升级使用分析

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 文档名称 | 升级使用分析 | 版本号 | 1.00.01 | | |
| 文档编号 |  | | |
| 文档类别 | 使用说明 | 文档阶段 | 初稿 | | |
| 项目名称 | TWS | 作者 | 何继胜 | | |
| 承担部门 | 软件研发部 | 批准 |  | | |
| 文档日期 | 2019年7月4日 | 使用范围 | 公司内部 | 页数 | 13 |

目录

[1 文档版本 3](#_Toc13491299)

[2 综述 3](#_Toc13491300)

[2.1 版本分区 3](#_Toc13491301)

[2.2 各分块用途 3](#_Toc13491302)

[2.3 升级大致步骤 4](#_Toc13491303)

[2.4 DFU文件格式 4](#_Toc13491304)

[3 升级聊天 5](#_Toc13491305)

[4 设备升级状态切换 6](#_Toc13491306)

[5 命令 6](#_Toc13491307)

[5.1 命令消息格式 6](#_Toc13491308)

[5.2 文件传输状态/传输部分 6](#_Toc13491309)

[5.3 SYNC\_REQ/SYNC\_CFM 6](#_Toc13491310)

[5.4 START\_REQ/START\_CFM 7](#_Toc13491311)

[5.5 文件传输-校验-重启 8](#_Toc13491312)

[5.5.1 START\_DATA\_REQ/DATA\_BYTES\_REQ 8](#_Toc13491313)

[5.5.2 DATA/DATA\_BYTES\_REQ 8](#_Toc13491314)

[5.5.3 IS\_CSR\_VALID\_DONE\_REQ/IS\_CSR\_VALID\_DONE\_CFM 9](#_Toc13491315)

[5.5.4 TRANSFER\_COMPLETE\_IND/TRANSFER\_COMPLETE\_RES 9](#_Toc13491316)

[5.6 处理新镜像 10](#_Toc13491317)

[5.6.1 重启初始化 10](#_Toc13491318)

[5.6.2 未与手机通信 11](#_Toc13491319)

[5.6.3 与手机通信 11](#_Toc13491320)

[5.7 升级完成 11](#_Toc13491321)

[5.8 错误处理 12](#_Toc13491322)

[5.9 辅助命令 12](#_Toc13491323)

[5.10 废弃的命令 12](#_Toc13491324)

[6 升级阶段Step 12](#_Toc13491325)

[6.1 APP 12](#_Toc13491326)

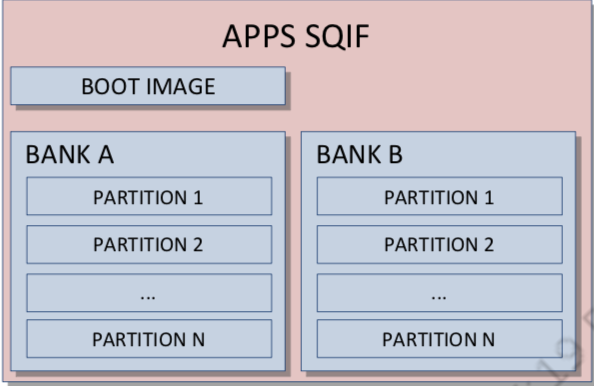
[6.2 Device 13](#_Toc13491327)

# 文档版本

|  |  |  |
| --- | --- | --- |
| 日期 | 版本号 | 简要描述 |
| 2019/7/4 | 1.00.00 | 初稿 |
| 2019/7/8 | 1.00.01 | 主流程完成，细节有待补充 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 综述

## 版本分区



## 各分块用途

|  |  |  |
| --- | --- | --- |
| ID | Partition | Purpose / Data stored |
| 0 | Nonce | Nonce used for decryption |
| 1 | Applications SQIF header | Information on the partitions in the Apps. SQIF |
| 3 | Audio SQIF header | Information on the partitions in the Audio SQIF |
| 4 | Curator Read-Only (R/O) FileSystem | Curator patches |
| 5 | Apps. P0 executable image | Firmware processor image |
| 6 | Firmware Configuration FileSystem | Firmware Configuration MIB Keys |
| 7 | Read-Only FileSystem | Files in the customer R/O file system |
| 8 | Read-Write (RW) FileSystem | Files in the customer RW file system |
| 9 | Apps. P1 executable image | Developer processor image |
| 10 | Device Configuration FileSystem | Device Configuration MIB Keys |
| 11 | Apps. RW Configuration Keys | Persistent Store Keys |
| 12 | Qualcomm® KymeraTM System DSP Architecture executable image | Audio subsystem image |

