# 第1章 实验环境操作

## 1.1. 任务引导

### 1.1.1. 平台简介

《物联网虚拟仿真实验平台》是一个模拟物联网硬件的平台，该平台仿真了 RFID 各个频段的设备以及 WSN 网关及二十几种常见传感器，并且该平台具有与真实设备一致的开发接口，常见的物联网应用开发项目均可依托于该平台完成。

### 1.1.2. 学习目标

本任务的目的是为了让同学们掌握《物联网虚拟仿真实验平台》的操作方法。

## 1.2. 主界面简介

物联网虚拟仿真平台主界面由五大部分组成，如图 1-2-1 所示，包含有菜单栏、工具栏、工具箱、实验台、设备/消息列表。


图 1-2- 1 物联网虚拟仿真平台主界面图

菜单栏汇集了虚拟平台的全部功能、工具栏汇聚虚拟平台较常用的功能、工

具箱汇聚了虚拟平台的所有虚拟设备。

用户可在工具箱中点击“鼠标左键”拖动自己需要的设备、实验台则是放置工具箱拖动设备显示设备的位置；

设备/消息列表有两个功能的，一个是设备列表，另一个是消息列表；设备列表显示实验台中的全部设备，消息列表则是显示实验台设备发送数据或接受数据显示的信息。如：电源接电，断电等提示

## 1.3. 功能简介

菜单栏包含有“开始（F）”、“编辑（E）”、“布局（L）”、“视图（V）”、“测试程序（T）”和“帮助（H）”6 个菜单，每个菜单下又包含若干个功能菜单，下面逐一进行介绍。

### 1.3.1. 开始（F）

菜单栏中的开始菜单有新建、打开、保存、另存为、设置串口数、退出等六个功能，如图 1-2-2 所示。

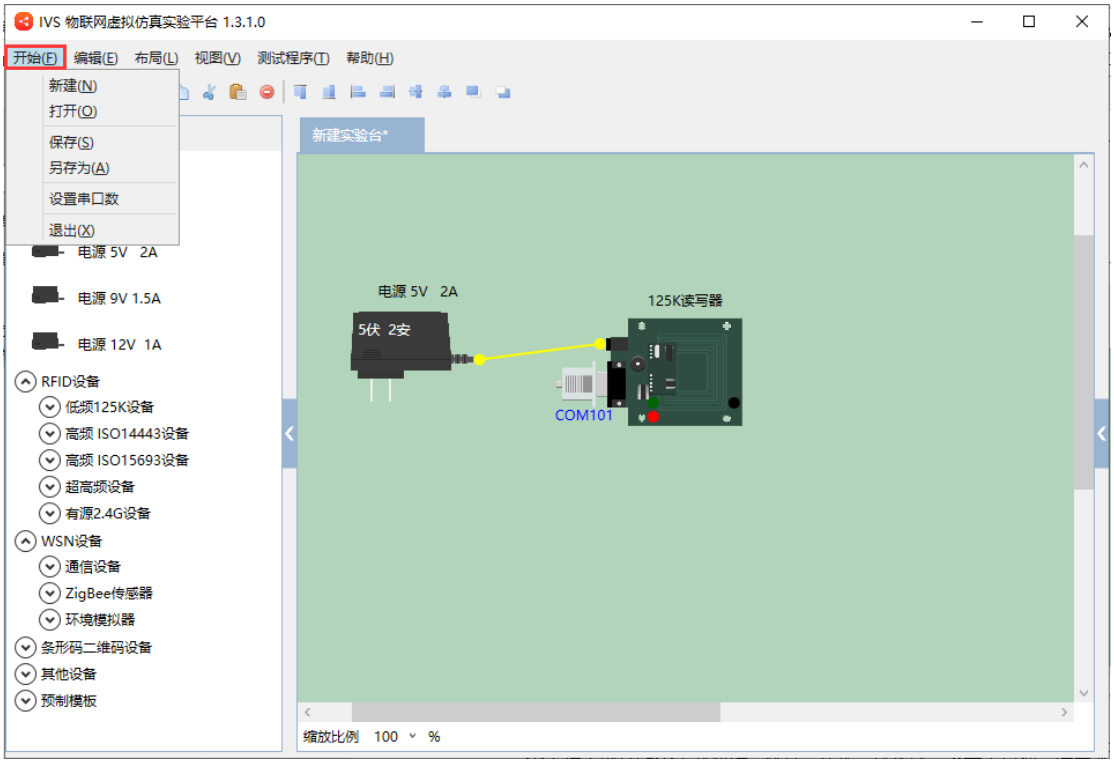



图 1-2- 2 开始功能图

用户可在开始菜单中执行相应操作，或在工具栏中（从左往右）前 4 个图标分别对应着新建、打开、保存、另存为四个功能，点击相应的图标可执行相应操作。如图 1-2-3 所示。

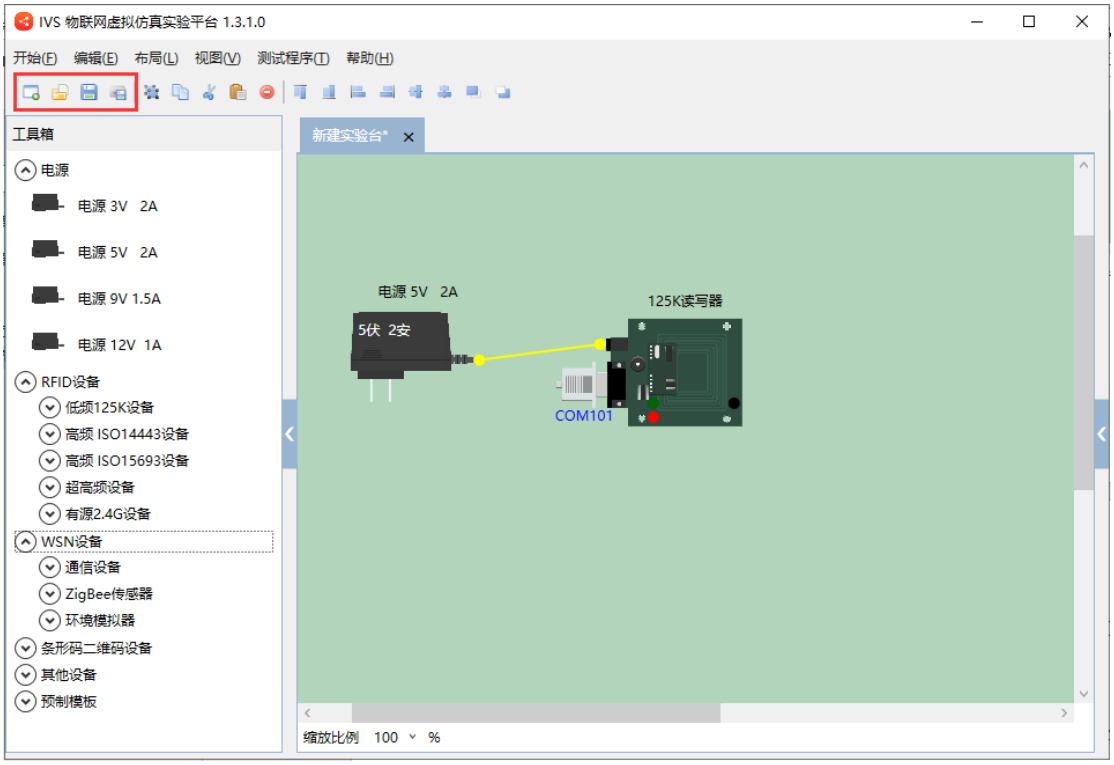



图 1-2- 3 工具栏图

新建功能实现新建一个实验平台，在这个平台上可以放置实验设备，其实现有两种方法：一种是单击新建菜单，另一种时单击工具栏中的新建图标如①所示，即可完成新建实一个验台如②所示，需要注意的是，在打开物联网虚拟仿真实验平台时，默认情况下已经新建了一个实验平台。新建实验台如图 1-2-4 所示。

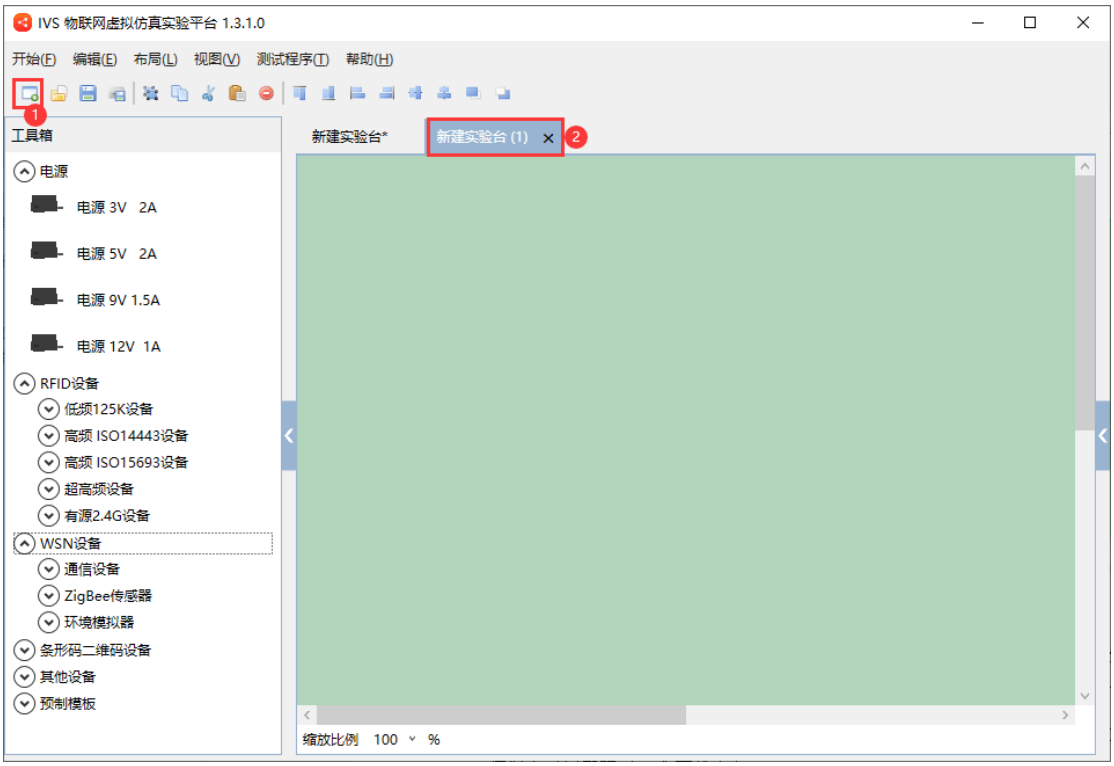



图 1-2- 4 新建实验台

将实验平台中搭建的设备进行保存，方便下次使用。可点击开始菜单栏框中的另存为选项或者工具箱中的保存，实验平台最终保存的格式为“.ivm”格式。保存如图 1-2-5 所示。

