第34卷 增刊 计 算 机 工 程 2008年9月
Vol.34 Supplementary Issue Computer Engineering September 2008
·软件开发与测评· 文章编号：1000—3428(2008)增刊—0043—03 文献标识码：A 中图分类号：TP316

综合化航空电子的系统管理技术

施 刚，钱泰来
(华东计算技术研究所，上海 200233)

摘 要：随着微电子技术、计算机技术及信息技术的迅猛发展，航空电子系统完成的功能也越来越复杂，已经从原来独立功能子系统逐渐向高度综合化的航空电子系统方向发展。该文研究在综合化航空电子平台下，采用层次化、模块化的系统管理技术，通过健康管理、故障管理、安全管理、配置管理，解决在综合化环境下的可靠性、可用性问题。

关键词：综合化航空电子；通用系统管理；运行时蓝图

System Management Techniques of Integrated Modular Avionics

SHI Gang, QIAN Tai-lai
(East China Institute of Computer Technology, Shanghai 200233)

【Abstract】 Driven by the advancements in microelectronics, computer technology, information system, and avionics systems are becoming more complex along with the increasing operational requirements, and highly integrated modular avionics has emerged as an alternative to the traditional federated architecture comprised by individual functional units. This paper discusses the layered and modular design of the system management techniques based on integrated modular avionics, and in the context of health monitoring, fault management, safety management, and system configuration, the solution to meet the reliability and feasibility under the integrated modular avionics is presented.

【Key words】 integrated modular avionic; general system management; runtime blueprint

1 概述

随着微电子技术，计算机技术、信息技术的飞速发展，航空电子系统完成的功能也越来越复杂，航空电子已经从原来的分独立的功能子系统逐渐到高度综合化的航空电子系统方向发展，以进一步提升航空电子系统的作战效能。

为了使得综合化航空电子的特点是采用开放式、层次化的系统结构，标准化的功能接口，以此来保证系统资源的最大化共享和模块间的高效安全互联互通能力。欧洲联合标志航空电子系统结构联合委员会(ASAAC)[1-3]制定了一系列有关开放式航空电子系统软件、通用功能模块、网络通信、封装、软件的标准草案，并准备在新一代飞机项目中使用该标准开发，来降低产品生命周期的成本，提高航空电子系统的作战性能和可操作性[4]。

在该标准中，采用了通用系统管理(包括健康管理、故障管理、安全管理、配置管理4个软件功能模块)，对整个航空电子系统的资源进行统一管理，数据安全透明的交换，数据安全管理，系统加载和卸载，工作的模式切换，故障的检测、隔离和恢复和系统重构。本文参考 ASAAC 标准，结合高可靠嵌入式实时操作系统，给出一种综合化航空电子系统管理的实现方法。

2 综合化航空电子的体系结构

综合化航空电子的软件体系结构自上而下分3个层次：应用层、操作系统层和模块支持层。应用层仅和应用相关，和操作系统及硬件无关；操作系统层和应用及硬件均无关；模块支持层和硬件相关，和操作系统及应用都无关，从而支持各层软件和硬件的独立升级，其体系结构如图1所示。

