

# BC35-G&BC28&BC95 R2.0

## 中国电信物联网开放平台 DFOTA 用户指导

### NB-IoT 系列

版本: BC35-G&BC28&BC95 R2.0\_中国电信物联网开放平台\_DFOTA\_用户指导\_V1.0

日期: 2018-11-30

状态: 受控文件

上海移远通信技术股份有限公司始终以为客户提供最及时、最全面的服务为宗旨。如需任何帮助，请随时联系我司上海总部，联系方式如下：

上海移远通信技术股份有限公司

上海市徐汇区虹梅路 1801 号宏业大厦 7 楼 邮编：200233

电话：+86 21 51086236 邮箱：[info@quectel.com](mailto:info@quectel.com)

或联系我司当地办事处，详情请登录：

<http://www.quectel.com/cn/support/sales.htm>

如需技术支持或反馈我司技术文档中的问题，可随时登陆如下网址：

<http://www.quectel.com/cn/support/technical.htm>

或发送邮件至：[support@quectel.com](mailto:support@quectel.com)

## 前言

上海移远通信技术股份有限公司提供该文档内容用以支持其客户的产品设计。客户须按照文档中提供的规范、参数来设计其产品。由于客户操作不当而造成的人身伤害或财产损失，本公司不承担任何责任。在未声明前，上海移远通信技术股份有限公司有权对该文档进行更新。

## 版权申明

本文档版权属于上海移远通信技术股份有限公司，任何人未经我司允许而复制转载该文档将承担法律责任。

版权所有 ©上海移远通信技术股份有限公司 2018，保留一切权利。

**Copyright © Quectel Wireless Solutions Co., Ltd. 2018.**

# 文档历史

## 修订记录

版本	日期	作者	变更表述
1.0	2018-11-30	吴丁园/ 唐正	初始版本

## 目录

文档历史 .....	2
目录 .....	3
表格索引 .....	3
图片索引 .....	4
<b>1 引言 .....</b>	<b>5</b>
<b>2 准备工作 .....</b>	<b>6</b>
2.1. 创建应用 .....	6
2.2. 生成公私密钥 .....	7
2.3. 制作固件升级包 .....	10
2.3.1. 获取差分固件升级包 .....	10
2.3.2. 对升级包进行数字签名 .....	10
2.4. 上传固件升级包并升级固件 .....	11
<b>3 DFOTA 升级 .....</b>	<b>13</b>
3.1. 创建升级任务 .....	13
3.2. 设备升级 .....	16
<b>4 DFOTA 升级过程及注意事项 .....</b>	<b>18</b>
4.1. 升级过程 .....	18
4.1.1. 下载阶段 .....	18
4.1.2. 升级阶段 .....	18
4.1.3. 恢复网络阶段 .....	18
4.2. 注意事项 .....	19
<b>5 终端 MCU 适配建议 .....</b>	<b>21</b>
5.1. 查询方式通讯说明 .....	21
5.2. 中断方式通讯说明 .....	21
5.2.1. 中断方式通讯说明（单 MCU） .....	21
5.2.2. 中断方式通讯说明（双 MCU） .....	22

## 表格索引

表 1: DFOTA 升级过程终端注意事项.....	19
表 2: 未收到 FIRMWARE UPDATE OVER 终端处理方法 .....	19

## 图片索引

图 1: 管理页面 .....	7
图 2: 下载签名工具 .....	8
图 3: 生成公私密钥 .....	8
图 4: 公钥上传页面 .....	9
图 5: 上传公钥文件 .....	9
图 6: 对差分固件升级包进行数据签名 .....	10
图 7: 添加固件包页面 .....	11
图 8: 上传已签名差分固件升级包至中国电信物联网开放平台 .....	11
图 9: 新增群组页面 .....	13
图 10: 新增群组 .....	13
图 11: 绑定待升级设备 .....	14
图 12: 创建批量任务页面 .....	14
图 13: 创建批量升级任务 .....	14
图 14: 选择需要升级的设备群组 .....	15
图 15: 选择对应的差分固件升级包 .....	15
图 16: 升级成功 .....	17
图 17: 终端单 MCU 功能连接框图 .....	21
图 18: 终端双 MCU 功能连接框图 .....	22

# 1 引言

本文档主要描述了如何通过 DFOTA 在中国电信物联网开放平台上实现 BC35-G、BC28 以及 BC95 R2.0 模组远程固件升级。

## 备注

本文档提及的中国电信物联网开放平台与华为 OceanConnect IoT 平台兼容。使用时需确保平台是最新版本。

## 2 准备工作

### 2.1. 创建应用

在 DFOTA 升级之前，需要确保设备在中国电信物联网开放平台上已经成功注册，且能正常收发数据。只有在设备可以与中国电信物联网开放平台进行正常通讯时，才可以进行 DFOTA 升级的操作。

创建应用时，请注意导入设备的 **Profile** 必须包含 **omCapabilities** 能力（若未包含，请在 **Profile** 中添加如下 **Profile** 模板中的红色部分），否则在平台上无法上传对应设备的差分固件升级包，平台也无法对该设备创建固件升级任务。具体 **Profile** 开发指导请联系中国电信物联网开放平台获取。

以下是支持升级的一个 **Profile** 模板，供参考：

```
{
  "devices": [
    {
      "manufacturerId": "Quectel",
      "manufacturerName": "Quectel",
      "model": "NBloTDevice",
      "protocolType": "CoAP",
      "deviceType": "WaterMeter",
      "omCapability": {
        "upgradeCapability": {
          "supportUpgrade": false
        },
        "fwUpgradeCapability": {
          "supportUpgrade": true,
          "upgradeProtocolType": "LWM2M",
          "downloadProtocolType": "CoAP"
        }
      },
      "serviceTypeCapabilities": [
        {
          "serviceId": "Brightness",
          "serviceType": "Brightness",
          "option": "Master"
        }
      ]
    }
  ]
}
```



```
{
  {
    "serviceId": "WaterData",
    "serviceType": "WaterData",
    "option": "Optional"
  }
}
]
```

