**HBOT项目软件开发需求**

2023年5月13日

文档历史记录Document history

|  |  |  |  |
| --- | --- | --- | --- |
| 版本Rev. | 描述Description | 日期Date | 编辑Edited by |
| V1.0 | 初版制订Draft | May 13, 2023 | Walter |
| V1.1 | 增加串口通讯协议 | May 30, 2023 | Walter |
| V1.2 | 1. 增加广播名字 2. 增加用户私有服务说明 |  |  |

目录Contents

[功能需求简介 2](#_Toc134871555)

[蓝牙服务 2](#_Toc134871556)

[串口通讯 2](#_Toc134871557)

[GPIO功能 2](#_Toc134871558)

[DFU 服务 4](#_Toc134871559)

[Primy service: 00001530-1212-efde-1523-785feabcd123 4](#_Toc134871560)

[DFU设计例程DFU designing examples 4](#_Toc134871561)

[附录Appendix 5](#_Toc134871562)

[AES-128加密AES-128 encryption 5](#_Toc134871563)

[AES简介 5](#_Toc134871564)

[AES-128\_ECB demo code 6](#_Toc134871565)

# 1 功能需求简介

* 蓝牙服务
* 串口通讯功能，半双工串口通讯（后接RS-485）
* GPIO功能，部分GPIO的输入及输出功能
* DFU功能
* 蓝牙通讯加密功能（项目临近结束再完成）

蓝牙服务

类似桑拿房实现的如蓝牙配对，数据传输，加密等功能。蓝牙名称：OneBase HBOT

软件需求：

1. 完成蓝牙通讯的接收函数，能接收来自APP的数据包
2. 完成蓝牙通讯的发送函数，能发送自定义数据包到APP
3. 根据通讯协议文档Waylen Allen - Master Firmware Communication Specification v1.0.xlsx解析自定义数据。这部分工作会比较繁琐，请查阅通讯协议文档评估，如果工作量超出原来报价，自定义数据的解析可以交给我来做。(客户不愿意增加费用)
4. 提供自定义服务UUID列表（类似桑拿房）
5. 按RESET键（GPIO P1.06）清除之前绑定的ShortUserID并进入配对模式

# 2 串口通讯

串口配置:9600,8,N,1

通讯模式：半双工

硬件配置：Tx管脚P0.26；Rx管脚P1.15

软件需求：

1. 完成串口初始化函数
2. 完成串口发送函数
3. 完成串口接收函数

## 串口通讯简要说明

串口通讯主要有两个作用，分别是：

* 控制空调开关及读取空调工作状态
* 读取传感器数据

## 空调串口通讯范例

串口通讯采用MODBUS协议。

串口通讯读写空调范例：

开空调

[10:34:44.597]发→◇18 06 00 0C 00 01 8A 00

[10:34:44.633]收←◆18 06 00 0C 00 01 8A 00

读取空调状体

[10:34:45.354]发→◇18 03 00 0C 00 01 46 00

[10:34:45.378]收←◆18 03 02 00 01 64 46

关空调

[10:34:46.019]发→◇18 06 00 0C 00 00 4B C0

[10:34:46.041]收←◆18 06 00 0C 00 00 4B C0

读取空调状态

[10:34:46.739]发→◇18 03 00 0C 00 01 46 00

[10:34:46.761]收←◆18 03 02 00 00 A5 86

## 传感器串口通讯范例

读取湿度传感器数据

[10:34:44.597]发→◇81 03 00 30 00 01 46 00

[10:34:44.633]收←◆81 03 03 01 00 40 64 46

读取10个传感器数据

[10:34:44.105]发→◇81 03 00 30 00 0A DA 02

[10:34:44.633]收←◆81 03 22 01 00 40 01 00 40 01 00 40 01 00 40 01 00 40 01 00 40 00 40 00 40 01 00 40 01 00 40 01 00 40 01 00 40 4E DD

# 3 GPIO功能

软件需求

1. 完成下列GPIO配置

|  |  |  |  |
| --- | --- | --- | --- |
| GPIO管脚名称 | GPIO类型 | 宏定义名称 | 用途说明 |
| P0.15 | 输入 | IO\_Oxygen\_IN | 制氧机的工作状态：0关机1开机 |
| P0.22 | 输入 | IO\_AirComp\_IN | 空压机的工作状态：0关机1开机 |
| P1.06 | 输入 | IO\_RESET | 清除ShortUserID并进入配对模式 |
| P0.13 | 输出 | IO\_Oxygen\_OUT | 制氧机控制管脚：0关机1开机 |
| P0.20 | 输出 | IO\_AirComp\_OUT | 空压机的控制管脚：0关机1开机 |