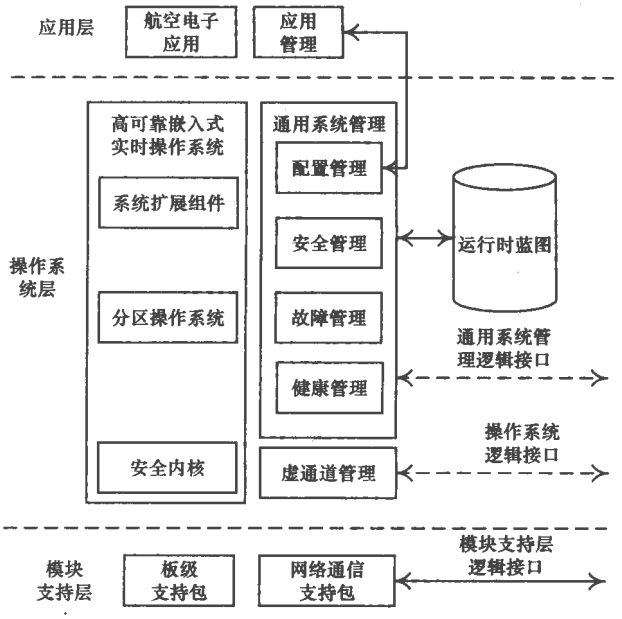

图1 综合化航空电子的体系结构

模块支持层包括板级支持包和通信网络支持包，支持硬件测试和通信网络的配置，实现操作系统与应用软件的远程下载。通过硬件模块支持层，屏蔽硬件的差异，在硬件发生

作者简介：施 刚(1970－)，男，高级工程师，主研方向：嵌入式实时操作系统；钱泰来，工程师

收稿日期：2008-08-28

变更时，仅需修改相应的模块支撑层程序，就可使操作系统安全运行，提高了航空电子应用软件对不同硬件环境的适应能力。

操作系统层包括高可靠嵌入式实时操作系统内核、虚通道管理和通用系统管理。高可靠嵌入式实时操作系统内核分为 2 层：安全关键内核和分区运行环境。安全关键内核基于 MMU 实行保护，提供分区一致时钟管理实现分区轮转调度，从而形成时空域保护。在模块支持层上，采用了基于虚通道的技术，实现逻辑链路到物理链路的映射，封装应用与应用间、应用与操作系统间、处理机模块间以及处理机和外部接口间的数据链路，完成透明的数据交换。虚通道独立于实际传输的介质，来屏蔽数据链路的差异，实行通信协议组件化、模块化。虚通道中的数据由通用系统管理的安全管理进行加密或解密，数据传输是单向性，解决数据传输的安全性。

系统管理负责对整个航空电子系统的资源进行层次化统一管理，实现数据安全透明的交换，数据安全管理，系统加载和卸载，工作的模式切换，故障的检测、隔离和恢复和系统重构。

3 通用系统管理技术

3.1 分层次的系统管理体系结构

系统管理分为 3 个级别：飞机级 (Aircraft)、综合区级(Integration Area)、资源级(Resource Element)。其中飞机级的系统管理负责管理整个航空电子资源管理，综合区级的系统管理一个或多个资源级的资源，将功能接近的应用划成一个组，能根据作战任务动态的创建和删除，综合区级按照树形结构组织，增加了系统的可扩展能力；资源级系统管理是最底层的系统管理，负责单个模块的资源管理。采用层次化的结构，对整个航电系统能够按照子系统进行划分，增加了应用部署的灵活性，增强了故障的定位能力和恢复能力。系统管理结构见图 2。

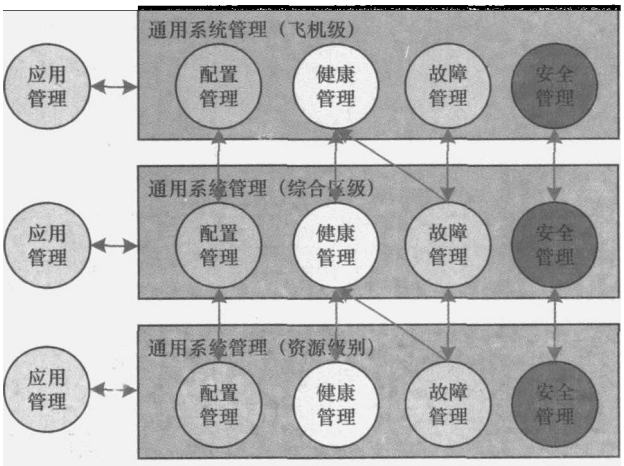

图 2 系统管理的结构

系统管理分 2 个部分：应用管理和通用系统管理。其中，应用管理和飞机的功能相关，运行在应用分区之上。通用系统管理和飞机的功能无关，运行在系统分区上，能执行特权指令。操作系统和通用系统管理模块之间除了标准的 ARNIC 653 接口，还有操作系统和通用系统管理模块之间专用接口，通过专用接口，实现对应用程序、操作系统和硬件的状态监视，实现应用的部署，保障信息安全。

