基于单片系统控制器的A/B系统升级技术研究

周恒　刘禹池　孔祥明　周时莹　于诗洋　刘禹宏

（中国第一汽车股份有限公司研发总院，长春 130013）

【摘要】针对空中下载（OTA）升级失败时单片系统（SoC）电子控制单元（ECU）无法进行软件回滚的问题，提出了一种A/B系统升级技术，通过读取ECU中杂项（MISC）分区信息，将程序下载至备份分区，并通过设计A/B系统的优先级来选择激活分区，进行安装启动或安装失败时软件回滚，同时，设计了A/B系统的差分升级技术。经搭建系统测试，采用该技术的控制器在升级失败后可进行软件回滚，验证了回滚技术的可行性、有效性及稳定性。

关键词：空中下载　MISC分区　A/B系统　软件回滚　差分升级

中图分类号：U461　　**文献标志码：**A　　**DOI：** 10.20104/j.cnki.1674-6546.20230204

Research on Upgrading Technology of A/B System Based on Vehicle SoC Controller

Zhou Heng, Liu Yuchi, Kong Xiangming, Zhou Shiying, Yu Shiyang, Liu Yuhong

(Global R&D Center, China FAW Corporation Limited, Changchun 130013)

【Abstract】 The A/B system upgrading technology is proposed to solve the problem that the System on Chip (SoC) Electronic Control Unit (ECU) cannot roll back the software when the Over-The-Air (OTA) upgrading failed. The technology downloads the program to the backup slot by reading the MISC of ECU slot information, and starts the installation by designing the priority level of the A/B system to select the active partition or rolls back the software in case of upgrading failed. At the same time, the differential graded technology of A/B system is designed. The ECU using this technology can perform software rollback when upgrading fails ,and the feasibility, effectiveness and stability of rolling back software technology are verified by building a test environment.

Key words: Over-The-Air (OTA), MISC Slot, A/B system, Software rolling back, Differential graded

【引用格式】 周恒，刘禹池，孔祥明，等. 基于单片系统控制器的A/B系统升级技术研究[J]. 汽车工程师，2024(11)：1-6.

ZHOU H, LIU YC , KONG X M, et al. Research on Upgrading Technology of A/B System Based on Vehicle SOC Controller[J].Automotive Engineer, 2024(11): 1-6.

1　前言

伴随着汽车的智能化和网联化发展，整车搭载的控制器数量与日俱增，车载软件更加复杂、迭代速度更快，传统的线下更新或维修的成本及管理难度越来越高，因此，整车制造商通过无线网络对汽车控制器进行下载更新的需求愈发强烈，空中下载（Over-The-Air，OTA）功能成为车载软件更新的必然趋势[1-3]。

目前常见的OTA升级架构是云端服务器端通过车载通信终端（Telematics BOX，T-BOX）将升级包下载至网关，由网关对网络架构中的以太网节点和控制器局域网络（Controller Area Network，CAN）节点的控制器进行升级[4-5]。陈祖锐等[6]提出将升级程序直接刷写在应用程序分区中的升级技术，其局限性在于，应用程序升级失败后，原分区中的程序已被擦除，控制器将始终处于引导加载程序（Bootloader）中无法正常工作。陶媛媛等[7]针对以太网控制器采用备份区设计方案，程序升级失败回滚时，备份区程序将被复制到正常区域运行，程序复制过程导致升级时间较长。严娟等[8]针对网关自升级，将闪存（Flash）分为两个功能完全相同且互为备

