宝能 BAONENG

密级	机密

宝能汽车有限公司	编号：
文档名称	版本：V1.0

OTA 系统车端功能技术规范

信息分类		涉密等级	
责任部门	智能网联研究院	责任人	

会签页

文件编号：		文件名称：		
会 签				
	部门	姓名	签字	日期
编制：				
校对：				
审核：				
批准：				
各专业部门会签：				
	属性	属性负责人	签字	日期
发布日期：		版本		

修订记录：

版本	日期	作者	修订内容

目 录

1 概述

1.1 背景

宝能汽车有限公司成立于 2017 年 3 月，是深圳市宝能投资集团有限公司旗下整车资源聚合和业务发展的平台。主要业务涵盖传统及新能源整车及核心零部件的研发、制造、销售与售后服务以及其他相关业务。致力于打造“研发-制造-销售-后市场”的完整产业链。

宝能汽车有限公司拥有几大生产基地和研究院，其中广州新能源汽车产业园位于黄浦区中新知识城九龙大道西侧，项目规划用地 3.29 平方公里，投资总额达 300 亿，规划产能每年 50 万台，预计 2021 年开始投产。宝能汽车广州研究院是宝能汽车 R&D 体系的重要组成部分，负责中高端纯电动平台车型的研究与开发，开发车型服务于广州宝能汽车产业基地。广州基地主要布局中高端新能源汽车，打造高性能、高品质、低成本的 G1 电动专属平台， G1 平台在 5 年内拟开发 6 款产品： 2 款轿车（A+ 级 GS16， B 级 GS18）， 3 款 SUV（A0+级 GX14/A+级 GX16/B 级 GX18）， 1 款 MPV（A+级 GM17）。针对 G1 平台首款量产车型 GX16 的 SOP 为 2021.12。

宝能汽车有限公司随着汽车越来越智能化，电子模块和软件技术在整车上的应用程度也越来越高，为了提升对宝能汽车车主的服务质量，改善驾乘体验，及时高效的解决问题， 并降低运营成本，研究总院智能网联研究院规划开发 OTA 平台，实现针对整车 ECU 软件的远程更新功能，并逐步应用到宝能汽车全系车型。

1.2 目的

本文档主要描述了 OTA 系统客户端产品需求规格，用以明确项目实施范围，指导开发人员实现，辅助测试人员验证。

1.3 术语定义

缩写/术语	释义
VIN	车辆统一识别码
OTA-MASTER	本文档中专用指代 OTA SDK 的宿主设备，等同于 TBOX
UC-Master	OTA 控制程序主模块
TSP	车联网远程服务提供商

TSP-Client	TSP-客户端
Power-on	车辆上电状态
TBOX	远程终端
IHU	车机
UC-Slave	OTA 控制程序从模块
UA	差分升级代理引擎
confVersion	服务器配置信息版本号
Release note	新版本说明
IHU Apk	车机 OTA 应用程序（IHU 提供）

1.4 引用

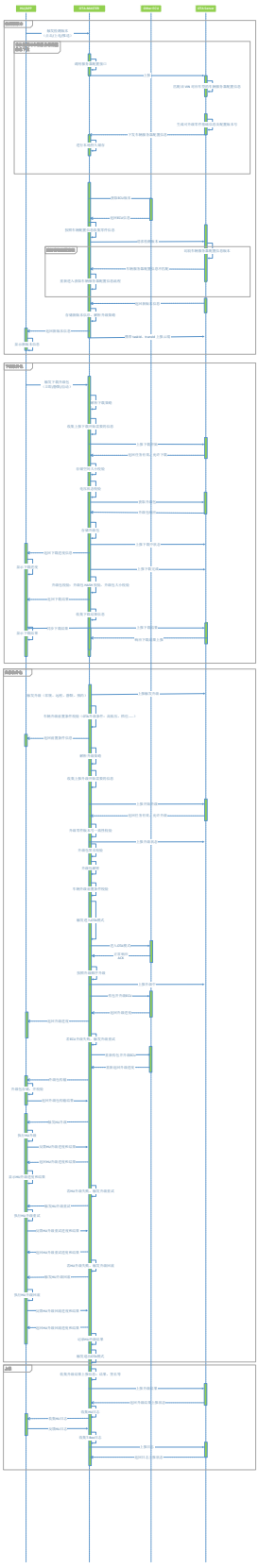
无

2 功能列表

编号	功能模块	L1 功能	L2 功能	功能描述
01	检测新版本	检测触发	获取服务器配置信息	上报云端车辆 VIN，完成信息校验并获取车辆服务器配置信息，作为车辆升级基础信息
02			上电检测	车辆每日首次上电事件触发的新版本检测
03			主动推送	云端通过 TSP 发起的推送消息触发的新版本检测
04			手动检测	用户手动点击车机检测按钮触发的新版本检测
05			手机 APP 远程检测	用户点击手机 APP 触发的远程检测新版本
06		检测过程	获取零件信息	根据本地车辆服务器配置信息获取车辆当前零件软硬件版本信息
07			上报云端	车辆及零件信息上报云端
08			云端解析	云端匹配车辆升级任务并返回
09			解析云端升级策略	接收并解析由云端返回升级策略
10		检测结果	车辆未备案	车辆 VIN 在云端不存在
11			网络异常	网络连接断开等造成的检测失败
12			已是最新版本	没有发现新版本
13			发现新版本	检测到新版本（新版本号、Release note、软件包大小等）
14	下载	下载触发	手动下载	用户主动点击进行软件包下载
15			手机 APP 远程下载	操作手机 APP 远程下载软件包
16			自动下载	在车机界面开启自动后，车辆检测新版本成功自动下载（OTA 应用后台）
17			静默下载	车辆自动开始软件包下载（OTA 应用后台）
18		下载准备	判断存储空间是否足够	判断当前软件包存储空间是否足够
19			判断网络类型（预留）	网络类型是否符合下载要求
20			判断车辆电源状态	判断当前车辆是否为 Power-on 状态
21		下载过程	上报云端开始下载状态	上报服务器车辆开始下载软件包状态
22			判断任务是否有效	判断下载软件包对应的升级任务是否有效

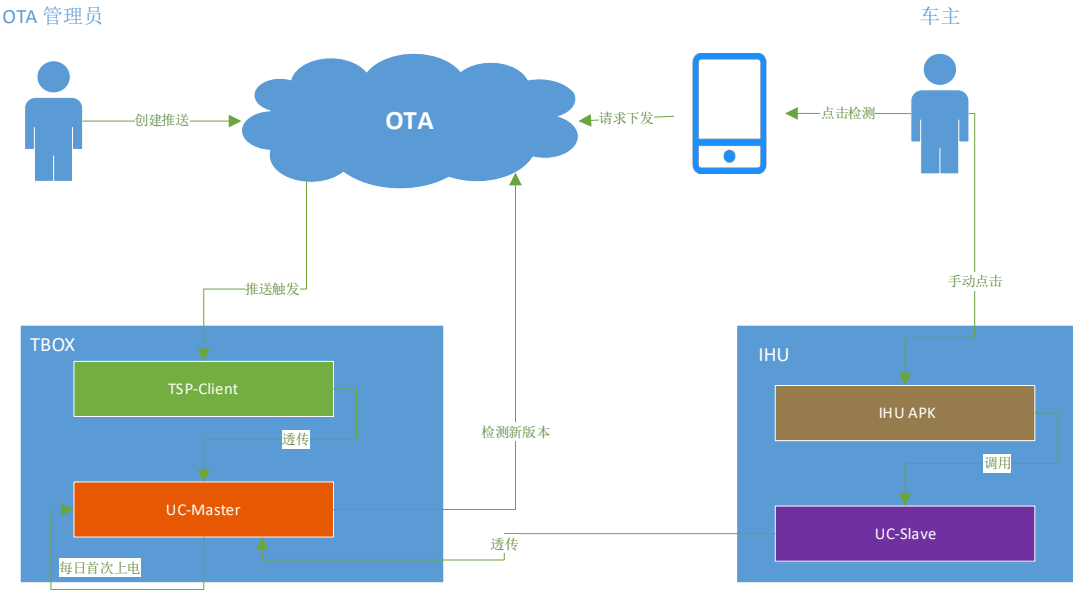
23			开始下载 软件包	请求服务器（CDN）下载软件包
24			展示下载进度	在 HMI 上展示下载进度
25			断点续传	网络断开重连后继续下载
26			断电恢复	车辆重新上电后继续下载
27		下载结束	软件包校验	对下载的软件包进行完整性校验
28			下载结果显示	显示下载成功、任务失效等结果
29			上报云端下载 结束状态	上报服务器车辆下载结束状态
30	安装	安装触发	立即安装	软件包下载完成后 用户通过 HU 或手机 APP 选择立刻安装
31			预约安装	用户通过 HU 或手机 APP 选择其他时间段 车辆自动安装
32			静默安装	由云端主动触发用户无感知的安装
33		安装准备	免责声明	升级服务条款
34			用户确认	用户确认升级动作
35			车辆升级 条件校验	车辆升级必须满足的状态
36			准备升级环境	OTA 升级的准备过程， 包含升级包验签、解密等
37		OTA 模式	进入/退出 OTA 模式	车辆正式刷写时进入 OTA 模式和刷写结束 后退出 OTA 模式
38		安装过程	安装升级包	刷写 ECU 升级包，包含整包和差分
39			安装重试	首次刷写失败后重复安装的过程
40			失败回滚	升级失败后刷写原始版本
41		安装结果	安装结果确认	确认各零件安装结果
42			安装结果上报	上报服务器车辆升级状态 和零件安装结果
43			更新 OTA 状态	UC-Master 更新状态机至初始状态
44	上报	OTA 升级状态	车辆升级状态	车辆检测新版本到安装成功的 状态记录
45		OTA 升级 事件信息	车辆升级事件	车辆升级过程中发生的事件信息记录
46		OTA 程序 运行日志	日志文件	UC-Master 运行日志文件记录

3 总体流程图



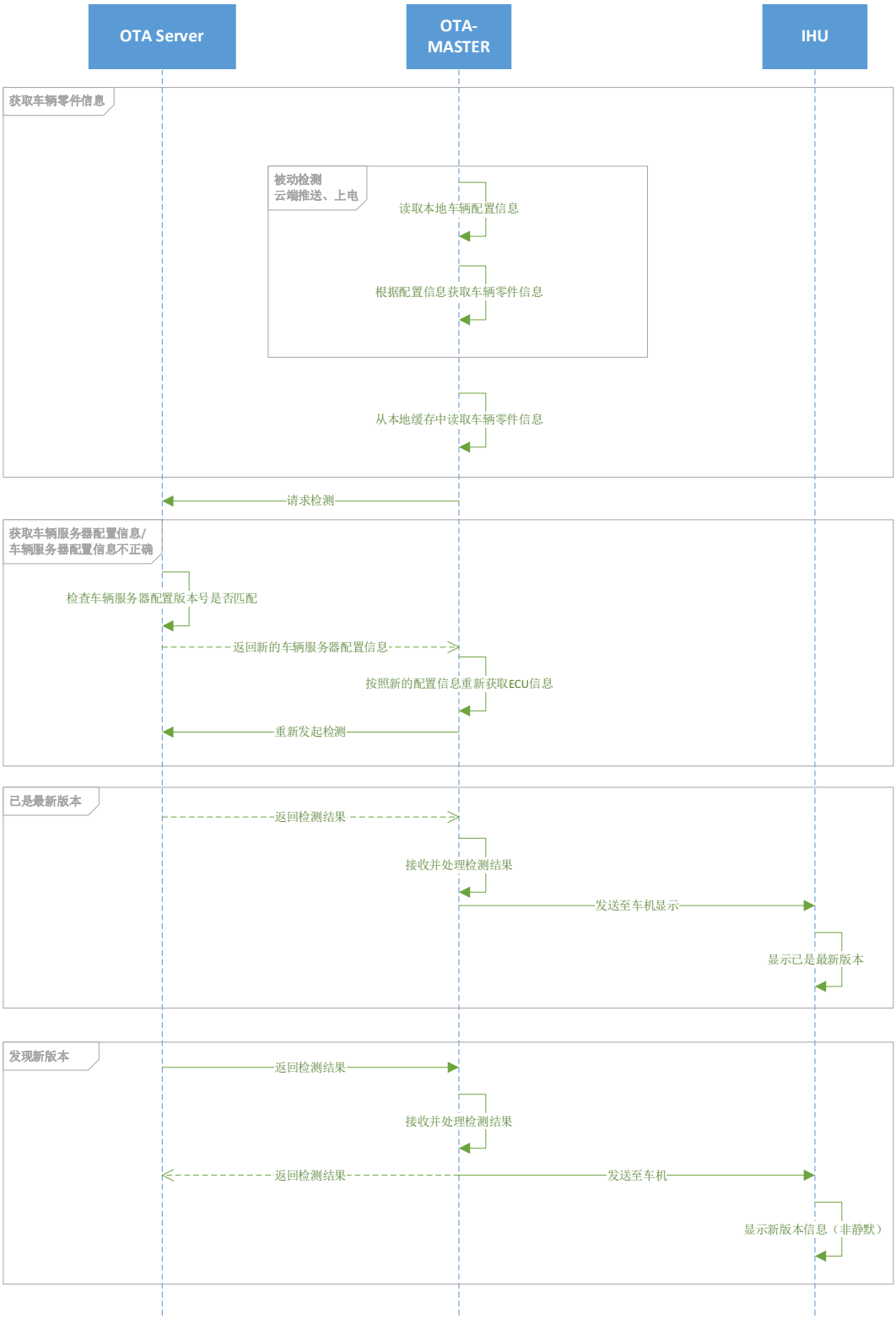
4 检测新版本

4.1 业务架构图



4.2 需求规格

4.2.1 流程图



4.2.2 功能概述

车端检测动作执行前需要触发检测，根据车辆及网络情况提供不同的触发方式。目前检测触发方式有 4 种：车辆每日首次上电触发，OTA 平台主动推送触发，用户手动点击车机触发和用户操作手机 APP 触发。

检测过程是车端检测 OTA 云端是否有升级任务的过程。UC-Master（按照车辆服务器配置信息）获取零件信息后通过向 OTA 云端上报服务器配置版本号及获取到的车辆零件信息，OTA 云端响应该请求，并向车端返回请求结果。

若车辆服务器配置信息不正确，则平台返回车辆对应的新的服务器配置信息，车辆此时按照新的服务器配置信息重新获取当前车辆零件信息。

如果没有新升级任务，OTA 平台将返回无最新版本信息；如果有新升级任务，OTA 平台将返回升级策略给 UC-Master。UC-Master 对升级策略进行解析后生成升级策略文件，持久存储在指定目录，并按照升级策略中的下载方式等将 OTA 平台的响应结果同步给 IHU 和手机 APP 进行人机交互显示（非静默下载）。

4.2.3 获取服务器配置信息

车辆每一次和云端进行交互时，由 TBOX 负责定义通信层的 VIN 数据，UC-Master 不维护 OTA 业务中需要使用的 VIN 字段。

车辆在首次检测时，车端会调用“获取服务器配置信息接口”从 OTA 平台请求获取车辆服务器配置信息并保存，作为实现车辆 OTA 功能的基础信息。

1. 功能描述

车辆首次检测时调用“获取车辆服务器配置信息接口”UC-Master 向 OTA 服务器请求获取车辆服务器配置信息。包含服务器配置版本号，需要 OTA 升级的 ECU 列表两部分内容。

