M031 LDROM和APROM程式綁定UID

NuMicro® 32位系列微控制器範例代碼介紹

文件資訊

應用簡述	本範例程式介紹如何通過綁定 MCU 的 UID 碼，實現程式與 MCU 的綁定
BSP 版本	M031_Series_BSP_CMSIS_V3.04.000
開發平台	NuMaker-M032SE V1.3

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 and microprocessor 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. 概述

新唐的 M031 系列 MCU，每一顆都有一個 96 位元的唯一 ID（UID）碼，本文介紹如何將程式綁定 UID 碼，以避免他人將 MCU 中的韌體拷貝出來，燒錄到新的 MCU，複製出一樣的產品。

1.1 原理

本範例程式會將 LDROM 和 APROM 程式中都加入對 UID 碼的判斷，來決定程式的執行流程，這樣儘管將執行正常的 MCU 的 LDROM 和 APROM 韌體讀出來燒錄到另外一顆同型號的 MCU 中，也得不到正常的執行結果。

有時候，為了方便用戶升級程式，需要將韌體發給用戶進行升級，但又希望升級的機器限制在已經燒錄過 LDROM 程式的 MCU，通過本範例程式的方式，便可實現該功能。

本範例程式包含兩個程式“LDROM_Bind_UID”和“APROM_Bind_UID”。“LDROM_Bind_UID”放於 LDROM，其密鑰判斷流程如圖 1-1 所示；“APROM_Bind_UID”放於 APROM，其密鑰判斷流程如圖 1-2 所示。

注：“LDROM_Bind_UID”會用到 SRecord 工具包（http://srecord.sourceforge.net/），使用 srec_cat.exe 將編譯生成的程式檔及密鑰檔合成一個檔“LDROM_Bind_UID.bin”。

