

综合电子系统重构时间分析方法研究

郑小鹏,王小辉,陈春燕

(中国运载火箭技术研究院研究发展部,北京 100076)

摘要: 针对综合电子系统重构的不确定性、多样性导致的系统状态复杂的问题,对不同重构模式下的重构时间进行分析。首先研究系统架构和软硬件配置,建立系统重构和重构时间模型,提出应用迁移优化算法。然后通过综合电子系统重构验证平台模拟故障,分析计算不同类型故障导致系统重构消耗的时间。实验证明,不同类型的故障导致的系统重构时间不同,优化重构蓝图和迁移过程可以有效缩短重构时间。

关键词: 综合电子系统;重构;时间分析;系统验证

中图分类号: TN702

文献标识码: A

DOI:10.16157/j.issn.0258-7998.212469

中文引用格式: 郑小鹏,王小辉,陈春燕. 综合电子系统重构时间分析方法研究[J]. 电子技术应用, 2022, 48(5): 110–113.

英文引用格式: Zheng Xiaopeng, Wang Xiaohui, Chen Chunyan. Research on reconfiguration time analysis method of integrated modular avionics system[J]. Application of Electronic Technique, 2022, 48(5): 110–113.

Research on reconfiguration time analysis method of integrated modular avionics system

Zheng Xiaopeng, Wang Xiaohui, Chen Chunyan

(Research and Development Department of China Academy of Launch Vehicle Technology, Beijing 100076, China)

Abstract: As the uncertainty and diversity of the reconstruction of the integrated modular avionics system lead to complex problems of the system state, the reconstruction time under different reconstruction modes is analyzed. First, by studying the system architecture and software and hardware configuration, the system reconstruction and reconstruction time model is established, and the application migration optimization algorithm is proposed. Then the integrated modular avionics system reconstruction verification platform simulates the failure, and calculates the time consumed by the system reconstruction caused by different types of failures. The results of simulation reveal that different types of failures lead to different system reconstruction times, and optimizing the reconstruction blueprint and migration process can effectively shorten the reconstruction time.

Key words: integrated modular avionics system; reconfiguration; time analysis; system verification

0 引言

综合电子系统重构是指在系统资源或运行环境故障影响下,为保障系统功能和性能正常,重新配置系统的软硬件资源的过程。综合电子系统逻辑映射具有多样性和不确定性^[1],如何在保证系统正常重构情况下,在满足系统的可靠性和安全性要求下,提高系统的资源利用率和架构灵活性,已成为综合电子系统的重要研究方面。

目前,对综合电子系统重构的研究主要包含系统重构配置、重构机制、重构模型的建立与优化、重构蓝图的设计与生成等^[2-4]。Chu^[5]等提出一种在考虑功能冗余要求的情况下优化综合电子系统配置方案的方法,针对具有功能冗余要求的通用综合电子系统,给出了配置方案模型及其相关的可调度性和可靠性约束。Fontoura^[6]等提出通过重构状态空间的转换,将增强 AADL 规范的故障模型与重构逻辑相结合,来表示容错能力。罗庆^[7]等提出一种基于改进 Q 学习的重构蓝图生成方法,综合考

虑重构影响、重构时间、重构降级以及负载均衡等多优化目标。综上所述,国内外目前很少对于综合电子系统重构时间分析的研究,求解综合电子系统重构时间的方法大多来自仿真实验,这使得综合电子系统重构的可靠性分析面临着安全隐患。

本文通过对综合电子系统、系统重构和重构时间进行建模,依据对综合电子系统架构、重构策略和重构过程的研究,搭建综合电子系统可重构平台,基于理论基础和重构验证平台对重构时间进行分析和验证。

1 综合电子系统建模分析

根据综合电子系统的组成和特点,对综合电子系统软硬件进行建模,描述在系统硬件上的软件的配置模型,分析故障触发下的系统重构,建立重构时间模型,设计应用迁移优化算法。

1.1 综合电子系统模型

综合电子系统由系统硬件和系统软件组成。为实现

可重构综合电子系统,在系统上搭载多个处理器,实现多核心并行处理机制。

1.1.1 系统硬件模型

综合电子系统的核心组件包括处理器、存储器、总线和外围设备等。对系统中的处理器和总线建模,令处理器为 C ,总线为 B ,系统内核心硬件集合表示为:

$$S=\{C_1, C_2, \dots, C_m, \dots, B\} \quad (1)$$

处理器集合表示为:

$$C=\{C_1, C_2, \dots, C_m\} \quad (2)$$

每个处理器包含多个核心,处理器核心集合表示为:

$$C_i=\{P_1, P_2, \dots, P_m\} \quad (3)$$

系统总线是处理器间数据传输的通道,主要包含总线宽度和传输带宽,表示为:

$$B(B_{\text{type}}, B_{\text{bw}}) \quad (4)$$

1.1.2 系统软件模型

综合电子系统包含一系列软件应用,表示为:

$$App=(App_1, App_2, \dots, App_n) \quad (5)$$

相关属性表示为:

$$App_i(A_{\text{cmd}}, A_{\text{data}}, A_{\text{req}}) \quad (6)$$

式中, A_{cmd} 代表软件可执行程序大小, A_{data} 代表软件运行时数据所需存储空间, A_{req} 代表软件优先级。

为保证软件正常运行,将软件部署在处理器核心上,部署关系表示为:

$$AC_i=App_i \rightarrow C_i P_m \quad (7)$$

系统配置是软硬件间建立关系的映射,表示为:

$$SC_i=\{AC_1, AC_2, \dots, AC_i, \dots, AC_n\} \quad (8)$$

其中, AC_i 表示应用 App_i 的部署情况, SC_i 表示系统的配置。

1.2 系统重构模型

综合电子系统的故障类型主要有处理器故障和处理器核心故障,处理器 C_i 故障表示为 F_i ,处理器 C_i 的核心 $C_i P_j$ 故障表示为,系统故障定义为 F_j :

$$Fault \in F_i \cup F_j \quad (9)$$

综合电子系统重构迁移模型表示为系统在故障触发下从一个配置运行状态迁移到新的配置运行状态,定义为:

$$RC_i=SC_j \xrightarrow{\text{Fault}} SC_k \quad (10)$$

其中 RC_i 代表系统重构蓝图, SC_j 表示系统在故障发生前的运行状态, SC_k 表示在故障发生后系统进入的状态。当系统在状态 SC_j 下发生不可恢复的故障,进入到故障状态 SC_{fault} ,图 1 表示系统 10 种运行状态对应的 16 种重构蓝图的状态迁移图。

1.3 重构时间模型

若处理器内某个核心发生故障,可以由其他核心承担故障核心应用的运行,核心间应用迁移相对简单,包含应用撤销和应用绑定,核间重构时间模型表示为:

$$t_{\text{EL}}=t(A_R)+t(A_B) \quad (11)$$

其中, $t(A_R)$ 表示应用撤销需要的时间, $t(A_B)$ 表示应用绑定需要的时间。

若系统内某处理器发生故障,需要将该处理器上部署的应用迁移到其他处理器上,在迁移过程中产生应用撤销、应用加载、应用绑定及状态同步等动作。处理器间重构时间模型表示为:

$$t_{\text{EEL}}=t(A_R)+t(A_B)+t(A_D) \quad (12)$$

其中, $t(A_L)$ 表示故障应用重新加载需要的时间, $t(A_D)$ 表示故障应用恢复需要的时间。

系统重构包含了核间重构和处理器间重构,其重构时间的长短直接由迁移过程规划决定,为了减少迁移产生时间,不同处理器间通常采用并行迁移方式。执行优化算法会产生两个集合,一个是可并行迁移的应用 A_{en} ,另一个是只能单独迁移的应用 A_{dis} 。其算法步骤如下:

(1) 获得需要迁移的应用列表;

(2) 依据并行迁移属性对应用分类,并放入集合和集

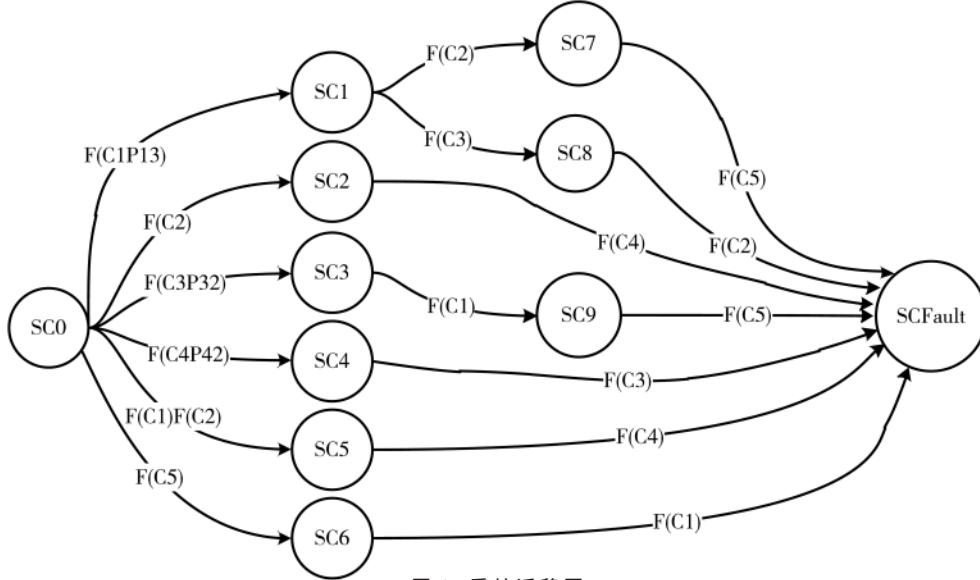


图 1 系统迁移图

合中；

(3)对于集合,依据硬件资源约束将同时迁移的应用划分为一组,最终将分为若干可并行迁移的应用组,每一个应用组表示为:

$$\{App_i, \dots, App_j\} \quad (13)$$

(4)探索最小迁移策略:验证每个可并行迁移应用组的可行性,并进行调整;