## 备注

与中国电信物联网开放平台 1.5 版本对接过的设备，其对应的 Profile 基本没有包含 omCapabilities 能力，若后续需要测试 DFOTA 功能，请在 Profile 中添加如上 Profile 模板中的红色部分内容。

## 2.2. 生成公私密钥

1. 登陆中国电信物联网开放平台，进入“管理”→“管理”→“工具”页面，进入离线签名工具 *signtool.zip* 下载页面。如图所示。



图 1：管理页面

点击“下载”，下载signtool.zip。

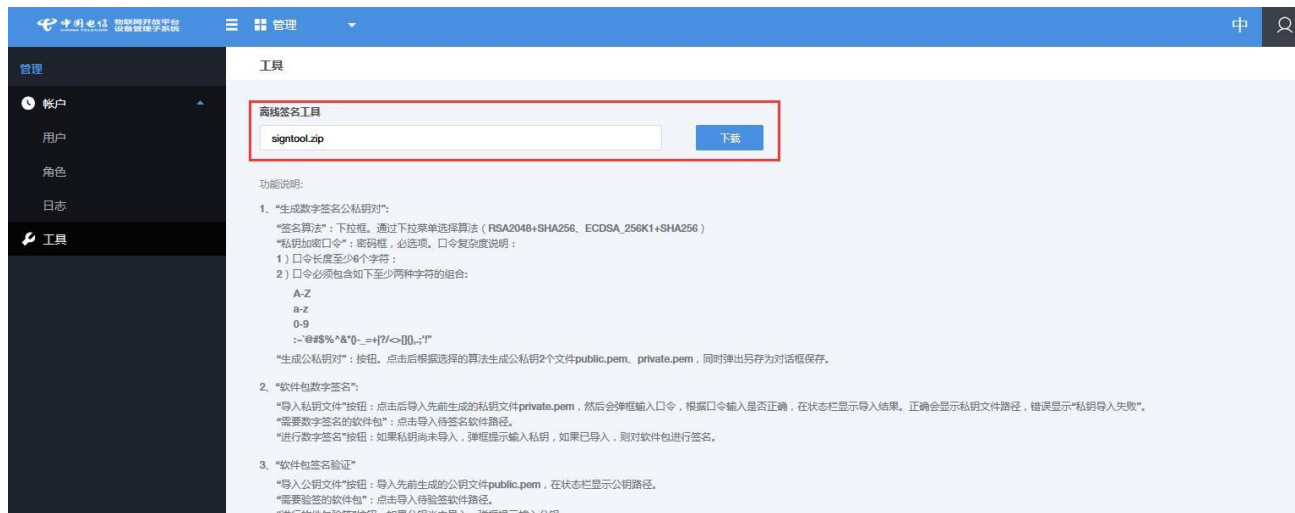


图 2：下载签名工具

- 运行 `signtool.exe` 打开工具，选择“签名算法”为“**RSA2048+SHA256**”，输入“加密口令”，例如 `Quectel123`（由中国电信物联网开放平台分配）；点击“生成公私密钥”，将生成一对公私密钥文件 `private.pem` 和 `public.pem`。如下图所示。



图 3：生成公私密钥

3. 进入“设备管理”→“包管理”→“公钥管理”→“上传页面”，上传公钥文件 *public.pem* 到中国电信物联网开放平台，“厂商名称”与应用 Profile 里的厂商名称是对应的，如下所示。

