UHF RFID EPC Gen-2 标准
ElecKits ST25RU3992（AS3992）读写模块
使用手册

（本文档支持 Eleckits Roger、MIRCO 及 Colt 模块）

本手册是应用矽控电子（中远嵌入式）ElecKits ST25RU3992（AS3992）读写模块的操作手册。将详细描述 AS3991/ST25RU3992（AS3992）读写模块的性能、UHF RFID 电子标签的存贮体系及操作、读写器的系统结构、命令码结构、动态函数库的使用说明。用户在使用 AS399X 读写模块开发项目时请先详细阅读本说明书。如有任何问题，请及时向供应商联系。

前言

UHF RFID 无线射频识别系统是一种非接触自动识别技术，其基本原理是利用射频信号的空间耦合的传输特性，实现对识别物体所带信息的自动化读取和识别。

RFID 识别系统由三个部分组成：硬件部分、应用软件部分以及 RFID 数据格式的标准与通信协议。其中的硬件部份主要包括：RFID 读写器（阅读器，Reader）、电子标签（应答器，Tag）以及天线。在使用中，RFID 读写器循环扫描（轮询）读取电子标签数据，一旦标签进入读写器的天线有效范围内，读写器就可以读取 RFID 标签中的数据，从而完成对产品的信息收集。读写器可将数据通过通信接口传到主控制器或主机上，以作进一步的数据处理。

RFID 系统的工作频率有多种，目前应用较为广泛的为 125KHz、13.56MHz、920MHz。
在商品应用领域使用较多的是 EPC UHF G2 标准，它是应用 900MHz 的 UHF 甚高频作为无线传输媒介。其相较于其它的标准，优点主要体现在传输距离远（可达 10 米以上）、标签价格更为便宜。 随着国内经济的快速发展，相信 EPC 体系会有着广阔的前景。

ST25RU3992（AS3992）读写器/读写模块不仅支持 ISO18000-6C 协议，还兼容 18000-6A/B 协议，可完成对符合这些协议的电子标签的所有操作，并提供完善的用户接口和用户端 PC 机或自主的控制器的操作函数，方便用户可靠、快速地完成对 UHF 电子标签的操作。用户可以应用读写器直接完成对电子标签的相关操作，如标签发行、标签识别等。也可以将读写模块嵌入到自己的产品中，使自身的产品具有电子标签识别的功能。

在本技术手册中，我们将详细说明 AS3991/ST25RU3992（AS3992）读写器/读写模块的系统结构、操作步骤、外部通信接口、操作命令集、应用函数动态库以及我们提供的测试应用程序使用指南。还包括《EPC UHF G2》标准对于电子标签部份的详细说明。用户在完整地阅读完本手册后，可以较为方便地了解电子标签的应用概念，并完成对电子标签的操作。最终将 AS399X 系列读写器/读写模块应用到自身的系统中。用户在使用 AS399X 读写器前，请先阅读本说明书。对于较为专业的用户，可以直接查看自己所需的部份。而对于一般用户来说，完整地阅读本书，相信会对你的工作有较大的帮助。

AS399X 系列读写器/读写模块是我公司应用 austriamicrosystems 公司出产的 AS3991/ST25RU3992（AS3992）芯片、新华龙电子公司的 C8051F340 芯片以及其它射频电路设计的。它具有集成度更高、性能更稳定、价格更合适等优点，可适用于识别 EPC 电子标签的多种应用场合。并可以嵌入到用户的产品中构成更多的应用。

我们公司正一直致力于非接触射频读写器/读写模块产品的研发及应用，不断地积累经验和技术，相信将会为用户提供更为完善的技术支持。

同时我们看到，EPC 技术在国内应用目前尚在发展阶段，各种应用所需的读写器/读写模块各不相同。而各种读写器/模块中的器件的组合、功能的实现会对最终产品的性能及产品价格会有较大的影响。经常地：用户可能只需要读写器/模块的某项功能或发射功率较低，这样就会选用较为便宜的读写器产品。为此我们愿提供满足用户所需的相关产品，可以按照用户的需要，如模块功能、PCB 板尺寸、发射机功率等进行定制，这样产品的价格会降低，而以较好的性价比提供给用户。

