基于系统安全性的嵌入式系统设计与实施探讨

陈静勇
中国中车　湖南　株洲　412002

摘　要：嵌入式系统已经广泛应用于人们生活与生产中，随着嵌入式系统的广泛应用，人们对于嵌入式系统的安全性也提出了更高的要求。本文针对嵌入式系统的安全性进行了研究，并对嵌入式系统安全性设计与实施进行了分析与探讨，通过构建嵌入式系统安全需求模型，制定了基于安全性设计的嵌入式系统设计方案，并通过安全性验证与测试实验，验证了该方案的可行性与有效性。本文从嵌入式系统概述与安全性分析入手，深入探讨了嵌入式系统设计原则，并提出了一种基于系统安全性的嵌入式系统设计方案，通过对该方案进行实验验证和分析，证明该方案具有较高的可行性。

关键词：系统安全性；嵌入式系统；可靠性；安全性分析；

引言

嵌入式系统是一种将系统设计与硬件设备相结合的特殊产品，其功能主要是为人们提供生活生产所需的服务。随着嵌入式系统的广泛应用，人们对嵌入式系统的安全性提出了更高的要求。在实际应用中，嵌入式系统与外界环境紧密结合，受到外界环境的影响较大，这就使得嵌入式系统容易受到攻击，从而导致系统无法正常运行。因此，针对嵌入式系统进行安全性分析，制定相应的安全设计策略是非常有必要的。本文在深入分析嵌入式系统特点的基础上，从安全需求和设计策略两个方面探讨了嵌入式系统安全性设计与实施问题。通过实验验证了该方案具有可行性。

1 嵌入式系统概述与安全性分析

1.1 嵌入式系统基本概念

嵌入式系统（Embedded System）是以应用为中心，以计算机技术为基础，软硬件可裁剪，适用于特定应用场合的专用计算机系统。它主要由嵌入式微处理器（ARM）、嵌入式操作系统（Embedded OS）、外围设备三大部分组成。随着科技的不断发展，嵌入式系统的种类也在不断增多。目前市场上比较常见的有基于PC机和基于单片机的嵌入式系统，还有基于网络通信和基于移动通信等特殊应用场合的嵌入式系统。

1.2 嵌入式系统设计原则

嵌入式系统设计要遵循的基本原则有：可靠性原则、安全性原则、实时性原则以及通用性原则。可靠性是嵌入式系统最主要的性能指标之一，对于嵌入式系统来说，如果不能保证其可靠性，那么整个嵌入式系统就无法正常运行。安全性是嵌入式系统设计的一个重要方面，在嵌入式系统中，安全性的重要性不容忽视。嵌入式系统是一个特殊的产品，其安全性在设计中必须得到高度重视，严格按照其安全需求进行设计与实施。通用性是嵌入式系统应用的一个重要特点，只有具有良好通用性的产品才能被广泛应用。在嵌入式系统中，通用性是指在特定场合下应用的产品必须具有良好的通用性。

1.3 嵌入式系统安全性概述

嵌入式系统是以应用为中心，以计算机技术为基础，软硬件可裁剪，适用于特定应用场合的专用计算机系统。嵌入式系统的安全性主要包括四个方面：一是硬件安全，即嵌入式系统硬件设备的安全性；二是软件安全，即嵌入式系统软件的安全性；三是使用安全，即嵌入式系统使用过程中的安全性；四是数据安全，即嵌入式系统数据信息的安全性。随着嵌入式技术的发展，嵌入式系统的应用越来越广泛，其安全需求也越来越高。针对不同类型的嵌入式系统，其安全需求也不尽相同。因此在进行嵌入式系统设计与实施时需要结合其应用环境，以确保其安全性。

1.4 安全性分析方法

嵌入式系统的安全性分析主要有形式化方法、定量方法和定性方法。形式化方法是一种用于分析安全问题的工具，它是一种形式化的安全模型，通过建立系统模型，能够对系统的安全性进行评估，并给出相应的解决方案。半形式化方法是一种在形式化基础上结合半形式化技术的安全分析方法，该方法通过将安全需求转化为安全属性来描述安全性。定量方法主要包括概率语言模型、模糊概率语言模型和随机语言模型等。定性方法主