## 升级大致步骤

* 在p1核中接收各分区数据
* 处理各分区数据
* 写入各分区到分块中
* 校验分区数据
* 拷贝不可修改的分区数据
* 重启
* 验证新镜像
* 设置从新分区启动

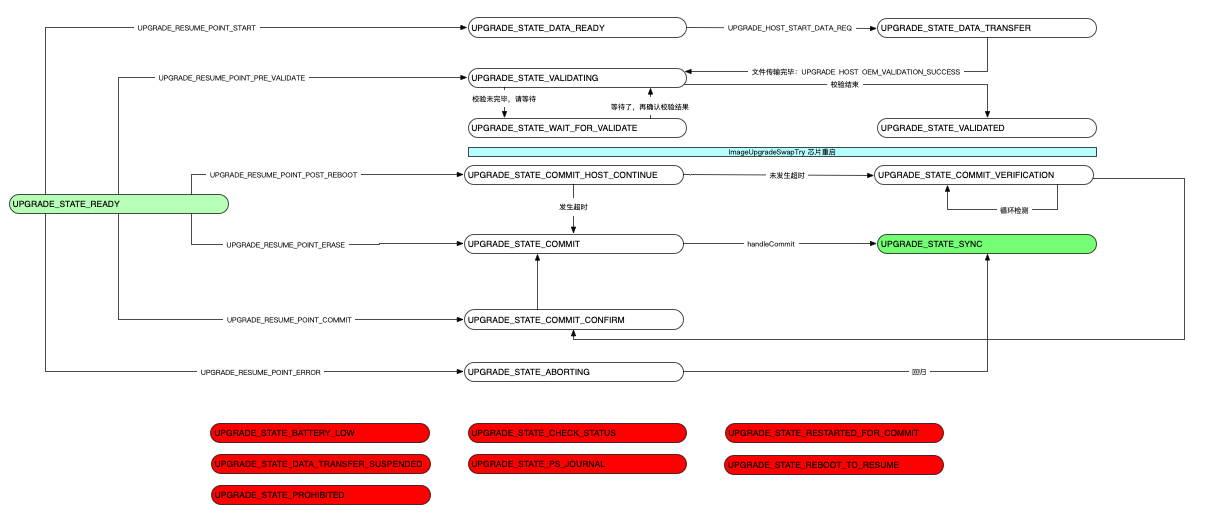
## DFU文件格式

|  |  |
| --- | --- |
| Field and description | Length (bytes) |
| DFU file header identifier = APPUHDR5 | 8 |
| DFU file header data length (Na) | 4 |
| DFU file header data | Na |
| Partition header identifier = PARTDATA | 8 |
| Partition length (Ni) | 4 |
| Partition type | 2 |
| Partition number | 2 |
| Partition data | Ni-2-2 |
| Partition header identifier = PARTDATA | 8 |
| ... | ... |
| DFU file footer identifier = APPUPFTR | 8 |
| DFU file footer data length (Nz) | 4 |
| DFU file footer data | Nz |

