07_Appendix_C3_OTA升级系统对零件ECU自升级的技术需求规范_V5.6

SOR No.	SOR-AAS-000007	Version: 5.4

Appendix C3

附件 C3

OTA Update System Technical Specification for the self-upgrade of ECU

OTA 升级系统对零件 **ECU** 自升级的技术需求规范

修订历史 Revision History

版本 Rev.	日期 Date	作者 Author	修订描述 Change Description
5.0	2022/2/1	李燕琼	OTA初始发布 HH OTA Initial Release
5.1 5.2 5.3	2022/4/1	李燕琼	补充SOR号，架构图，补充OTA模式
5.4	2022/5/10	李燕琼、王奥运	补充整车OTA模式和零件参考升级流程(原引用于HH_Bootloader Requirement Specification_V1.2_20211108)
5.5	2022/7/4	王奥运	1、删除SocketWrap(零件兼容)需求 2、升级主流程调整swithSlotStauts顺序 3、删除0xFF98/0xFF97 DID需求
5.6	2022/7/27	王奥运	1、新增断点续传详细方案和规范

本标准起草部门：OTA

Drafting Department: OTA

本标准起草人：李燕琼 王奥运

Drafting Author: JulesLi AoyunWang

1. 通用信息 General information

a. 目的 Purpose

本文档旨在规范HH采购供应商的零件ECU自升级的设计和开发技术需求。

This document specifies the technical requirements for the ECU design and development for the system self-upgrade purchased by HH.

b. 适用范围 Scope of application

本文适用于所有HH对供应商所采购的零件ECU节点的系统自升级。

This article applies to the system self-upgrade of all ECU nodes purchased by suppliers of HH.

c. 术语定义 Glossary

序号 No.	术语或缩写 Glossary and Abbreviation	描述/Description
1	A/B Swap	The storage space is divided into two logical slots, each Slot has the same partition, and only one Slot resource is used when the system is running. The new version of the software is installed in a Slot that is not currently in use.
2	SoC	System of Chip
3	MCU	Micro Controller Unit
4	OTA	Over the Air
5	Master ECU	OTA Master ECU
6	Slave ECU	OTA Savle Smart and Embed ECU
7	DoIP	UDS on IP ISO 14229-5 and ISO-13400
8	DoCAN	UDS on CAN ISO 14229-3 and ISO-15765
9	DoLIN	UDS on LIN ISO 14229-7 and ISO-17987
10	SHE	Secure Hardware Environment
11	TEE	Trusted Execution Environment
12	UDS	Unified Diagnostic Service ISO-14229
13	ECU	Electronic Controller Unit
14	CAN	Controller Area Network
15	LIN	Local Interconnect Network
16	BDCM	Body Domain Control Module
17	VDCM	Vehicle Domain Control Module
18	IDCM	Infotainment Domain Control Module

19	CGW	Central Gateway

2. 系统需求 System requirement

a. 功能说明 Function Description

OTA升级系统的架构如下图所示，Master控制整个升级流程，智能Slave ECU和嵌入式Slave ECU分别通过UDS中DoIP和DoCAN/DoLIN等协议从Master接受诊断刷写控制命令来完成升级前置条件检查，升级包下载，签名校验，升级状态上报，以及升级完成后AB分区新版本切换。如果收到的是差分包，则需要实施差分还原动作。根据升级包大小和安装时间尽力优化升级效率综合考虑使用差分升级库实现差分还原升级或Zip等压缩升级，差分升级库由HH提供,供应商负责编译集成到对应Slave ECU。在满足升级工况和升级模式要求的前提下，实施升级动作，并上报升级结果，如果升级失败，需要根据规范流程做失效处理。

供应商正式发布的软件需满足HH信息安全规范和国内外法规:如GB、EU-R156等，并提供能够反映系统OTA自升级的稳定性相关的测试报告如系统循环升级10000次未出现失败。为了保证升级效率，不同CAN/LIN节点需支持并行刷写，同一路 CAN/LIN 节点支持队列刷写，域内不同路由 DoIP需支持并行刷写,并通过技术手段满足升级时间要求。

