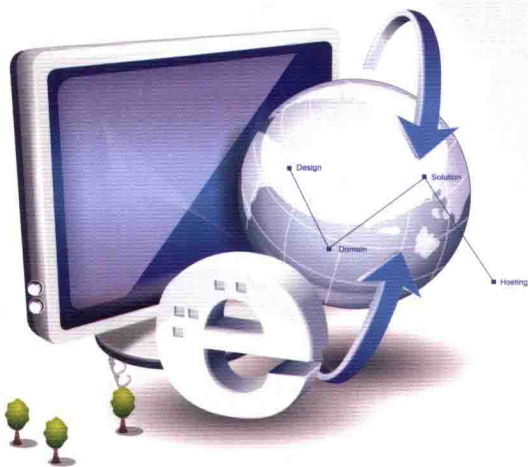


物联网工程专业系列教材

RFID技术与应用 实训教程

主 编 刘和文 李 雪 谢忠敏
副主编 文 燕 邹承俊



中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书共 14 个模块：前 12 个模块为基本技能训练，主要内容为 RFID 设备认知及应用体验，低频、高频、超高频读写操作，RFID 通信协议命令测试，有源 2.4GHz 读卡操作，RFID 接入 ZigBee，IAR 的安装与基本操作，RFID-ZigBee 底层开发入门及上位机 RFID 相关计算机软件设计入门等，能力训练由易到难、由简单到综合，知识的学习由浅入深、循序渐进；后两个模块为综合训练，内容为基于标签的 RFID 读写开发和基于数据库的 RFID 读写开发，第二个训练是在第一个训练的基础上进行进一步开发，通过完成完整的工作任务来获得综合职业能力。本书在每个训练项目中都详细地列出了训练目的、训练设备、训练课时、训练评分表以及实验报告等内容，方便教学。

图书在版编目 (C I P) 数据

RFID 技术与应用实训教程 / 刘和文, 李雪, 谢忠敏
主编. — 北京: 中国水利水电出版社, 2017. 12
物联网工程专业系列教材
ISBN 978-7-5170-6205-9

I. ①R… II. ①刘… ②李… ③谢… III. ①无线电
信号—射频—信号识别—应用—高等职业教育—教材
IV. ①TN911.23

中国版本图书馆CIP数据核字(2017)第326339号

策划编辑：寇文杰 责任编辑：高 辉 加工编辑：张青月 封面设计：李 佳

书 名	物联网工程专业系列教材 RFID 技术与应用实训教程 RFID JISHU YU YINGYONG SHIXUN JIAOCHENG
作 者	主 编 刘和文 李 雪 谢忠敏 副主编 文 燕 邹承俊
出版发行	中国水利水电出版社 (北京市海淀区玉渊潭南路 1 号 D 座 100038) 网址: www.waterpub.com.cn E-mail: mchannel@263.net (万水) sales@waterpub.com.cn
经 售	电话: (010) 68367658 (营销中心)、82562819 (万水) 全国各地新华书店和相关出版物销售网点
排 版	北京万水电子信息有限公司
印 刷	三河市铭浩彩色印装有限公司
规 格	184mm×260mm 16 开本 12.75 印张 322 千字
版 次	2017 年 12 月第 1 版 2017 年 12 月第 1 次印刷
印 数	0001—1000 册
定 价	30.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换
版权所有·侵权必究

前 言

物联网是继计算机、互联网与移动通信网之后的又一次信息产业浪潮,而射频识别(RFID)技术既是物联网的关键核心技术之一,也是物联网专业知识的核心内容。本书作者在对物联网专业人才培养模式进行深入研究的基础上,充分围绕物联网核心技术之一的RFID技术,融基础理论、实验实训于一体,结合企业实际项目案例进行编排,以培养适应社会和企业需要的复合型高素质技术人才。

教材特色

本书结合实际的RFID操作平台,为提高学生的实际动手能力,对RFID技术所涉及的知识点分别进行独立训练,最后以两个综合开发实训项目进行知识的整合和应用。本书以通俗的语言和真实案例,帮助读者更好地理解 and 掌握RFID技术,使读者在掌握RFID技术方面有一个实际体验过程,让读者体会到“学有所用”,并具有收获感。本书图文并茂、实用性强,在写作构思和结构编排等方面充分体现了“理实一体”的高职高专特色。

教材内容

本书共14个模块:前12个模块为基本技能训练,主要内容为RFID设备认知及应用体验,低频、高频、超高频读写操作,RFID通信协议命令测试,有源2.4GHz读卡操作,RFID接入ZigBee, IAR的安装与基本操作,RFID-ZigBee底层开发入门及上位机RFID相关PC软件设计入门等,能力训练由易到难、由简单到综合,知识的学习由浅入深、循序渐进;后两个模块为综合训练,内容为基于标签的RFID读写开发和基于数据库的RFID读写开发,第二个训练是在第一个训练的基础上进行进一步开发,通过完成完整的工作任务来获得综合职业能力。本书在每个训练项目中都详细地列出了训练目的、训练设备、训练课时、训练评分表以及实验报告等内容,方便教学。

