1. **实验目的**

* **了解UHF的基本概念、国际标准、协议内容**
* **了解UHF的操作指令**

1. **实验内容**

* **使用UHF900Demo对卡片进行常规操作**

1. **实验环境**

* **UHF900Demo软件**

1. **实验原理**

**4.1UHF协议**

超高频射频识别系统的协议目前有很多种，主要可以分为两大协议制定者：一是 ISO（国际标准化组织）；二是 EPC Global。ISO 组织目前针对 UHF（超高频）频段制定了射频识别协议 ISO 18000－6，而 EPC Global 组织则制定了针对产品电子编码（Electronic Product Code）超高频射频识别系统的标准。目前，超高频射频识别系统中的两大标准化组织有融合的趋势，EPC Class 1 Generation 2 标准可能会变成 ISO 18000-6 标准的 Type c。本文主要讨论的是针对 ISO18000－6标准的射频识别系统，本节讨论的是 ISO 18000－6 协议中与系统架构相关的物理层参数。

对于ISO18000－6协议有两个标准可供选择，分别是ISO18000-6B和ISO18000-6C（EPC C1G2）标准。这两个标准可以说各有优点。

**ISO18000-6B标准**

准定位于通用标准，应用比较成熟，产品性能相对稳定，数据格式和标准相对简单。ISO18000-6B标准的主要特点包括：标准成熟、产品稳定、应用 广泛；ID号全球惟一；先读ID号，后读数据区；1024bits或2048bits的大容量；98Bytes或216Bytes的大用户数据区；多标签 同时读取，最多可同时读取数十个标签；数据读取速度为40kbps。符合ISO18000-6B标准的电子标签主要适用于资产管理等领域。目前国内开发的 集装箱标识电子标签、电子车牌标签、电子驾照（司机卡）均采用此标准的芯片。

ISO18000-6B标准的特点，从读取速度和标签数量来讲，在卡口、码头作业等标签数量不大的应用场合，应用ISO18000-6B标准的标签基 本能满足需求。目前，中国海关物流监管系统中所使用的“电子车牌识别系统”使用的就是ISO18000-6B标准的电子标签.

O18000-6B标准的不足之处在于：近几年发展停滞，有被EPC C1G2取代的趋势；用户数据的软件固化技术不太成熟，但这种情况可以通过芯片厂家将用户数据嵌入解决。

**SO18000-6C（EPC C1G2）标准**

RFID超高频高频ISO18000-6C(EPC CLASS1 G2)中文协议标准是针对RFID射频识别应用的一个国际标准，国内称超高频，该标准定义了工作在860Mhz-960Mhz带宽达100MHz下电子标签与阅读器的空气接口及数据通信规范，超高频读写器多采用跳频发射方式，不受不同区域变化时无线电频段的影响，因而允许同一个标签可以在全球任何地方被对应协议的读写器读取。标签具有防冲突性能、可在全球各种环境下部署、具有读/写现场可编程性和更快的标签读/写速度、能在读卡器密集的环境中运行等功能。

ISO18000-6C(EPC CLASS1 G2)标签从逻辑上将标签存储器分为四个存储区，每个存储区可以由一个或一个以上的存储器字组成。这四个存储区是：

1. EPC 区(EPC)：存EPC号的区域，本读写器规定最大能存放15字EPC号。可读可写。
2. TID 区(TID)：存由标签生产厂商设定的 ID 号，目前有4字和8字两种ID 号。可读，不可写。
3. 用户区(User)：不同厂商该区不一样。Inpinj 公司的 G2 标签没有用户区。Philips 公司有28字。可读可写。
4. 保留区(Password)：前两个字是销毁(kill)密码，后两个字是访问(access)密码。可读可写。

四个存储区均可写保护。写保护意味着该区永不可写或在非安全状态下不可写；读保护只有密码区可设置为读保护，即不可读。

SO18000-6C的特点是：速度快，数据速率可达40kbps～640kbps；可以同时读取的标签数量多，理论上能读到1000多个标签；首先读EPC号码，标签 的ID号需要用读数据的方式读取；功能强，具有多种写保护方式，安全性强；

CC1G2标准具有通用性强、符合EPC规则、产品价格低、兼容性好等众多优点。

**SO18000-6C 6B/C协议的区别：**

1. 6B一般用在闭环的领域，像烟草等资产管理领域；6C一般在开环的领域，比如物流行业；

2. ISO18000-6B一次最多可以读取10个标签，用户数据区较大，数据传输速率40Kbps左右，一般用于资产管理领域。

3. EPC C1G2即ISO18000-6C，可同时读取数百个标签，用户数据区较小，数据传输速率在40Kbps-640Kbps,通常用于物流管理。

4. 对于数据存储来说，6B是“前台”形式的，所以要求标签容量很大，而6C是“后台”形式的，读标签时只要读到EPC就行然后再和后台数据库关联读出标签内的数据信息，对标签容量的要求较低。

