**7 片内flash的空中升级**

7.1 使用片内flash空中升级的要求和约束条件

当使用CC2640F128内部的flash时，flash的开始的6个page也就是开始的24KB是预留给flash interrupt vectors，BIM和永久保留的OAD Target App。OAD Target App中用到了一部分固化在ROM中的TI-RTOS的代码。BIM和OAD Target App还用到了flash的page 31中的一些存储空间。Page 31的起始地址是0x1F000, CCFG也用到了这一部分空间。BIM和OAD Target App都是被设计为不可升级的。

OAD image默认是放在从0x6000到0xEFFF的9个flash page 中一共36KB的空间内。因为Page 0是不能升级的，所以image中的代码必须在flash中包含它自己的instance。而不是依赖ROM中的TI-RTOS来实现。OAD image也和其他的代码共享CCFG。CCFG是不能通过OAD来升级。

OAD Target和OAD image共享相同的RAM。但是在每次器件复位后只有一个程序可以使用这些共享的RAM。OAD image必须是一个完整的用户代码。它要可以独立于固化的OAD Target运行。

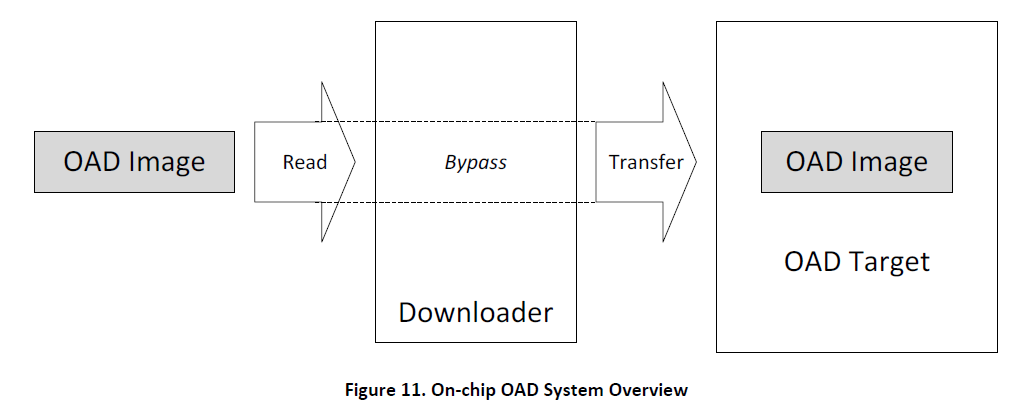
BLE stack默认在从0xF000到0x1DFFF的15个flash的page中共60KB。 SNV在从0x1E000到0x1EFFF的一个flash的page中共4KB。如果OAD image太大放不到它自己的36KB的空间内，可以考虑裁剪BLE stack的部分功能来腾出空间放OAD image。这一部分将在7.5.5章进一步讨论。

OAD Target App即OAD image A与OAD image B共用同一个BLE stack。BLE stack是不能OAD的。

Flash的第一页和最后一页不能Erase的，如果这样做使芯片进入一个不安全的状态，如果这时候发生复位，芯片会“变砖”。一旦芯片“变砖”没有JTAG或是serial boot loader是无法恢复的。

7.2 系统概述

在Figure 11中所示的OAD系统中，系统由OAD image，Downloader和OAD Target组成。



OAD Target就是我们CC2650。OAD image就是你要下载到OAD Target中的用户代码。OAD image格式应该是intel hex格式的.hex文件。Downloader可以由运行在PC机上的“BLE Device Monitor”和运行程序”HostTest application”的CC2540 dongle来组成。Downloader也可以由任何专用的应用程序或者手机上APP来实现，只要它实现了7.3章所描述的OAD Profile客户端。

TI专用的OAD Profile定义了OAD Target与Downloader之间的通讯。这个Profile里面定义了一系列相应的characteristics来支持image identification, image block request/response and image count setup等功能。