作者简介：陈静勇，1976出生，男，汉族，江西萍乡人，硕士研究生，职称：工程师，研究方向：嵌入式系统。

要是通过对嵌入式系统进行观察、描述等方式，来确定其安全性，并给出相应的解决方案。下面将对嵌入式系统的安全性分析进行具体介绍。

2 系统安全性需求分析与设计

2.1 系统安全性需求分析

系统安全性需求主要包括硬件安全、软件安全和用户需求。硬件安全主要是指对嵌入式系统的元器件进行加固和管理，防止其受到恶意的攻击；软件安全是指对嵌入式系统的操作程序进行有效的管理和控制，防止其被非法用户恶意修改；用户需求是指用户通过正常的操作获取系统所需数据，或者对数据进行编辑处理。因此，在嵌入式系统设计中，需要对安全性进行全面评估，以确定嵌入式系统所需的硬件和软件安全等级。在确定安全等级后，可以选择合适的硬件和软件方案来满足安全需求。最后，还需要对嵌入式系统的用户需求进行分析，以保证整个系统能满足用户需求。

2.2 系统可靠性设计

嵌入式系统的可靠性是衡量其质量的重要指标，其主要包括系统在使用过程中的安全、系统的稳定运行、系统的故障处理和故障恢复等。通常情况下，嵌入式系统可以正常运行，但是在一些特殊情况下，比如突然断电、设备故障等，嵌入式系统很可能无法正常运行。因此，为了保证嵌入式系统的安全性，需要采取相应的设计策略来提高嵌入式系统的可靠性。首先，需要对嵌入式系统进行可靠设计；其次，需要通过增加设备可靠性和采取可靠措施等方法来提高嵌入式系统的可靠性；最后，还可以通过安装安全防护装置等方法来提高嵌入式系统的可靠性。

2.3 安全性设计原则

嵌入式系统的安全性设计需要遵循以下几个原则：首先，设计必须符合相关的标准和规定，并通过测试来确认其可靠性；其次，必须满足嵌入式系统的需求，并根据用户需求对其进行优化，以提高系统的可靠性；再次，在进行嵌入式系统设计时，应采取相应的措施来保障系统的安全性；最后，在嵌入式系统设计时，需要对硬件、软件和用户需求等进行全面评估，以确定是否符合安全要求。因此，在进行嵌入式系统设计时，必须遵循上述原则，并通过有效措施来确保其安全性。在进行嵌入式系统设计时，还需要注意以下几个方面：选择合适的安全方案；加强嵌入式系统的防护能力。

2.4 安全性实施策略

嵌入式系统的安全性设计必须从以下几个方面进行：增强硬件设备的可靠性，包括加固元器件和增加冗余设计等；完善软件功能，以防止非法用户恶意修改嵌入式系统软件，从而影响其正常运行；加强嵌入式系统的防护能力，包括加强硬件防护和软件防护等；加强嵌入式系统的安全管理，包括建立完善的安全管理机制和制定严格的安全管理制度等。通过上述措施，可以有效提高嵌入式系统的安全性，从而为人们提供更加安全可靠的服务。在嵌入式系统设计中，还需要注意以下几个方面：选择合适的硬件和软件方案；加强设备可靠性；优化系统防护能力。

3 嵌入式系统安全性验证与测试

3.1 安全性验证方法

在软件开发的生命周期中，安全性验证是一个不可或缺的环节。它确保了系统在面对潜在威胁时能够保持其完整性和可靠性。根据验证的范围和深度不同，我们可以将安全性验证方法分为几类。其中，逻辑验证、静态验证和动态验证是最为常见且广泛应用的三种方法。逻辑验证主要关注于系统的功能层面，通过一系列严格的测试来评估系统的行为是否符合预期。这包括对嵌入式系统执行各种操作的能力进行检查，比如对数据传输、文件访问等关键任务的验证。除此之外，非功能测试也同样重要，这些测试通常涉及系统的异常处理能力、错误恢复机制以及在面对特定输入条件下的行为表现。静态验证则侧重于对嵌入式系统内部结构和实现细节的深入分析，以此来发现可能存在的漏洞和安全缺陷。这种验证方式通常包括硬件描述语言（HDL）模拟、代码静态分析等技术，目的在于识别可能的逻辑错误、不一致之处或是设计上的疏忽。动态验证则更加注重于系统运行时的安全性，它通过实时监控系统行为并记录日志来发现潜在的问题。动态测试往往伴随着大量的调试工作，需要工程师具备高超的编程技巧和对系统行为的深刻理解。它有助于及时发现那些在传统静态测试中不易被注意到的隐患，从而在问题变得严重之前加以解决。

