民机飞控计算机余度设计及可靠性分析

杨菊平,董 妍,程俊强
(中国航空工业计算技术研究所,陕西 西安 710068)

摘 要:为了确保飞行控制系统的任务可靠性和安全可靠性,国外先进民机飞行控制计算机均采用余度技术。非相似余度技术采用完全不同的硬件和软件组成余度通道,产生和监控飞行控制信号,可避免多通道余度系统共性故障的产生,达到较高的可靠性。文中针对非相似余度设计技术,深入研究波音和空客飞机飞控计算机的余度技术,分析其飞控系统的可靠性,再根据我国的技术实力和研发能力,提出了我国民机飞控计算机余度设计的一种方案,并且用可靠性理论进行了验证。

关键词:飞控计算机;余度技术;相似余度;非相似余度
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2014)06-0211-04
doi:10.3969/j.issn.1673-629X.2014.06.052

Redundancy Design and Reliability Analysis of Airplane's Flight Control Computer

YANG Ju-ping, DONG Yan, CHENG Jun-qiang
(China Aeronautics Computing Technique Research Institute, Xi'an 710068, China)

Abstract: To insure task reliability and safety reliability of flight control system, non-similar redundancy technique has been adopted by foreign advanced airplane's flight control computer. Non-similar redundancy technology uses different hardware and software to build redundancy channel, which generates and controls flight control signal. It can match high reliability because of avoiding the correlated faults. It lucubrates redundancy technique of flight control computer of Boeing and Airbus, analyzes the reliability of them. Then, raise an project of redundancy technique of flight control computer according to domestic technical strength and developing ability, and validate the project using reliability theories.

Key words: flight control computer; redundancy technique; similar redundancy; non-similar redundancy

0 引 言

目前,世界各国对电传飞行控制系统安全可靠性提出的指标一般是:军用飞机为 1.0×10^{-7}/飞行小时;民用飞机为 1.0×10^{-10} ~ 1.0×10^{-9}/飞行小时[1-2]。余度技术是提高系统任务可靠性、安全可靠性和容错能力的有效手段。余度计算机可分为相似余度和非相似余度两种形式。对于采用相似余度的飞控计算机系统,多台结构完全相同的计算机,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,因此通道间的耦合十分紧密。然而,余度通道耦合越紧,共性故障[3-6]的发生率就越高,使整个系统崩溃的可能性就越大。自电传飞行控制系统应用于民用飞机的设计后,对系统的可靠性和安全性提出了更高的要求,为此,国外的民用飞机研制大都采用了非相似余度技术,有效地抑制了一些共性故障,并已成功地用于空客 A320、A330/340 和波音 777 等[7-8]。

文中主要针对非相似余度设计技术,研究波音 777 和空客 A320 的余度设计技术,分析我国在航空领域的技术实力和研发能力,提出对我国民机飞控计算机余度技术的一种方案,并且用可靠性分析工具进行验证。

1 波音、空客飞机飞控计算机余度技术研究

波音和空客的民用飞机在采用电传飞控系统之后,其飞行控制计算机的余度均采用了非相似余度设计模式[7,9],但两公司的设计方法又各不相同,下面以

收稿日期:2013-08-19 **修回日期**:2013-11-26 **网络出版时间**:2014-02-24
基金项目:航空科学基金项目(20101931004)
作者简介:杨菊平(1980-),女,四川剑阁人,工程师,研究方向为计算机应用。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140224.0930.063.html

波音 777 和空客 A320 为例,分别对这两种非相似余度技术进行研究。

1.1 波音 777 飞控计算机余度设计技术研究

波音 777 的飞控计算机是 3 * 3 非相似余度计算机,包括三个相同的主飞控计算机(左 PFC、中 PFC 和右 PFC),每个主飞控计算机中有三个非相似的计算机通道。三个计算机通道分别使用三个不同的处理器 AMD 29050、Motorola 68040 和 Intel 80486[10-11],各处理器的硬件接口和外围电路也不相同。主计算机之间、通道之间由三余度 ARINC629 进行通信,每个通道包括有三个模块,即处理器、I/O 和电源[12],如图 1 所示。