7.3 OAD Profile

这个Profile是为了给客户提供一种简单的定制化的OAD profile而设计的。对于片内flash OAD来说这个Profile最基本的功能有：根据image header的要求来接受OAD请求；将OAD image储存到OAD target device片内的flash中；如果下载成功复位芯片，使下载的用户的应用代码可以由BIM运行。Downloader是client的角色，而OAD target device是server的角色。

7.3.1 依赖关系

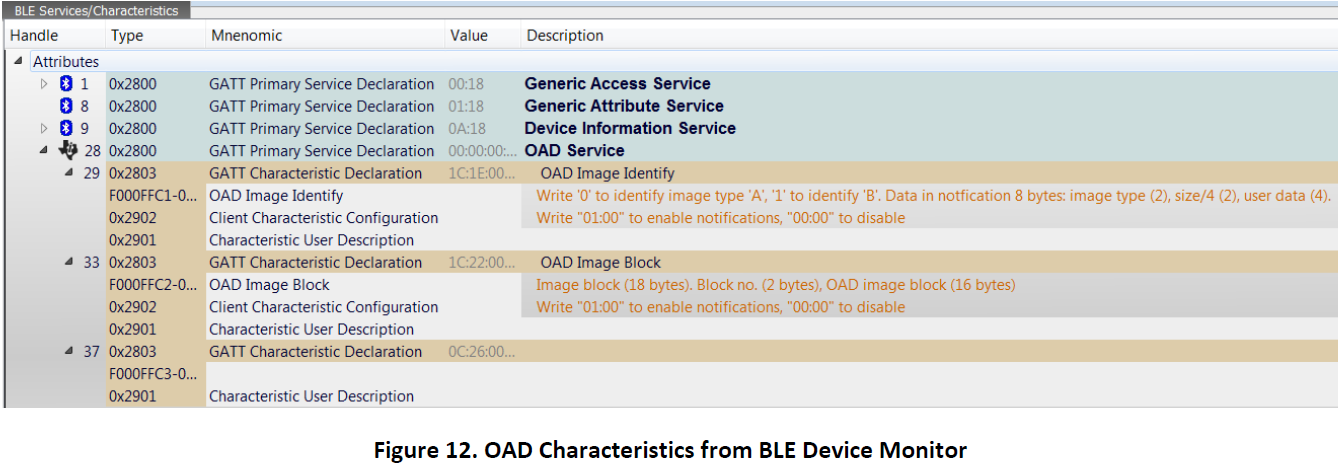
OAD profile根据最终客户的应用来决定连接参数和发起OAD的条件。

7.3.2 Message

这里使用“无回复写入”作为从downloader到OAD target device的默认的消息类型。这种类型的消息可以减少代码体积并尽可能的增加传输速率。之所以这样决定是应为,如果用“有回复写入”类型的消息如GATT Notification需要调用函数GATT\_ClientInit()，这样会明显的增加代码的体积。在噪声或者RF信号很差的环境中，这种“无回复写入”类型的GATT消息可能无法成功的传输整个image。这就需要在软件中加入超时和重传机制。因此downloader将被初始化成client, “有回复写入”的Notification被选为默认的从OAD target device 到downloader的消息类型。

7.3.3 Characteristics

OAD的profile只有三个characteristics. Downloader负责发现OAD target device上的这三个characteristics的handle。这些characteristics的结构如下图所示。

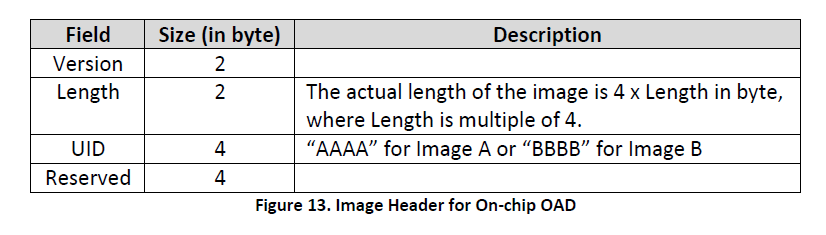


7.3.3.1 OAD image Identify Characteristics

Image识别 characteristics被用来交换片内flash OAD中的嵌入到OAD image中的image header信息。或者被用来交换片外flash OAD中Downloader为OAD image生成的元数据。OAD Target用这个元数据来决定是否要发起OAD。“01:00”应该写到这个characteristics的 Client Characteristic Configuration后文统一简称CCC来使能notification。