# 升级聊天

|  |  |
| --- | --- |
| APP | DEVICE |
| [Hi，设备，把现在的状态告诉我](#_SYNC_REQ/SYNC_CFM) | |
| 现在是xxx状态，你想让我做什么？ | |
| [你先告诉我，你现在电量是什么？](#_SYNC_REQ/SYNC_CFM) | |
| 哦，我的电量永远是0X666 | |
| 嗯，看来我要根据你的状态，去做下一步事情了，我来想想。你现在有这些阶段   * 00/data\_transfer/start: * 01/validation/pre\_validate: * 02/transfer\_complete/pre\_reboot: * 03/in\_progress/post\_reboot: * 04/commit/commit:   [嗯，现在是00阶段，你就做data\_transfer/start操作吧](#_START_DATA_REQ/DATA_BYTES_REQ) | |
| 哎，好的，我去初始化分区，获取第一个分区的大小，取消相关定时器。嗯，我该告诉你第一个分区GENERIC\_1ST\_PART的大小 | |
| 哦，我既然知道了文件信息（偏移、数据长度），我就给你发数据了 | |
| 收收收，再告诉你，现在准备接受的数据信息 | |
| [……重复接受文件数据……](#_DATA/DATA_BYTES_REQ) | |
| 啊，数据接受完了，我该校验数据去了 | |
| [终于发送完毕了，告诉我，校验的最终结果是什么](#_IS_CSR_VALID_DONE_REQ/IS_CSR_VALID_) | |
| 我还在校验，别急，等一会再来问我 | |
| [校验好了没有？](#_TRANSFER_COMPLETE_IND/TRANSFER_COMP) | |
| 已经校验好了 | |
| 好的，收到 | |
| 那我准备交换镜像了，之后会送重启，重启之后，会有些其他操作 | |
| 开始重启…gooooooo… | |
| 现在重启了，我来初始化一下，嗯，UPGRADE\_RESUME\_POINT\_POST\_REBOOT，我应该切换到UPGRADE\_STATE\_COMMIT\_HOST\_CONTINUE。你要是60s内没有给我消息，我就准备升级了 | |
| 幺，你启动啦，赶紧告诉我，你现在的状态 | |
| 我当前是UPGRADE\_STATE\_COMMIT\_HOST\_CONTINUE状态 | |
| 验证结果告诉我一下 | |
| 我可能还在运行 | |
| COMMIT，现在你可以提交了 | |
| 好的，收到 | |
| 升级完成了 | |
| 终于升级成功了！ | |

# 设备升级状态切换



红色部分，还没搞清楚怎么转换的。

# 命令

## 命令消息格式

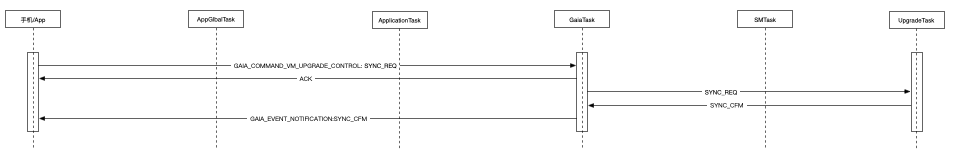
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0Bytes | 1 | 2 | 3 | Length + 3 |
| OpCode\* | Length\* | | Data\* | |

## 文件传输状态/传输部分

* GENERIC\_1ST\_PART
* HEADER
* DATA\_HEADER
* DATA
* FOOTER

## SYNC\_REQ/SYNC\_CFM

查看设备升级状态。



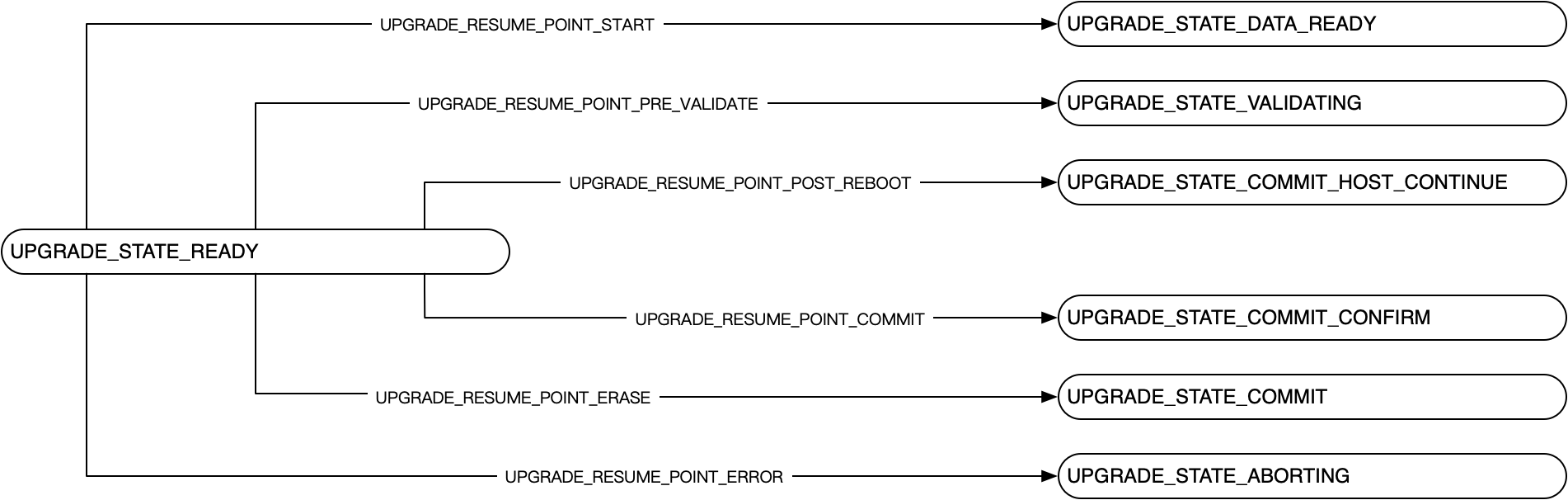
|  |  |
| --- | --- |
| Phone->Device | SYNC\_REQ |
| 4字节 | 会话ID，id\_in\_progress |