通用系统管理是基础软件平台的核心功能由如下 4 个部分组成：

(1)配置管理：支持系统的引导加载，系统资源(时间、内存、进程、通信链路)的统一分配，系统调度策略和故障恢复策略等的制定，能根据策略完成系统重构。

(2)健康性管理：监控系统软硬件状态和系统的状态、过滤故障，并向故障管理报告。

(3)故障管理：通过详细检测，并对故障过滤和汇总，根据故障类型通过配置管理实现基于蓝图/策略的故障恢复处理功能。

(4)安全管理：认证和加密之密钥的管理和发布，制定安全级别和清除数据，完成认证和加密算法，并实现安全审计。

通用系统管理之间，应用管理和通用系统管理之间通过逻辑接口进行调用，逻辑接口通信建立在虚通道的基础之上。

3.2 健康管理

健康管理监视从资源级、综合区级到飞机级的健康状态，主要的职责是搜集硬件、操作系统、应用引起故障与错误，通过蓝图定义的策略进行故障与错误过滤，将上报到同一级别的故障管理和上一级别的健康管理，提供全系统运行状态视图。在应用层，硬件层，操作系统层插入健康监视器，监视器向操作系统层的监控服务，由监控服务统一处理。监视器工作的模式可以是主动也可以是被动，例如应用除零发生错误时，触发 CPU 异常，CPU 向监视器报告，这时监视器的工作模式是被动的；当信息传输时，监视器验证数据的完整性，这时监视器工作在主动工作模式。通过 2 种不同的错误检测机制，有效收集健康信息。监控器收集到错误信息时传递到故障过滤器，故障过滤器过滤掉瞬时性的故障，再将并对已确认的永久性故障或间歇性故障报告给同一层次的故障管理，由故障管理做进一步处理。通过运行时蓝图定义过滤策略，过滤策略工作模式采用是有限状态机的方式工作模式，当故障达到定义的阀值时，触发错误报告。各层次通用系统管理通过心跳对系统管理进行健康检测，由上一层的健康管理发出询问，下层的健康管理进行应答，形成层次化的健康信息视图。

3.3 故障管理

故障管理收到健康管理错误报告后，对故障进行识别，定位故障，并对相关性分析，并通过配置管理隔离、恢复故障，同时对故障记录日志。故障主要是通过健康管理提供的错误码，并根据错码码调用高测试覆盖率的检测获取更多的信息来识别，检测的内容包括网络连接的状况检测和资源模块的高测试覆盖率 IBIT 检测。故障管理收集到详细信息报告后，根据蓝图的策略对错误报告进行分析，定位故障。由于单点故障会引发多个故障，当发生故障时，故障管理分析是否是由单点故障引起多个故障，并分析故障之间的关系。对于出现的故障，故障管理进行记录日志，供事后分析。当本层的故障管理无法处理时，向上一层的健康性管理报告错误。故障处理的规则包括忽略、通过配置管理进行重构或由应用本身通过应用管理恢复。采用运行时蓝图，能灵活配置故障管理处理的策略和行为。

3.4 安全管理

安全管理自上而下从飞机级、综合区级、资源级分层管理，确保经过加密、解密和审计的受保护数据能够安全传输，将检测破坏安全的事件写入安全日志。安全管理负责生成、分配、使用、存储、备份、恢复、查询、更新和和销毁密钥。信息加密可采用硬件加密或软件加密算法实现，加密模块可注入。当线程传输高安全的信息时，信息通过安全管理进行

加密；接收方收到信息后通过安全管理进行解密。在大容量存储模块中对安全级别高的数据进行加密，数据访问采用访问控制表控制。当系统进行重构时，安全管理负责对释放的内存进行擦除，对于高安全的数据时，先认证授权再擦除，避免误操作。安全模块的策略也是通过运行时蓝图配置。

3.5 配置管理和系统重构

配置管理负责着整个分布式系统管理工作，在系统加电后，根据蓝图初始配置信息，完成硬件设备上电，分区系统初始化，操作系统的加载，应用的加载，连接虚通道并构建系统。配置管理是一个有限状态机，由应用管理或故障管理事件触发，进行相应的操作。系统配置和重构有以下几种情况下发生：在系统初始化或下电时，触发系统状态的改变；当故障管理发现故障，通知应用管理，应用管理和配置管理协同工作，对系统进行重构进行恢复；由飞行员触发的任务状态的改变，通过应用管理进行重构。配置管理通过可替换模块进行管理，模块化的硬件体系结构见图 3。

