M031 LDROM和APROM程序绑定UID

NuMicro® 32位系列微控制器范例代码介绍

文件信息

应用简述	本范例代码介绍如何通过绑定 MCU 的 UID 码，实现程序与 MCU 的绑定
BSP 版本	M031_Series_BSP_CMSIS_V3.04.000
开发平台	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，每一颗都有一个 96 位的唯一 ID（UID）码，本文介绍如何将程序绑定 UID 码，以避免他人将 MCU 中的固件拷贝出来，烧录到新的 MCU，复制出一样的产品。

1.1 原理

本示例代码会将 LDROM 和 APROM 程序中都加入对 UID 码的判断，来决定程序的执行流程，这样尽管将运行正常的 MCU 的 LDROM 和 APROM 固件读出来烧录到另外一颗同型号的 MCU 中，也得不到正常的运行结果。

有时候，为了方便用户升级程序，需要将固件发给用户进行升级，但又希望升级的机器限制在已经烧录过 LDROM 程序的 MCU，通过本示例代码的方式，便可实现该功能。

本示例代码包含两个工程“LDROM_Bind_UID”和“APROM_Bind_UID”。“LDROM_Bind_UID”放于 LDROM，其密钥判断流程如图 1-1 所示；“APROM_Bind_UID”放于 APROM，其密钥判断流程如图 1-2 所示。

注：“LDROM_Bind_UID”会用到 SRecord 工具包（http://srecord.sourceforge.net/），使用 srec_cat.exe 将编译生成的程序文件及密钥文件合成一个文件“LDROM_Bind_UID.bin”。