2) 完成输入管脚的电平读取函数（两个输入IO需要做100ms的防抖处理）

3）完成输出管脚的电平输出函数（能写0和1）

air conditioner

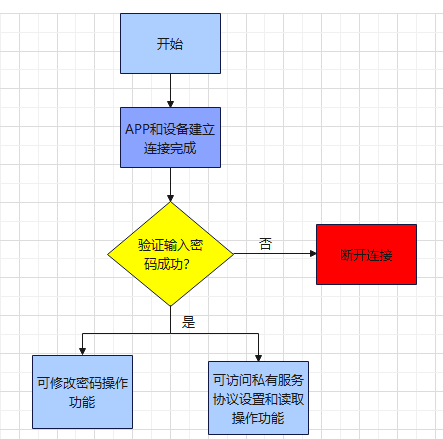
# 蓝牙广播名字

OneBase HBOT

# 蓝牙用户私有服务

## Primy service: 0000 FF00-0000-1000-8000- 00805f9b34fb

|  |  |  |  |
| --- | --- | --- | --- |
| Type | UUID | Feature | Description |
| 用于密码验证 | 0000FF01-0000-1000-8000-00805f9b34fb | W/N | 默认密码：  Default pw：  12345678 |
| 自定义命令反馈与  输入  Device control/sync related  data exchange | 0000FF02-0000-1000-8000-00805f9b34fb | W/N |  |



# 蓝牙DFU 服务

For detailed explanation of DFU, Please refer to Nordic website

## Primy service: 00001530-1212-efde-1523-785feabcd123

|  |  |  |  |
| --- | --- | --- | --- |
| Type | UUID | Feature | Description |
| DFU Packet | 00001532-1212-efde-1523-785feabcd123 | W | 无反馈写  Write  without response |
| DFU Control Point | 00001531-1212-efde-1523-785feabcd123 | W/N | 设备反馈信息  DFU response |
| DFU Version | 00001534-1212-efde-1523-785feabcd123 | R | 版本Rev |

## DFU设计例程DFU designing examples

For Android: https://github.com/NordicSemiconductor/Android-nRF-Connect

For https://github.com/NordicSemiconductor/Android-nRF-Toolbox

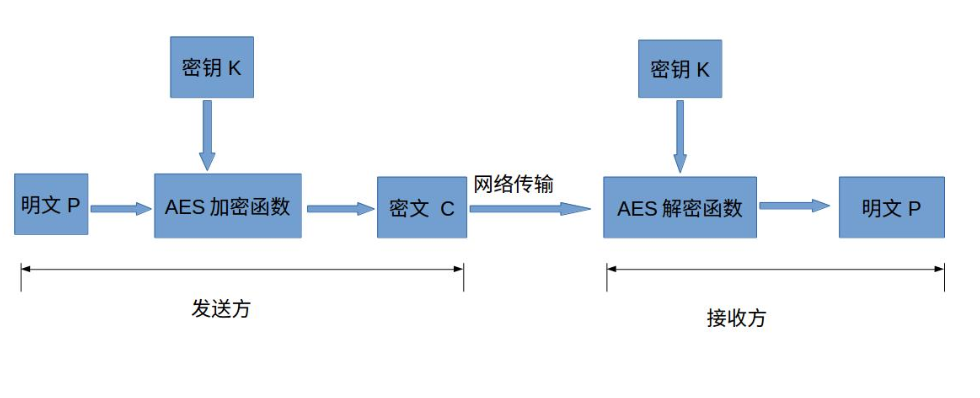
For IOS: https://github.com/NordicSemiconductor/IOS-nRF-Connect

https://github.com/NordicSemiconductor/IOS-nRF-Toolbox

## 附录Appendix

## 5.2.AES-128加密AES-128 encryption

### AES简介



下面简单介绍下各个部分的作用与意义：

（1）明文P：没有经过加密的数据。unencrypted data

（2）密钥K：Key

用来加密明文的密码，在对称加密算法中，加密与解密的密钥是相同的。密钥为接收方与发送方协商产生，但不可以直接在网络上传输，否则会导致密钥泄漏，通常是通过非对称加密算法加密密钥，然后再通过网络传输给对方，或者直接面对面商量密钥。密钥是绝对不可以泄漏的，否则会被攻击者还原密文，窃取机密数据。

（3）AES加密函数：

设AES加密函数为E，则 C = E(K, P),其中P为明文，K为密钥，C为密文。也就是说，把明文P和密钥K作为加密函数的参数输入，则加密函数E会输出密文C。

（4）密文C：经加密函数处理后的数据

（5）AES解密函数：

设AES解密函数为D，则 P = D(K, C),其中C为密文，K为密钥，P为明文。也就是说，把密文C和密钥K作为解密函数的参数输入，则解密函数会输出明文P。

### AES-128\_ECB demo code

1）AES-128\_ECB 加密的密匙是蓝牙连接初始密码（**1234567812345678**）

2）AES-128\_ECB 加密一次只能加密 16 字节通讯数据,通信双方需要按照16字节整数倍进行数据加密，解密。**不够16字节需要补足**

举例：

**明文P**：

0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,

0xA1,0xA2,0xA3,0xA4,0xA5,0xA6,0xA7,0xA8,0xA9,0xAA,0xAB,0xAC,0xAD,0xAE,0xAF,0xA1

**AESKey:1234567812345678**

**（1）加密处理过程：**

**加密后得到数据，即密文为：m\_tmp\_buf：**

    for (uint8\_t i = 0; i < len; i += 16) {

        AES128\_ECB\_encrypt(&AES\_P[i], AES\_Key, &m\_tmp\_buf[i]);

    }

1. **解密过程：**

**密文为：m\_tmp\_buf**

**AESKey：1234567812345678**

  for (uint8\_t i = 0; i < len; i += 16) {

        AES128\_ECB\_decrypt(&tmp\_buf[i], AESKey, &m\_tmp\_buf[i]);

    }

**而后就可以得到对应的明文：temp\_buf了**