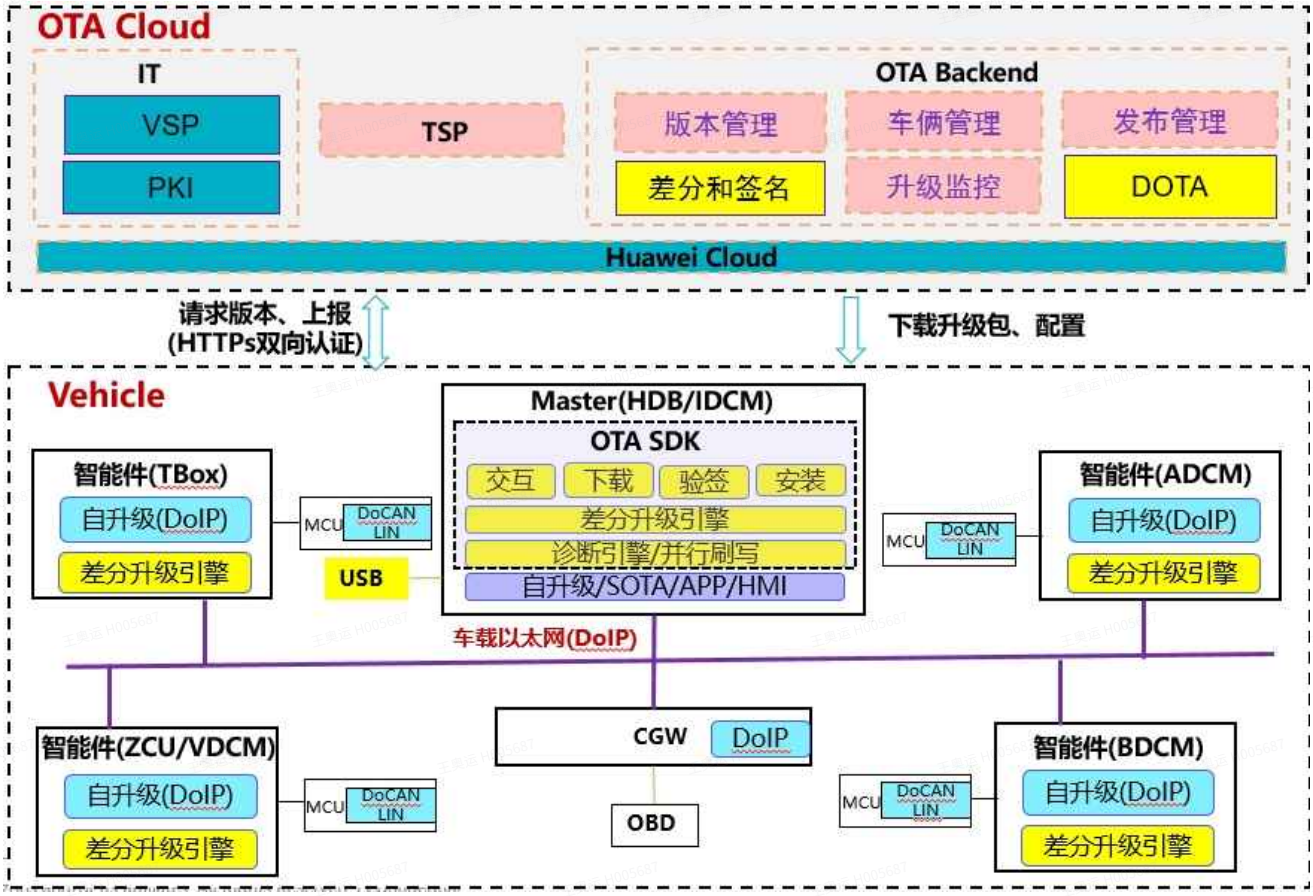
参考零件自升级流程见第7章，UDS诊断标准参考HH企业标准，其中DoIP推荐实现TLS 特性。

The architecture of OTA upgrade system is as follows. Master controls the entire upgrade process. The intelligent or embedded Slave ECU use DoIP or DoCAN/DoLIN to receive the diagnostic control commands on UDS from the Master to complete the pre-upgrade condition checking, downloading, signature verification, upgrade status reporting, and new AB slot switchover after the upgrade. If a differential package is arrived, it will be recovered to a newer package by using the differential update library. We should try our best to optimize the update efficiency according to the size of the package and the installing time comprehensively by the differential or zip compression update. The library of upgrade will be provided by HH, and the supplier is responsible for compiling and integrating it into the Slave ECU. On the premise of the upgrade condition and upgrade mode, ECU must carry out the upgrade action, and report the status and result, If upgrade failed, it necessary to deal with the failure.

The software release of the supplier should meet information security specifications of HH and domestic and foreign regulations, such as GB,EU-R156, etc., and provide the self-test report of system OTA stability, such as no failure of system cyclic upgrade for 10000 times。Different CAN/LIN nodes should support parallel flash, the same CAN/LIN node should support queue flash, and the DoIP of different routes in the domain should support parallel flash to ensure upgrade efficiency . And meet the upgrade time requirements through technical means.

Refer to Chapter 7 for the self upgrading process of reference parts. Refer to HH enterprise standard for UDS diagnostic standards. DoIP recommends the implementation TLS features

b. 系统结构示意图 System structure



3. 能力要求 Capacity Requirements

a. 性能要求 Performance Requirements

系统稳定性要求：零件ECU区域内控制器和下挂节点系统升级失败率均不能超过 1/10000。

智能零件ECU区域内控制器及下挂节点并行刷写最大升级时间不能超过 15 分钟，嵌入式零件MCU控制节点及下挂节点并行刷写最大升级时间不能超过 5 分钟，单MCU节点不超过3分钟。

System stability requirements: The upgrade failure rate of controllers and downlink nodes in the ECU area cannot exceed 1/10000.The maximum parallel brush upgrade time of controller and down-hanging node in ECU area of intelligent parts should not exceed 15 minutes, and the maximum parallel brush upgrade time of MCU control node and down-hanging node of embedded parts should not exceed 5 minutes, and the single MCU node cannot exceed 3 minutes.

b. 计算能力 Computing Requirements

为支持升级模块的正常工作，应确保可用的CPU计算和存储资源为OTA升级程序运行使用。安装工作中，出现CPU负载过重时，应及时开启系统性能j监控，阻止低优先级程序对CPU资源的消耗，优先确保升级过程顺序进行。

In order to support the normal operation of the upgrade module, ensure that the available CPU computing and storage resources are used by the OTA upgrade program. During the installation, when the CPU load is too heavy, the system performance shall be started in time to prevent the consumption of CPU resources by low priority programs, and give priority to ensuring the sequence of the upgrade process.

c. 差分升级 Differential Update

HH提供差分还原库及接口，供应商按照约定的规则调用差分库实施差分升级包的还原，参考第七章。

HH provides the differential recovery library and interface, and the supplier calls the differential recovery library to implement the differential upgrade package according to the agreed rules，Refer to Chapter 7.

d. 分区表 Partition Table

为降低升级事故造成的危害，目标升级对象，应当采用A/B Swap的升级方式，主控ECU需有充足的存储空间做OTA包缓存及版本回滚。供应商在设计分区（Nor, Nand/eMMC/MCU ROM）结构时，应与OTA供应商和确认哪些目标对象使用双分区，表1-1、表1-2为分区示意供参考。

A为运行区(只读)， B为备份区（可写），支持A/B Swap零件需实现传输升级包时写入到升级备份区域(支持预分发的智能ECU除外)，以节省缓存和升级时间。Boot不强制要求升级，如果不支持，需和HH说明。

In order to reduce the harm caused by upgrade accident, the ECU MUST support A/B Swap，The master ECU must have sufficient storage space for OTA packet caching and version rollback. When the Vendors design the partitioning (Nor,Nand/Emmc/MCU ROM)structure, it is necessary to confirm with OTA supplier which target object need use double partition . Table 1-1 and 1-2 are partitioning scheming for reference only.

