文章编号:1671-4598(2019)12-0142-04 DOI:10.16526/j.cnki.11—4762/tp.2019.12.032 中图分类号:TP311 文献标识码:A

基于安全分区操作系统的容错计算机软件架构

马小博[1], 王 芳[2], 程俊强[1]
(1. 西安航空计算技术研究所, 西安 710068;
2. 空装驻西安地区军事代表局第六代表室, 西安 710068)

摘要: 机载计算机的综合化程度越来越高, 综合了飞行器的多种任务功能, 需要满足不同系统不同余度配置的安全要求; 这种高可靠的容错计算机对软件的要求越来越高, 为了确保不同系统应用程序在时间上空间上的彼此隔离互不影响, 在高安全性的实时操作系统中提出了分区 (Partition) 的概念; 介绍了一种高可靠机载容错计算机的系统结构, 以及在 INTEGIRTY 分区操作系统下容错计算机的软件架构、系统调度、余度管理等。

关键词: 容错; 分区操作系统; 系统调度; 余度管理

Fault—tolerant Computer Software Architecture Based on Partition Operating System

Ma Xiaobo[1], Wang Fang[2], Cheng Junqiang[1]
(1. Xi'an Aeronautics Computing Technique Research Institute, AVIC, Xi'an 710068, China;
2. Air Force Equipment Department Sixth Military Delegate Room at, Xi'an 710068, China)

Abstract: Airborne Computer are becoming more and more integrated , It integrates multiple mission fun actions of aircraft, Airborne Computer need to meet the safety requirements of different redundancy of systems。 The Computer' s software require more Complicated , In order to ensure different system applications are isolated from each other in time and space, the concept of Partition is proposed in operating system。 The paper introduces an architecture of a highly reliable fault—tolerant computer and its software architecture、system scheduling and redundancy management under ITEGRITY partition OS.

Keywords: fault—tolerant; partition OS; redundancy management; system scheduling

0 引言

飞行器的安全关键系统采用了高可靠容错计算机平台, 计算机执行包括飞行控制、发动机控制、公共设备管理等多种平台的子系统功能, 这种综合多种功能的容错计算机相比较以前单独支持一个子系统的专用计算机在操作系统、容错余度管理等方面发生了较大的变化, 以飞行控制计算机为例, 支持单个子系统功能的飞行控制容错计算机只需要包含飞控系统的多余度管理与解算, 而综合多功能任务的飞控高可靠容错计算机既要具有飞控系统的多余度安全, 同时又需要满足发动机控制、机电管理等不同系统、不同余度配置的安全要求。另一方面高可靠容错计算机从系统结构、容错技术等方面要适应不断变化的微电子技术和计算机技术的发展, 保持飞行器平台具有相对的稳定性, 更要具有灵活的系统配置能力[1]。

随着功能综合化程度的提高, 容错计算机中的软件越来越复杂, 地位也越来越重要, 对操作系统的要求越来越高。但是传统的实时操作系统由于并不是针对这些日益复杂的要求而开发的, 因此在实时性、可靠性、安全性等方面或多或少的存在一些缺陷, 已经不能满足飞管平台综合化的新要求, 因此必须研究满足高安全性的实时操作系统, 保证应用软件的可重用性与可移植性[2]。保证多应用软件和操作系统与硬件的无关性, 保证通信和容错的透明性, 从而降低系统全寿命周期费用、缩短研制开发周期[3]。

本文就是针对新技术下出现的综合化容错计算平台, 研究支持该平台的软件体系结构、分区结构、余度管理、系统调度、健康监控等关键技术。

1 高安全分区操作系统

绿山公司的"INTEGRITY RTOS"从时域 (CPU 时间) 和空间域 (存储空间) 确保了资源可用性。在空间域中, 系统按照需求分配给每个分区 (在 INTEGRITY 中称为 Kernel Space 或 Address Space) 固定的存储区域, 各个分区的存储区域使用彼此独立, 没有影响[4]。在时域, 系统按照需求在一个主帧周期 (Major Frame Period, 亦即 ARINC653 标准中的主时间帧, Major Time Frame) 中分配给每个分区一定的 CPU 时间, 各个分区中在自己的 CPU 时间内执行, 各分区的任务不能用生成子任务的方式占用其他分区的 CPU 时间。采用分区技术, INTEGIRTY 保证了各个分区 (任务) 间不受干扰, 防止错误蔓延。而系统内核空间拥有自己的内核栈, 保证应用分区不会影响系统的安全。同时 INTEGRITY 系统还支持符合 ARINC653 标