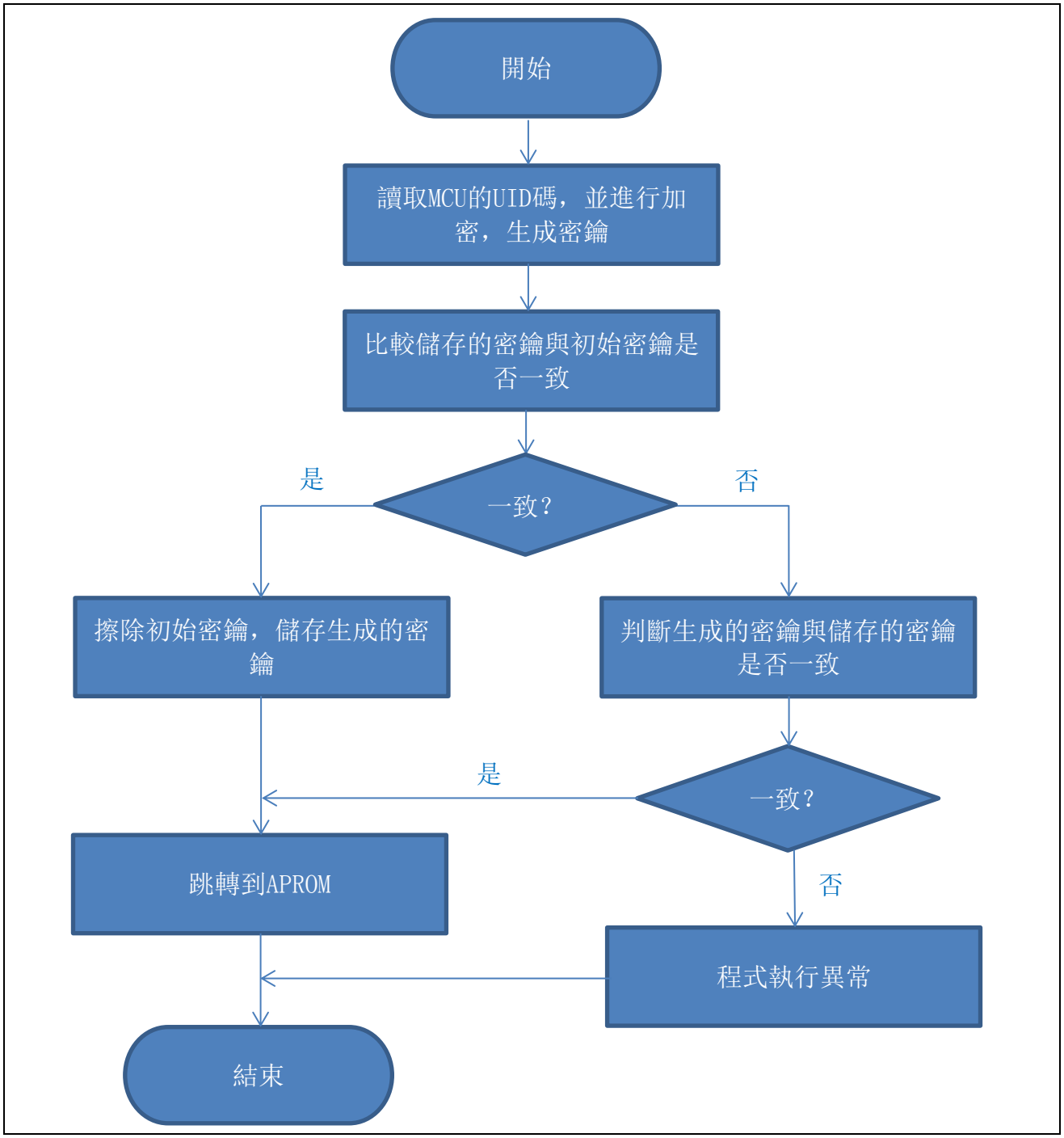

圖 1-1 LDROM 程式密鑰判斷流程圖

注：必須保證產品出廠之前，MCU 已經上電執行過一次，以保證儲存在 LDROM 中的初始密鑰被擦除。

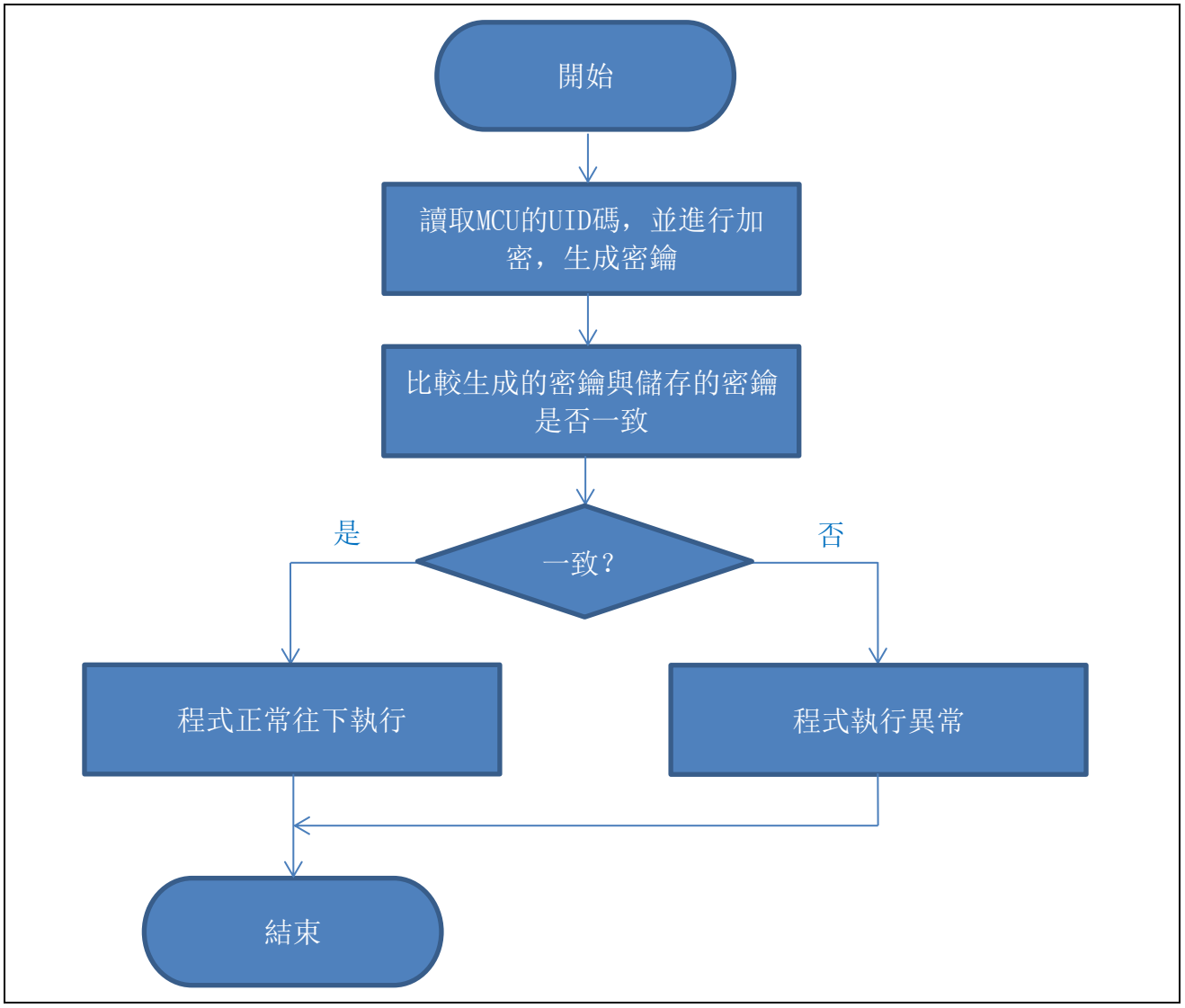

圖 1-2 APROM 程式密鑰判斷流程圖

1.2 執行結果

通過“NuMicro ICP Programming Tool”將 LDROM_Bind_UID.bin 及 APROM_Bind_UID.bin 燒錄到“NuMaker-M032SE