doi:10.3969/j.issn.1000-436x.2013.z1.022

高可靠嵌入式计算机系统的发展

孔德岐，李亚晖，郭鹏
（中航工业西安航空计算技术研究所 机弹载航空重点实验室，陕西 西安 710119）

摘 要：通过归纳高可靠嵌入式计算机系统的技术特征，分析高可靠嵌入式计算机系统的实现途径，对高可靠嵌入式计算系统的演进进行了系统论述，分别从基础可靠性、系统可用性、系统完整性和系统可信性等技术途径详细地分析了高可靠计算机系统的发展思路，并结合高可靠技术的发展趋势，提出了涵盖完整性等级、容错范围和余度范围等 3 个维度的高可信嵌入式计算机体系架构，以使人们对高可靠嵌入式计算机系统的认识更加清晰，从而把握高可靠嵌入式计算机系统发展的要点。

关键词：嵌入式计算机；高可靠技术；容错技术；故障检测
中图分类号：TP311.52 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0170-06

Development of dependable embedded computer systems

KONG De-qi, LI Ya-hui, GUO Peng
(Airborne and Missile-borne Aviation Key Lab, Aeronautical Computing Technique Research Institute，Xi'an 710119, China)

Abstract: The technical features and implement methods of dependable embedded computers were concluded and analyzed, of which the evolution was systemically described. The development process was depicted by four phases, the basic reliability, the system availability, the system integrity and the system dependability. Based on the trend of dependable technology, the dependable computer architecture was proposed with three dimensions, integrity level, fault-tolerant scope and redundancy scope, in order to emphasize the key technologies in the safety critical domain.

Key words: embedded computer; dependability technology; fault-tolerant technology; failure detection

1 引言

嵌入式计算机系统是计算机应用的一种重要形式，是以应用为中心，以计算机技术为基础，软硬件可剪裁，适合于应用系统对功能、可靠性、成本、体积、功耗等有严格要求的专用计算机系统[1,2]，其系统的主要构成如图 1 所示。嵌入式计算机系统的可靠运行能力越来越受到人们的关注，因此发展高可靠嵌入式计算机系统也成为了一种趋势。高可靠嵌入式计算机系统是综合满足系统可靠性、安全性和完整性等非功能需求的嵌入式系统，其中，可靠性、安全性和完整性是相互关联的系统属性，可靠性强调系统连续服务能力，而安全性则强调系统避免出现危险性故障的能力；完整性是强调系统正确服务的能力。

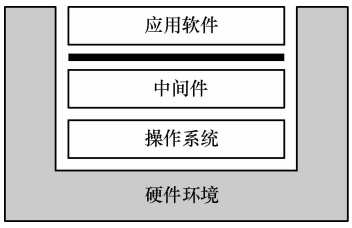

图 1 嵌入式计算机系统的主要组成

随着技术的发展，高可靠计算机系统的实现途径在不断地演进着，通过分布式容错和高完整性计算技术可构建新型的余度容错架构，能够减小系统计算机的容错粒度，提高系统的可扩展性和维修性；通过故障诊断与预测可在事前对嵌入式计算机的健康状况进行评估，并在评估的基础上找出薄弱环节，做到在事前维修和维护的目的。通过自愈和重构技术可有效提高系统在运行过程中的可靠性和有效