数据	字段	释义
服务器配置信息版本号	confVersion	进行检测、上报车辆信息时，OTA 平台根据该字段标识车端的配置信息是否需要更新
车辆零件基础信息	RequestId1	ECU 诊断 ID（ECU 标识信息）
	ResponseId1	ECU 响应 ID
	FunctionId1	ECU 功能 ID
	firmwareCode1	ECU 软件 ID，该字段主要针对智能 ECU，如用于区分 OTA-MASTER 中的 MPU 和 MCU，为逻辑字段，由车厂、ECU 供应商和艾拉比协商确定，UC-Master 通过 Did 和 firmwareCode 确定 ECU 的唯一性
	ecuId1	ECU 编号，获取 ECU 详细信息时，可通过该字段进行二次确认

	InstallType1	ECU 安装类型，标识该 ECU 通过哪种方式实现 OTA 升级（UC-Client/DPC 等）
	TranferType1	ECU 传包类型，标识该 ECU 的软件包传输目标（UC-Client/DPC 等）
	RequestId2	ECU 诊断 ID（ECU 标识信息）
	ResponseId2	ECU 响应 ID
	FunctionId2	ECU 功能 ID
	firmwareCode2	ECU 软件 ID，该字段主要针对智能 ECU，如用于区分 OTA-MASTER 中的 MPU 和 MCU，为逻辑字段，由车厂、ECU 供应商和艾拉比协商确定，UC-Master 通过 Did 和 firmwareCode 确定 ECU 的唯一性
	ecuId2	ECU 编号，获取 ECU 详细信息时，可通过该字段进行二次确认
	InstallType2	ECU 安装类型，标识该 ECU 通过哪种方式实现 OTA 升级（UC-Client/DPC 等）
	TranferType2	ECU 传包类型，标识该 ECU 的软件包传输目标（UC-Client/DPC 等）
	…	…

2. 触发时机

（1） “服务器配置信息”损坏或被篡改；

（2） UC-Master 无法在持久存储中获取这个“服务器配置信息”；

（3） 检测新版本时上报的“服务器配置版本号”与 OTA 平台反馈的“服务器配置版本号”对比后不一致；

3. 获取流程

（1） UC-Master 在获取车辆服务器配置信息触发后向 OTA 平台发起请求；

（2） OTA 平台处理 UC-Master 获取车辆服务器配置信息请求；

a) 查找该车辆对应车型的车辆服务器配置信息成功，响应 UC-Master 请求，将车辆服务器配置信息下发 UC-Master；

b) 查找该车辆对应车型的车辆服务器配置信息失败，响应 UC-Master 错误码；

（3） UC-Master 等待 OTA 平台响应；

a) UC-Master 等待超时，未收到 OTA 平台反馈，UC-Master 将终止获取车辆服务器配置信息流程，等待下次检测，重新发起车辆服务器配置信息获取流程；

（4） UC-Master 收到 OTA 平台响应；

（5） UC-Master 解析获取的车辆服务器配置信息；

（6） UC-Master 将车辆服务器配置信息持久存储；

4. 获取车辆零件信息

（1） 触发时机

每次车辆上电时会根据车辆服务器配置信息中 ECU 基础信息即 ECU 列表（ECUs List）去搜集对应 ECU 的详细信息（版本信息），若与当前保存的信息不一致，则会更新并将其持久储存至本地，以备检测新版本时直接调用（手动检测、手机 APP 检测）。

（2） 车辆获取服务器配置信息后，请求 OTA-MASTER 按照车辆服务器配置信息中的零件基本信息获取车辆零件详细信息（如下表）；

字段	描述
软件版本号	必须，软件版本号是 OTA 平台判断 ECU 是否存在更新的重要标识
序列号	必须，序列号是 OTA 平台判断 ECU 合法性的重要标识
硬件版本号	可选，硬件版本号主要用于 OTA 平台展示 ECU 详情
供应商编码	可选，供应商编码主要用于 OTA 平台展示 ECU 详情

（3） OTA-MASTER 按照本地存储的车辆服务器配置信息向对应 ECU 进行详细信息获取；

a. 本地存储的车辆服务器配置信息获取为空或者获取失败，会再次触发从平台获取车辆服务器配置信息；

i. 获取失败，终止获取动作，等待下次车辆 Power-on 触发；

（4） OTA-MASTER 获取到对应每个 ECU 的信息后，交由 UC-Master 进行车辆零件信息本地持久化存储；

a. 可升级的 ECU 信息列表中的所有 ECU 详细信息获取成功（UC-Master 与 OTA-MASTER 接口中定义的信息全部返回成功），将全部 ECU 信息更新并存储本地车辆零件信息文件中；

b. 可升级的 ECU 信息列表中的部分 ECU 详细信息获取成功（UC-Master 与 OTA-MASTER 接口中定义的信息全部返回成功），将更新成功获取的 ECU 信息并存储至本地车辆零件信息文件中；

c. 可升级的 ECU 信息列表中的所有 ECU 详细信息获取失败，终止获取动作，等待下次车辆 Power-on 触发；

5. 特别说明

UC-Master 请求 OTA-MASTER 获取零件软硬件版本信息时，可分为传统件、单一分区智能件和双分区智能件（此处举例为 A/B 分区且差分升级），以下对于获取双分区智能件版本进行描述。

初始阶段，假定该零件 S 的 A、B 分区对应版本均为 V1.0，且 A 分区活动分区。检测新版本前，UC-Master 请求 OTA-MASTER 获取该该零件 S 的当前版本信息，OTA-MASTER 每次仅能够获取该零件的活动分区的版本号，此时收集到的该零件版本号为 V1.0。第一次升级时，云端配置差分升级任务 S：V1.0→V2.0，则车辆检测新版本成功后，零件 S 满足 V1.0→V2.0，故发生升级动作。

升级时，按照 UA 程序读取零件 S 当前活动分区 A 的系统文件信息进行与差分文件 V1.0→V2.0 的差分还原算法，得出 V2.0 对应的系统文件，并将其写入 B 分区。若升级失败，则重启后仍然运行当前活动的 A 分区；若升级成功，则重启后运行原 B 分区对应的非活动分区，此时即为运行 V2.0 系统文件对应分区，原 V1.0 系统文件对应分区 A 变更为非活动分区。

此时，OTA—MASTER 每次收集零件 S 的当前版本信息时，仅能够获取到 B 分区的版本号 V2.0，并以此作为零件软件版本信息上报。假设第二次升级时，云端配置差分升级任务 S：V2.0→V3.0，则车辆显然能够检测成功，并发送升级动作。

升级时，按照 UA 程序读取零件 S 当前活动分区 B 的系统文件信息进行与差分文件 V2.0→V3.0 的差分还原算法，得出 V3.0 对应的系统文件，并将其写入 A 分区。若升级失败，则重启后仍然运行当前活动的 B 分区；若升级成功，则重启后运行原 A 分区对应的非活动分区，此时即为运行 V3.0 系统文件对应分区，原 V2.0 系统文件对应分区 B 变更为非活动分区。

综上，我们可以顺利地得出结论。对于 A/B 分区升级的零件，每次升级时，仅需要云端针对当前运行版本配置升级任务，即可完成升级。

4.2.4 手动检测

4.2.4.1 检测触发

（1）用户在 IHU 上点击【检测新版本】按钮；

（2）IHU 通过调用 APK 发送“触发检测”消息给 UC-Master；

（3）UC-Master 接收到“触发检测”消息；

4.2.4.2 检测过程

检测触发后，UC-Master 直接读取本地持久存储中的零件信息后，向 OTA 云端上报服务器配置版本号及获取到的车辆零件信息，OTA 云端响应该请求，车端收到请求并解析的过程。

1. OTA 云端响应请求

（1） 服务器首先校验车辆上报的检测信息中包含的 confVersion 值是否与当前 OTA 管理平台配置的相同；

a. 若 confVersion 不匹配，则服务器下发新的服务器配置信息至客户端，UC-Master 此时重新获取车辆信息；

（2） confVersion 信息校验通过后，服务器开始匹配已发布任务中是否包含该车辆；

（3） 若该车辆无对应的升级任务，则服务器返回“没有新版本”信息至 UC-Master；

（4） 若该车辆有对应任务，则返回升级策略信息至 UC-Master；

2. 解析云端升级策略

（1） UC-Master 接收并解析该升级策略文件，其中主要包含下载策略、安装策略等内容，具体如下；

策略	信息	描述
检测	transId	对应检测到的升级任务在服务器的批次标识
	taskId	升级任务在服务器对应的 id
	targetVersionNo	升级策略中包含的车辆升级大版本号
	firmwareVersion	升级策略中包含的零件升级版本号
	Release note	升级策略中包含的新版本发布说明及零件版本详细描述
下载	常规下载	车主可感知、可操控的下载类型
	静默下载	车主不可感知、无法操控的下载类型
	网络类型（预留）	软件包下载需满足的网络环境，如 WIFI、2G、3G、4G、5G
	downloadUrl	软件包对应下载地址，包含目标版本软件包及存在回滚时的源版本软件包（OSS、CDN）
	fileSize	软件包 SIZE
	shaCode	软件包 hash
	软件包（加密）原始大小	软件包加密前 SIZE
安装	立即安装	车主可感知、可操控的安装类型
	静默安装	车主不可感知、无法操控的下载类型
	taskTips	安装前提示车主操作的文字描述
	disclaimer	更新升级的服务条款

	upgradeConditions	升级必须满足的车辆条件，如保持 P 档
	estimatedUpgradeTime	提示车主本次更新预计用时
	pkgType = 0	ECU 升级为全量刷写
	pkgType = 2	ECU 升级为增量更新
	ecuFirmwareVersionInfos	ECU 零件编号、诊断地址等基本信息
	srcPkgInfo	零件升级的原始版本信息
	dstPkgInfo	零件升级的目标版本信息
	零件升级预计耗时	ECU 安装的预计用时
	dependenyFlag	零件升级必须依赖于当前车辆其他零件所处的版本
	upgradeSeq	零件安装刷写的顺序
	groupSeq	多个零件升级的强制绑定关系
	rollbackMode	零件升级失败后是否需要回滚

（2） 升级策略解析成功后，将升级策略信息持久存储在本地，供检测新版本结果、下载和安装使用；

4.2.4.3 检测结果

（1） 若因网络原因服务器无法响应检测请求，则提示车主“网络异常，请稍后再试”；

（2） 若服务器返回已是最新版本，则提示车主“已是最新版本”；

（3） 若服务器返回有新版本信息，UC-Master 携带 taskId 与 transId 上报服务器并提示车主新版本号、Release note 等信息，并提示用户进行软件包下载（常规下载，非静默下载和自动下载）。

（4） 静默下载情况下，即使有新版本信息返回，HMI 仍显示“已是最新版本”；

4.2.5 上电检测

4.2.5.1 检测触发

上电检测触发是每日（每个自然日）车辆首次上电之后，车辆自动触发检测动作。

（1）车辆启动，上下电模块通过应用报文将上电事件发送给 OTA-MASTER；

（2）OTA-MASTER 通知 UC-Master 车辆已经上电；

（3）UC-Master 从持久存储中读取“当天已上电检测版本计数”的值 A；

（4）UC-Master 比较 A 和 1 的大小；

a. A<1；触发检测动作，并将 A+1,存储到持久存储中；

b. A>1 或 A=1,将不触发检测动作，等待下一个时间范围的上电触发；

4.2.5.2 检测过程

同 4.2.4.2 章节“手动检测>检测过程”

4.2.5.3 检测结果

（1） 若因网络原因服务器无法响应检测请求，则本次上电检测进程结束，等待下次上电触发；

（2） 若服务器返回已是最新版本，则本次上电检测进程结束，等待下次触发；

（3） 若服务器返回有新版本信息，UC-Master 携带 taskId 与 transId 上报服务器并提示车主新版本号、Release note 等信息，并在车机当前界面（OTA 应用非前台运行）提示用户进行软件包下载（常规下载，非静默下载和自动下载）。

4.2.6 主动推送检测

4.2.6.1 检测触发

OTA 平台推送触发是 OTA 平台通过 TSP 将通知消息发送给 TSP-Client 后，TSP-Client 通过 OTA-MASTER 通知 UC-Master 检测新版本。

（1）OTA 平台管理员点击 OTA 平台上的“推送”按钮；

（2）OTA 平台将“触发检测”消息发送给 TSP 平台；

（3）TSP 平台接收“触发检测”；

（4）TSP 平台将“触发检测”消息推送给 TSP-Client；

（5）TSP-Client 接收到“触发检测”消息；

a. OTA-MASTER 如果处于休眠状态或未休眠但车辆不在线，将唤醒 OTA-MASTER 接收推送消息，并由 OTA-MASTER 通知 UC-Master 执行检测动作（以本地缓存中的零件信息上报检测）；

b. OTA-MASTER 如果不处于休眠状态（车辆在线），将接收推送指令，通知 UC-Master 执行检测动作(重新请求 OTA-MASTER 按照车辆服务器配置信息获取最新的车辆零件信息)；

4.2.6.2 检测过程

同 4.2.4.2 章节“手动检测>检测过程”

4.2.6.3 检测结果

（1） 若因网络原因服务器无法响应检测请求，则本次推送检测进程结束，等待下次推按触发；

（2） 若服务器返回已是最新版本，则本次推送检测进程结束，等待下次触发；

（3） 若服务器返回有新版本信息，UC-Master 携带 taskId 与 transId 上报服务器并提示车主新版本号、Release note 等信息，并在车机当前界面（OTA 应用非前台运行）或下次车机开机时（当前车机未开机或未点亮）提示用户进行软件包下载（常规下载，非静默下载和自动下载）。

4.2.7 手机 APP 检测

4.2.7.1 检测触发

（1）用户在手机 APP 上点击“检测新版本”按钮；

（2）手机 APP 通过请求 TSP 发送“触发检测”消息给 OTA-MASTER 后传递给 UC-Master；

（3）UC-Master 接受到“触发检测”消息；

4.2.7.2 检测过程

同 4.2.4.2 章节“手动检测>检测过程”

