

doi:10.3969/j.issn.1001-893x.2014.06.002

引用格式:唐法荣,刘宇.民机 CNS 系统动态重构技术[J].电讯技术,2014,54(6):700-706. [TANG Fa-rong, LIU Yu. Dynamic Reconfiguration Technology for CNS System of Civil Aircraft[J]. Telecommunication Engineering, 2014, 54(6):700-706.]

民机 CNS 系统动态重构技术*

唐法荣**,刘宇

(中电科航空电子有限公司,成都 611731)

摘要:动态重构是一项充分利用软硬件资源的技术。在介绍民机 CNS 系统和动态重构基本原理基础上,给出了一种动态重构的通用功能模块的设计方案,描述了利用有限状态机和排列组合原理计算系统配置的方法,并根据系统资源状况和应用的优先级对资源进行初次分配及再分配,设计出了一种动态重构算法,该算法能很好地兼顾资源备份式重构和资源抢占式重构。同时,指出对动态重构的品质设计需从可用性、可靠性、维护性方面考虑。最后,使用 Simulink 对动态重构算法的正确性进行了仿真验证。

关键词:民用飞机;通信导航监视系统;动态重构;模块化;资源备份;资源抢占

中图分类号:V243;TP273 **文献标志码:**A **文章编号:**1001-893X(2014)06-0700-07

Dynamic Reconfiguration Technology for CNS System
of Civil Aircraft

TANG Fa-rong, LIU Yu

(CETC Avionics Co., Ltd., Chengdu 611731, China)

Abstract: Dynamic reconfiguration is a technology which makes full use of software and hardware resource. The communication, navigation and surveillance (CNS) system of civil aircraft and the basic principle of dynamic reconfiguration are introduced, then a common function module for dynamic reconfiguration is presented. The calculation method for the system configuration is described by using a finite state machine and permutation and combination theory, and according to the state of system resources and priority of application for the primary and secondary allocation of resources, a dynamic reconfiguration algorithm is designed, which can effectively consider resource backup reconfiguration and resource preemption reconfiguration. It is pointed out that the usability, reliability and maintainability should be considered in quality design for dynamic reconfiguration. Finally, the correctness of dynamic reconfiguration algorithm is verified through Simulink's simulation.

Key words: civil aircraft; CNS system; dynamic reconfiguration; modularization; resource backup; resource preemption

1 引言

近年来,动态重构逐渐成为航空电子领域的一

项炙手可热的新兴技术。该技术以高速交换技术为基础,通过软硬件冗余备份、资源再分配、应用功能

* 收稿日期:2013-12-04;修回日期:2014-04-24 Received date:2013-12-04;Revised date:2014-04-24

基金项目:工信部基金项目(MJ-S-2001-17)

Foundation Item: Foundation of Ministry of Industry and Information Technology (MJ-S-2001-17)

** 通讯作者:tangfr@cetca.net.cn Corresponding author:tangfr@cetca.net.cn

再造等技术手段,防止航电系统全部或部分应用功能失效,确保即使在故障存在的条件下系统仍能按需安全工作,从而极大地降低航电系统生命周期费用,提高可靠性,增加飞机的可派遣能力。

在国外航空界,动态重构主要用于军事领域。在经典的四代航空电子系统演变中,第三代综合化航空电子结构已经具备动态重构雏形;在第四代综合化航空电子结构中,动态重构已达到较高水平,重构更为彻底,已经延伸到射频前端。在国内,动态重构研究主要集中在军航领域,由于该专业具有极强的保密性,相关信息很难在公开刊物上发现。在民机领域,国内真正启动民用大飞机项目在 2008 年前后,系统开展民机航电系统研究的历史相当短,从事民机动态重构技术研究的科研单位则更少。在工信部“基于 SCA 的 CNS 系统顶层设计及其关键技术研究”项目驱动下,本文将以动态重构算法为中心对民机 CNS 系统动态重构的基本原理、动态重构设计及其关键品质设计等方面进行较为深入的探讨。