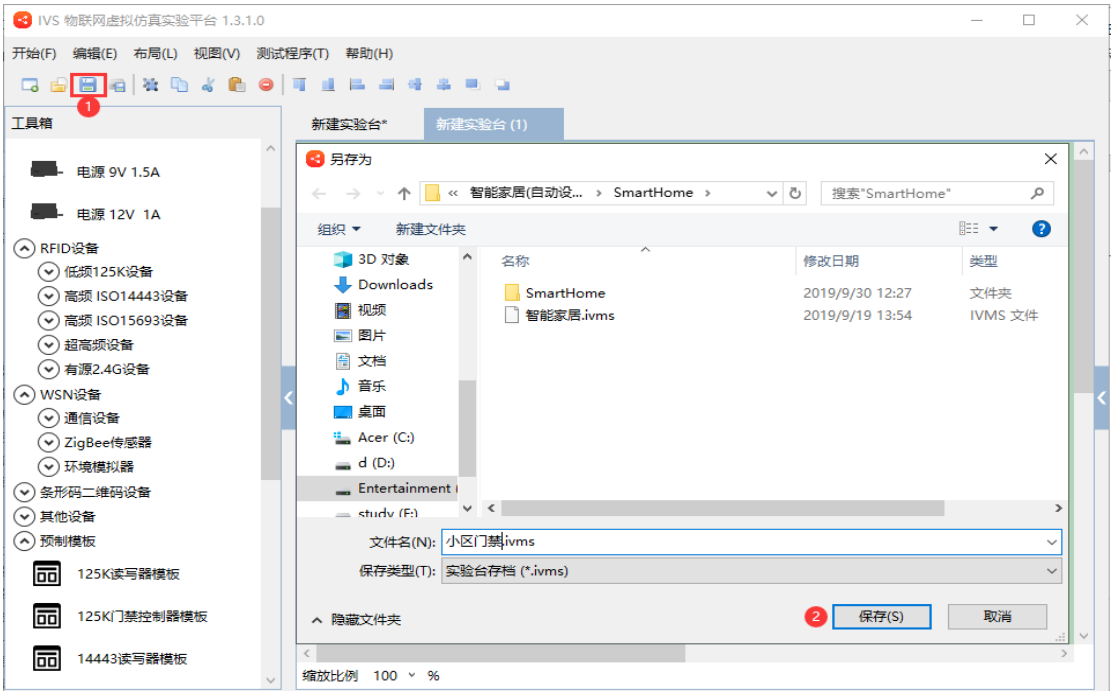



图 1-2- 5 保存工程

设置串口数：点击【开始】菜单栏选择设置串口数，如图 1-2-6 所示，设置串口数界面出现，在文本框中输入需要设定的串口数值，如图 1-2-7 所示。

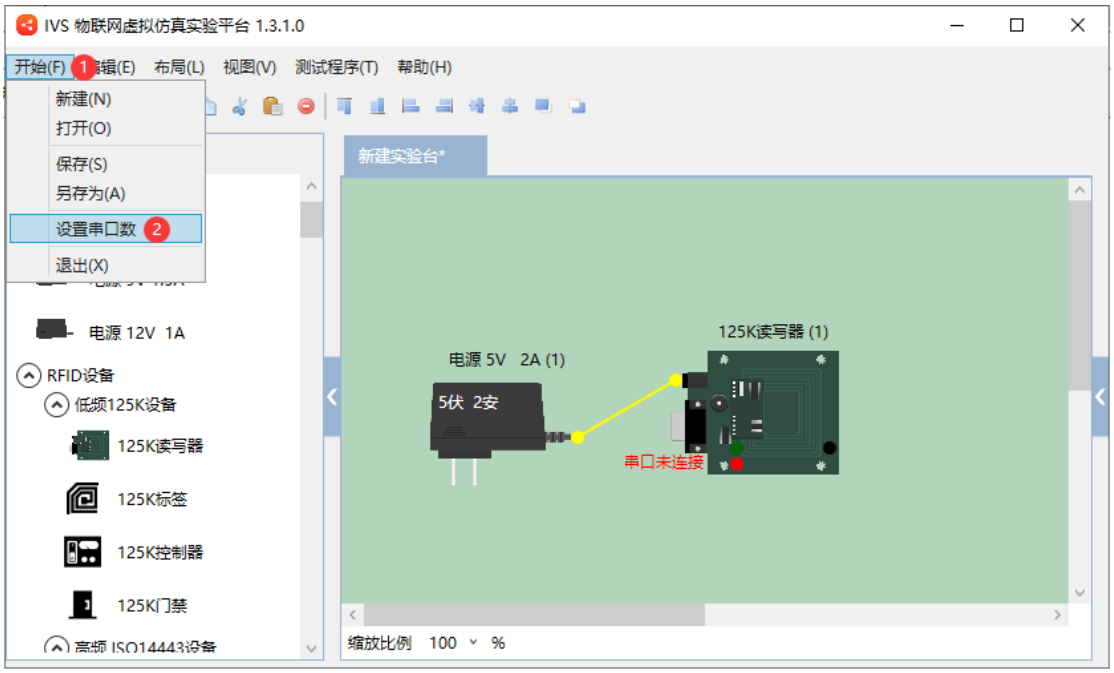



图 1-2- 6 选择设置串口数

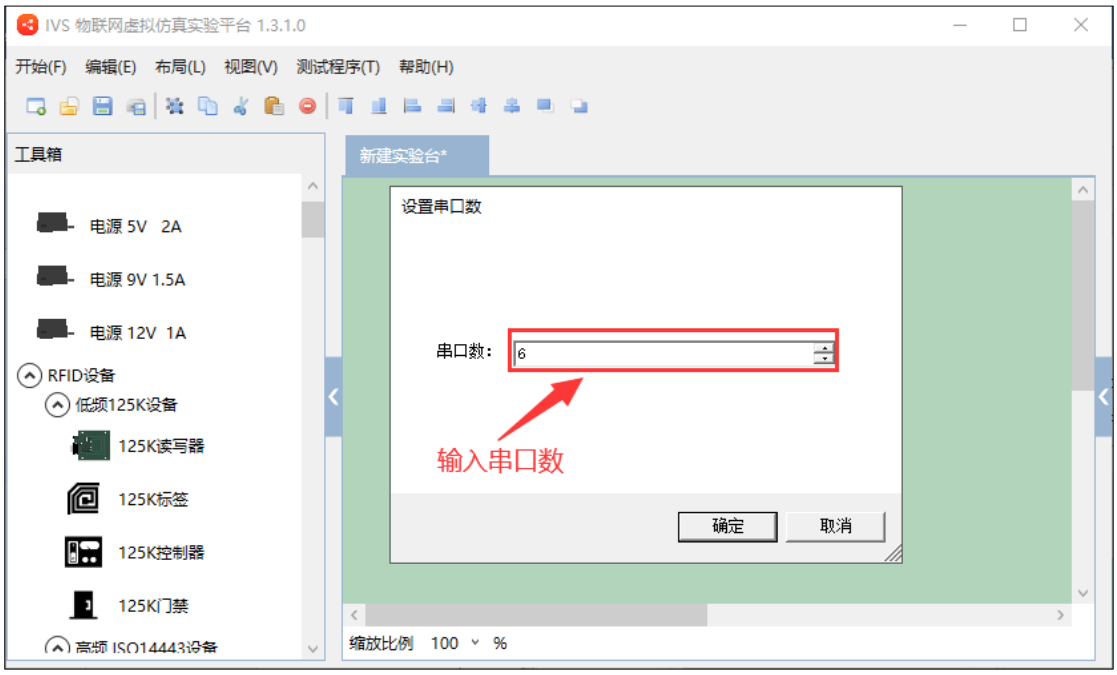



图 1-2- 7 设置串口数

串口数设置成功后，需要重新启动虚拟仿真实验平台才能改变，系统默认的串口数是 20 个。查看串口是否设置成功，在工具箱中找一个读写器拖入到实验

台中，然后选中读写器，单击鼠标右键，选择连接串口，如图 1-2-8 所示，弹出连接串口界面，查看串口数是否与设置的串口数相同，如图 1-2-9 所示。

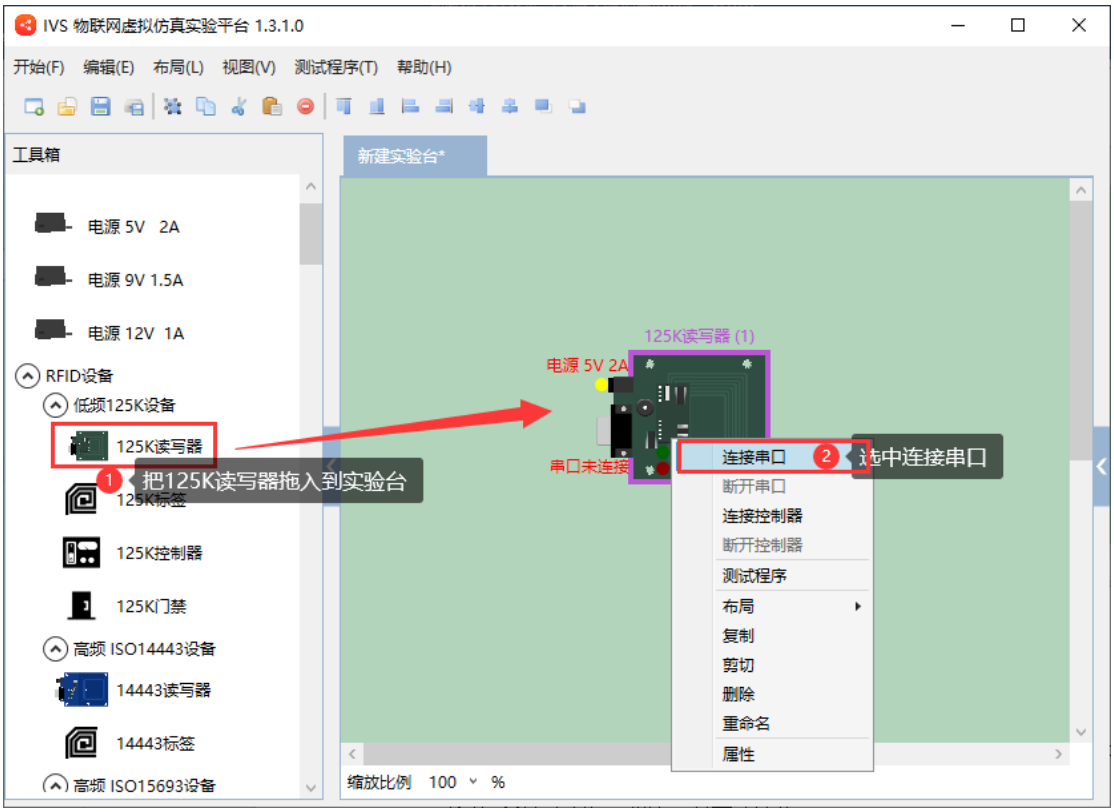



图 1-2- 8 打开连接串口

