硬件安全在电子系统设计中的考虑

何坤元

杭州士兰微电子股份有限公司，浙江 杭州 310012

摘　　要： 本文探讨了电子系统设计中硬件安全的重要性，分析了当前硬件安全威胁的现状，并提出了硬件安全实现的策略和防护技术。文章强调了硬件安全需求分析、安全设计原则、防护技术应用以及发展趋势等方面，并通过案例分析展示了硬件安全在实际应用中的重要性。

关 键 词： 硬件安全；电子系统设计；安全威胁；安全防护技术；功能安全

Hardware Security Considerations in the Design of Electronic Systems

He Kunyuan

Hangzhou Silan Microelectronics Co., Ltd, Zhejiang, Hangzhou 310012

Abstract: This paper discusses the importance of hardware security in electronic system design, analyzes the current status of hardware security threats, and proposes strategies and protection techniques for hardware security implementation. The article emphasizes the aspects of hardware security demand analysis, security design principle, application of protection technology and development trend, and demonstrates the importance of hardware security in practical application through case study.

Keywords: hardware security; electronic system design; security threat; security protection technology; functional security

引言

随着信息技术的飞速发展，电子系统已经深入到我们生活的方方面面，从智能手机、电脑到汽车、医疗设备，电子系统无处不在。然而，随着电子系统的普及，硬件安全问题也日益凸显。近年来，我们已经看到了多起硬件安全事件，包括供应链攻击、物联网设备被黑客利用、固件和 BIOS 漏洞等，这些事件不仅威胁到个人用户的信息安全，也对企业和社会稳定带来了严重影响。在电子系统设计中，硬件安全是一个至关重要的考虑因素，它直接关系到系统的正常运行、数据的安全性和用户的隐私保护。

一、电子系统设计中硬件安全实现

（一）硬件开发阶段的安全性功能分析

在电子系统硬件开发阶段，安全性功能分析是一个关键的步骤，它确保硬件能够在整个生命周期内安全可靠地运行。根据功能安全标准，硬件阶段功能安全研究过程主要包括：技术安全概念的硬件实现、潜在的硬件故障、与软件开发的协调。启动硬件阶段功能安全研究的原则是制定满足安全要求的硬件开发所需的活动和流程的计划[1]。硬件阶段功能开发过程如图 -1 所示。

技术安全的硬件实现要求将安全相关的系统需求转化为具体的硬件设计。这包括选择合适的硬件组件、设计冗余机制以防止单点故障，以及实施监控和诊断功能以确保硬件的持续安全性。

潜在的硬件故障分析包括识别可能导致系统失效的硬件故障模式，并评估这些故障对系统安全性的影响。通过故障树分析（FTA）和故障模式与影响分析（FMEA），开发团队可以识别和优先考虑最关键的安全风险，并设计相应的缓解措施。

与软件开发的协调是硬件安全分析过程中的另一个重要方面。由于现代电子系统通常包含复杂的软件组件，硬件和软件的紧密集成是确保系统整体安全性的关键。这要求硬件开发团队与软件开发团队紧密合作，确保硬件设计能够支持软件的安全功能，并且两者能够无缝地协同工作。

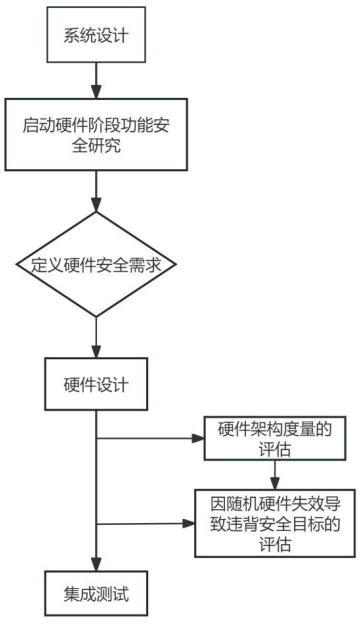

图 -1

启动硬件阶段功能安全研究的原则是制定一个详细的计划，该计划概述了满足安全要求所需的硬件开发活动和流程。这个计划应该包括设计、验证和确认活动的具体步骤，以及如何管理安全相关的变更和更新。通过这样的计划，开发团队能够确保硬件产品不仅在设计阶段符合安全标准，而且在生产、测试和维护过程中也能持续满足这些标准。

（二）硬件安全需求分析

在电子系统设计中，硬件安全需求分析是一个系统化的过程，它涉及到识别潜在的安全威胁、评估这些威胁对系统的影响，并确定必要的安全措施来防范这些威胁。这一步骤要求设计师在项目的早期阶段就考虑安全需求，并在整个设计过程中持续关注。

