Computer Science and Application 计算机科学与应用, 2016, 6(4), 242-247
Published Online April 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.64030

Hans汉斯

Research on Technology of Real-Time and Dependable Component

Cheng Peng[1], Le Wei[2]

[1]Computing Center Department, Chengdu University of Information Technology, Chengdu Sichuan
[2]Computer Science Department, Chengdu University of Information Technology, Chengdu Sichuan
Email: pengcheng@cuit.edu.cn

Received: Apr. 9th, 2016; accepted: Apr. 26th, 2016; published: Apr. 29th, 2016

Abstract

This paper introduces the recognitions and research actions of academe currently on real-time components and components' ultra dependability safeguard technology, investigates the connotation about real-time characters of real-time components and components' dependability, analyzes the essence and merged rules of real-time and Dependable properties, discusses the problems needed to solve for real-time and dependable components, and prepares for following researches.

Keywords

Real Time, Dependability, Component, Reuse, Security, Risk Prevention, Reliability

实时可信的构件技术研究

彭　城[1]，魏　乐[2]

[1]成都信息工程大学计算中心，四川 成都
[2]成都信息工程大学计算机学院，四川 成都
Email: pengcheng@cuit.edu.cn

收稿日期：2016年4月9日；录用日期：2016年4月26日；发布日期：2016年4月29日

文章引用: 彭城, 魏乐. 实时可信的构件技术研究[J]. 计算机科学与应用, 2016, 6(4): 242-247.
http://dx.doi.org/10.12677/csa.2016.64030

摘　要

本文介绍了当前学术界在实时构件和构件高可信保障技术方面的认知和作为，研究了实时构件的实时特征和构件可信性的内涵，分析了实时可信构件的实时性和可信性的本质，以及两者融合的必然性，对实时可信构件所需解决的问题进行了探讨，为下一步将要开展的构件模型及其设计工作奠定基础。

关键词

实时，可信，构件，重用性，安全性，防危性，可靠性

1. 引言

计算机的应用模式在经历了主机模式和个人机模式后，目前正向普适计算[1] (Pervasive Computing)模式发展。在普适计算模式下，嵌入式实时系统将会渗透到人们生活的各个方面，而嵌入式实时软件的质量和开发效率往往会对一个嵌入式产品的成功起着决定性的影响。传统的嵌入式实时系统大多采用低级的程序设计语言编写，并在专用的硬件和操作系统之上运行，运行效率、资源利用率以及与硬件的集成是考虑的主要方面，模块化和复用性是在第二位的。但随着开发要求的提高(时间、成本)，实时系统的构件化越来越受到重视，对于嵌入式实时系统利用构件化技术来提高嵌入式软件质量和开发效率就成了实时软件工程研究的重要内容。

现在，嵌入式实时系统在航空航天、国防、交通运输和核电能源等诸多安全关键领域中得到了广泛的应用，这类系统可称之安全关键系统 SCS (Safety Critical Systems) [2]，要求其具有“动则成功”的能力，另外，随着不稳定因素的增加，这类系统的安全性也被提上日程。但随着安全关键系统日益庞大和复杂，带来了系统可靠性和安全性下降、投资增加、研发周期加长、风险增加等一系列问题。利用构件化技术来开发嵌入式实时系统，使系统的高重用性得到了保障，同时考虑到将实时性、可靠性、防危性和安全性封装在构件当中，将会使 SCS 具有投资小、周期短、研发一次成功、系统安全可靠的特性。也就是说，对实时可信的构件技术进行研究具有重要的现实意义，并将成为今后构件技术发展的一个趋势。

2. 研究历史和现状

2.1. 实时构件技术的研究

对于实时构件的研究曾经存在这样误解：认为构件不适用于实时应用，且常常受到中间层降低性能或不够快的批评。这一误解的根源在于未能区分“实时”和“快”的差别[3]。为了支持实时应用，构件应该作以下的扩展：增加实时调度策略和机制；增加实时事件支持以提供对实时事件驱动的支持；增加实时服务质量(QoS)的支持，支持实时 Qos 的表达和执行；增加实时应用编程支持；进行必要的裁剪，以适用于嵌入式系统；进行性能优化。

