1040608 无感升级方案

• 需求背景

- 1. 用户痛点:
 - (1) 一般升级过程需要车辆保持安全状态(如停车、进入OTA模式),升级过程周期长且部分车辆功能无法正常使用,用户体验较差
- (2) 升级过程中可能出现零件刷写失败,为使零件回退到安全状态(即升级前版本),非AB分区零件需下载、重刷回滚包以实现版本回退,导致刷写时间进一步增加,且存在回滚包刷写失败情况,威胁车辆安全

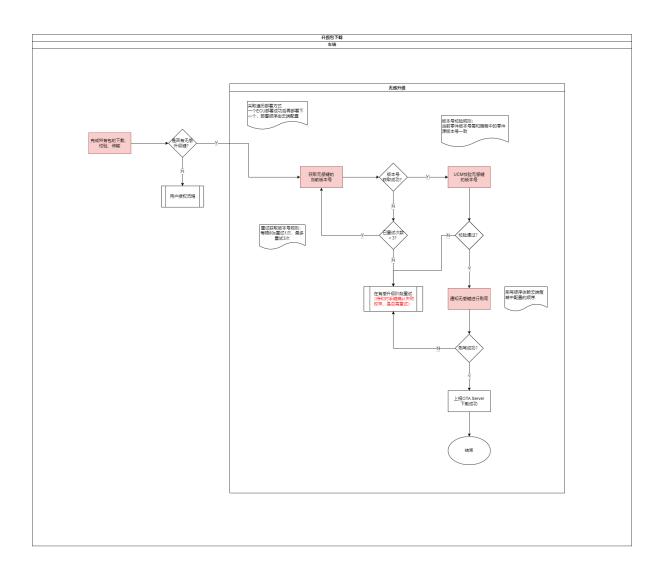
2. 解决方案:

- (1) AB分区零件支持在备用分区(B分区)进行包的下载、刷写,而车辆当前正在使用的A分区不受影响,支持"边用车边升级",缩短了用户有感知的刷写时间,用户体验较佳
- (2) 即便B分区目标版本刷写失败,A分区也能够保持当前在用版本,无需重新刷写回滚包,节省时间且提高了安全性

• 实现方案

- 1. 前提
 - (1) 设备需为AB分区
 - (2) 刷写过程所占用的资源不影响正常业务功能
 - (3) 支持断点续升

2. 设计



(1) 云端:

- a. 配置零件属性时,需配置该零件升级属性,并下发至车端
 - i. 零件升级属性指该零件在本次升级中是否需在无感阶段升级,枚举为: AB、部分AB、单分区
 - ii. 安装策略中配置AB键刷写时机, 枚举: 下载阶段、安装阶段

(2) 车端:

- a. 下载完本次升级所有包并完成校验、验签、解密、传输动作后,根据零件升级属性、安装策略判断出本次需要无感升级的零件
 - i. 如本次升级的零件均为单分区零件,则跳过无感升级、直接进入【用户授权】流程(参考prd)
 - ii. 如本次升级存在需要下载阶段刷写的AB键或部分AB键,则执行步骤b
- b. 信息校验:
 - i. 任务有效性校验
 - ii. 零件版本信息校验 (需根据安装策略中版本号强校验开关状态判断是否校验零件信息,仅开关on需校验)
 - ① 零件当前版本号需与升级策略中配置的零件源版本号一致
 - ② 零件当前版本号需低于策略中该零件的目标版本号
- c. 遍历刷写:

- i. 根据云端下发的升级顺序,UCM依次通知AB键或部分AB键刷写<mark>(依赖:需ecu自行判断全部刷写/模块刷写)</mark>,即一个ECU刷写完成后再刷写下一个
 - ① 支持整包、差分包刷写
 - ② 过程监控:
- 升级时长: UCM根据云端下发的ecu最大升级时长监控刷写过程,若最大升级时长内ecu未返回刷写结果,则UCM判定该ECU刷写失败
- · 条件轮询:刷写过程中轮询下载过程监控条件(云端配置轮询周期),如条件不满足 UCM暂停刷写, 待条件满足后恢复刷写
 - 示例如下:

字段	描述	枚举
下载过程监控条件	下载过程中车端需轮询的条件	蓄电池电压
		动力电池电量百分比
		车速
		自动驾驶
下载过程条件轮询周 期	车端轮询判断下载监控条件的周期	/

- 异常恢复:断电、恢复上电后,UCM重新判断任务有效性,校验通过后从断点处恢复刷写(<mark>依赖:需ecu支持断点续传</mark>)
- ③ 无论无感键刷写成功/失败,均通知下一个无感键刷写,直至本次所有AB键(包括部分AB键)刷写完成
 - 刷写失败定义: ecu反馈刷写失败或超时未反馈刷写结果
 - 刷写失败重试:在有感升级阶段进行重试
- d. 通知用户授权:全部AB键刷写完成后,通知用户授权,用户授权后进入有感升级阶段
- e. 有感升级阶段-AB键刷写重试规则: (重试次数由云端策略下发)
 - i. 主控根据云端定义的ecu升级顺序依次通知相关零件开始刷写,顺序轮到AB键或部分AB键时,主控判断:
 - 若该ecu为全部AB且无感阶段刷写成功,则跳过该键、执行下一个键的刷写
 - 若该ecu为全部AB且无感阶段刷写失败,则通知该键重新刷写
 - 若该ecu为部分AB且无感阶段其AB模块刷写成功,则通知其刷写非AB模块
 - 若该ecu为部分AB且无感阶段其AB模块刷写失败,则通知其刷写(包括AB和非AB模块)
- f. 激活:无感件刷写成功后,通过切换分区激活B分区版本,激活时间因零件而异,参考下表

	无感升级	有感升级	激活
单分区	不支持: 刷写过程自身功能 受影响	支持: 升级完成后自动激活	无独立激活步骤
全AB零件	支持: 升级过程允许失败	支持:不要需要无感升级或无感 升级失败时	有感升级完成后 独立激活步骤
部分AB零件	支持:子AB模块支持,升级过程允许失败	支持: 1. 子AB不要需要无感升级或无感升级失败时 2. 子非AB模块升级	支持:无独立湾模块升级成功后模块间版本匹配