收稿日期：2013-08-13

性，消除由单一故障导致的任务执行失败，提高系统的可靠运行能力[3~6]。高可靠计算机系统的发展过程可归纳为 4 个主要阶段，如图 2 所示。

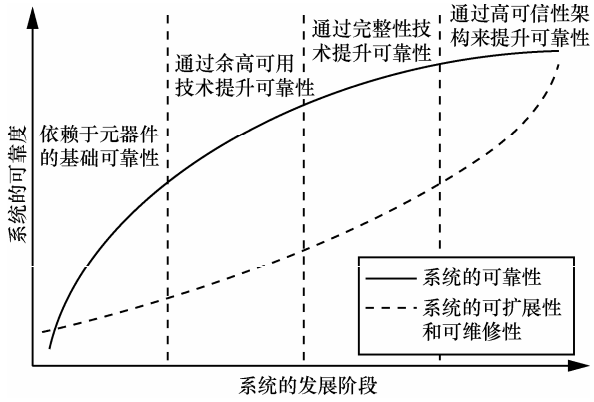

图 2　高可靠嵌入式计算机系统发展趋势

1) 第一阶段，通过提高硬件的可靠性来实现系统的可靠工作。

2) 第二阶段，通过提高系统的可用性来实现系统的可靠工作。

3) 第三阶段，通过提高系统的完整性来实现系统的可靠工作。

4) 第四阶段，通过提高系统的可信性来实现系统的可靠工作。

2　提高硬件可靠性的途径

嵌入式计算机系统的主要组成部分有嵌入式操作系统、嵌入式微处理器、外围硬件设备、开发调试平台和控制与应用程序，如图 1 所示。

通过提高硬件的可靠性来实现高可靠计算机系统的措施主要有，选择高质量的元器件和采用降额设计技术。

2.1　采用高质量的元器件

根据可靠性的定义，系统的可靠性可用系统的平均故障时间来衡量。而系统的平均故障时间是由组成系统的各个元器件的平均故障时间决定的[7]。

$$\begin{aligned} Rate_{\text{component}} &= 1/MTTF_{\text{component}} \\ Rate_{\text{system}} &= \sum Rate_{\text{component}} \\ MTTF_{\text{system}} &= 1/Rate_{\text{system}} \end{aligned} \tag{1}$$

由式(1)可知系统组件的故障率之和越低，系统的可靠性就越高。组件的故障率为组件平均故障时间的倒数，因此采用平均故障时间越高的元器件，其故障率就越低，而总的故障率之和也就越低，则系统的可靠性就越高。由此可知采用高质量的元器件可提高系统的可靠性。

2.2　采用降额设计技术

一般情况下，元器件在额定应力值下能正常工作，然而在额定值下工作的元器件，其失效率即故障率往往比较大。使用降额设计技术限制构成电子设备的元器件在使用中所承受的应力（电、热和机械应力），将元器件在低于其设计的额定值下使用可延缓其参数退化，增加元器件的使用寿命即增加其平均故障时间，由前文可知平均故障时间越高则构成系统的可靠性就越高[8]。因此采用降额设计技术也可提高系统的可靠性。

3　提高系统可用性的途径

在高可靠嵌入式计算机系统的设计中，除了提高硬件的可靠性之外，还可通过提高系统的可用性来提高系统的可靠性。这方面可通过余度设计技术及软件恢复技术来实现。

3.1　余度设计技术

余度是获得高可靠系统的一种设计方法。根据美军 MIL-F-9490D 的定义，余度是需要出现 2 个或 2 个以上故障，而不是一个单独故障，才引起既定不希望发生工作状态的一种设计方法[9,10]。余度的设计方式主要有 3 种：1) 采用 2 个或 2 个以上的，且每个都能执行给定功能的部件、分系统或通道；2) 采用监控装置，可自动检测故障，完成指示、部件切换等；3) 前 2 种方式的混合。

余度设计技术是通过组件复本的方式来提高系统的容错能力从而提高系统的可靠性。而这些组件能按照所定义的一组容错模型（如主动的、被动的，以及选择混合的）来提高容错能力。容错复本可通过以下几种模型实现：主动复本、被动复本、主体/影子复本、*N* 版本复本和检查点[11]。这几种复本容错模型可针对具体情况应用在不同的场景中，从而保障系统能够平稳持续地服务。

因此，采用余度设计技术提高了系统的容错能力，从而提高了系统的可靠性。

3.2　软件恢复技术

嵌入式计算机系统不仅是由硬件组成的，软件也是构成嵌入式计算机系统的一部分。若在软件设计中出现错误则同样会造成系统的崩溃而不可用。因此，提高软件的可靠性也是提高系统可靠性的一种途径。软件恢复技术是提高软件可靠

性的一种方法。

在很多软件系统中，都会出现软件衰老现象。软件衰老是指，软件系统在平稳运行一段时间之后，出现系统资源衰竭，从而使系统出现服务进度、质量下降，甚至挂起停机的现象，造成系统运行不稳定[12]。软件衰老是软件可靠性的大敌，且软件衰老是不可避免的。

造成软件衰老的原因主要有 2 个：Heisenbug 和致使资源衰竭的 bug。Heisenbug 是那种仅当多个特定事件均得到满足的情况下才出现故障的 bug。这类 bug 是几乎不能被排除的。而致使资源衰竭的 bug 是指由软件开发过程中的一些缺陷造成的。常见的有硬盘交换分区被填满、内存耗尽、缓冲区溢出等。这类 bug 在一般的开发和测试过程中往往因其不造成程序执行中断等表象特征而很难被完全发现。