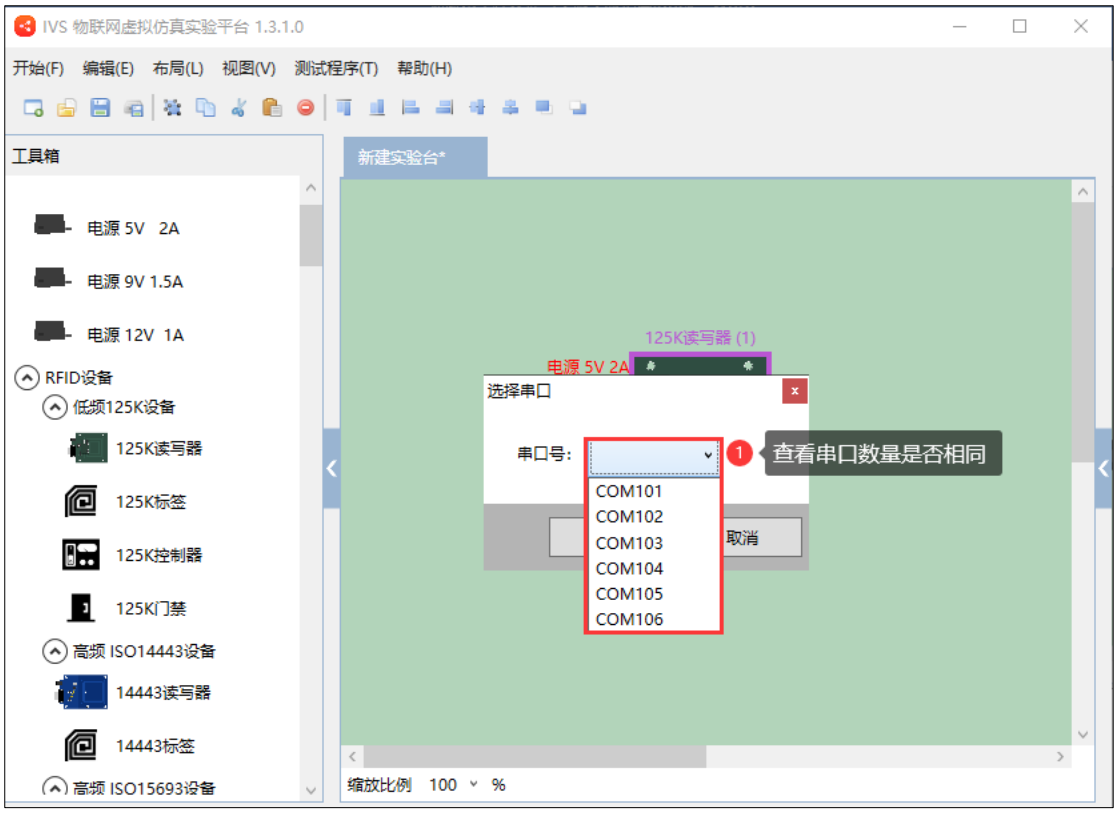



图 1-2- 9 查看串口数

## 1.3.2. 编辑（E）

编辑菜单包含有全选、复制、剪切、粘贴和删除五个功能，完成对实验平台上的实验设备的添加、删除、调整等操作，如图 1-2-10 所示。

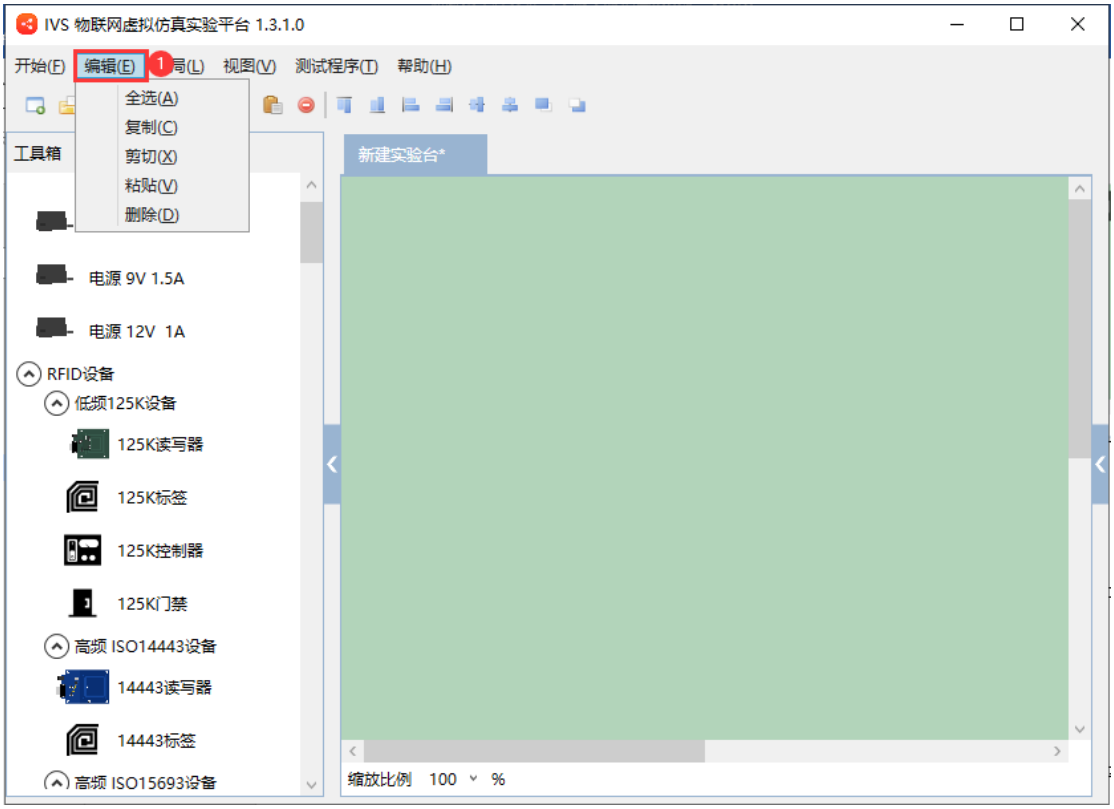



图 1-2- 10 编辑菜单栏

### 1. 布局（L）

布局菜单包含有上对齐、下对齐、左对齐、右对齐、横向平均、纵向平均、置顶和置底等 8 个功能，也可以在工具栏中使用快捷键，主要实现实验平台上的实验设备摆放位置调整，使得实验平台设备摆放更美观，如图 1-2-11 所示。

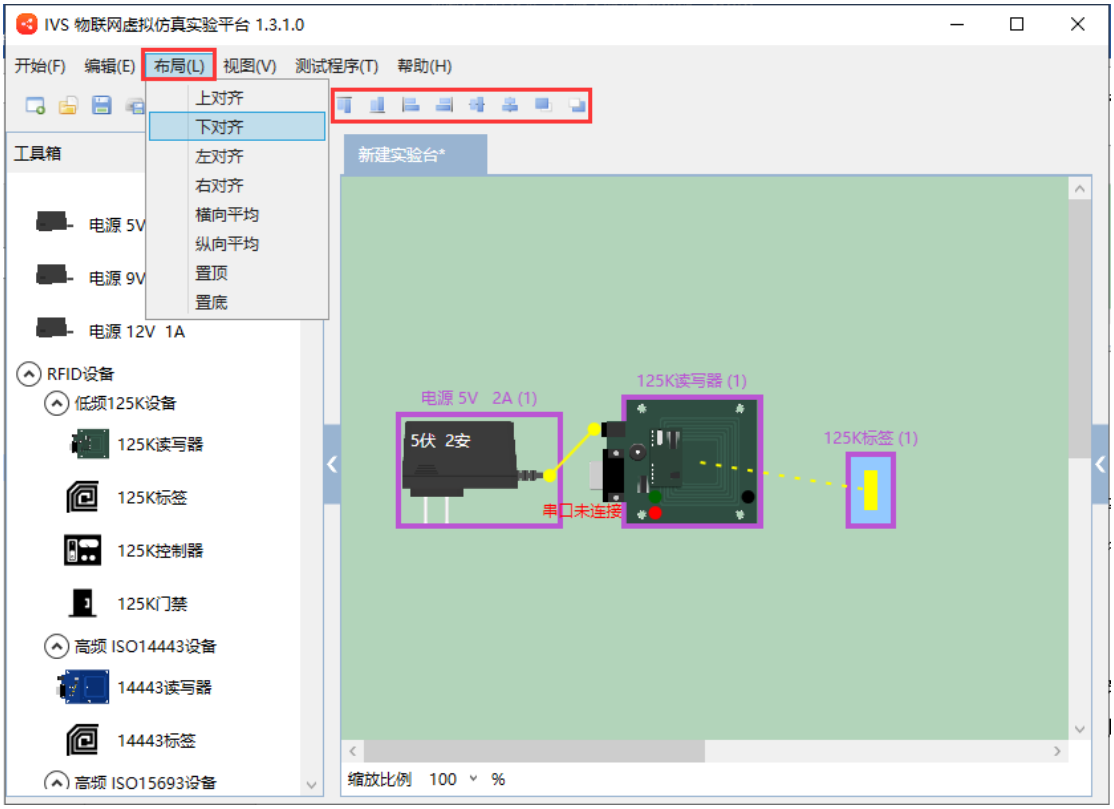



图 1-2- 11 设备对齐方式

## 1.3.3. 视图（V）

视图菜单包含有工具箱、设备列表和消息列表三个功能，主要完成平台软件窗口布局，是否显示工具箱窗口、设备列表窗口和消息列表窗口，方便软件使用，如图 1-2-12 所示。