A is the runnable area (read-only) and B is the backup area (writable). Parts supporting a / b swap need to be written to the upgrade backup area when the upgrade package needs to be transmitted (except for intelligent ECUs supporting pre distribution), so as to save cache and upgrade time. Boot does not require mandatory upgrade. If it is not supported, it needs to be explained with HH.

Boot	Bootloader
Kernel x2	Kernel Image
System x2	Rootfs, Driver, System libs/Apps

Vendor x2	Build-in applications by Vendor(HAL, IPC, ..)
data	Data of System application and build-in app, download cache
Security Storage	Security Storage Zone: Keys and Certs.
Log	Log store
OTA Package	The latest release backup

表1-1：SoC侧分区示意　Tale 1-1 SOC partition

Boot	Bootloader
App x2	OS and Application
Data	Data or Flash driver

表1-2：MCU侧物理分区示意　Tale 1-2 MCU partition

e. 资源需求 Resource Requirements

预留足够的存储和计算供OTA升级使用，具体可参考芯片手册和HH确认。

Reserve enough storage and computing for OTA upgrade, please refer to the chip manual and HH for confirmation.

4. 通信能力 Communication Capacity

a. 通信通道 Communication Channel

Master和ECU通过ETH传输升级指令、状态和数据。

如果ECU是一个域控制器，应当转发Master和子节点之间的升级数据：

Master和子节点基于ETH通信，域控制器需对指定的端口的TCP/UDP报文，定向路由。

Master和子节点都基于CAN FD通信，域控制器在CAN STACK完成报文的转发。

Master连接CAN FD，子节点连接CAN，域控制器在应用层面实施报文转发。

Master连接CAN，子节点连接LIN，域控制器在应用层面实施报文转发。

Master and ECU transmit upgrade commands，status ,data.

If ECU is a domain controller，it should forward the upgrade data between Master and sub-nodes:

If Master and sub-nodes communication based on ETH, and the domain controller needs to direct the routing of TCP/UDP packets on the specified port.

If Master and sub-nodes communication based CAN/CAN-FD，and the message should be forwarded on CAN stack in domain controller.

If Master connect CAN-FD, sub-nodes connect CAN, domain controller implements message forwarding at the application level.

If Master connect CAN, sub-nodes connect LIN, domain controller implements message forwarding at the application level.

b. 通信协议 Communication Protocol

ECU内部SoC和MCU之间的通信协议，由供应商自行规划，性能和安全方面设计应当得到的审核。

Master与域控制器ECU之间，基于DoIP协议通信来传输升级指令、状态和数据。

Communication protocols between SoC and MCU within ECU, planned by supplier, performance and security design should be reviewed by HH.

Between Master and Domain Control ECU, DoIP is used to transfer upgrade instructions, status and data.

5. 安全能力 Security and Safety Capacity

a. 功能安全 Functional Security

为确保在升级过程中及时发现异常，管控升级状态，ECU需要实时监测重要的系统信号或状态变化，如SoC和MCU温度，CPU负荷，DDR使用率，EMMC使用率和寿命，电源电压，通信状态，安全事故等，发现异常时及时预警。系统应当开启看门狗等能监测系统启动是否成功，同时能发现上一次非正常OFF导致的下载或升级异常。可升级零件应当支持A/B Swap升级，确保升级安装过程中是功能安全的，不会影响正常行驶和使用，若发现异常进入升级状态应当立即中止升级任务。零件ECU升级包安装完成后不能主动重启，收到主控切换新版本后应当做严格的功能安全检查后方可重启。

In order to ensure the timely detection of abnormalities during the upgrade process and control the upgrade status, ECU needs to monitor important system signals or status changes in real time, such as SOC and MCU temperature, CPU load, DDR utilization rate, EMMC utilization rate and life, power supply voltage, communication status, safety accidents, etc., and give early warning in case of abnormalities. The system should turn on the watchdog, which can monitor whether the system is started successfully, and find the abnormal download or upgrade caused by the last abnormal off. Upgradeable parts shall support a / b swap upgrade to ensure that the upgrade installation process is functionally safe and will not affect normal driving and use. In case of abnormal entry into the upgrade state, the upgrade task shall be terminated

immediately. After the installation of the part ECU upgrade package, it cannot be restarted actively. After receiving the new version of the master control switch, it shall be restarted after strict functional safety inspection.

b. 信息安全 Cyber Security

信息安全方面要求，应当遵循GB，R155和HH信息安全规范中的要求。

Common cyber security requirements should follow the requirements of GB，R155 and HH information security specifications.

c. OTA模式 OTA mode

当主控节点检查升级条件满足后进入OTA模式，OTA模式下会周期性的发送OTA模式信号到整车所有零件，对应零件ECU收到信号后有如下要求。

When the master node checks that the upgrade conditions are met, it enters the OTA mode. Under the OTA mode, it will periodically send the OTA mode signal to all parts of the whole vehicle. After receiving the signal, the corresponding part ECU has the following requirements.