硬件安全需求分析的第一步是对系统可能面临的安全威胁进行全面识别。这包括：

1. 对供应链的威胁，如供应商提供的组件可能被篡改或植入恶意代码。

2. 对固件和 BIOS 的威胁，如这些基础软件可能被篡改以执行恶意操作。

3. 对硬件设计的威胁，如侧信道攻击和物理不可克隆功能（PUFs）的弱点可能被利用

4. 对物联网设备的安全风险，如这些设备可能成为网络攻击的入口点

5. 对高级持续性威胁（APT）的防御，攻击者可能利用硬件漏洞长期潜伏在系统中。

在明确了安全威胁后，设计师需要设定相应的安全目标[2]。这些目标应该与识别的威胁相对应。例如，如果供应链安全是一个关注点，那么安全目标可能包括确保所有组件都来自可信的供应商，并实施严格的验证和审计流程。接下来，为了达成既定的安全目标，设计师必须精心制定一系列具体的安全需求，这些需求将成为硬件设计和实现的行动指南，这包括采用严格的供应链管理实践，确保所有供应商都经过彻底的审查，并保障组件在运输和存储过程中的安全。同时，加强固件和 BIOS 的安全性是不可或缺的，这可以通过数字签名和加密技术的应用来实现，以防止任何未授权的修改。

在硬件设计阶段，安全性必须被内化到设计的核心，这意味着要设计出安全的硬件架构，利用硬件安全模块，并确保引导和启动过程的安全性[3]。对于物联网设备，增强安全措施尤为关键，必须采用安全的通信协议和加密数据传输措施，以防止数据泄露和未经授权的访问。例如，设计师可以集成可信平台模块（TPM）来保护设备的身份和存储的密钥，使用安全的引导过程如测量启动（Measured Boot）来确保系统的完整性，以及实施像 SSL/TLS 这样的协议来加密设备间的通信。通过这些措施，硬件设计能够抵御各种安全威胁，保护用户数据和隐私。

鉴于高级持续性威胁（APT）的复杂性，设计师还需提升系统对这些威胁的防御能力，这可以通过部署异常检测机制、及时的安全更新和有效的防御策略来实现。综合这些具体的安全需求和措施，设计师能够确保电子系统在面临多样化的安全威胁时，依然能够保持稳固和可靠。

（三）硬件安全设计原则

硬件安全设计的主要原则涉及确保硬件系统从设计到制造再到使用的整个生命周期内能够抵御各种安全威胁和攻击。

1. 硬件安全设计应遵循最小权限原则，即每个组件和用户都应该仅具有执行其功能所必需的最小权限。这有助于限制安全漏洞的影响范围，并减少潜在的攻击面。

2. 硬件安全设计应考虑纵深防御原则，即采用多层次的安全措施来保护系统[4]。这包括物理安全措施、硬件级安全机制和软件级安全措施等，以形成相互支持的防御体系。

3. 硬件安全设计应注重安全验证和测试。设计师应该通过严格的安全测试和验证流程来确保硬件安全设计的有效性和可靠性。这包括对硬件组件进行安全性评估和测试，以发现和修复潜在的安全漏洞，关系到对硬件的设计、制造和部署过程进行全面的审查，以确保硬件的安全性符合标准。

4. 硬件安全设计应考虑可更新性和可维护性。随着安全威胁的不断演变，硬件系统需要能够及时更新和修补安全漏洞。设计师应该设计硬件系统，使其能够轻松地更新固件和软件，以应对新的安全威胁。

二、电子系统中硬件安全防护技术与应用

（一）硬件安全防护技术概述

为了确保电子系统的安全，硬件安全防护技术扮演着至关重要的角色。这种技术通过多种物理和技术手段来保护硬件资源，防止未授权访问、数据篡改和破坏等安全威胁。加密技术对敏感数据进行加密处理，以防止在数据传输和存储过程中被非法获取和修改。认证技术则对用户身份进行严格验证，确保只有授权用户才能访问系统资源，从而防止未授权的使用和访问。

此外，防篡改技术通过物理或化学手段对硬件设备进行处理，增加其抗篡改和破坏的能力，保证硬件的完整性和可靠性。防电磁泄漏技术则通过屏蔽和滤波等方法，减少电磁泄漏的风险，防止敏感信息通过电磁波被外部窃取[5]。最后，安全启动技术确保在电子系统启动过程中，仅加载经过验证的软件和固件，有效防止恶意代码的运行，保障系统的安全启动和运行。

（二）硬件安全防护技术应用

硬件安全防护技术在各个领域中的应用至关重要，它为我们的日常生活和工业生产提供了稳固的安全保障[6]。在智能手机中，硬件安全防护技术如指纹识别、面部识别和加密存储等，广泛应用以保护用户的隐私和数据安全；电脑系统则利用 TPM（可信平台模块）安全启动和全盘加密等技术，有效防止未授权访问和数据泄露，确保用户信息的安全；在汽车领域，车载电子系统的安全同样至关重要，ECU（电子控制单元）加密、诊断接口保护和 CAN（控制器局域网络）总线安全等技术，保障了汽车电子系统的正常运行和驾驶安全；工业控制系统则依赖于 PLC（可编程逻辑控制器）安全、工业协议安全和设备认证等技术，以确保工业生产过程的稳定和安全。