2 CNS 系统概览

通信导航监视(CNS)系统是民用飞机航空电子系统的重要组成部分。通信子系统完成机内和机外话音及数据通信,包括甚高频(VHF)数据/话音通信、高频(HF)数据/话音通信、卫星通信(SATCOM)数据/话音通信、机内通话、音频综合、选择呼叫(SELCAL)、调谐控制、应急通信等多种功能。

导航子系统功能作用于民航客机起飞、巡航和进近着陆各个阶段,保障飞机安全航行。导航子系统包含 VOR、DME、ILS、GPS、ADF、RA 等设备。

监视子系统主要为飞机提供周边环境感知能力,作为航电系统主要传感器和信息源之一,包括气象回避、机载防撞、航管应答与增强近地告警功能。

3 动态重构基本原理

动态重构是以开放、标准和模块化的 IMA 硬件平台为基础,CNS 系统除对信号处理、信息处理、图像处理部分电路进行模块化设计外,还把 IMA 设计思想进一步扩展,对系统所用射频(RF)、中频(IF)电路亦进行模块化抽象,将其统一设计为通用功能模块(CFM),安装在一起,构成如图 1 所示的硬件平台。

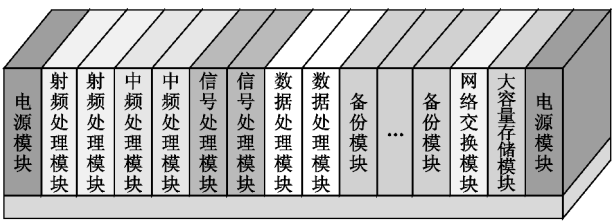


图 1 CNS 系统 IMA 平台
Fig. 1 The IMA platform of CNS system

图 1 中具有不同基础功能的通用模块在加载并运行指定功能的应用程序之后,经过交换矩阵或者网络总线进行互联,形成系统内的通信、导航、监视等应用功能。当某通用功能模块或应用程序故障时,按照动态重构算法在系统中选择合适备用模块和应用程序镜像,然后在网络交换模块支持下,根据重构策略数据库中的预定义过程,替代已发生故障功能模块或应用程序,从而实现动态重构。图 2 是动态重构原理框图。

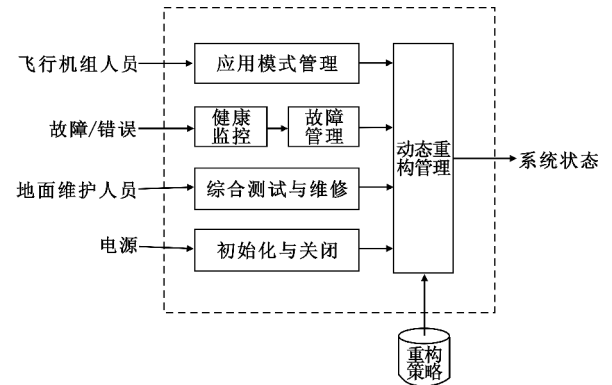


图 2 动态重构原理框图
Fig. 2 Block diagram of dynamic reconfiguration

触发系统动态重构的条件包括 4 种:应用模式改变(飞行机组人员触发);故障/错误(系统内故障管理功能触发);综合测试与维护(地勤维护人员触发);系统初始化与关闭(电源)。

系统上电,执行一系列预定动作后,开启动态重构及其他系统管理程序,进入系统缺省状态,形成初始配置。此时,飞行机组人员可根据不同飞行阶段(滑行、爬升、巡航、下降、降落)任务情况确定使用不同的通信导航监视功能,并把应用需求通知到“动态重构管理”,激励其产生动态重构。