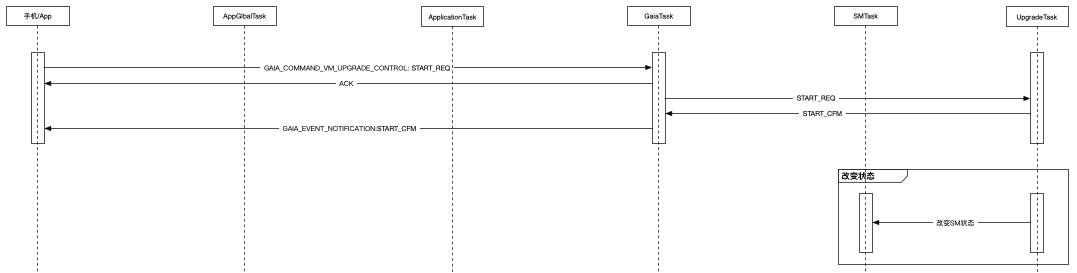
|  |  |
| --- | --- |
| Device->Phone | SYNC\_CFM |
| 1字节 | 升级状态信息 upgrade\_in\_progress\_key，类似于升级阶段。详情请看《[升级阶段Step](#_升级阶段Step)》章节。 |
| 4字节 | 会话ID，id\_in\_progress |
| 1字节 | 协议版本 PROTOCOL\_CURRENT\_VERSION |

正常情况，设备的状态变更为：UPGRADE\_STATE\_READY。

## START\_REQ/START\_CFM

设备上，根据升级所处的阶段，跳转到不同状态上。





App，根据不同阶段，准备发送不同命令。

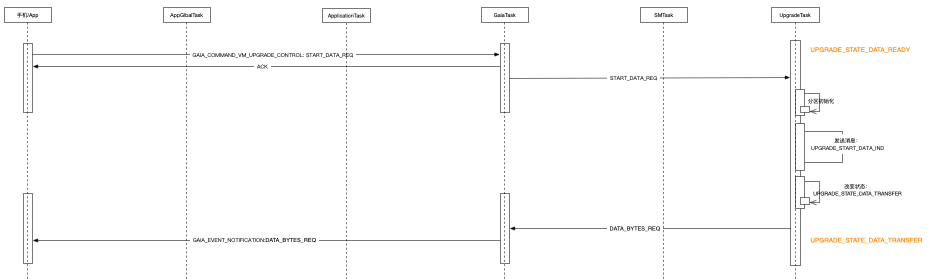
|  |  |
| --- | --- |
| Phone->Device | START\_REQ |
| 无数据 |  |

|  |  |
| --- | --- |
| Device->Phone | START\_CFM |
| 1字节 | status，永远都是0。 |
| 2字节 | batteryLevel，电池等级，永远都是0X666 |

## 文件传输-校验-重启

### START\_DATA\_REQ/DATA\_BYTES\_REQ

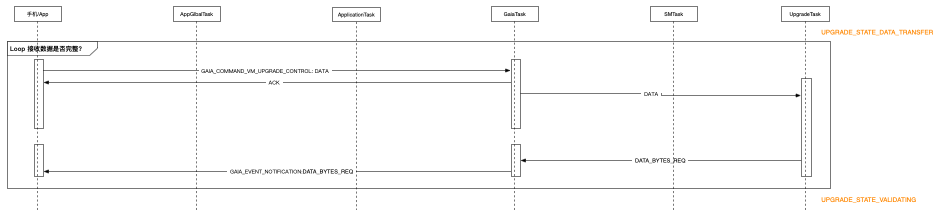
开始传输升级文件，获取到文件的偏移和需要传输的数据长度。



|  |  |
| --- | --- |
| Phone->Device | START\_DATA\_REQ |
| 无数据 |  |

|  |  |
| --- | --- |
| Device->Phone | DATA\_BYTES\_REQ |
| 4字节 | numBytes，这个文件块的大小 |
| 4字节 | startOffset，文件与起始位置的偏移 |