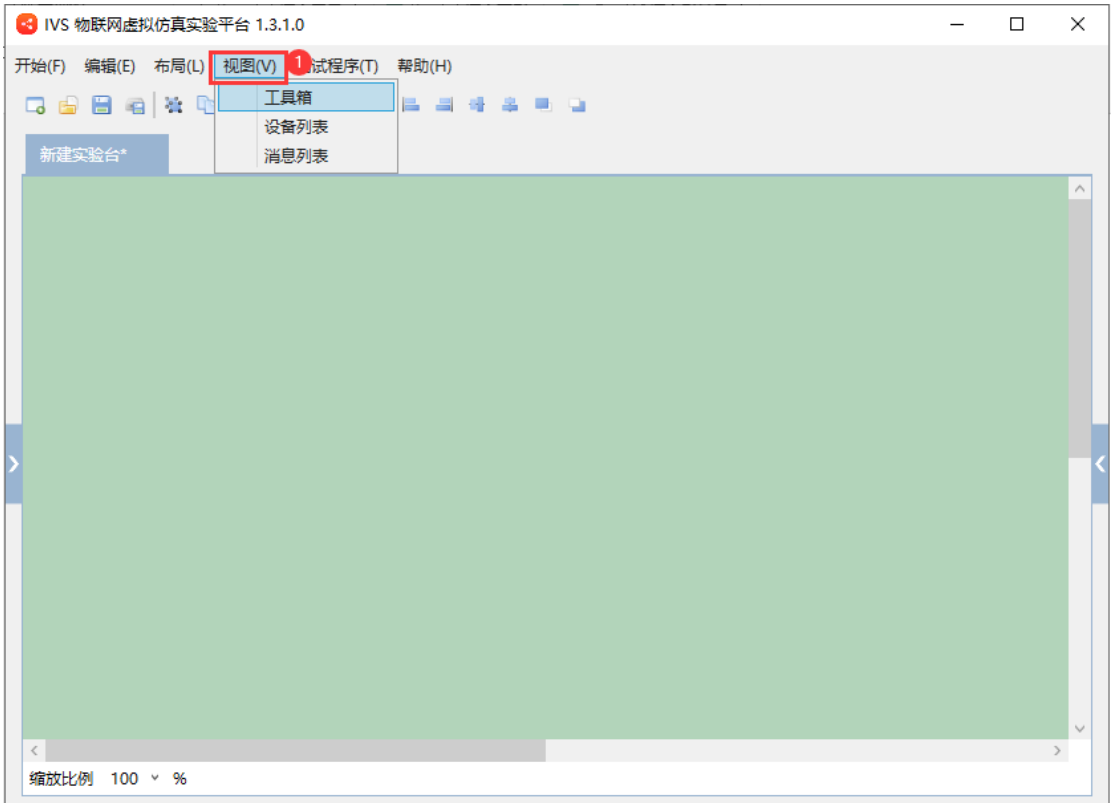



图 1-2- 12 工具箱

## 1.3.4. 测试程序（T）

测试程序菜单包含有 125K 测试程序、125K 门禁控制器测试程序、14443 测试程序、15693 测试程序、超高频测试程序、有源 2.4G 测试程序、无线传感网测试程序(实验级协调器测试程序、实验级网关测试程序)。是平台内置的对各种虚拟设备进行测试的程序，测试设备是否搭建成功，以及相关功能的实现。各个测试程序会在硬件搭建过程中使用到，并进行详细讲解，测试程序如图 1-2-13 所示。