7.3.3.1.1 Image Header

对于片内OAD，Image Header位于OAD Image的开始的部分。它开始于第5个字节，或者CRC和CRC Shadow的后面。 CRC和CRC Shadow总共4个字节并且位于OAD Image的开头。Downloader从OAD Image中获取Image Header中的信息，并写入OAD Image Identify characteristic的数据中。Image header的具体描述见Figure 13。



7.3.3.2 OAD image Block Characteristics

OAD image Block Characteristics用来请求和传输OAD image的数据。当这个Characteristics 的CCC被写入“01:00”时使能notification，写入“00:00”关闭notification。

7.3.3.3 OAD image Count Characteristics

OAD image Count Characteristics用来设置需要下载的OAD image的数量。它是专门用在片外OAD的中的，默认值是1。

7.3.4 发起片上OAD的步骤

在建立一个新连接后，首先跟新connect interval来满足快速 OAD， 并且使能OAD image Block Characteristics和OAD image Identify Characteristics的notification。之后Downloader给OAD Target的OAD image Identify Characteristics写入数据。写入的数据来自于OAD Image的Image Header。

一旦收到downloader写入到image Identify Characteristics的数据，OAD target 将把收到的OAD image的信息和自己正在运行的image做比较。默认情况下只有image size和version number用来检查和决定是否接受新image升级。image size和version number用来决定image是image A还是image B。

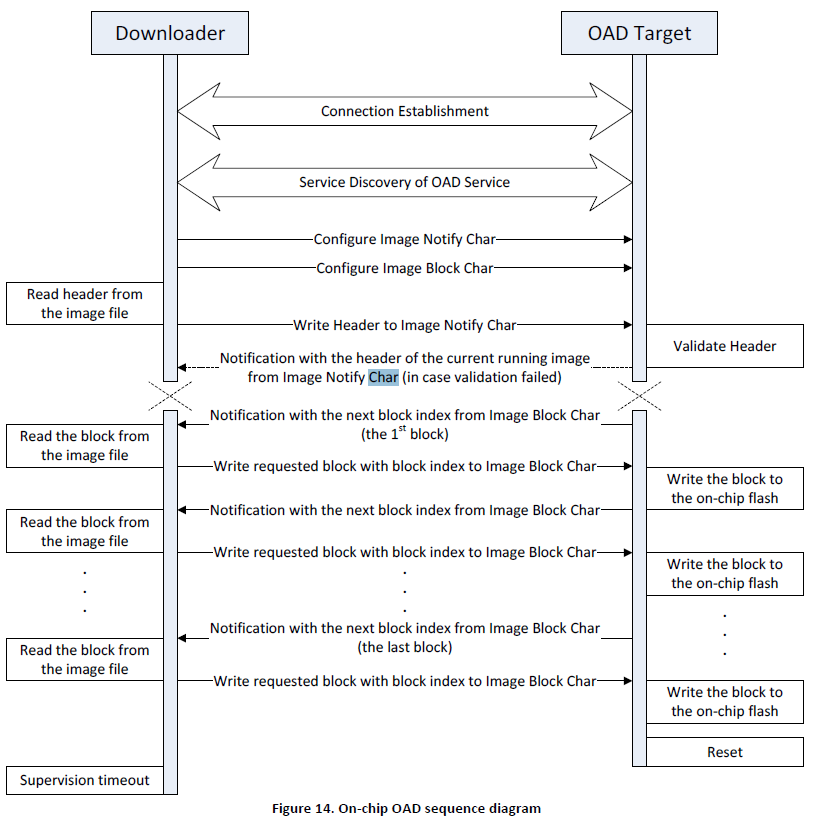
如果OAD Target决定接受OAD image，OAD target将向downloader发送一个OAD image Block Characteristics中的notify来向downloader请求新image的第一个数据块。如果OAD Target发现new image不符合开始OAD的标准。它将发送一个OAD image Identify Characteristics中的notify来告知downloader。OAD Target 发送的notify包含自己的Image Header用来表示拒绝。在这种情况下OAD的进程将在Figure 14中虚线X的地方终止。