系统初始化完成后就已启动健康监控功能。在工作过程中的任何时刻,倘若检测到应用功能故障,即刻驱动“动态重构管理”模块执行动态重构。

结束飞行任务后,飞行机组人员人工触发系统关闭信号,通知“动态重构管理”模块保存必要信息,释放所有软硬件资源,最后关闭电源。

“综合测试与维护”用于模拟“故障”和“应用模式改变”触发动态重构管理功能,方便系统在地面按需回放各种动态重构场景。

4 动态重构设计

4.1 模块化设计

模块化设计是健康监控及进一步实现动态重构的前提和基础,其设计产物是通用功能模块。作为动态重构的基本单位之一,CNS 系统内的通用功能模块种类多达 8 种,因此模块化设计是否成功很大程度上决定了系统动态重构管理的成败。模块化设计本身极其抽象,兼具主客观各种因素,有相当的难度,需要全面衡量诸如模块类型、功能粒度、处理能力、存储能力、技术透明性、互操作性、可生产性、可配置性、扩充能力、维护性、容错性、公共服务等诸多要素,并最终在这些不同要求之间获得平衡或折衷。

借用软件设计中面向对象思想,对 8 种通用功能模块的共同点逐一分析,将差异做进一步封装,同时结合 ASAAC 建议^[1],形成如图 3 所示原理图。

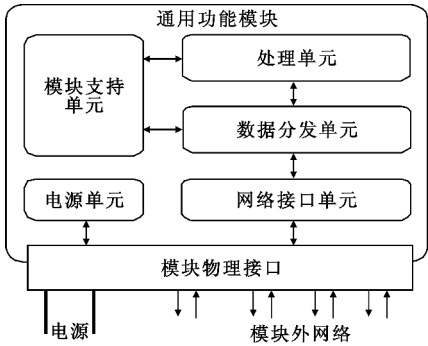


图 3 通用功能模块原理图
Fig. 3 Block diagram of CFM

通用功能模块由电源单元、模块支持单元、处理单元、数据分发单元、网络接口单元以及模块物理接口组成。

电源单元:转换标准背板电压为模块所需电压,并对电源电压滤波。

模块支持单元:存储模块标识信息,引导通用功能模块初始化,本地监控及配置应用功能。

处理单元:在模块支持单元协调控制下,处理单元运行特定可执行代码,实现系统赋予的应用功能。

一般为通用处理器、信号处理器、图形处理器、大容量存储器,甚至是射频或中频处理电路。

数据分发单元:负责模块内各单元间数据分发。

网络接口单元:与外部网络互连,根据系统策略,可采用 FC、RapidIO、Gbit 以太网等通信手段。

模块物理接口:通过接插件安装入机箱背板。

4.2 系统状态迁移

与普通民机航空电子设备需要认证一样,具有重构能力的 CNS 系统亦不例外,所以提供动态重构可预期证据显得异常重要,期望系统在任何时候状态始终是确定的。有鉴于此,设计者希望知道系统到底有多少种系统状态。注意到系统状态是系统配置的一一映射,换言之,可通过计算系统配置数量确定的状态。

由于系统配置与系统中应用功能种类、各种通用功能模块的备份数量密切相关,为简化计算模型,假定:

- (1) CNS 系统使用射频、中频、信号处理、数据处理、图像处理、网络交换、电源和大容量存储模块;
- (2) 电源模块能持续其他通用功能模块供电,其持续性由电源模块上的特殊电路设计保证;
- (3) 网络交换模块能保证其他通用功能模块自由互连;
- (4) 通用模块能够从大容量存储模块无障碍获取各种数据;
- (5) 每种应用均使用射频、中频、信号处理、数据处理、图像处理模块,其数量分别为 $m、n、j、k、l$;
- (6) 系统提供 c 种应用功能。

射频模块数量为 m ,能够为 c 种应用服务,考虑到同类模块标识等信息的不同,因此选法有 P_m^c 种。同理中频模块选法有 p_n^c 种,信号处理模块有 p_j^c 种,数据处理模块有 p_k^c 种,图形处理模块有 p_l^c 种,运用乘法原理得到系统配置数为

$$P_m^c \times P_n^c \times P_j^c \times P_k^c \times P_l^c \tag{1}$$

考虑到工程实际, c 不应超过 $m、n、j、k、l$ 的最小者,即满足

$$c \leq \min(m, n, j, k, l) \tag{2}$$

式(1)是一种较理想状况下的计算,工程应用中通常存在以下限制:

限制 1:射频模块分为 x 类,各类数量分别为 $m_1、m_2、m_3、\cdots m_x$,服务应用功能数量按类分别为 $Rc_1、Rc_2、Rc_3、\cdots Rc_x$;

限制 2:中频模块分为 y 类,各类数量分别为 $n_1、n_2、n_3、\cdots n_y$,服务应用功能数量按类分别为 $Ic_1、Ic_2、Ic_3、\cdots Ic_y$;

限制 3: $c_G(c_G < c)$ 种应用功能在 CNS 系统中会使用图像处理模块。需要射频模块有 x' 类,各类数量分别为 $m_1、m_2、m_3、\cdots m_{x'}$;需要中频模块有 y' 类,各类数量分别为 $n_1、n_2、n_3、\cdots n_{y'}$ 。

在此基础上,系统状态数改为

$$\begin{aligned} & \left(\sum_{i=1}^{x'} P_{m_i}^{Re'_i}\right) \times \left(\sum_{i=1}^{y'} P_{n_i}^{Ic'_i}\right) \times P_j^{c_G} \times P_k^{c_G} \times P_l^{c_G} + \\ & \left(\sum_{i=1}^{x'} P_{(m_i-Re'_i)}^{(Re-Re'_i)} + \sum_{i=x'+1}^x P_{m_i}^{Re_i}\right) \times \\ & \left(\sum_{i=1}^{y'} P_{(n_i-Ic'_i)}^{(Ic-Ic'_i)} + \sum_{i=y'+1}^y P_{n_i}^{Ic_i}\right) \times P_{(j-c_G)}^{(c-c_G)} \times P_{(k-c_G)}^{(c-c_G)} \end{aligned} \quad (3)$$

其中

$$\sum_{i=1}^x m_i = m \quad (4)$$

$$\sum_{i=1}^x Rc_i = c \quad (5)$$
$$\sum_{i=1}^y n_i = n \quad (6)$$
$$\sum_{i=1}^y Ic_i = c \quad (7)$$
$$\sum_{i=1}^{x'} Rc'_i = c_G \quad (8)$$
$$\sum_{i=1}^{y'} Ic'_i = c_G \quad (9)$$

系统动态重构就意味着系统状态迁移,触发系统重构的事件包括加电、掉电、任务模式改变、故障、测试维护,其中任务模式改变与飞机飞行剖面的起飞(P1)、爬升(P2)、巡航(P3)、下降(P4)、着陆(P5)密切相关。考虑到测试与维护是任务模式改变和故障驱动重构的地面演练,如图 4 给出了有限状态机示意图。