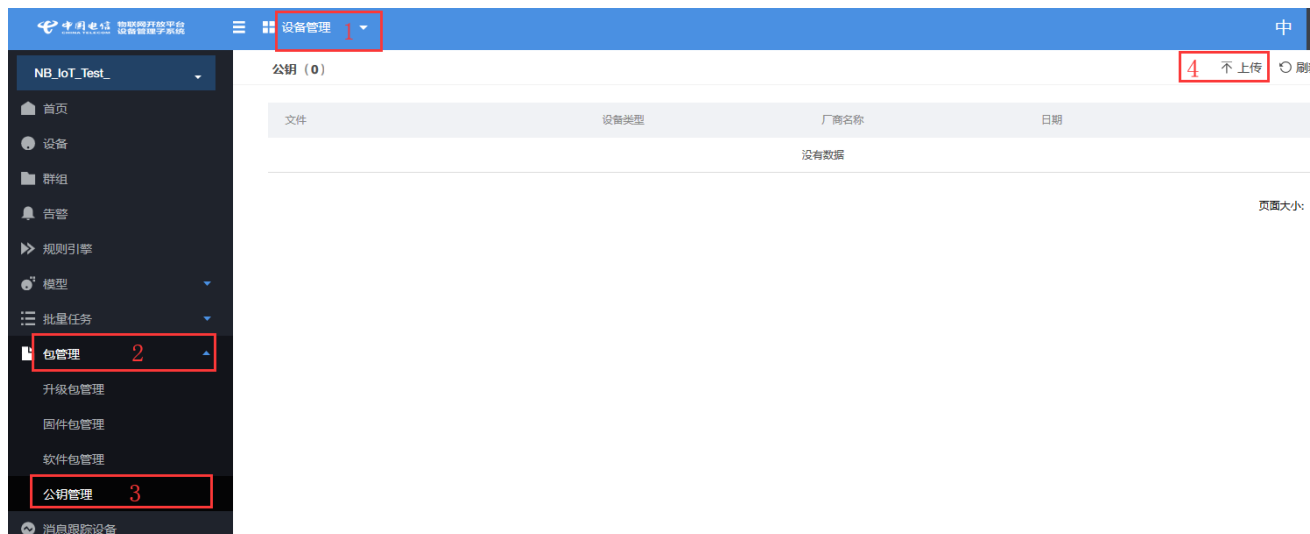


图 4：公钥上传页面

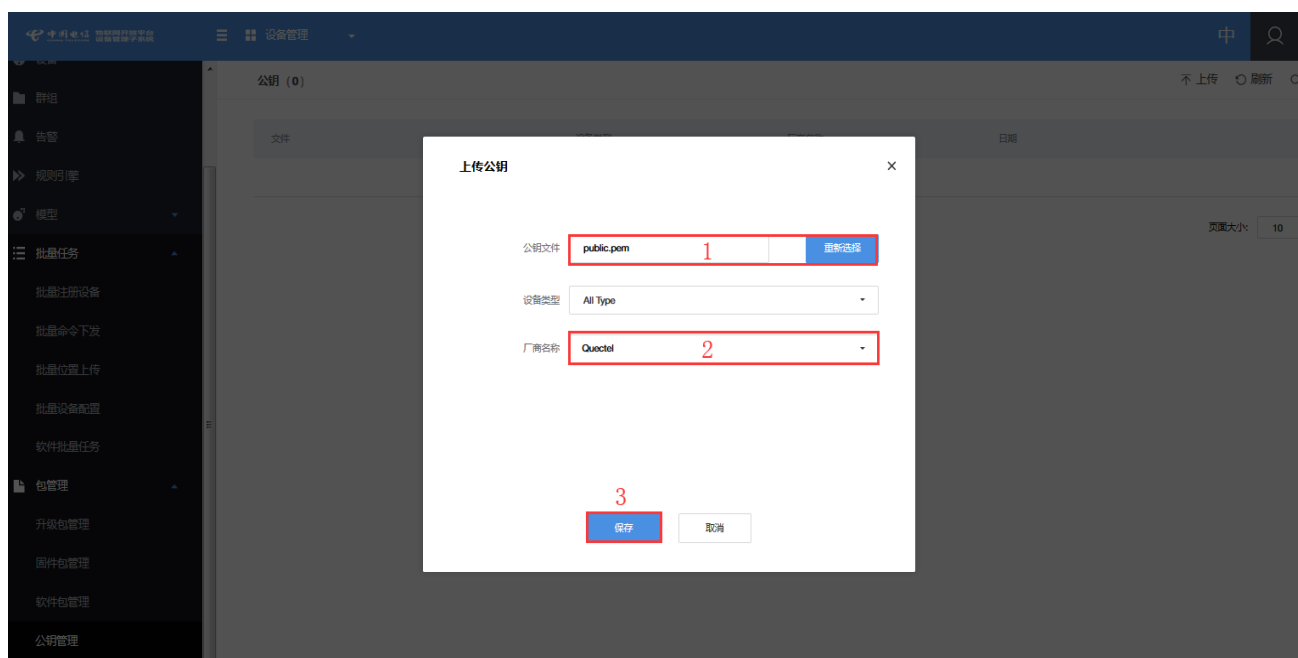


图 5：上传公钥文件

## 2.3. 制作固件升级包

### 2.3.1. 获取差分固件升级包

差分固件升级包需要从模块供应商处获取。

### 2.3.2. 对升级包进行数字签名

1. 运行 `signtool.exe`，在“签名算法”中选择私钥对应的“RSA2048+SHA256”签名算法。
2. 在“私钥文件”中导入 `private.pem` 私钥文件并输入之前设置的密码，例如 `Quectel123`。
3. 在“需要数字签名的软件包”处导入差分固件升级包，须注意差分固件升级包的文件是 `bin` 格式，（例如 `BC35GJBR01A03_TO_BC35GJBR01A04.bin`），但对差分固件升级包进行数字签名的文件格式需要是 `zip` 压缩文件，所以需要将差分固件升级包的 `bin` 文件压缩成 `zip` 格式的压缩文件（例如 `BC35GJBR01A03_TO_BC35GJBR01A04.zip`）。
4. 点击“进行数字签名”，显示签名成功，在差分固件升级包同级目录下则会生成文件名包含 `signed` 备注的已签名差分固件升级包（例如 `BC35GJBR01A03_TO_BC35GJBR01A04_signed.zip`）。

整体流程如下图所示。



图 6：对差分固件升级包进行数据签名

## 备注

上传至平台的已签名差分固件升级包是 zip 格式，因此生成的 zip 格式的已签名差分固件升级包（例如 BC35GJBR01A03\_TO\_BC35GJBR01A04\_signed.zip）不用做解压处理。

## 2.4. 上传固件升级包并升级固件

1. 登陆中国电信物联网开放平台，进入“设备管理”→“包管理”→“固件包管理”→“添加固件包”页面。



图 7：添加固件包页面

2. 上传已签名的差分固件升级包并完成其他必填信息，如下图所示，例如，“版本”填写为 BC35GJBR01A04、“设备类型”填写为 WaterMeter、“厂商名称”填写为 Quectel、“型号”填写为 NBloTDevice，“协议”填写为 CoAP。最后点击“保存”按钮。

