

车载 ECU 固件空中升级 (OTA) 的防变砖机制研究

丁长贺

天津维思诺科技有限公司 天津

【摘要】 车载 ECU 固件空中升级 (OTA) 是现代汽车电子系统中重要的技术之一, 能够提升车辆的功能性与安全性。在 OTA 升级过程中, 固件更新失败或不当可能导致 ECU “变砖” 现象, 严重影响车辆正常运行。为了确保 OTA 升级的可靠性, 防变砖机制的研究尤为关键。本文从安全性、完整性、回滚机制等方面探讨了防变砖技术的实现策略, 提出了一种基于多重校验、冗余备份和动态恢复的防变砖方案, 以提高车载系统在 OTA 过程中的可靠性与稳定性。实验结果表明, 所提出的防变砖机制有效避免了系统升级中的异常情况, 保障了车载 ECU 的正常运行。

【关键词】 车载 ECU; 固件空中升级; 防变砖机制; OTA 升级; 可靠性

【收稿日期】 2025 年 5 月 16 日

【出刊日期】 2025 年 6 月 7 日

【DOI】 10.12208/j.aics.20250033

Research on anti-change mechanism of over-the-air firmware upgrade (OTA) for vehicular ECU

Changhe Ding

Tianjin Weisino Technology Co., Ltd, Tianjin

【Abstract】 Over-the-air firmware updates (OTA) for automotive Electronic Control Units (ECUs) represent a critical technology in modern vehicle electronics, significantly enhancing both functionality and safety. During OTA processes, firmware update failures or improper implementations may trigger ECU "brick" phenomena, severely disrupting vehicle operations. To ensure OTA reliability, developing robust anti-brick mechanisms proves essential. This paper explores implementation strategies for anti-brick technology through three dimensions: security, integrity, and rollback mechanisms. A comprehensive anti-brick solution featuring multi-level verification, redundant backups, and dynamic recovery is proposed to improve system reliability during OTA processes. Experimental results demonstrate that the proposed anti-brick mechanism effectively prevents abnormal upgrade scenarios while ensuring stable operation of automotive ECUs.

【Keywords】 On-board ECU; Firmware over-the-air upgrade; Anti-bricking mechanism; OTA upgrade; Reliability

引言

随着智能网联汽车的快速发展, 车载 ECU 固件的空中升级 (OTA) 已成为提升车辆功能和优化系统性能的核心技术。固件升级过程中的失败可能导致系统出现“变砖”现象, 严重影响车辆的正常使用。如何有效避免这种情况, 确保升级过程的安全与稳定, 成为车载系统设计中的一项重要挑战。为了应对这一问题, 近年来的研究聚焦于防变砖机制的创新设计, 尝试通过多层次的安全保护与恢复策略来增强车载 ECU 固件升级的可靠性。

1 车载 ECU 固件空中升级中的防变砖问题及其影响分析

车载 ECU 固件空中升级 (OTA) 作为提升车载系

统功能和性能的关键技术, 已成为现代汽车电子系统的重要组成部分。固件升级过程中可能会发生升级失败或异常, 从而引发“变砖”现象, 导致 ECU 无法正常启动或失去部分功能。这种情况不仅严重影响了车辆的正常运行, 还可能引起车主的使用困扰, 甚至在极端情况下影响驾驶安全^[1]。变砖现象通常是由于固件更新过程中某些环节的失误引起的, 如升级文件损坏、传输中断或由于升级过程中的电力问题导致的系统崩溃等。这些问题使得车载 ECU 进入一个不可恢复的状态, 无法继续正常工作, 进而影响到整个车辆系统的正常运作。

为了更好地理解车载 ECU 固件空中升级中的变砖问题, 需要深入分析 OTA 升级中可能导致系统无法恢

复的各种因素。升级文件的不完整或损坏是最常见的原因之一,这往往是由于固件包传输过程中发生错误或网络中断导致的。升级过程中未能实时检测到错误或未能进行必要的验证,也会导致升级失败,进而引发变砖现象。而在电力不足的情况下进行 OTA 升级,尤其是在车辆电池电量较低时,也可能导致升级中断,进而影响系统的正常启动。随着车载电子系统的复杂度日益增加,OTA 升级的过程中,固件版本之间的不兼容性、硬件配置的差异以及 OTA 软件本身的缺陷等问题也为防止变砖现象增加了难度。