4.2.7.3 检测结果

（1） 若因网络原因服务器无法响应检测请求，则提示车主“网络异常，请稍后再试”；

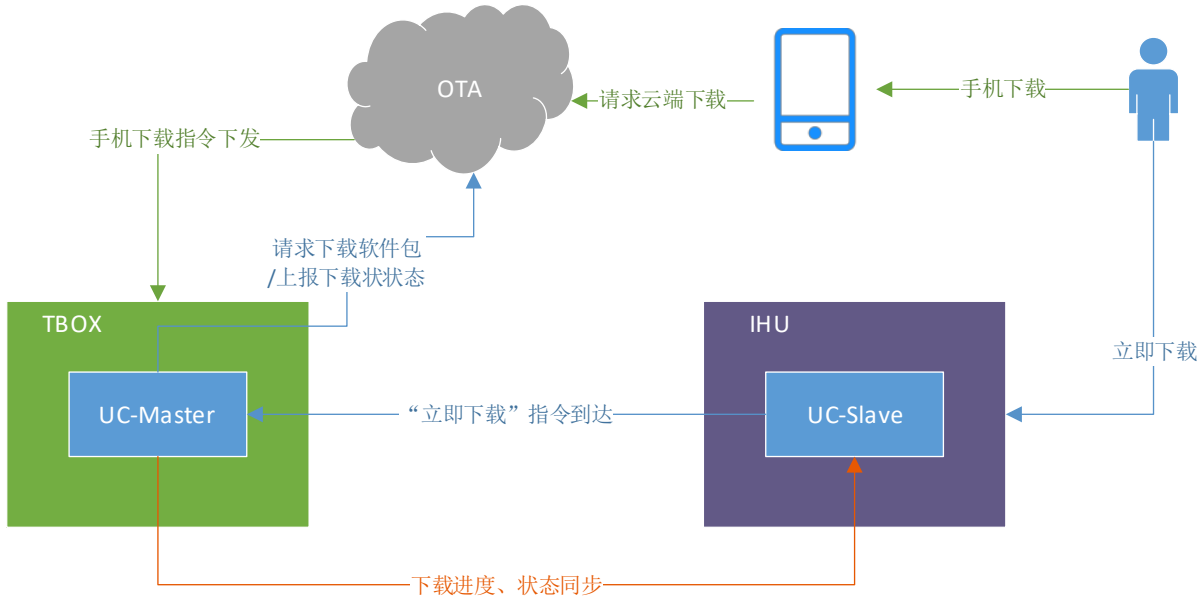
（2） 若服务器返回已是最新版本，则提示车主“已是最新版本”（ 常规下载，非静默下载和自动下载）；

（3） 若服务器返回有新版本信息，UC-Master 携带 taskId 与 transId 上报服务器并在本地保存该新版本信息后同步至 UC-Slave 并最终反馈车机进行展示（车机在线，直接显示通知或弹窗；车机不在线，等待下载车辆上电再显示）；

（4） 静默下载情况下，即使有新版本信息返回，手机 APP 仍显示“已是最新版本”；

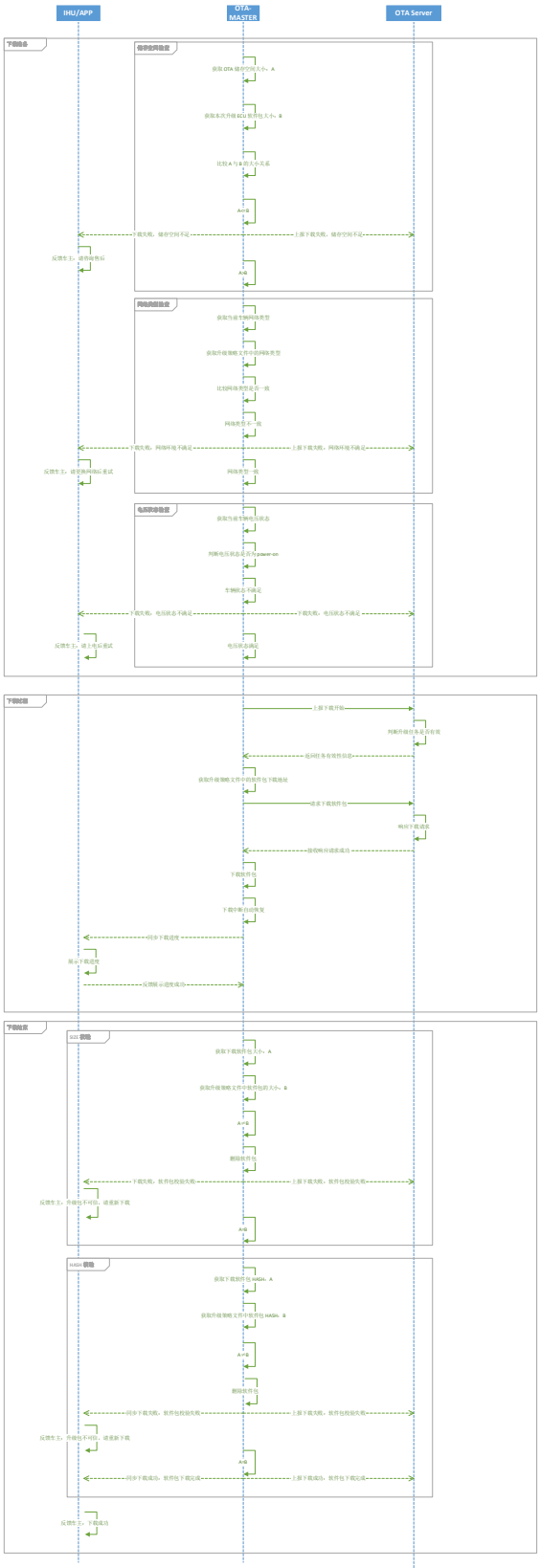
5 下载软件包

5.1 业务架构图



5.2 需求规格

5.2.1 流程图



5.2.2 功能概述

检测新版本成功后，UC-Master 监测到下载触发信号后，开始判断车辆当前条件状态是否满足下载，并根据本地升级策略文件解析的软件包下载 URL 开始下载软件包，最后对下载的软件包进行完整性等校验的过程。

5.2.3 立即下载

5.2.3.1 下载触发

（1） 用户在车机 OTA 应用界面点击【下载】;

（2） 用户在车机非 OTA 应用界面点击新版本检测成功的通知弹窗消息体；

5.2.3.2 下载准备

下载准备是在下载动作触发后，判断车辆状态是否满足下载条件。包括 OTA-MASTER（此处指代软件包存储设备）可用 OTA 储存空间是否满足存储软件包要求、网络类型是否与 OTA 平台要求的下载网络类型一致、车辆当前电源状态是否为 Power-on。

注：本项目一期阶段不涉及“网络类型的判断”，但考虑到扩展性，保留此项。

1. OTA-MASTER 可用 OTA 储存空间检查

（1） UC-Master 读取磁盘可用空间大小（OTA-MASTER 分配的仅供 OTA 使用固定空间），假设值为 A；

（2） 读取失败，终止后续动作执行，UC-Master 同步“下载失败”消息给 HMI，并上报 OTA 平台，下载失败原因；

（3） 读取成功后，UC-Master 从升级策略中读取所有本次升级 ECU 软件包文件总大小，经过计算后得到需要最小存储空间的大小，假设为 B；

a. B = 安装包+解密包（没有加密则为 0）+解压后包（原始包大小）；

（4） UC-Master 比较 A 和 B；

a. A<B 或者 A=B，不满足下载条件，终止后续动作执行，UC-Master 同步“下载空间不足”消息给 HMI，并上报 OTA 平台，下载失败原因（存储空间不满足）；

b. A>B，满足升级包存储空间要求，执行后续动作；

2. 车辆网络类型检查

（1） UC-Master 获取车辆当前网络类型（信号由 OTA-MASTER 透传）；

a. 获取失败，终止后续动作执行，UC-Master 同步“下载失败”消息给 HMI，并上报 OTA 平台，下载失败原因（网络不满足）；

（2） 获取成功后，UC-Master 获取升级策略中云端配置的下载所需的网络类型；

（3） UC-Master 比较车辆当前网络类型和升级策略文件中的网络类型是否一致；

a. 网络类型不一致，不满足下载条件，终止后续动作执行，UC-Master 同步“此网络类型下不允许下载”消息给 HMI，并上报 OTA 平台，下载失败原因；

（4） 网络类型一致，执行下列动作；

3. 车辆电源状态检查

（1） UC-Master 获取车辆当前上电状态（信号由 OTA-MASTER 透传）；

a. 获取失败，终止后续动作执行，UC-Master 同步“下载失败”消息给 HMI，并上报 OTA 平台，下载失败原因（上电信号无法获取）；

（2） 获取成功后，UC-Master 比较车辆当前电源状态是否为 Power-on；

a. 电源状态不一致，不满足下载条件，终止后续动作执行，UC-Master 同步“此电源状态下不允许下载”消息给 HMI，并上报 OTA 平台，下载失败原因（电源不满足）；

（3） 电源状态为 Power-on，则开始下载；

5.2.3.3 下载过程

下载过程是指车辆从 OTA 平台（CDN）下载 ECU 软件包、下载进度和下载结果同步给 HMI 的过程。

下载状态	状态定义	状态约定
待下载	表示已经获取任务信息，可以启动下载过程	检测新版本成功待下载
下载中	表示正在下载升级包	下载中
下载中止	包括网络异常、数据异常等造成的升级包下载中断	下载暂停
下载等待	表示建立通道连接，升级包下载前的状态	开始下载
下载完成	表示升级包下载完成，未进行安装包校验	软件包下载完成待校验
下载成功	表示升级包下载完成，安装包校验成功	下载成功
下载失败	表示升级包下载完成，安装包校验失败	下载失败

（1） 下载开始、下载恢复均需要满足上述下载准备的限制条件；

（2） 当下载准备完成后，满足下载条件，UC-Master 向 OTA 平台上报下载开始；

a. OTA 平台反馈此升级任务已失效，UC-Master 终止下载，同时同步“任务失效”消息给 HMI；

b. OTA 服务器反馈升级任务有效，UC-Master 进行软件包下载；

c. 注：本项目一期阶段不涉及“任务有效的判断”，但考虑到扩展性，保留此项。

（3） UC-Master 从升级策略文件中获取软件包下载地址；

（4） UC-Master 根据升级包的下载地址，向 OTA 平台（CDN）请求下载升级包；

a. OTA 平台（CDN）未响应请求（重复请求 100 次，每次间隔 3/5/8/15/30/60/120/900/900/900s…），UC-Master 等待超时，暂停当前下载动作，同步下载中止状态至 UC-Slave，并等待重试成功；

i. UC-Master 每次进行重试前，均会向与 TBOX 约定的整车条件状态集合中实时获取当前是否处于整车上电的状态；

ii. 若识别到当前车辆未上电，则 UC-Master 等待下个重试时间到达；

iii. 若识别到当前车辆已上电，则 UC-Master 继续下载；

iv. 特别地，若车辆下电，则 UC-Master 根据 TBOX 休眠后自动中止下载；

b. 当处于下载中止状态时，车机接收 UC-Slave 的状态，在 HMI 显示“下载已中止：当前网络信号差。系统将在网络恢复后，自动开始下载”。

i. 若车主此时未进入 OTA 应用界面，则不主动在车机页面进行弹窗或通知提示；

ii. 在 OTA 应用界面显示“恢复下载”按钮，以便用户主动恢复；

c. 车辆断电情况下，待车辆下次 Power-on 后，UC-Master 继续下载；

（5） 相应下载请求成功后，UC-Master 从 OTA 平台（CDN）下载升级包；

（6） UC-Master 在下载升级包过程中记录下载的进度，并同步下载进度给 HMI；

a. 下载过程中，网络异常造成的下载中断时，UC-Master 尝试重新连接（重复请求 100 次，每次间隔 3/5/8/15/30/60/120/900/900/900s…），UC-Master 等待超时，暂停当前下载动作，同步下载中止状态至 UC-Slave，并等待重试成功；

i. UC-Master 每次进行重试前，均会向与 TBOX 约定的整车条件状态集合中实时获取当前是否处于整车上电的状态；

ii. 若识别到当前车辆未上电，则 UC-Master 等待下个重试时间到达；

iii. 若识别到当前车辆已上电，则 UC-Master 继续下载；

iv. 特别地，若车辆下电，则 UC-Master 根据 TBOX 休眠后自动中止下载；

b. 当处于下载中止状态时，车机接收 UC-Slave 的状态，在 HMI 显示“下载已中止：当前网络信号差。系统将在网络恢复后，自动开始下载”。

i. 若车主此时未进入 OTA 应用界面，则不主动在车机页面进行弹窗或通知提示；

ii. 在 OTA 应用界面显示“恢复下载”按钮，以便用户主动恢复；

c. 车辆断电情况下，待车辆下次 Power-on 后，UC-Master 继续下载；

d. 下载超时规则：根据网速计算，speed<1024byte/min 时，进行超时重试；

5.2.3.4 下载结束

下载结束是指对软件包进行完整性校验、安全存储、下载结果上报 OTA 平台及下载进度和下载结果同步给 HMI 的过程。

（1） 软件包下载完成后，通过 SIZE 值进行大小校验；

a. UC-Master 获取软件包的大小，得出软件包的大小，假设为 A；

b. UC-Master 从升级策略文件中获取软件包的大小，假设为 B；

c. UC-Master 比较 A 和 B 是否一致；

i. A 和 B 不一致，则删除升级包，并上报 OTA 平台下载失败，同时将“下载失败”消息同步给 HMI，反馈车主“升级包不可信，请重新下载”。车主再次触发下载，UC-Master 将重新开始下载软件包；

ii. A 和 B 一致，则进行 HASH 校验；

（2） 升级包下载完成，通过 HASH 值进行完整性校验；

a. UC-Master 通过 SHA256 对升级包进行计算，得出升级包的 HASH 值,假设为 A；

b. UC-Master 从升级策略文件中获取软件包的 HASH，假设为 B；

c. UC-Master 比较 A 和 B 是否一致；

i. A 和 B 不一致，则删除升级包，并上报 OTA 平台下载失败，同时将“下载失败”消息同步给 HMI，车主再次触发下载，UC-Master 将重新开始下载软件包；

ii. A 和 B 一致，则存储软件包至本地，并上报 OTA 平台下载成功，同时将“下载成功”消息同步给 HMI；

（3） 下载结束会将下载过程中的剩余空间校验、下载速度、下载重试、断点续传等以事件的形式上报到 OTA 平台；

（4） 软件包下载过程中或下载结束后，每过 3 天，UC-Master 均会进行一次检测新版本请求，以确保当前任务真实有效。若检测到其他任务，则删除本地已下载软件包，提示用户新的版本检测结果；

5.2.4 手机 APP 远程下载

手机 APP 远程下载是指由手机 APP 点击下载后，经由云端下发下载指令至 TBOX，并由 TBOX 透传该下载指令至 UC-Master 后，开始下载并在下载过程中产生状态变更时上报 OTA 云端状态，并返回下载状态和下载结果至手机 APP。

5.2.4.1 下载触发

用户在手机 APP 中 OTA 应用界面点击【下载】。

5.2.4.2 下载准备

下载动作触发后，若当前车辆不在线，则需要唤醒 TBOX，并下发指令给 TBOX，当 TBOX 返回消息确认收到消息后，返回结果至手机 APP，APP 提示用户下载动作将在车辆启动后开始。

若车辆当前在线，则进入下载准备的条件判断（同立即下载）。

其余内容同 5.2.3.2 章节“立即下载>下载准备”

5.2.4.3 下载过程

同 5.2.3.3 章节同“立即下载>下载过程”

5.2.4.4 下载结束

同 5.2.3.4 章节“立即下载>下载结束”

5.2.5 静默下载

5.2.5.1 下载触发

检测新版本成功后，UC-Master 识别本次任务下载方式为“静默下载”，自动触发下载。

5.2.5.2 下载准备

下载准备是在下载动作触发后，判断车辆状态是否满足下载条件。包括 OTA-MASTER（此处指代软件包存储设备）可用 OTA 储存空间是否满足存储软件包要求、网络类型是否与 OTA 平台要求的下载网络类型一致、车辆当前电源状态是否为 Power-on。