收稿日期:2019-08-29; **修回日期**:2019-09-20。

作者简介:马小博(1979-),男,陕西渭南人,高级工程师,主要从事容错计算机方向的研究。

准的分区调度。

2　容错计算平台系统架构

高可靠容错计算机系统作为飞行器的安全关键部件需要利用系统中的多个冗余节点来保障其可靠性。按照最高安全等级的故障容限，余度计算机应能够达到“两次故障工作、三次故障安全”的故障容限，这种故障容限需要由 4 余度容错系统或者高检测率的 3 余度容错系统实现[5]。对于 3 余度系统，要实现“两次故障工作、三次故障安全”的故障容限，每个冗余节点内部必须能 100％的检测出工作节点自身的故障[6]。

2.1　工作方式

高可靠容错计算机系统包括三个节点计算机，节点计算机内部的功能模块通过容错串行总线互连，并且需要保持高覆盖率的故障检测，因此节点计算机内部必须包含完备的监控组件，由监控组件对计算机工作过程中产生的数据信息进行比较监控。节点计算机之间采用同步工作方式，系统任务分配在各个节点计算机上执行，节点内的核心处理模块通过错串行总线实现 CCDL（交叉数据链路）的功能，实现节点内部的信息交换。同时三节点计算机通过容错高速串行网络管理系统各节点之间的信息交换，节点内将监控有效的数据发送到各个节点，同时收取其他节点监控有效的数据，按照一定的逻辑顺序，各节点共同选取某一节点的有效数据和信息，并将有效数据和信息交由运行在容错计算机上的不同应用进行计算，对计算结果进行相同的监控与表决后输出有效的计算结果，节点机内的一次故障，不会导致该节点机的失效。

2.2　硬件组成

节点计算机的配置形式如图 1 所示，每个节点机由 5 个功能模块组成，分别为数据处理模块 1（CPM1）、数据处理模块 2（CPM2）、专用接口模块（IOM）、电源模块（PSM）、总线通讯模块（NSM）。其中 CPM1 负责作为主模块负责所有系统的应用程序运行，实现容错计算机的应用功能；CPM2 实现对数据处理模块 1 的监控，及时发现数据处理模块的软硬件错误，从而达到故障告警的作用，并能将故障信息告知其他两个节点；IOM 作为专用接口模块实现与外部专用设备的信息交互，输入输出信号转换等；NSM 实现与外部交联设备的网络信息交互，同时实现与其他节点计算机的数据信息交互实现了一种串行容错总线的功能。

2.3　关键技术

3 节点容错计算机除了在硬件上需要完整的硬件监控组件。工作方式会发生变化，容错的工作方式，特别是软件结构的重大变化：包括余度管理中节点机同步、节点机表决监控、输入输出数据处理等，存在着较大的变化。同时为适应实现更多的应用功能的需求，同时满足高可靠的容错需要，其分区方式分区调度等也是开发的难点。通过分区操作系统实现多应用的隔离和资源共享，通过分层级的