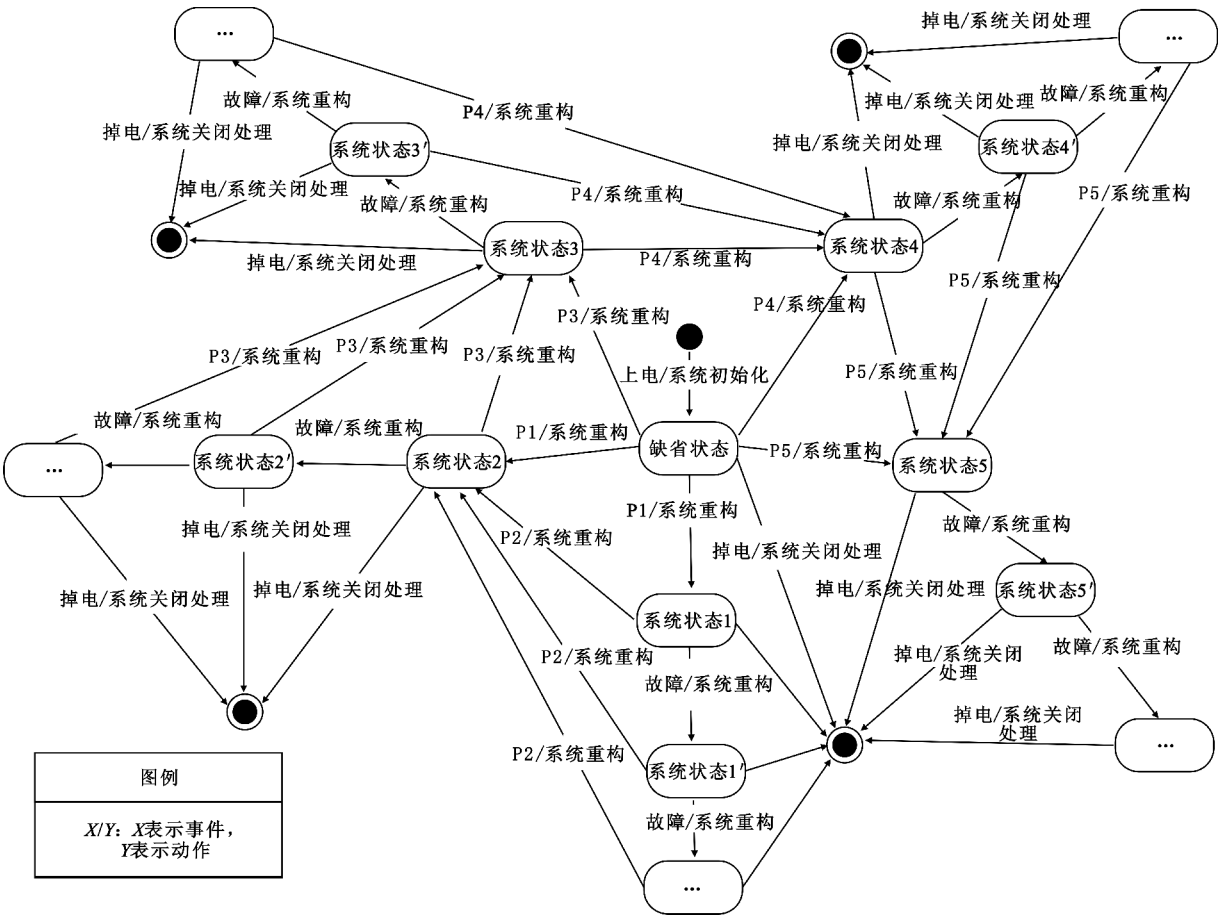


图 4 CNS 系统状态迁移图
fig. 4 State transition graph of CNS system

限于篇幅,图 4 没有画出所有状态,但这并不改变该图为有限状态图的本质,原因在于 CNS 系统内

的应用功能和通用功能模块数量均是有限的,必然存在一种方法总能以应用功能为索引有限次遍历和

覆盖所有通用功能模块。

4.3 动态重构算法设计

动态重构算法设计的核心目的是解决资源初次分配及再分配问题,由资源备份式算法和资源抢占式算法组成。顾名思义,前一种算法在重构过程中使用系统备份资源,后一种算法在重构过程中使用从其他低优先级应用功能剥夺的系统资源,后者是前者的延续和补充。系统动态重构过程优先使用资源备份式算法,在备份资源不能满足重构需求时使用资源抢占式算法。

图 5 是动态重构算法的顶层描述,电源“上电”驱动系统工作在缺省状态并根据上电自检情况填写系统资源表信息。工作中,如果任务模式发生改变,应将新任务中不再使用的资源释放;如果故障发生,应确定是否当前工作在缺省状态,在缺省状态下资源故障不需要引发动态重构。无论是改变任务模式还是故障引起的重构,均首先判断资源是否足够,资源充足则执行备份式重构,反之执行抢占式重构,然后等待下一次重构事件。系统任何时候接收到“掉电”事件,均立即执行系统关闭处理。关于备份式重构更详细的设计信息见图 6,抢占式重构更详细的设计信息见图 7。