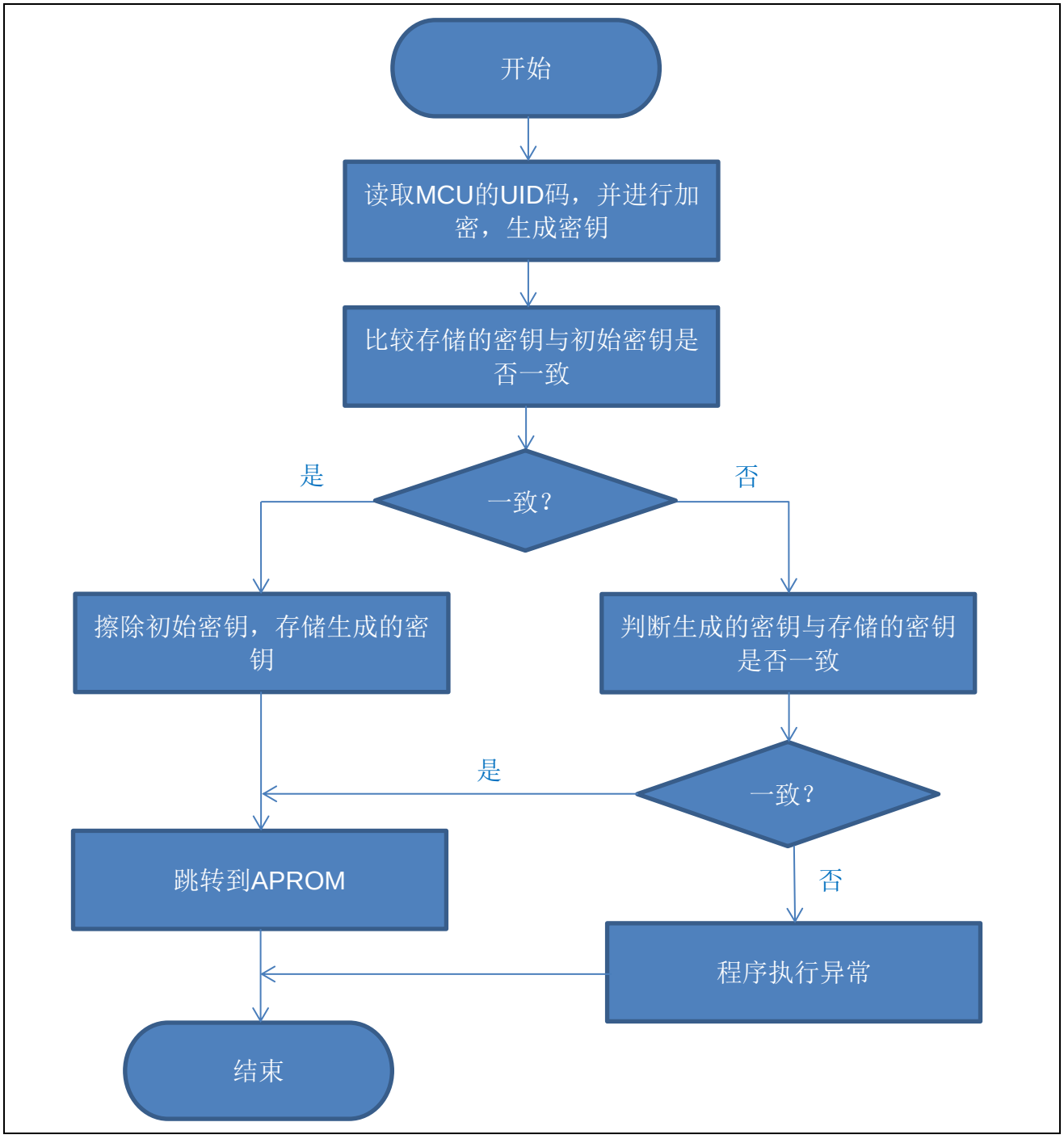

图 1-1 LDROM 程序密钥判断流程图

注：必须保证产品出厂之前，MCU 已经上电运行过一次，以保证存储在 LDROM 中的初始密钥被擦除。

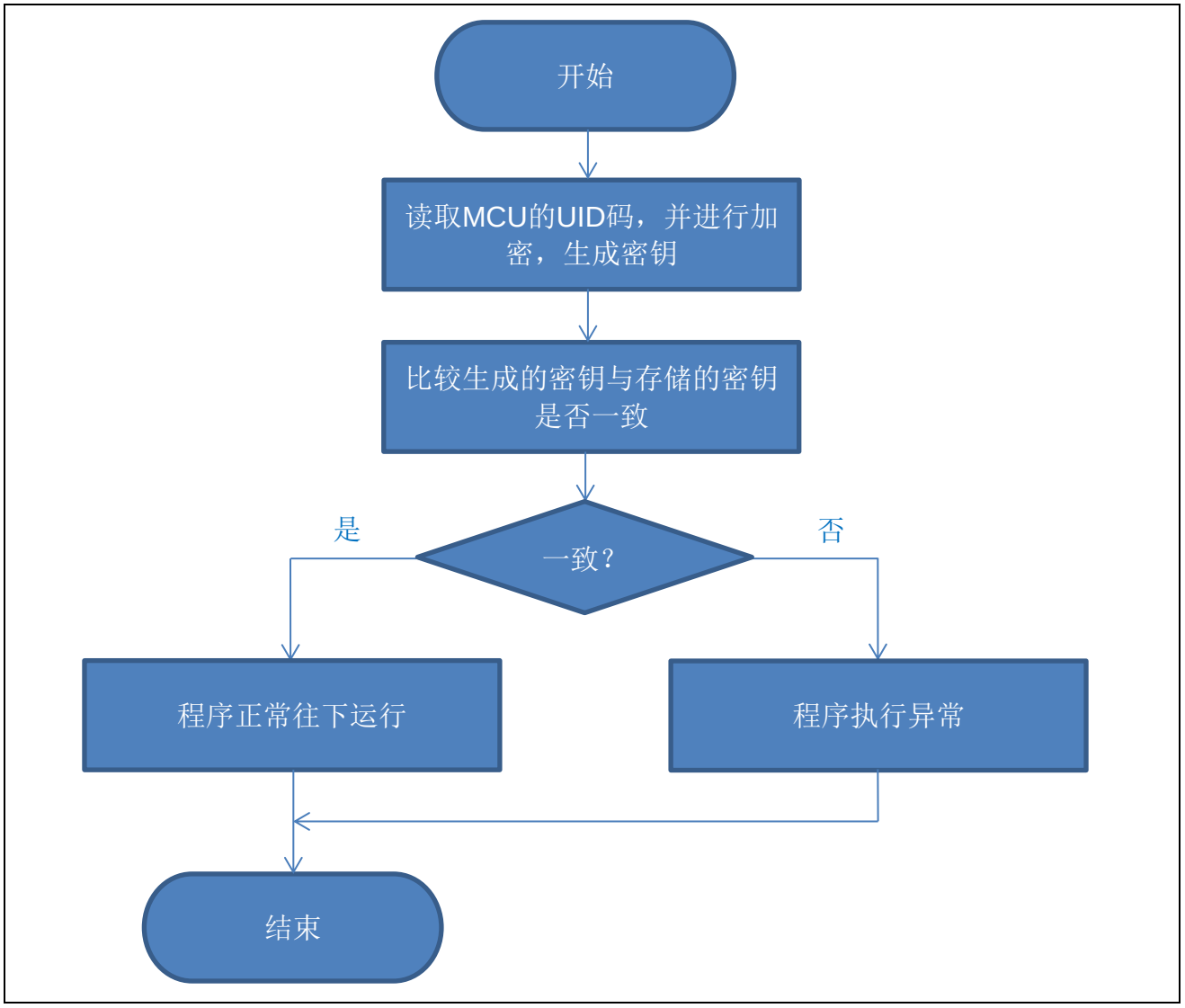

图 1-2 APROM 程序密钥判断流程图

1.2 执行结果

通过“NuMicro ICP Programming Tool”将 LDROM_Bind_UID.bin 及 APROM_Bind_UID.bin 烧录到“NuMaker-M032SE V1.3”板子，同时配置 MCU 的启动方式为“LDROM with IAP”，运行时的打印信息如图 1-3 所示。