对实时构件关注较早的是 OMG 组织，该组织于 1996 年 12 月发布了实时 CORBA 白皮书[4]，阐明了 OMG 组织所考虑的实时 CORBA 技术的基本范畴和 OMG 组织的有关实时系统的概念。此后，OMG 组织于 1997 年 9 月提出了实时 CORBA 1.0 的 RFP [5]，得到了来自 Alcatel，Hewlett，OOC，Sun 等成员独立或者联合提交的实时 CORBA 规范草案。最终，于 1999 年 3 月，OMG 组织经过讨论修改，发布了实时 CORBA 1.0 规范[6] (2001 年 9 月推出了 2.0 版)。它在 CORBA 基础上定义了一组标准的接口以及策略供用户来控制和配置系统的处理器资源、内存资源和通信资源，这些标准控制机制包括线程池、CORBA

优先级、互斥机制和全局调度服务等；内存资源的标准控制机制主要有请求队列等；而通信资源的标准控制机制则有协议特性设置和显式绑定等，从而满足实时性。

对实时构件的研究不但要考虑到实时构件模型的建立，还要研究实时软件的构件化开发方法学和开发环境。这方面的工作主要集中在构件组装、代码(或代码框架)的自动生成和对生成的软件系统的非功能属性的分析验证等方面。比较典型的研究工作包括：C.V illela 等通过扩展已有的工具环境 SIMOO-RT 来支持实时软件的构件化开发的整个过程[7]；Ulrich Hannemann 等利用形式化证明工具 PVS 提出了一种自顶向下的形式化的构件设计方法来保证实时软件的构件化设计的正确性[8]；Stephen S.等提出了一种可定制的实时构件的框架和定制方法及相关支持工具[9]等。

2.2. 可信性研究

当计算机发展到一个比较成熟的阶段，可信需求显得迫切而关键，而对可信性的研究归根结底就是对可信计算的研究。可信计算是新近发展的一门学科，着力于解决计算世界当前所面临的普遍的安全威胁和不可信危机，它是一个广泛的概念，是对若干传统计算技术的综合。Babbage 于 1830’S 年在他的论文“计算机器”中首次提到了可信计算(dependable computing)的概念，1999 年 IEEE 太平洋沿岸容错系统会议改名为“可信计算会议”，标志着可信计算成为学术界新的研究热点。

目前，对可信计算的研究主要处于摸索阶段，国内外许多研究机构都从不同的角度，对可信进行了阐述。美国国家科学基金会认为，一个可信的信息系统所应考虑的方面包括[10]：security，privacy，safety，reliability；德国达姆施塔特大学的计算机科学和工程系的数据库和分布式系统组认为，可信性是比任何其它特征都具综合性的一个性质，它是涵盖[11]：end to end security，availability，reliability，timeliness，consistency，predictability，scalability 所有特性的特性；微软在 2002 年 12 月一份白皮书中，将可信计算的四个目的总结为：security，privacy，reliability，business integrity；国内武汉大学张焕国等人认为：所谓可信是指计算机系统所提供的服务是可靠的、可用的、信息和行为上是安全的。相对应的可信计算平台是能够提供可信计算服务的计算机软硬件实体，它能够提供系统的可靠性、可用性、信息和行为的安全性[12]。

2.3. 实时与可信的融合

早些时候，构件技术在分布式系统中用得较为广泛，在这些应用中并不关心其实时性能，而更注重可信性。为了确保可信性，人们习惯地借助于已充分地研究和成功地使用过的容错技术。OMG 在 2001 年 9 月推出了 FT CORBA 规范，这规范的出现也推动了容错 CORBA 中间件产品的开发和上市。其中著名的成果有：DOORS，Eternal 和 Electra 等。