### DATA/DATA\_BYTES\_REQ



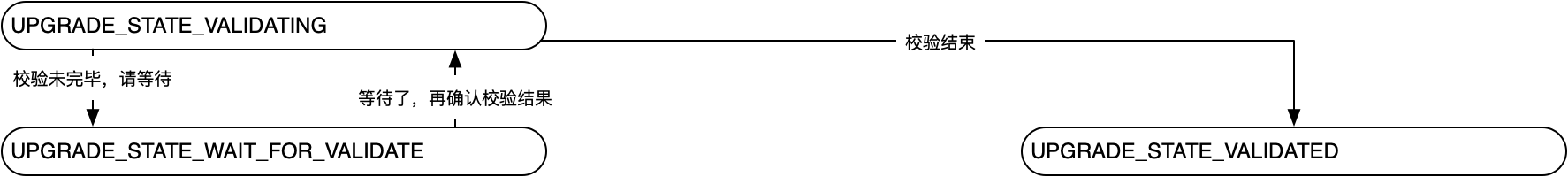
|  |  |
| --- | --- |
| Phone->Device | START\_DATA\_REQ |
| 1字节 | 是否是当前阶段的最后一包 |
| N字节 | 升级数据 |

|  |  |
| --- | --- |
| Device->Phone | DATA\_BYTES\_REQ |
| 4字节 | numBytes，这个文件块的大小 |
| 4字节 | startOffset，文件与起始位置的偏移 |

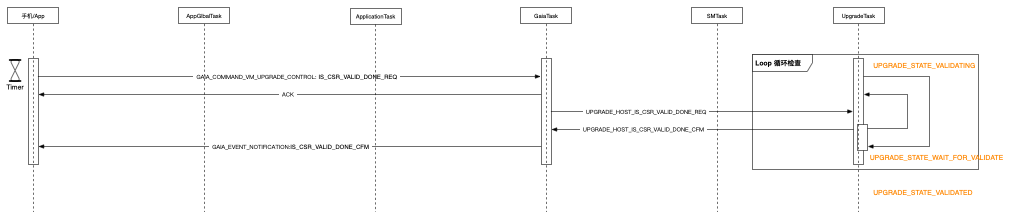
如果文件接受完毕，就不给上层发送DATA\_BYTES\_REQ命令了。

App端在发送完文件之后，进入VALIDATION阶段，发送命令：0X16/UPGRADE\_IS\_VALIDATION\_DONE\_REQ/UPGRADE\_HOST\_IS\_CSR\_VALID\_DONE\_REQ。

### IS\_CSR\_VALID\_DONE\_REQ/IS\_CSR\_VALID\_DONE\_CFM



设备端，使用task给自己发送消息，等到下一次自己执行的时候，查看版本文件的验证结果，如果验证有了结果则停止。



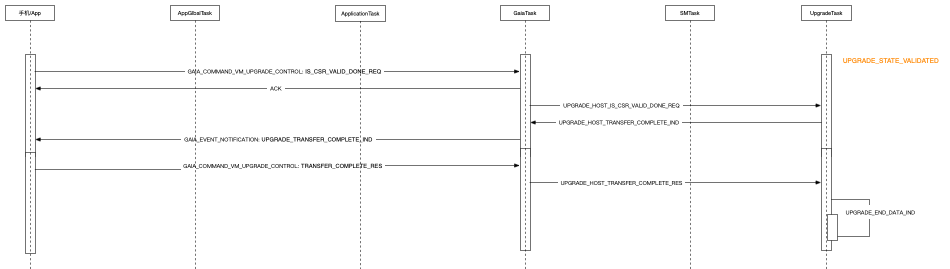
|  |  |
| --- | --- |
| Phone->Device | IS\_CSR\_VALID\_DONE\_REQ |
| 无数据 | |

|  |  |
| --- | --- |
| Device->Phone | IS\_CSR\_VALID\_DONE\_CFM |
| 2字节 | backOffTime，让APP迟点再次调用IS\_CSR\_VALID\_DONE\_REQ |