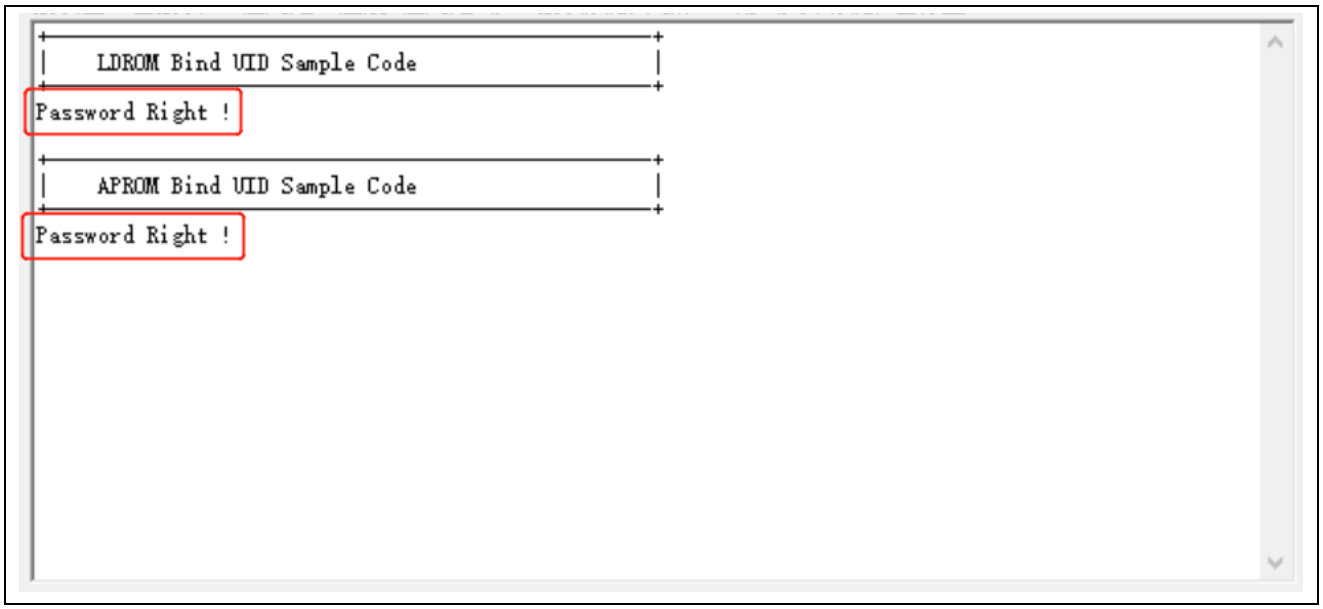

图 1-3 运行正常打印信息

通过“NuMicro ICP Programming Tool”从“NuMaker-M032SE V1.3”板子读出 MCU 的 LDROM 和 APROM 程序，然后烧录到另外一块“NuMaker-M032SE V1.3”板子，同样设置 MCU 的启动方式为“LDROM with IAP”，运行时打印信息如图 1-4 所示。

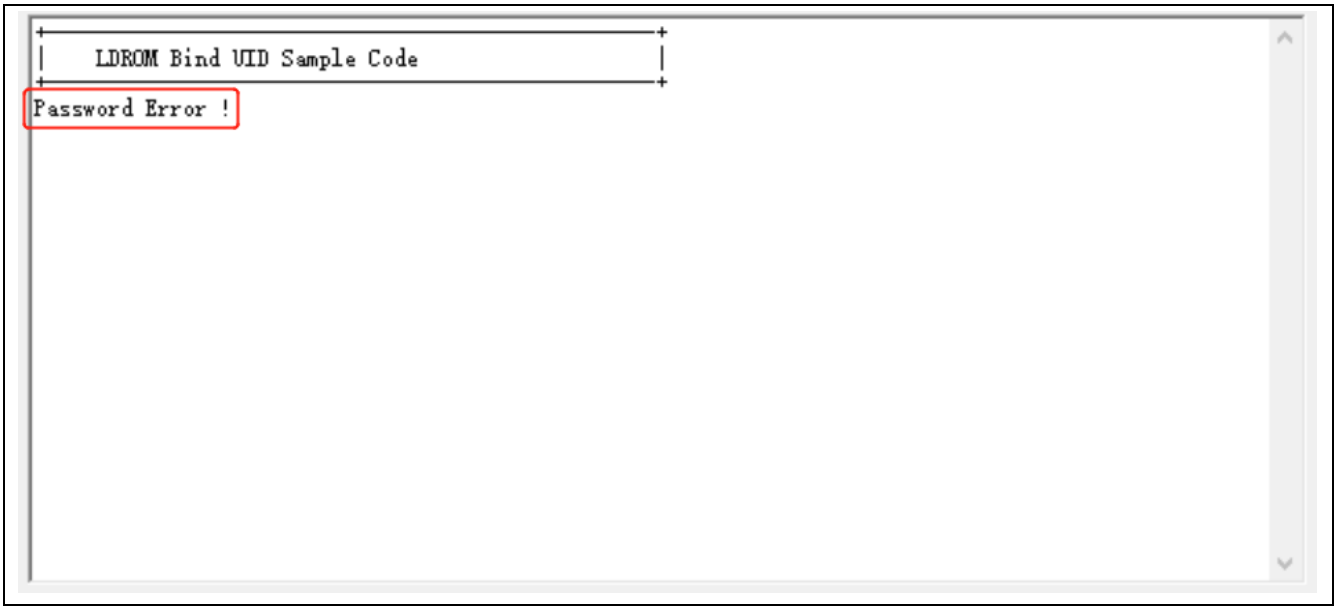

图 1-4 LDROM 程序运行异常打印信息

单独将读出来的 APROM 程序，烧录到另外一块“NuMaker-M032SE V1.3”板子，且配置 MCU 的启动方式为“APROM”，运行时打印信息如图 1-5 所示。