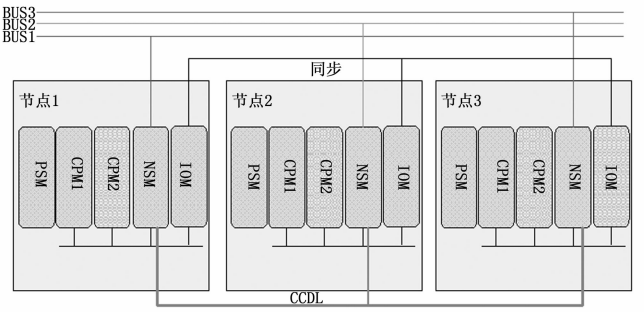

图 1　高可靠容错计算机系统架构

软件结构划分清晰的软件界面，实现更加完整的功能验证。通过分析软硬件变化特征，提出适应新架构的余度管理策略，满足实时性等要求。

3　INTEGRITY 分区操作系统

INTEGRITY 实时操作系统（INTEGRITY RTOS）是由美国绿山软件公司（Green Hills Software，INC.，GHS）所开发的嵌入式实时操作系统。目前已在航空航天等领域有广泛应用。INTEGRITY RTOS 从时域（CPU 时间）和空间域（存储空间）确保了资源可用性。在空间域中，系统按照需求分配给每个分区（在 INTEGRITY 中称为 Kernel Space 或 Address Space）固定的存储区域，各个分区的存储区域使用彼此独立，没有影响。在时域，系统按照需求在一个主帧周期（Major Frame Period，亦即 ARINC653 标准中的主时间帧，Major Time Frame）中分配给每个分区一定的 CPU 时间，各个分区中在自己的 CPU 时间内执行，各分区的任务不能用生成子任务的方式占用其他分区的 CPU 时间。采用分区技术，INTEGIRTY 保证了各个分区（任务）间不受干扰，防止错误蔓延。而系统内核空间拥有自己的内核栈，保证应用分区不会影响系统的安全。同时 INTEGRITY 系统还支持符合 ARINC653 标准的分区调度。

INTEGRITY 还具有内核确定性，在系统调用时并不关中断，从而确保了系统调用的确定性。INTEGRITY 的架构支持多个带保护的虚拟地址空间（Protected Virtual Address Spaces）。每个虚拟地址空间可以包含多个应用任务。INTEGRITY 内核以及内核级任务则保护在内核分区中。

4　高可靠容错计算机软件架构

高可靠容错计算机软件从功能的角度来说分为两层：应用软件层、操作系统层[7]。应用软件层的功能包括飞行控制、推力控制、公共设备管理等子系统功能，以及余度管理、资源管理、BIT 等平台管理功能。操作系统层负责系统的分区调度安全和资源访问安全，多个硬件平台之间的同步操作，健康监控以及模块支持接口驱动。

应用执行接口定义了应用软件层与核心软件层之间的接口。该接口的定义使得核心软件层的更新不会影响应用

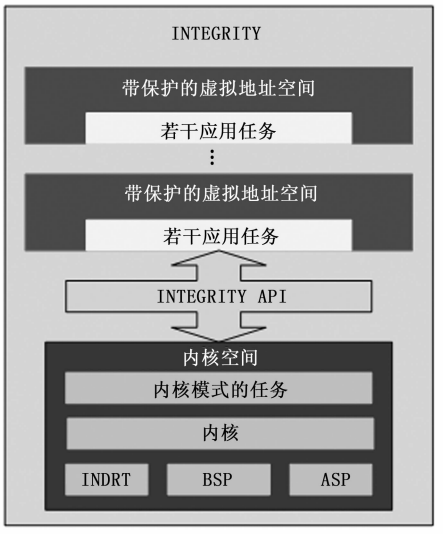

图 2 INTEGRITY RTOS 架构模型

软件层。驻留在硬件平台上的软件包括：

1）应用分区：多个专用的应用软件分区，按照相关的关键级别进行开发和验证。应用分区在鲁棒的空间和时间分区条件下，只能通过系统调用与系统交互。

2）操作系统核心：提供规范定义的 API 和行为，提供应用软件执行的标准和通用的环境，包括调度、通信、同步与异步操作、存储器管理、异常/中断处理接口等服务，包含相关的硬件接口和自测试。