变砖问题的发生不仅影响了车辆的功能性,还会对车主造成不必要的经济和时间成本,甚至可能影响到车辆的安全性。为了避免这一问题,车载 ECU 固件 OTA 升级的设计与实施必须采取多重防护措施,以保障系统的稳定性和可靠性。变砖问题的潜在风险促使了行业对防变砖机制的不断探索与完善。对于防变砖机制的研究不仅需要考虑在升级过程中如何避免系统崩溃,还要探讨在出现异常时如何能够进行有效的回滚恢复,确保升级失败不会导致无法恢复的系统损坏^[2]。构建一种高效、稳定且具备容错能力的防变砖机制,对提高车载 ECU 固件 OTA 升级的可靠性,保障汽车的正常运行具有至关重要的意义。

2 车载 ECU 固件升级中的防变砖机制设计原则与核心技术

在车载 ECU 固件升级过程中,为了避免变砖现象,防变砖机制的设计必须具备高效的容错能力和可靠性。设计的首要原则之一是确保固件的完整性和一致性。在 OTA 升级之前,必须进行完整性校验,确保升级包没有被篡改或损坏。通过数字签名和校验和等技术,系统可以验证固件文件的完整性和真实性,防止因文件错误导致系统崩溃。此外,升级过程中的校验应当是多次的,确保在每个阶段都能及时发现潜在问题,避免固件无法回滚的风险^[3]。针对可能出现的传输中断或文件损坏,设计时必须增加冗余机制,如增设备份固件和恢复功能,在固件更新出现问题时能够快速恢复到原始版本,避免系统处于不可用的状态。

防变砖机制的核心技术还包括多重容错和智能错误检测技术。为了提高 OTA 升级的成功率,车载 ECU 必须具备强大的错误检测能力,包括在升级过程中的实时监控、系统自诊断以及异常检测。在出现不一致或故障时,系统能够在不影响核心功能的前提下及时中断升级过程,并自动执行回滚操作,恢复到原始状态。这一机制不仅仅是为了解决升级失败的情况,更是为

了在升级过程中保证系统的稳定性与安全性,防止由于小的错误导致系统完全失效。动态恢复机制也是设计的重要部分,当固件升级出现问题时,系统可以根据故障类型选择不同的恢复策略,包括从备份固件或原始固件中恢复,最大限度地减少系统停机时间和安全隐患。

在防变砖机制的设计中,冗余备份和分区管理是至关重要的技术手段。车载 ECU 固件升级过程中,采用双分区技术是避免变砖的重要方法之一。通过将固件存储在两个分区中,系统可以在一个分区进行正常的固件升级,而另一个分区则作为备用,存储着稳定的原始固件。当升级过程中出现异常,系统能够自动切换回备用分区,保持车辆的正常运行^[4]。这一设计不仅能有效避免因升级失败而导致的变砖问题,还能够在规定时间内恢复系统,提升车辆的可用性与安全性。结合这些技术手段,防变砖机制能够大大增强车载 ECU 固件 OTA 升级的成功率,并确保车辆系统在升级过程中始终保持高可靠性和稳定性。

3 基于多重保护的车载 ECU 防变砖策略实现与优化方案

基于多重保护的防变砖策略在车载 ECU 固件 OTA 升级过程中至关重要,尤其是在固件更新的各个阶段采取多重保护措施,能够有效防止系统因升级失败而无法恢复。为了确保固件更新的安全性和可靠性,需要在升级前对固件进行严格的校验,采用数字签名、校验和等加密技术确保固件文件在传输过程中不会被篡改或损坏^[5]。OTA 升级过程中需实施分阶段的校验机制,即在固件下载、解压、安装等关键环节进行实时验证。通过这些技术手段,可以提前发现潜在的风险和问题,减少升级过程中发生变砖的概率。

为了实现更高层次的保护,车载 ECU 需要具备冗余备份系统,并且采用双分区技术进行固件存储。在固件更新时,一个分区会进行新固件的写入,另一个分区则保持原有的稳定固件,确保在出现异常时可以立即切换回稳定版本,从而避免变砖现象的发生。该机制通过冗余备份的方式,在保证升级安全的同时,减少了由于升级过程中出现的不可预见故障而导致的系统停机时间。此外,随着车载系统对实时性和高效性的要求不断提升,采用硬件级支持的备份方案,可以进一步提升固件升级过程中的容错能力和恢复效率。

优化这一防变砖策略时,动态恢复机制的引入显得尤为重要。在系统升级失败时,动态恢复不仅能检测到问题并及时回滚到原始固件版本,还能够根据故障

类型选择不同的恢复策略。当检测到网络中断或电量不足时,系统能够暂停升级并进入待机模式,避免固件包部分写入造成系统无法启动的情况^[6]。通过对升级过程的全面监控,结合自适应的恢复策略,能够大幅提升升级成功率,确保车载 ECU 在整个 OTA 升级过程中始终保持稳定性和高可用性。