如果你有任何需要，请及时联系我们，我们将为你提供完善的服务。

目 录

第一章 AS399X 读写器系统体系

AS399X 读写器/读写模块是我公司研制生产的用于符合 ISO18000-6C 协议或 18000-6A/B 协议电子标签的读写机具。它独立完成对符合标准的电子标签的读写及控制操作，可广泛应用于需以电子标签作为存贮媒体的应用系统或产品中。它可以作为用户系统中的一部份，受控于主控制器，完成用户系统设定的对电子标签的所有操作。用户应用本读写器/模块，能够简便地构成自己的 RFID 应用系统。

1.1 AS399X 读写器系统结构及功能说明

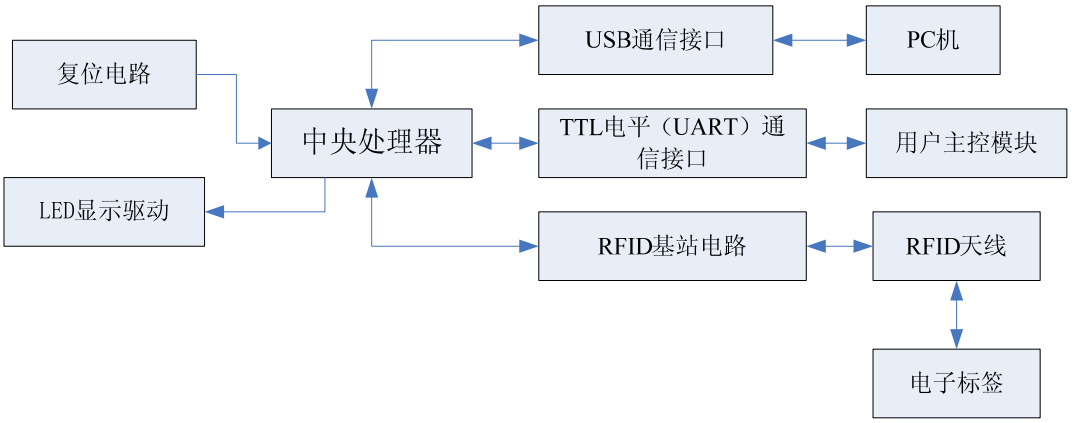
1.1.1 AS399X 读写器系统结构

AS399X 读写器/读写模块的核心部分包括一个微处理器和一个 RFID 基站芯片。它能独立完成对电子标签的所有操作，具有与用户主系统的命令数据通信能力，可按照用户提供的命令完成对电子标签的读写操作，并将所得数据返回给用户系统，这个用户系统可以是一个主控板或 PC 机。

AS399X 读写模块提供 UBS 或 UART 通信方式与用户系统进行通信，极大地方便了用户的联接和应用。

AS399X 读写器/读写模块硬件主要由 C8051F340 中央微处理器、RFID 基站芯片（AS399X）、高频电路、模块天线、复位电路、LED 状态显示电路等组成。它具有集成度更高、性能更稳定、性价比更好等特点。

其硬件结构图为：



1.1.2 AS399X 读写器功能说明

AS399X 读写器/读写模块可以完成对电子标签的所有读写操作，其操作由连接的主控系统发出的读写命令控制完成，具体可以完成如下功能：

- 模块操作
  完成对读写器提供 LED 显示控制以及外部 I/O 的控制。
- 读写器/模块系统参数设置
  完成对读写器系统的参数进行设置，如发射机功率、天线状态以及接受部分灵敏度等参数的设置。
- 电子标签的访问操作
  完成对电子标签的所有访问操作，包括轮询标签、唤醒标签、读标签数据、写标签数据、灭活标签、锁定标签、休眠标签等功能。
- 与外部主机的通信
  提供与外部主机的通信方式，包括 UART TTL 电平通信、USB 通信接口。

应用这些通信方式，用户可以实现与 AS399X 读写器/模块的通信，发送相关的命令来完成

对电子标签的操作。

读写器/模块可以很方便地嵌入到用户系统中，较快地完成系统的功能。可以在一个通信总线上同时加装多台读写器/模块，分别进行控制。

1.1.3 AS399X 读写器性能

标签协议：支持 ISO18000-6C（EPC GEN2）、ISO18000-6A/B 协议
工作频率：920.625—924.375MHz，符合国家 RFID 标准
902.75—927.25MHz，美国 RFID 标准
865.7—867.5MHz，欧洲 RFID 标准
可设置 840—960MHz 之间的可用工作频段
跳频方式：FHSS 自动跳频
发射机功率：可由用户软件设置，最大 20dBm，100mW
工作电压：DC +3.3V 2A；+5.5V 可选
天线接口：1 个
天线匹配电阻：50 ohm
与主机接口：TTL
USB
通信波特率：115200bps，9600bps
N，8,1,0
输入/输出接口：2 个输入接口，2 个输出接口
状态指示驱动：3 个 LED 灯显示
主要器件：C8051F340
AS399X
RCP890A05
工作温度：-20—+80 度