学时参考

每个基本技能训练一般安排2个学时,根据内容与难度可调整到1个或3个学时,共计24个学时。每个实验至少安排6个学时,可根据学生基础和实际实验的进展相应地增加学时(如每个实验安排10个学时),共计12~20个学时。因此,本实训教程共需36~44个学时。

适用对象

本书可以作为高等职业院校物联网应用技术、电子信息工程技术、通信技术等相关专业的教材或教学参考书,也可以作为物联网相关课程的实验教材,同时还可以作为物联网相关工程技术人员学习物联网技术、设计开发物联网应用系统的参考书。

本书采用校企合作的方式,由成都农业科技职业学院一线专业课教师主编完成,实验平

目 录

前言	
训练一 RFID 设备认知及应用体验	1
训练二 低频 LF-125kHz 读卡操作	2
训练三 高频 HF-13.56MHz 读写操作	16
训练四 EPC 编码	19
训练五 超高频 UHF-900MHz 读写操作	24
训练六 RFID 通信协议命令测试 (超高频)	39
训练七 有源 2.4GHz 读卡操作	52
训练八 RFID 接入 ZigBee	55
训练九 IAR 的安装与基本操作	64
训练十 IAR-C 语言应用基础	71
训练十一 RFID-ZigBee 底层开发入门	83
训练十二 上位机 RFID 相关计算机软件 设计入门	118
综合训练一 基于标签的 RFID 读写开发	133
综合训练二 基于数据库的 RFID 读写开发	161
附录 考核方式	196
参考文献	197

训练一 RFID 设备认知及应用体验

一、基本技能训练名称

RFID 设备认知及应用体验

二、学时安排

2 学时

三、实验器材与设备

RFID 读写器、RFID 标签、门禁系统。

四、目的要求

1. 了解 RFID 系统构成，认识各部件。
2. 体验 RFID 功能，体验 RFID 在物联网中的作用。

五、内容与步骤

1. 认识 RFID 读写器、RFID 标签。
2. 参观体验实验室门禁系统。
3. 在条件和时间允许的情况下，参观体验诸如停车场、图书馆等场所的 RFID 系统，了解其系统构造和功能。

六、基本技能训练思考题与结果分析

1. RFID 在物联网中的作用？
2. 读写器与标签的区别？

训练二 低频 LF-125kHz 读卡操作

一、基本技能训练名称

低频 LF-125kHz 读卡操作

二、学时安排

2 学时

三、实验器材与设备

1. 计算机、串口连接线缆。
2. 博创 RFID 系统：UP-TECH RFID MODULE 125kHz 读写器、低频 e5551 应答器（电子标签）、UP-RFID-DEMO 模块测试软件、串口调试助手。
3. 泛太 RFID 系统：FT/RFID-125kHz 读写器、RFID125kApp.exe（上位机操作程序）、串口调试助手、EM4100 白卡（电子标签）。

四、目的要求

1. 了解 125kHz 的基本概念、国际标准、协议内容。
2. 了解 125kHz 的标准接口。
3. 了解 125kHz 的应用范围及领域。
4. 通过读卡，熟悉 RFID 系统的组成与连接。
5. 掌握读写器的使用，理解电子标签的卡号。

五、内容与步骤

（一）了解 LF-125kHz 技术基础

125kHz RFID 系统采用电感耦合方式工作，由于应答器成本低、非金属材料和水对该频率的射频具有较低的吸收率，所以 125kHz RFID 系统在动物识别、工业和民用水表等领域获得广泛应用。

其实 RFID 技术首先是在低频得到了广泛的应用和推广。该频率主要是通过电感耦合的方式进行工作，也就是在读写器线圈和感应器线圈间存在着变压器耦合作用。通过读写器交变场的作用在感应器天线中感应的电压被整流，可作供电电压使用。磁场区域能够被定义得很好，但是场强下降得太快。

特性：

- 工作在低频的感应器的工作频率一般从 120kHz 到 134kHz，TI 公司的部分产品的工作频率为 134.2kHz。该频段的波长大约为 2500m。
- 除了金属材料影响外，低频一般能够穿过任意材料的物品而不降低它的读取距离。
- 工作在低频的读写器在全球没有任何特殊的许可限制。

- 低频产品有不同的封装形式。好的封装形式有十年以上的使用寿命，但价格昂贵。
- 虽然该频率的磁场区域下降很快，但是能够产生相对均匀的读写区域。
- 相对于其他频段的 RFID 产品，该频段数据传输速率比较慢。
- 感应器的价格相对于其他频段来说要贵。