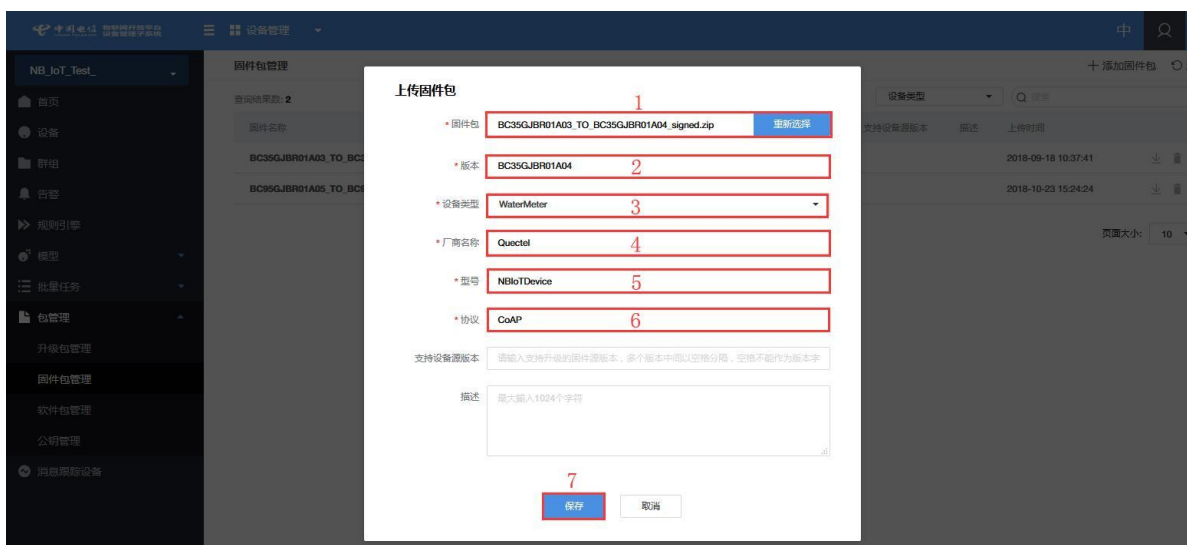


图 8：上传已签名差分固件升级包至中国电信物联网开放平台

## 备注

设备类型、厂商名称、型号、协议必须与应用的 Profile 严格一致，否则上传差分固件升级包和 DFOTA 升级任务将失败。

---

# 3 DFOTA 升级

## 3.1. 创建升级任务

1. 在“设备管理”→“群组”→“新建群组”中新增群组，例如新建的“群组名称”为 DFOTA。



图 9：新增群组页面

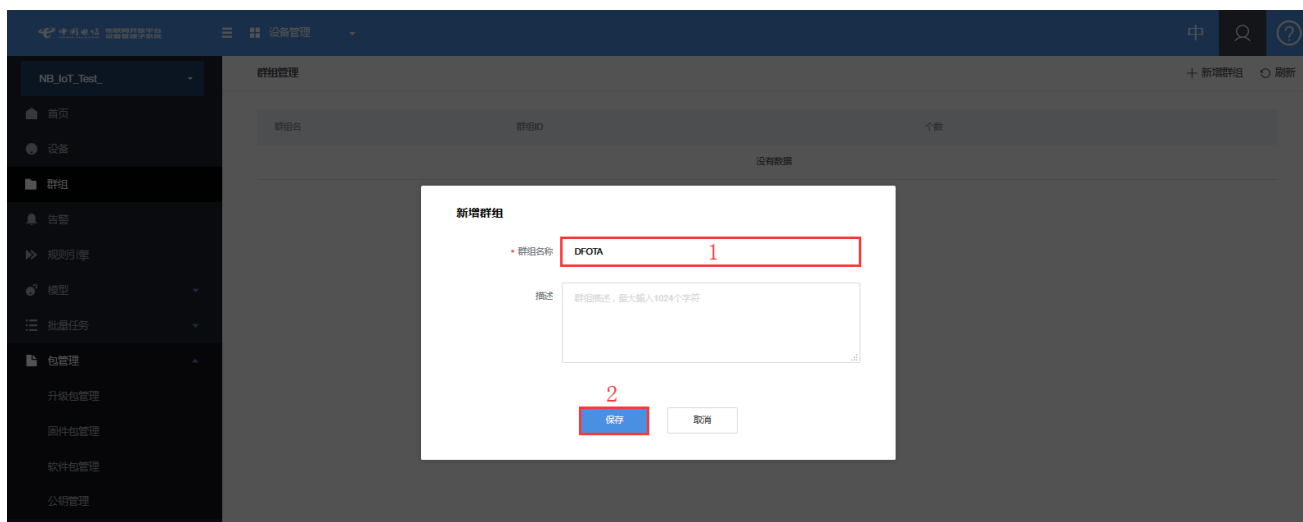


图 10：新增群组

2. 点击新建的群组名，例如“DFOTA”，在“设备管理”→“群组”→“群组管理 > DFOTA”→“设备”→“绑定设备”页面中将需要升级的设备绑定到新增群组。如下图所示。

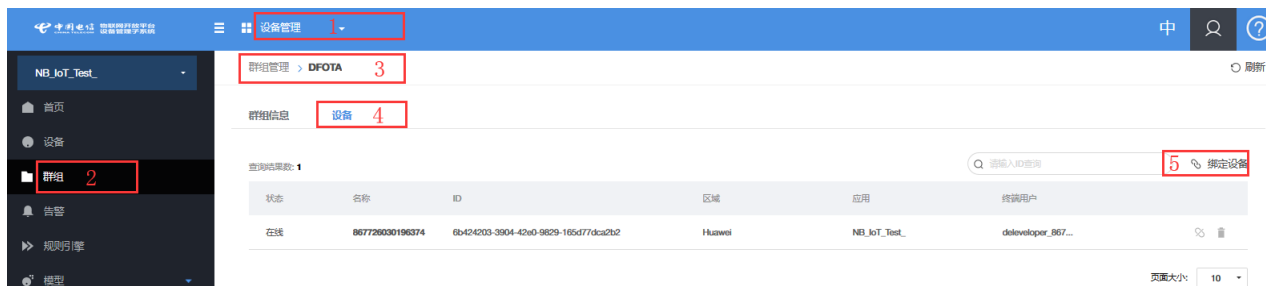


图 11：绑定待升级设备

3. 在“设备管理”→“批量任务”→“软件批量任务”→“固件升级”→“创建批量任务”弹出页面中创建批量升级任务，如图所示。（下图中“任务名”、“重试策略”和“重试次数”是默认的参数设置，可根据需求自定义）