份的区域，升级时只针对其中一个区域进行升级，升级失败则利用另一个区域进行回滚，但并未说明具体的升级流程及差分升级技术。

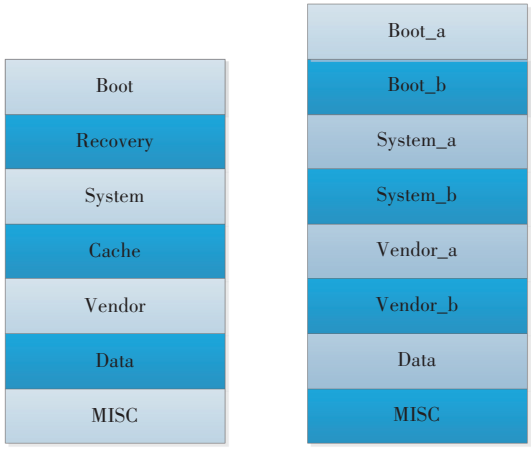
本文提出一种A/B系统升级技术：针对分区管理问题，设计杂项（Miscellaneous，MISC）分区记录A/B系统的属性信息，升级时选择对应的系统分区进行刷写升级，并设计系统属性信息的优先级；重新设计升级包下载、安装启动及失败回滚程序，优化差分升级时升级包还原与A/B系统刷写间的关系。

2 A/B系统控制器分区

2.1 硬件存储分区

传统控制器只有一套分区存储当前执行的系统，而A/B系统控制器一般有两套分区（Slot A和Slot B）[9]，激活分区（Active Slot）存放当前执行的系统，备份分区（Backup Slot）存放回滚备用的系统，两套系统可以独立工作（用户数据只有一份，为两套系统共用）。其中，Slot是A/B系统的一个逻辑概念，同一存储设备上处于同一个系统的分区集合称为Slot。

传统控制器与A/B系统控制器在存储空间上的区别如图1所示，各分区具体功能如表1、表2所示。



（a）传统控制器分区　　（b）A/B系统控制器分区

图1　控制器存储空间对比

表1　传统控制器分区及功能

分区名	功能
引导（Boot）	存放内核（Kernel）和内存盘（Ramdisk）
恢复（Recovery）	存放Recovery系统的Kernel和Ramdisk
系统（System）	存放平台的进程和库文件
缓存（Cache）	存放缓存文件和数据
开发厂商（Vendor）	存放开发厂商定制的应用和库文件
数据（Data）	用户数据分区
杂项（MISC）	系统与Recovery、Bootloader通信数据

表2　A/B系统控制器分区及功能

分区名	功能
Boot_a/Boot_b	存放Kernel和Ramdisk
System_a/System_b	存放应用程序和库文件
Vendor_a/Vendor_b	存放定制应用和库文件
Data	用户数据分区
MISC	存放A/B系统关键信息

2.2 升级方式

单片系统（System on Chip，SoC）控制器包含一个主系统、一个Recovery系统，升级时将数据包下载到Cache分区，下载完成后向MISC分区写入指令，表明下次启动时进入Recover模式并使用该升级包进行升级，重启Bootloader读取指令后进入Recovery系统，使用下载的数据包更新主系统并重新启动。激活（active）属性选择激活分区运行，收到升级任务时，将数据包直接下载到备份分区安装，更新启动信息（Slot_Info）属性，控制器重启后对本次升级的数据包进行校验，校验通过后，运行新程序完成升级。

2.3 MISC分区定义

A/B系统存在两套系统分区，控制器启动时Bootloader需读取MISC分区中的Slot_Info，识别激活分区并引导启动应用程序，此启动信息将在应用程序的升级包验证、下载刷新及软件回滚时进行必要的更新。MISC分区属性信息结构如图2所示，各属性信息功能如表3、表4所示。

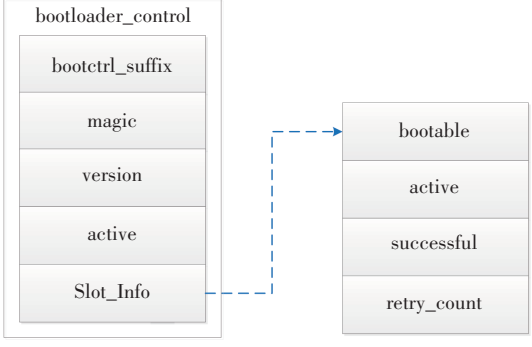


图2　MISC分区属性信息结构

表3　bootloader_control结构说明

内容	功能
引导控制后缀（bootctrl_suffix）	当前系统字符串标记位
魔术字（magic）	标识引导加载程序控制（bootloader_control）类型
版本（version）	引导信息（BootInfo）版本号
激活（active）	Slot_Info中为active的Slot号
启动信息（Slot_Info）	Slot属性信息