如果进入了UPGRADE\_STATE\_VALIDATED状态，表示验证完毕，IS\_CSR\_VALID\_DONE\_CFM返回的时候，没有任何数据。

### TRANSFER\_COMPLETE\_IND/TRANSFER\_COMPLETE\_RES

设备在UPGRADE\_STATE\_VALIDATED状态，收到IS\_CSR\_VALID\_DONE\_CFM，告知设备，传输已经完成(TRANSFER\_COMPLETE\_IND)，App在收到该消息时，给予消息TRANSFER\_COMPLETE\_RES回复。



|  |  |
| --- | --- |
| Device->Phone | TRANSFER\_COMPLETE\_IND |
| 无数据 | |

Phone接收到该消息时，修改传输阶段(step)，变更为：TRANSFER\_COMPLETE。

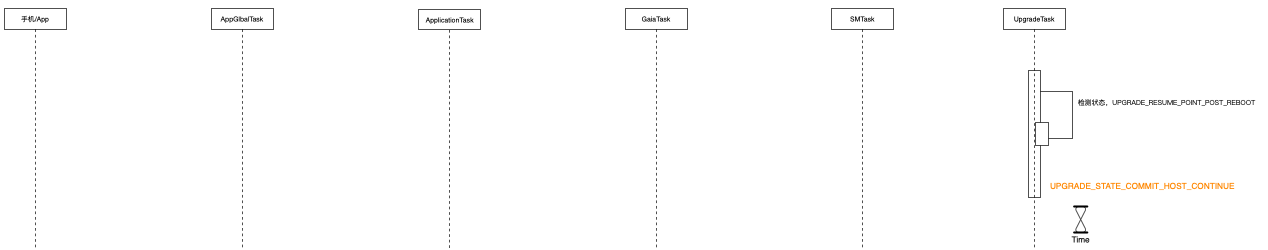
|  |  |
| --- | --- |
| Phone->Device | TRANSFER\_COMPLETE\_RES |
| 1字节 | action，0-CONTINUE 1:ABORT，设备操作，默认0 |

设备在收到TRANSFER\_COMPLETE\_RES消息是，记录当前升级的步骤UPGRADE\_RESUME\_POINT\_POST\_REBOOT，执行ImageUpgradeSwapTry操作，芯片会重启。重启的时候，进入初始化阶段，发现之前升级了。继续升级步骤继续处理。