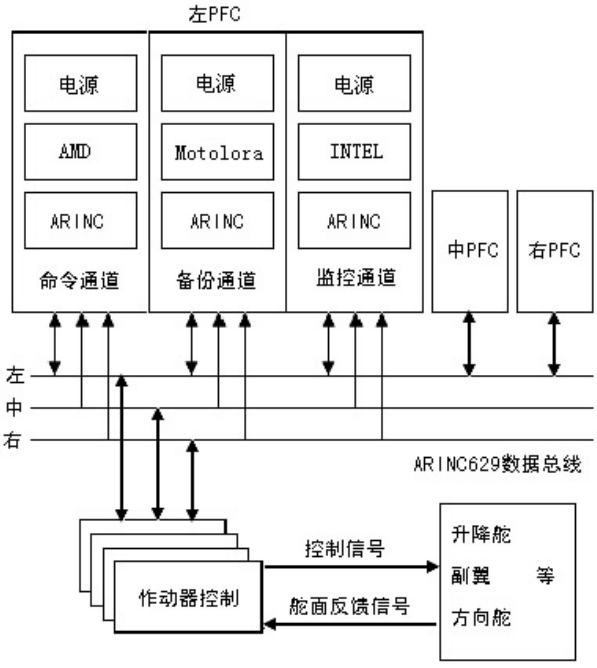


图 1 波音 777 主飞控计算机结构

在硬件方面,三个主飞控计算机都处于活跃状态,每个主飞控计算机都进行所有舵面控制指令的计算,并获得所有主控制舵面作动器、配平系统和驾驶员人感系统的控制指令。主飞控计算机和 ARINC 总线均被分为左、中和右三组,三个 PFC 同时监听三组总线,但只能向同组的总线传递数据,一组总线出现故障不会影响其他两组的正常工作。每个计算机内的有效通道分别处于命令、备份或监控状态。命令通道在指定的 ARINC629 总线上发送全部的舵面控制命令和系统状态数据,其他两个通道执行监控功能,向 ARINC629 总线上发送硬件状态验证和通道间余度管理所必需的数据。当命令通道出现故障时,备份通道立即切换到工作状态,变成新的命令通道,若再有一个通道发生故障时,该 PFC 失效,切除该 PFC。

在软件方面,三个版本的软件由不同的软件小组编写,在相同的规范下,用相同的设计语言(ADA),在三种不同的编译器上编译[13]。虽然确保了三个版本软件之间的非相似性,但不能消除由相同语言产生的共性故障。

波音 777 主飞控计算机共有 9 个处理器,PFC 失效之前可以容忍的故障数为 5。假设系统每个通道的失效率为 λ 且服从指数分布,虽然三个通道使用不同的处理器,但由于各处理器的功能相同,硬件技术的日趋成熟,各处理器的故障率处于同一数量级,可近似认为相等,均为 λ_H;虽然三个版本的软件使用不同的编译器,但由于设计规范相同,编程语言相同,也可近似认为三版本软件的故障率相等,均为 λ_S,则主飞控计算机的可靠性[13-14]为

$$R_{B777}(t) = 1 - (1 - 3e^{-2(\lambda_H+\lambda_S)t} + 2e^{-3(\lambda_H+\lambda_S)t})^3 \quad (1)$$

若考虑软件版本间的相关性,假定两个版本之间的相关故障率分别为 λ_{12}、λ_{13} 和 λ_{23},三个版本间的相关故障率为 λ_{123},则此时主飞控计算机的可靠性[5-6]为

$$R_{B777}(t) = e^{-(\lambda_{12}+\lambda_{13}+\lambda_{23}+\lambda_{123})t}(1 - (1 - 3e^{-2(\lambda_H+\lambda_S)t} + 2e^{-3(\lambda_H+\lambda_S)t})^3) \quad (2)$$

1.2 空客 A320 飞控计算机余度设计技术研究

空客 A320 采用三余度/二余度(相似硬件,非相似软件)技术,飞行控制计算机采用双通道配置,一个通道为命令通道,另一个通道为监控通道,两个通道采用相同的 CPU 芯片,软件采用不同的算法实现。A320 包括 7 个飞控计算机,两个升降舵/副翼计算机(ELAC)、3 个扰流片/升降舵计算机(SEC),两个飞行增稳计算机(FAC),其中 ELAC 和 SEC 为主飞控计算机[2,13-14]。它们根据正常、备用或直接模态处理飞行员和自动驾驶仪的输入。另外增加两个飞控数据集中器(FCDC),用于主飞控计算机和其他飞控系统之间进行通信。A320 飞控计算机的结构如图 2 所示。