	A	B
1	OTA模式定义 OTA mode define	周期CAN信号发送 100ms 优先级高 The periodic CAN signal is sent for 100ms, and the priori is high
2	OTA 模式信号 OTA mode signal	00:正常状态 normal 01:下载 download 02：门锁升级 door and lock upgrading 03:高压件升级 High voltage upgrading 04：嵌入式件升级 Embed ECU upgrade（非门锁非高压 non-lock non-High-V）05:以太网件升级 Ethernet ECU upgrading (非门锁，非高压 non-lo non-High-V) 6-7预留 Reserve
3	BDCM	02、03、04、05：KL15=on and Local ON 允许锁车不能下电,座椅加热和大灯 交互灯禁用 锁设防保持 It is allowed to lock the car without power off, the seat heating and headlamp interaction lights are disabled, the door lock is fortified and maintained.
4	VDCM	03：禁止上高压 Do not apply high voltage 02、03、04、05：档位P、N档，不能切换，E 加紧,空调禁用 The gears P and N cannot be switched, the EPB is tightened, and the air conditioner is disabled
5	IDCM	01：不休眠待机(TBOX. IDCM. CGW) No sleep and standby 02：门锁升级提示 notice door and lock upgrading 02、03、04、05：不黑屏，设置整个分区权限，MIC/Audio 闭，TOUCH OFF, 不响应下电操作(KL15=off)，大屏显示提示升级中 No black screen, set t permission of the whole partition, MIC / audio is turned off, touch is off, and does not respond to the power down operation (kl15 = off). The large screen display prompts th the upgrade is in progress.
6	CGW	02、03、04、05：OBD口禁用，不休眠 OBD port is disabled and does not sleep

d. 下载条件 Download Conditions

下载对象是已经下载到Master的升级包，ECU有电的状态下，在总线负载许可的前提下可以实施。

The download object is the upgrade package that has been downloaded to the Master. When ECU is in the state of power, it can be implemented under the premise of bus load permission.

e. 升级条件 Upgrade Conditions

Master 会做全局的整车升级条件检查如： 电源模式，变速箱档位，手刹，车速，蓄电池电量，电压充电状态等，Slave ECU进入升级前也应当对应自身系统是否适合升级做相应条件检查，此部分可参考放置在诊断预置升级条件检查中。

The master will check the overall vehicle upgrade conditions, such as power mode, transmission gear, handbrake, vehicle speed, battery power, voltage, charging state, etc. before the slave ECU enters the upgrade, it should also check whether its own system is suitable for the upgrade. This part can be placed in the diagnosis precondition check for reference.

6. 升级包管理 Upgrade package management

a. 升级包结构 Upgrade package structure

总体上，升级包由配置信息、证书、签名、升级脚本（可选）、升级文件等组成。

配置信息应当包含：名称、校验算法套件、包大小、所属域、升级工况选项、对其他ECU版本依赖、升级文件信息等。应对升级包做签名处理, 升级文件应当按照不同功能模块来组织，可以支持外设Firmware、分区镜像、压缩包等形式文件，升级包的详细结构须跟HH评审，并达成一致的理解。

In general, the upgrade package consists of configuration information, certificates, signatures, upgrade scripts (optional), upgrade files, and so on. Configuration information should include: name, validation algorithm suite, package size, domain, upgrade working condition options, dependencies on other ECU versions, upgrade file information, etc.

The upgrade package should be signed. Upgrade files should be organized according to different functional modules, can support peripheral Firmware, partition mirror, compression package and other forms of file.

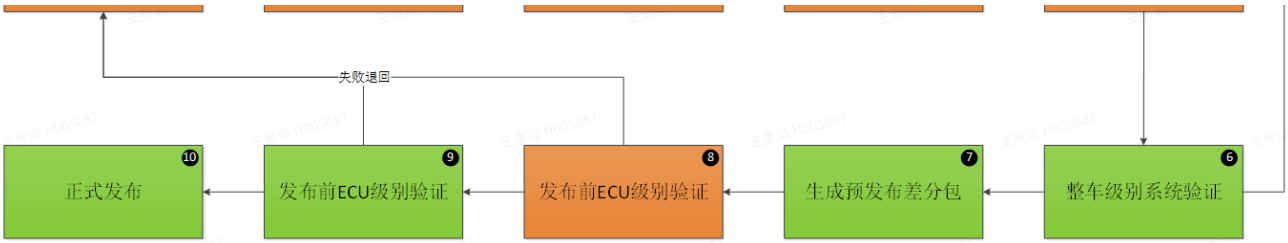
The detail structure of the upgrade package must be reviewed in depth with HH and agreed upon.

b. 版本管理 Version Management

供应商在发布版本时，版本命名应该遵循HH的软件命名规则。

When Supplier releases a version, the version name should follow HH's software naming rules.

c. 升级包的发布流程 Package release process



橙色为供应商负责，绿色为HH负责。

第二、六步验证失败，直接退回供应商；第八、九步验证失败， OTA供应商需在第一时间介入处理。

Orange is for supplier and green is for HH.

If step 2&6 is failed, returned to the supplier.

If step 8&9 is failed, OTA supplier should intervene in the first time.

d. 证书和密钥 Certificates and keys

升级包由HH云端自动签名后下发到master再分发到各零件ECU进行升级，master侧会做整车升级大版本的验签，有安全要求的Slave ECU供应商需向HH申请证书，用以对零件ECU升级包验签。

证书基于x.509标准，安全启动时若要用到证书，申请的证书应当符合处理器供应商和HH双方的要求，所有证书和密钥确保以密文存储在指定的安全存储区域里。证书若出现状态异常，如过期、泄露、吊销等，应当于重新申请。

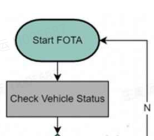
After the upgrade package is automatically signed by HH cloud, it is distributed to the master and then distributed to each part ECU for upgrade. The master will check and sign the large version of the whole vehicle upgrade. The slave ECU supplier with safety and security requirements needs to apply for a certificate from HH to verify signature of the part ECU upgrade package.