1.2 RFID 读写器系统组成

1.2.1 系统组成

RFID 读写器系统包括如下部分：

RFID 读写模块 一块
RFID 读写天线 一块
与 PC 机连接的通信电缆 一条
EPC UHF GEN2 电子标签 一个
RFID 读写器开发资料及应用程序

1.2.2 系统安装

RFID 读写模块既可以直接连接到用户 PC 机上，作为一个电子标签读写器独立使用，又可以作为用户应用系统的一部分，嵌入到用户系统中。

以下步骤说明 RFID 读写器连接到用户 PC 机上的步骤，用户可以应用本系统提供的测试软件对 RFID 标签进行操作，以熟悉对电子标签的使用。

1） 将 RFID 读写器用 USB 线连接到 PC 机上；
2） 接入 RFID 读写模块的外部电源；
3） 打开 PC 机电源，将 RFID 系统盘拷贝到计算机中，安装系统软件；

1.3 用户系统开发步骤

如果你是第一次使用本系列的产品，或者第一次应用 RFID 电子标签做应用系统，请按照以下描

述的流程展开你的开发工作，会对你有所帮助。

1. 依据系统需求，确定符合要求的产品。

若直接与计算机连接，可以采用 RFID 读写器；若需要将模块接入到你自己的终端产品，可以采用 RFID 读写模块；若以上二项都不满足你的要求，请与供应商联系定制所需产品。

并请按照自己的应用要求选择相关的外接天线。天线的性能会对读写器的读写距离有很大的影响。

2. 依据系统需求，确定符合要求的 RFID 标签

由于各个厂商生产的 RFID 标签的容量及功能各有一些不同，其价格及供货情况也会不一样，故用户在选用某一厂商的卡片时，应综合考虑自己的要求进行选择。

一般应以性能、供货渠道、价格等因素来考虑。

3. 阅读 RFID 标签技术资料，详细了解该 RFID 标签的数据存取结构，操作方式以及电子标签可执行的命令。设计用户数据的存储结构。

4. 选择主机与 RFID 读写器/读写模块之间的通信方式

RFID 读写器的操作是由主系统发出控制命令来完成的，目前我们提供的 RFID 读写器/读写模块提供了两种与主系统之间的命令传输方式：

TTL 电平 UART

USB

5. 阅读《通信指令集》，了解 AS399X 读写器/模块与主控方的通信指令。

6. 应用系统开发

用户在开发自己的系统前，应详细阅读所有的资料，并通过使用我们提供的读写器测试应用程序，了解 RFID 标签的功能及相关命令的使用。这些会对用户系统的开发提供很大的帮助。

本系统提供了完整的用户系统开发所需资料，包括 RFID G2 UHF 标准资料、RFID 读写器/模块命令手册以及读写器应用程序。请参阅相关章节，相信这些对你的产品研制一定会有帮助。

7. 用户定制模块

用户如果认为现有的读写器/模块的功能、性能或性价比等不适合自己的要求，请及时与供应商联系，我们可以按照你的要求进行定制，最终会较好的性价比形成适合你需求的产品。

第二章 EPC UHF G2 电子标签说明

在应用电子标签进行系统应用前，用户需先详细了解 UHF 电子标签的功能、存贮结构以及操作命令。这对于今后各章中进一步理解读写器操作命令的各项参数也是很重要。

本章将详细描述《EPC G2 UHF RFID》标准、标签操作命令集以及标签的数据响应格式。EPC G2 命令集包括对标签操作的基础命令集以及各厂商的提供的标签的可选用命令集。一般来说，所有厂商提供的标签均应符合该标准，其操作步骤与本章描述相同，但亦有可能会在此基础上提供其专用命令，用户在对标签操作前，需参考相关厂商的产品说明书。