A320 的主飞控计算机均能控制 A320 的飞行(但在控制权限上有差别),ELAC 和 SEC 采用非相似余度技术,ELAC 的处理器为 Motorola 68010 微处理器,SEC 的处理器为 Intel 80186 微处理器[2,14]。每个主飞控计算机都有两个独立的处理器,分别作为指令支路和监控支路。因此 A320 有四种不同的支路:ELAC 的指令支路和监控支路,SEC 的指令支路和监控支路。每个支路上运行不同的软件,因此也有四种不同的软件包。若某计算机的指令支路与监控支路之间的差值超限,则该计算机失效,切断它与外围设备的连接,并起用备用计算机。

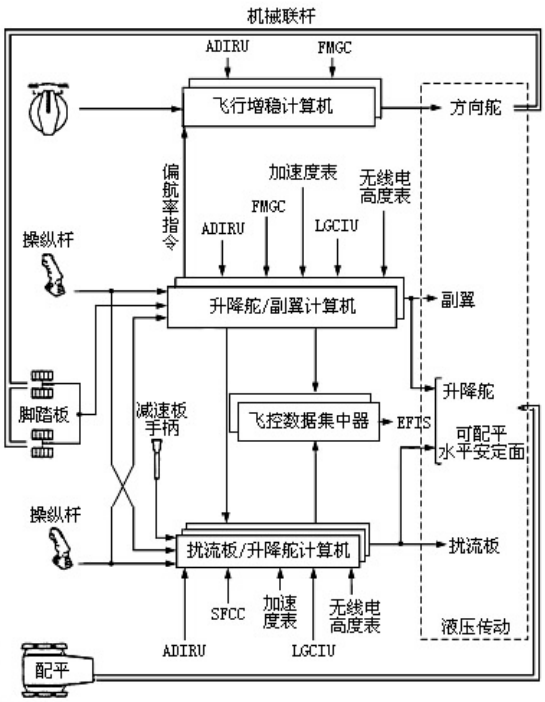
A320 的主飞控计算机共有 10 个处理器,在主飞控计算机失效前可以容忍 4 次故障。假设系统每个支路的失效率为 λ 且服从指数分布,同理认为处理器的故障率近似相等,均为 λ_H;由于 A320 有四种不同的软件包,不能近似地认为它们相等,假定 ELAC 指令支

路软件包的故障率为 λ_{E-C}、监控支路软件包的故障率为 λ_{E-M},SEC 指令支路软件包的故障率为 λ_{S-C}、监控支路软件包的故障率为 λ_{S-M},则主飞控计算机的可靠性[5-6]为

$$R_{A320}(t) = 1 - (1 - e^{-(\lambda_{E-C}+\lambda_{E-M}+2\lambda_H)t})^2(1 - e^{-(\lambda_{S-C}+\lambda_{S-M}+2\lambda_H)t})^3 \quad (3)$$

若考虑软件版本间的相关性,对于 A320 来说就相对复杂多了,这里仅考虑每个计算机内两个版本间相关故障对系统可靠性的影响,假定 ELAC 计算机内两版本间的相关故障率为 λ_{E-CM},SEC 计算机内两版本间的相关故障率为 λ_{S-CM},则此时主飞控计算机的可靠性[5-6]为

$$R_{A320}(t) = (1 - (1 - e^{-(\lambda_{E-C}+\lambda_{E-M}+2\lambda_H)t})^2(1 - e^{-(\lambda_{S-C}+\lambda_{S-M}+2\lambda_H)t})^3) \times (1 - (1 - e^{-\lambda_{E-CM}t})(1 - e^{-\lambda_{S-CM}t})) \quad (4)$$



