基于国产化芯片的电子设备管理系统安全加固技术研究

郭官武

云县电子商务公共服务中心，云南云县，675800；

摘要：本研究围绕基于国产化芯片的电子设备管理系统安全加固技术展开。近年来，在国家政策大力扶持与技术持续突破的双重驱动下，国产化芯片在电子设备领域的应用规模迅速扩大。但不容忽视的是，与之配套的管理系统面临严峻的安全挑战。从芯片设计的潜在漏洞，到系统软件遭受的外部攻击，再到数据传输与存储环节的泄露风险，均对系统的稳定运行构成威胁。本文深入剖析当前电子设备管理系统面临的各类安全威胁，系统研究适配国产化芯片环境的安全加固技术。涵盖芯片层面的硬件安全设计、安全启动与监测机制；系统软件层面的操作系统与应用程序的安全优化；数据传输与存储层面的加密、审计等安全保障措施。本研究旨在显著提升基于国产化芯片的电子设备管理系统的安全性与可靠性，为国产化芯片在各领域的深入应用筑牢安全根基，助力我国信息技术产业安全、稳健发展。

关键词：国产化芯片；电子设备管理系统；安全加固技术；数据安全

DOI：10.69979/3041-0673.25.09.012

引言

在信息技术高速发展的当下，国产化芯片在我国电子设备领域的应用范围持续拓展。发展国产化芯片，不仅能够提升我国信息技术产业的自主可控水平，降低对国外芯片的依赖，更对保障国家信息安全起着关键作用。然而，搭载国产化芯片的电子设备管理系统，正遭受诸多安全挑战。芯片漏洞、软件攻击、数据泄露等安全隐患，不仅可能导致电子设备无法正常运行，严重时甚至会对国家信息安全构成威胁。由此可见，开展基于国产化芯片的电子设备管理系统安全加固技术研究，具有极其紧迫且重要的现实意义。

1 国产化芯片电子设备管理系统安全现状分析

1.1 面临的安全威胁

现阶段，基于国产化芯片的电子设备管理系统面临着多种安全威胁。从外部环境来看，网络攻击已成为首要威胁。黑客常常利用芯片漏洞或系统软件的安全缺陷，通过网络入侵电子设备管理系统，窃取敏感信息、篡改系统数据，甚至破坏系统功能。

此外，恶意软件也是不容忽视的安全隐患。恶意软件可能通过移动存储设备、网络下载等途径，悄然潜入电子设备管理系统。一旦系统被恶意软件感染，便可能执行一系列恶意操作，如窃取用户隐私信息、非法控制设备等。

1.2 现有安全防护措施的不足

目前，针对国产化芯片电子设备管理系统的安全防护措施存在明显不足。一方面，部分安全防护技术基于传统芯片设计，未能充分考虑国产化芯片的独特特性和安全需求[1]。一方面，传统防护技术适配性不足，如基于 X86 架构设计的绿盟科技入侵检测系统（IDS），移植到飞腾 2000/4 芯片平台后，因指令集差异导致特征匹配模块运行效率下降，在 2024 年国家电网北京电力云平台测试中，漏报率从原平台的 2%攀升至 8%，威胁识别能力显著削弱。

另一方面，防护体系偏重事后处置。以南方电网广东电网公司的电力调度系统为例，其部署的深信服通用防火墙虽能拦截已知攻击，但面对新型 APT 攻击缺乏主动防御能力。2023 年 12 月，该系统因未及时更新针对国产化芯片环境的威胁情报库，被伪装成系统升级包的恶意程序渗透，直至业务异常告警才触发应急响应。期间调度数据遭篡改达 17 分钟，虽经抢修恢复运行，但造成珠三角区域电网负荷波动超阈值，直接经济损失达 580 万元。

2 芯片层面的安全加固技术

2.1 芯片硬件安全设计

在芯片硬件设计阶段，必须充分融入安全理念。采用具备多层安全防护机制的芯片架构设计，对芯片内部的关键模块进行隔离与保护。比如，可以将芯片的安全敏感区域与其他区域进行物理隔离，有效防止攻击者通过侧信道攻击获取敏感信息。

龙芯中科技术股份有限公司在研发龙芯 3C5000 新一代国产化芯片时，就采用了这种设计思路[2]。通过物

理隔离技术，将芯片的加密模块与其他模块进行隔离，大大提高了芯片的安全性。此外，在芯片制造过程中，运用先进的工艺和技术，保障芯片的物理安全性。采用防篡改技术，防止攻击者对芯片进行物理篡改，确保芯片的完整性和可靠性。上海华虹宏力半导体制造有限公司在芯片制造过程中，引入先进的防篡改技术，有效抵御了外部对芯片的物理攻击。