3）系统分区：提供 APEX 之外的接口需求，在鲁棒的空间和时间分区条件下，执行硬件设备通讯管理和容错管理。

4）系统专用功能：主要包括专用硬件接口、下载、调试、自测试。

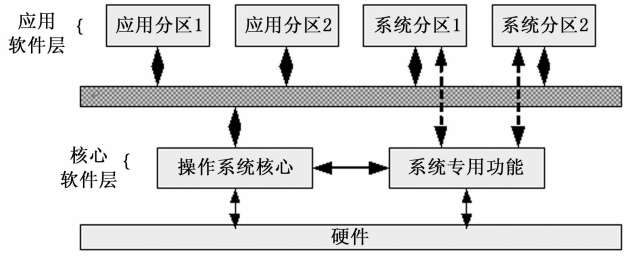

图 3 软件结构

4.1 软件分区结构

计算机包括不同安全级别的控制管理软件，如果内部不分区，其中的所有的软件都要求是适合于那个飞行功能的同一个关键级别[8]。这样将其功能上非关键的软件包含进来，一般来说可能是好的事情，但是影响要求安全级别高的服务，如连续性自测试 BIT，只是通知性的消息给飞行员。处理器内的分区可以允许具体的功能分成关键级别不同的几个软件组成部分，可以把不同关键级别的软件放在同一处理器中。然后每一软件部分可以适合于它自己的关键级别的开发和认证，从而减少整体成本。如果没有分区，由于担心低关键级别的软件成份会影响到高关键级别的软件的功能必须把低关键级别提高到高关键级别上去。分区会消除故障传播的风险而且允许每一个软件成份的关键级别被更局部地评估。高可靠容错计算机操作系统中，使用分区机制对综合后的应用进行保护。分区高可靠容错计算机系统中的一组功能相关的应用，这些应用在配置和执行时作为一个单一的对象来对待。操作系统对每一个分区进行时间和空间上的保护，在空间上，保证一个分区内的应用不会破坏另一个分区内的应用及其私有数据；在时间上，一个分区的执行不会影响到其他的分区。为了实现高可靠容错计算机应用软件组件之间的时间和空间隔离、应用软件组件和共享输入输出处理软件组件以及健康监控软件组件之间的时间和空间隔离、以及操作系统与其它软件组件之间的时间和空间隔离，高可靠容错计算机系统软件从隔离保护的角度分为两层，即独立分区软件层和核心软件层。INTEGRITY RTOS 下的容错计算机系统软件分区静态配置见图 4。

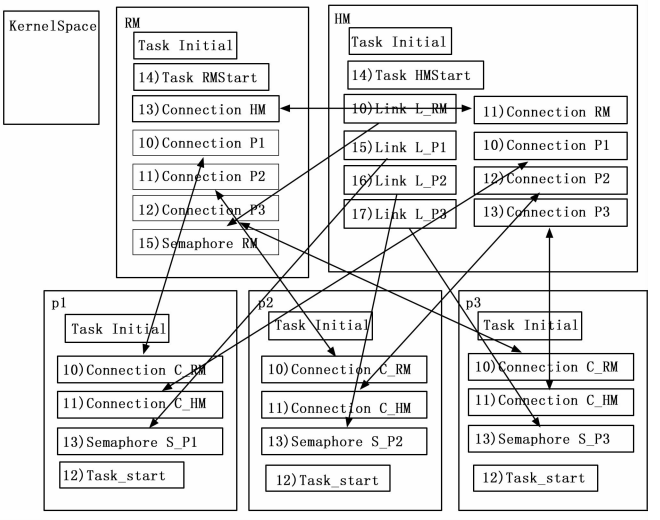

图 4 Integrity 中分区建立图

4.2 余度管理

余度管理是容错计算机的重要和关键功能，能够实现容错计算机的同时刻运行，实现容错计算机的数据信息交互与共享，实现容错计算机的故障实时监测，实现容错计算机的故障切换和故障隔离[9]。因此一个容错计算机系统的容错能力高低，其余度管理算法与策略起到了至关重要的作用。在新的容错架构与高安全的 Integrity 分区操作系统下，余度管理由独立的分区实现，由于他们的设计对整个系统的安全产生影响，其安全级别必须满足系统内最高安全级别任务的要求，余度管理分区是每个主帧周期首先调度的分区，而健康监控分区是每个主帧周期最后调用的分区。

余度管理分区的主要任务包括：同步、输入信息采集、输入信息表决与监控、输出信息表决与监控、输出信息控

制输出及应用分区通讯信息构建。

4.2.1　同步

同步是为了消除不同节点之间的主帧周期的异步度，是模块在同一时间运行相同的帧任务，并保证节点之间数据交互的时间一致性[10]。在没有分区情况的传统同步是软硬件双握手的方式进行同步，同步功能处在周期任务的启示部分，由于增加了分区功能，同步要实现整个所有分区的大主帧周期调度，并且同步由属于余度管理分区，因此赋予最高优先级任务，在同步期间需要停止主帧周期的时间计数，并在同步完成后从零时间开始新一帧的时间周期。即从整个时间轴上看，分区调度情况如图 5 所示。