实时和容错分别被有着不同关注重点的用户所使用，实时 CORBA 规范和容错 CORBA 规范也只关心了本领域的具体事宜，两者独立地解决本领域的相关问题，也得到了相关的认同。但在 20 世纪 90 年代后期，出现了 mission—critical 的应用的新需求 ，这类需求同时含有实时要求和可信性要求，也就是需要实时与可信性的相互融合[13]。国外目前少数单位的研究中较有名的有 CarnegieMelon 大学和华盛顿大学的研究小组，国内如电子科大等一些高校也正在从事这方面的研究。可以看出实时与可信的融合是一个新的研究课题，迄今还没有大家都能够接受的研究成果出现。

3. 实时可信构件的实质

3.1. 实时的内涵

在描述实时性时，时间是一种重要的资源，主要体现在：对外部事件的响应和任务执行都必须在限

定的时间内完成；在限制的时间内完成消息的发送和接收输出结果的正确性不仅取决于计算所形成的理辑结果，还要取决于结果产生的时间[14]。实时的内涵包括：

1) 可预测性：是指执行的操作按预先定义或确定的方式执行。其操作执行的时间是可预知的。

2) 及时性：是指按照实时活动的最后期限和当前可用的资源来进行调度，使操作能在最后期限到达前完成。

3) 用户控制：是指用户对系统(构件)的行为具有有效的控制能力。

4) 任务定向：是指任务的成功程度依赖于整个系统所获得的与实时约束有关的信息。

5) 紧急性：实时活动的紧急程度，服务失败造成的后果

6) 可靠性：失败的概率。恢复的概率等。

7) 低延迟：回馈的时间参数和控制的响应速度。

3.2. 可信性的含义

1985 年 Laprie 正式提出可信性(dependability)以便与可靠性(reliability)相区别。简言之，可信性指系统在规定时间与环境内可交付可信服务的能力。可信性是一个复杂的综合性概念，针对于构件来说，我们认为它所包含的特征有：重用性、可靠性、防危性、安全性。

重用性：在相似领域内，早先开发出来的构件在建立新系统时能够很方便地使用和在新系统中某个时刻可用的概率。

可靠性：构件在一个完整的时间间隔之内正常服务的能力。可以描述为一个时间函数 R(t)，被定义为系统在某个时间段正确执行的概率。

防危性：在给定的时间内不发生灾难性事故的概率。和可靠性不同，防危性强调的是防止危险发生，必要时可停止服务。

安全性：美国计算机安全专家 Bruce Schneier 这样认为：“安全不是产品；安全是一条链子，包括了硬件、软件、网络、使用者以及相互交互的复杂系统。在这条链子上，任何一个环节出现问题，安全将不存在，这条链子的强度由链子最弱一环的强度决定。”安全性又可分为保密性和完整性，保密性表示未经访问许可禁止访问敏感数据的能力。完整性指保持数据一致性的能力。这里的安全性指在构件中实现经过授权许可的用户比较容易方便地接触到数据和系统，同时防止一些人未经许可地获得数据，防止一些恶意的人对系统进行攻击的能力[15]。

为构件保障上述特性，可以从许多方面着手：可以加强构件的体系结构和代码设计，使得它们天生强壮；可以引入冗余机制，采用资源复制的方式提高系统可靠性和可用性；可以在构件设计中通过引入 PKI 技术，封装加密算法来提高构件安全性。但是，如何以一种统一的方式考虑构件可信性保障问题，是实时可信构件技术要研究的课题。