1. OTA-MASTER 可用 OTA 储存空间检查

（1） UC-Master 读取磁盘可用空间大小，假设值为 A；

（2） 读取失败，终止后续动作执行，UC-Master 上报 OTA 平台下载失败；

（3） 读取成功后，UC-Master 从升级策略中读取所有本次升级 ECU 软件包文件总大小，经过计算后得到需要最小存储空间的大小，假设为 B；

a. B = 安装包+解密包（没有加密则为 0）+解压后包（原始包大小）；

（4） UC-Master 比较 A 和 B；

a. A<B 或者 A=B，不满足下载条件， UC-Master 上报 OTA 平台下载失败，原因：存储空间不满足。并终止后续动作执行，本次静默下载结束；

b. A>B，满足升级包存储空间要求，执行后续动作；

2. 车辆网络类型检查

（1） UC-Master 获取车辆当前网络类型；

a. 获取失败，UC-Master 上报 OTA 平台下载失败，原因：网络不满足。并终止后续动作执行，本次静默下载结束；

（2） 获取成功后，UC-Master 获取升级策略中云端配置的下载所需的网络类型；

（3） UC-Master 比较车辆当前网络类型和升级策略文件中的网络类型是否一致；

a. 网络类型不一致，不满足下载条件，UC-Master 上报 OTA 平台下载失败，原因：网络不满足。并终止后续动作执行，本次静默下载结束；

（4） 网络类型一致，执行下列动作；

3. 车辆电源状态检查

（1） UC-Master 获取车辆当前电源状态；

a. 获取失败，UC-Master 上报 OTA 平台下载失败，原因：电源无法获取。并终止后续动作执行，本次静默下载结束；

（2） 获取成功后，UC-Master 比较车辆当前电源状态是否为 Power-on；

a. 电源状态不一致，不满足下载条件，UC-Master 上报 OTA 平台下载失败，原因：电源状态不满足。并终止后续动作执行，本次静默下载结束；

（3） 电源状态为 Power-on，则开始下载；

5.2.5.3 下载过程

下载过程是指车辆从 OTA 平台（CDN）下载 ECU 软件包并提示下载结果的过程（静默下载且非静默安装）。

（1） 下载开始、下载恢复均需要满足上述下载准备的限制条件；

（2） 当下载准备完成后，满足下载条件，向 OTA 平台上报下载开始；

a. OTA 平台反馈此升级任务已失效，UC-Master 终止下载，UC-Master 上报 OTA 平台下载失败，原因：电源状态不满足。并终止后续动作执行，本次静默下载结束；

b. OTA 反馈升级任务有效，UC-Master 进行软件包下载；

（3） UC-Master 从升级策略文件中获取软件包下载地址（仅一个软件包，包含所有 ECU）；

（4） UC-Master 根据升级包的下载地址，向 OTA 平台（CDN）请求下载升级包；

a. 下载过程中，网络异常造成的下载中断时，UC-Master 尝试重新连接（重复请求 100 次，每次间隔 3/5/8/15/30/60/120/900/900/900s…），UC-Master 等待超时，暂停当前下载动作，同步下载中止状态至 UC-Slave，并等待重试成功；

i. UC-Master 每次进行重试前，均会向与 TBOX 约定的整车条件状态集合中实时获取当前是否处于整车上电的状态；

ii. 若识别到当前车辆未上电，则 UC-Master 等待下个重试时间到达；

iii. 若识别到当前车辆已上电，则 UC-Master 继续下载；

iv. 特别地，若车辆下电，则 UC-Master 根据 TBOX 休眠后自动中止下载；

b. 当处于下载中止状态时，车机接收 UC-Slave 的状态，在 HMI 显示“下载已中止：当前网络信号差。系统将在网络恢复后，自动开始下载”。

i. 若车主此时未进入 OTA 应用界面，则不主动在车机页面进行弹窗或通知提示；

ii. 在 OTA 应用界面显示“恢复下载”按钮，以便用户主动恢复；

c. 车辆断电情况下，待车辆下次 Power-on 后，UC-Master 继续下载；

d. 下载超时规则：根据网速计算，speed<1024byte/min 时，进行超时重试；

（5） 相应下载请求成功后，UC-Master 从 OTA 平台（CDN）下载升级包；

a. 下载超时规则：根据网速计算，speed<1024byte/min 时，进行超时重试；

5.2.5.4 下载结束

下载结束是指对软件包进行完整性校验、安全存储、下载结果上报 OTA 平台及下载结果同步给 HMI（静默下载且非静默安装）的过程。

（1） 软件包下载完成后，通过 SIZE 值进行大小校验；

a. UC-Master 获取软件包的大小，得出软件包的大小，假设为 A；

b. UC-Master 从升级策略文件中获取软件包的大小，假设为 B；

c. UC-Master 比较 A 和 B 是否一致；

a) A 和 B 不一致，则删除升级包，并上报 OTA 平台下载失败，原因：“升级包 SIZE 校验失败”，同时 UC-Master 将重新开始下载软件包（因校验不满足的自动重试下载共 3 次）；

b) A 和 B 一致，则进行 HASH 校验；

（2） 升级包下载完成，通过 HASH 值进行完整性校验；

a. UC-Master 通过 SHA256 对升级包进行计算，得出升级包的 HASH 值,假设为 A；

b. UC-Master 从升级策略文件中获取软件包的 HASH，假设为 B；

c. UC-Master 比较 A 和 B 是否一致；

a) A 和 B 不一致，则删除升级包，并上报 OTA 平台下载失败，原因“升级包 HASH 校验失败”，同时 UC-Master 将重新开始下载软件包（因校验不满足的自动重试下载共 3 次）；

b) A 和 B 一致，则存储软件包至本地，并上报 OTA 平台下载成功，同时将“下载成功”消息同步给 HMI，在车机下次开机时反馈车主“软件下载已完成，即刻升级吧”；

（3） 下载结束会将下载过程中的剩余空间校验、下载速度、下载重试、断点续传等以事件的形式上报到 OTA 平台；

5.2.6 自动下载

5.2.6.1 下载触发

（1） 车主在 HU 上开启了“自动下载”；

（2） UC-Master 检测新版本成功后，主动请求 HU 获取当前“自动下载”是否已开启；

a. 若当前车机不在线，则等待下次车辆上电后重新请求，进入下载流程；

（3） 开始自动下载；

5.2.6.2 下载准备

同 5.2.5.2 章节“静默下载>下载准备”

5.2.6.3 下载过程

下载过程中，车主点击进入 OTA 应用，则直接显示当前下载状态，如下载中，下载的进度等。

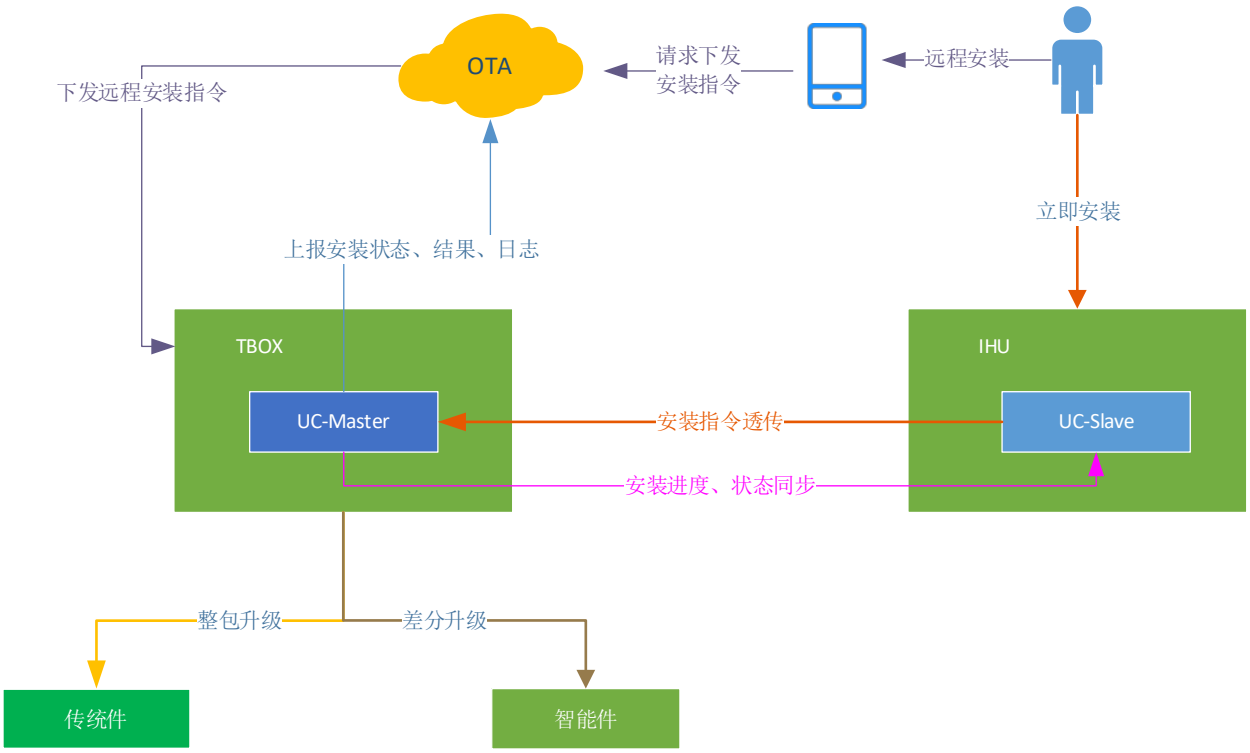
同 5.2.5.3 章节“静默下载>下载过程”

5.2.6.4 下载结束

同 5.2.5.4 章节“静默下载>下载结束”

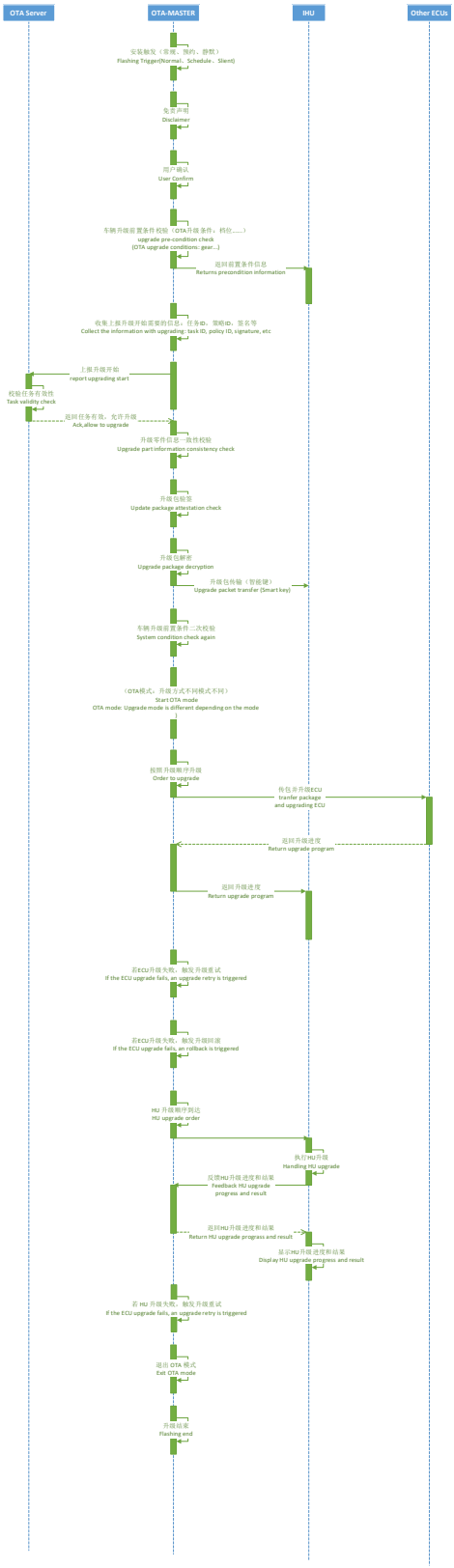
6 安装升级包

6.1 业务架构图



6.2 需求规格

6.2.1 流程图


OTA Server
OTA-MASTER
IHU
Other ECUs
安装触发（常规、预约、静默）
Flashing Trigger(Normal、Schedule、Silent)
免责声明
Disclaimer
用户确认
User Confirm
车辆升级前置条件校验（OTA升级条件，档位……）
upgrade pre-condition check
(OTA upgrade conditions: gear...)
返回前置条件信息
Returns precondition information
收集上报升级开始需要的信息，任务ID，策略ID，签名等
Collect the information with upgrading: task ID, policy ID, signature, etc
上报升级开始
report upgrading start
校验任务有效性
Task validity check
返回任务有效，允许升级
Ack_allow to upgrade
升级零件信息一致性校验
Upgrade part information consistency check
升级包验签
Update package attestation check
升级包解密
Upgrade package decryption
升级包传输（智能键）
Upgrade packet transfer (Smart key)
车辆升级前置条件二次校验
System condition check again
（OTA模式，升级方式不同模式不同）
Start OTA mode
OTA mode: Upgrade mode is different depending on the mode
按照升级顺序升级
Order to upgrade
传包并升级ECU
tranfer package
and upgrading ECU
返回升级进度
Return upgrade program
返回升级进度
Return upgrade program
若ECU升级失败，触发升级重试
If the ECU upgrade fails, an upgrade retry is triggered
若ECU升级失败，触发升级回滚
If the ECU upgrade fails, an rollback is triggered
HU 升级顺序到达
HU upgrade order
执行HU升级
Handling HU upgrade
反馈HU升级进度和结果
Feedback HU upgrade
progress and result
返回HU升级进度和结果
Return HU upgrade prograss and result
显示HU升级进度和结果
Display HU upgrade progress and result
若 HU 升级失败，触发升级重试
If the ECU upgrade fails, an upgrade retry is triggered
退出 OTA 模式
Exit OTA mode
升级结束
Flashing end

6.2.2 功能概述

软件包下载成功后，通过安装触发，UC-Master 开始执行安装流程。基本包含用户对于升级的确认、车辆升级前置条件的校验、软件包校验、升级环境的准备、软件包的传输与刷写等过程，以及安装结果的提示和上报等。

6.2.3 立即安装

6.2.3.1 安装触发

立即安装是指升级包下载完成后，用户主动点击【立即安装】触发安装进程。

6.2.3.2 安装准备

1. 车辆升级前置条件校验（由车机触发）

安装触发后，需要车主同意免责声明、确认升级后，UC-Master 提取存储在本地的升级策略文件中的各项条件请求 OTA-MASTER 获取车辆状态。

（1） UC-Master 读取升级策略文件中的“车辆升级前置条件”；

（2） UC-Master 请求 OTA-MASTER 获取车辆状态；

（3） OTA-MASTER 按照升级策略文件中的各项条件，获取车辆状态；

（4） OTA-MASTER 读取车辆状态，包括车速，档位等信息；

（5） MASTER 将读取的车辆当前的状态反馈给 UC-Master；

（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 如果有部分条件不满足，将告知车辆状态不满足，将安装前置条件和车辆实际状态呈现给用户，请用户更改车辆状态；

b. 如果对比完成全部满足，进入任务有效性校验流程；

车辆升级条件（举例）
电源状态（整车使用动力电池供电状态）
车速（0-5）
蓄电池电压（TBD）
蓄电池电量（TBD）
动力电池电量（TBD）
档位（P 档）
手刹状态/EPB（UP）
整车未充电