表4　Slot_Info结构说明

内容	功能
可引导(bootable)	表示当前分区是否包含正确引导程序
激活(active)	表示当前分区为首选的启动引导
成功引导(successful)	标记当前分区是否已正确引导系统启动
重试次数(retry_count)	最大尝试次数

3　关键技术

3.1　GPT分区及属性

全局唯一标识分区表(GUID Partition Table，GPT)[10]将用户数据区域(User Data Area)的存储介质划分为多个区域，即系统分区(SW Partitions)，并通过分区表(Partition Table)对系统分区进行维护。在分区表中，每个条目保存一个系统分区的起始地址、大小等属性信息，通过读取系统分区能获取分区信息，进而对分区进行升级操作或属性修改。本文采用嵌入式多媒体卡(embedded Multi Media Card，eMMC)存储器的GPT分区，其结构如图3所示。

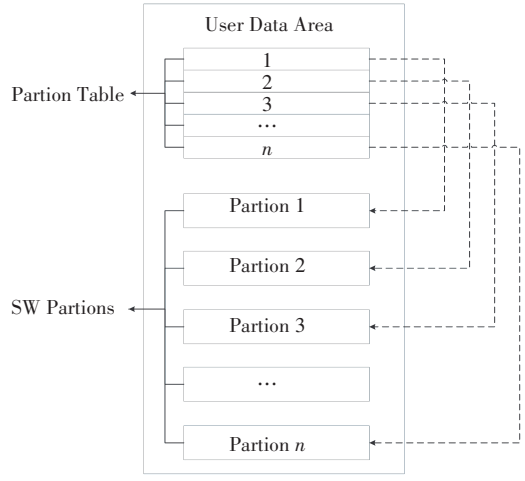


图3　eMMC存储器分区结构

3.2　差分升级

差分升级(即增量更新)[11]通过将数据文件的旧版本与新版本进行差分，得到升级部分的补丁，即差分包；用户下载差分包后，系统利用差分算法将旧版本数据与差分包进行组合，得到新版本的数据文件对目标分区进行升级，差分升级原理如图4所示。

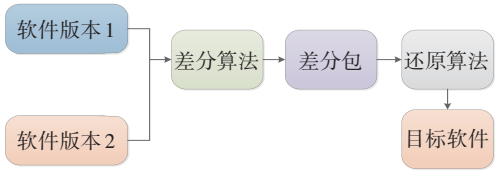


图4　差分升级原理

4　A/B系统升级技术

4.1　刷写流程

程序下载刷写过程中，Bootloader会通过读取MISC分区中的Slot_Info属性判断Slot A和Slot B是否具备active属性，若具备则定位到active属性的Slot设置successful属性，若均不具备，则设置Slot A为acitve属性，retry_count=3。然后利用升级包对备份分区进行升级，设置Slot_Info属性，将A/B系统属性中active属性进行交换，完成升级包刷写。升级包下载刷写流程如图5所示，刷写过程中的Slot_Info变化如图6所示。

