具UID進階保護的IO切換範例

NuMicro® 32 位系列微控制器範例代碼介紹

文件資訊

代碼簡述	透過判斷自定義 UID 決定 IO 是否切換的範例代碼
BSP 版本	M051 Series BSP CMSIS v3.01.001
開發平台	NuTiny–EVB–M051_V3.0

The information described in this document is the exclusive intellectual property of Nuvoton Technology Corporation and shall not be reproduced without permission from Nuvoton.

Nuvoton is providing this document only for reference purposes of NuMicro microcontroller based system design. Nuvoton assumes no responsibility for errors or omissions.

All data and specifications are subject to change without notice.

For additional information or questions, please contact: Nuvoton Technology Corporation.

www.nuvoton.com

1 功能介紹

1.1 簡介

Nuvoton M051 系列微處理器提供UID (Unique Identifier)，開發者在應用上可透過識別UID的正確性，決定應用是否繼續執行，確保產品不被任意複製仿冒。單純的UID識別安全性似乎不足，因此將提供一個可自行增加識別複雜度範例，開發者可以基於微處理器的UID，再進行自定義的運算，使用運算過的UID識別有更佳的安全性。

1.2 原理

為了方便開發可直接將晶片UID讀出並加以運算，接著合併應用程序再寫入晶片，此範例分為三個區塊，請參考圖1-1，下列將對每區塊做說明:

1. **NuLink.exe** : Nuvoton 提供的簡易工具，必須搭配 NuLink ICE 使用，在此使用 NuLink.exe 進行 UID 讀取及燒入修改後的應用。
2. **TCDEF.exe** : Visual C++ 所編譯，提供將 NuLink 讀回的 UID 經自定義運算後，與 Keil 所產生的應用 bin 檔做合併。
3. **APROM.bin** : 開發者應用專案，必須包含預留運算後 UID 的區域，及如何識別運算後 UID 的判斷程序。

方便操作，關於上述流程，最後使用批次檔將流程整合，若開發者已完成UID自定義運算，及如何識別UID自定義運算後的程序，直接操作批次檔即可。

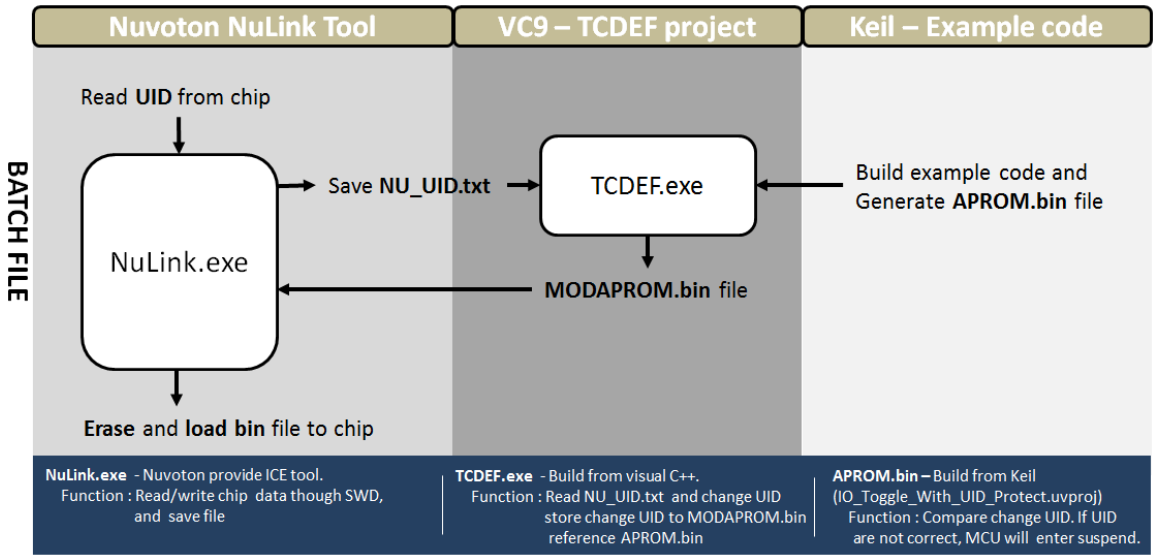

圖1-1 範例流程簡介

從晶片讀出的UID執行完自定義運算後，將存放於APROM保留位置，APROM保留位置在 example code 與 TCDEF.exe 定義要相同，如圖1-2 。