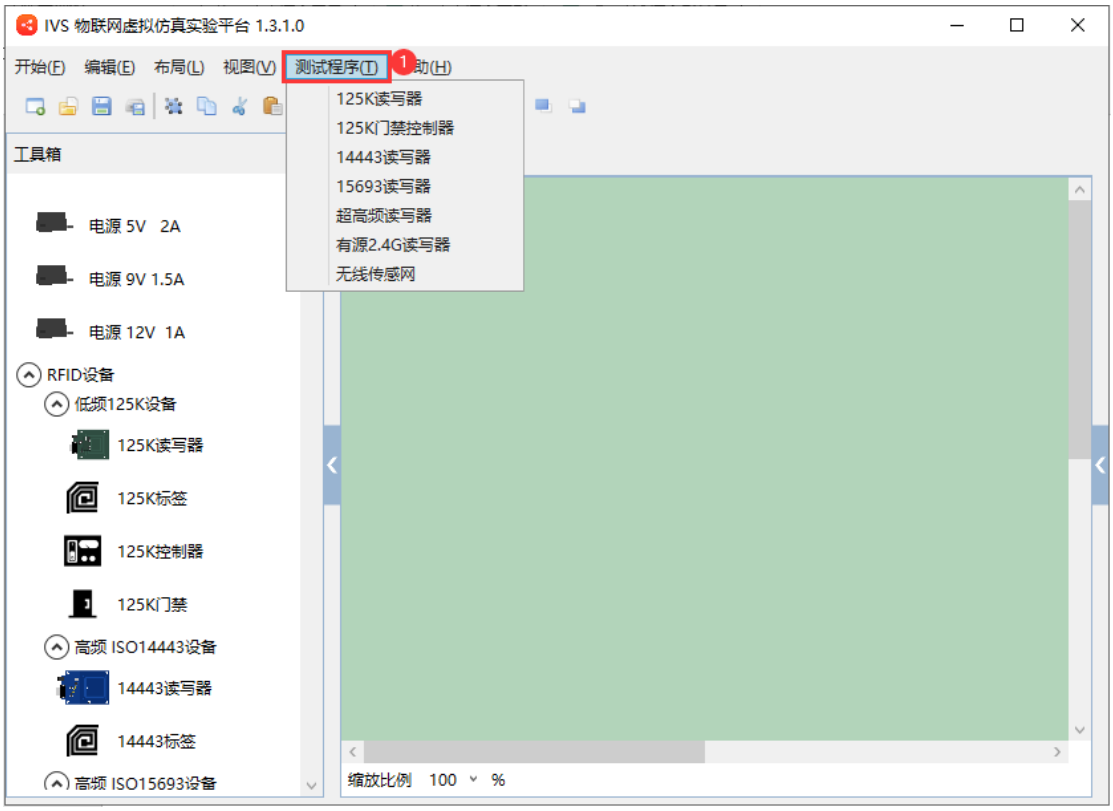



图 1-2- 13 测试程序

## 1.3.5. 帮助（H）

菜单显示虚拟平台的版本说明和公司信息等内容。下面通过门禁系统的硬件搭建，详细说明物联网虚拟仿真实验平台的使用，如图 1-2-14 所示。

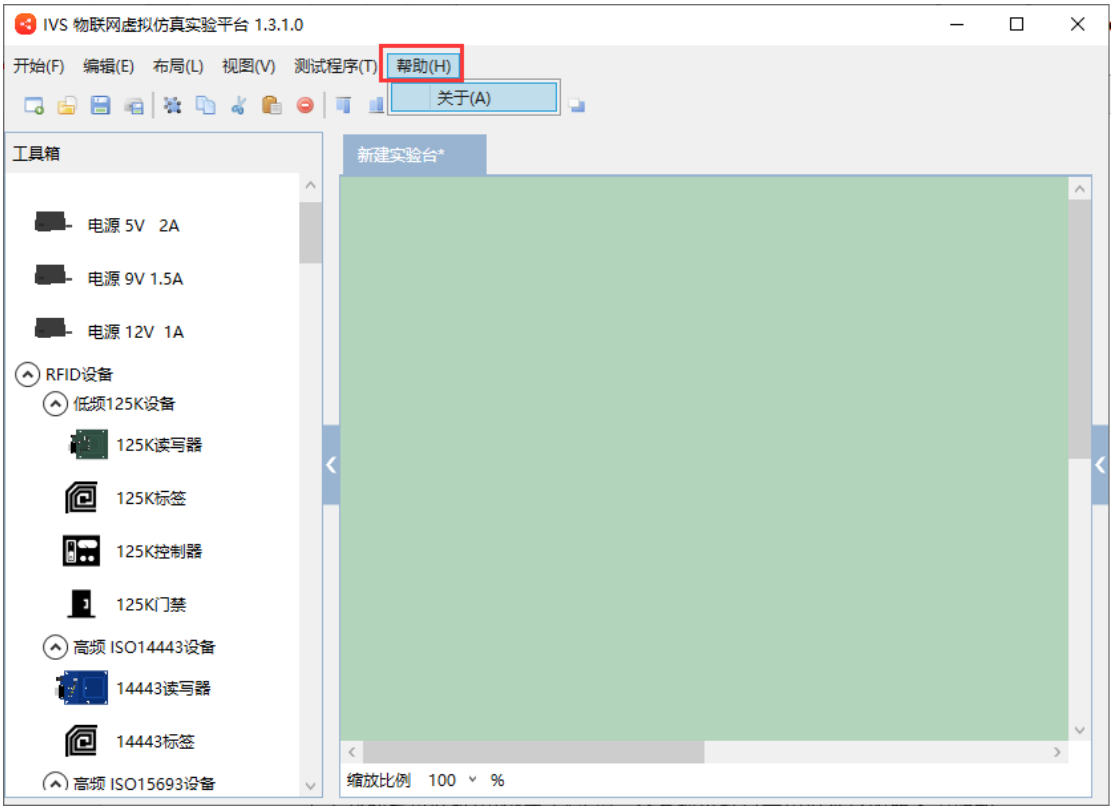



图 1-2- 14 帮助

## 1.4. 设备详解

### 1.4.1. 125K 设备

**低频设备特点：**

低频设备工作频率范围为 30kHz~300kHz。典型工作频率有：125KHz，133KHz。

低频标签一般为无源标签，其工作能量通过电感耦合方式从阅读器耦合线圈的辐射近场中获得。

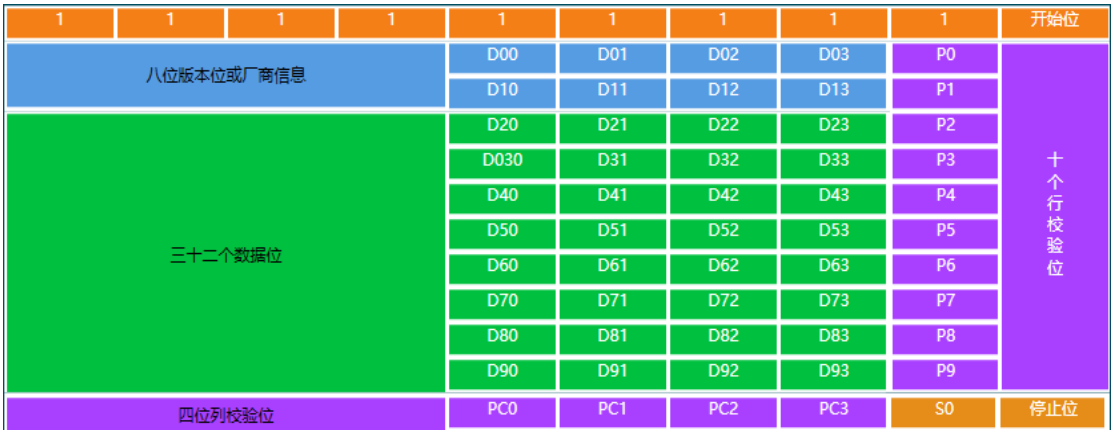
低频标签的阅读距离一般情况下为 0~5cm。

低频电子标签灵活性差，不易被识别，只能适合低速、近距离识别应用。

低频标签的典型应用有：动物识别、工具识别、电子闭锁防盗等。

低频设备相关的国际标准有：ISO18000-2、ISO11784/11785 等

**125K 标签结构（EM4100）：**




1) 低频 125K 标签由开始位、厂商版本位、行校验位、列校验位、停止位组成，标签内存容量为 64 字节，可读不可写。

2) 开始位：开始位发送器是通过发送起始位而开始一个字符传送，起始位使数据线处于逻辑 0 状态，提示接受器数据传输即将开始。

3) 厂商版本位：是由标签生产厂商区别标签的型号或者版本而写入的位。

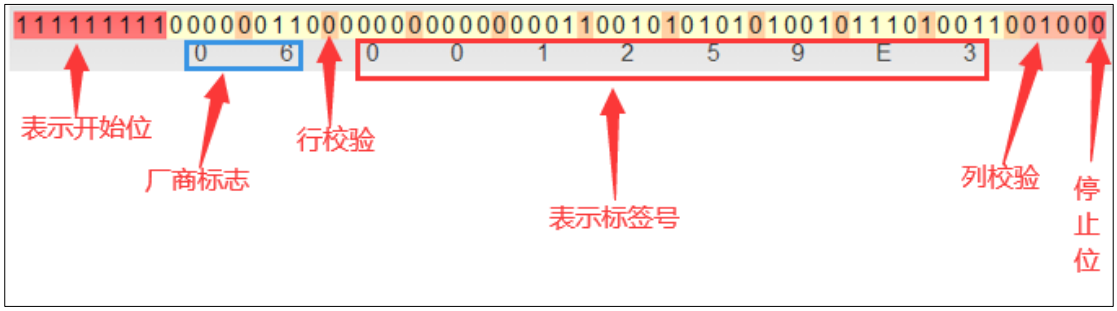
4) 数据位：是用来存储标签号。

5) 行校验位，行校验位可以认为是一个特殊的数据位，校验位一般用来判断接收的数据位有无错误，一般是奇偶校验。

6) 列校验位，列校验位可以认为是一个特殊的数据位，校验位一般用来判断接收的数据位有无错误，一般是奇偶校验。

7) 停止位，停止位在最后，用以标志一个字符传送的结束，它对应于逻辑 1 状态。

数据传输示例：厂商版本为 0x60，卡号为 0x001259E3，数据传输如下图所示。




## 韦根转换方法

韦根是由卡号倒数 5、6 位和后 4 位分别换算成 10 进制组成。

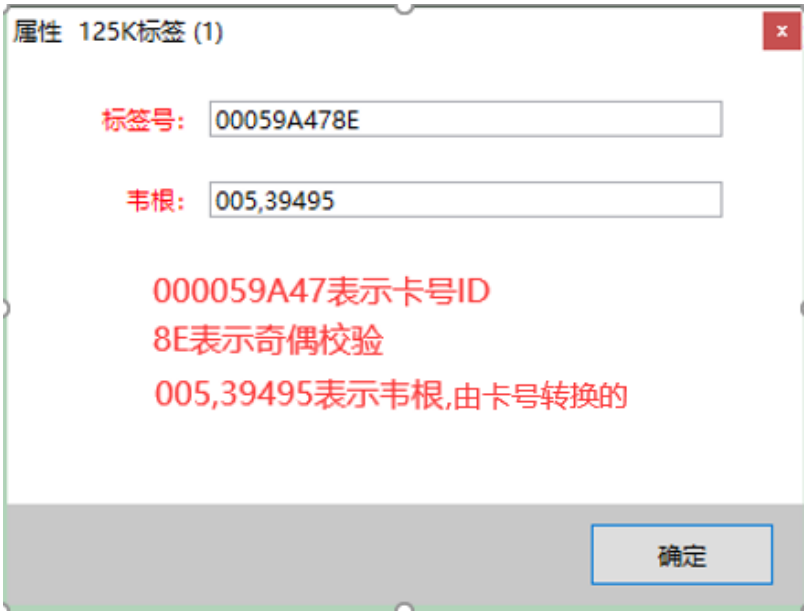
示例：卡号：0x001259E3 转换成韦根

倒数五六位为：12(十六进制)→18(十进制)

后四位：59E3(十六进制)→23011(十进制)

所以：0x001259E3 转换成韦根为 018，23011

仿真平台标签示例：




### 125K 设备功能

125K 设备只具有读卡功能，通过读取到的标签 ID 数据转换成韦根显示。在生活中的应用都是通过后台数据库进行操作的。如：小区门禁系统是通过判断读取到的卡号是否存在在后台数据库中，如果存在，则执行开门，否则不执行动作。

## 1.4.2. 14443 设备

### 高频 14443 设备

标签典型工作频率为 13.56MHz。一般以无源为主，标签与进行数据交换时，标签必须位于 RFID 阅读器天线辐射的近场区内。

标签的阅读距离一般情况下为 4~10cm。

标签的典型应用有：公交卡、银行卡、食堂饭卡等。

设备相关的国际标准有：ISO/IEC14443 等

## 14443 卡存储结构

| 扇区 | 区块 | 块地址 | 扇区 | 区块 | 块地址 | 扇区 | 区块 | 块地址 | 扇区 | 区块 | 块地址 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 扇区0 | 区块0 | 0 | 扇区4 | 区块0 | 16 | 扇区8 | 区块0 | 32 | 扇区12 | 区块0 | 48 |
| | 区块1 | 1 | | 区块1 | 17 | | 区块1 | 33 | | 区块1 | 49 |
| | 区块2 | 2 | | 区块2 | 18 | | 区块2 | 34 | | 区块2 | 50 |
| | 区块3 | 3 | | 区块3 | 19 | | 区块3 | 35 | | 区块3 | 51 |
| 扇区1 | 区块0 | 4 | 扇区5 | 区块0 | 20 | 扇区9 | 区块0 | 36 | 扇区13 | 区块0 | 52 |
| | 区块1 | 5 | | 区块1 | 21 | | 区块1 | 37 | | 区块1 | 53 |
| | 区块2 | 6 | | 区块2 | 22 | | 区块2 | 38 | | 区块2 | 54 |
| | 区块3 | 7 | | 区块3 | 23 | | 区块3 | 39 | | 区块3 | 55 |
| 扇区2 | 区块0 | 8 | 扇区6 | 区块0 | 24 | 扇区10 | 区块0 | 40 | 扇区14 | 区块0 | 56 |
| | 区块1 | 9 | | 区块1 | 25 | | 区块1 | 41 | | 区块1 | 57 |
| | 区块2 | 10 | | 区块2 | 26 | | 区块2 | 42 | | 区块2 | 58 |
| | 区块3 | 11 | | 区块3 | 27 | | 区块3 | 43 | | 区块3 | 59 |
| 扇区3 | 区块0 | 12 | 扇区7 | 区块0 | 28 | 扇区11 | 区块0 | 44 | 扇区15 | 区块0 | 60 |
| | 区块1 | 13 | | 区块1 | 29 | | 区块1 | 45 | | 区块1 | 61 |
| | 区块2 | 14 | | 区块2 | 30 | | 区块2 | 46 | | 区块2 | 62 |
| | 区块3 | 15 | | 区块3 | 31 | | 区块3 | 47 | | 区块3 | 63 |

1) 高频 14443 标签分为 16 个扇区，每个扇区由 4 块组成(块 0、块 1、块 2、块 3)，共 64 个块，每个块的存储容量是 16 个字节，因此 14443 标签的容量为 1KB。
2) 第 0 扇区的块 0（即块地址 0），它用于存放厂商代码其中包含卡号，已经固化，不可更改，只可以读取。
3) 每个扇区的块 0、块 1、块 2 为数据块，用于存贮数据(扇区 0 的块 0 除外)。
4) 每个扇区的块 3 为控制块，用于控制各个数据块的权限，以及控制位的权限。其中控制块中的数据，包括了密钥 A(6 个字节)、控制权限(4 个字节)、密钥 B(6 个字节)。
5) 每个扇区的密钥和控制权限都是独立的，可以根据实际需要设定各自的密钥及控制权限，控制权限为 4 个字节。整条控制位的数据共有 16 个字节，扇区中的每个块（包括数据块和控制块）的存取条件是由密钥和控制权限共同决定的。