2. 升级任务有效性校验

车辆升级前置条件校验通过后，UC-Master 向云端发起任务有效性校验，校验当前待安装任务是否仍然有效。

注：本项目一期阶段不涉及“任务有效的判断”，但考虑到扩展性，保留此项。

（1） UC-Master 读取升级策略文件中的“任务 ID”；

（2） 上报服务器该“任务 ID”；

（3） 服务器判断该“任务 ID”对应的升级任务是否仍然有效；

（4） 服务器返回任务有效性信息至 UC-Master；

（5） UC-Master 无法接收服务器返回消息时，分别等待 10/20/30s 后重新请求响应，若始终无法得到服务器关于本次任务的否定答复，则视为任务仍然有效，进行下一步流程；

（6） UC-Master 接收到服务器返回消息；

a. 若任务无效，则反馈 HMI“任务已失效，请等待后续更新推送”，并终止安装，上报服务器安装结束；

（7） 若任务有效，则进入零件信息校验过程；

3. 零件信息校验

任务有效性校验通过后，UC-Master 校验待升级零件版本信息是否与升级策略中一致。

（1） UC-Master 读取升级策略文件中的待升级零件源版本信息；

（2） UC-Master 请求 OTA-MASTER 获取当前待升级零件实际版本信息；

（3） OTA-MASTER 获取零件版本信息失败（重复获取 3 次）则退出本次安装，并反馈 HMI“准备升级环境失败，请稍后再试”，上报服务器安装结束；

（4） UC-Master 接收 OTA-MASTER 反馈的当前零件实际版本信息，并对比二者是否一致；

a. 若无法匹配，则反馈 HMI“准备升级环境失败，请稍后再试”，并退出安装，上报服务器安装结束 ；

（5） 升级策略文件中的零件源版本与实际获取的当前零件版本一致，则进入软件包校验过程；

4. 软件包验签

零件版本信息校验通过后，UC-Master 校验软件包。

信息	说明
srcPkg	源版本软件包
srcPkgHash	源版本软件包摘要
srcSignFile	源版本软件包签名文件，文件内容即源版本软件包签名数据和公钥

srcSignFileHash	源版本软件包签名文件摘要
dstPkg	目标版本软件包
dstPkgHash	目标版本软件包摘要
dstSignFile	目标版本软件包签名文件，文件内容即目标版本软件包签名数据和公钥
dstSignFileHash	目标版本软件包签名文件摘要

（1） 校验目标版本软件包摘要，通过 Security 模块计算目标版本软件包的摘要 realHash，比较 realHash 与 dstPkgHash，一致进入下一步，不一致退出遍历；

（2） 校验目标版本软件包签名文件摘要，通过 Security 模块计算 dstSignFile 的摘要 realSignHash，比较 realSignHash 与 dstSignFileHash，一致进入下一步，不一致退出遍历；

（3） 校验源版本软件包、源版本软件包签名文件摘要，方法同上，校验通过进入下一步，不通过退出遍历（存在整包回滚时）；

（4） 校验目标版本软件包签名，UC-Master 把签名信息 dstSignFileHash 和被签名数据 dstSignFile，传给 PKI 提供的验签的接口，验证升级包签名的正确性。若 PKI 返回验签成功，进入下一步；验签失败退出遍历；

（5） 校验源版本软件包签名，方法同上，验签成功进行下一个 ECU 校验，验签失败退出遍历（存在整包回滚时）；

（6） 存在 ECU 软件包验签失败，删除已下载的软件包并反馈 HMI“准备环境失败：升级包不可信。请重试更新”，同时退出安装，上报服务器安装结束；

（7） 所有软件包验签成功后进入解密流程；

5. 软件包解密

软件包信息校验通过后，UC-Master 对加密软件包进行解密。

信息	说明
isEncrypt	软件包是否加密
oriHash	加密前软件包摘要
encHash	加密后软件包摘要
pkgKey	软件包的加密因子

（1） 通过 isEncrypt 判断软件包是否加密，如果加密则进入下一步，否则跳过此软件包解密，继续执行遍历；

（2） 通过本地的升级策略文件中获取软件包的加密因子，获取成功则进入下一步，不成功则退出遍历；

（3） 读取软件包的内容，通过加密因子使用 AES256 的解密方式（与平台对应）还原数据，并写入到解密后的文件（oriFIle）中，写入成功则进入下一步，不成功则退出遍历；

（4） 校验还原后软件包的摘要，通过 Security 模块计算 oriFile 的摘要 realOriHash，比较 readOriHash 与 oriHash，一致进入下一步，不一致退出遍历；

（5） 存在 ECU 软件包解密失败，删除已下载的软件包并反馈 HMI“准备环境失败：升级包解密失败，请重试”，同时退出安装，上报服务器安装结束；

（6） 所有软件包解密成功后进入下一步流程；

6. 车辆升级前置条件二次校验

升级包验签解密成功后， UC-Master 提取存储在本地的升级策略文件中的各项条件请求 OTA-MASTER 获取车辆状态，进行升级前的二次校验。

（1） UC-Master 读取升级策略文件中的“车辆升级前置条件”；

（2） UC-Master 请求 OTA-MASTER 获取车辆状态；

（3） OTA-MASTER 按照升级策略文件中的各项条件，读取车辆状态；

（4） OTA-MASTER 读取车辆状态，包括车速，档位等信息；

（5） OTA-MASTER 将读取的车辆当前的状态反馈给 UC-Master；

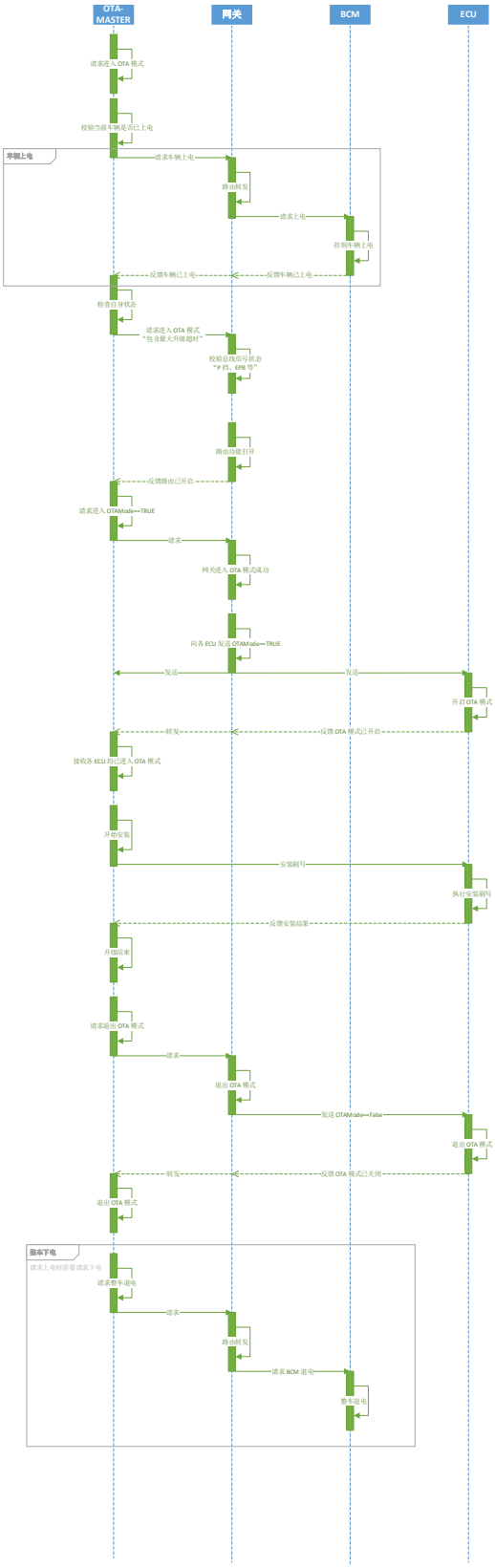
（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 对比完成，将对比结果信息同步给 HMI，如果有条件不满足，将反馈 HMI“准备环境失败：车辆条件不满足。请稍后再试” 同时退出安装，上报服务器安装结束。如果对比完成全部满足，进入 OTA 模式；

7. OTA 模式

为保证车辆升级过程中处于安全、稳定和优质体验的状态下，车辆正式升级前，UC-Master 调用 OTA-MASTER 进入 OTA 模式的接口，OTA-MASTER 发送进入 OTA 模式的请求至 CGM，从而使整车进入 OTA 模式。

（1） 流程图



（2） 流程描述

a. UC-Master 请求 OTA-MASTER 进入 OTA 模式；

b. OTA-MASTER 检查当前车辆是否上电；

c. 若车辆未上电，则请求网关转发上电指令控制 BCM 使整车处于上电状态；

d. 车辆上电状态下，OTA-MASTER 检查自身状态是否可以进入 OTA 模式；

e. OTA-MASTER 请求网关进入 OTA 模式，并发送本次升级最大超时时间；

f. 网关校验总线信号状态；

g. 网关打开路由功能并反馈 OTA-MASTER 路由已开启；

h. OTA-MASTER 请求进入 OTAMode==TRUE；

i. 网关进入 OTA 模式成功并向各 ECU 发送 OTAMode==TRUE；

j. 各 ECU 开启 OTA 模式并经由网关向 OTA-MASTER 反馈自身 OTA 模式已开启；

k. OTA-MASTER 接收各 ECU 已进入 OTA 模式；

l. OTA-MASTER 开始执行安装进程并对各 ECU 进行升级；

m. 各 ECU 报告自身安装状态；

n. 升级结束后，OTA-MASTER 请求退出 OTA 模式；

o. 网关向各 ECU 发送 OTAMode==FALSE；

p. 各 ECU 退出 OTA 模式；

q. 各 ECU 反馈 OTA 模式已关闭；

r. OTA 模式退出 OTA 模式；

s. 若开始流程中包含车辆上电操作，则此时需要 OTA-MASTER 经由网关请求 BCM 整车退电；

（3） 特别说明

a. 预约安装模式下，预约时间到达后，OTA-MASTER 唤醒 UC-Master 执行安装，并检查车辆是否已上电，若车辆未上电，则 OTA-MASTER 先请求上下电模块将车辆保持在上电状态，之后再校验车辆前置条件，前置条件校验通过后准备进入 OTA 模式；

b. 需要细化 TBOX 此时需要校验的总线信号状态，TBOX 的工作状态（如不能处于远程诊断/控制进程，不能处于通话中等）；

c. 需要与主机厂细化，哪些信号在 CGM 进入 OTA 模式前/后是可以被路由的，哪些指令在 OTA 模式前/后是可以被路由的；

d. 需要细化 CGM 此时需要校验的总线信号状态，如 P 档，EPB 状态，自身解锁状态，电源等；

e. 需要与各模块及子系统细化，在收到 OTAModeStatus==True 后，需要关闭哪些功能，进入哪些工作状态。优先处理整车电源与三电系统，保证车辆进入 OTA 模式后的锁止状态；

f. OTA Master 需要确认

i. 所有模块置位内部 OTA 模式标志位为 True；

ii. 所有 target ECU 支持自身进行 OTA 升级；

iii. 所有 target ECU 支持其他模块进行 OTA 升级；

（3） OTA 模式功能定义

本章节内容仅作为基础版本作为整车厂参考，用以要求在 OTA 模式下各 ECU 功能释放与屏蔽，在最终确定前，可能会被持续更新。

模块名称	功能释放	功能屏蔽	要求
车机	车机需要记忆所有设置项，在 OTA 升级结束时，恢复设置项的内容	蓝牙通话、功放、媒体、影像、语音交互（语音唤醒、语音识别、语音对话、语音控制）、手势识别、AR-HUD、车窗投影、Audio 音响、控制输入（尾门、方向盘管柱、左右前后门开关、换挡杆、驻车开关、组合开关、座椅调节、危险警告、中控锁、方向盘开关、中控台开关面板）、多媒体娱乐、蓝牙电话、行车记录系统、手机无线充电、Navigation 导航、DMS 驾驶员监控系统、车内监控子系统、电子后视镜	远程升级、预约升级时保证车机屏幕不点亮，监测到左前门打开时再点亮
仪表		仪表禁止报警灯显示	
网关		禁止路由转发 OBD 接口的诊断报文；	

		停止应用报文路由。（除 OTA 必须的应用报文外）	
远控终端		无法使用远程控制、数字钥匙、数据上传、CALL 类功能	
档位控制器		禁止换挡电磁阀开启； 禁止发出档位控制单元发出换挡请求； 发动机处于怠速且车速为 0 时、Bootloader 模式下、硬复位复位过程中，保持 P 档状态不变； 不响应换挡动作，即拨换挡杆时，不发送档位变化的信号，保持档位处于 P 档	
制动系统	驻车制动控制子系统 电子手刹（静态夹禁、热盘再夹紧、液压辅助请求	发动机处于怠速且车速为 0 时、Bootloader 模式下、硬复位复位过程中，保持驻车制动状态不变	
车身域控制器		启动按钮屏蔽，遥控启动、远程启动屏蔽，OTA 状态期间，屏蔽灯光（除双闪）、雨刮功能，操作开关不响应灯光雨刮	
电源模式	保持当前电源模式不变	禁止用户手动切换电源模式	
驻车辅助	在 OTA 刷写技术后，需恢复到 OTA 升级前的相关自身设置项或状态（驻车辅助系统探头配置类型）	不响应驻车辅助功能，即驻车辅助系统不探测障碍物，蜂鸣器不鸣响，驻车辅助系统的工作指示灯不点亮	
低功耗		禁止后视镜加热输出；	

		禁止方向盘加热输出； 禁止座椅通风、座椅加热和座椅调节输出； 禁止鼓风机输出。	
灯光系统	车内灯光常量	背光输出禁止； 氛围灯输出禁止； 报警灯输出禁止； 位置灯输出禁止； 外部灯光系统禁止（远光灯、近光灯等）	
防盗	保持上电不解防功能		
门窗控开关	始终保持物理方式开锁	车门、车窗、尾门、天窗保持关闭	
方向盘开关组		方向盘的开关所有功能屏蔽（方向盘开关有哪些按键，自动驾驶/辅助驾驶等相关功能/音量/FM/全景影像等需要屏蔽）	
中控台开关组		中控台开关屏蔽所有开关功能（音量/重启/空调自动/空调关闭/前除霜/整车控制器模式等）	
整车控制器	如果接收到来自空调、电池管理器、充配电总成、电机控制器的冷却风扇和水泵的需求，整车控制器最大以 50%的占空比控制器风扇和水泵工作； 相关的外设（风扇、水泵）不能记录通讯故障，保持原状态	车辆无动力输出，不论油门深度怎么变化，档位保持在 P 档；	