主要应用：

- 畜牧业的管理系统。
- 汽车防盗和无钥匙开门系统。
- 马拉松赛跑系统。
- 自动停车场收费和车辆管理系统。
- 自动加油系统。
- 酒店门锁系统。
- 门禁和安全管理系统。

符合的国际标准：

- ISO 11784 RFID 畜牧业的应用—编码结构。
- ISO 11785 RFID 畜牧业的应用—技术理论。
- ISO 14223-1 RFID 畜牧业的应用—空气接口。
- ISO 14223-2 RFID 畜牧业的应用—协议定义。
- ISO 18000-2 定义低频的物理层、防碰撞和通信协议。
- DIN 30745 主要是欧洲对垃圾管理应用定义的标准。

下面对 e5551 应答器芯片（博创提供）的性能和电路组成等进行说明。

1. 主要技术性能

e5551 芯片是 ATMEL 公司生产的非接触式、无源、可读写、具有防碰撞能力的 RFID 器件，中心工作频率为 125kHz。具有以下主要特性：

- 低功耗，低工作电压。
- 非接触能量供给和读写数据。
- 工作频率范围为 100kHz~150kHz。
- EEPROM 存储器容量为 264 位 (bit)，分 8 块，每块 33 位。
- 具有 7 块用户数据，每块 32 位，共 224 位。
- 具有块写保护。
- 采用请求应答实现防碰撞。
- 完成块写和检验的时间小于 50ms。
- 可编程选择传输速率和编码调制方式。
- 可工作于密码方式。

2. 内部电路结构

e5551 芯片的内部电路组成框图如图 2-1 所示，该图给出了 e5551 芯片和读写器之间的耦合方式。读写器向 e5551 芯片传送射频能量和读写命令，同时接收 e5551 芯片以负载调制方式送来的数据信号。

e5551 芯片由模拟前端、写解码、比特率产生器、调制器、模式寄存器、控制器、测试逻辑、存储器、输入寄存器、编程用高压产生器等部分构成。

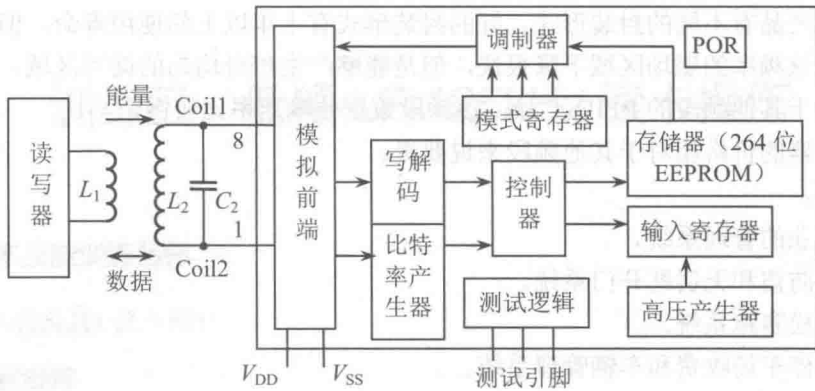


图 2-1

e5551 芯片在射频工作时，仅使用 Coil1（引脚 8）和 Coil2（引脚 1），外接电感 L_2 和电容器 C_2 ，构成谐振回路。在测试模式时， V_{DD} 引脚和 V_{SS} 引脚分别为外加电压正端和地，通过测试引脚实现测试功能。

（1）模拟前端（射频前端）。

模拟前端（Analog Front End, AFE）电路主要完成芯片对模拟信号的处理和变换，包括电源产生、时钟提取、载波中断的检测、负载调制等部分。

（2）控制器。

控制器主要完成如下四种功能：

- 在上电有效后及读期间，用配置存储器数据装载模式寄存器保证芯片以设置方式工作。
- 控制对存储器的访问。
- 处理写命令和数据写入。
- 在密码模式中，将接收到的操作码后 32 位值与存储的密码进行比较和判别。

（3）比特率生成与写解码。

比特率生成电路可产生射频的 8、16、32、40、50、64、100、128 分频后的数据比特率。写解码电路在写操作期间解读有关写操作码，并对写数据流进行检验。

（4）高压（HV）产生器。

它在写入时产生对 EEPROM 编程时所需的高电压。

（5）模式寄存器。

模式寄存器存储来自 EEPROM 区块 0 的模式数据，它在每块开始时被不断刷新。

（6）调制器。

调制器由数据编码器和调制方式两级电路组成，如图 2-2 所示。其输入为来自存储器的二进制 NRZ 码，输出用于对载波的负载进行调制。

1) 编码。

- 曼彻斯特码：逻辑 1 为倍频率 NRZ 码的 10，逻辑 0 为倍频率 NRZ 码的 01。
- Biphase 码：每个位的开始电平跳变，数位 0 时中间附加一跳变。