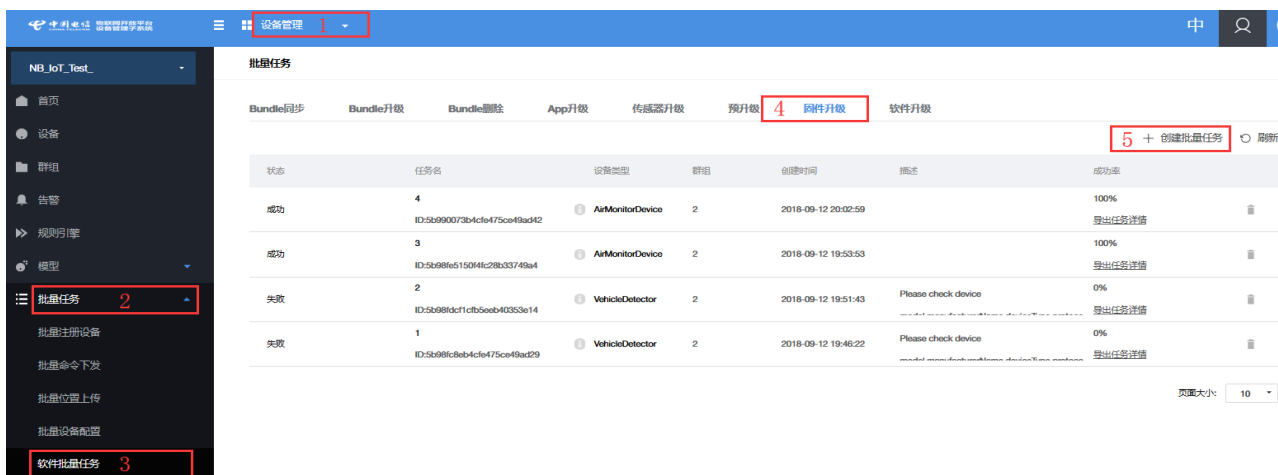


图 12：创建批量任务页面



图 13：创建批量升级任务



4. 选择需要升级的设备群组。如下图所示。

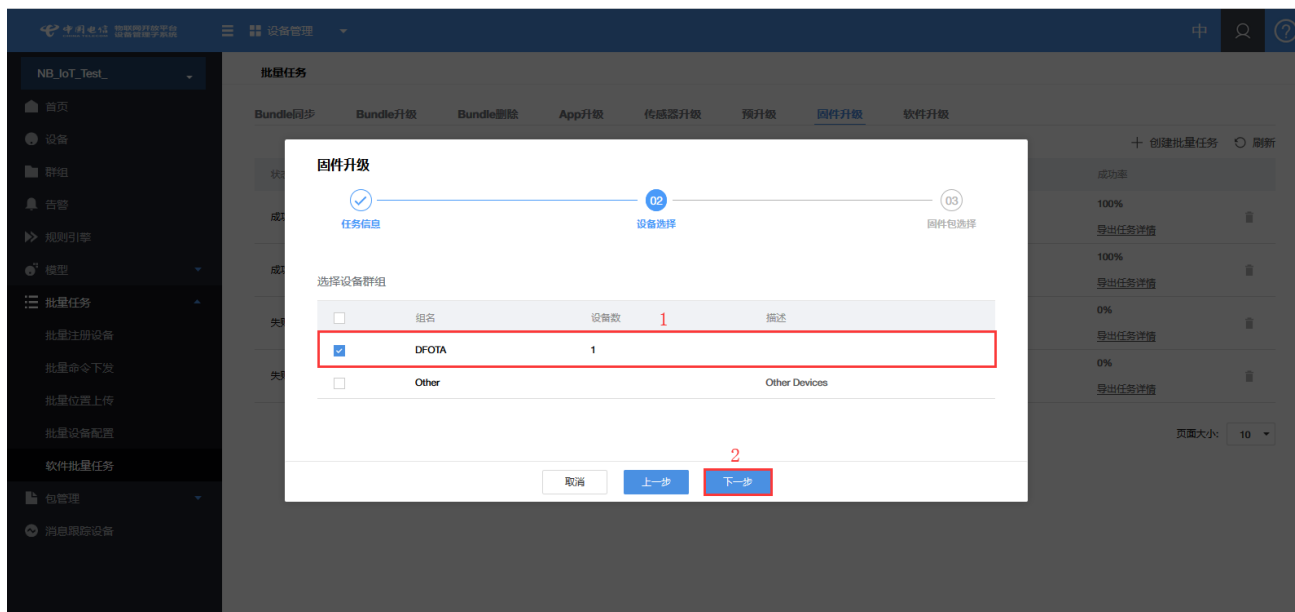


图 14：选择需要升级的设备群组

5. 选择对应的差分固件升级包，完成平台升级任务的创建。如下图所示。

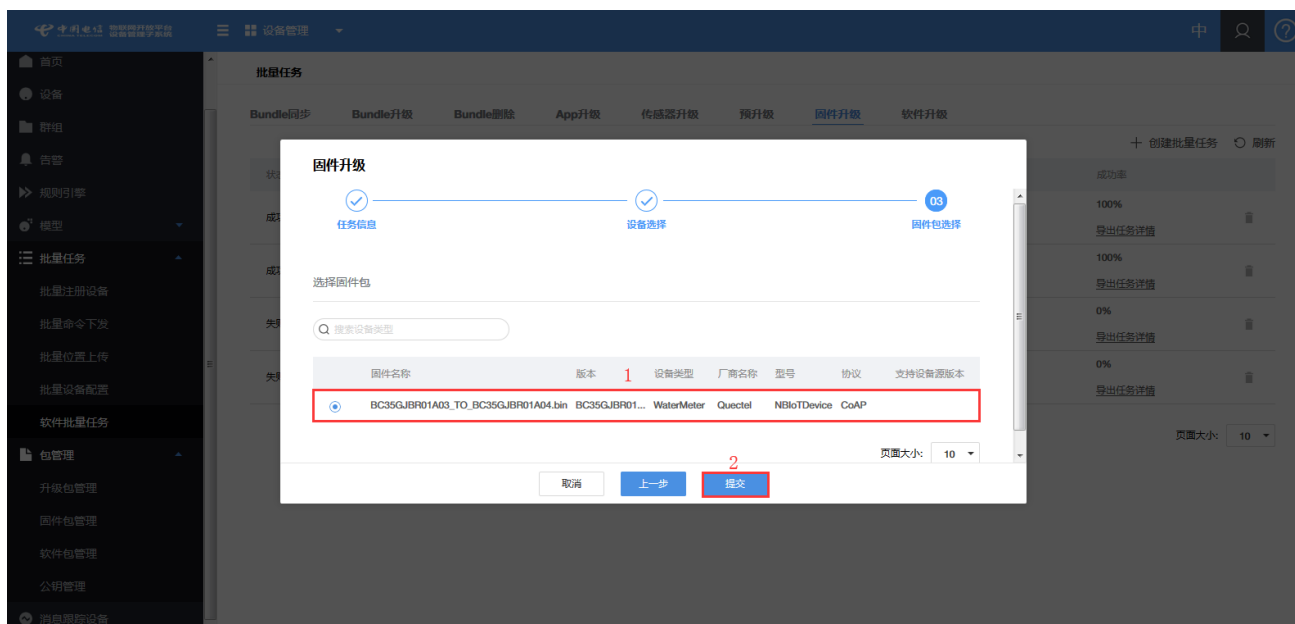


图 15：选择对应的差分固件升级包

## 3.2. 设备升级

1. 升级任务创建成功之后，终端设备发送上行数据包，触发平台的 DFOTA 升级，升级过程包括下载差分固件升级包和更新固件。

<b>AT+QLWFOTAIND?</b>	//查询 DFOTA 升级模式
<b>+QLWFOTAIND:0</b>	//DFOTA 升级模式为自动升级模式
<b>OK</b>	
<b>AT+QLWULDATA=3,313233</b>	//终端设备发送上行数据包触发 DFOTA 升级
<b>OK</b>	
<b>+QLWEVTIND:5</b>	//平台下发 observe /5/0/3 请求订阅升级状态
<b>FIRMWARE DOWNLOADING</b>	//终端设备开始下载固件升级包
<b>FIRMWARE DOWNLOADED</b>	//终端设备下载固件升级包完成
<b>FIRMWARE UPDATING</b>	//终端设备开始本地固件更新，期间模组可能会多次重启，因此需要一些时间。
<b>REBOOT_CAUSE_SECURITY_FOTA_UPGRADE</b>	//终端设备进行重启操作
<b>Neul</b>	
<b>OK</b>	
<b>FIRMWARE UPDATE SUCCESS</b>	//终端设备升级成功
<b>+QLWEVTIND:0</b>	//终端设备注册到中国电信物联网开放平台
<b>+QLWEVTIND:3</b>	//平台订阅资源 19/0/0
<b>FIRMWARE UPDATE OVER</b>	//终端设备升级完成

2. 模组固件升级完成，平台显示升级成功。如下图所示。