## 14443 设备功能

**休眠：**控制标签的工作状态，读写器可下发控制指令，控制标签进入休眠状

态，只有被唤醒的标签才能与读写器进行通信。

**请求**：建立标签与读写器的通信链路，请求模式有两种：一种是只与未休眠的标签建立通信，另一种是天线范围内的标签建立通信包括休眠标签。

**寻卡**：用以获得读写器天线场区内标签的 ID 数据。

**密钥**：用以对指定卡片的指定数据块进行认证，通过密钥认证后方可操作。

**读取数据**：用以读取指定数据块的数据，前提是读取的数据块验证成功且有读取的权限。

**写入数据**：用以向指定的数据块写入数据，前提是写入的数据块验证成功且有写入的权限且写入的数据必须满足 16 个字节。

**电子钱包**：用以向指定的数据块设置为特定的格式，对特定的数据块可以实现充值消费。

## 仿真平台示例：


**存储格式**：14443 标签的数据存储格式是以 16 进制存储。块中数据显示为 32 位。

**标签号**：块 0 的前 4 个字节是标签号。

**控制块**：每个扇区的最后一个块是控制块，标签默认的密钥 A 与密钥 B 都是 FFFFFFFFFFFF。

**控制权限**：是 FF078069，表示最高权限，也就是说每个块只要认证密钥成功（认证其中一个）都可以进行读写等操作(块 0 除外)。

电子钱包：这里设置电子钱包格式为：00000000FFFFFFFF0000000008F708F7

前四个字节存储的是金额，第 5~8 字节是对前四个自己取反，第 9~12 字节存储的是金额，与前四个字节一致。

最后四个字节中 08 表示的是块地址，F7 表示的是对块地址 08 取反，如果块 4 为电子钱包，那么这里显示的块地址就是 04，取反为 FB。

示例：设置块八为电子钱包块，充值 100 元，块八的数据显示为：64000000 9BFFFFFF 64000000 08F708F7

**解析**：标签是以 16 进制格式存储的，因此把 100 转换成十进制，如下所示

100（十进制）→64(十六进制)

64(取反) →9B

## 1.4.3. 15693 设备

### 高频 15693 设备

标签工作频率为 13.56MHz。一般以无源为主，标签与进行数据交换时，标签必须位于 RFID 阅读器天线辐射的近场区内。

标签的阅读距离一般情况下为 1m 之内。

标签的典型应用有：图书馆应用、货物身份识别等。

设备相关的国际标准有：ISO/15693、ISO/18000-3 等。

### 15693 卡存储结构

| | 字节0 | 字节1 | 字节2 | 字节3 | |
|---|---|---|---|---|---|
| 块 -4 | UID0 | UID1 | UID2 | UID3 | 低字节UID |
| 块 -3 | UID4 | UID5 | UID6 | UID7 | 高字节UID |
| 块 -2 | Internally used | EAS | AFI | DSFID | 其他功能块 |
| 块 -1 | 00000000 | 00000000 | 00000000 | 00000000 | 访问控制块 |
| 块 0 | 00000000 | 00000000 | 00000000 | 00000000 | 用户数据块 |
| 块 1 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 块 2 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 块 3 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 块 4 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 块 5 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 块 6 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 块 7 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 块 8 | 00000000 | 00000000 | 00000000 | 00000000 | |

1) 高频 15693 标签分为 32 个数据块(块-4，块-3 组成的 UID 编码数据块、块 -2 其他功能块、块-1 访问控制块、块 0~块 27 用户数据块)，每个数据块由 4 个字节组成,标签容量为 128 字节=1024bit。
2) 块-4 ，块-3 存储卡片中的卡号，已经固化，可读不可写(块-4 是存储低字节 UID，块-3 是存储高字节 UID)。
3) 块-2 第一个字节存储的是用户保留块，第二个字节存储的是 EAS(电子商品防盗功能)数据块,第三个字节存储的是 AFI(应用族标识符)数据块,第四个存储的是 DSFID(数据存储格式识别)数据块。
4) 块-1 存储的是访问控制块，第一个字节分别存储的是（从低位到高位排列）用户保留区、EAS 数据块、AFI 数据块、DSFID 数据块，块 0~块 3 的访问状态，第二个字节存储的是块 4~块 11 的访问状态，第三个字节存储的是块 12~块 19 的访问状态，第四个字节存储的是块 20~ 块 27 的访问状态（访问状态为 1 个 2 进制数,0 代表可写,1 代表不可写，访问控制块当修改为不可写后不能进行更改）
5) 块 0~ 块 27 是用户数据块，用户可以将需要存储的数据写入到卡片中。

## 15693 设备功能

**读取标签 ID**：读写器可读取电子标签的 ID 数据，而且可以同时读取读写器

作用范围内的所有标签数据。

**读取数据：**用以读取指定数据块的数据，读取数据可以分为读取单个数据块与多个数据块。

**写入数据：**用以向指定的数据块写入数据，写入数据可以分为写入单个数据块与多个数据块，写入的数据必须满足字节数。

**锁定数据块：**锁定单个数据块的数据（在块-1 访问控制块中把锁定的数据块的状态改为 1）注意，这样的锁定时不可逆的，因此要慎用。

**设置 AFI：**往标签中写入 AFI 的值。作用通过 AFI 判断不同标签的类型(族标识)是否相同。

**锁定 AFI：**锁定标签的 AFI，则标签 AFI 不能更改。

**设置 DSFID：**往标签中写入 DSFID 的值。

**锁定 DSFID：**锁定标签的 DSFID，则标签 DSFID 不能更改。

**获取信息：**获取标签的基本信息，如：容量，AFI，DSFID 等。

**获取块安全状态：**主要是查看块有没有被锁定，锁定为安全。

## 仿真平台示例：

**标签号：**块－4 为低位，左低右高，CFD09EF3 排列为 F39ED0CF，块为-3 为高位，8A0104E0 排列为 E004108A；因此，标签号为 E004108AF39ED0CF。

**EAS：**00 表示没有激活防盗功能。

## 1.4.4. 超高频设备

### 超高频设备

标签工作频率为 902MHz～928MHz，其特点是天线小、传输距离远、成本高，标签灵活性强，轻易就可以识别得到。

标签的阅读距离可以达到 10m 以上。

标签的典型应用有：高速收费(ETC)等。

设备相关的国际标准有：ISO/18000-6 等。

### 超高频存储结构

| 存储区 | 块地址 | 存储信息 | 数据 |
|---|---|---|---|
| 保留内存 | 0 | 杀死口令 | 0000 |
| | 1 | | 0000 |
| | 2 | 访问口令 | 0000 |
| | 3 | | 0000 |
| EPC存储器 | 0 | 校验位 | 9812 |
| | 1 | 控制（PC）位 | 3000 |
| | 2 | 电子产品码(卡号) | E200 |
| | 3 | | 8367 |
| | 4 | | 6705 |
| | 5 | | 0125 |
| | 6 | | 1560 |
| | 7 | | 7500 |


## 1.4.5. 有源 2.4G 设备

### 有源 2.4G 特点

标签工作频率为 2.400GHz~2.4835GHz，其特点是低电压，高效率

体积小，低成本，双向高速数据传输。

标签的典型应用有：无线遥控，无线鼠标等。

### 有源 2.4G 设备功能

**读取标签 ID**：读写器可读取有源电子标签的 ID 数据，而且可以同时读取读写器作用范围内的所有标签数据。

**设置读写器 ID**：可以设置读写器的 ID 数据。

**设置标签 ID**：可以设置写器作用范围内的标签 ID，在设置标签 ID 的时候，

保持读写器范围内只有一张标签。

**设置标签周期：**设置标签发送数据的周期。

### 1.4.6. Zigbee 设备

协调器(Coordinator)

用来创建一个 Zigbee 网络,并为最初加入网络的节点分配地址,每个 Zigbee 网络需要且只需要一个协调器(Coordinator)。

路由器(Router)

也称为 Zigbee 全功能节点，可以转发数据，起到路由的作用，也可以收发数据，当成一个数据节点，还能保持网络，为后加入的节点分配地址。

终端节点(End Device)