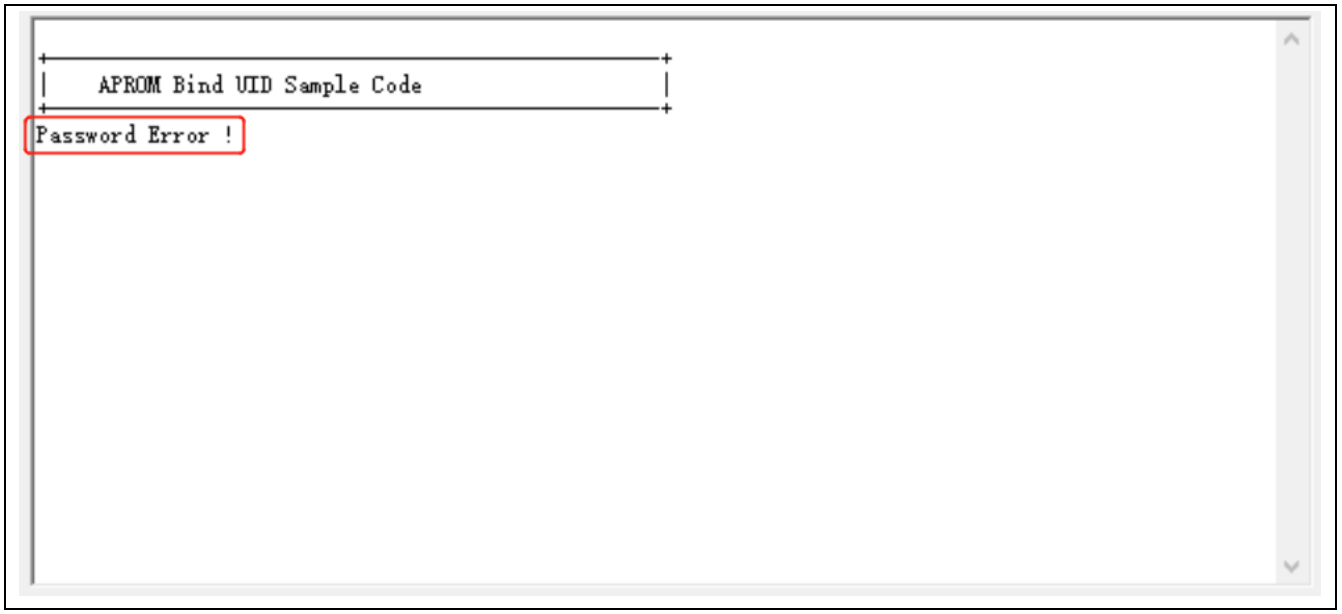

图 1-5 APROM 程序运行异常打印信息

2. 代码介绍

初始密钥设置（用户可自行更改）：

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

将 UID 进行加密（用户可以根据自己的加密算法进行更改）：

```
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;
    }
}
```

判断密钥与初始密钥是否一致，若一致，则擦除初始密钥，写入由 UID 加密后的新密钥；若不一致，判断 UID 加密后的密钥与存储的密钥是否一致：

```
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. 软件与硬件需求

3.1 软件需求

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

3.2 硬件需求

- 电路组件
  - NuMaker-M032SE V1.3

4. 目录信息

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

图 4-1 目录信息

5. 范例程序执行

1. 根据目录信息章节进入 ExampleCode 路径中的 KEIL 文件夹，分别双击 LDROM_Bind_UID.uvproj 和 APROM_Bind_UID.uvproj。
2. 进入编译模式界面
   - 编译
3. 运行程序
   - 通过 NuMicro ICP Programming Tool 烧录程序及配置
   - 运行程序

6. 修订纪录

Date	Revision	Description
2022.04.29	1.00	初始发布。.

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.