2) 调制方式。

PSK 调制的脉冲频率为 $RF/2$ 、 $RF/4$ 或 $RF/8$ ， RF 为载波频率 f_c 。它的相位变化情况有以下几种：

- PSK1：数位从 1 变为 0 或从 0 变为 1 时，相位改变 180° 。

- PSK2: 每当数位 1 结束时, 相位改变 180°。
- PSK3: 数位从 0 变为 1 (上升沿) 时, 相位改变 180°。

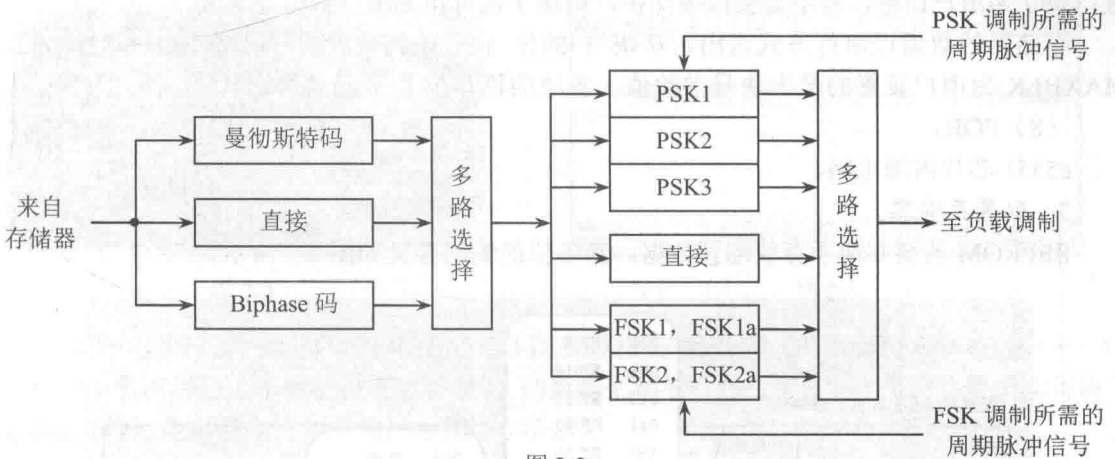


图 2-2

FSK 调制有以下四种:

- FSK1: 数位 1 和 0 的脉冲频率为 $RF/8$ 和 $RF/5$ 。
- FSK1a: 数位 1 和 0 的脉冲频率为 $RF/5$ 和 $RF/8$ 。
- FSK2: 数位 1 和 0 的脉冲频率为 $RF/8$ 和 $RF/10$ 。
- FSK2a: 数位 1 和 0 的脉冲频率为 $RF/10$ 和 $RF/8$ 。

3) 注意问题。

下面的组合不可使用:

- 当编码为曼彻斯特码或 Biphas 码时, 为 PSK2 调制或比特率为 $RF/8$ 且脉冲频率为 $RF/8$ 的 PSK 调制。
- 比特率为 $RF/50$ 或者 $RF/100$ 的 PSK 调制, PSK 的脉冲频率不为比特率的整数倍。

(7) 存储器。

存储器 EEPROM 的结构如表 2-1 所示, 它由 8 块构成, 每块 33 位, 共 264 位, 第 0 位为锁存位。每一块的所有 33 位都可被编程, 编程所需电压来自片内。但若某块的锁存位被置 1, 则该块被锁存, 不能通过射频再次编程。

表 2-1

0	1~32	块
L	用户数据或密码 (口令)	7
L	用户数据	6
L	用户数据	5
L	用户数据	4
L	用户数据	3
L	用户数据	2
L	用户数据	1
L	配置数据	0

存储器 EEPROM 的结构如下:

块 0 为芯片工作的模式数据, 它不能作为通常数据被传送; 块 1 至块 6 为用户数据存储区; 块 7 为用户口令, 若不需要口令保护, 则块 7 也可作为用户数据存储区。

存储器的数据以串行方式送出, 从块 1 的位 1 开始到最大块 (MAXBLK) 的位 32, MAXBLK 为用户设置的最大块号参数值。各块的锁存位 L 不能被传送。