通常定义为执行具体功能的设备。

**虚拟仿真平台 zigbee 节点介绍**

# 第2章 应用搭建与测试

## 2.1. 任务引导

### 2.1.1. 学习目标

本章的目的是让同学们掌握应用设备的搭建与测试程序的使用。

## 2.2. 125K 寻卡实验操作

### 2.2.1. 实验思路

在虚拟仿真实验平台中搭建好设备，启动测试程序，通过串口通信，读取到

125K 标签号与韦根号，并显示在测试程序文本框中。

## 2.2.2. 实验设备

125K 读写器、串口线、 5V2A 电源、 125K 标签。

## 2.2.3. 实验步骤

**步骤一：选择设备**

启动虚拟仿真实验平台，在工具箱中找到 125K 设备，拖入到实验台中，如图 2-2-1 所示。

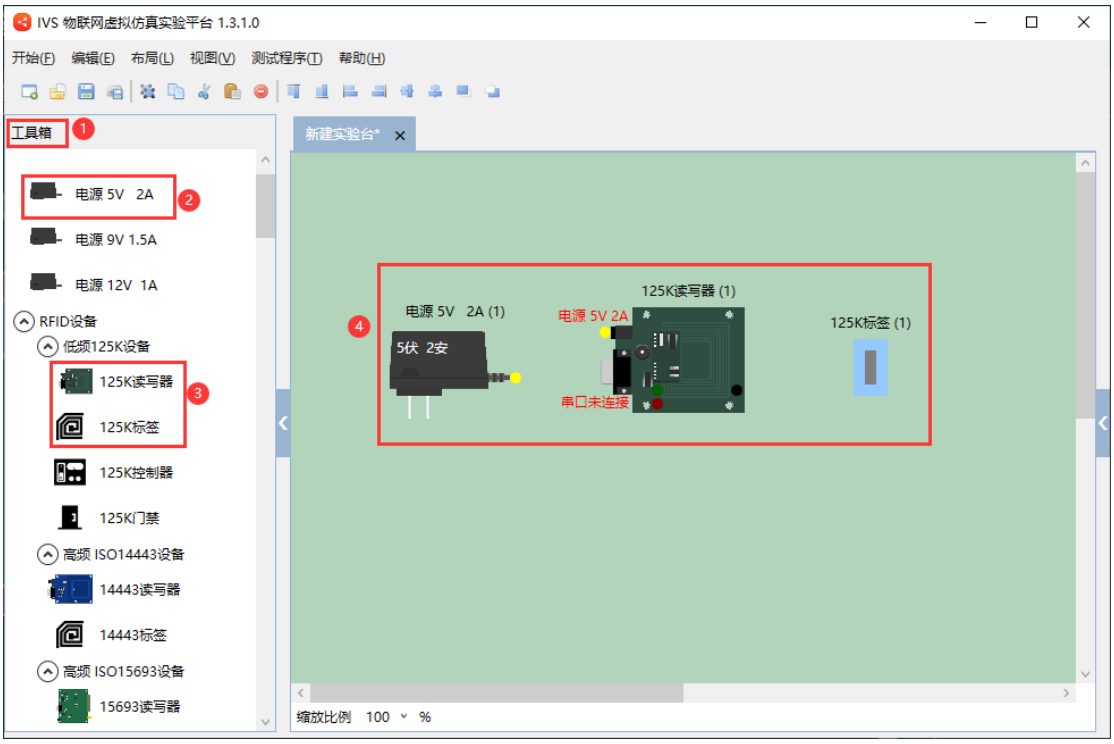



图 2-2- 1 选择设备

**步骤二：设备供电**

选中电源，单击鼠标右键，选择接电，如图 2-2-2 所示，然后选择需要供电的设备(125K 读写器)，接电完成，如图 2-2-3 所示。

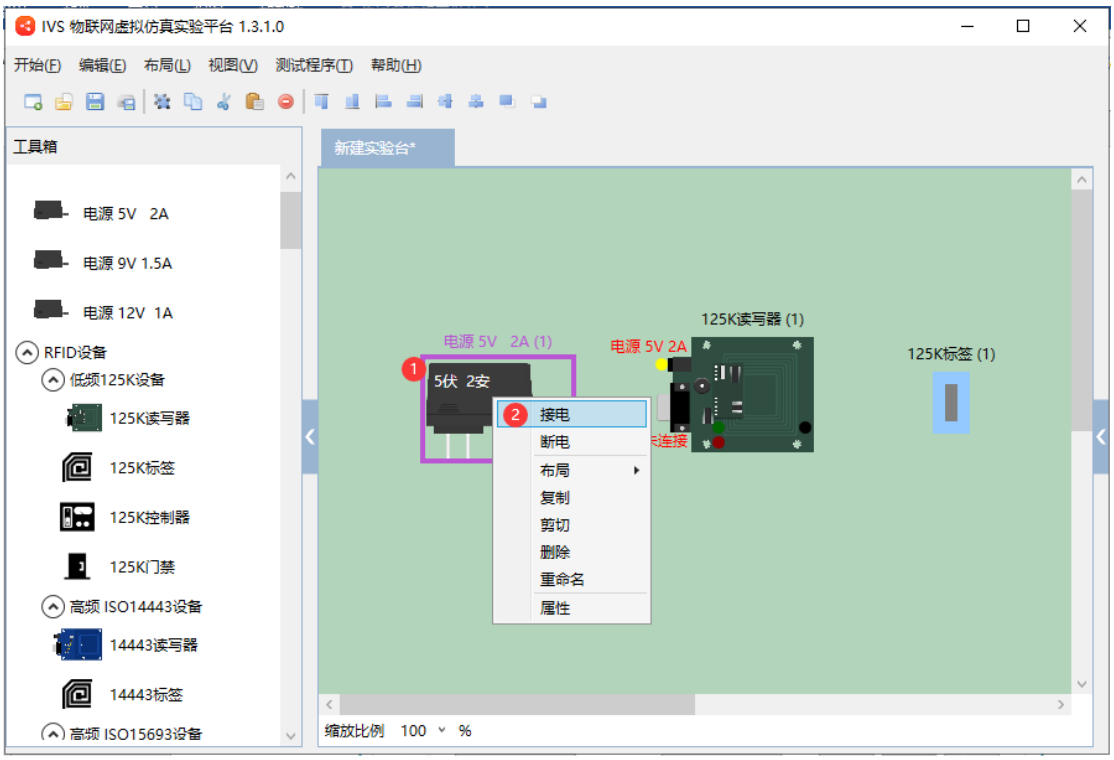



图 2-2- 2 选择接电

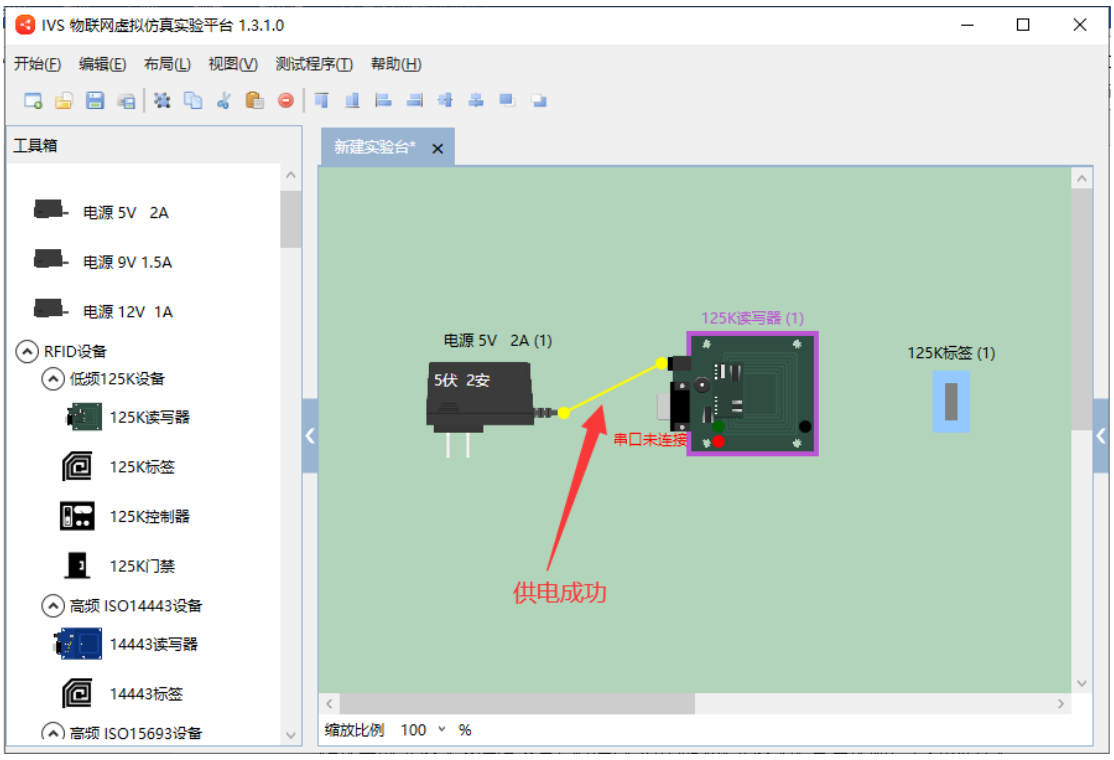



图 2-2- 3 接电成功

**步骤三：分配通信端口**

给读写器分配一个通信端口，选中 125K 读写器，单击鼠标右键，选择串口

连接，如图 2-2-4 所示，弹出串口选择框，选择一个未被使用的串口号，单击确定，如图 2-2-5 所示。

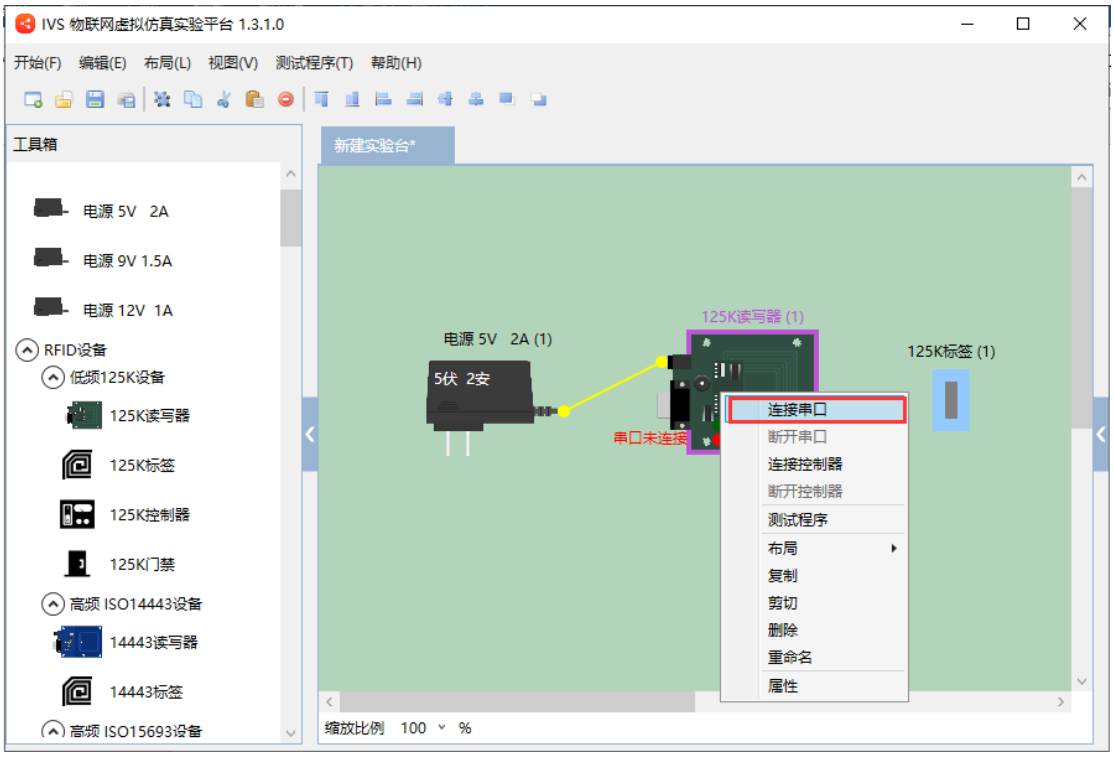