软件恢复技术是延缓软件衰老现象的一种方法。软件恢复技术是一种“预反应式”容错机制。它主要通过周期性地暂停软件运行，清除系统运行的内部状态，然后重启恢复到干净的初始或中间状态，抢先预防可能发生的严重故障，因此软件恢复技术也被称为“抢占式”预防维护技术。软件恢复技术一般应用在要求高可用性和数据完整性的服务器软件上。但需要强调的是，有些软件自身没有自动保存中间结果和载入进度的功能，若单纯使用软件恢复技术则达不到减缓软件衰老的目的。这时可与检查点技术相结合，使用检查点技术在合适的时候保存干净的中间状态，然后使用软件恢复技术恢复到保存的状态载入数据继续运行，从而达到目的。

4 提高系统完整性的途径

完整性的定义为输出错误的概率，对一些应用也可定义为未检测故障发生的概率。高可靠嵌入式计算机系统的第三阶段是提高系统的完整性，可通过提高数据计算的完整性、数据存储的完整性和数据传输的完整性实现。

4.1 数据计算的完整性

锁步技术是保证数据计算完整性的一种方法，锁步技术的结构如图 3 所示。

锁步技术的特点[13,14]主要有以下 5 点。

1) 两方都复制所有的处理、存储器访问和 I/O 功能。

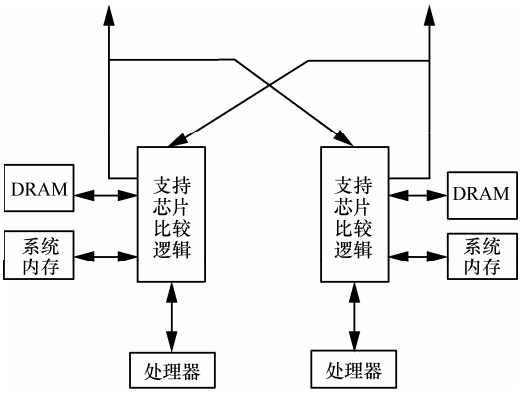

图 3 锁步技术结构

2) 比较逻辑确定何时一方有故障。

3) 每一方都能与另一方进行外部通信。

4) 一旦检测出故障，处理器就自己离线。

5) 如果故障是可恢复的（如检测到存储器中有一个 SEU，并且将正确的数值从对方加载过来），处理器就重新将自身插入到操作中。

锁步技术的优点如下。

1) 锁步处理减少了冗余的要求。

2) 与可靠的 BIT/BITE 相结合，锁步处理器可以提供 100%的故障覆盖。

3) 能够提供交叉通道的信任，但不需要进行交叉通道的表决。

4) 在处理拜占庭式的失效状态（Byzantine failure conditions）时所需要的处理模块（资源）最小。

5) 能提供自愈式的降级。

且经实际测试比较，对故障状态的补偿，锁步处理能使所需要的通道数量最小。

4.2 数据存储的完整性

保持数据存储完整性的方法主要有 *n*+1 存储、海明容错码（纠 1 检 2）等。

4.2.1 *n*+1 存储

n+1 存储是指按照一定的容错算法，将数据存放在 *n*+1 个硬盘上，实际数据占用的有效空间为 *n* 个硬盘的空间总和，而第 *n*+1 个硬盘上存储的数据是校验容错信息，当这 *n*+1 个硬盘中的其中一个硬盘出现故障时，从其他 *n* 个硬盘中的数据也可以恢复原始数据，这样，仅使用这 *n* 个硬盘也可以带伤继续工作（如采集和回放素材），当更换一个新硬盘后，系统可以重新恢复完整的校验容错信息[15,16]。由于在一个硬盘阵列中，多于一个硬盘同时出现故障率的几率很小，所以一般情况下，使用 *n*+1 存储，