(8) POR。

e5551 芯片内部电路。

3. 配置存储器

EEPROM 的块 0 用于存放配置数据, 其各位的编码含义如图 2-3 所示。

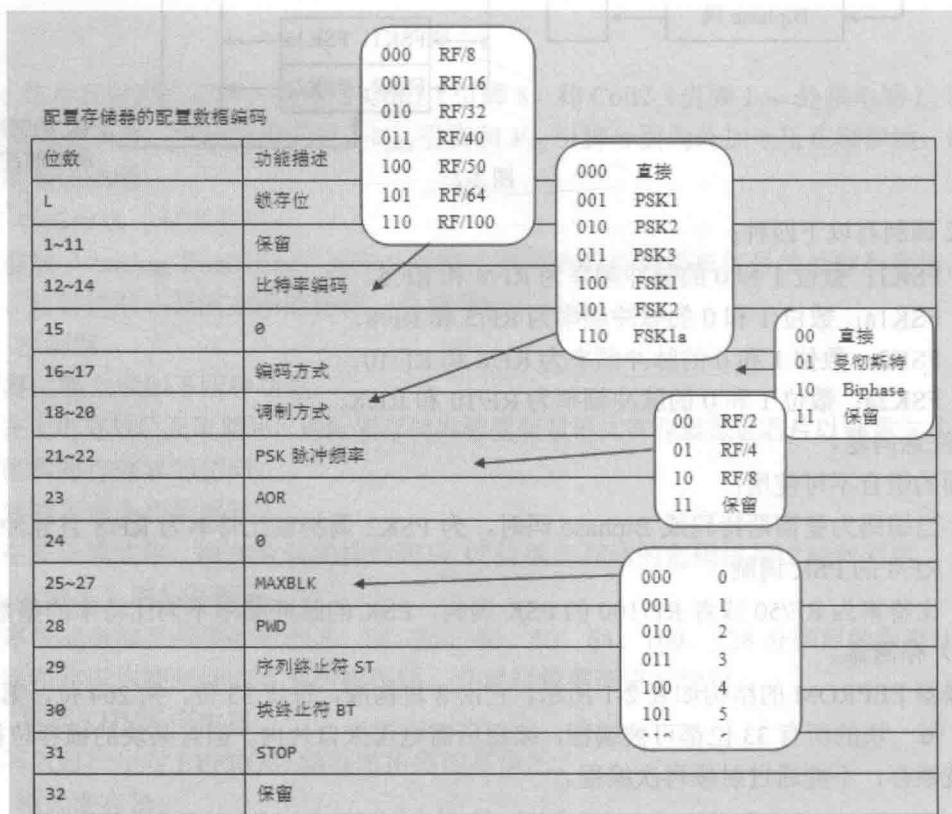


图 2-3

4. 初始化

电源上电后, e5551 芯片按配置数据进行初始化 (需 256 个载波时钟周期, 约 2ms), 采用所选用的编码调制方式工作。

(二) 读卡 (博创系统)

(1) 准备好硬件, RFID LF-125kHz 模块和配套 125kHz 标签。

(2) 使用串口连接线缆将 RFID 模块的串口与计算机的串口连接, 将 5V 电源连接到 RFID 模块的电源接口, RFID 模块的指示灯会亮, 如图 2-4 所示。

(3) 打开串口调试助手, 波特率设为 9600, 将标签放入读写器天线辐射区内, 即可读取卡号, 如图 2-5 所示。

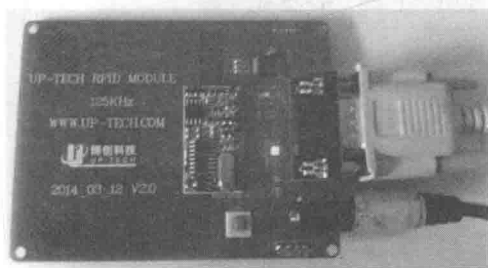


图 2-4



图 2-5

(4) 关闭串口调试助手，打开 UP-RFID-DEMO 模块测试软件 UP_RfidTools.exe (RFID 模块测试软件)。

(5) 打开串口 (不需要设置波特率)，切换到低频 LF125kHz 界面，将标签置于读写器天线辐射区内，便可获取标签卡号，如图 2-6 所示。



图 2-6

(三) EM4100 写卡与读卡 (泛太系统)

EM4xxx 是一种只读的射频感应卡，内部 ROM 里面保存着 10 位十进制的卡号数据，卡片内置天线，可以与读写器进行信息交互。EM4xxx 标签采用 Manchester (曼彻斯特) 调制方式编码。会周而复始地向外部读写器发送 64 个数据位的信息，位的传输速率为 RF/64，即每一位信息时长为 64 个外部电磁场波动周期。64 位信息位中包括 9 位 1 的同步引导头、40 位的卡号数据、14 位奇偶校验以及 1 位停止位。全部 64 位信息由制造商生产时编程刻录在 ROM 中，其卡号数据是全球唯一的，如图 2-7 所示。