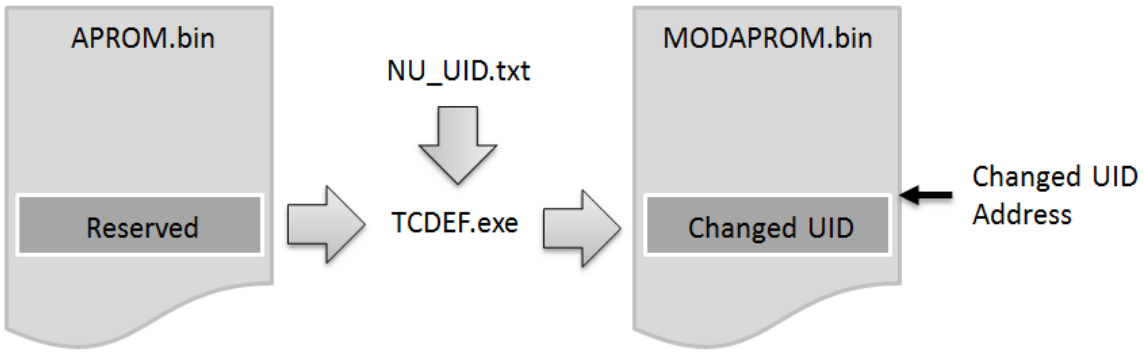

圖1-2 自定義運算後UID的存放位置

此範例自定義運算的部分預留，提供整個流程方法，最後比較晶片UID及存放於APROM的UID是否相同。

1.3 執行結果

1. 執行 IO_Toggle_With_UID_Protect.bat，顯示如下圖 1-3 command line 視窗，執行上述所介紹之流程，完成燒入後，按下任意鍵將結束 command line 視窗，晶片將重新執行自定義

