

飞行管理系统 AADL 建模与分析

汤小明¹, 苏罗辉², 宋科璞²

(1. 西北工业大学 自动化学院, 陕西 西安 710075;

2. 飞行自动控制研究所, 陕西 西安 710065)

摘 要:航空电子系统软件的建模与分析是保证军用和民用飞机高可靠、高性能的重要手段,也是模型驱动软件体系结构的重要组成部分。飞行管理系统作为航空电子系统的重要组成部分,传统上,对该系统的可调度性分析是在系统设计完成后,在实现与验证阶段进行的,这使得系统无法进行的准确地软硬件需求分析。采用先进的建模方法 AADL 对其进行建模,为飞行管理系统的可调度性分析、可靠性分析以及通信延迟等分析提供了可能,使得在系统需求分析阶段就可以准确确定系统的软硬件需求,并能大大降低系统的更改验证成本。首先论述了建模语言 AADL 的基本构成以及与航空电子应用接口规范 ARINC653 的对应关系;然后描述了飞行管理系统的功能构成,并建立了飞行管理系统的 AADL 模型;最后详细论述了系统调度理论, AADL 工具, 飞管系统 AADL 模型的仿真分析。通过仿真分析为飞管系统的处理器选型、系统设计、软件设计与优化提供了依据。

关键词:航空电子系统;模型驱动 AADL;飞行管理系统;实时调度分析

中图分类号: TP311

文献标识码: A

文章编号: 1673-629X(2010)03-0191-04

Modeling and Analysis of Flight Management System with AADL

TANG Xiao-ming¹, SU Luo-hui², SONG Ke-pu²

(1. College of Automation, Northwest Polytechnical University, Xi'an 710075, China;

2. Flight Automation Control Research Institution, Xi'an 710065, China)

Abstract: Avionics software model and analysis are the important approaches to enhance the reliability and performance for military and civil aeroplane, and the important components for model driven software architecture. The flight management system, as the subsystem of avionics system, traditionally, is analysed for schedulability in implementation or verification process, which makes the requirement of software and hardware is very hard to be determined. The advanced modeling method AADL is applied to the flight management system, which is to be likely to analyse the schedulability, reliability and end-to-end flow latency, and dramatically decrease the cost for validation and verification because of modification. Describe the basic components of AADL specification and the mapping between ARINC653 and AADL at first. Meanwhile the architecture and the AADL model of flight management system are also proposed. And then the schedulability theory and analysis are discussed. In the end, the simulation and analysis of flight management system model with AADL are studied, and the AADL tools are researched for such purpose, which provides the guide for selection of CPU parameter, design of system, and development and optimization of software.

Key words: avionics system; model drive AADL; flight management system; real time scheduling analysis

0 引言

体系结构分析与建模语言 AADL (Architecture Analysis and Design Language) 是一种用来对性能关键实时嵌入式系统软硬件体系结构进行设计与分析的本体和图形语言^[1], 其不仅能够描述系统功能特性, 也能描述非功能特性, 甚至系统的动态特性。适合具有对

时间、吞吐量、可靠性、安全以及保密等约束的嵌入式系统使用, 应用场合包括航空、航天、汽车以及自主系统等领域^[2]。

AADL 能够提供处理器、存储器、总线以及设备等硬件平台建模, 进程、线程、子程序、参数、数据以及调用序列、模式转换等的软件平台建模, 以及软硬件综合建模与分析, 如系统可调度性分析、端到端延迟分析、功耗分析、总线负载分析、资源分配分析以及优先级反转分析等等。此外, AADL 还支持对 ARINC 653 分区、错误模型、冗余度体系等的建模, 这些面向领域的功能扩展非常适合航空电子系统的建模。AADL 的

收稿日期: 2009-02-17; 修回日期: 2009-09-19

基金项目: 航空基金资助项目 (20060718001)