(1) 连机实验准备。

将 FANTAI_125kHz 开发板水平放置于实验平台上，取出开发套件中的交叉串口线，将

FANTAI_125kHz 开发板与计算机连接。

1	1	1	1	1	1	1	1	1	九个同步头
8 位版本信息或厂商信息				D00	D01	D02	D03	P0	P0-P910 个行校验位
				D10	D11	D12	D13	P1	
				D20	D21	D22	D23	P2	
				D30	D31	D32	D33	P3	
				D40	D41	D42	D43	P4	
32 个卡号数据位				D50	D51	D52	D53	P5	
				D60	D61	D62	D63	P6	
				D70	D71	D72	D73	P7	
				D80	D81	D82	D83	P8	
				D90	D91	D92	D93	P9	
4 个列校验位				PC0	PC1	PC2	PC3	0	停止位

图 2-7

将 K1 电源开关拨到 ON 位置, K2 电源拨到 OFF 位置 (K2 为 ZigBee 模块供电开关), 拨码开关拨到 1、2 位置 (ON 反方向), 即 PC 直接与 FANTAI_125kHz 开发板串口通信。

将 DC5V 电源通过电源线与 FANTAI_125kHz 开发板板载电源插座连接, 电源指示灯 D1 至 D5 点亮, 随后 D1 至 D3 熄灭。

连接好并通电后的示意图如图 2-8 所示。

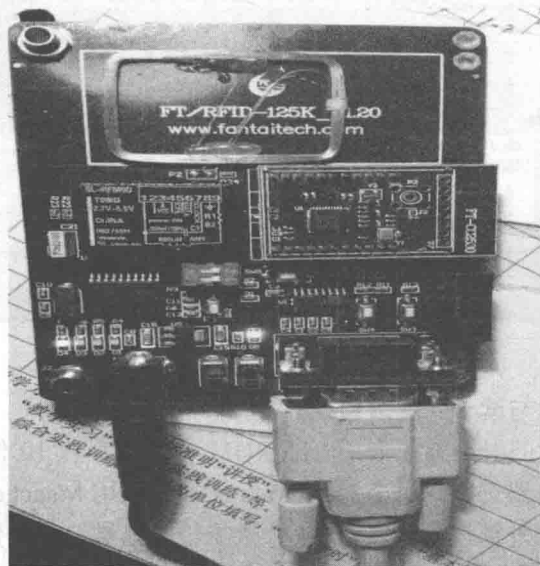


图 2-8

(2) 下载 U2270b 读写器固件程序 (选做)。

运行目录 “x:\RFID 光盘资料\低频 125k(U2270B)\FANTAI_125k 低频读写器开发软件” 下的 stc-isp-15xx-v6.84.exe 软件, 如图 2-9 所示。

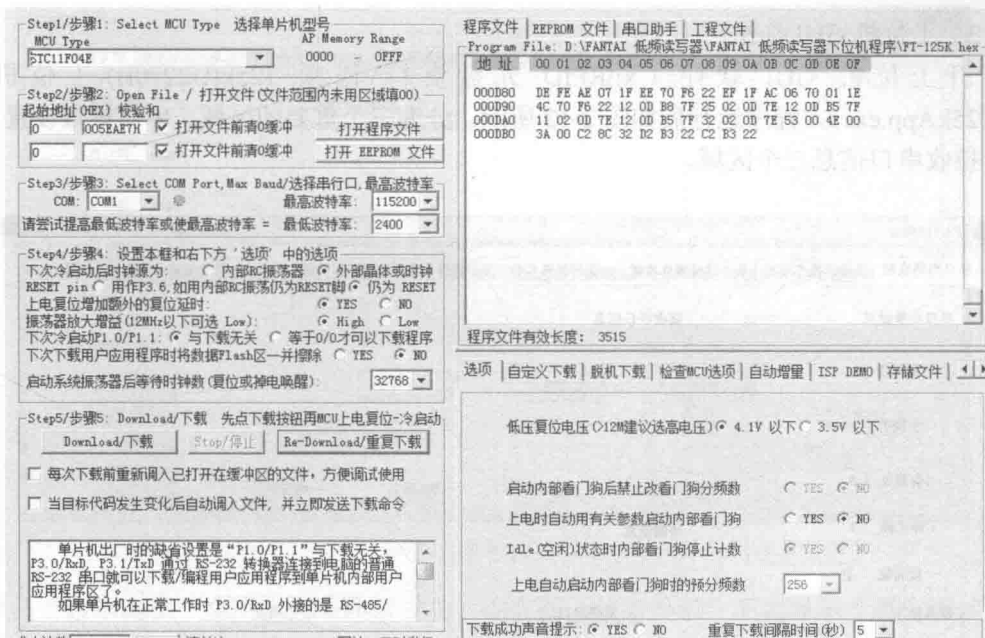


图 2-9

步骤一：在 MCU Type 下拉菜单中选择 FANTAI_125kHz 开发板上 MCU 对应的型号，FT-RFID-125kHz_V1.0 开发板上的 MCU 型号为 STC11F04E。