(5)只能单独迁移的应用按顺序执行,得到最终优化后的最短时延迁移策略最优解集:

$$S_{TD} = \{[App_i, \dots, App_j], \dots, [App_k, \dots, App_l], A_m, \dots, App_n\} \quad (14)$$

最优解集中方括号内表示可并行迁移应用,最后的单独应用表示顺序迁移应用。

2 综合电子系统重构验证平台

为验证系统重构过程对系统正常运行的影响,本文搭建了综合电子系统重构验证平台,通过模拟系统运行中产生的故障,计算系统重构消耗的时间,分析重构过程的可靠性和安全性。

系统的总体架构主要包含综合电子系统和重构管理监控系统,验证平台执行流程主要由两系统间指令和数据的交互产生,如图2所示。

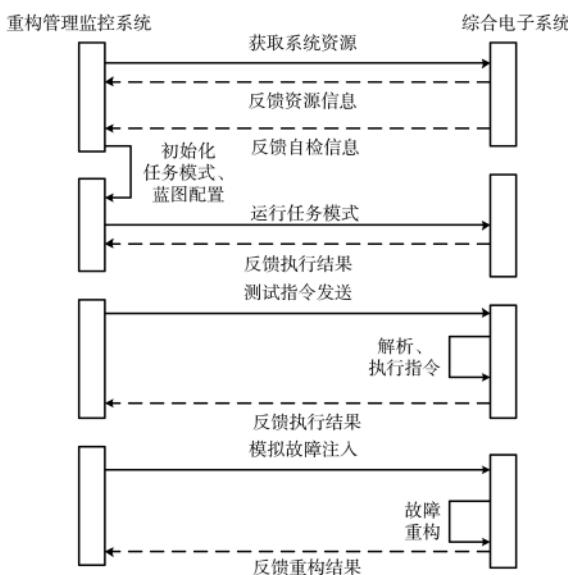


图2 执行总体流程

综合电子系统重构验证平台执行流程如下:

(1)综合电子系统首先对软硬件资源进行虚拟化管理,然后向重构管理监控系统资源信息和自检信息。

(2)通过系统间的通信来配置任务模式蓝图,并将任务执行结果反馈给重构管理监控系统。

(3)综合电子系统接收重构管理监控系统的测试指令并对其进行解析和执行,将执行结果反馈给重构管理系统。

(4)重构管理监控系统通过故障模拟,将故障通过指令注入综合电子系统,综合电子系统执行重构恢复正常状态后,将系统状态反馈给重构管理监控系统。

3 实验验证分析

本文通过综合电子系统重构验证平台对综合电子系统重构时间进行实验验证。通过计算重构过程消耗的时间、重构蓝图的部署来验证重构过程的有效性和正确性。

3.1 实验环境

综合电子系统重构验证平台软件应用相关属性如表1所示。综合电子系统应用的初始配置如表2所示。

表1 平台软件属性

应用名称	应用标识	应用大小/MB	应用执行周期/ms	执行所需内存/MB	所需磁盘空间/MB
健康管理	APP ₁	28	1	12	62
飞行管理	APP ₂	30.8	4	6	86
飞行控制	APP ₃	32.6	2	8	54
相机成像	APP ₄	40.5	5	10	256
重构管理监控软件	--	420	--	100	500

表2 应用初始部署

处理器模块	处理器核心	应用部署
处理器 A (主处理器)	核心 1	健康管理
	核心 2	相机成像 飞行管理 飞行控制
处理器 B (备处理器)	核心 1	健康管理

3.2 实验过程设计

向综合电子系统注入三种类型的故障进行重构时间的分析和验证,分别是处理器单核心故障、处理器故障和多级故障。本文重构时间验证基于处理器A作为主处理器,处理器B作为备用处理器,向综合电子系统处理器A中注入核心1故障、核心2故障和处理器故障并分别进行实验验证和数据分析。对每个注入综合电子系统的故障都使用基于强化学习的智能重构^[8]方法生成对应的重构蓝图。

3.3 重构时间分析验证

当发生处理器A核心1故障,需要对部署在核心1上的应用进行迁移,由于核心2可以承担故障应用的运行,只需进行核心间重构,将核心1上的应用迁移到核心2即可;当发生处理器核心2故障时,需要对部署在核心2上的软件进行迁移重构;当处理器A发生故障时,需要对处理器A上部署的所有应用进行重新部署。迁移过程消耗的时间理论值如表3所示。