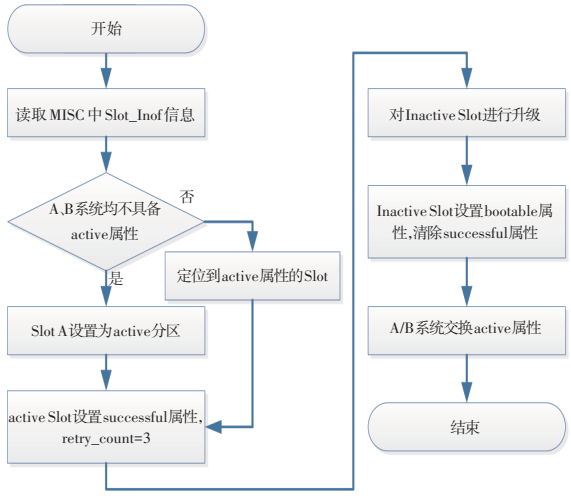


图5　A/B系统升级包下载刷写流程

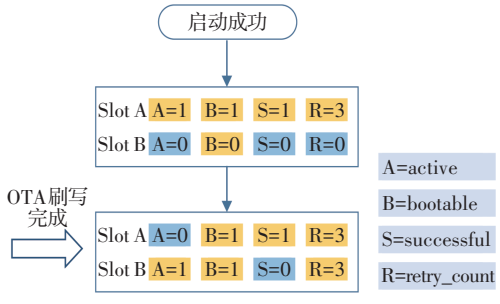


图6　A/B系统下载刷写阶段Slot_Info属性变化

4.2　升级启动流程

升级包刷写完成重启时，Bootloader会通过GPT分区读取MISC分区中的Slot_Info属性，选择优先级高的分区加载启动，启动流程如图7所示，定义启动优先级由高到低如表5所示。如果激活分区和备份分区的优先级一致，默认将Slot A设定为active且设retry_count=3后启动。控制器启动成功后，Bootloader修改Slot_Info中的successful属性信息，属性变化如图8所示。一旦升级成功(刷写和验证均成功)，不允许回滚。

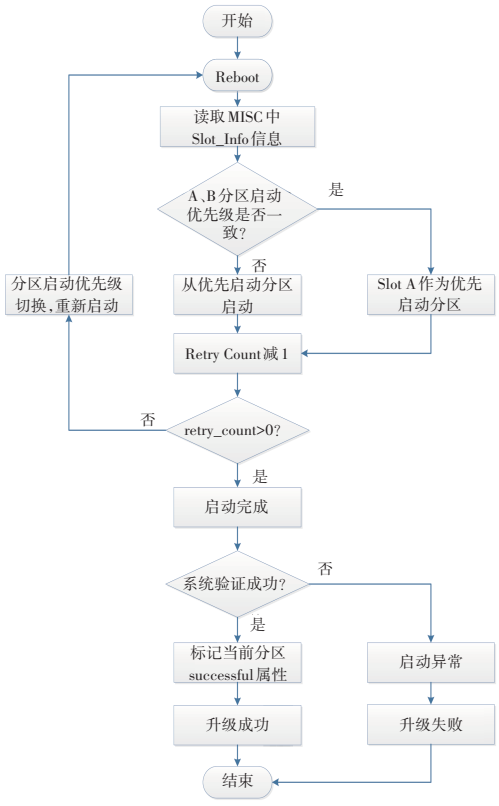


图7　A/B系统启动流程

表5　A/B系统启动优先级

优先级	内容
1	具备active & bootable & successful属性的Slot
2	具备active & bootable & retry_count>0属性的Slot
3	具备bootable & successful属性的Slot
4	具备bootable属性的Slot