7.3.5 Image Block Transfers

Image Block Characteristics可以让两个设备一次请求和相应一个数据块传输。Image 数据块的大小定义为16 byte, 见oad.h中的OAD\_BLOCK\_SIZE。O5AD Target向Image Block Characteristics发送一个包含正确的数据块的索引的notify，以此来向downloader请求一个image的数据块。然后Downloader向Image Block Characteristics中写入image的数据块来相应OAD target的请求。当OAD Target准备好消化下一个image数据块的时候，它将向Image Block Characteristics发送包含需要的数据块的索引的notify。Downloader随后相应这个请求。

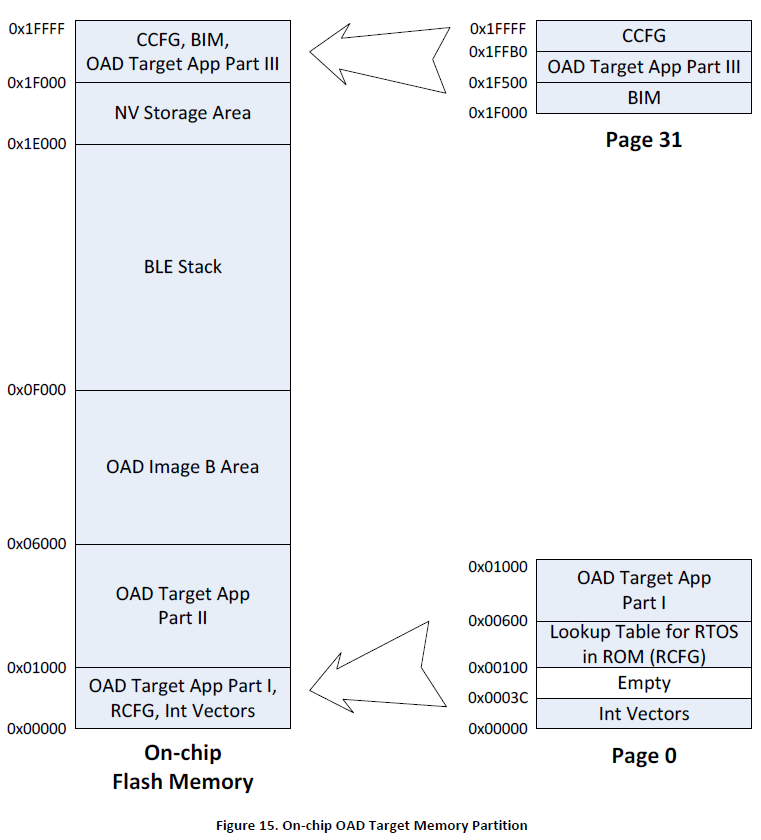
7.3.6 Completion of the On-chip OAD Process

当OAD Target收到最后一个数据块后，它将计算整个储存的OAD image的CRC。OAD Target以此来检验image是否被正常接收并正确存储到flash中。然后OAD Target将废除自己的image并且reset使BIM可以运行新的image替代原来的image。然后烦恼就到了downloader那里。在OAD target检验和实例化的过程中，downloader将会遭遇到很多次的BLE连接丢失。Downloader会重新scanning，重新建立连接并检验新的image是否真的在运行。



7.3 OAD Target

在片内OAD时，OAD Target的flash中有Interrupt Vector, RCFG,永久保留的OAD Target App(Image A),Image B, BLE stack, NV Storage Area, BIM, 和CCFG。如Figure 15所示。



BIM的设计提供了一种灵活性，可以有两个正确的image随时准备运行。BIM决定运行哪个image。只有image B可供下载。OAD Target APP也就是image A是永久保留的。它依赖于在flash的第一页和最后一页的代码。