步骤二：单击“打开程序文件”按钮，按照路径“x:\FANTAI 低频读写器\FANTAI 低频读写器下位机程序\FT-125k.hex”打开程序文件。

步骤三：波特率设置选择默认。

步骤四：在“下一次冷启动时钟源为”选项内选择“外部晶体或时钟”选项，其他默认设置。

步骤五：单击“Download/下载”按钮，此时会出现如图 2-10 所示的提示。

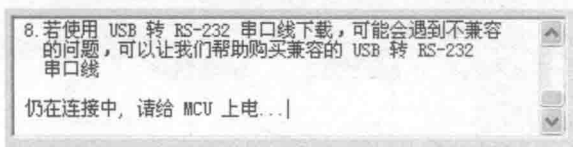


图 2-10

此时，将 FANTAI_125kHz 开发板板载电源开关 K1 由 OFF 拨到 ON 位置（如果已经在 ON 位置，则重新关闭后打开），FANTAI_125kHz 开发板上电。如果各个配置正确，程序会下载到 FANTAI_125kHz 开发板中，提示成功信息如图 2-11 所示。



图 2-11

关闭开发板电源，关闭程序。

(3) 上位机 GUI 操作。

打开上位机 GUI 软件 (x:\RFID 光盘资料\低频 125k(U2270B)\上位机程序\RFID125kApp.exe), 程序运行后如图 2-12 所示。分为三个重要的区域: 串口参数设置、功能设置、接收串口信息三个区域。