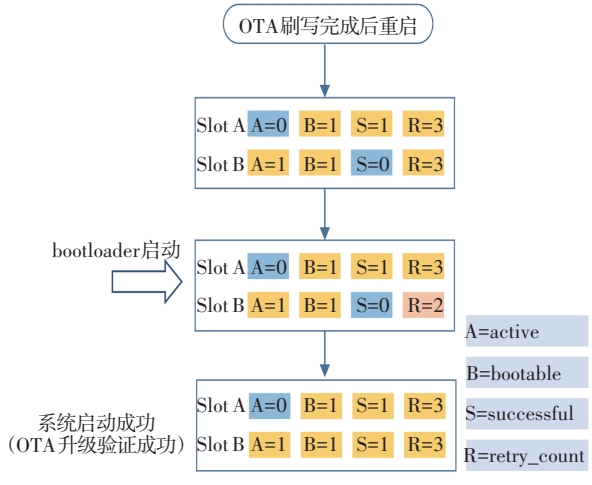


图8　A/B系统升级成功后Slot属性变化

若初次启动失败，控制器会再次尝试启动程序，当尝试次数达到最大时执行软件回滚，A/B系统执行分区切换启动，其Slot_Info属性变化如图9所示。

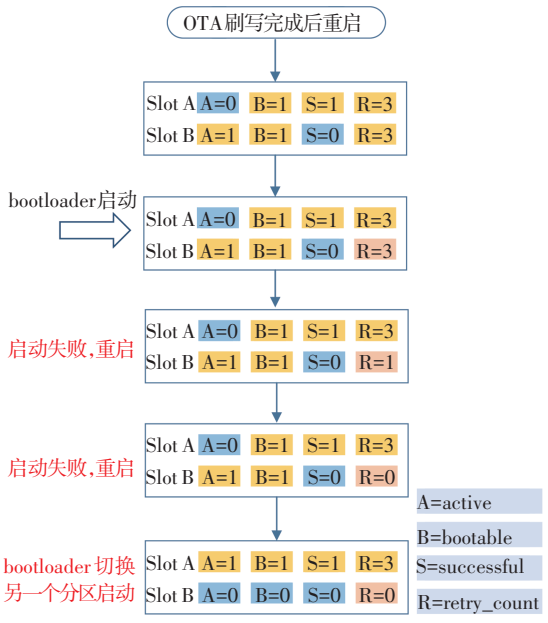


图9　A/B系统回滚时Slot属性变化

4.3　A/B系统差分升级

A/B系统的差分升级使用当前分区作为原始文件，不需要额外的存储空间保存原始包，加快了升级过程，但需确保当前分区在运行期间未被修改过。在还原数据时，将差分的镜像（image）按块还原后直接写入备份分区，再计算哈希（Hash）值判断合法性，其升级流程如图10所示。

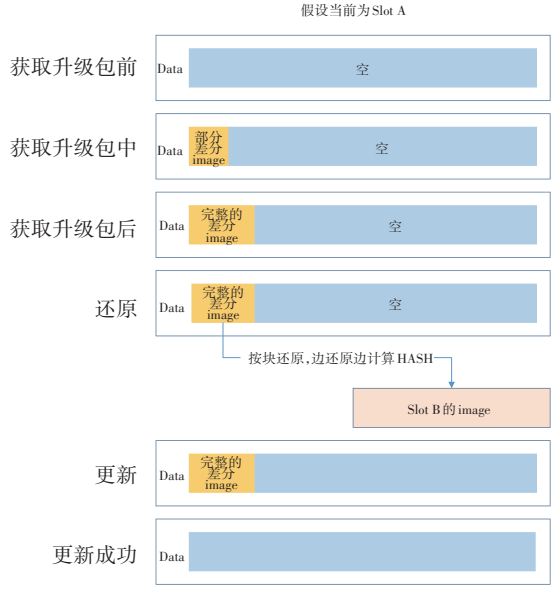


图10　A/B系统差分升级流程

5　开发测试与验证

5.1　测试系统

A/B系统升级技术测试环境主要分为微处理器单元（Micro Processor Unit，MPU）系统和上位机

诊断系统,系统测试框图及设备分别如图11、图12所示。更新模块(Updater)属于用户层(UserSpace),与上位机进行交互,中间软件层(Middleware)包括引导控制模块(BootCtrl)、刷写模块(Flush)、供电模块(Power),内核层(KnernelSpcae)的eMMC驱动(eMMC Driver)用于加载升级时的内存信息,eMMC包含A/B系统分区相关信息,两个系统之间通过以太网口通信,上位机诊断系统可以触发获取当前MPU的版本号、传输升级包、进行升级等动作。