作者简介: 汤小明 (1979-), 男, 博士研究生, CCF 高级会员, 研究方向为嵌入式软件体系结构、实时操作系统以及分布式计算。

以上优越特征使得我们选用其对飞行管理系统进行了建模,并基于模型对系统进行了分析。

AADL 模型采用自主研制的高可靠实时操作系统 FCOS 作为其基础运行环境,该操作系统是一款比较成熟的专用操作系统,目前已经成功应用于我们研制的无人飞机、导弹系统中。FCOS 支持 ARINC653 规范^[3],采用时间空间分区技术实现不同分区间的应用在时间和空间上的完全独立,提供不同级别、不同阶段的故障隔离与屏蔽能力,并支持 FCOS 操作系统提供商、各应用分区开发商以及系统集成商之间相互独立开发的能力。根据 AADL 规范,进程(Process)组件不参与系统调度,仅提供对其包含线程的空间保护,在 FCOS 中对应分区(Partition),分区内的任务对应 AADL 的线程,线程是系统调度的基本单位,每个进程至少需要包含一个线程。AADL 提供基于 RMA 的可调度性分析^[4],RMA 也是 FCOS 采用的基本调度算法。此外,FCOS 规定分区间通信采用端口(Port),其中采样端口对应 AADL 的数据端口(Data port),队列端口对应 AADL 的事件数据端口(Event data port),端口采用单向通信方式,AADL 建模时也需要考虑到这种约束,如果进程或分区间需要双工通信方式,则需要建立两条通信通道。FCOS 中的通道(Channel)对应 AADL 的连接(Connection)。

1 飞行管理系统 AADL 建模

飞行管理系统(Flight Management System)是飞机重要的子系统,能够协助飞行员完成从起飞到着陆的各项任务,管理、监视和自动操纵飞机实现全航程的自动飞行。FMS 集导航、制导、控制及座舱显示于一体,其主要功能可分为飞行规划、导航、性能优化、制导及信息显示^[5,6]。其主要功能包括:

(1) 飞行规划。

飞行规划负责规划整个航路,指定从起飞机场到目的地机场之间的飞行航线、航路点、起飞程序、降落程序等,以及备选的降落点。飞行规划也包括对风和温度的预测数据,及一些飞行限制值,如某飞行高度上的速度限制、某个航路点的速度限制和高度限制等。

(2) 性能优化。

计算飞机的飞行剖面 and 高度、速度限制值,以最小化飞行成本。计算参数包括最大高度、优化高度、最大速度、最小速度、经济速度、长距离巡航速度、最大爬升角等。

(3) 综合导航与制导。

计算俯仰、滚转和速度、推力指令。这些指令输入飞行指引、自动飞行控制系统和自动油门系统,用来控

制飞机的水平航向、垂直航向或以指定的速度捕获/跟踪飞行路径。同时生成仪表上显示的数据。

(4) 控制显示。

控制显示单元 CDU 是飞行管理系统进行人机交互的重要组成部分,是访问和控制飞行管理计算机中信息的主要的飞行员接口。一般采用页式管理,包括初始化和参考页面、航路页面、离场和进场页面、导航无线电页面等等。

飞行管理系统的实现还需要两个数据库:性能数据库和导航数据库。性能数据库是飞机的气动模型和发动机性能模型,利用这些信息可保证飞机沿最优垂直剖面飞行。导航数据库内的数据是飞机飞行区域的机场、航路点、导航台的地理位置、结构以及航路组成结构等,根据这些信息进行导航计算及导航台自动调谐^[7]。

AADL 中线程分为周期任务(Period Task)、非周期任务(Aperiod Task)、偶发任务(Sporadic Task)以及后台任务(Background Task)等四类任务。周期任务是指任务按照一定的之间间隔(即周期)触发运行的任务;非周期任务是指任务由事件随机触发的任务,非周期任务对事件的触发间隔没有约束;偶发任务是指具有最小分发间隔约束事件驱动的任务,偶发任务对事件最大触发频率有约束的任务,当大于该频率而触发的任务,系统将不予处理。