FMGC:飞行管理制导计算机　　ADIRU:大气数据/惯性基准装置
LGCIU:起落架控制接口设备　　EFIS:电子仪表系统
SFCC:扰流板/襟翼控制计算机

图 2　空客 A320 飞控计算机结构

1.3　波音 777 和空客 A320 余度技术的比较

波音 777 和空客 A320 飞控计算机均采用了非相似余度技术,但在计算机功能分配、余度结构、容错能力和软件差异性设计方面都体现了各自的特点。在余度结构和容错能力上,B777 能利用更少的硬件资源获取更高的可靠性,比 A320 更为合理;在相关故障的抑制方面,由于 A320 软件相关故障对系统的可靠性的影响相对较小,A320 又明显优于 B777。

2　我国民机飞控计算机余度设计的思考

我国有较完备的航空工业体系,从飞机主机、航空发动机到航空机载设备,都有完整的研发和制造基地,研发能力仅次于美、欧、俄。

根据对国外民机飞控计算机余度技术的研究,综合我国在航空领域的研发实力,对我国民机飞控计算机余度设计提出如下建议:

(1)我国民机电传系统的余度结构采用 4 余度技术,通道使用不同的处理器,每个通道由两个支路构成比较监控结构。

(2)我国民机电传系统的软件系统使用三个版本的软件,通道的每个支路上运行两个版本的软件,每个通道的软件版本组合均不相同。

假设软件的版本分别为 v1、v2 和 v3,给出一种我国民机飞控计算机余度技术设计的方案,如图 3 所示。

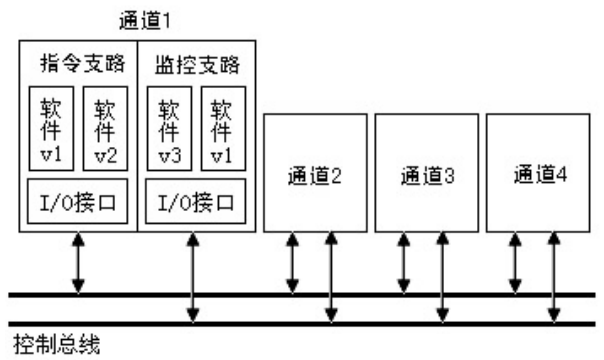


图 3　我国民机飞控计算机余度设计示意图

飞控计算机的四个通道同时工作,且都能全权限地控制飞机飞行。软硬件的设计都采用非相似余度技术,当某通道出现一次硬件故障或两次软件故障时,通道失效。假设系统每个支路的失效率为 λ 且服从指数分布,同理认为处理器、软件各版本的故障率近似相等,分别为 λ_H、λ_S,则飞控计算机的可靠性[5-6]为

$$R_C(t) = 1 - (1 - e^{-2\lambda_H t}(1 - (1 - e^{-\lambda_S t})^2)^2)^4 \quad (5)$$

不考虑共性故障对可靠性的影响,假定 A320 的软件故障率近似相等,飞行 10 000 小时后,该设计方案与 B777、A320 的可靠性比较如表 1 所示。

表 1　我国民机与 B777、A320 的余度方案比较

飞机	λ_H	λ_S	处理器个数	软件版本数	余度数	可靠性 t=500 h	可靠性 t=1 000 h
B777	$1*10^{-5}$	$1*10^{-4}$	9	3	5	0.999 999 43	0.999 972 21
A320	$1*10^{-5}$	$1*10^{-4}$	10	4	4	0.999 987 74	0.999 699 65
我国民机	$1*10^{-5}$	$1*10^{-4}$	8	3	4	0.999 999 95	0.999 998 03

从比较结果可以看出,我国民机飞控计算机余度技术的方案节约了硬件资源(只用了 8 个处理器),结构更为合理,可靠性更高。

3 结束语

波音 777 和空客 A320 的飞控计算机均采用了非相似余度设计技术,它们在系统结构、功能分配、容余能力上又各有特点,在余度结构上 B777 优于 A320,在共性故障的抑制上,A320 又优于 B777。结合我国的实际情况,给出了我国民机飞控计算机余度设计的一种合理方案,它利用更少的资源,更优化的结构,获得了更高的可靠性。

参考文献:

[1] 杨菊平,陈 益. 民用飞机飞控计算机的现状与展望[J]. 航空计算技术,2007,37(5):131-134.