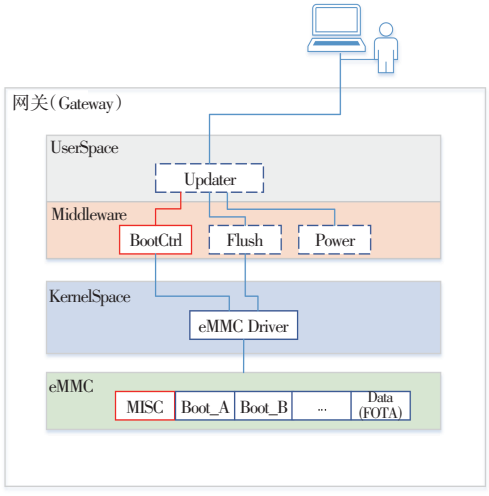


图11 A/B系统升级测试框图

图12 A/B系统升级测试实物图

5.2 存储空间配置

本文以IMX8X的eMMC内存为例介绍存储空间的分区,其分区结构如表6所示。

5.3 测试方案设计

针对A/B系统与传统系统升级技术的差异点,设计测试时,需重点考虑升级异常条件下程序回滚功能有效性、A/B系统双分区运行稳定性及差分升级稳定性等,测试类型分为正常系和异常系。

测试时,首先通过搭建的测试系统验证单控制器升级回滚情况,测试通过后,将已开发的A/B系统控制器安装到实车上,并利用已上线运营的OTA整套升级系统布置多控制器升级包,验证实车环境下失败程序的回滚功能。

表6 eMMC内存分区结构

序号	名称	设备结点	功能
1	uboot	mmcblk0p1	通用引导加载程序
2	Verison	mmcblk0p2	版本信息
3	Boot_a	mmcblk0p3	存放内核和内存盘
4	Boot_b	mmcblk0p4	存放内核和内存盘
5	ramdisk_a	mmcblk0p5	分区A的内存盘
6	ramdisk_b	mmcblk0p6	分区B的内存盘
7	factory	mmcblk0p7	工厂信息
8	MISC	mmcblk0p8	系统与Recovery、引导加载程序通信数据
9	system_a	mmcblk0p9	存放应用程序和库文件
10	system_b	mmcblk0p10	存放应用程序和库文件
11	vendor_a	mmcblk0p11	存放开发厂商定制的应用和库文件
12	vendor_b	mmcblk0p12	存放开发厂商定制的应用和库文件
13	data	mmcblk0p13	用户数据分区
14	dtlog	mmcblk0p14	存储日志
15	otalog	mmcblk0p15	存储OTA日志
16	ota	mmcblk0p16	存储OTA数据
17	bspinfo	mmcblk0p17	boot模式信息

5.4 验证结果

根据上述测试内容和方法,利用搭建的测试系统和实车测试得到验证结果,如表7所示。每项测试内容至少需要正向测试50次,每次结果均满足要求时方可认定该项功能正常。

表7 A/B系统升级技术测试内容及结果

序号	测试内容	结果	成功率/%
1	Slot_Info分区信息获取	成功	100
2	全量升级及差分升级稳定性	成功	100
3	刷新过程擦除异常断电,版本回滚	成功	100
4	刷新下载时异常断电,版本回滚	成功	100
5	刷新异常升级文件,版本回滚	成功	100
6	上电引导启动分区稳定性	成功	100
7	引导激活分区程序运行稳定性	成功	100
8	升级过程超时及负响应版本回滚	成功	100

测试结果表明:利用MISC分区管理A/B系统的属性信息,解决了升级启动分区选择问题;针对升级包刷写问题,提出了升级包选择分区下载技术,保证升级包刷写有效性,同时设计了升级启动流程,控制器能够安全启动并在升级失败时进行回

滚，实现控制器A/B系统升级。

6 结束语

本文提出一种A/B系统升级技术，优化了升级包的下载刷写、安装启动流程及A/B系统差分升级流程。通过对测试系统及实车不同控制器进行大量升级测试，验证了控制器A/B系统升级稳定性和回滚时系统分区切换的有效性，控制器升级失败后的回滚成功率为100%，解决了因OTA升级失败导致车辆控制器功能失效的问题。

参 考 文 献

[1] 田端祥, 段晖, 陈洁, 等. 远程升级技术在汽车智能网联系统中的运用[J]. 内燃机与配件, 2022(5): 214-216.
TIAN D X, DUAN H, CHEN J, et al. Application of Remote Upgrade Technology in Automobile Intelligent Network System[J]. Internal Combustion Engine & Parts, 2022(5): 214-216.