系统建模中主要使用周期任务,周期任务集 TS 的数学模型由四元组 (s_i, e_i, d_i, p_i) 表示,其中 s_i 为初始请求时间, e_i 为任务执行时间, d_i 为相对死线, p_i 为任务周期。一个由 n 个实时周期任务组成的系统表示为 $TS = (\{T_i\}, \{s_i\}, \{e_i\}, \{d_i\}, \{p_i\})$ 。文中论述的 FMS 系统各任务 $s_i = 0, p_i = d_i$ 。因此任务模型将简化为 $TS = (\{T_i\}, \{e_i\}, \{p_i\})$ 。

基于以上论述的飞行管理系统功能划分,飞行管理系统有 6 个处理线程组成,如图 1 所示。分别是导航传感器处理线程 Navigation Sensor Processing、综合导航线程 Integrated Navigation、制导线程 Guidance Processing、飞行规划线程 Flight Plan Processing、飞机性能优化线程 Aircraft Performance Calculation、控制显示线程 Handle Page Request。任务模型为 $T_{NSP} = (15, 50), T_{INav} = (40, 100), T_{GP} = (30, 50), T_{FPP} = (30, 200), T_{APC} = (100, 500), T_{HPR} = (1, 50)$, 单位为 ms, 各任务之间采用共享数据进行通信,如图 1 所示。任务之间通信采用共享数据区,为了避免共享数据区的生产者-消费者问题,任务和任务之间的通信区采用单工方式,如果需要进行双工通信,则需要建立两个单工共享数据区。

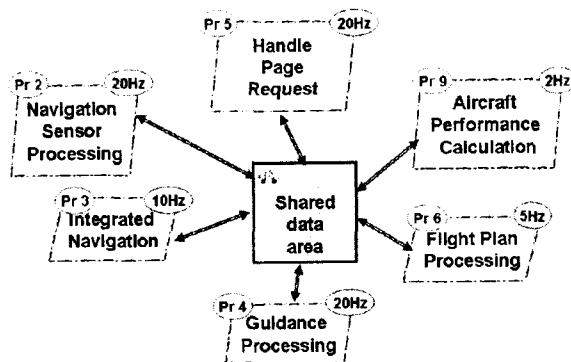


图1 飞行管理系统任务划分

该飞行管理系统6个线程的AADL建模如图2所示。

<pre> thread NavigationSensorProcessing properties Dispatch - Protocol = >Periodic; Period = >50 Ms; Compute - Execution - Time = > 5 Ms .. 15 Ms; end NavigationSensorProcessing; thread IntegratedNavigation properties Dispatch - Protocol = >Periodic; Period = >100 Ms; Compute - Execution - Time = > 10 Ms .. 40 Ms; end IntegratedNavigation thread GuidanceProcessing properties Dispatch - Protocol = >Periodic; Period = >50 Ms; Compute - Execution - Time = > 8 Ms .. 30 Ms; end GuidanceProcessing; </pre>	<pre> thread FlightPlanProcessing properties Dispatch - Protocol = >Periodic; Period = >200 Ms; Compute - Execution - Time = > 10 Ms .. 30 Ms; end FlightPlanProcessing; thread AircraftPerformanceCalculation properties Dispatch - Protocol = >Periodic; Period = >500 Ms; Compute - Execution - Time = > 1 Ms .. 100 Ms; end AircraftPerformanceCalculation; thread HandlePageRequest properties Dispatch - Protocol = >Periodic; Compute - Execution - Time = > 1 Ms .. 1 Ms; Period = >50 Ms; end HandlePageRequest; 以上线程的运行处理器平台的 AADL建模如下: processor implementation PowerPC. Mhz500 properties SEI: : cycle - time = >700 ps; end PowerPC. Mhz500 </pre>
---	---

图2 飞行管理系统 AADL 建模

2 模型可调度性分析

对于安全关键的航空电子领域,为了支持系统的实时性和确定性,需要在系统设计阶段对实时系统进行可调度分析,并结合实际运行平台进行验证。由于本飞行管理系统中任务主要为周期任务,本部分主要论述周期任务集 TS 的可调度性分析理论和基于以上建立 AADL 模型的实践。

对于周期任务集 TS,如果每个任务的每个死线在一个调度 S 下都能得到满足,则称调度 S 对于这个实时系统 TS 为有效调度。对于一个 TS,如果存在一个有效调度,则称该 TS 为可行的。如果一个调度算法能