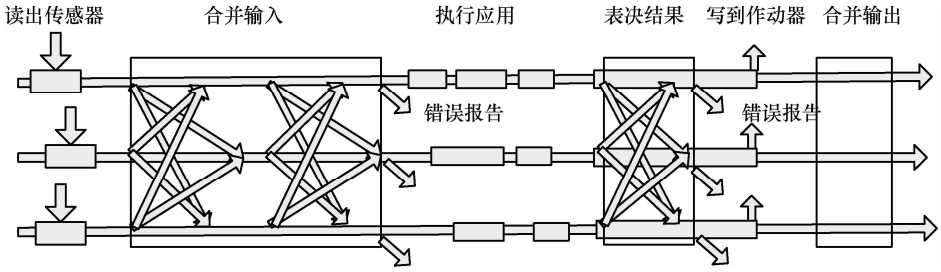

图 4　冗余通道中的数据完整性监控与校验

安全性是可以得到保障的。

4.2.2　海明容错码

海明容错码是一种被广泛采用的很有效的校验方法，是只要增加少数几个校验位，就能检测出 2 bit 同时出错、亦能检测出 1 bit 出错并能自动恢复该出错位正确值的有效手段，后者被称为自动纠错[17]。它的实现原理为，在 k 个数据位之外加上 r 个校验位，从而形成一个 $k+r$ bit 的新的码字，使新码字的码距比较均匀地拉大。把数据的每个二进制位分配在几个不同偶校验位的组合中，当某一位出错后，就会引起相关的几个校验位的值发生变化，这不但可以发现出错，还能指出是哪一位出错，为进一步自动纠错提供了依据。

不论是(n+1)存储还是海明容错码，这 2 种存储机制均可以在数据发生错误时，检测出错误并对数据进行纠正，保证了数据存储的正确性和完整性。

4.3　数据传输的完整性

在数据的传输过程中，可能受到噪声干扰等多种原因而导致传输的数据发生错误，若不采取适当的措施，则数据的接收者就会收到一个错误的数据，从而影响对数据的操作甚至因此而产生致命的错误[18,19]。因此，在数据传输方面，保证数据的完整性是非常必要的。而在数据传输的完整性方面，较常用的技术为传输校验码“CRC”，使用 CRC，数据的接收者可以在收到数据的同时对接收到的数据进行完整性检验，即用收到的数据和校验码进行模 2 除法，若所得结果为 0，则表示接收到的数据是正确的，若结果不为 0，则可根据结果进行相应的操作。

4.4　数据操作的完整性

数据操作的完整性主要是针对数据操作的行为进行监控，也就是对数据操作的故障检测机制进行监控，通过对故障的检测、故障诊断和故障屏蔽等技术措施实现数据操作的高完整性[20,21]。故障检测的对象包括数据来源、数据产生时机和数据值域范围等。数据检测行为主要是通过多副本之间的表决来实现，采用有效的诊断机制识别故障，并把错误信息进行记录。故障屏蔽是实现数据完整的应对措施，利用表决结果中取得的正确数据值来掩盖错误数据，从而达到数据操作的高完整性，处理过程如图 4 所示。

5　提高系统可信性的途径

随着信息技术和电子技术的发展，嵌入式系统功能越来越强大、其结构也越来越复杂，且大多数嵌入式设备已接入互联网，这些进步为嵌入式系统的设计带来新的挑战。因此，嵌入式系统高可信能力的提高显得越来越紧迫。ISO/IEC15408 标准中给出了可信性的定义：可信的组件、操作或过程的行为在任意操作条件下是可预测的，并能很好地抵御应用程序软件、病毒以及一定的物理干扰造成的破坏。可信性包括：可用性、可靠性、安全性、完整性、机密性和可维护性等[22,23]，如图 5 所示。

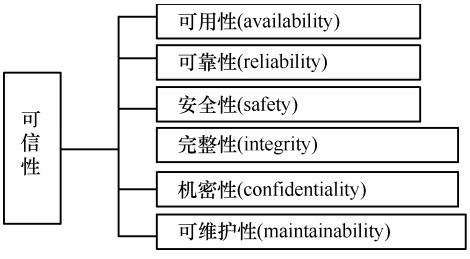

图 5　可信性的内涵

在嵌入式计算机系统中，可信性是高可靠技术的综合发展趋势，它涵盖高可靠技术的众多技术特征。为了能够综合可信属性来达到嵌入式计算机系统的高可靠需求，提高系统可信性的技术途径主要为高可信架构设计技术。