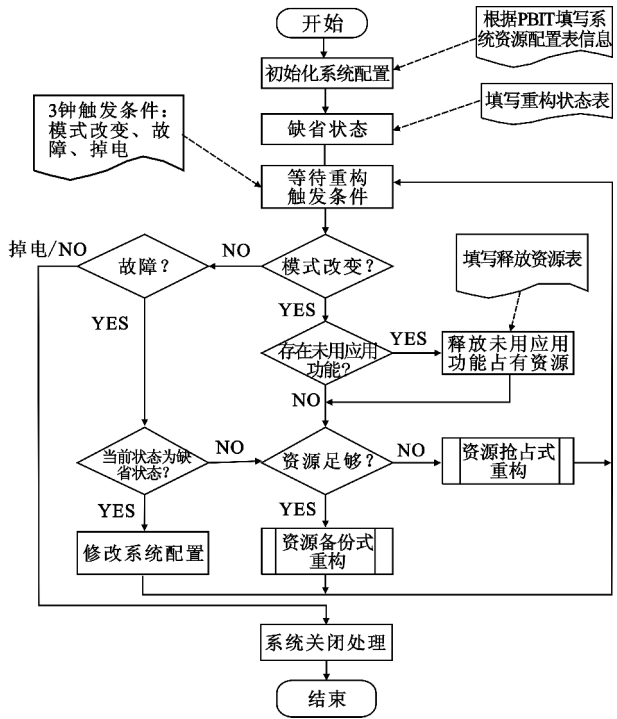


图 5 动态重构算法顶层设计
Fig. 5 The top-level design of dynamic reconfiguration algorithm

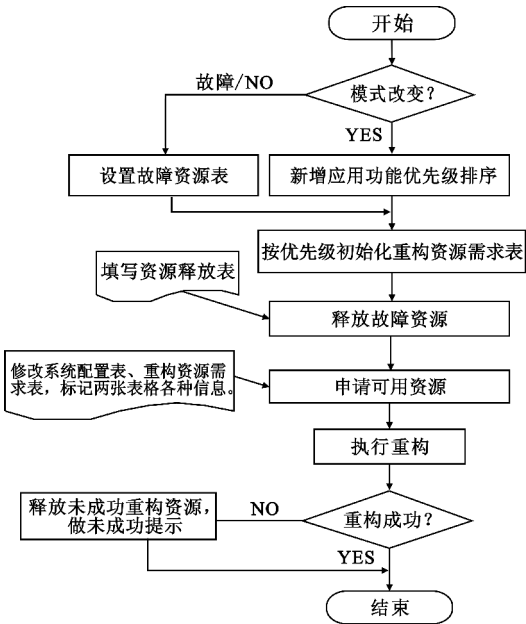


图 6 备份式算法流程
Fig. 6 The process of backup algorithm

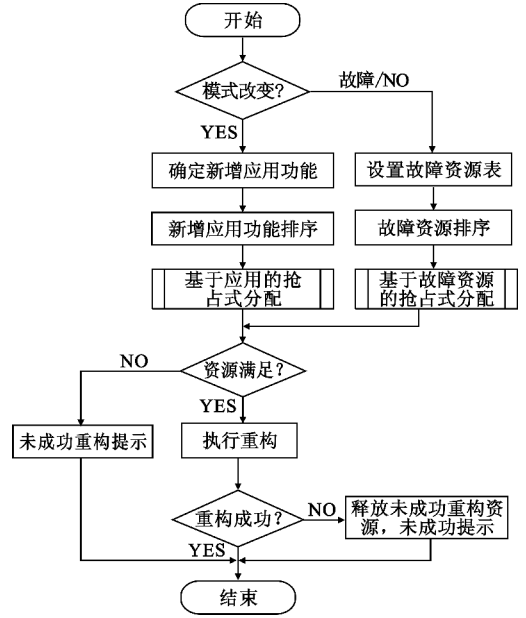


图 7 抢占式算法流程
Fig. 7 The process of preemptive algorithm

一般而言,模式改变引起的重构会导致新增多个应用功能的需求,而故障引起的重构仅导致局部通用功能模块资源甚至仅是通用功能模块上处理单元的需求,在备份式算法中,把故障和模式改变引起的申请统一到资源级,并最终与重构资源需求表的形式体现,这样可极大地简化后续资源申请的实现。对于抢占式算法,因模式改变和故障触发引发的资源分配需求差异巨大,为使设计逻辑更简洁清晰,对