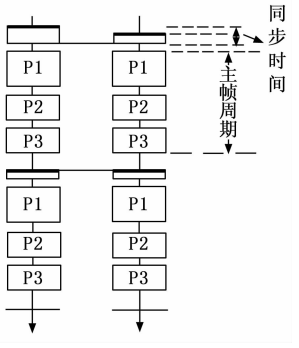

图 5　同步与分区调度

4.2.2　输入输出处理

由于综合化平台后的输入输出任务增加，并且优先级有所不同，为了保证每个任务分区的输出能够尽快执行，将输入输出处理按照主帧周期内分区的安排顺序，分成优先级由高到低的任务，在每个任务分区之间安排余度管理分区的执行，其结构如图 6 所示。

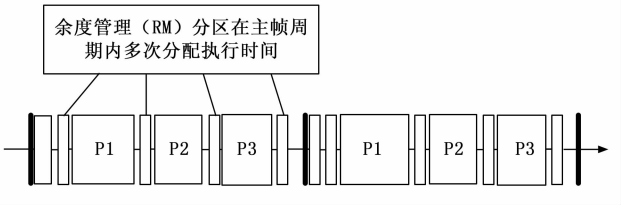

图 6　余度管理分区调度

为了确保每个任务执行前，相关的输入任务已经执行完成，必须规划前一任务的输出执行时间和当前任务的输入处理时间，保证每个任务之间的余度管理时间片大于该时间的和，使下一任务可以获得当前有效的输入数据。

4.2.3　表决监控

高可靠容错计算机的工作方式结合了监控对和通道多数表决的两种方式，这种架构的表决监控可组合为多种方式，本文为简化分区下的表决监控算法，在确保能够有效表决出真实有效数据和监控出故障节点的前提下，将节点机之间的输入/输出信号表决监控分为两组进行，三节点计算机内每一通道的处理机 1 为一组，三节点计算机内每一通道的处理机 2 为另外一组，每一组监控包括通道内监控（处理机 1 和处理机 2）和通道间监控。

假设当前为处理机 1 组，则表决监控原则：

1）三节点计算机处理机 1 表决监控一致、通道内监控表决一致。表决值取中间值，监控值为有效；

2）三节点计算机处理机 1 表决监控一致、通道内监控表决不一致。表决值取中间值，监控值为有效；本通道处理机 2 故障。

3）三节点计算机处理机 1 表决监控不一致（2：1）、通道内监控表决一致。表决值取中间值，监控值为有效；节点故障。

4）三节点计算机处理机 1 表决监控不一致、通道内监控表决不一致。表决值取中间值，监控值为有效；本通道处理机 1 故障。

三节点计算机处理机 2 为主的另一组表决监控原则与处理机 1 的表决监控原则类同。

5　结束语

本文介绍了一种新型的分布式高可靠容错计算机的系统结构及软件结构，结合新的计算机架构带来的软件挑战，给出了该容错计算机平台下的分区工作、同步、周期任务、信息的输入输出以及表决监控等软件解决方案，分析了综合化趋势下的高可靠容错计算机对高安全操作系统的要求，WindRiver、GreenHills 及国内专业院所等商用嵌入式操作系统厂商已开发出了满足 Arinc653 的操作系统。

参考文献：

[1] Green Hills Software，Inc. MULTI Builder［EB/OL］. www.ghs.com，2005.

[2] 牛文生. 机载计算机技术［M］. 北京：航空工业出版社，2013.

[3] AEEC. Avionics Application Software Standard Interface Part1 Required Services［S］. Maryland：SAE－ITC，2015（8）.

[4] 韩　炜. 可信嵌入式软件开发方法与实践［M］. 北京：航空工业出版社，2017.

[5] 解文涛，王　锐. 一种飞行器管理计算机的设计与实现［J］. 计算机测量与控制，2016，24（7）：1671－4598.

[6] 陈丁剑. 多通道余度模型中高可靠表决结构和算法［J］. 测控技术，2013（31）：31－33.

[7] Lenzen C，Locher T，Wattenhof R. Tight bounds for clock synchronization［J］. Journal of the ACM，2010，57（2）：1－42.

[8] 黄　辉，杨金民，张大方. 拜占庭容错服务的适应性失效检测研究［J］. 微电子学与计算机，2006，23（s1）：202－204.

[9] 安金霞，朱纪洪，王国庆，等. 多余度飞控计算机系统分级组合可靠性建模方法［J］. 航空学报，2010，31（2）：301－309.

[10] Anta A，Tabuada P. On the benefits of relaxing the periodicity assumption for networked control systems over can［A］. IEEE RTSS［C］. 2009.