热管理控制器		进入 OTA 时，如果空调处于打开状态，空调制冷或制热功能关闭，鼓风机关闭、空调面板关闭、电子风扇需求无效，在整个 OTA 期间，空调功能不响应，保持关闭状态； 进入 OTA 时，如果空调功能是关闭的，OTA 期间，空调功能不响应，保持关闭状态，包括空调面板的功能也是关闭的（前后空调面板都关闭）； 进入 OTA 时，如果 BMS 有压缩机冷却或加热需求，要求压缩机降功率输出，最大以 50%的功率输出（低于 50%，以实际需求输出），OTA 期间，如果 BMS 冷却或加热需求停止，则关闭压缩机； 进入 OTA 时，如果 BMS 无压缩机冷却或加热需求，则制冷和加热压缩机关闭，在 OTA 期间 BMS 有压缩机冷却或加热需求，热管理控制器响应，最大以 50%的功率输出（低于 50%，以实际需求输出）； 进入 OTA 时，前后除霜功能是打开的，将除霜功能关闭， 在整个 OTA 期间，除霜功能不响应，保持关闭状态，	

		进入 OTA 时，如果除霜功能是关闭的，OTA 期间，除霜功能不响应，保持关闭状态；	
电池管理控制器	动力电池在进行充放电时，需反馈充放电状态；需要响应车载终端的需求； 在进行低压模块刷写时，需要高压系统能够进入放电状态，由动力电池放电给低压用电器供电，动力电池需将主接触器吸合的状态发出，以便 DCDC 进行降压给低压用电器供电；	在进入 OTA 状态时，如未处于放电状态，则在 OTA 状态期间，不响应插充电枪充电和对外放电，只响应车载终端的请求，如果 OTA 期间，进行了插入充电抢，则 OTA 升级结束后，再进行充电； 交流充电时，预约充电和预约 OTA，预约充电时间到，先充电，OTA 时间到，退出充电，进行 OTA，OTA 结束后，再进入充电，直流充电，预约充电和预约 OTA 哪个时间先到，先执行哪个，另一个不执行； 在 OTA 状态期间，在进行高压模块刷写时，动力电池需要断开	
DCDC	接收来自动力电池管理的降压请求和退出降压的命令，并将自身的状态发出来给车载终端和动力电池管理器		
蓄电池	刷写高压模块时，需要蓄电池给车上的用电器供电，需要反馈自身的类型、电量信息、温度信息；	蓄电池如果在智能充电状态，需将智能充电状态发出来，在进入 OTA 状态时，响应车载终端的要求，退出智能充电状态，如未处于智能充电状态，则在 OTA 状态	

		期间，不再进入智能充电， OTA 升级结束后，再恢复正常工作状态；	
座椅	座椅调节、座椅记忆功能正常，OTA 状态退出后，恢复到正常模式	座椅控制模块的通风、加热、按摩、震动功能屏蔽	
其他			

6.2.3.3 安装过程

安装过程是指车辆进入 OTA 模式后，执行升级包传输和安装的过程。按照升级顺序，在相应的 ECU 需要被安装时，由 OTA-MASTER 进行软件包传输（传输方式为 DoIP 的 ECU，其软件包需先传输到 GW，在转发至其本身）。智能键传输后会进行整包刷写或差分还原过程，非智能件传包即为刷写。

在安装阶段发生任何状态变更时，均及时上报云端。

安装状态	状态定义	状态约定
待升级	表示升级包已经下载成功，可以启动升级过程	软件包下载成功待安装
触发升级	表示用户点击立即升级；此时 APP 侧需要进入禁止操作环节	用户点击立即升级
条件不满足	表示进行升级条件判断时，判断结果为失败	升级前置条件不满足
取消升级	在倒计时阶段，需要执行的远程升级、预约升级被 IHU 侧取消	用户点击取消升级
开始升级	表示车辆具备升级条件，正式进入升级环节	升级中
升级完成	表示升级过程完成，所有待升级 ECU 均升级成功	全部安装成功
升级未完成	表示升级过程完成，待升级 ECU 全部没有升级至目标版本	全部回滚成功
升级失败	表示升级过程完成，待升级 ECU 出现回滚失败	存在回滚失败

1. 安装升级包

（1） UC-Master 读取升级策略文件中的“零件升级顺序”；

a. 读取失败则退出安装，反馈 HMI“升级失败：安装条件不满足。请稍后再试”，并上报服务器本次安装结果；

（2） UC-Master 将获取到的零件升级顺序报告 OTA-MASTER，OTA-MASTER 按照升级顺序循环安装各 ECU。循环内部流程如下：

a. OTA-MASTER 记录当前安装的 ECU 开始升级时间；

b. OTA-MASTER 获取当前 ECU 的目标版本软件包绝对路径并判断该软件包是否存在，若文件不存在进入 ECU 安装失败流程，上报服务器本次安装失败，反馈 HMI“升级失败：升级包不存在。请重新检测”；

c. OTA-MASTER 调用安装接口，传入 ECU 基本信息和软件包路径，若接口调用失败进入 ECU 安装失败流程，上报服务器本次安装失败，反馈 HMI“升级失败：安装引导失败。请稍后再试”；

d. OTA-MASTER 将 ECU 的状态改为安装中，等待指定的安装代理程序反馈进度和结果；

a) OTA-MASTER 发送刷写指令给 ECU（整包或差分）；

b) ECU 收到指令后执行刷写动作，并通过预设接口将刷写进度报告给 OTA-MASTER；

e. OTA-MASTER 将安装进度和安装结果同步给 UC-Master；

f. UC-Master 收到安装进度和结果后，将进度和结果信息转发给 HMI（非静默安装）；

（3） 第一个 ECU 安装动作执行完成，OTA-MASTER 按照升级策略文件中的升级顺序继续安装剩余 ECU（重复上述（1）-（2）步骤）；

（4） 在安装过程中，OTA-MASTER 收到安装失败结果、未收到结果，进入 ECU 安装失败流程；

2. 安装失败重试

（1） 安装失败时，若未进入刷写流程，如上述流程中的升级文件不存在和安装接口调用失败则 UC-MASTER 将 ECU 的安装结果改为安装失败，记录 ECU 安装结束时间，终止安装流程，并上报服务器安装结束；

（2） 已进入刷写流程，UC-MASTER 将 ECU 的安装结果改为安装失败，同时将已重试次数加 1，若已重试次数小于升级策略文件中的最大重试次数则将 ECU 的安装状态改为初始状态并进行重试（同安装升级包过程，利用源版本软件包进行刷写）；

（3） 若已重试次数等于最大重试次数，则将 ECU 的安装状态改为安装结束，记录 ECU 的安装结束时间，需要回滚则进入 ECU 回滚流程，无需回滚则终止安装流程，并上报服务器安装结束；

3. 重试失败回滚

（1） ECU 安装、重试失败后，为了保证 ECU 正常工作，可以选择将 ECU 回退为源版本，UC-Master 根据升级策略文件中该 ECU 的“回滚”信息，确认是否执行回退流程；

（2） OTA-MASTER 对该安装、重试失败的 ECU 执行回滚动作（流程同安装升级包过程，利用源版本软件包进行刷写）；

（3） ECU 回滚操作只进行一次，若回滚失败，UC-Master 将 ECU 状态改为回滚结束，将 ECU 的回滚结果改为回滚失败，终止安装流程，并上报服务器安装结束；

（4） 当该升级失败的零件回滚成功后，其余已升级成功的零件也需要回退；

6.2.3.4 安装结果

安装动作执行完毕后进入安装结束流程，该流程依次执行安装结果确认、上报安装结果给 OTA 平台、更新状态机等操作。

1. 安装结果确认

UC-Master 遍历本次安装的的 ECU 列表，对每一个 ECU 的安装结果进行确认，如果 ECU 的安装结果是安装成功，则获取 ECU 当前的版本号并与本地升级策略文件中定义的目标版本比对，一致则认为确实安装成功，否则认为安装失败。如果 ECU 的安装结果是除安装成功以外的状态，则认为本次任务升级失败。

车辆安装结果为升级成功和升级失败，零件安装结果分为升级成功、升级失败回滚成功、升级失败回滚失败。

2. 上报安装结果

安装结果确认后，UC-Master 调用上报模块的安装上报接口，上报安装结果给 OTA 平台。

3. 更新 OTA 状态

安装结束后 UC-Master 需要更新状态机，车辆升级状态不满足、升级包解密失败造成的安装结束，OTA 回到下载完成状态，车主仍然可以再次触发安装。其余原因造成的安装结束，OTA 状态都将置为初始状态，并删除安装上下文同时上传日志。

6.2.4 手机 APP 立即安装

6.2.4.1 安装触发

手机 APP 立即安装是指升级包下载完成后，用户主动在手机 APP 上在点击【立即安装】触发安装进程。

用户点击【立即安装】后，进入免责声明界面，用户确认后安装指令经过云端发送至 TBOX，此时需要 TBOX 判断整车是否处于上电状态（车辆防盗系统是否启动，座椅压力感应是否激活）。若整车未上电则手机 APP 执行后续升级操作（进入安装准备）；若整车已上电则反馈手机 APP“请在车机端进行升级”。

在升级过程中，UC-Master 按照立即安装的逻辑将安装进度、状态等传递给 UC-Slave，以保障升级过程中，检测到车主进入车辆后，车机屏幕及时点亮，向用户展示当前升级状态。

6.2.4.2 安装准备

1. 车辆升级前置条件校验（由手机触发）

安装触发后， OTA-MASTER 首先请求上下电模块将整车上电（车辆未上电时），再通知 UC-Master 执行安装准备。UC-Master 提取存储在本地的升级策略文件中以及远程升级必要判断（防盗、座椅）的车辆前置条件请求 OTA-MASTER 获取车辆状态。

（1） （1）-（5）参考“立即安装>安装准备>车辆前置条件校验”...

（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 对比完成，如果有部分条件不满足，UC-Master 上报 OTA 平台安装失败，原因：车辆条件不满足。并终止后续动作执行，本次手机 APP 立即安装结束；

车辆升级条件（举例）
电源状态（整车使用动力电池供电状态）

车速（0-5）
蓄电池电压（TBD）
蓄电池电量（TBD）
动力电池电量（TBD）
档位（P 档）
手刹状态/EPB（UP）
整车未充电
防盗系统（激活）
座椅压力感应（激活）

2. 升级任务有效性校验

车辆升级前置条件校验通过后，UC-Master 向云端发起任务有效性校验，校验当前待安装任务是否仍然有效。

注：本项目一期阶段不涉及“任务有效的判断”，但考虑到扩展性，保留此项。

（1） （1）-（5）参考“立即安装>安装准备>升级任务有效性校验”；

（6） UC-Master 接收到服务器返回消息；

a. 若任务无效，UC-Master 上报 OTA 平台安装失败，原因：任务失效。并终止后续动作执行，本次手机 APP 立即安装结束；

（7） 若任务有效，则进入零件信息校验过程；

3. 零件版本信息校验

任务有效性校验通过后，UC-Master 校验待升级零件版本信息是否与升级策略中一致。

（1） UC-Master 读取升级策略文件中的待升级零件源版本信息；

（2） UC-Master 请求 OTA-MASTER 获取当前待升级零件实际版本信息；

（3） OTA-MASTER 获取零件版本信息失败（重复获取 3 次，每次间隔 3/5/8s），UC-Master 上报 OTA 平台安装失败，原因：零件版本信息获取失败。并终止后续动作执行，本次手机 APP 立即安装结束；

（4） UC-Master 接收 OTA-MASTER 反馈的当前零件实际版本信息，并对比二者是否一致；

a. 若无法匹配，UC-Master 上报 OTA 平台安装失败，原因：零件版本信息获取失败。并终止后续动作执行，本次手机 APP 立即安装结束；

（5） 升级策略文件中的零件源版本与实际获取的当前零件版本一致，则进入软件包校验过程；

4. 软件包验签

零件版本信息校验通过后，UC-Master 校验软件包。

（1） *（1）-（5）参考“立即安装>安装准备>软件包验签”...*

（6） 存在 ECU 软件包验签失败，删除已下载的软件包, UC-Master 上报 OTA 平台安装失败，原因：验签失败。并终止后续动作执行，本次手机 APP 立即结束；

（7） 所有软件包验签成功后进入解密流程；

5. 软件包解密

软件包信息校验通过后，UC-Master 对加密软件包进行解密。

（1） *（1）-（4）参考“立即安装>安装准备>软件包解密”...*

（5） 存在 ECU 软件包解密失败，删除已下载的软件包，UC-Master 上报 OTA 平台安装失败，原因：软件包解密失败。并终止后续动作执行，本次手机 APP 立即结束；

（6） 所有软件包解密成功后进入下一步流程；

6. 车辆升级前置条件二次校验

升级包验签解密成功后， UC-Master 提取存储在本地的升级策略文件中的各项条件请求 OTA-MASTER 获取车辆状态，进行升级前的二次校验。

（1） *（1）-（5）参考“立即安装>安装准备>车辆前置条件二次校验”;*

（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 对比完成，如果有部分条件不满足，UC-Master 上报 OTA 平台安装失败，原因：车辆条件不满足。并终止后续动作执行，本次手机 APP 立即安装结束；

（7） 车辆条件校验成功，则进入 OTA 模式；

7. OTA 模式

同 6.2.3.2 章节“立即安装>安装准备”

6.2.4.3 安装过程

安装过程是指车辆进入 OTA 模式后，执行升级包传输和安装的过程。按照升级顺序，在相应的 ECU 需要被安装时，由 OTA-MASTER 进行软件包传输（传输方式为 DoIP 的 ECU，其软件包需先传输到 GW，在转发至其本身）。智能件传输后会进行整包刷写或差分还原过程，传统件传包即为刷写。

1. 安装升级包

（1） UC-Master 读取升级策略文件中的“零件升级顺序”；

a. 读取失败则退出安装，UC-Master 上报 OTA 平台安装失败，原因：零件升级顺序获取失败。并终止后续动作执行，本次手机 APP 立即安装结束；

（2） UC-Master 将获取到的零件升级顺序报告 OTA-MASTER，OTA-MASTER 按照升级顺序循环安装各 ECU。循环内部流程如下：

a. OTA-MASTER 记录当前安装的 ECU 开始升级时间；

b. OTA-MASTER 获取当前 ECU 的目标版本软件包绝对路径并判断该软件包是否存在，若文件不存在进入 ECU 安装失败流程，UC-Master 上报 OTA 平台安装失败，原因：升级文件不存在。并终止后续动作执行，本次手机 APP 立即安装结束；

c. OTA-MASTER 调用安装接口，传入 ECU 基本信息和软件包路径，若接口调用失败进入 ECU 安装失败流程，UC-Master 上报 OTA 平台安装失败，原因：安装引导失败。并终止后续动作执行，本次手机 APP 立即安装结束；

b. OTA-MASTER 将 ECU 的状态改为安装中，等待指定的安装代理程序反馈进度和结果；

a) OTA-MASTER 发送刷写指令给 ECU（整包或差分）；

b) ECU 收到指令后执行刷写动作，并通过预设接口将刷写进度报告给 OTA-MASTER；

c. OTA-MASTER 将安装进度和安装结果同步给 UC-Master；

（3） 第一个 ECU 安装动作执行完成，OTA-MASTER 按照升级策略文件中的升级顺序继续安装剩余 ECU（重复上述（1）-（2）步骤）；

（4） 在安装过程中，OTA-MASTER 收到安装失败结果、未收到结果，进入 ECU 安装失败流程；

2. 安装失败重试

（1） 安装失败时，若未进入刷写流程，如上述流程中的升级文件不存在和安装接口调用失败则 UC-MASTER 将 ECU 的安装结果改为安装失败，记录 ECU 安装结束时间，终止安装流程，并上报服务器安装结束；