3.3. 实时可信构件的定义

对构件的定义影响较大的主要有三个：在 1996 年的 ECOOP 会议上提出的软件构件是一个具有规范接口和确定的上下文依赖的组装单元，软件构件能够被独立部署和被第三方组装；Szy perski 给出的软件构件是可单独生产、获取、部署的二进制单元，它们之间可以互相作用构成一个功能系统；CMU/SEI 的构件是一个不透明的功能实现，能够被第三方组装，符合一个构件模型。构件有两个本质属性：重用和易用。为了达到易用，标准化是必不可少的[16]。再考虑到实时和可信两个属性，我们给出实时可信构件的定义：

定义：实时可信构件是被标准化的具有重用性、可靠性、防危性和安全性的，能够提供实时应用软

件资源。

4. 实时可信构件技术的研究内容和方法

4.1. 研究内容

对实时可信构件的实时性的研究需要解决在构件模型中如何有效地表示实时属性；在构件的分析设计模型中如何提供构件实时属性的恰当描述；在进行领域设计时如何解决并行、异步等一系列的问题。结合实时 CORBA 规范，需要重点解决的首先是基于动态优先级调度，完成这一任务的难点是，对于动态优先级驱动的系统，还没有行之有效的分析和验证手段[17]。其次是服务调度模型，现在虽然已经有多个模型提出，但是如何使得调度模型更加合理、有效、简洁方面，还有待研究。接着是如何实现构件的优先级到本地操作系统优先级的映射。最后是优先级倒置问题，实时可信构件支持可信服务，其优先级倒置问题就更为复杂。

研究软构件个体的可信技术，包括在构件的设计、开发、测试和验证方法上都要对可信属性有所考虑和评估，这就要求在程序设计和开发方法，从代码级上有所体现。对于支撑平台来说，在构件开发时可以提供一个保证其可信性属性的开发框架，以目前中间件提供的开发框架为基础，增添一些对可信属性进行评估和度量的工具当然这涉及到研究对可信系统和构件的可信属性进行建模、分析和预测的技术。此外，还应该考虑构件在运行过程中，如何在环境的变化下维护其可信属性。当然在实现实时可信构件时有可能会出现冲突，那么这时就必须选择合适的平衡点。

基于以上分析，实时可信的构件技术主要研究的内容为：

1) 支持实时可信服务软件的构件体系结构。重点研究构件的实时可信性能保证机制，立足于传统成熟架构规范基础之上，研究自适应的可信构件体系结构，实现对现有基础结构的实时可信的扩展，包括可信构件的表达和标识、存储和检索、生成和组装、以及构件运行管理。

2) 实时可信构件的功能与性能分离机制。分离系统功能实现与系统性能保障，把实现应用系统性能保障的模块抽象成通用的性能服务构件，基于性能策略库选择、定制及动态策略与机制，为应用系统提供性能保障。

3) 实时可信构件的运行管理机制。从构建模型的自适应能力以及自适应的系统集成框架两个方面着手，研究构件的上下文感知技术和系统的自适应调度机制，为最终用户系统提供实时可信的服务保证。

4) 从设计方案级出发，形式化描述各类可信服务构件的功能参数和性能指标，建立基于可信服务构件的应用系统的数学模型；分析已有的评估模型，研究一种针对基于可信服务构件的应用系统的正确性和多项性能指标进行一体化评估验证的解决方案。

4.2. 研究方法和成果预期

对实时可信构件的研究，首先应该在体系结构上提供对实时和可信服务的支持。我们的研究基于 OMG 提供的实时 CORBA 体系结构之上，并且采用了 PKI 技术，把实时性和安全性作为实时可信构件的功能参数，放在构件内部来实现；将可靠性和防危性作为非功能参数来进行描述，放在一个称之为复制代理的部件中实现。这样做的目的是为了保证构件的实时性，因为为了保障构件的可靠性，需要使用冗余机制，这必然会对构件的实时性造成影响。此外我们还引入了一个全局监视器，其主要功能是监视硬件、操作系统和构件的运行，当发现异常时监视器及时的向复制代理和资源管理器报告。复制代理负责完成关键数据的复制，并保证数据或事务处于一致性状态；资源管理器主要负责整个系统资源的分配，以解决实时可信构件在实时性和可信性等各方面的冲突，按照一定的策略在实时可信的各项指标间取得一个平衡。为了解决构件的上下文感知技术和系统的自适应调度机制，我们采用了反射式中间件的思想，