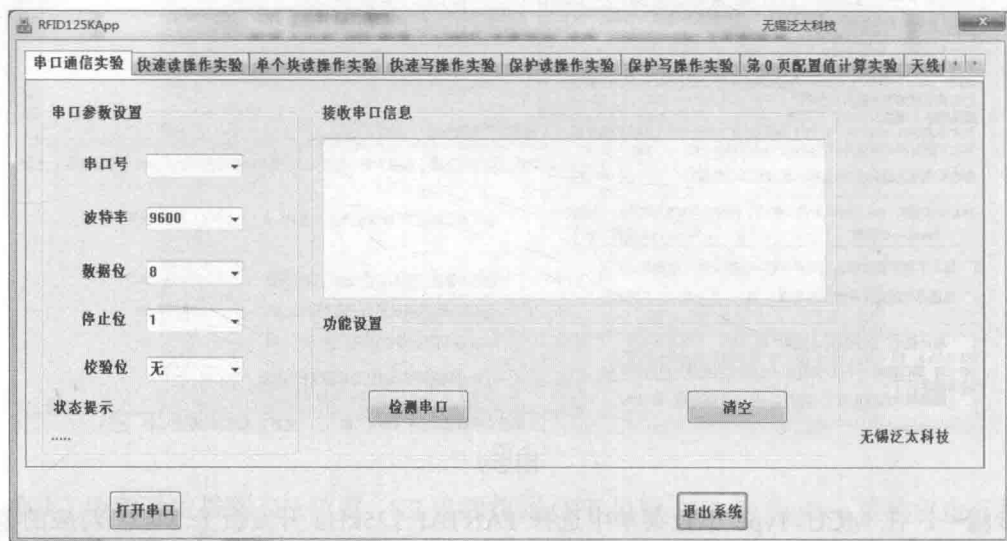


图 2-12

1) 联机通信。

在进入界面以后, 单击“检测串口”按钮, 如果有可用的串口, 则会在“状态提示”下面显示出可用的串口号, 如图 2-13 所示。

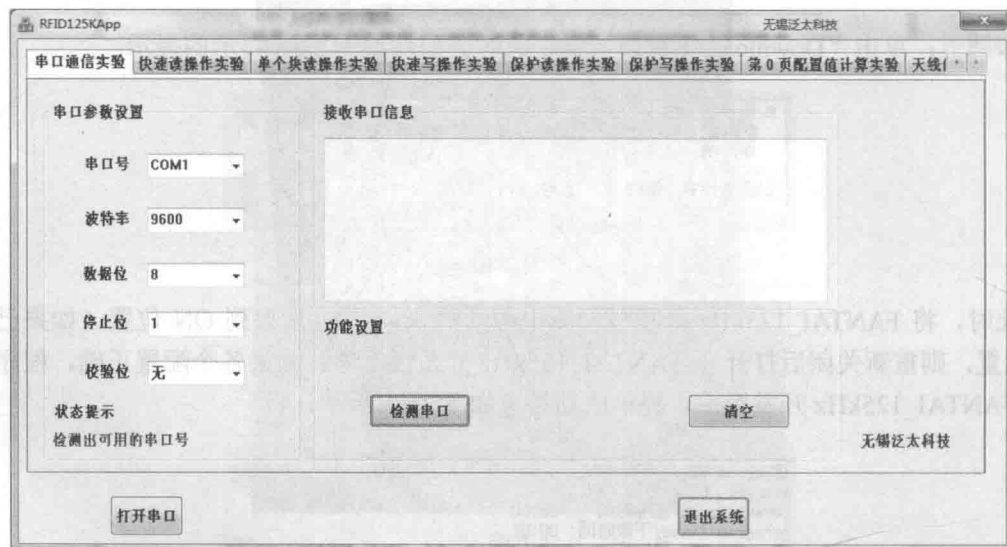


图 2-13

下一步为打开串口, 单击“打开串口”按钮后, 隐藏的“通信测试”按钮将出现, 如图 2-14 所示。

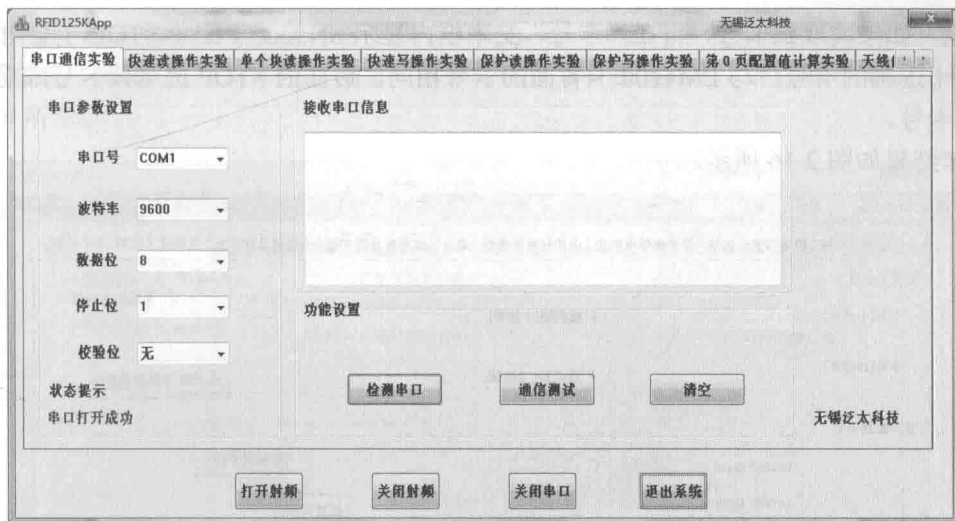


图 2-14

单击“通信测试”按钮，如果通信成功，则会在“状态提示”下面显示“通信测试成功”；否则显示“通信测试失败”。在“接收串口信息”的文字栏中将会返回“a56d01”字样，表示连接可靠稳定，如图 2-15 所示。

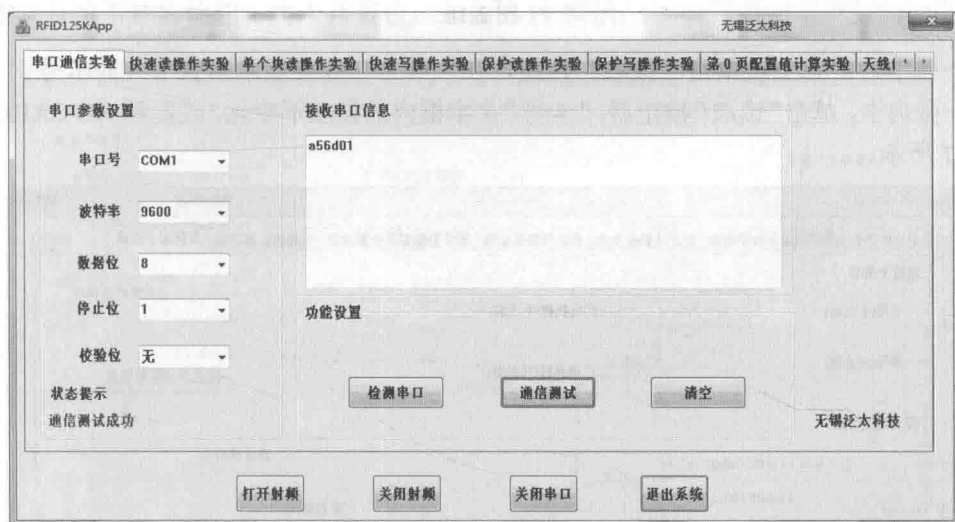


图 2-15

这时便可以进行下面的实验了。

注意：一般情况下，计算机默认的串口端口号为 COM1，波特率选择 9600，否则发送信息将出现错误。

2) EM4100 读卡操作。

注意，由于读写器非常不稳定，读卡前，先关闭上一步的程序和开发板电源，然后重新打开程序和电源。在程序中只进行“检测串口”和“打开串口”操作，不要再进行“通信测试”操作。

选中“低频读卡实验”选项卡，将 EM4xxx 标签放在在天线感应场内（相距 3~5cm 或直接放在其天线上），单击“读取”按钮，在单击此按钮的同时注意观察开发板上 D4 指示灯会