图 2-2- 4 选择连接串口

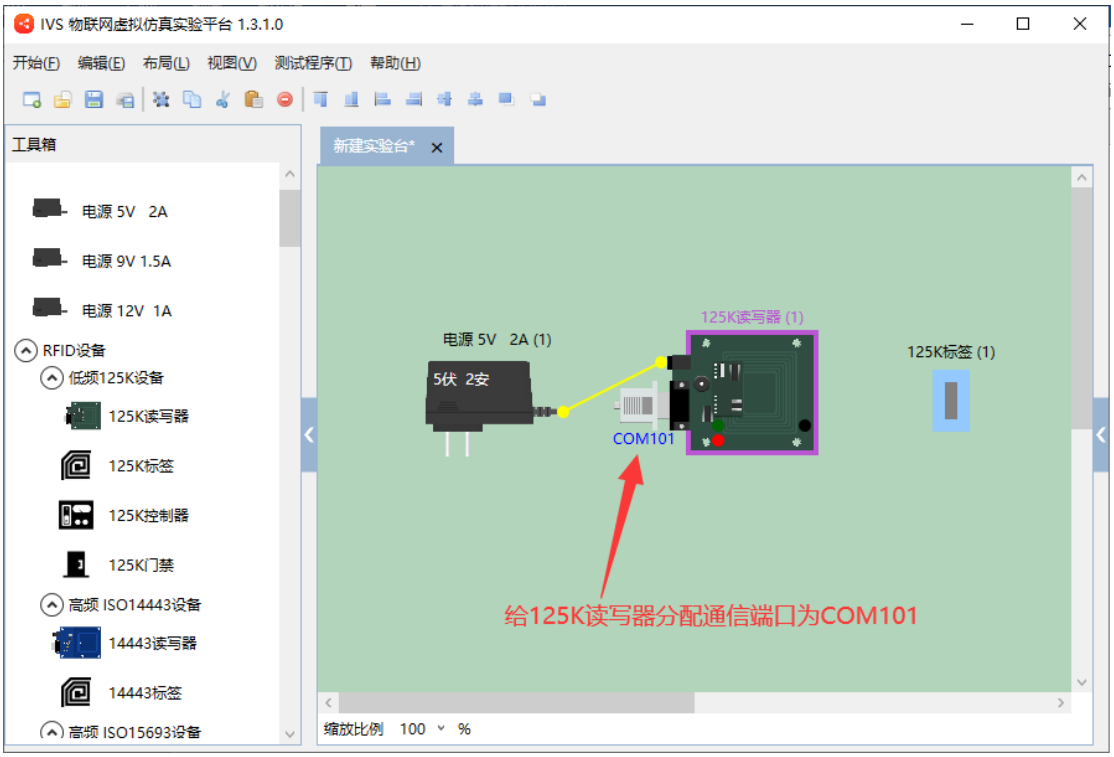



图 2-2- 5 分配通信串口 COM101

**步骤四：启动测试程序**

单击菜单栏中测试程序，选择 125K 读写器，如图 2-2-6 所示，测试程序打开成功如图 2-2-7 所示。

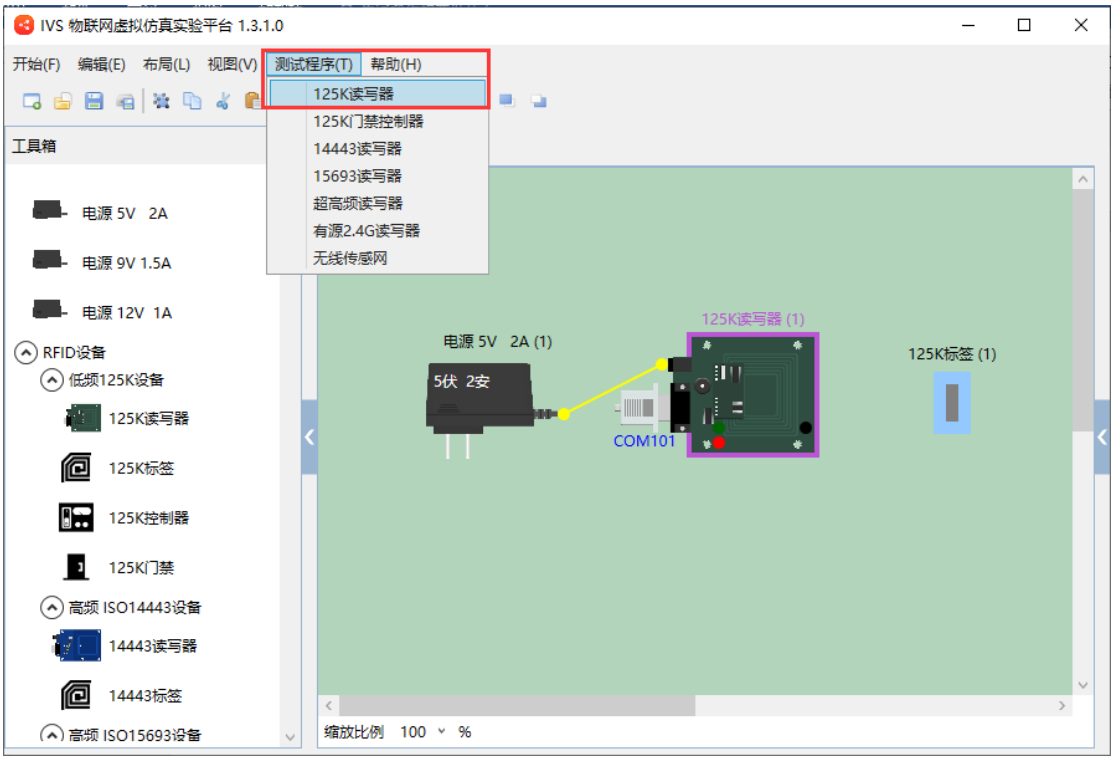



图 2-2- 6 选择 125K 读写器测试程序

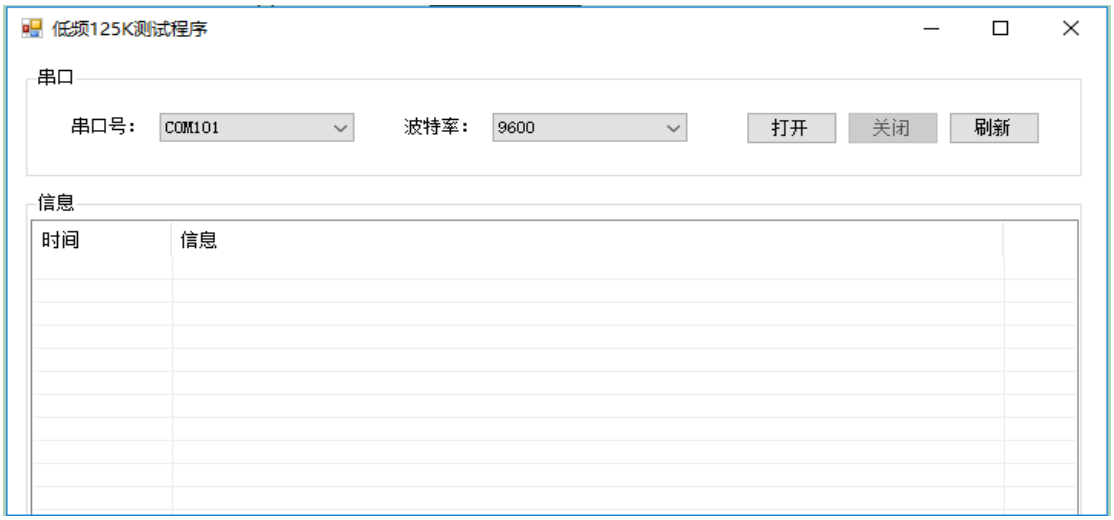



图 2-2- 7 125K 测试程序

**步骤五：打开串口**

选择与 125K 读写器一致的串口号，单击【打开】指令，使测试程序与 125K 读写器建立通信，操作结果会在信息栏中显示，如图 2-2-8 所示。


图 2-2- 8 打开串口

**步骤六：读取标签**

在虚拟仿真平台中，把 125K 标签从 125K 读写器场区外拖入到场区内，才能读取到标签号并显示在信息栏中，如图 2-2-9 所示。


图 2-2- 9 读取标签

**步骤七：查看标签**

选中标签，单击鼠标右键，选择属性，如图 2-2-10 所示。查看标签属性中的标签号与韦根号与读取的数据是否一致，如图 2-2-11 所示。

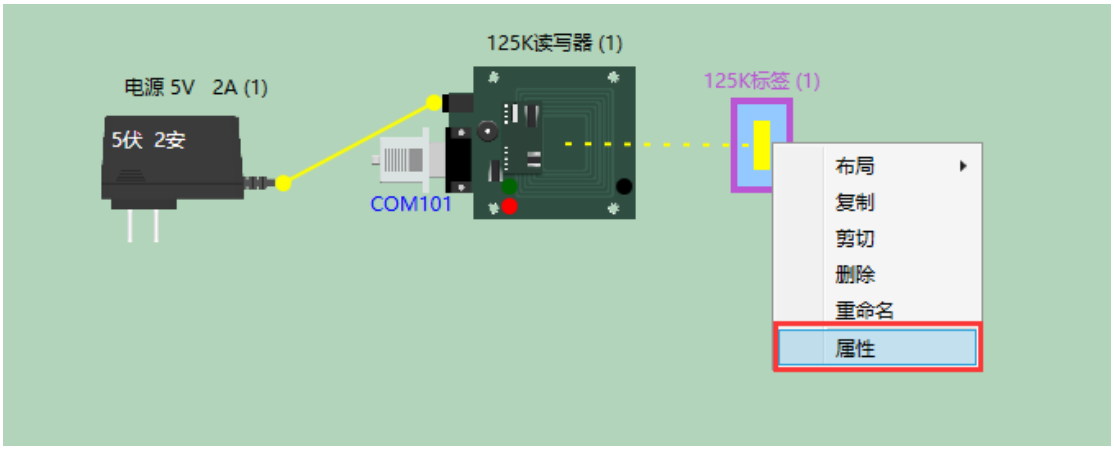



图 2-2- 10 选择标签属性


图 2-2- 11 查看数据

注意：

125K 标签在读写器场区内会有黄色虚线提示。

读取标签时，需要把标签从厂区外移到厂区内，如果是在读写器范围内移动，则读取标签失败。