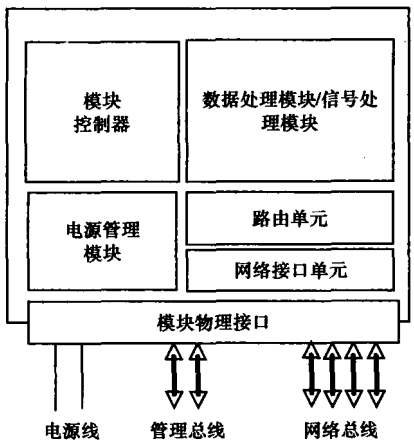

图 3 模块化的硬件体系结构

其中，电源管理模块控制模块的上下电，路由模块接收路由信息，跨模块的传输通过网络接口单元进行传输，模块内通过路由单元进行路由，路由表由运行时蓝图动态配置，模块控制单元运行模块的系统管理，运行模块级的系统管理。应用的处理功能安装处理模块上，安装大数据运算或流程控制分别采用 DSP 或 CPU。采用模块化的硬件体系结构，层次化的系统管理，能够做到模块级互换，最大程度实现了资源共享。系统的初始化过程系统启动步骤如下：

(1)初始化过程是电源管理模块首先上电，打开缺省的虚通道，等待模块支持层的消息；

(2)网络模块上电，建立缺省的网络配置；

(3)大容量存储模块上电，自动加载存储模块的操作系统和存储模块的蓝图，启动飞机级的通用系统管理和应用管理，完成该模块的模块级通用系统管理引导；

(4)大容量存储模块的资源级通用系统管理启动分布式文件系统服务，应用代码和系统蓝图可访问；

(5)飞机级的通用系统管理，通过缺省的网络配置向网络模块下发网络的路由信息，并通过健康管理接口检测上电网络工作状态，建立网络连接关系；

(6)飞机级的系统管理模块根据蓝图对综合区级管理模块上电，启动操作系统，通过分布式文件系统加载综合区级的蓝图，完成综合区级的系统管理初始化；

(7)综合区系统管理对根据蓝图配置对资源级的模块上电，并根据综合区级的蓝图进行上电检测，建立综合区系统网络连接；

(8)资源级下载操作系统和蓝图，启动资源级的系统管理；

(9)综合区系统管理和资源级系统管理根据蓝图的策略在资源级加载配置和应用代码，启动配置，建立虚通道，启动工作线程。

在启动过程中，按最小化上电的原则对需要的模块上电。在综合区内有 3 种备份模块：热备份，待机备份和冷备份。其中，热备份模块上电并加载应用对关键的应用重构时间短；待机备份模块上电仅加载操作系统不加载应用，重构时加载应用，重构时间较长，但使用灵活；冷备份启动时不上电，根据策略由系统管理打开，减少电源开销和电磁辐射。系统集成人员能根据故障类型及系统状态、应用的重要性及所采取的策略，系统工作模态或故障引起的恢复时间依据任务的重要性(分为安全关键、生存关键和任务关键)分别有不同的时间要求，分级别进行蓝图配置，在系统部署过程中，系统管理分析飞机级、综合区级、资源级的蓝图完整性(包括软件代码、依赖关系及虚通道的完整性、硬件资源的可保证性)，然后再进行加载，保证应用的完整性和可用性。重构时采用静态重构策略，由定义好的蓝图指定重构的步骤和动作，保障重构时间的确定性。

4 结束语

随着航空电子综合化、模块化方向发展，研究可替换模块的硬件体系结构，通过分层次的系统管理，达到最大程度资源，从而提高整个航空系统的可靠性和安全性。本文参考欧洲航空标准，嵌入式实时软件基础平台，设计综合化航空电子的系统管理实现技术，其中部分工作已在相关项目中得到了应用和验证。

参考文献

[1] ASAAC, STANAG 4626[Z]. Modular and Open Avionics Architectures Part I, 2008.

[2] STANAG 4626[Z]. ASAAC, Modular and Open Avionics Architectures Part II, 2008.

[3] STANAG 4626[Z]. ASAAC, Guielines of System Issues Part VI, 2008.

[4] 中国人民解放军总装备部. GJB5357-2005 航空电子应用软件接口要求[S]. 2005.