}为70,环境亮度为5000 cd/m^2)

Fig. 7 Luminance contrast vs specular luminance

($P_{PJND}=70, L(f)=5000$ cd/m^2)

4 结束语

本文以PJND理论为基础,结合平显应用环境和显示特点,建立了基于PJND的平显可读性评价模型。通过仿真研究了干扰以及背景色度变化对平显可读性的影响规律。借助天空环境光实验室对PJND评价方法进行了实验验证。

3.1节中实验数据表明:用PJND值能够评价平显可读性质量;实际应用中可通过调节亮度对比度来保持平显PJND值恒定不变,进而满足平显可读性要求。但满足平显可读性的PJND最小值为多少,不同环境亮度下亮度对比度应该达到多少,还需进一步实验验证。

3.2节中实验数据表明:不同背景色度、同样环境亮度下,对亮度对比度要求不同。背景色度差异越大(CJND值越大),对亮度对比度要求越小。

由于干扰数值不易测量,3.3节中只根据平显的PJND模型仿真了干扰变化对可读性的影响规律。仿真结果表明:当干扰值较小时,可通过增大亮度对比度来满足平显可读性;干扰值超过一定范围,只能通过物理遮挡来保证平显的可读性。

现有关于PJND的研究成果中都以液晶显示设备作为研究对象,国内外,关于PJND应用于平显的资料较少,平显应用环境及其显示特点有其特殊性,所以PJND理论在平显领域的应用还需进一步深入研究。同时应进行大量工程试验来完善基于PJND的平显可读性评价方法。

参考文献

[1] 丁全心. 机载瞄准显示系统[M]. 北京:航空工业出版社,2015:33.

[2] VASSIE C K. Specification and assessment of the visual aspects of cockpit displays[C]//SID Symposium Digest of Technical Papers, 1998, 29(1):1199-1203.

[3] CARTWRIGHT S R, GILLESPIE C M, ALLAN G W, et al. Sunlight readability of displays: a numerical scale[C]// The 4th Oxford Conference on Spectroscopy, 2003, 4826: 176-180.

[4] VASSIE C K, CHRISTOPHER W C. Just acceptable and desirable luminance levels for fast jet cockpit displays [C]//Proceedings of SPIE 4022, Cockpit Displays VII: Displays for Defense Applications, 2000. doi: 10. 1117/12. 397737.

[5] JARRETT D N. 座舱工程 [M]. 孔渊,曲卡尔,译. 北京:航空工业出版社,2015:142-143.

[6] WOLF D C. Modeling image quality for automotive display technologies[D]. Dundee: Abertay University, 2014.

[7] British Defence Standards. DEF STAN 00-970 crew stations-general requirements guidelines for the design of crewstation lighting and displays[S]. UK, 1999.

[8] MIL-PRF-22885/108F. Sunlight readable display (dripproof, waterlight, splashproof, EMI/RFI shielding, high impact shock resisitant, common termination system, night vision goggle compatible)[S]. USA, 2014.

[9] BLACKWEL H R. Description of a comprehensive family of Relative Contrast Sensitivity (RCS) functions of luminance to reflect differences in size of task detail, task eccentricity and observer age[J]. Journal of the Illuminating Engineering, 2013, 11(1):52-63.

[10] KELLY E F. Sensitivity of display reflection measurements to apparatus geometry[C]//SID Symposium Digest of Technical Papers, 2002. doi:10. 1889/1. 1830211.

(上接第63页)

[13] LEVITIN G. Optimal structure of fault-tolerant software systems[J]. Reliability Engineering & System Safety, 2005, 89(3):286-295.

[14] 陈光宇,黄锡滋,唐小我. 故障树模块化分析系统可靠性[J]. 电子科技大学学报,2006, 35(6):989-992.

[15] LEVITIN G. Optimal structure of fault-tolerant software systems[R]. Tel Aviv: Israel Electric Corporation Ltd, 2003.