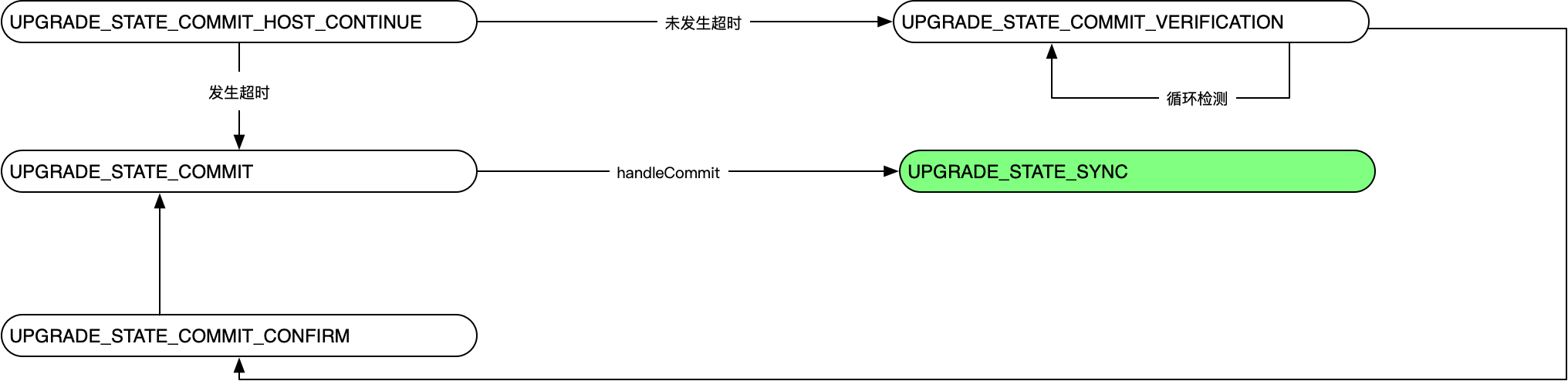
## 处理新镜像

重启之后，在初始化阶段，检测到是UPGRADE\_RESUME\_POINT\_POST\_REBOOT，立刻进入UPGRADE\_STATE\_COMMIT\_HOST\_CONTINUE状态，并设置定时器，App要60s内连接上来。如果定时时间内没有连接APP，校验镜像合法性，如果合法，默认用户确认；如果非法，升级失败。