UID 的應用程序。

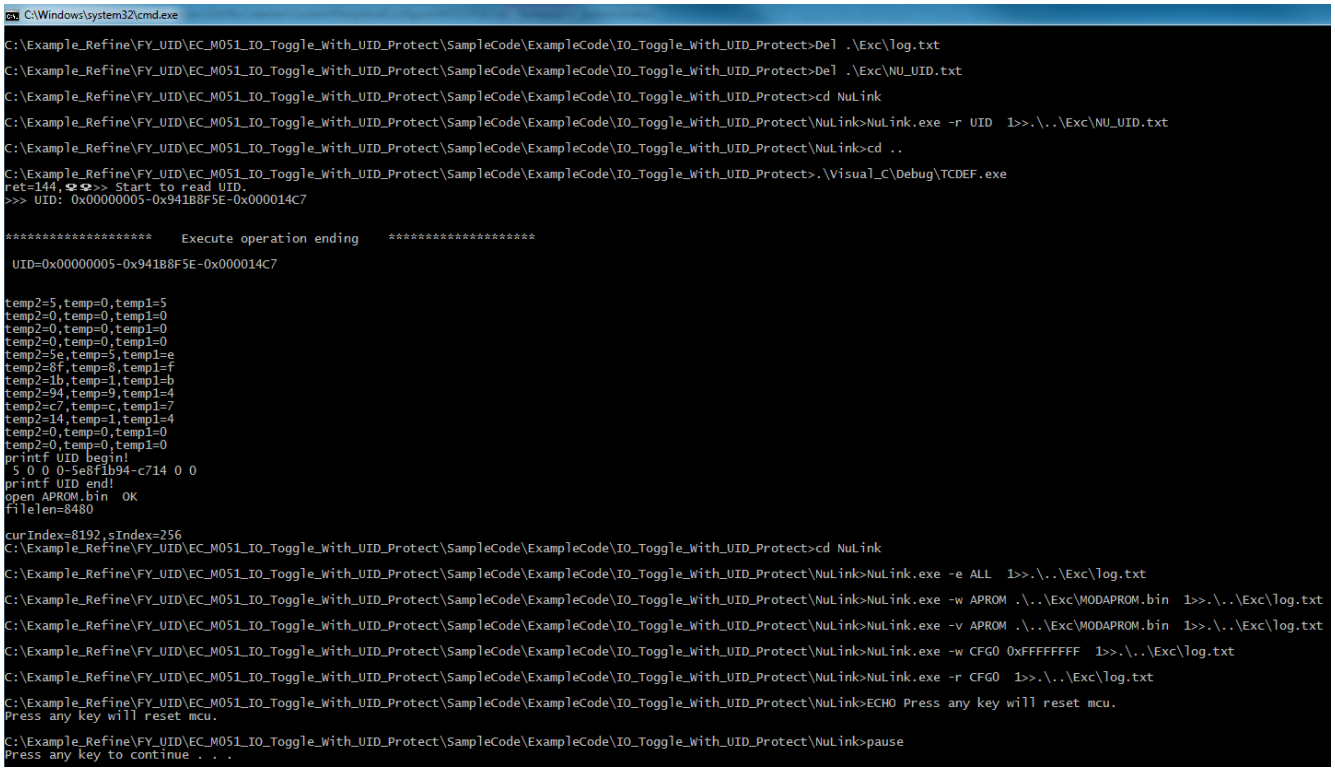

圖1-3 批次檔執行結果

2. 比對晶片 UID 與 自定義運算後 UID 相同，晶片將持續由 PB13 Toggle。

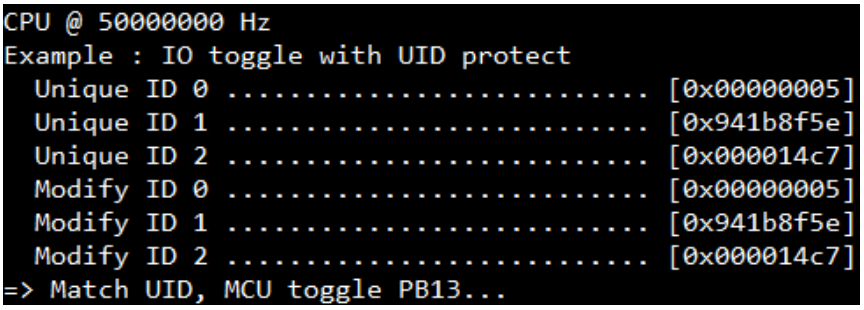

圖1-4 由UART輸出範例執行結果

2 代碼介紹

2.1 Batch file - IO_Toggle_With_UID_Protect.bat

刪除 log.txt and NU_UID.txt file

```
Del .\Exc\log.txt
Del .\Exc\NU_UID.txt
```

讀取晶片 UID 並儲存於 NU_UID.txt file

```
NuLink.exe -r UID >> .\..\Exc\NU_UID.txt
```

執行 TCDEF.exe

```
.\Visual_C\Debug\TCDEF.exe
```

晶片抹除

```
NuLink.exe -e ALL >> .\..\Exc\log.txt
```

燒入 MODAPROM.bin 並驗證

```
NuLink.exe -w APROM .\..\Exc\MODAPROM.bin >> .\..\Exc\log.txt
NuLink.exe -v APROM .\..\Exc\MODAPROM.bin >> .\..\Exc\log.txt
```

寫入 Config0 並讀出存於 log.txt

```
NuLink.exe -w CFG0 0xFFFFFFFF >> .\..\Exc\log.txt
NuLink.exe -r CFG0 >> .\..\Exc\log.txt
```

晶片重新執行

```
NuLink.exe -reset
```

2.2 TCDEF.exe

自定義UID存放開始位置及位移

```
#define APROMUIDADD                 0x2000  //Store UID change data start address of APROM
#define UIDOFFSET                   0x100   //Store UID change data offset of APROM
```

開發者自定義UID運算編輯函式

```
void changUIDData()
{
    int i = 0;
    for (i = 0; i < 12; i++);
    /************* User change UID implement ***************/
}
```

2.3 KEIL – Example code

自定義UID存放位置保留及定義，必須與TCDEF.exe 定義相同

```
#define UID_START_ADDR              0x00002000   // UID start address of APROM
#define UID_ADDR_OFFSET             0x100        // UID address offset of APROM

__attribute__((at(UID_START_ADDR + UID_ADDR_OFFSET))) static const uint32_t
gau32UIDAddr[4]= {2,2,2};
```

判斷晶片UID是否與自定義運算後的UID相同，若有自定義運算，需自行加入如何判讀自定義UID。

```
/************* User change UID compare implement ***************/
/* Compare original UID and change UID */
if((au32mcuUID[0] == au32modfiyUID[0]) && (au32mcuUID[1] == au32modfiyUID[1]) &&
    (au32mcuUID[2] == au32modfiyUID[2]))
    {
        printf("=> Match UID, MCU toggle PB13...\n");
        while(1)
        {
            Delay_count(500);
            P35 = 0;
            Delay_count(500);
            P35 = 1;
        }
    }
```

3 軟體與硬體環境

- **軟體環境**
  - BSP 版本
    - M051 Series BSP CMSIS v3.01.001
  - IDE 版本
    - Keil uVersion 5.24
  - Visual C++ 版本
    - Microsoft Visual C++ 2008
  - NuLink.exe 版本
    - Nuvoton NuLink Command Tool v2.06.6871
- **硬體環境**
  - 電路元件
    - NuTiny–EVB–M051_V3.0

4 目錄資訊

EC_M051_IO_Toggle_With_UID_Protect	
Library	Sample code header and source files
CMSIS	Cortex® Microcontroller Software Interface Standard (CMSIS) by Arm® Corp.
Device	CMSIS compliant device header file
StdDriver	All peripheral driver header and source files
SampleCode	
ExampleCode	Source file of example code
IO_Toggle_With_UID_ Protect	
KEIL	Example files of KEIL project.
Exc	Temporary and log files.
NuLink	Nuvoton NuLink tools.
Visual_C	Visual C++ project for UID changed.

5 如何執行範例程式

1. 根據目錄資訊章節進入 ExampleCode 路徑中的 KEIL 資料夾，雙擊 IO_Toggle_With_UID_Protect.uvproj。
2. 進入編譯模式介面
   a. 編譯
3. 執行 IO_Toggle_With_UID_Protect.bat
   a. 確認 MCU 及 NuLink 已正確連接至 PC.
   b. 執行 UID 運算及燒入程序
   c. 重新執行晶片程序

6 修訂紀錄

Date	Revision	Description
Jul. 16, 2019	1.00	1. 初始發佈.

Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvoton as a result of customer's Insecure Usage, customer shall indemnify the damages and liabilities thus incurred by Nuvoton.

Please note that all data and specifications are subject to change without notice.
All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.