V1.3”板子，同時配置 MCU 的啟動方式為“LDROM with IAP”，執行時的輸出資訊如圖 1-3 所示。

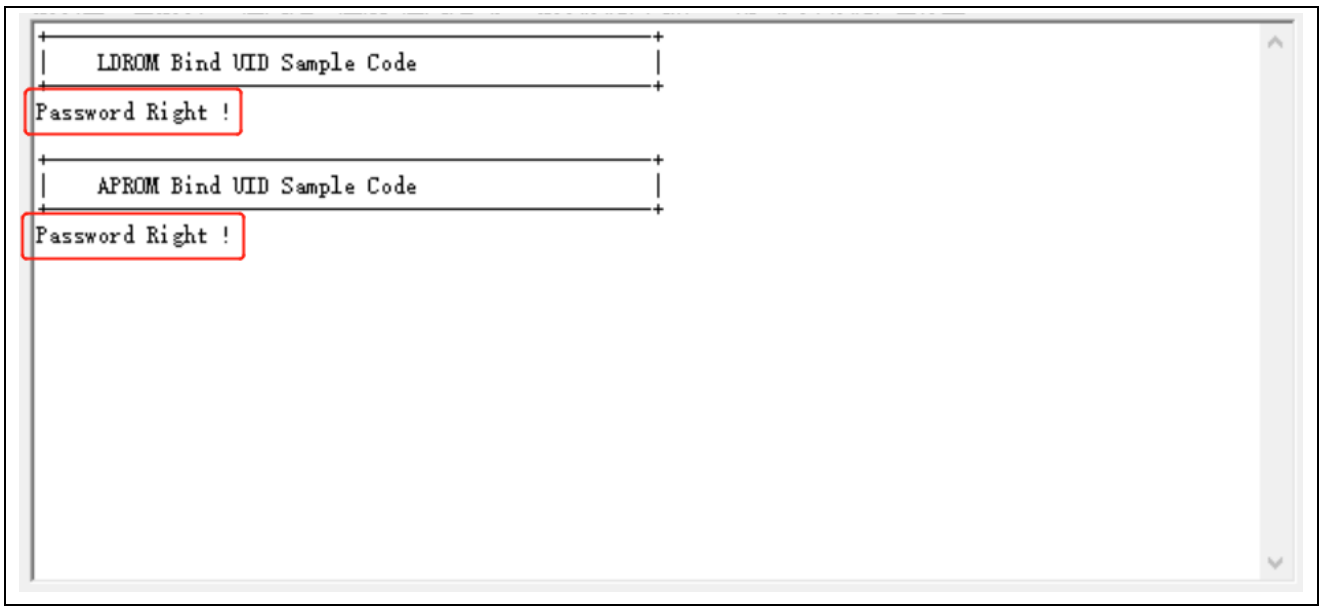

圖 1-3 執行正常輸出資訊

通過 “NuMicro ICP Programming Tool” 從 “NuMaker-M032SE V1.3” 板子讀出 MCU 的 LDROM 和 APROM 程式，然後燒錄到另外一塊 “NuMaker-M032SE V1.3” 板子，同樣設置 MCU 的啟動方式為 “LDROM with IAP” ，執行時輸出資訊如圖 1-4 所示。