3.2 安全性测试工具

静态验证工具主要包括UML类图、有限状态机、状态图和状态迁移图等。UML类图主要用来描述系统的结构和状态，在进行系统的安全性测试时，首先要对系统的结构进行分析，然后再将其转换成UML类图，最后再进行系统的安全性测试。动态验证工具主要包括进程同步与中断测试、软件模块间的通信、代码级的错误检测、硬件资源监控等。在进行嵌入式系统的安全性测试时，首先要将嵌入式系统与外界环境相隔离，然后对嵌入式系统进行功能测试、静态分析和动态分析等。静态验证工

具主要用于对嵌入式系统进行功能和非功能测试。

3.3 安全性测试案例分析

为了验证本文提出的基于系统安全性的嵌入式系统设计方案的可行性，以一种基于FPGA的安全门为例，对其进行测试。首先，利用UML类图对安全门进行建模，然后对其进行安全性分析和测试。其中，UML类图的作用是对嵌入式系统进行功能和非功能测试以及安全性分析和测试；FPGA的作用是对嵌入式系统进行逻辑验证和测试。在进行安全门电路模型设计时，可以采用FPGA来实现。下面将对安全门电路进行建模和分析，以验证安全性设计方案的可行性。

4 案例分析与实验结果

4.1 案例分析

首先，通过对系统安全性的分析，以系统中嵌入式处理器为例，阐述如何对系统进行安全性设计。具体来说，嵌入式处理器需要保证系统具有可靠的性能和足够的处理能力。另外，在系统安全设计中需要将计算与存储功能分离。如果把计算功能作为一种资源进行管理，那么，系统就会出现资源不足、性能不稳定等情况。为了保证系统安全性的设计，在设计嵌入式处理器时，应该按照程序逻辑的要求对处理器进行合理划分，将硬件与软件进行分离。另外，为了避免嵌入式处理器的安全问题导致操作系统受到破坏，可以采用数据隔离的方式，将程序逻辑与存储逻辑进行分离。

4.2 实验设计

在嵌入式系统的安全设计中，主要考虑到程序逻辑、数据隔离和系统资源三个方面，其中，程序逻辑是最关键的内容。为了测试系统安全性设计的有效性，可以进行如下实验：将嵌入式系统与传统系统相比较，对嵌入式系统的安全性进行测试，并对测试结果进行分析；对嵌入式系统的程序逻辑与存储逻辑进行隔离，对程序逻辑进行测试，并将测试结果与传统系统相比较；将嵌入式系统中的存储逻辑与程序逻辑进行隔离，对程序逻辑进行测试，并将测试结果与传统系统相比较。通过以上实验可以发现，嵌入式系统具有较高的安全性。

4.3 实验结果分析

基于系统安全性的嵌入式系统设计方案是一种非常有效的嵌入式系统安全设计方法。该方法能够有效解决嵌入式系统中的安全问题，并保证系统在运行过程中具有较高的安全性。在系统安全需求模型的基础上，可以建立起相应的设计方案，并通过安全性验证与测试实验，来验证该方案的有效性。实验结果表明，采用该方案设计出来的嵌入式系统具有较高的安全性，能够有效避免安全问题导致的系统无法正常运行。

5 结语

随着社会的不断进步，嵌入式系统已经广泛应用于人们的生活与生产中，对人们的生产与生活产生了很大的影响。在实际应用中，嵌入式系统的安全性也是非常重要的，尤其是在网络时代，嵌入式系统的安全性更是直接关系到人们的生命财产安全。因此，在设计与实施嵌入式系统时，必须充分考虑其安全性问题，制定科学合理的设计策略。本文主要针对嵌入式系统进行了简要概述，并对嵌入式系统安全性进行了深入分析和探讨。希望通过本文的研究与分析可以为嵌入式系统设计与实施提供一定借鉴与参考，进一步提高嵌入式系统设计与实施质量。

参考文献

[1]黄志球,徐丙凤,阚双龙,等.嵌入式机载软件安全性分析标准、方法及工具研究综述[J].软件学报,2014,25(02):200-218.

[2]姜文,范力思.应用系统安全性解决方案探索[J].现代工业经济和信息化,2016,6(23):85-86.

[3]姜灵敏.网络会计信息系统安全性综合评价[J].产业与科技论坛,2006,(01):102-105.

[4]方艳梅.深度伪造对人脸识别支付系统安全性的挑战与应对[J].金融科技时代,2020,28(03):13-17.

[5]施淼.提升系统安全性WinXP必禁的服务[J].科技咨询导报,2007,(13):8.