5. 价格上的差异：6C标签相对6B标签的价格是更加的便宜，降低成本。

4.2命令操作

指令帧类型说明：

|  |  |
| --- | --- |
| 类型 | 描述 |
| 0x00 | 命令帧：由上位机发送给RFID开发板 |
| 0x01 | 响应帧：由RFID开发板返回给上位机 |
| 0x02 | 通知帧：由RFID开发板返回给上位机 |

**每一条指令帧都有对应的响应帧。响应帧表示指令是否已经被执行了。**

**单次轮询指令和多次轮询指令还有相应的通知帧。发送通知帧的个数是由 MCU 根据读取的情况，自主的发给上位机。当读写器读到一个标签就发一个通知帧，而当读写器读到多个标签就发多个通知帧。**

**4.2.1完成一次EPC Class1 Gen2协议中轮询Inventory操作**

该指令中不包含 Select 操作。每次轮询指令执行前后都会自动打开和关闭功放。单次轮询 Inventory 指令中，Query 操作参数由另外一条指令来配置，固件中已经有初始值。单次轮询 Inventory 指令如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Header | Type | Command | PL(MSB) | PL(LSB) | CheckSum | End |
| AA | 00 | 22 | 00 | 00 | 22 | DD |

**4.2.1通知帧定义**

芯片接收到单次轮询指令后，如果能够读到 CRC 校验正确的标签，芯片 MCU 将返回包含 RSSI、PC、EPC和 CRC 的数据。读到一个标签 EPC 就返回一条指令响应，读到多个标签则返回多条指令响应。如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Header | Type | Command | PL(MSB) | PL(LSB) | RSSI | Pc(MSB) | PC(LSB) |
| AA | 02 | 22 | 00 | 11 | C3 | 30 | 00 |
| EPC(MSB) |  |  |  |  |  |  |  |
| E2 | 80 | 68 | 94 | 00 | 00 | 50 | 06 |
|  |  | EPC(LSB) |  | CRC(MSB) | CRC(LSB) | CheckSum | End |
| E4 | 91 | DD | 92 | 96 | D0 | 26 | DD |

指令类型 Type: 0x02 RSSI: 0XC3

指令代码 Command: 0x22 PC: 0x3000

指令参数长度 PL: 0x0011 CRC : 0x96 D0

EPC: 0xE2 80 68 94 00 00 50 06 E4 91 DD 92 校验位 Checksum: 0x26

RSSI 值反映的是芯片输入端信号大小，不包含天线增益和定向耦合器衰减等。RSSI 为芯片输入端信号强度，十六进制有符号数，单位为 dBm。

**4.2.1通知帧定义**

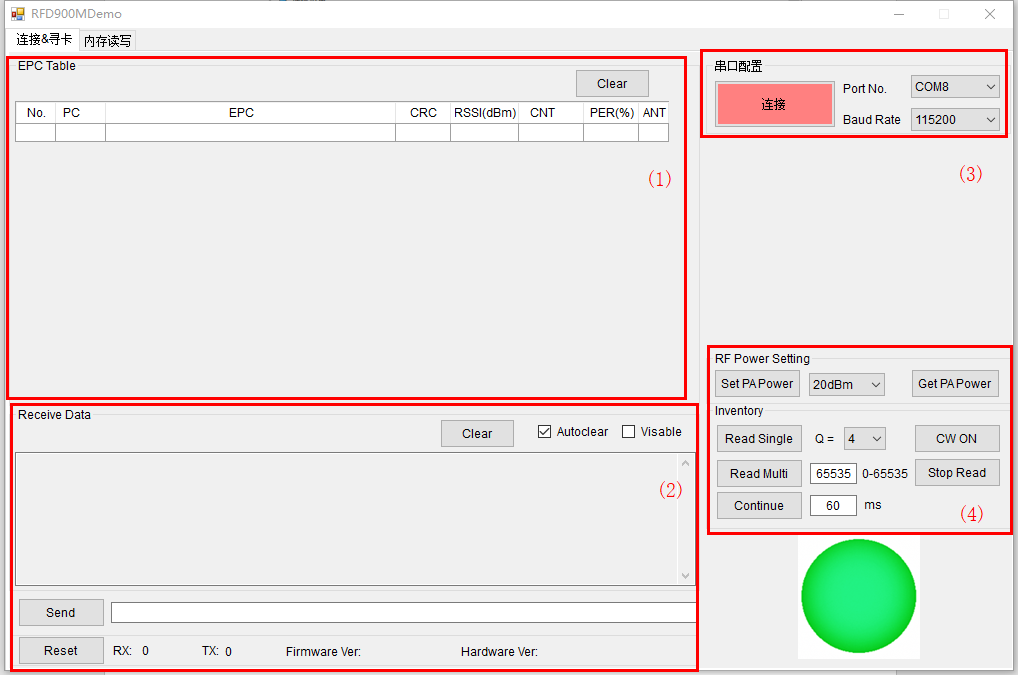
如果没有收到标签返回或者返回数据 CRC 校验错误，将返回错误代码 0x15，如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Header | Type | Command | PL(MSB) | PL(LSB) | Parameter | CheckSum | End |
| AA | 01 | FF | 00 | 11 | 15 | 16 | DD |