高可信嵌入式计算机的体系架构的容错技术主要体现在 3 个维度[24]，如图 6 所示。在纵向维度上可以从处理器指令级、操作系统级、中间件级到

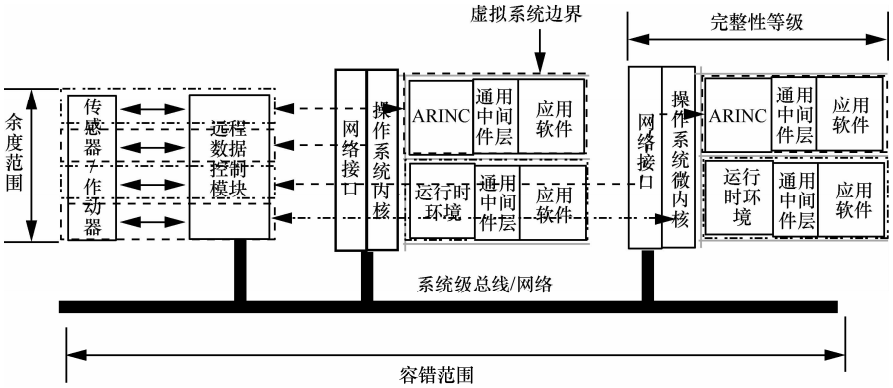

图 6　高可信嵌入式计算机的体系架构

应用级进行容错，从而保证数据的高完整性；在横向维度上可以从计算节点、通信网络、控制节点到终端传感器节点进行分布式容错，从而保证全系统的数据传输与计算的完整性；在垂直维度上，利用多通道冗余技术实现系统错误容忍。

6　结束语

嵌入式计算机系统作为计算机的一种应用形式，随着科技的发展以及人们的应用需求，嵌入式计算机系统被广泛地应用在各行各业，因此嵌入式计算机系统的安全性和可靠性也越来越受到人们的重视。嵌入式计算机系统在可靠性方面面临着许多挑战，比如组件的可靠性、系统的可用性、数据的完整性等，本文从嵌入式计算机系统发展的 4 个阶段，分别从硬件、设计技术以及体系结构等方面对高可靠嵌入式计算机系统的演进进行了阐述。在可靠性要求非常严格的领域，如航空领域，发展高可靠性的嵌入式系统是非常必要的。

参考文献：

[1] 欧国建, 石为人.面向多嵌入式系统的构架研究[J].计算机应用, 2009, 12(29):203-206.
OU G J, SHI W R. Research of framework for multi-embedded system[J]. Journal of Computer Applications, 2009,12(29):203-206.

[2] 徐琼, 徐科挺. 计算机嵌入式操作系统研究[J].科技资讯, 2012, 4(10):13-15.
XU Q, XU K T. Research of computer embedded OS system[J]. Science & Technology Information, 2012, 4(10):13-15.

[3] 徐明, 沈希, 钱陆均. 嵌入式计算机系统技术[J].工业仪表与自动化装置, 2005,6(11):101-104.
XU M, SHEN X, QIAN L J. The technology of an embedded microprocessor unit system[J]. Industrial Instrumentation & Automation, 2005,6(11):101-104.

[4] OBERMAISSER R, KOPETZ H. A Candidate for an ARTEMIS Cross-Domain Reference Architecture for Embedded Systems[D]. Vienna University of Technology, 2009.

[5] KAYALI S. Reliability and qualification of III/V semiconductor devices for space applications[J]. Electronic Packaging&Space Parts News: EEE Links,1999,5(4):l4-l9.

[6] SURI N. DECOS: Dependable Embedded Components and Systems [D]. Darmstadt University of Technology, 2007.

[7] 陈颖, 孙博, 谢劲松等. 高可靠元器件的使用环境、试验条件和失效机理[M]. 可靠性物理与失效分析技术, 2007.
CHEN Y, SUN B, XIE J S, *et al*. Typical Use Environmental Conditions, Test Conditions and Failure Mechanisms of High Reliability Electronic Components[M]. Electronic Product Reliability and Environmental Testing, 2007.

[8] 邓超,于平,施炜雷.电路仿真在可靠性设计中的应用[J].微计算机信息,2008, 24(11):268-270.
DENG C, YU P, SHI W L. The application of circuit simulation on designing for reliability[J]. Microcomputer Information, 2008, 24(11): 268-270.

[9] 刘小雄, 章卫国, 李广文. 电传飞行控制系统的余度设计技术[J]. 飞机设计, 2006,3(1):35-38.
LIU X X, ZHANG W G, LI G W. Redundancy techniques for fly-by-wire flight control systems[J]. Aircraft Design, 2006, 3(1):35-38.

[10] 石贤良. 飞行控制计算机系统余度管理技术研究[D].西安: 西北工业大学, 2009.
SHI X L. Research of Redundancy Management Technology in Flight Control Computer System[D]. Xi'an: Northwestern Polytechnical University, 2009.