够产生一个有效调度,则称该 TS 在该调度算法下是可调度的。如果在一个调度算法下,每一个可行系统都可调度,则称该调度算法最优。

目前,主要有三种比较成熟的调度算法可用于实时系统的调度:(1)时钟驱动(Clock - Driven);(2)处理器共享(Processor - Sharing);(3)优先级驱动(Priority - Driven)。其中优先级驱动调度算法的应用远远超过其它两种调度算法,该算法分为两种:动态优先级(Dynamic - Priority)和固定优先级(Fixed - Priority)。虽然动态优先级调度比固定优先级调度更有效,但是由于间接开销(overhead)而在实际应用中很少使用。

对于动态优先级调度算法,最有名的要数最早死线优先算法(Earliest - Deadline First EDF),该算法将死线最接近当前时间的任务设置为最高优先级。对于单处理器系统,EDF 算法是最优算法。但对于双或多处理器,EDF 并不是最优算法,另外,对于这样的系统目前还没有最优算法。

对于固定优先级调度算法,最有名的要数速率单调(Rate - Monotonic RM)和死线单调(Deadline - Monotonic DM)算法。RM 算法将最小周期的任务赋予最高优先级,DM 算法将最小相对死线的任务赋予最高优先级。当 TS 系统中所有任务的周期等于相对死线时,DM 和 RM 等价。对于单处理系统,DM 算法为最优算法。当某些任务的死线不等于周期时,RM 算法不是最优算法。

定理1:如果实时任务系统 TS 由 n 个任务组成,每个任务的相对死线等于周期,该 TS 由 DM 或 RM 可调度,如果

$$U_{\text{sum}}(T) = \sum_{i=1}^n \frac{e_i}{p_i} \leq n(2^{1/n} - 1)$$

$$\lim_{n \rightarrow \infty} \sum_{i=1}^n \frac{e_i}{p_i} \leq n(2^{1/n} - 1) \approx \ln 2 = 0.69$$

飞行管理系统的任务为6时,由定理1可知,系统可调度利用率为73.4%。

目前已经有许多工具支持 AADL 架构设计和分析,STOOD 是最早支持 AADL 的软件工具,ASSERT 项目也支持 AADL,该项目主要研究基于证明的系统工程(PBSE),AdeS 工具主要用来对 AADL 描述的体系结构行为进行仿真。文中论述的飞管系统 AADL 模型采用开源 AADL 工具环境(OSATE)进行设计与分析验证。该环境是在开源 Eclipse 平台之上的一套插件,它提供了一个集成的开发环境用于 AADL 模型编辑、编译和前端分析,具体功能有:

- 1) 语法敏感的文本编辑器。
- 2) 基于开源 ANTLR 的语法词法解析器,以及与

文本编辑器集成的错误报告机制。

3) AADL XML 浏览和编辑环境。

4) 语法敏感的 AADL 模型结构对象编辑器,以及 AADL 属性浏览器。

5) AADL XML 向文本 AADL 转换器。

6) AADL 向 MetaH 转换器。

7) 基于 Eclipse GEF 的图形 AADL 编辑器。

另外,OSATE 已经开发成功多个分析插件用于执行各种架构的一致性检查、可靠性分析、数据质量和安全分析以及资源调度等。

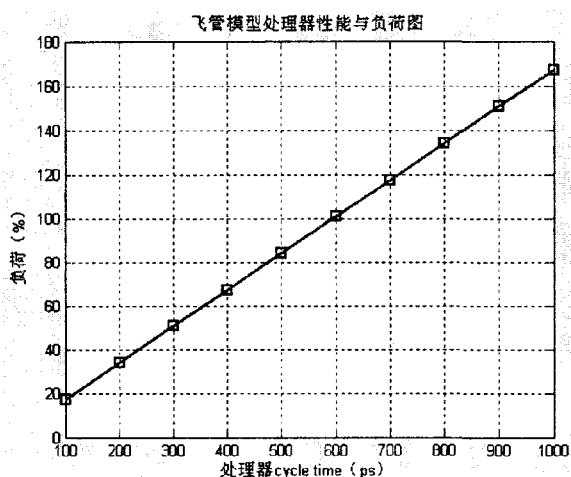


图 3 处理器性能与负荷图

图 3 显示了飞管 AADL 模型在速率单调调度算法条件下,处理器性能与系统利用率之间的关系图,由图可以看出处理器性能与负荷之间为线性关系。根据该仿真结果,结合系统可调度性理论^[8],可以得出该飞行管理系统必须在处理器 cycle_time < 450ps 的条件下,才能满足 6 任务可调度性要求,即利用率小于 73.4%。在有些安全关键的实时系统实现中,为了保证系统的可靠性和容错性,还需要保证一定的系统余量。以上基于飞管系统 AADL 模型的仿真分析为处理器选型、系统设计、软件设计与优化提供了依据,同

时可以在系统、软硬件实现成本之间达到最优。

3 结束语

文中主要论述了飞行管理系统 AADL 建模,系统单处理器、多处理器调度理论以及 AADL 模型的仿真分析。目前 AADL 还不支持对 ARINC653 规范中健康监控的建模,进一步将结合 FCOS 操作系统和飞行管理系统对健康监控的 AADL 建模进行研究。此外,根据实际应用,基于 AADL 模型的分级调度、空闲挪用调度等算法还需要进一步评估与分析,针对一些复杂的任务管理系统,多处理器系统的分析与建模所涉及的任务分派、迁移以及均衡等等问题也需要展开进一步的研究。

参考文献:

- [1] SAE International. Architecture Analysis and Design Language(AADL)[M]. [s.l.]:[s.n.],2004.
- [2] Dissaux P. Using the AADL for mission critical software development[C]//2nd European Congress ERTS, Embedded real time software. Toulouse:[s.n.],2004.
- [3] Airlines electronic engineering committee. ARINC specification 653-2[M]. [s.l.]:Aeronautical radio,inc.,2005.
- [4] Sokolsky O, Lee I. Schedulability Analysis of AADL Models [M]. [s.l.]:IEEE,2006.
- [5] Liden S. The Evolution of Flight Management Systems[C]// Digital Avionics Systems Conference. Phoenix, AZ:[s.n.], 1994:157-169.
- [6] SAE International. Flight Management Systems Review[M]. [s.l.]:[s.n.],2007.
- [7] 王江云, 杨晓阳. 民航飞行管理系统建模与仿真实现[J]. 飞行力学,2008,26(2):56-59.
- [8] Singhoff F, Legrand J. Scheduling and Memory requirements analysis with AADL[C]// International ACM SIGADA Conference. Atlanta, USA:[s.n.],2005.

(上接第 190 页)

- [J]. JM-RI,1997,7(2):447-450.
- [4] Orkisz M M. Improved vessel visualization in MR angiography by nonlinear anisotropic filtering[J]. MRM,1997,37(6): 914-918.
- [5] Frangi A F, Niessen W J, Vincken K L, et al. Multiscale vessel enhancement filtering[J]. Lecture Notes in Computer Science, 1998,1496:130-137.
- [6] Eiho S, Qian Y. Detection of coronary artery tree using morphological operator[J]. Computers in Cardiology, 1997, 24: 525-528.
- [7] Haris K, Efstratiadis S N. Model-based morphological seg-

mentation and labeling of coronary angiograms[J]. IEEE Trans Med Imag,1999,18(10):1003-1014.

- [8] Chaudhuri S, Chatterjee S, Katz N, et al. Detection of blood vessels in retinal images using two-dimensional matched filters[J]. IEEE Trans Med Imag,1989,8(3):263-269.
- [9] 李颖超, 刘越, 王涌天. 基于多尺度 Hessian 矩阵和 Gabor 滤波的造影图像冠脉中心线提取[J]. 中国医学影像技术, 2007,23(1):133-136.
- [10] 徐智, 郁道银, 谢洪波, 等. 心血管造影图像中的心血管提取[J]. 中国生物医学工程学报,2003,22(1):6-11.