The screenshot displays the DFOTA upgrade success interface. On the left, a sidebar menu shows the 'Batch Tasks' (批量任务) section. The main content area is titled 'Task Details' (任务详情) and shows the following information:

- Task Name: 任务名 5
- Task ID: 5b9f534e50f4c28b337a696
- Task Status: 任务状态 成功 (highlighted with a green box)
- Success Rate: 成功率 100%
- Total Count: 总数 1
- Completed Count: 已完成个数 1
- Success Count: 成功个数 1
- Failure Count: 失败个数 0
- Create Time: 2018-09-17 15:10:06
- Retry Strategy: 重试策略 自定义
- Group: DFOTA
- Device Type: WaterMeter
- Manufacturer: Quectel
- Model: NB-IoTDevice
- Protocol: CoAP
- Version: BC35GJBR01A04
- Firmware Name: BC35GJBR01A03\_TO\_BC35GJBR01A04.bin
- Retry Count: 重试次数 5

Below the task details, a 'Task List' (任务列表) table is shown with one entry:

状态	设备名称	设备ID	描述
成功	867725030008282	eea9a3dd-e551-43ab-8abf-393c8684d395	Firmware updated successfully

The 'Task List' table has a red box around the first row, and a red '2' is placed above the '关闭' (Close) button at the bottom center of the interface.