The certificate is based on the X.509 standard, If the certificate is used in secure boot, the applied certificate shall meet the requirements of both the processor supplier and HH. All certificates and keys shall be stored in the specified secure storage area in ciphertext. If the certificate is in an abnormal state, such as expiration, disclosure, revocation, etc., it shall be reapplied in.

7. 升级流程 Update flow

如下图1，展示了HH提供的参考升级流程。

The following figure 1 shows reference of the update flow provided by HH.



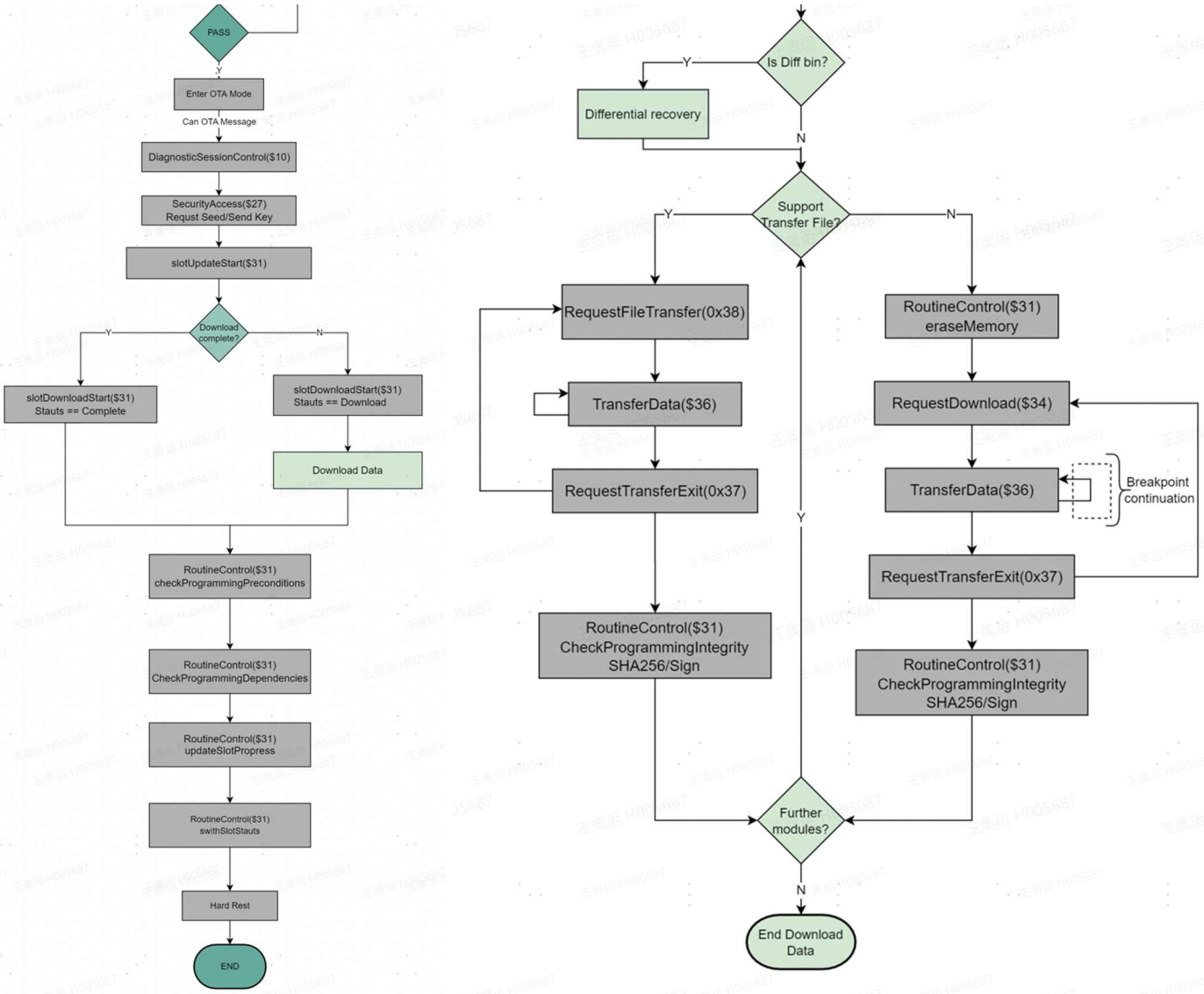


图1 升级流程

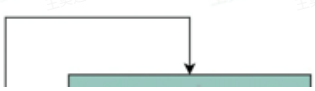
Figure 1 Update Flow

HH要求需要支持以下功能，参考列表：

HH requires that the following functions be supported:

A/B分区切换 A/B SWAP	通过指令AB分区切换，并校验AB分区切换是否成功，具体逻辑见《图2 A/B SWAP》 Switch AB partition by command, and verify whether the switch succeeds. For specific logic, see A/B SWAP in Figure 2.
回滚 Rollback	通过指令回滚，并校验分区回滚是否成功，具体逻辑见《图3 回滚》