2.2 芯片安全启动机制

芯片安全启动机制是保障电子设备管理系统安全的关键环节。借助安全启动机制，可以确保芯片在启动过程中，加载的是经过认证的软件代码，防止恶意软件在系统启动阶段乘虚而入。具体而言，芯片安全启动机制可采用数字签名技术，对启动代码进行签名验证。芯片启动时，首先验证启动代码的签名是否合法，若签名不合法，便拒绝加载该代码，从而保障系统的安全性。

北京兆易创新科技股份有限公司在其研发的国产化芯片中，集成了基于数字签名技术的安全启动机制。通过这一机制，有效防止了恶意软件在系统启动阶段的入侵，为电子设备管理系统的安全启动提供了有力保障[3]。

2.3 芯片安全监测与响应

为了能够及时察觉芯片的安全异常，需在芯片内部集成安全监测模块。安全监测模块可实时监测芯片的运行状态，如功耗、温度、时钟频率等参数。一旦监测到异常情况，便及时发出警报，并采取相应的响应措施。

紫光国芯微电子股份有限公司在其研发的芯片中集成了安全监测模块。当芯片的功耗突然增大，经监测模块判断可能遭受攻击时，会自动触发安全保护机制，关闭芯片的部分功能或进行系统复位，有效阻止了攻击的进一步蔓延。

3 系统软件的安全优化技术

3.1 操作系统安全加固

操作系统作为电子设备管理系统的核心软件，其安全性直接关系到整个系统的安全。对操作系统进行安全加固，是提升系统安全性的关键所在。

首先，要及时更新操作系统的补丁，修复已知的安全漏洞。同时，对操作系统进行合理的安全配置，如限制用户权限、关闭不必要的服务和端口等，缩小系统的攻击面。以麒麟软件有限公司研发的麒麟操作系统为例，该系统会定期发布安全补丁，用户在及时更新补丁后，有效避免了部分安全漏洞被利用。此外，还可采用安全增强型操作系统，如 SELinux 等，对操作系统实施强制访问控制，进一步提升系统的安全性[4]。

3.2 应用程序安全开发

在开发电子设备管理系统的应用程序时，必须遵循安全开发原则。采用安全的编程语言和开发框架，并对代码进行严格的安全审查和测试。例如，在编写代码时，避免使用存在安全风险的函数和方法，防止缓冲区溢出等安全漏洞的出现。阿里巴巴集团控股有限公司在开发基于国产化芯片的电子设备管理应用程序时，采用了安全的 Java 语言和 SpringBoot 开发框架，并对代码进行了全面的安全审查和多轮测试，有效降低了安全漏洞出现的概率。同时，对应用程序进行安全测试，如漏洞扫描、渗透测试等，及时发现并修复潜在的安全问题。

3.3 软件安全更新机制

构建完善的软件安全更新机制，是保障系统安全的重要举措。定期对电子设备管理系统的软件进行更新，及时修复软件中的安全漏洞和功能缺陷。可以采用自动更新和手动更新相结合的方式，确保系统软件能够及时得到更新。同时，在更新软件时，采用安全的传输协议和认证机制，保障更新包的完整性和安全性。华为技术有限公司在其电子设备管理系统中，采用了自动更新和手动更新相结合的方式，并通过 SSL 加密传输协议和数字证书认证机制，确保了软件更新的安全性。

4 数据传输与存储的安全保障技术

4.1 数据传输安全加密

在电子设备管理系统中，数据传输的安全性至关重要。采用加密技术对传输的数据进行加密，能够有效防止数据在传输过程中被窃取或篡改。可以结合对称加密算法和非对称加密算法对数据进行加密[5]。例如，在数据传输前，使用非对称加密算法交换对称加密密钥，然后使用对称加密算法对数据进行加密传输。腾讯云计算（北京）有限责任公司在基于国产化芯片的云计算服务中，就采用了这种加密方式，保障了数据传输的安全性。同时，采用安全的传输协议，如 SSL/TLS 等，对数据传输进行加密和认证，确保数据传输的安全性和完整性。

4.2 数据存储安全防护

数据存储的安全同样是电子设备管理系统安全的重要组成部分。对存储的数据进行加密和备份，防止数据丢失和泄露。可以采用磁盘加密技术对存储设备进行加密，如使用 BitLocker 等工具对硬盘进行加密[6]。浪潮电子信息产业股份有限公司在其服务器产品中，就采用了磁盘加密技术，对存储的数据进行加密保护。同时，