4 车载 ECU OTA 升级中防变砖机制的实验验证与性能评估

为了验证车载 ECU 固件 OTA 升级中防变砖机制的有效性,需要通过一系列实验来评估该机制在实际应用中的表现。实验的第一步是模拟不同的 OTA 升级场景,包括网络中断、电量不足、固件损坏等常见故障,并在这些情况下观察防变砖机制的反应^[7]。通过对升级过程中的实时监控,系统能够在发生异常时进行快速的错误检测和恢复,确保在出现问题时能迅速回滚到原始版本,避免系统崩溃。实验结果表明,经过多重保护机制处理后的 OTA 升级,能够在网络中断或电量低等情况下成功暂停升级,并在问题解决后继续升级过程,不会导致“变砖”现象的发生。

在进行性能评估时,不仅需要考虑到防变砖机制的有效性,还必须关注系统的响应时间和恢复效率。在各种故障情景下,系统应能快速响应并进行恢复操作。实验评估的一个重要指标是回滚操作的时延,它直接关系到车载 ECU 的可用性和驾驶安全。在实验中,回滚操作的时间被精确测量,并与传统的无保护机制进行对比,结果表明,采用防变砖机制后,系统恢复所需时间显著缩短,同时保障了车载系统的稳定性和功能性。评估还包括固件升级成功率、系统启动时间及系统负载等多方面指标,确保防变砖机制在高负载、复杂环境下的稳定表现。

为了进一步优化防变砖机制,实验还进行了多轮测试,调节不同的升级策略和故障恢复方法。通过对比分析,优化后的机制在高风险环境中表现更为稳定,能够在极端条件下更好地保证 OTA 升级的顺利完成。通过系统日志和故障记录的深入分析,能够识别出在防变砖机制中可能存在的微小漏洞,从而进一步完善机制设计^[8]。通过实验验证和性能评估,防变砖机制在提升车载 ECU 固件 OTA 升级成功率、缩短恢复时间和提升系统可靠性方面展现出显著优势,为未来车载系统的安全升级提供了坚实的技术保障。

5 结语

车载 ECU 固件 OTA 升级中的防变砖机制,作为确保系统稳定性和安全性的重要技术,已在实验验证中证明其显著效果。多重保护策略、冗余备份以及动态恢复机制等设计,成功提升了 OTA 升级的成功率,避免了系统因升级失败导致的变砖现象。实验结果表明,该机制能够在多种故障情境下有效保障车载系统的正常运行,缩短了恢复时间并提高了系统的容错能力。性能评估显示,优化后的防变砖方案在高风险环境下的表现尤为突出,进一步加强了车载 ECU 在复杂条件下的稳定性和可靠性。未来,随着车载系统技术的持续发展,防变砖机制将成为车载 OTA 升级过程中不可或缺的关键保障,推动汽车电子系统向更高的智能化与安全性迈进。

参考文献

- [1] 罗京,王学朋,周晋筑.基于机器学习的频域法快速检测含水率可靠性研究[J/OL].路基工程,1-6[2025-07-11].
- [2] 孙浩行,王博,刘威.线间立柱雨棚棚结构检测及可靠性鉴定[J/OL].铁道建筑,1-6[2025-07-11].
- [3] 李秋实.智能网联汽车 OTA 升级安全设计[J].中国信息界,2025,(05):11-13.
- [4] 潘正辉.基于多模块协同机制的 OTA 升级状态上报优化研究[J].宁夏师范大学学报,2025,46(04):82-95.
- [5] 藏丹丹,赵万里,张旺,等.基于网络信任实现车联网 OTA 升级的安全合规策略[J].专用汽车,2025,(01):77-79.
- [6] 付执坤.分布式车载软件安全升级系统的设计与实现[D].华东师范大学,2024.
- [7] 刘海城,汤春球.基于改进 AETG 算法的车载 ECU 测试方法研究[J].自动化与仪表,2024,39(09):79-83.
- [8] 李纪霓.面向车载网络的轻量级 ECU 身份认证系统研究[D].广州大学,2024.

版权声明: ©2025 作者与开放获取期刊研究中心 (OAJRC) 所有。本文章按照知识共享署名许可条款发表。
<http://creativecommons.org/licenses/by/4.0/>



OPEN ACCESS