	Roll back the partition through the command and verify whether the rollback is successful. For the specific logic, see Rollback in Figure 3.
并行刷写 Parallel flash	智能件和嵌入式件需要支持并行刷写，提高刷写速率，支持网关和升级件的遇到负反馈时的重试机制，具体逻辑见《图4 并行刷写》 Intelligent parts and embedded parts need to support parallel flash, improve the brush rate, and support the retry mechanism when the gateway and upgrade parts meet negative feedback. For the specific logic, see Fig.4 Parallel flash.
日志上报 Upload log	零件侧需支持分级(分ERR，WARN，INFO，DEBUG)日志收集，调试模式记录所有升级过程中的日志，但可通过DID控制开关，正常模式下记录所有ERR，WARN，INFO类型日志，通过0x35/0x38服务上传不同类型的日志文件，供HH分析和解决问题，具体逻辑见《图7.5 日志上报逻辑》 The part side shall support the (err, warn, info, debug) level log collection, the debug mode that can be turn on/off by DID, record all logs in the upgrade process, and record all err, warn, info logs in the normal mode. Use the 0x35/0x38 service to upload different types of log files for HH to analyze and solve problems. For details, see Figure 7.5 Log Reporting Logic.
差分还原 Differential recovery	HH提供差分还原库及接口，判定为差分包，需要读取本地老包，再利用算法合成刷写的新包，具体逻辑见《图6 差分还原动作》 HH provides the differential recovery library and interface, which is judged as differential subcontract. It needs to read the local old package and use the algorithm to synthesize and brush the new package. The specific logic is shown in Figure 6 Differential recovery.
断点续传 Breakpoint continuation	当出现断电和断网情况，在未超时情况下，重新上电和网络恢复，可以支持从断点位置继续传输 When a power failure or network disconnection occurs, the system can be powered on again and the network is restored without timeout. Transmission can continue from the breakpoint
传输文件要求 File Transfer Requirements	在支持*.hex、*.s19基础上，0x38和0x34服务需要支持*.bin和*.zip文件传输，通过减少文件大小，提高传输速率，Drive、APP等程序文件生成独立的升级包，文件地址连续，升级全部内容。 In addition to supporting *. Hex and *. S19, the 0x38 and 0x34 services need to support *. Bin and *. Zip file transfer.By reducing the file size and increasing the transfer rate, Drive, APP and other program files generate independent upgrade packages with continuous file addresses and upgrade all contents.
预分发 Preload	支持升级包边下载，边传输，减少传输文件的时间，缩短升级时间 Upgrade packages can be downloaded and transferred at the same time, reducing file transfer time and shortening the upgrade time