（2） 已进入刷写流程，UC-MASTER 将 ECU 的安装结果改为安装失败，同时将已重试次数加 1，若已重试次数小于升级策略文件中的最大重试次数则将 ECU 的安装状态改为初始状态并进行重试（同安装升级包过程，利用源版本软件包进行刷写）；

（3） 若已重试次数等于最大重试次数（默认 3 次），则将 ECU 的安装状态改为安装结束，记录 ECU 的安装结束时间，需要回滚则进入 ECU 回滚流程，无需回滚则终止安装流程，并上报服务器安装结束；

3. 重试失败回滚

（1） ECU 安装、重试失败后，为了保证 ECU 正常工作，可以选择将 ECU 回退为源版本，UC-Master 根据升级策略文件中该 ECU 的“回滚”信息，确认是否执行回退流程；

（2） OTA-MASTER 对该安装、重试失败的 ECU 执行回滚动作（流程同安装升级包过程，利用源版本软件包进行刷写）；

（3） ECU 回滚操作只进行一次，若回滚失败，UC-Master 将 ECU 状态改为回滚结束，将 ECU 的回滚结果改为回滚失败，终止安装流程，并上报服务器安装结束；

（4） 当该升级失败的零件回滚成功后，其余已升级成功的零件也需要回退；

6.2.4.4 安装结果

安装动作执行完毕后进入安装结束流程，该流程依次执行安装结果确认、上报安装结果给 OTA 平台、更新状态机等操作。

1. 安装结果确认

UC-Master 遍历本次安装的的 ECU 列表，对每一个 ECU 的安装结果进行确认，如果 ECU 的安装结果是安装成功，则获取 ECU 当前的版本号并与本地升级策略文件中定义的目标版本比对，一致则认为确实安装成功，否则认为安装失败。如果 ECU 的安装结果是除安装成功以外的状态，则认为本次任务升级失败。

车辆安装结果为升级成功和升级失败，零件安装结果分为升级成功、升级失败回滚成功、升级失败回滚失败。

2. 上报安装结果

安装结果确认后，UC-Master 调用上报模块的安装上报接口，上报安装结果给 OTA 平台（参考 7.2.2.2 章节）。

3. 更新 OTA 状态

安装结束后 UC-Master 需要更新状态机，车辆升级状态不满足、升级包解密失败造成的安装结束，OTA 回到下载完成状态，下次预约安装仍然可以再次触发。其余原因造成的安装结束，OTA 状态都将置为初始状态，并删除安装上下文同时上传日志（参考 7.2.2.4 章节）。

6.2.5 预约安装

6.2.5.1 安装触发

1. 车机端预约

预约安装是指车主在软件包下载成功后，选择预约时间并在预约时间到达后车辆自动进入安装的过程。

车主在车机端选择预约时间后，UC-Master 将该时间上报至 OTA 服务器并发送至 OTA-MASTER，由 OTA-MASTER 维护计时器，时间到达后自动触发安装（预约时间到达后，OTA-MASTER 先请求上下电模块将整车上电，再通知 UC-Master）。

2. 手机 APP 预约

手机 APP 预约安装是指车主在手机 APP 端选择预约时间后通过云端同步至 TBOX，在预约时间到达后完成自动化安装的过程。

车主在手机 APP 端选择预约时间后，通过云端将预约时间发送至 TBOX，若 TBOX 处于休眠状态时，需要唤醒 TBOX，再将配置同步至 TBOX，TBOX 再将预约时间配置项发送给 UC-Master（自身留存），待 HU 上电后，再经过 UC-Slave 同步（重试 3 次)至 HU 作为展示；当云端同步配置至 TBOX 失败时，需要返回配置失败至 APP；

3. 预约处理

预约时间到达后，若车辆当前已上电，则 TBOX 同步升级请求至 HU，HU 弹框提示等待用户操作指令。当 TBOX 收到 HU 的立即升级指令则开始升级。如 HU 返回取消指令或超时消息，则取消升级，并同步取消升级消息至云端，云端同步消息至 APP。

若当前车辆未上电，则执行如下预约升级流程。

6.2.5.2 安装准备

1. 车辆升级前置条件校验

安装触发后， OTA-MASTER 首先请求上下电模块将整车上电，再通知 UC-Master 执行安装准备。UC-Master 提取存储在本地的升级策略文件中的车辆前置条件请求 OTA-MASTER 获取车辆状态。

（1） （1）-（5）参考“立即安装>安装准备>车辆前置条件校验”...

（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 对比完成，如果有部分条件不满足，UC-Master 上报 OTA 平台安装失败，原因：车辆条件不满足。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：车辆条件不满足。请选择其他时间”；

车辆升级条件（举例）
电源状态（整车使用动力电池供电状态）
车速（0-5）
蓄电池电压（TBD）
蓄电池电量（TBD）
动力电池电量（TBD）
档位（P 档）
手刹状态/EPB（UP）
整车未充电
防盗系统（激活）
座椅压力感应（激活）

2. 升级任务有效性校验

车辆升级前置条件校验通过后，UC-Master 向云端发起任务有效性校验，校验当前待安装任务是否仍然有效。

注：本项目一期阶段不涉及“任务有效的判断”，但考虑到扩展性，保留此项。

（1） （1）-（5）参考“立即安装>安装准备>升级任务有效性校验”；

（6） UC-Master 接收到服务器返回消息；

a. 若任务无效，UC-Master 上报 OTA 平台安装失败，原因：任务失效。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：任务失效。请等待后续更新推送”；

（7） 若任务有效，则进入零件信息校验过程；

3. 零件版本信息校验

任务有效性校验通过后，UC-Master 校验待升级零件版本信息是否与升级策略中一致。

（1） UC-Master 读取升级策略文件中的待升级零件源版本信息；

（2） UC-Master 请求 OTA-MASTER 获取当前待升级零件实际版本信息；

（3） OTA-MASTER 获取零件版本信息失败（重复获取 3 次，每次间隔 3/5/8s），UC-Master 上报 OTA 平台安装失败，原因：零件版本信息获取失败。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：升级环境不满足。请选择其他时间再试”；

（4） UC-Master 接收 OTA-MASTER 反馈的当前零件实际版本信息，并对比二者是否一致；

a. 若无法匹配，UC-Master 上报 OTA 平台安装失败，原因：零件版本信息获取失败。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：升级环境不满足。请选择其他时间再试”；

（5） 升级策略文件中的零件源版本与实际获取的当前零件版本一致，则进入软件包校验过程；

4. 软件包验签

零件版本信息校验通过后，UC-Master 校验软件包。

（1） （1）-（5）参考“立即安装>安装准备>软件包验签”...

（6） 存在 ECU 软件包验签失败，删除已下载的软件包, UC-Master 上报 OTA 平台安装失败，原因：验签失败。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：软件包不可信。请重新下载”；

（7） 所有软件包验签成功后进入解密流程；

5. 软件包解密

软件包信息校验通过后，UC-Master 对加密软件包进行解密。

（1） （1）-（4）参考“立即安装>安装准备>软件包解密”...

（5） 存在 ECU 软件包解密失败，删除已下载的软件包，UC-Master 上报 OTA 平台安装失败，原因：软件包解密失败。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：升级环境不满足。请选择其他时间再试”；

（6） 所有软件包解密成功后进入下一步流程；

6. 车辆升级前置条件二次校验

升级包验签解密成功后， UC-Master 提取存储在本地的升级策略文件中的各项条件请求 OTA-MASTER 获取车辆状态，进行升级前的二次校验。

（1） （1）-（5）参考“立即安装>安装准备>车辆前置条件二次校验”;

（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 对比完成，如果有部分条件不满足，UC-Master 上报 OTA 平台安装失败，原因：车辆条件不满足。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：车辆条件不满足。请选择其他时间”；

（7） 车辆条件校验成功，则进入 OTA 模式；

7. OTA 模式

同 6.2.3.2 章节“立即安装>安装准备”

6.2.5.3 安装过程

安装过程是指车辆进入 OTA 模式后，执行升级包传输和安装的过程。按照升级顺序，在相应的 ECU 需要被安装时，由 OTA-MASTER 进行软件包传输（传输方式为 DoIP 的 ECU，其软件包需先传输到 GW，在转发至其本身）。智能键传输后会进行整包刷写或差分还原过程，非智能件传包即为刷写。

4. 安装升级包

（1） UC-Master 读取升级策略文件中的“零件升级顺序”；

a. 读取失败则退出安装，UC-Master 上报 OTA 平台安装失败，原因：零件升级顺序获取失败。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：升级环境不满足。请选其他时间再试”；

（2） UC-Master 将获取到的零件升级顺序报告 OTA-MASTER，OTA-MASTER 按照升级顺序循环安装各 ECU。循环内部流程如下：

a. OTA-MASTER 记录当前安装的 ECU 开始升级时间；

b. OTA-MASTER 获取当前 ECU 的目标版本软件包绝对路径并判断该软件包是否存在，若文件不存在进入 ECU 安装失败流程，UC-Master 上报 OTA 平台安装失败，原因：升级文件不存在。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：升级环境不满足。请选其他时间再试”；

c. OTA-MASTER 调用安装接口，传入 ECU 基本信息和软件包路径，若接口调用失败进入 ECU 安装失败流程，UC-Master 上报 OTA 平台安装失败，原

因：安装引导失败。并终止后续动作执行，本次预约安装结束，并在下次车机开机时提醒车主“预约安装失败：升级环境不满足。请选其他时间再试”；

d. OTA-MASTER 将 ECU 的状态改为安装中，等待指定的安装代理程序反馈进度和结果；

a) OTA-MASTER 发送刷写指令给 ECU（整包或差分）；

b) ECU 收到指令后执行刷写动作，并通过预设接口将刷写进度报告给 OTA-MASTER；

e. OTA-MASTER 将安装进度和安装结果同步给 UC-Master；

（3） 第一个 ECU 安装动作执行完成，OTA-MASTER 按照升级策略文件中的升级顺序继续安装剩余 ECU（重复上述（1）-（2）步骤）；

（4） 在安装过程中，OTA-MASTER 收到安装失败结果、未收到结果，进入 ECU 安装失败流程；

5. 安装失败重试

（1） 安装失败时，若未进入刷写流程，如上述流程中的升级文件不存在和安装接口调用失败则 UC-MASTER 将 ECU 的安装结果改为安装失败，记录 ECU 安装结束时间，终止安装流程，并上报服务器安装结束；

（2） 已进入刷写流程，UC-MASTER 将 ECU 的安装结果改为安装失败，同时将已重试次数加 1，若已重试次数小于升级策略文件中的最大重试次数则将 ECU 的安装状态改为初始状态并进行重试（同安装升级包过程，利用源版本软件包进行刷写）；

（3） 若已重试次数等于最大重试次数，则将 ECU 的安装状态改为安装结束，记录 ECU 的安装结束时间，需要回滚则进入 ECU 回滚流程，无需回滚则终止安装流程，并上报服务器安装结束；

6. 重试失败回滚

（1） ECU 安装、重试失败后，为了保证 ECU 正常工作，可以选择将 ECU 回退为源版本，UC-Master 根据升级策略文件中该 ECU 的“回滚”信息，确认是否执行回退流程；

（2） OTA-MASTER 对该安装、重试失败的 ECU 执行回滚动作（流程同安装升级包过程，利用源版本软件包进行刷写）；

（3） ECU 回滚操作只进行一次，若回滚失败，UC-Master 将 ECU 状态改为回滚结束，将 ECU 的回滚结果改为回滚失败，终止安装流程，并上报服务器安装结束；

（4） 当该升级失败的零件回滚成功后，其余已升级成功的零件也需要回退；

6.2.5.4 安装结果

安装动作执行完毕后进入安装结束流程，该流程依次执行安装结果确认、上报安装结果给 OTA 平台、更新状态机等操作。

1. 安装结果确认

UC-Master 遍历本次安装的的 ECU 列表，对每一个 ECU 的安装结果进行确认，如果 ECU 的安装结果是安装成功，则获取 ECU 当前的版本号并与本地升级策略文件中定义的目标版本比对，一致则认为确实安装成功，否则认为安装失败。如果 ECU 的安装结果是除安装成功以外的状态，则认为本次任务升级失败。

车辆安装结果为升级成功和升级失败，零件安装结果分为升级成功、升级失败回滚成功、升级失败回滚失败。

特别地，预约安装场景下，安装成功或失败后，需要在下次车机开机时提醒用户。

2. 上报安装结果

安装结果确认后，UC-Master 调用上报模块的安装上报接口，上报安装结果给 OTA 平台（参考 7.2.2.2 章节）。

3. 更新 OTA 状态

安装结束后 UC-Master 需要更新状态机，车辆升级状态不满足、升级包解密失败造成的安装结束，OTA 回到下载完成状态，下次预约安装仍然可以再次触发。其余原因造成的安装结束，OTA 状态都将置为初始状态，并删除安装上下文同时上传日志（参考 7.2.2.3 章节）。

6.2.6 静默安装

6.2.6.1 安装触发

静默安装是指软件包下载成功后，OTA-MASTER 按照服务器配置的静默安装时间（该时间在新版本检测成功时已经由升级策略文件下发，由 UC-Master 转发至 OTA-MASTER，由 OTA-MASTER 维护计时器）通知 UC-Master 进行安装的过程。

静默时间到达后，TBOX 判断当前车辆是否处于整车上电状态。若已处于整车上电或车机上电状态（此时 TBOX 由蓄电池或动力电池供电），则放弃本次静默升级，等待后续触发；若

TBOX 未上电（TBOX 自身供电）。则进入静默升级流程。

6.2.6.2 安装准备

1. 车辆升级前置条件校验

安装触发后， OTA-MASTER 首先请求上下电模块将整车上电，再通知 UC-Master 执行安装准备。UC-Master 提取存储在本地的升级策略文件中的车辆前置条件请求 OTA-MASTER 获取车辆状态。

（1） （1）-（5）参考“立即安装>安装准备>车辆前置条件校验”...

（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 对比完成，如果有部分条件不满足，UC-Master 上报 OTA 平台安装失败，原因：车辆条件不满足。并终止后续动作执行，本次静默安装结束；

（7） 车辆条件校验成功，则进入升级任务有效性校验；

车辆升级条件（举例）
电源状态（整车使用动力电池供电状态）
车速（0-5）
蓄电池电压（TBD）
蓄电池电量（TBD）
动力电池电量（TBD）
档位（P 档）
手刹状态/EPB（UP）
整车未充电
防盗系统（激活）
座椅压力感应（激活）

2. 升级任务有效性校验 Validation of the upgrade task

车辆升级前置条件校验通过后，UC-Master 向云端发起任务有效性校验，校验当前待安装任务是否仍然有效。

注：本项目一期阶段不涉及“任务有效的判断”，但考虑到扩展性，保留此项。

（1） （1）-（5）参考“立即安装>安装准备>升级任务有效性校验”;

（6） UC-Master 接收到服务器返回消息；

a. 若任务无效，UC-Master 上报 OTA 平台安装失败，原因：任务失效。并终止后续动作执行，本次静默安装结束；

（7） 若任务有效，则进入零件信息校验过程；

3. 零件版本信息校验

任务有效性校验通过后，UC-Master 校验待升级零件版本信息是否与升级策略中一致。

（1） UC-Master 读取升级策略文件中的待升级零件源版本信息；

（2） UC-Master 请求 OTA-MASTER 获取当前待升级零件实际版本信息；

（3） OTA-MASTER 获取零件版本信息失败（重复获取 3 次，每次间隔 3/5/8s），UC-Master 上报 OTA 平台安装失败，原因：零件版本信息获取失败。并终止后续动作执行，本次静默安装结束；

（4） UC-Master 接收 OTA-MASTER 反馈的当前零件实际版本信息，并对比二者是否一致；

a. 若无法匹配，UC-Master 上报 OTA 平台安装失败，原因：零件版本信息获不匹配。并终止后续动作执行，本次静默安装结束；

（5） 升级策略文件中的零件源版本与实际获取的当前零件版本一致，则进入软件包校验过程；

4. 软件包验签

零件版本信息校验通过后，UC-Master 校验软件包。

（1） （1）-（5）参考“立即安装>安装准备>软件包验签”...