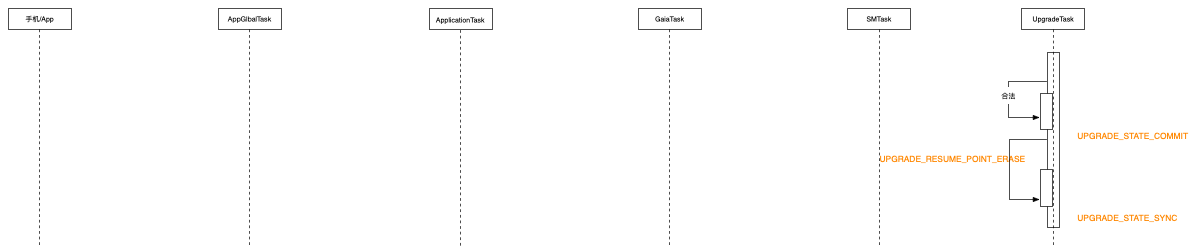
### 重启初始化



定时器，60s，如果未与App发生通讯，默认用户确认。

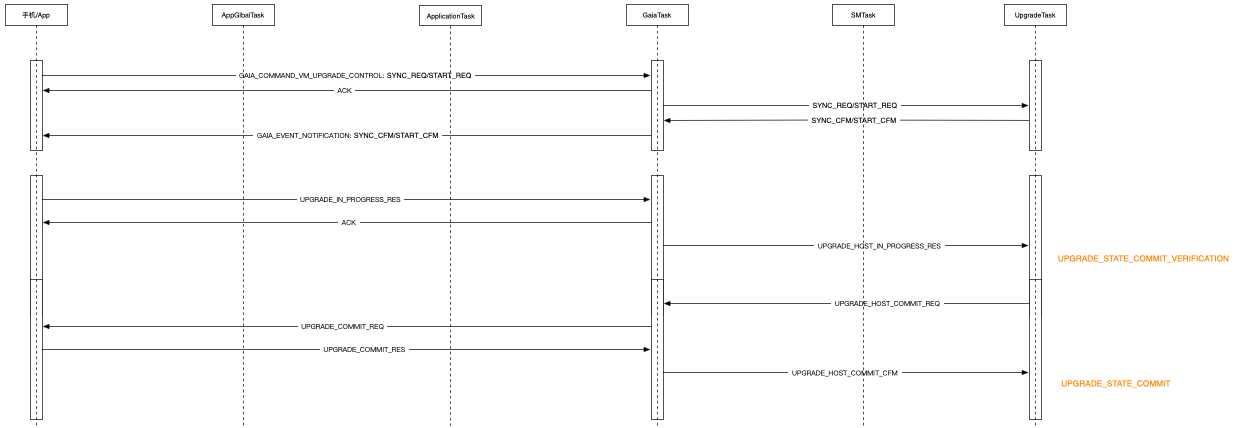


### 未与手机通信



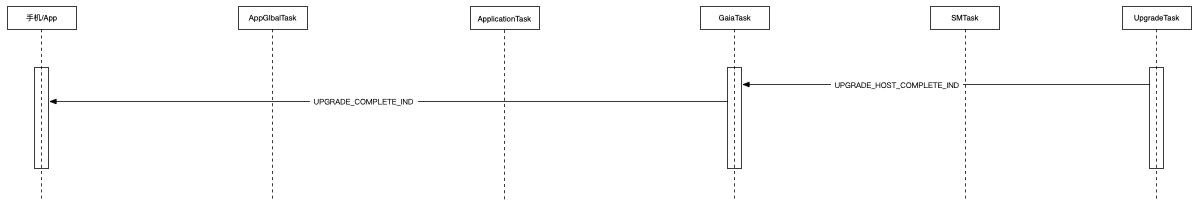
### 与手机通信

* ~~IN\_PROGRESS\_IND/~~IN\_PROGRESS\_RES
* COMMIT\_REQ/COMMIT\_CFM



默认确认和手机APP确认，最终进入的状态都是：UPGRADE\_STATUS\_COMMIT。

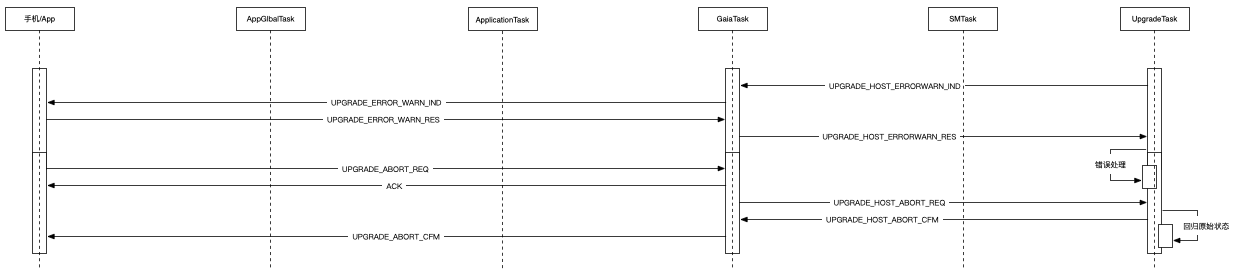
## 升级完成



在升级完成之后，app需要重新初始化，表示升级完成。

## 错误处理

* ERRORWARN\_IND/ERRORWARN\_RES
* ABORT\_REQ/ABORT\_CFM



## 辅助命令

* VERSION\_REQ/VERSION\_CFM：获取版本信息
* VARIANT\_REQ/VARIANT\_CFM：获取当前设备标识符

## 废弃的命令

SUSPEND\_IND 废弃，后期不在使用

RESUME\_IND 废弃，后期不在使用

PROGRESS\_REQ 废弃，后期不在使用

PROGRESS\_CFM 废弃，后期不在使用

IN\_PROGRESS\_IND 废弃，后期不在使用

SYNC\_AFTER\_REBOOT\_REQ 废弃，后期不在使用

ERASE\_SQIF\_REQ 废弃，后期不在使用

ERASE\_SQIF\_CFM 废弃，后期不在使用

# 升级阶段Step

## APP

|  |  |  |
| --- | --- | --- |
| 状态 | 值 | 描述 |
| DATA\_TRANSFER | 0x00 | This is the resume point "0", that means the upgrade will start from the beginning, the UPGRADE\_START\_DATA\_REQ request. |
| VALIDATION | 0x01 | This is the 1st resume point, that means the upgrade should resume from the UPGRADE\_IS\_CSR\_VALID\_DONE\_REQ request. |
| TRANSFER\_COMPLETE | 0x02 | This is the 2nd resume point, that means the upgrade should resume from the UPGRADE\_TRANSFER\_COMPLETE\_RES request. |
| IN\_PROGRESS | 0x03 | This is the 3rd resume point, that means the upgrade should resume from the UPGRADE\_IN\_PROGRESS\_RES request. |
| COMMIT | 0x04 | This is the 4th resume point, that means the upgrade should resume from the UPGRADE\_COMMIT\_CFM confirmation request. |

## Device

|  |  |  |
| --- | --- | --- |
| 状态 | 值 | 描述 |
| START | 0x00 | Resume from the beginning, includes download phase. |
| PRE\_VALIDATE | 0x01 | Resume from the start of the validation phase, i.e. download is complete. |
| PRE\_REBOOT | 0x02 | Resume after the validation phase, but before the device has rebooted to action the upgrade. |
| POST\_REBOOT | 0x03 | Resume after the reboot |
| COMMIT | 0x04 | Resume at final stage of an upgrade, ready for host to commit |
| ERASE | 0X05 | Final stage of an upgrade, partition erase still required |
| ERROR | 0X06 | Resume in error handling, before reset unhandled error message have been sent |

启动的时候，默认值为START。