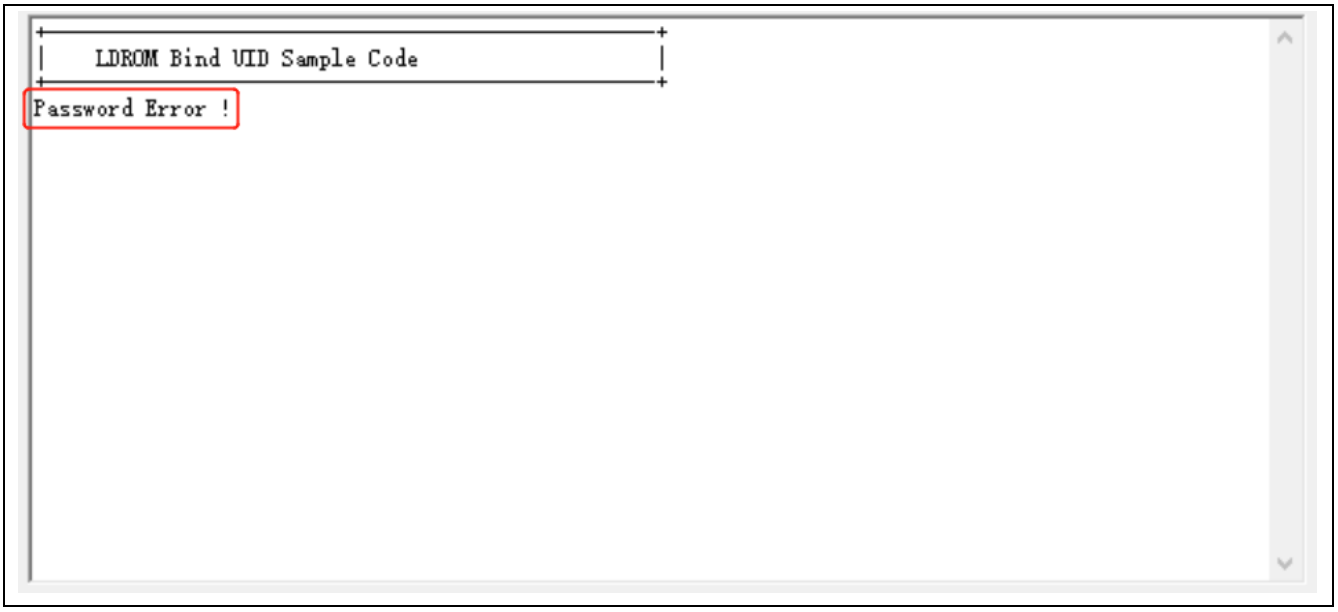

圖 1-4 LDROM 程式執行異常輸出資訊

單獨將讀出來的 APROM 程式，燒錄到另外一塊 “NuMaker-M032SE V1.3” 板子，且配置 MCU 的啟動方式為 “APROM” ， 執行時輸出資訊如圖 1-5 所示。