1. **实验步骤**
2. 首先将开发板连接至PC，打开PC的设备管理器，可看到串口，如下，当前PC中的串口为COM9，实际电脑可能与此不同，视具体情况而定。



1. 打开UHF900Demo软件，并设置连接端口，确定端口与设备管理器端口一致时，点击连接



在连接&寻卡页面主要分为4部分，分别是：

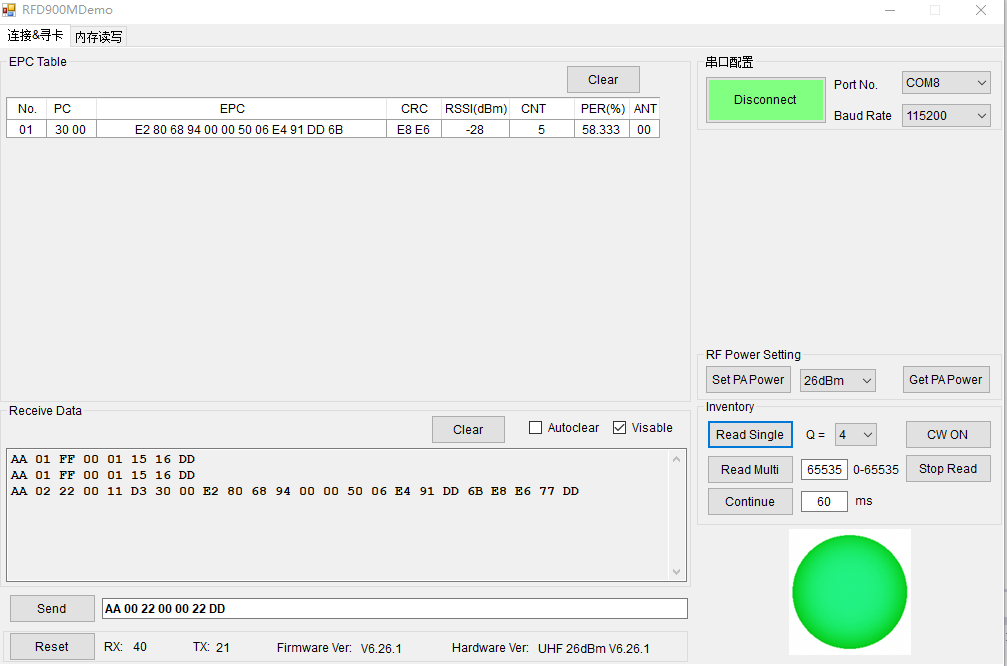
(1)读卡寻卡区、显示了读到卡号、校验信息等。

(2)指令区，即上位机软件与UHF开发板通信的指令。

(3)串口区域，软件使用时，通常使用默认配置。

(4)寻卡操作区，包含设置/读取寻卡功率、寻卡操作。

1. 将卡片置于天线上方，点击Read Single按钮，可读到信息，如下



读取内容说明：

EPC：标签的epc号，也就是标签的卡号。

CRC：标签卡号的校验值。

RSSI：标签卡号的信号强度值。

CNT：读到标签的次数。

在发出寻卡指令后，可见在软件操作的指令区即可显示数据包发送、接收的信息。

1. 点击内存读写按钮，这里我们主要以RFU区域为主，选中左边的卡号，在Read/Write Tag Memory区域中配置MemBank为RFU，读取指针Word Pointer为00 00，读取字长Word Counter为00 01即可，Access Password为默认即 00 00 00 00，点击Read按钮，可见在Data栏里返回数据，尝试编辑修改，然后点击Write，再点击Read读取，可以看到内存的读写已经完成；