[2] 孙 岩,苏 媛,洪冠新,等. 世界大型商用飞机飞控技术演变与发展分析[J]. 民用飞机设计与研究,2009(S1):92-96.

[3] 杨 伟. 容错飞行控制系统[M]. 西安:西北工业大学出版社,2007.

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

[5] 李烈彪,李 仙. 计算机系统的可靠性技术[J]. 计算机技术与发展,2007,17(11):142-144.

[6] 刘小雄,章卫国,李广文. 电传飞行控制系统的余度设计技术[J]. 飞机设计,2006(1):35-38.

[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] Collinson R P G. Fly-by-wire flight control[J]. Computer & Control Engineering Journal,1999,12(12):141-153.

[9] 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.

[10] Ahlstrom K,Torin J. Future architecture for flight control systems[C]//Proc of 20th digital avionics systems conference. Daytona Beach,FL:IEEE,2001.

[11] 周小超,陆 熊. 非相似余度飞控计算机设计及可靠性分析[J]. 计算机与现代化,2013(5):135-137.

[12] Berthomieu B,Diaz M. Modeling and verification of time dependent systems using time Petri nets[J]. IEEE Transactions on Software Engineering,1991,17(3):259-273.

[13] Patrick D,O'Connor T. 实用可靠性工程[M]. 李 莉,王胜开,译. 北京:电子工业出版社,2005.

[14] 熊峻江,王甲峰,袁 立,等. 余度设计中的系统可靠性最优分配模型[J]. 航空学报,2004,25(1):45-48.

(上接第 210 页)

4 结束语

赛博空间威胁作为一个新兴的全球性问题已经受到了许多发达国家决策者的高度重视与关注。赛博空间战的实质是利用多领域多技术手段获取信息优势,赛博空间对抗随着信息技术的不断发展也将不断融入更多新的技术模式与应用,信息时代的赛博空间战或许不容易看到如传统战争中那样鲜血淋漓的死亡与挣扎过程,但是同样会充满着流血与牺牲,必须时刻关注它的技术发展趋势,不能忽视它对实际战争的巨大影响。只有不断调整自身并且积极适应发展新领域与新技术,才能切实维护自己的尊严与利益。

参考文献:

[1] United States Army Training and Doctrine Command. The United States Army's Cyberspace operations concept capability plan 2016-2028[R]. Washington,D C:US DoD,2010.

[2] US DoD. JP1-02:department of defense dictionary of military and associated terms[M]. Washington,D C:US DoD,2011.

[3] 周光霞,孙 欣. 赛博空间对抗[J]. 指挥信息系统与技术,2012(2):6-10.

[4] 孙智信,赵 炤,李自力,等. 网络全域_Cyberspace 的概念辨析与思考[J]. 火力与指挥控制,2012,37(4):1-5.

[5] 蒋盘林. 数字化战场和现代通信战[J]. 电子对抗技术,1999,14(1):1-5.

[6] Schneider D. Wireless networking dashes in a new direction [J]. IEEE Spectrum,2010,47(2):9-10.

[7] Adee S. Wireless sensors that live forever[J]. IEEE Spectrum,2010,47(2):14-14.

[8] 祝 利,林岳峥. 赛博空间电子战目标分析[J]. 航天电子对抗,2012,28(3):43-46.

[9] 肖新光. 管中窥豹-Stuxnet、Duqu 和 Flame 的分析碎片与反思[J]. 信息安全与通信保密,2012(7):18-19.

[10] 梁浩哲. 面向 COP 的战场态势信息可视化技术研究[D]. 长沙:国防科学技术大学,2007.

[11] 李 强,李加祥. 论指挥控制战与电子战[J]. 火力与指挥控制,1995,20(3):60-62.

[12] 李德毅. 指挥控制战研究和对策[J]. 舰船电子工程,1998(5):6-11.

[13] 王 刚,任清华. 赛博空间指挥控制问题研究[J]. 中国电子科学研究院学报,2011,6(3):243-247.

民机飞控计算机余度设计及可靠性分析

作者： 杨菊平， 董妍， 程俊强， YANG Ju-ping， DONG Yan， CHENG Jun-qiang
作者单位： 中国航空工业计算技术研究所,陕西 西安,710068
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(6)