图 16: 升级成功

# 4 DFOTA 升级过程及注意事项

## 4.1. 升级过程

### 4.1.1. 下载阶段

1. 当终端发起注册或者上报数据到平台，平台感知终端在线，如果平台有升级任务，则会下发请求查询版本号、小区 ID、信号强度以及升级状态等。
2. 如果平台判断可以发起升级，则会下发 `observe /5/0/3` 请求订阅升级状态，订阅成功之后平台下发升级包 URI 给终端。模组获取平台下发的 URI 之后，升级状态从 `IDLE` 转换成 `DOWNLOADING`，模组通知终端 MCU 开始从平台下载升级包数据，模组会发送“`FIRMWARE DOWNLOADING`”给终端 MCU，此时终端 MCU 不可给模组断电，也不可发送数据传输相关的 AT 命令。如果下载过程中发生异常导致下载失败，升级状态从 `DOWNLOADING` 转换到 `IDLE`，模组同时向终端 MCU 发送“`FIRMWARE DOWNLOAD FAILED`”，此时若设备已正常联网注册，则终端 MCU 可以正常处理业务。之后平台的服务器下发 `read /5/0/5` 请求查询失败原因，并下发 `observe cancel` 请求，模组停止 DFOTA 任务，并向终端 MCU 发送“`FIRMWARE UPDATE OVER`”，表示 DFOTA 任务结束。
3. 若升级包下载完成并校验成功，升级状态由 `DOWNLOADING` 转换到 `DOWNLOADED`，模组向终端 MCU 发送“`FIRMWARE DOWNLOADED`”。若升级包下载完成但校验失败，升级状态转换到 `IDLE`，平台的服务器将查询失败原因，下发 `observe cancel` 请求，模组会停止 DFOTA 任务，并向终端 MCU 发送“`FIRMWARE UPDATE OVER`”，表示 DFOTA 任务结束，终端 MCU 可以正常处理业务。

### 4.1.2. 升级阶段

当校验完成，平台下发 `execute /5/0/2` 请求模组升级，升级状态由 `DOWNLOADED` 转换到 `UPDATING`，模组向终端 MCU 发送“`FIRMWARE UPDATING`”。在此状态，终端 MCU 不可以给模组断电，不可以发送数据传输相关 AT 命令。

### 4.1.3. 恢复网络阶段

1. 若升级成功，升级状态由 `UPDATING` 转换到 `IDLE`，模组向终端 MCU 发送“`FIRMWARE UPDATE SUCCESS`”，待模组成功入网后，终端 MCU 可以正常处理业务。平台服务器下发 `observe cancel` 请求后，模组会停止 DFOTA 任务，并向终端 MCU 发送“`FIRMWARE UPDATE OVER`”，表示 DFOTA 任务结束，终端 MCU 可以正常处理业务。

2. 若升级失败,升级状态由 UPDATING 转换到 DOWNLOADED,模组向终端 MCU 发送“FIRMWARE UPDATE FAILED”,等待模组成功入网后,终端 MCU 可以开始正常处理业务。之后平台的服务器查询失败原因,并下发 observe cancel 请求,模组则会停止 DFOTA 任务,并向终端 MCU 发送“FIRMWARE UPDATE OVER”,表示 DFOTA 任务结束,终端 MCU 可以正常处理业务。

## 4.2. 注意事项

- DFOTA 过程中若终端 MCU 对模组进行断电、重启、休眠等操作,可能会造成模组 DFOTA 失败。因此,在此期间,终端 MCU 需要终止业务,禁止向模组发送 AT 命令,禁止断电、重启、休眠模组等操作。

表 1: DFOTA 升级过程终端注意事项

序号	DFOTA 升级过程中终端注意事项
1	模组收到平台模组升级消息,发送“FIRMWARE DOWNLOADING”消息通知终端 MCU,模组要开始自身软件升级
2	终端 MCU 收到模组进行 DFOTA 升级的消息后,需进入 DFOTA 升级保护状态,应该保障模组不断电、不休眠、不发送数据传输相关的 AT 命令给模组
3	模组 DFOTA 升级完成后,发送“FIRMWARE UPDATE OVER”消息给终端 MCU
4	终端 MCU 收到模组 DFOTA 升级完成的“FIRMWARE UPDATE OVER”消息后,结束 DFOTA 升级保护状态,进入正常工作模式,MCU 可以正常处理业务;如果终端控制设备要下电,需发送 AT+CSCON?查询终端状态,如果返回“+CSCON:1,0”可以执行断电操作;如果返回其他结果,则需继续等待
5	终端 MCU 处于正常工作状态下时,给 NB-IoT 模组通过 AT 命令发送完数据后,如果终端 MCU 要控制 NB-IoT 模组断电,需发送 AT+CSCON?查询终端状态,如果返回“+CSCON:1,0”,则可以执行断电操作;如果返回其他结果,则需继续等待

- 终端 MCU 收到“FIRMWARE DOWNLOADING”消息后,如果持续 35 分钟没有收到“FIRMWARE UPDATE OVER”消息,建议参考下表处理:

表 2: 未收到 Firmware Update Over 终端处理方法

所处状态	DFOTA 升级过程中终端注意事项
Firmware Downloading	重启模组,重启后 MCU 需保障模组不掉电直到模组输出“FIRMWARE UPDATE OVER”消息(最长 35 分钟)
Firmware Downloaded	重启模组,重启后 MCU 需保障模组不掉电直到模组输出“FIRMWARE UPDATE OVER”消息(最长 35 分钟)

Firmware Updating	重启模组，重启后 MCU 需保障模组不掉电直到模组输出 “FIRMWARE UPDATE OVER” 消息（最长 35 分钟）
Firmware Update Success	无需处理，可进行正常业务
Firmware Download Failed	无需处理，可进行正常业务
Firmware Update Failed	无需处理，可进行正常业务

## 5 终端 MCU 适配建议

模组通过串口和终端 MCU 进行通讯，当前主要有两种串口通讯方式：查询方式和中断方式。建议在通过 DFOTA 进行模组固件升级时，根据实际情况适配终端 MCU。

### 5.1. 查询方式通讯说明

当采用查询方式进行模组与终端 MCU 之间的通讯时：

1. 每次终端 MCU 发送完消息，需要等待监听串口新消息，导致终端 MCU 被串口监听任务占用，不能及时处理自身业务；
2. 如果终端每次发送完数据后长时间被监听串口任务占用，会导致功耗增大；
3. 模组 DFOTA 使用概率极低，如果每天为确认是否有 DFOTA 升级进行等待，引起功耗增加，电池损耗太大。