（6） 存在 ECU 软件包验签失败，删除已下载的软件包, UC-Master 上报 OTA 平台安装失败，原因：验签失败。并终止后续动作执行，本次静默安装结束；

（7） 所有软件包验签成功后进入解密流程；

5. 软件包解密

软件包信息校验通过后，UC-Master 对加密软件包进行解密。

（1） （1）-（4）参考“立即安装>安装准备>软件包解密”...

（5） 存在 ECU 软件包解密失败，删除已下载的软件包，UC-Master 上报 OTA 平台安装失败，原因：解密失败。并终止后续动作执行，本次静默安装结束；

（6） 所有软件包解密成功后进入下一步流程；

6. 车辆升级前置条件二次校验

升级包验签解密成功后， UC-Master 请求 OTA-MASTER 提取存储在本地的升级策略文件中的各项条件获取车辆状态，进行升级前的二次校验。

（1） （1）-（5）参考“立即安装>安装准备>车辆前置条件二次校验”;

（6） UC-Master 将当前实际车辆条件与升级策略文件中的进行比对；

a. 对比完成，如果有部分条件不满足，UC-Master 上报 OTA 平台安装失败，原因：车辆条件不满足。并终止后续动作执行，本次静默安装结束；

（7） 车辆条件校验成功，则进入 OTA 模式；

7. OTA 模式

同 6.2.3.2 章节“立即安装>安装准备”

6.2.6.3 安装过程

安装过程是指车辆进入 OTA 模式后，执行升级包传输和安装的过程。按照升级顺序，在相应的 ECU 需要被安装时，由 OTA-MASTER 进行软件包传输（传输方式为 DoIP 的 ECU，其软件包需先传输到 GW，在转发至其本身）。智能键传输后会进行整包刷写或差分还原过程，非智能件传包即为刷写。

1. 安装升级包

（1） UC-Master 读取升级策略文件中的“零件升级顺序”；

a. 读取失败则退出安装，UC-Master 上报 OTA 平台安装失败，原因：零件升级顺序获取失败。并终止后续动作执行，本次静默安装结束；

（2） UC-Master 将获取到的零件升级顺序报告 OTA-MASTER，OTA-MASTER 按照升级顺序循环安装各 ECU。循环内部流程如下：

a. OTA-MASTER 记录当前安装的 ECU 开始升级时间；

b. OTA-MASTER 获取当前 ECU 的目标版本软件包绝对路径并判断该软件包是否存在，若文件不存在进入 ECU 安装失败流程，UC-Master 上报 OTA 平台安装失败，原因：升级文件不存在。并终止后续动作执行，本次静默安装结束；

c. OTA-MASTER 调用安装接口，传入 ECU 基本信息和软件包路径，若接口调用失败进入 ECU 安装失败流程，UC-Master 上报 OTA 平台安装失败，原因：安装引导失败。并终止后续动作执行，本次静默安装结束；

d. OTA-MASTER 将 ECU 的状态改为安装中，等待指定的安装代理程序反馈进度和结果；

a) OTA-MASTER 发送刷写指令给 ECU（整包或差分）；

b) ECU 收到指令后执行刷写动作，并通过预设接口将刷写进度报告给 OTA-

MASTER；

e. OTA-MASTER 将安装进度和安装结果同步给 UC-Master；

（3） 第一个 ECU 安装动作执行完成，OTA-MASTER 按照升级策略文件中的升级顺序继续安装剩余 ECU（重复上述（1）-（2）步骤）；

（4） 在安装过程中，OTA-MASTER 收到安装失败结果、未收到结果，进入 ECU 安装失败流程；

2. 安装失败重试

（1） 安装失败时，若未进入刷写流程，如上述流程中的升级文件不存在和安装接口调用失败则 UC-MASTER 将 ECU 的安装结果改为安装失败，记录 ECU 安装结束时间，终止安装流程，并上报服务器安装结束；

（2） 已进入刷写流程，UC-MASTER 将 ECU 的安装结果改为安装失败，同时将已重试次数加 1，若已重试次数小于升级策略文件中的最大重试次数则将 ECU 的安装状态改为初始状态并进行重试（同安装升级包过程，利用源版本软件包进行刷写）；

（3） 若已重试次数等于最大重试次数，则将 ECU 的安装状态改为安装结束，记录 ECU 的安装结束时间，需要回滚则进入 ECU 回滚流程，无需回滚则终止安装流程，并上报服务器安装结束；

3. 重试失败回滚

（1） ECU 安装、重试失败后，为了保证 ECU 正常工作，可以选择将 ECU 回退为源版本，UC-Master 根据升级策略文件中该 ECU 的“回滚”信息，确认是否执行回退流程；

（2） OTA-MASTER 对该安装、重试失败的 ECU 执行回滚动作（流程同安装升级包过程，利用源版本软件包进行刷写）；

（3） ECU 回滚操作只进行一次，若回滚失败，UC-Master 将 ECU 状态改为回滚结束，将 ECU 的回滚结果改为回滚失败，终止安装流程，并上报服务器安装结束；

（4） 当该升级失败的零件回滚成功后，其余已升级成功的零件也需要回退；

6.2.6.4 安装结果

安装动作执行完毕后进入安装结束流程，该流程依次执行安装结果确认、上报安装结果给 OTA 平台、更新状态机等操作。

1. 安装结果确认

UC-Master 遍历本次安装的的 ECU 列表，对每一个 ECU 的安装结果进行确认，如果 ECU 的安装结果是安装成功，则获取 ECU 当前的版本号并与本地升级策略文件中定义的目标版本比对，一致则认为确实安装成功，否则认为安装失败。如果 ECU 的安装结果是除安装成功以外的状态，则认为本次任务升级失败。

车辆安装结果为升级成功和升级失败，零件安装结果分为升级成功、升级失败回滚成功、升级失败回滚失败。

特别地，静默安装场景下，安装失败后，需要在下次车机开机时提醒用户。

2. 上报安装结果

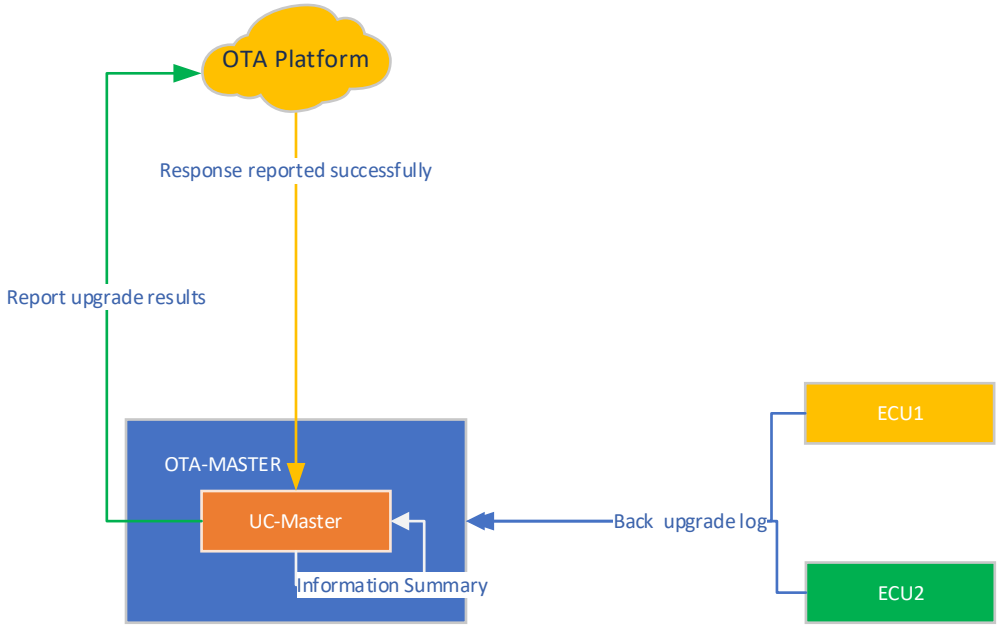
安装结果确认后，UC-Master 调用上报模块的安装上报接口，上报安装结果给 OTA 平台（参考 7.2.2.2 章节）。

3. 更新 OTA 状态

安装结束后 UC-Master 需要更新状态机，车辆升级状态不满足、升级包解密失败造成的安装结束，OTA 回到下载完成状态，下次静默升级仍然可以再次触发安装。其余原因造成的安装结束，OTA 状态都将置为初始状态，并删除安装上下文同时上传日志（详参考 7.2.2.3 章节）。

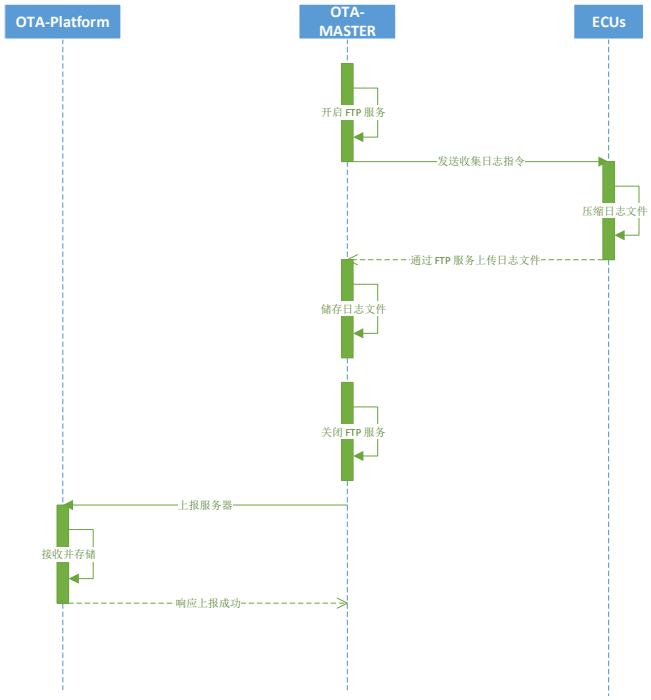
7 信息上报

7.1 业务架构图



7.2 需求规格

7.2.1 流程图



7.2.2 规格说明

7.2.2.1 车辆信息

车辆信息包括具备升级能力的 ECU 详细信息，如软件版本号、硬件版本号等，主要用于 OTA 平台展示，车厂管理人员可以很方便的查看车辆当前最新状况。

1. 上报时机

（1） 检测新版本

2. 上报流程

上报触发后，UC-Master 创建线程上报汽车端信息。

上报过程与检测流程一致（包括传递给 OTA 平台的参数、流程等）。

3. 上报内容

参见本文档检测新版本章节。

7.2.2.2 OTA 升级状态

OTA 升级重要节点主要指的是检测新版本（服务器生成）、下载和安装过程中的重要节点，如下载开始/结束、安装开始/结束等，上报服务器用以跟踪记录车辆升级状态。

1. 上报时机

下载和安装各状态发生时。

2. 上报流程

UC-Master 在升级过程中记录下载和安装结果，上报触发后，向服务器上报信息。

3. 上报内容

阶段	车辆状态
检测	未检测（管理平台生成）
	没有新版本（check 接口生成）
	检测到新版本
下载	待下载
	下载中
	下载中止
	下载等待
	下载完成
	下载成功
	下载失败
安装	待升级
	触发升级
	条件不满足
	取消升级
	开始升级
	升级完成
	升级未完成
	升级失败

7.2.2.3 OTA 升级事件

UC-Master 将 OTA 每个阶段的行为信息作为事件上报给 OTA 平台，车厂管理人员通过这些信息可以清晰地查看 OTA 轨迹，分析 OTA 升级失败时的主要原因。

1. 上报时机

下载和安装各状态发生时。

2. 上报流程

UC-Master 在升级过程中记录下载和安装结果，上报触发后，向服务器上报信息。

3. 上报内容

（1） 事件 ID

（2） 事件级别

a. INFO

b. WORN

c. ERROR

（3） 事件描述

（4） 事件发生时间

7.2.2.4 OTA 程序运行日志

UC-Master 将 OTA 程序在运行期间会将日志存于磁盘中，待升级结束或者 OTA 出现异常时将日志文件上传到平台，为分析问题提供依据。

1. 上报时机

客户端 OTA 回到初始状态且发生升级失败。

2. 上报流程

进入上报流程后，首先要对上报数据进行备份，防止因断电等因素造成数据丢失。然后执行上报操作，上报成功后删除备份数据，上报失败进行恢复上报流程。详细流程如下：

（1） 创建上报线程，若线程创建失败，直接上报；

（1） 备份数据，将上报数据备份到磁盘，若备份失败，直接上报；

（2） 执行上报，发起上报请求，等待 OTA 平台响应；

（3） 结果确认，根据上报结果执行以下操作：

a. 上报成功，删除备份数据，上报流程结束；

b. 上报失败，进入上报恢复流程；

a) 上报失败后，上报模块一直在后台不断尝试上报。OTA 程序创建一个专门用于执行恢复上报的线程，该线程内维护一个 List，出现上报失败情况后，将此次上报放入该 List 中，根据该 List 定期（30 秒）执行上报动作，直到上报成功为止；

b) UC-Master 启动后也会检查是否存在未完成的上报任务，若存在进入上报恢复流程；

3. 上报内容

（1） 文件类型：日志文件；

（2） 文件格式：zip/log/txt/gz/可以无后缀；

8 非功能性需求

8.1 安全性需求

1. 对本地存储数据签名加密，保证存储数据的完整性和秘密性；
2. 使用 HTTPS，保证与云端交互数据安全；
3. 支持升级包的签名解密，保证签名包的完整性和秘密性；

8.2 可靠性需求

1. 下载防掉电设计，下载掉电在重新上电，支持 HMI 恢复、断点续传；
2. 上报防掉电设计，上报信息上报失败，会在空闲时继续上报；
3. 进程间通讯支持上下线监控和断网重连；

8.3 兼容性需求

1. 支持主流硬件平台；
2. 支持主流操作系统 Android、Linux、QNX、RTOS 等；

8.4 可移植性需求

1. 程序可移植到 Linux、QNX、ALIOS、Android 系统；
2. UC 可以在车机、TBOX 以及其他具备联网能力的智能 ECU 上部署；

9 附录

1. 总体流程图


OTA_update.pdf

2. 检测新版本


OTA_check.pdf

3. 下载软件包


OTA_download.pdf

4. 安装升级包


OTA_install.pdf