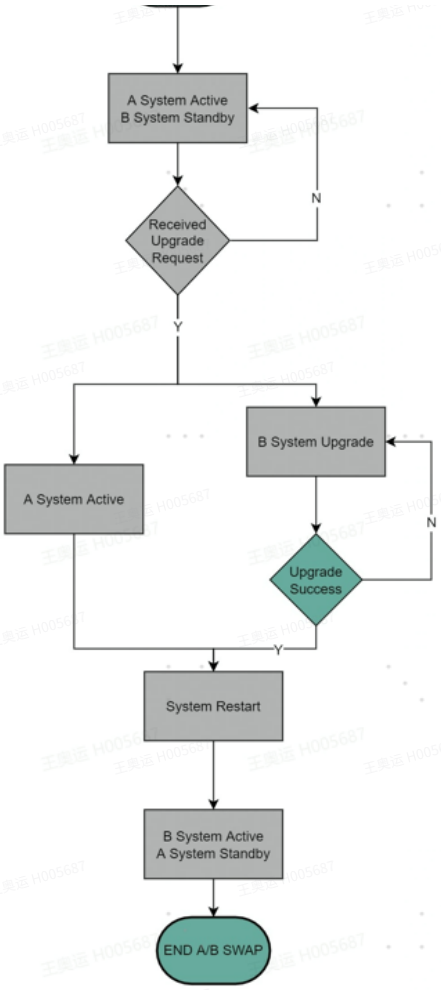


图2 A/B切换

Figure 2 A/B SWAP

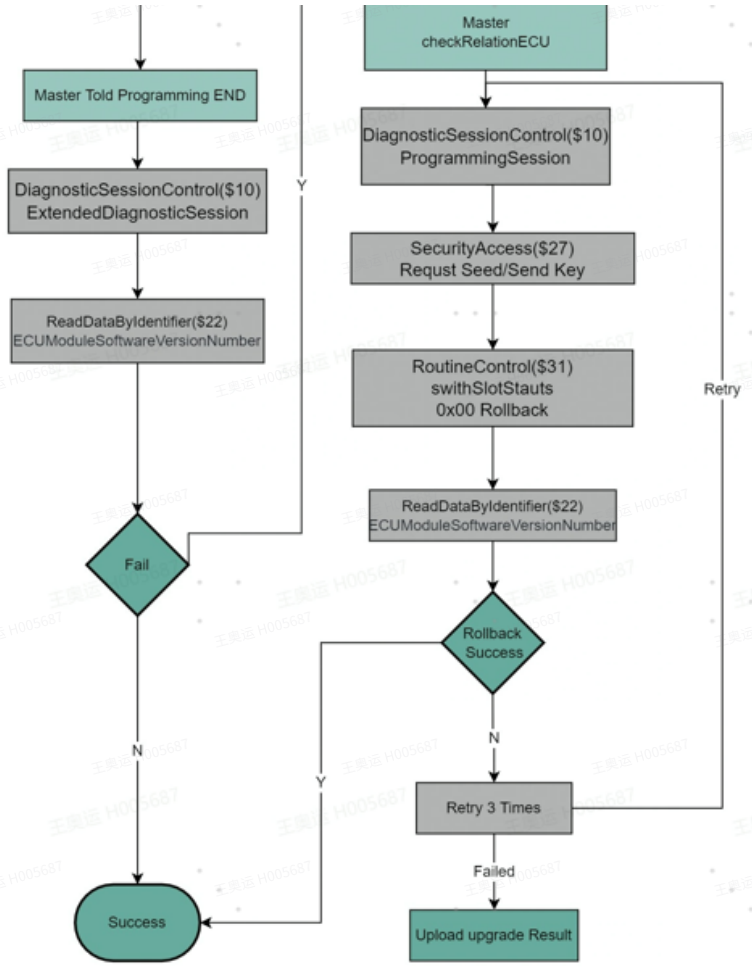


图3 回滚

Figure 3 Rollback

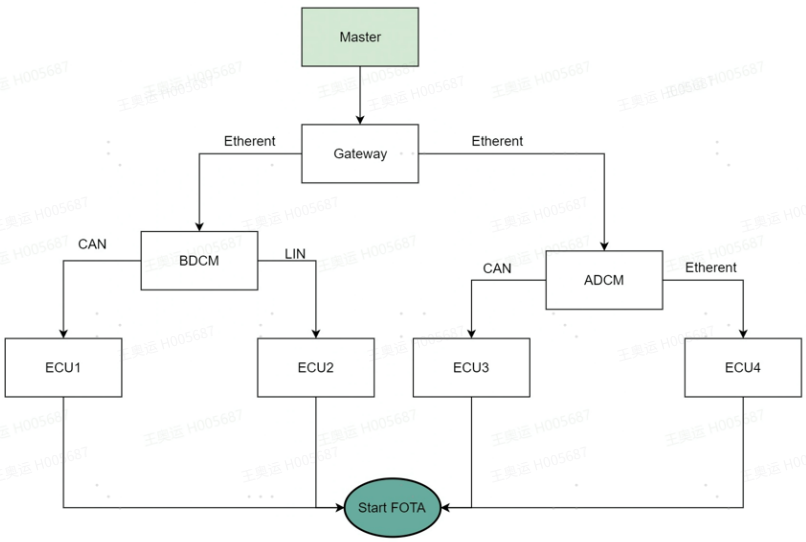


图4 并行刷写

Figure 4 Parallel flash

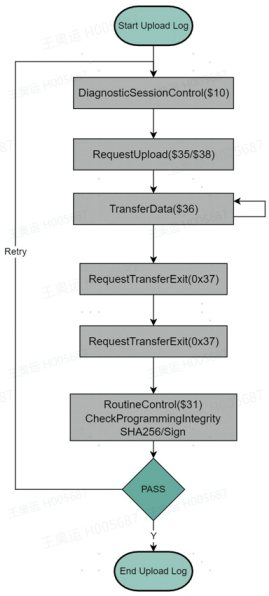


图5 日志上报

Figure 5 Upload Log

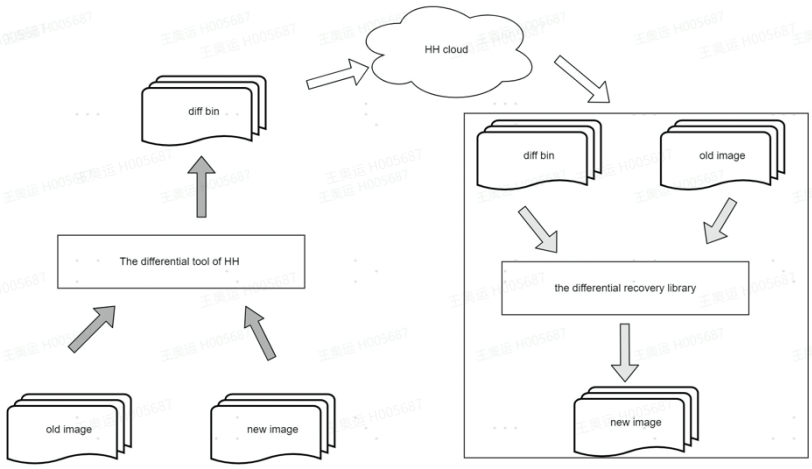


图6 差分还原

Figure 6 Differential recovery

8. 附录说明 Appendix descriptions

8.1 诊断服务需求 Diagnostic service requirements

	A	B	C	D	E	
1	Service ID 服务标识符	Diagnostic Services Name 诊断服务名称	Sub-function ID 子功能标识符	Sub-functions Description 子功能描述	*DID* *DID*	*DID Descrip* *DID描述*
2	0x10	DiagnosticSessionControl	0x01	DefaultSession		
3			0x02	ProgrammingSession		
4			0x03	ExtendedDiagnosticSession		
5	0x27	SecurityAccess	0x09	requestSeed		
6			0x0A	sendKey		
7	0x11	EcuReset	0x01	HardReset		
8					0xFF97	Reprogram
9	0x2E	WriteDataByIdentifier			0xF15A	WriteFinge
10	0x31	RoutineControl	0x01	StartRoutine	0xFF06	slotUpdat
11					0x0203	checkProg
12					0xFF07	slotDownl
13					0xFF04	swithSlotS
14					0xFF00	eraseMem
15					0xFF01	CheckProg
16					0xFF05	updateSlo
17					0x0202	CheckProg
18			0x03	RequestRoutineResult	0xFF07	slotDownl
19					0xFF04	swithSlotS
20					0xFF05	updateSlo
21	0x34	RequestDownload				
22	0x35	Requestupload				
23	0x36	TransferData				
24	0x37	RequestTransferExit				
25	0x38	RequestFileTransfer				

8.2 Routine Control

8.2.1 slotUpdateStart

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	slotUpdateStart	0xFF06

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	StartRoutine	0x01
4	#2~3	slotUpdateStart	0xFF06

8.2.2 checkProgrammingPreconditions

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	checkProgrammingPreconditions	0x0203

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	StartRoutine	0x01
4	#2~3	checkProgrammingPreconditions	0x0203
5	#4	Result	ox01 success 0x00 Failed

8.2.3 slotDownloadStart

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	slotDownloadStart	0xFF07
5	#4	Module Start Option	0x00 Download 0x01 Complete
6	#5	Module ID	Module ID

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	StartRoutine	0x01
4	#2~3	slotDownloadStart	0xFF07

请求列表：Request Routine Result

Request list: Request Routine Result

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	Request Routine Result	0x03
4	#2~3	slotDownloadStart	0xFF07

响应列表：Request Routine Result

List of responses: Request Routine Result

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	Request Routine Result	0x03
4	#2~3	slotDownloadStart	0xFF07
5	#4	Status	0x00 Success 0x01 Failed 0x02 Pending
6	#5	Progress	0x00 (0%) ... 0x64 (100%)