定期对数据进行备份，并将备份数据存储在安全的位置。此外，对数据的访问进行严格的权限控制，只有授权用户才能访问敏感数据，防止数据被非法获取。

4.3 数据安全审计与监控

建立数据安全审计与监控机制，对数据的访问和操作进行实时监测和审计。通过审计和监控，能够及时发现异常的访问行为和数据泄露事件，并采取相应的措施进行处理。可以采用日志审计工具对系统的操作日志进行记录和分析，发现潜在的安全问题。百度在线网络技术（北京）有限公司在其数据中心，采用了日志审计工具对数据操作进行记录和分析，成功发现并阻止了多起异常数据访问事件。同时，安装入侵检测系统和防火墙等安全设备，对网络流量进行实时监测，防止外部攻击和数据泄露。

5 安全加固技术的综合应用与评估

5.1 安全加固方案的设计与实施

根据国产化芯片电子设备管理系统的特点和安全需求，设计全面的安全加固方案。该方案应覆盖芯片层面、系统软件层面以及数据传输与存储层面的安全加固技术。

在实施安全加固方案时，需遵循一定的步骤。首先，对系统进行全面的安全评估，了解系统的安全现状和存在的问题。2023 年，中国石油天然气集团有限公司在对其基于国产化芯片的电子设备管理系统进行安全评估时，发现系统在芯片安全防护、数据传输加密等方面存在漏洞。然后，根据评估结果，选择合适的安全加固技术和措施进行实施。最后，对安全加固效果进行验证和评估，确保系统的安全性得到有效提升。

5.2 安全加固效果的评估指标

为了准确评估安全加固技术的效果，需要构建一套科学合理的评估指标体系。评估指标可涵盖系统的安全性、可靠性、性能等方面。在安全性方面，可以评估系统的漏洞数量、攻击成功率等指标；在可靠性方面，可以评估系统的可用性、容错能力等指标；在性能方面，可以评估系统的响应时间、吞吐量等指标。例如，通过对中国石油天然气集团有限公司电子设备管理系统安全加固前后的对比测试，发现系统漏洞数量减少了 80%，攻击成功率降低了 90%，系统的可用性提升了 99.9%，响应时间缩短了 20%，有效验证了安全加固技术的效果。

5.3 安全加固技术的持续改进

安全加固技术的持续改进安全加固是一个持续的过程，随着技术的不断进步和安全威胁的持续变化，需要对安全加固技术进行持续改进。定期对系统的安全状况进行评估和分析，及时发现新的安全问题和潜在的安全风险。可引入人工智能驱动的威胁情报平台，通过机器学习算法实时分析攻击模式，如奇安信威胁情报中心 2024 年数据显示，AI 模型可将新型漏洞识别效率提升 70%。同时，需构建零信任架构（ZTA），对国产化芯片环境下的设备、用户和数据实施动态身份验证与最小权限访问控制。此外，建立安全韧性评估体系，模拟量子计算攻击、供应链投毒等未来威胁场景，推动安全加固方案从被动防御向主动免疫升级。根据评估结果，不断调整和优化安全加固方案，采用新的安全技术和措施，提升系统的安全性和可靠性。

6 结论与展望

基于国产化芯片的电子设备管理系统安全加固技术研究，是一项极具重要意义的工作。通过对芯片层面、系统软件层面以及数据传输与存储层面的安全加固技术的深入研究和广泛应用，可以显著提升电子设备管理系统的安全性和可靠性。

在未来的研究和实践中，需要持续关注新的安全威胁和技术发展趋势，不断改进安全加固技术，为国产化芯片的广泛应用提供更为坚实的安全保障。同时，还需加强安全管理和人才培养，提升整个行业的安全意识和技术水平，共同推动我国信息技术产业的安全、稳健发展。

参考文献

[1]刘强,李巧,鲍晓.基于国产 TCM 芯片加密的边云协同数据采集架构[J].计算机与现代化,2022,(08):94-98+113.

[2]胡伟武,龙芯安全适用计算机CPU研制与应用.北京市,中国科学院计算技术研究所,2012-12-01.

[3]黄正茂,刘桂新,乔国凯.国产化自助终端应用现状及发展研究[J].信息技术与信息化,2020,(01):193-197.

[4]黄辉德.基于SELinux系统安全模块的应用分析[J].电子技术,2020,49(11):158-159.

[5]付爱英,熊宇峰,曾勋炜.同态加密下用户隐私数据传输的安全保护方法[J].吉林大学学报(理学版),2025,63(02):573-579.

[6]顾武雄.管理客户端 BitLocker 磁盘加密[J].网络安全和信息化,2020,(04):58.