物联网设备的普及也带来了新的安全挑战，硬件防火墙、安全存储和设备认证等技术的应用，保护了物联网设备免受恶意攻击，确保了数据传输的安全性[7]。这些技术的综合应用，不仅提升了设备本身的安全性，也为用户的数据和隐私提供了坚实的保护。

（三）硬件安全防护技术发展趋势

随着科技的飞速发展，硬件安全防护技术的趋势正朝着集成化、智能化、协同化和定制化的方向迈进[8]。半导体工艺的进步使得越来越多的安全功能能够被集成到硬件设备中，从而实现更高效的安全防护。同时，人工智能技术的应用使得硬件安全防护能够实现智能识别和响应，大幅提升安全防护效果。

此外，硬件安全防护技术将与软件安全防护技术相结合，形成一个全方位的安全防护体系。这种协同化的安全防护体系将能够更全面地应对各种安全威胁，确保电子系统的安全稳定运行[9]。同时，针对不同的应用场景和需求，定制化的硬件安全防护解决方案也将成为发展趋势。

三、硬件安全案例分析

（一）案例背景

某公司生产单相电子式电能表，在使用过程中发现部分电表在雷雨天气下会出现误计量的现象。经调查发现，这些电表没有经过电磁兼容性测试，导致在雷击产生的电磁脉冲干扰下，电表的计量芯片受到干扰，造成计量误差。

（二）案例分析

1. 问题原因

电表未能进行必要的电磁兼容性测试，因此缺少应对电磁脉冲干扰的防护措施。这可能是因为电表的电路设计存在不合理之处，导致其对电磁干扰的抑制能力不足。

2. 解决方案

为了确保电表在遭受电磁脉冲干扰时仍能正常工作，应当对电表进行全面的电磁兼容性测试。此外，还需要优化电表的电路设计，加入电磁干扰抑制电路。这可以通过采用屏蔽层来保护电路免受外部干扰，利用滤波电路来减少不必要的电磁辐射，以及通过接地线将干扰信号有效地引入大地，从而提高电表的抗干扰能力。

3. 改进效果

经过一系列的改进措施，电表的电磁兼容性得到了显著提升。即使在雷雨等恶劣天气条件下，电表也能正常工作，有效避免了因电磁干扰导致的误计量问题。这不仅提高了产品的可靠性，也增强了用户对公司的信任，从而提升了用户满意度。

（三）案例启示

硬件安全对于产品整体安全至关重要，因此必须给予充分的重视[10]。在产品设计阶段，就需要将电磁兼容性（EMC）问题纳入考虑范围，并实施相应的测试与优化措施。只有通过严格的电磁兼容性测试以及持续地改进工作，才能确保产品在复杂电磁环境中的安全性和可靠性。

结束语

硬件安全是构建安全可靠的电子系统的基石，面对日益复杂的威胁环境，需要我们不断探索和创新硬件安全防护技术，并将其融入到电子系统设计的各个环节。未来，硬件安全将朝着集成化、智能化、协同化和定制化的方向发展，不断探索新的防护技术，并将其与软件安全防护技术相结合，是构建更加完善的安全防护体系的必要途径。

参考文献

[1] 雷家鑫，裴晓飞. 旋变解码系统研究硬件阶段功能安全研究［J］. 汽车实用技术，2020,(09):80-83.DOI:10.16638/j.cnki.1671-7988.2020.09.026.

[2] 张茜歌，朱嘉诚，马俊，等. 基于故障传播模型的硬件安全性与可靠性验证方法［J］. 西北工业大学学报，2024,42(01):92-97.

[3] 李亚伟，章隆兵，王剑. 基于软硬件协同的细粒度安全域隔离机制［J］. 高技术通讯，2024,34(01):33-45.

[4] 章梁，舒强，姚雪平，等. 基于功能安全的 MOC-EPB 硬件设计［J］. 汽车零部件，2023,(09):53-57+62.DOI:10.19466/j.cnki.1674-1986.2023.09.011.

[5] 郑凯文. 基于机器学习的混合模式硬件木马检测［D］. 电子科技大学，2023.DOI:10.27005/d.cnki.gdzku.2023.005070.

[6] 陈嘉奇. 计算机网络中的硬件安全与维护策略［J］. 电子技术，2023,52(04):254-255.

[7] 靳国杰. CPU 硬件安全防护机制［J］. 保密科学技术，2022,(12):22-26.

[8] 杨彬彬. 基于阻变存储器的硬件安全技术研究［D］. 国防科技大学，2022.DOI:10.27052/d.cnki.gzjgu.2022.000104.

[9] 吴建华. 智能硬件终端安全加固技术研究［J］. 电脑知识与技术，2021,17(33):120-121.DOI:10.14004/j.cnki.ckt.2021.3345.

[10] 朱玉飞. 面向未来安全通信的核心硬件架构关键技术研究［D］. 国防科技大学，2021.DOI:10.27052/d.cnki.gzjgu.2021.000495.