在 ORB 中完成该功能。此外在构件的开发时提供一个保证其可信性属性的开发框架，并在软件开发时，借用面向方面的编程(AOP)的思想。

套用 Bruce Schneier 对安全的定义，如果实时构件所运行的整个硬件、软件平台是可信的，则整个系统就是可信的；如果整个硬件、软件平台是不可信的，那么最终整个系统的可信性，取决于系统可信性最薄弱的一个环节。但是我们的构件(软件)能够提供比一般软件更为可信的结果。

5. 结束语

本文以实时可信构件为研究对象，描述了实时构件和可信性的发展历史和现状，并以此为基础探讨了实时和可信的本质内涵，最后指出了实时可信构件技术所需要解决的问题以及解决这些问题的方法，为下一步工作的展开奠定基础。

参考文献 (References)

[1] Satyanarayanan, M. (2001) Pervasive Computing: Vision and Challenges. *IEEE Personal Communications*, **8**, 10-17.

[2] 杨仕平, 熊光泽, 桑楠. 安全关键系统高可信保障技术的研究[J]. 计算机科学, 2003(5): 97-101.

[3] Stankovic, J.A. (1988) Misconceptions about Real-Time Computing. *IEEE Computer*, **21**, 10-19.

[4] Object Management Group Real-Time CORBA: A White Paper. Issue 1.0. OMG, 1996.

[5] Object Management Group Real-Time CORBA1.0: Request for Proposed Paper. OMG, 1997.

[6] Object Management Group Realtime CORBA 1.0. March l999.

[7] Illela, C.V., Becker, L.B. and Pereira, C.E. (2001) Framework for Component-Based Development of Distributed Real-Time Systems. *Proceedings of* 6*th International Workshop on Object-Oriented Real-Time Dependable Systems*, 8-10 January 2001, 85-90.

[8] Hannemann, U. and Hooman, J. (2001) Formal Design of Real-Time Components on a Shared Data Space Architecture. *Computer Software and Applications Conference*, Chicago, 143-150. http://dx.doi.org/10.1109/cmpsac.2001.960610

[9] Yau, S.S. and Xia, B. (1998) An Approach to Distributed Component-Based Real-Time Application Software Development. *Object-Oriented Real-Time Distributed Computing Proceedings*, *IEEE*, Kyoto, 20-22 April 1998, 275-283.

[10] NSF Program Announcement/Solicitation: Trusted Computing. http://www.nsf.gov/pubs/2001/nsf01160/nsf01160.html

[11] Department of Computer Science of the Technical University Darmstadt. Trusted Systems. http://www.dvs1informatik.Tudarmstadt.de/DVS1/researc/index.htm1

[12] 张焕国, 罗捷, 金刚等. 可信计算研究进展[J]. 武汉大学学报(理学版), 2006(5): 513-518.

[13] 彭舰, 李征. 实现具有实时－容错性能的 CORBA 中间件的研究[J]. 计算机应用, 2006(6): 1251-1253.

[14] 骆志刚, 胡健, 刘锦德. 开放系统中的实时性[J]. 计算机科学, 2001(1): 57-60.

[15] 周明辉, 梅宏. 可信计算研究的初步探疑[J]. 计算机科学, 2004(7): 5-8.

[16] 古幼鹏. 嵌入式实时软件的构件化开发技术研究[D]: [博士学位论文]. 成都: 电子科技大学, 2005.

[17] 汪芸, 谢俊清, 沈卓炜, 顾冠群. 实时 CORBA 技术综述[J]. 东南大学学报, 2002(3): 311-316.