综合电子系统重构验证平台对3种故障分别进行100故障模拟,三种故障实验相关数据如表4所示。

表 3 重构迁移过程理论消耗时间值分析

故障类型	重构步骤	消耗时间/s
处理器 A	健康管理应用恢复	0.000 01
核心 1 故障	相机成像应用恢复	0.000 03
	飞行管理应用静态数据迁移	0.030 8
	飞行管理应用内存数据迁移	0.006
处理器	飞行管理应用恢复	0.000 3
核心 2 故障	飞行控制应用静态数据迁移	0.032 6
	飞行控制应用内存数据迁移	0.008
	飞行控制应用恢复	0.000 4
	飞行管理应用静态数据迁移	0.030 8
	飞行管理应用内存数据迁移	0.006
处理器 A 故障	飞行管理应用恢复	0.000 3
	飞行控制应用静态数据迁移	0.032 6
	飞行控制应用内存数据迁移	0.008
	飞行控制应用恢复	0.000 4

表 4 实验数据汇总

故障类型	处理器 A 核心 1 故障	处理器 A 核心 2 故障	处理器 A 故障
重构时间理论值	0.000 4	0.078 1	0.141 5
实验均值	0.000 39	0.077 6	0.140 6
最大差值	0.000 15	0.005 5	0.010 6
最小差值	0	0.000 4	0.000 1
均值差值	0.000 01	0.001 1	0.000 9
实验值方差	$0.879\ 98 \times 10^{-5}$	$0.961\ 00 \times 10^{-5}$	$1.225\ 0 \times 10^{-5}$

由表 4 可知,三种故障类型的实验值方差都很小,说明实验产生的重构时间比较稳定,重构蓝图的执行效果较好。

处理器 A 的核心 1 故障比核心 2 故障导致的重构时间显著要小,其原因是核心 1 故障引起的重构过程只有应用载处理器内部的部署表示,而核心 2 故障还需要进行应用指令和数据迁移,受处理器间传输带宽影响,重构消耗时间就更长。处理器 A 故障导致的重构时间最长,由于迁移的应用数量较多,需要对迁移过程进行优化,对于处理器 A、B 共同部署的应用还需要进行主备切换。

综上所示,综合电子系统重构时间与故障类型及其重构蓝图有关,故障对系统影响越大,重构蓝图越复杂,重构消耗时间也越长。

4 结论

本文基于可重构综合电子系统架构,研究了综合电子系统重构时间方法。首先基于综合电子系统模型,对系统的软硬件进行建模;然后通过分析系统运行过程中产生的故障类型对综合电子系统重构迁移过程进行建模。总结核间重构时间、处理器间重构时间和系统重构时间的计算公式,利用综合电子系统重构验证平台进行故障模拟和重构时间验证。实验证明,重构时间因不同故障类型导致的系统重构有所差异,通过优化重构蓝图和迁移过程可以有效缩短重构过程消耗的时间。

参考文献

- [1] 程桢.模型驱动的IMA系统资源配置分析与验证及优化方法研究[D].南京:南京航空航天大学,2016.
- [2] CUI Y, SHI J, WANG Z. Backward reconfiguration management for modular avionic reconfigurable systems[J]. IEEE Systems Journal, 2018, 12(1): 137–148.
- [3] 王世海,周思远,刘斌.一种基于遗传算法的IMA系统动态重构策略优化方法:CN108268710A[P].2018.
- [4] 王鹏,阎芳,白杰,等.一种综合模块化航电系统重构决策系统及决策方法:CN103825902B[P].2017.
- [5] CHU J, ZHAO T, JIAO J, et al. Optimal design of configuration scheme for integrated modular avionics systems with functional redundancy requirements[J]. IEEE Systems Journal, 2021, 15(2): 2665–2676.
- [6] FONTOURA A A D, NASCIMENTO F A M D, NADJMI-TEHRANI S, et al. Timing assurance of avionic reconfiguration schemes using formal analysis[J]. IEEE Transactions on Aerospace and Electronic Systems, 2020, 56(1): 95–106.
- [7] 罗庆,张涛,单鹏,等.基于改进 Q 学习的IMA系统重构蓝图生成方法[J].航空学报,2021,42(8):327–336.
- [8] 董世琨.综合电子系统智能重构技术研究[D].2020.

(收稿日期:2021-12-14)

作者简介:

郑小鹏(1984-),男,硕士,高级工程师,主要研究方向:飞行器总体设计。

王小辉(1981-),男,硕士,研究员,主要研究方向:飞行器总体设计、综合电子总体集成设计。

陈春燕(1982-),女,硕士,高级工程师,主要研究方向:综合电子总体集成设计。



扫码下载电子文档

版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所