两者进行分类处理。

5 关键品质考虑

5.1 可用性

可用性(Usability)是产品的基本自然属性^[2],是最终用户使用产品的可用程度,在产品和用户的相互作用中体现,其基本评价指标是效率、满意和安全。可用性在不同专业领域,评价的参数和指标不完全相同,不存在绝对适用标准。对于机载 CNS 系统动态重构:

- (1)精心设计飞行操作过程,使操作者把感知和思维集中在任务,不必分心考虑如何把自己的任务转换成计算机可识别的方式和过程;
- (2)模仿传统多功能显示、无线电调谐单元、音频控制面板、告警控制面板操作,把动态重构这种物理和概念上的变化对操作者屏蔽;
- (3)操作界面友好,即使没有较深通信导航监视专业知识,操作者也能理解人机界面结构与图标含义,尤其针对应急情况提供“一键操作”能力。

5.2 可靠性

可靠性(Reliability)是指产品在规定条件下,规定的时间内,完成规定功能的能力^[3]。从专业角度来看,可靠性越高,意味着平均故障间隔时间(MT-BF)越长。提升 CNS 系统的可靠性除采用资源备份手段外,还可以在硬软件设计方面挖掘潜力。在硬件设计方面,价格相同情况下,选择性能指标占优元器件;设计过程中,全面使用可靠性预计/分配、降额、热设计、EMC 设计、安全设计等手段。在软件设计方面,采用 VxWorks653、Integrity-178、LinuxOS-178 等安全等级更高的操作系统,对关键应用实施分区隔离,变动态重构集中管理为分布式管理;以更苛刻的软件开发标准,比如 DO-178C 或 NASA-STD-8719.13B 来指导软件开发,用更加严格的目标和过程来规范软件开发活动^[4],从而达到提高软件乃至系统可靠性目的。

5.3 维护性

维护性(Maintainability)是在给定条件下使用预定规程和资源进行维护时,设备保持在或恢复到执行要求功能状态的能力^[5]。在 CNS 系统中,通过

上电自检、周期自检以及启动自检为系统提供全方位故障诊断覆盖,在此基础上获得故障快速定位和隔离。此外,系统采用模块化设计方法,大大降低模块种类,易识别易记忆。不仅如此,系统结合动态重构特点,增加特有的综合测试与维护功能,快速重现飞行中出现的重构过程,更全面地改善维护性能。

6 算法仿真验证

CNS 动态重构算法使用 Matlab Simulink 7.8.0.347 仿真算法逻辑,人机界面使用 LabWindows 2010 编程展示,分别部署于不同计算机,两者之间基于 UDP/IP 以太网互连,使用上/下位机模式。图 8 是 Simulink 使用射频、中频、信号处理、数据处理原型模块建立的算法顶层模型,图中 4 个重构模型的子模型没有进一步示出。

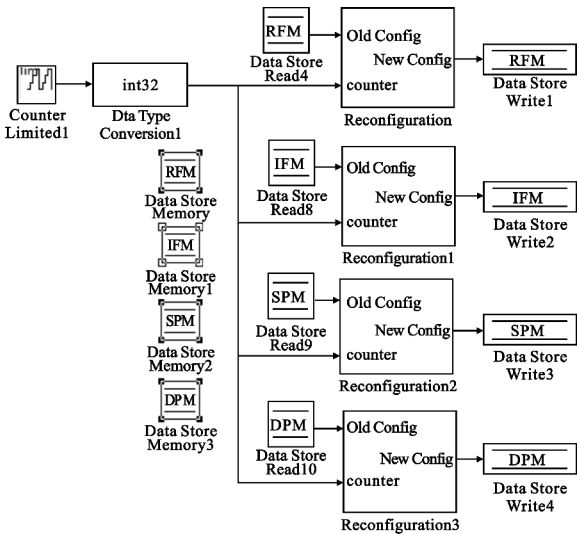


图 8 算法仿真顶层模型
Fig. 8 Algorithm simulation top model

建模完成后,按照任务模式和故障状态准备所有场景并依次输入仿真模型。图 9 是假定系统最多同时具备 10 种应用功能,每种应用功能需要射频、中频、信号处理、信息处理模块资源,每种功能模块备份 2 块,在系统初始状态时所有功能模块均正常的情况,执行场景:“应用功能 3”的射频模块和数据处理模块故障,“应用功能 5”的数据处理模块故障之后,仿真界面显示的模块使用以及应用功能状态情况。需要说明的是,场景数量取决于系统中应用功能数量以及为每种应用功能配备的模块数量。