### 5.2. 中断方式通讯说明

#### 5.2.1. 中断方式通讯说明（单 MCU）

当终端只有一个 MCU，同时负责终端自身业务以及终端和模组的通讯时：

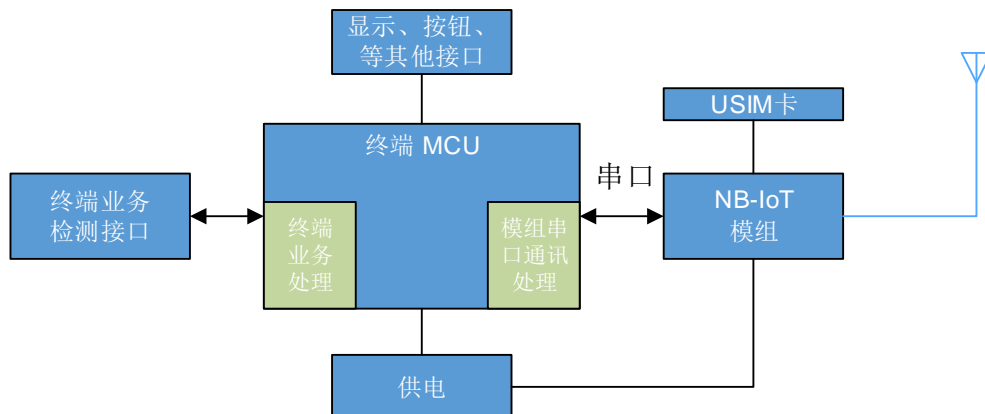


图 17：终端单 MCU 功能连接框图

- 1) 终端 MCU 和模组的串口通讯，建议采用中断方式，避免查询方式条件下终端 MCU 等待模组消息时间过长，影响终端检测业务；
- 2) 每次终端 MCU 上报数据发送完成后，串口工作在中断方式下，响应模组串口输出的升级提示信息（中断服务程序只做响应和简单接收，不做大任务处理，避免长时间占用中断）；
- 3) 采用中断方式，在终端 MCU 等待模组消息的同时，可以处理自身其他业务；
- 4) 当终端 MCU 中断响应接收到模组输出的升级消息“FIRMWARE DOWNLOADING”，终端 MCU 需要按照表 2 中处理方法，进入 DFOTA 升级保护模式，不对模组断电、不发送数据传输相关的 AT 命令给模组；

### 5.2.2. 中断方式通讯说明（双 MCU）

当终端有两个 MCU，一个负责终端自身业务，一个负责终端和模组的通讯时，负责与模组串口通讯的 MCU2 不会影响到处理终端自身业务的 MCU1；这种场景下，MCU2 既可以采用串口查询方式监听模组消息，也可使用中断方式工作：

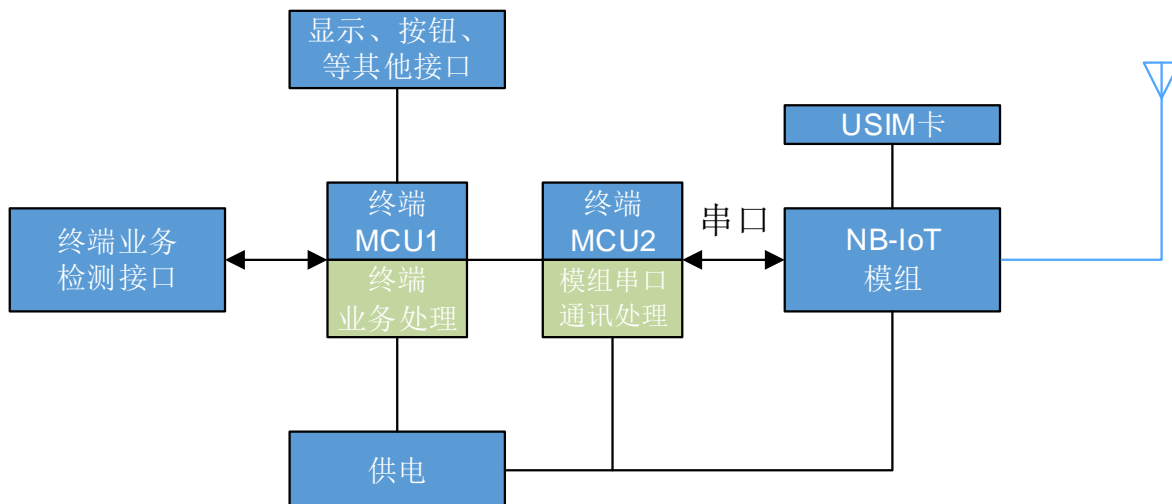


图 18：终端双 MCU 功能连接框图

- 1) 如果 MCU2 采用中断方式，具体实现方法请参照 5.2.1 章节；
- 2) 如果 MCU2 采用查询方式仅处理模组串口消息，每次 MCU1 完成自身业务数据发送后，MCU2 需要等待监听串口消息至少 2 分钟，以确认是否有 DFOTA 升级以及其他串口消息，等待期间终端业务由 MCU1 进行处理；
- 3) 串口采用查询方式时，由于 MCU1、MCU2 有等待时间，会导致功耗增大；
- 4) DFOTA 使用概率极低，每天增加等待时间，电池损耗较大，因此系统设计时应注意避免使用电池供电，或者详细评估电池供电容量以留足余量；
- 5) 当 MCU2 查询到平台下发的 DFOTA 下载消息“FIRMWARE DOWNLOADING”，MCU2 需要按照表 2 中处理方法，进入 DFOTA 升级保护模式，不对模组断电、不发送数据传输相关的 AT 命令给模组；
- 6) 如果平台不进行 DFOTA 升级，终端完成自身业务后，查询模组状态，如果进入 IDLE 状态，就可以按照终端后续流程处理。