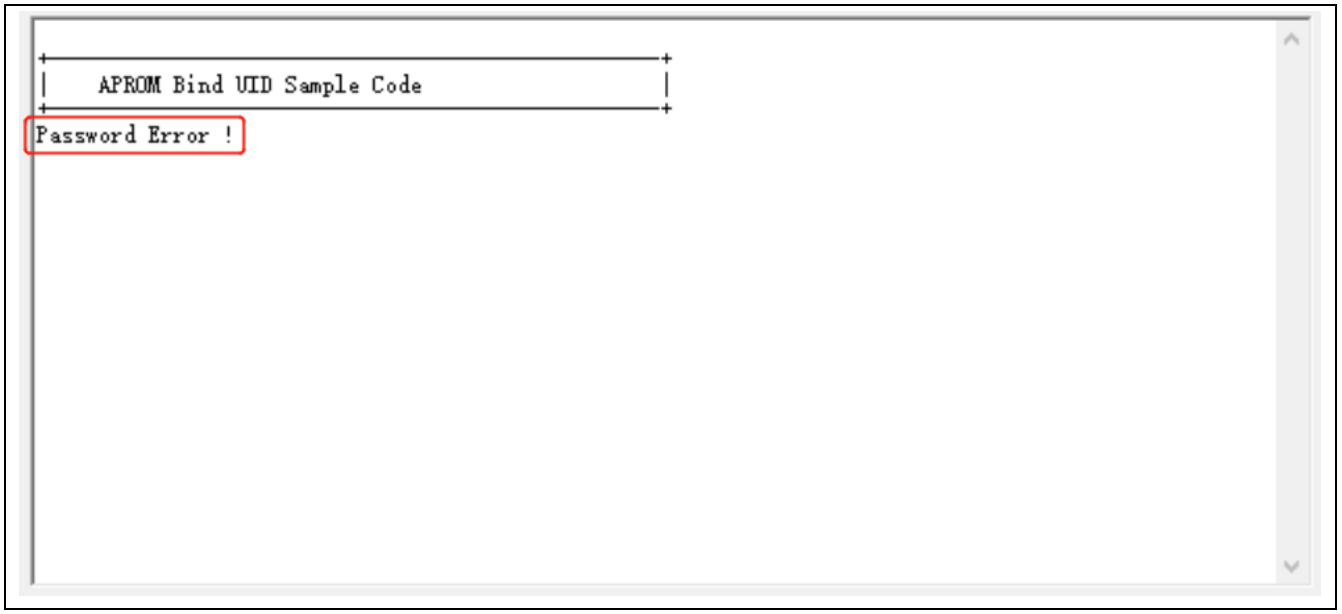

圖 1-5 APROM 程式執行異常輸出資訊

2. 代碼介紹

初始密鑰設置（用戶可自行更改）：

```
#define INIT_PASSWORD_0       0x12121212 /* Defined by user */
#define INIT_PASSWORD_1       0x34343434 /* Defined by user */
#define INIT_PASSWORD_2       0x56565656 /* Defined by user */
```

將 UID 進行加密（用戶可以根據自己的加密算法進行更改）：

```
void UID_Encrypt(uint32_t au32Uid[3])
{
    uint8_t i;

    /* Encrypt the UID, users can change it according to their encryption algorithm */
    for(i = 0; i < 3; i++)
    {
        au32Uid[i] = (~au32Uid[i]) * 5 / i;
    }
}
```

判斷密鑰與初始密鑰是否一致，若一致，則擦除初始密鑰，寫入由 UID 加密後的新密鑰；若不一致，判斷 UID 加密後的密鑰與儲存的密鑰是否一致：

```
uint8_t UID_PasswordCheck(void)
{
    uint8_t i;
    uint32_t au32Uid[3];
    uint32_t *pu32Password = (uint32_t *)PASSWORD_ADDR;

    UID_Read(au32Uid);
    UID_Encrypt(au32Uid);

#if defined(PASSWORD_INIT_ENABLE)
if((pu32Password[0] == INIT_PASSWORD_0) && (pu32Password[1] == INIT_PASSWORD_1)
&& (pu32Password[2] == INIT_PASSWORD_2))
    {
        UID_PasswordWrite(au32Uid);
    }
    else
#endif
    {
        for(i = 0; i < 3; i++)
        {
            if(au32Uid[i] != pu32Password[i])
            {
                return 0;
            }
        }
    }

    return 1;
}
```

3. 軟體與硬體需求

3.1 軟體需求

- BSP 版本
  - M031_Series_BSP_CMSIS_V3.04.000
- IDE 版本
  - Keil uVersion 4.74

3.2 硬體需求

- 電路元件
  - NuMaker-M032SE V1.3

4. 目錄資訊

EC_M031_LDROM_APROM_Bind_UID_V1.00	
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

圖 4-1 目錄資訊

5. 範例程式執行

1. 根據目錄資訊章節進入 ExampleCode 路徑中的 KEIL 資料夾，分別雙擊 LDROM_Bind_UID.uvproj 和 APROM_Bind_UID.uvproj。
2. 進入編譯模式介面
   - 編譯
3. 執行程式
   - 通過 NuMicro ICP Programming Tool 燒錄程式及配置
   - 執行程式

6. 修訂紀錄

Date	Revision	Description
2022.04.29	1.00	初始發布。

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.