[11] BEARD R V. Failure Accommodation in Linear System Through Self Reogrnnaization[D]. Cambridge, 1971.

[12] 李亚, 万群丽, 许满武. 软件恢复技术研究[J].计算机科学, 2003, 4(10):48-50.
LI Y, WAN Q L, XU M W. Research of software recovery technology[J]. Computer Science, 2003, 4(10):48-50.

[13] 陈浩. 处理器 Lockstep 技术研究[J]. 数字技术与应用, 2012, 8(12): 98-101.
CHEN H. Research on processor lockstep technique[J]. Digital Technology & Application,2012,8(12):98-101.

[14] 杨蓓, 吴振强, 符湘萍. 基于可信计算的动态完整性度量模型[J]. 计算机工程, 2012,38(2):78-81.
YANG B, WU Z Q, FU X P. Dynamic integrity measurement model based on trusted computing[J]. Computer Engineering, 2012, 38(2):78-81.

[15] KOPETZ H. An integrated architecture for dependable embedded systems[A]. Proceedings of the 23rd IEEE International Symposium

on Reliable Distributed Systems[C]. 2004. 250-262.

[16] 钱华明,李仲玉,马吉臣.海明码在提高导航数据传输可靠性中的应用[J]. 微计算机信息,2008, 24(12):225-227.
QIAN H M, LI Z Y, MA J C. The application of Hamming code in improvement of navigation transmission's reliability of date[J]. Microcomputer Information, 2008, 24(12):225-227.

[17] 李霄, 石文昌, 梁朝晖等. 进程运行时完整性度量的体系结构设计[J]. 微电子学与计算机, 2009, 26(9):183-186.
LI X, SHI W C, LIANG Z H, *et al*. Design of an architecture for process runtime integrity measurement[J]. Microelectronics & Computer, 2009, 26(9):183-186.

[18] 何坤.一种基于动态反馈的数据存储可靠性保证方法[J]. 电脑知识与技术, 2011,7(28):6901-6903.
HE K. Data reliability assurance method based on dynamic feedback[J]. Computer Knowledge and Technology, 2011, 7(28):6901-6903.

[19] 朱庆, 周艳. 分布式空间数据存储对象[J]. 武汉大学学报, 2006, 31(5):391-394.
ZHU Q, ZHOU Y. Distributed spatial data storage object[J]. Geomatics and Information Science of Wuhan University, 2006, 31(5):391-394.

[20] 吕雪锋, 程承旗, 龚健雅等. 海量遥感数据存储管理技术综述[J]. 中国科学, 2011, 41(12):1561-1573.
LV X F, CHENG C Q, GONG J Y, *et al*. Review of data storage and management technologies for massive remote sensing data[J]. China Tech Sci, 2011, 41(12):1561-1573.

[21] 孙鹏, 赵军锁, 张文君. 软件容错:技术与展望[J].计算机工程与科学, 2007,29(8):88-92.
SUN P, ZHAO J S, ZHANG W J. Software fault tolerance:techniques and prospects[J]. Computer Engineering & Science, 2007, 29(8):88-92.

[22] SWIFT M M, BERSHAD B N, LEVY H M. Improving the reliability of commodity operating systems[J]. ACM Trans on Computer Systems, 2005, 23(1):124-131.

[23] JAEGER T, SAILER R, SHANKAR U. PRIMA: policy-reduced integrity measurement architecture[A]. Proc of the 11th ACM Symposium on Access Control Models and Technologies[C]. Lake Tahoe, USA, 2006.19-28.

[24] 杨霞. 高可信嵌入式操作系统体系架构研究[J].计算机应用,2006, 26(5):120-124.
YANG X. Research of high dependable embedded OS system architecture[J]. Journal of Computer Applications, 2006, 26(5):120-124.

作者简介：

孔德岐（1962-），男，陕西西安人，中航工业西安航空计算技术研究所研究员，主要研究方向为计算机系统结构、高可靠计算机。

李亚晖（1976-），男，湖南新邵人，中航工业西安航空计算技术研究所高级工程师，主要研究方向为嵌入式计算机体系结构、嵌入式软件。

郭鹏（1987-），男，陕西渭南人，中航工业西安航空计算技术研究所助理工程师，主要研究方向为机载嵌入式软件、系统仿真与建模。