8.2.4 swithSlotStatus

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	swithSlotStatus	0xFF04
5	#4	Module Start Option	0x00 Rollback to old software 0x01 Activate new software

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	swithSlotStauts	0x01
4	#2~3	performPartitionSwitch	0xFF04

请求列表：Request Routine Results

Request list: Request Routine Result

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	Request Routine Result	0x03
4	#2~3	swithSlotStauts	0xFF04

响应列表：Request Routine Result

List of responses: Request Routine Result

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	Request Routine Result	0x03
4	#2~3	swithSlotStauts	0xFF04
5	#4	Status	0x00 Success 0x01 Failed 0x02 Pending
6	#5	Progress	0x00 (0%) ... 0x64 (100%)

8.2.5 updateSlotPropress

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	updateSlotPropress	0xFF05

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	StartRoutine	0x01
4	#2~3	updateSlotPropress	0xFF05

请求列表：Request Routine Results

Request list: Request Routine Result

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	Request Routine Result	0x03
4	#2~3	updateSlotPropress	0xFF05

响应列表：Request Routine Result

List of responses: Request Routine Result

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	Request Routine Result	0x03
4	#2~3	updateSlotPropress	0xFF05
5	#4	Status	0x00 Success 0x01 Failed 0x02 Pending
6	#5	Progress	0x00 (0%) ... 0x64 (100%)

8.2.6 earseMemory

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	earseMemory	0xFF00
5	#4	Adress and length format identifier	0x44
6	#5~8	Memory Address	...
7	#9~12	Memory Size	...

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	StartRoutine	0x01
4	#2~3	updateSlotPropress	0xFF00

8.2.7 CheckProgrammingIntegrity

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	CheckProgrammingIntegrity	0x0202
5	#4	verify Option	0x00 SHA256 0x01 Signature
6	#5~	crc or signature data	...

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	CheckProgrammingIntegrity	0x01
4	#2~3	CheckProgrammingIntegrity	0x0202

8.2.8 CheckProgrammingDependencies

请求列表：StartRoutine

Request list: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x31
3	#1	StartRoutine	0x01
4	#2~3	CheckProgrammingDependencies	0xFF01

响应列表：StartRoutine

List of responses: StartRoutine

	A	B	C
1	Byte	Parameter Name	Value
2	#0	Routine Control	0x71
3	#1	CheckProgrammingIntegrity	0x01
4	#2~3	CheckProgrammingDependencies	0xFF01
5	#4	Result	0x00 Success 0x01 Failed

8.3 RequestFlieTransfer

传输文件请求列表：

RequestFlieTransfer requests list:

	A	B	C
1	Byte	Parameter Name	Value
2	#0	RequestFileTransfer	0x38
3	#1	modeOfOpreation	0x01 addFile 0x02 deleteFile 0x03 replaceFile 0x04 readFile 0x05 readDir
4	#2~3	filePathAndNameLength	0x0000~0xFFFF
5	#4~#4+n-1	filePathAndName	.....
6	#4+n	dataFormatIdentifier	0x00~0xFF
7	#4+n+1	sizeFileParamterLength	0x00~0xFF
8	.....	.....	....

传输文件响应列表：

RequestFlieTransfer response list:

	A	B	C
1	Byte	Parameter Name	Value
2	#0	RequestFileTransfer	0x78
3	#1	Stauts	0x01
4	#2	length	0x00~0xFF
5	#3~	byte	....

8.4 ReadDataByIdentifier

8.4.1 ReprogrammaingAdressStauts

断点续传在传输文件出现中断的情况下，保留已下载的原文件，不进行删除，下次OTA升级可以继续未下载的内容继续下载！

Breakpoint continuation In case of interruption of file transfer, the downloaded original file is retained without deletion, and the undownloaded content can be continued to download in the next OTA upgrade!

对于文件系统，只存在一个压缩包进行升级，不用区分是哪个分区的升级包，控制器回复当前已传输包的偏移量即可！

For a file system, there is only one compressed package to be upgraded. You do not need to distinguish which partition is the upgrade package. The controller replies to the offset of the current transmitted package.

对于非文件系统，存在多个分区的每一个升级包的传输，会通过routinectrl 0x3101ff07的module_id来告知当前的分区，0xFF97的请求回复 ，根据module_id对应的分区来回复断点的偏移地址！

For non-file systems, each upgrade packet transfer with multiple partitions will be notified to the current partition via the module_id of Routinectrl 0x3101FF07, and 0xFF97's request will reply with the offset address of the breakpoint based on the partition corresponding to the module_id!

读取重编程新地址请求列表：

Read the list of reprogrammed new address requests:

	A	B	C
1	Byte	Parameter Name	Value
2	#0	ReadDataByIdentifier	0x22
3	#1~2	ReprogrammaingAdressStauts	0xFF97

读取重编程新地址响应列表：

Read the list of reprogrammed new address responses:

	A	B	C
1	Byte	Parameter Name	Value
2	#0	ReadDataByIdentifier	0x62
3	#1~2	ReprogrammaingAdressStauts	0xFF97
4	#3	byte	0x04
5	#4~	offset/address	.....

8.5 WriteDataByIdentifier

写入指纹请求列表：

Write fingerprint request list:

	A	B	C
1	Byte	Parameter Name	Value
2	#0	WriteDataByIdentifier	0x2E
3	#1~2	WriteFingerprintDataidentifier	0xF15A

写入指纹响应列表：

Write the fingerprint response list:

	A	B	C
1	Byte	Parameter Name	Value
2	#0	ReadDataByIdentifier	0x6E
3	#1~2	ReprogrammaingAdressStauts	0xF15A
4	#3	Fingerprint	....

9.OTA升级时序图

HHT_OTA文件系统升级时序图

HHT_OTA非文件系统升级时序图

详细设计以实际技术交流为准

The detailed design shall be subject to the actual technical communication.

文件结束 END OF DOCUMENT