[2] 武翔宇, 赵德华, 郝铁亮. 浅谈汽车OTA的现状与未来发展趋势[J]. 汽车实用技术, 2019(3): 214-216.
WU X Y, ZHAO D H, HAO T L. Analysis on Current Situation and Future Development Trend of Vehicle OTA [J]. Automobile Applied Technology, 2019(3): 214-216.

[3] 姜楠, 姜姗姗, 韩小鹏. 汽车在线升级系统（OTA）开发浅析[J]. 时代汽车, 2021(21): 11-12.
JIANG N, JIANG S S, HAN X P. The Analysis of Online Updates[J]. Auto Time, 2021(21): 11-12.

[4] 卜凡涛, 刘木林, 刘晓晔. 一种汽车控制器OTA功能方案[J]. 汽车电器, 2022(9): 67-68.
BU F T, LIU M L, LIU X Y. An OTA Function Scheme of A Car Controller[J]. Auto Electric Parts, 2022(9): 67-68.

[5] 李立安, 赵帼娟, 任广乐. OTA实现方案及汽车端设计分析[J]. 汽车实用技术, 2020(14): 16-19.
LI L A, ZHAO G J, REN G L. OTA Implementation Plan and the Vehicle Design Analysis[J]. Automobile Applied Technology, 2020(14): 16-19.

[6] 陈祖锐, 廖振伟, 谷城, 等. 基于UDSonCAN的Bootloader设计[J]. 汽车零部件, 2022(9): 36-39.
CHEN Z R, LIAO Z W, GU C, et al. Bootloader Design Based on UDSonCAN[J]. Automobile Parts, 2022(9): 36-39.

[7] 陶媛媛, 杜彬, 田彬. 基于车载控制器BootLoader的数据备份刷写软件方案实现[J]. 汽车电器, 2022(9): 39-41.
TAO Y Y, DU B, TIAN B. Implementation of Data Backup Flashing Based on Boot Loader of Vehicle Controller[J]. Auto Electric Parts, 2022(9): 39-41.

[8] 严娟, 张玉川, 杨鹏翔, 等. 基于以太网OTA远程升级的研究[J]. 上海汽车, 2020(3): 15-18+27.
YAN J, ZHANG Y C, YANG P X, et al. The Study on OTA Remote Updating of Ethernet[J]. Shanghai Auto, 2020(3): 15-18+27.

[9] 曹玉保. 基于双备份的兆易创新GD32程序升级方案研究[J]. 中国集成电路, 2021(增刊1): 23-26.
CAO Y B, Research on Scheme to Upgrade Program of GigaDevice GD32 Based on Double Backup[J]. China Integrated Circuit, 2021(S1): 23-26.

[10] 陈培德, 吴建平, 刘宏杰, 等. MBR磁盘转换为GPT磁盘的研究与实现[J]. 计算机技术与发展, 2022(7): 99-104.
CHEN P D, WU J P, LIU H J, et al. Research and Implementation of MBR Disk Conversion to GPT Disk[J]. Computer Technology and Development, 2022(7): 99-104.

[11] 陈德富, 周旭文, 邱宝象, 等. 一种轻量级的在线差分升级策略设计[J]. 工业控制计算机, 2022(9): 29-30+32.
CHEN D F, ZHOU X W, QIU B X, et al. Design of Lightweight Online Differential Update Strategy[J]. Industrial Control Computer, 2022(9): 29-30+32.

（责任编辑 白 夜）

修改稿收到日期为2024年7月23日。