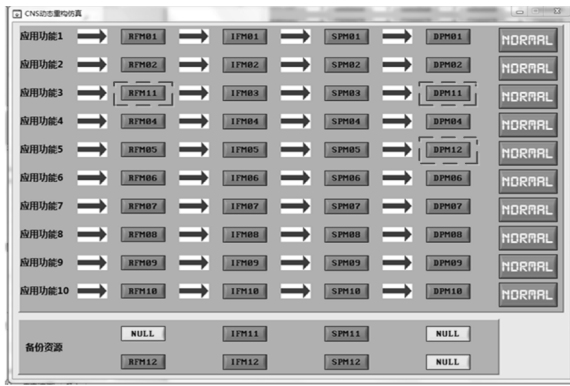


图9 仿真界面
Fig.9 Simulation interface

实际的工程系统是有界的, 所以其应用场景数量也是有限的。基于此, 采用归类有限穷举模式, 枚举出该系统下的所有场景, 用脚本语言对其进行描述, 并逐一把这些场景驱动运行在服务器上的动态重构仿真模型, 仿真模型在接收到重构指令后根据模型自身逻辑进行信号和数据处理流程, 输出仿真结果, 周而复始, 直至所有场景被全部执行。仿真验证情况表明, 仿真结果完全符合算法对资源选择的理论预期。

7 结束语

动态重构是一项非常有意义的工程应用研究课题, 覆盖系统、硬件、软件甚至机械、电气等诸多技术层面。本文介绍了动态重构基本原理、动态重构所关注的设计要素以及在此基础上构建的动态重构算法, 这些思路或方法对可重构系统具有一定的指导意义。但是, 实际系统还需要根据具体边界和限制条件适当调整。

关于动态重构, 还有很多工作需要继续深入开展, 比如大功率电路交换、动态重构算法完善、树状

管理、以重构为目标的模块化设计等。故障管理虽不是动态重构组成部分, 但其输出结果的置信度却直接关系动态重构成败, 作为技术延伸, 故障管理研究也是重要努力方向。另外, 动态重构对适航认证带来的挑战必须引起足够重视。

参考文献:

[1] Allied Standard Avionics Architecture Council. Modular and Open Avionics Architectures[M]. Brussels:NATO,2004.

[2] Nielsen J. 可用性工程[M]. 刘正捷,译. 北京: 机械工业出版社, 2004.

Nielsen J. Usability Engineering [M]. Translated by LIU Zheng-jie. Beijing:China Machine Press,2004. (in Chinese)

[3] 曾声奎. 可靠性设计与分析[M]. 北京: 国防工业出版社, 2011.

ZENG Sheng-kui. Design and analysis of reliability[M]. Beijing: National Defense Industry Press,2011. (in Chinese)

[4] SC-205, Software Considerations in Airborne Systems and Equipment Certification[S].

[5] 吕川. 维修性设计分析与验证[M]. 北京: 国防工业出版社, 2012.

LV Chuan. Design analysis and verification of maintenance[M]. Beijing: National Defense Industry Press, 2012. (in Chinese)

作者简介:



唐法荣(1973—),男,四川安岳人,2008年于电子科技大学获工程硕士学位,现为系统分析师/高级工程师,主要研究方向为民机通信导航系统架构、基于 DO-178C 的安全关键软件。

TANG Fa-rong was born in Anyue, Sichuan Province, in 1973. He received the M. S. degree from University of Electronic Science and Technology of China in 2008. He is now a senior engineer. His research concerns architecture of civil aircraft communication & navigation system, and safety critical software based on DO-178C.

Email: tangfr@cetca.net.cn