用户如发现我们所编写的内容与国际标准有不一致的地方，则应以国际标准为准。并请能及时通知我们，进行相关的确认。亦帮助我们进一步完善对国际标准的准确理解。

本章包括如下部分：

1） EPC G2 UHF 标准的接口参数

2） 电子标签的存贮器结构

3） 一些重要的 EPC 标签的概念说明

4） 电子标签操作命令集

2.1 EPC G2 UHF 标准的接口参数

对于每间公司生产的符合 EPC G2 UHF 标准的电子标签，其功能和性能均应符合 EPC G2 UHF 相关无线接口性能的标准。从用户应用标签的角度来说，我们不需要详细了解该标准的各项参数及读写器与电子标签之间的无线通信接口的协议。但对以下参数有一个大致的了解，对于用户应用电子标签会有较大的帮助。

以下为 EPC G2 UHF 物理接口概念以及其简明说明，以帮助用户对该标准有一个了解。详细说明请参考 EPC G2 UHF 标准文本。

系统介绍

EPC 系统是一个针对电子标签应用的使用规范。一般系统包括有读写器、电子标签、天线以及上层应用接口程序等部份。每家厂商提供的产品应符合国家的相关标准，所提供的设备在性能上有不同，但功能会是相似的。

无线通信过程

读写器向一个或一个以上的电子标签发送访问命令信息，发送方式是采用无线通信的方式调制射频载波信号。标签通过相同的调制射频载波接收功率。

读写器通过发送未调制射频载波和接收由电子标签发射（反向散射）的信息来接收电子标签中的数据。

工作频率：920.125MHz—924.875MHz,20 个频道（国家标准）

865.7MHz—867.5MHz，4 个频道（欧洲标准）

902.75MHz—927.25MHz，50 个频道（美国标准）等

EPC G2 UHF 的标准文本所规定的无线接口频率为：860MHz—960MHz，但每个国家在确定自己的使用频率范围时，会根据自己的情况选择某段频率作为自己的使用频段。

我国目前暂订的使用频率为：920MHz—925MHz。

用户在选用电子标签和读写器时，应选用符合国家标准的电子标签及读写器。一般来说，电子标签的频率范围较宽，而读写器在出厂时会严格按照国家标准规定的频率来限定。

频道工作模式：跳频扩频模式

读写器在有效的频段范围内，将该频段分为 20 个或 4 个或 50 个频段，在某个使用的时刻读写器与电子标签的通信只占用一个频道进行通信。为防止占用某个频道时间过长或该频道被其他设备占用而产生的干扰，读写器应用 FHSS 自动跳频技术动态跳到下一个频道。

用户在使用读写器时，如发现某个频道在某地已被其他的设备所占用或某个频道上的信号干扰很大，可在读写器系统参数设定中，先将该频道屏蔽掉，这样读写器在自动跳频时，会自动跳过该频道，以避免与其他设备的应用冲突。

发射功率：最大 20dBm

读写器的发射功率是一个很重要的参数。读写器对电子标签的操作距离主要会由该发射功率来确定，发射功率越大，则操作距离越远。

读写器的发射功率可以通过系统参数的设置来进行调整。可分为几级或连续可调，用户需根据自己的应用调整该发射功率，使读写器能在用户设定的距离内完成对电子标签的操作。对于满足使用要求的，将发射功率调到较小，会较少能耗。

天线：50Ohm,范围为 900—930 MHz

天线是读写系统中非常重要的一部份，它对读写器与电子标签的操作距离有很大的影

响。天线的性能越好，则操作距离可能会越远，操作的稳定性会更好。

天线的选择参数包括：天线增益，驻波比及天线的方向性和天线尺寸。一般应选择天线驻波比低的，应小于 1.5。用户在选用时需作较多的关注。

读写器与天线的连接有二种情况，一种是读写器与天线装在一起，称为一体机，另一种是通过 50Ohm 的同轴电缆与天线相连，称为分体机。

一个读写器可以同时连接多个天线或只有一个天线，在使用这种含多个天线的读写器时，用户需先设定天线的使用顺序。

密集读写器环境（DRM）

在实际应用场合，可能会同时存在多个读写器在一个空间范围内同时运行，这种情况被称为密集读写器环境，各个读写器会占用各自的操作频道对自己的某类电子标签自行操作。用户在使用时，需根据需要选用可在 DRM 环境下可靠运行的读写器。

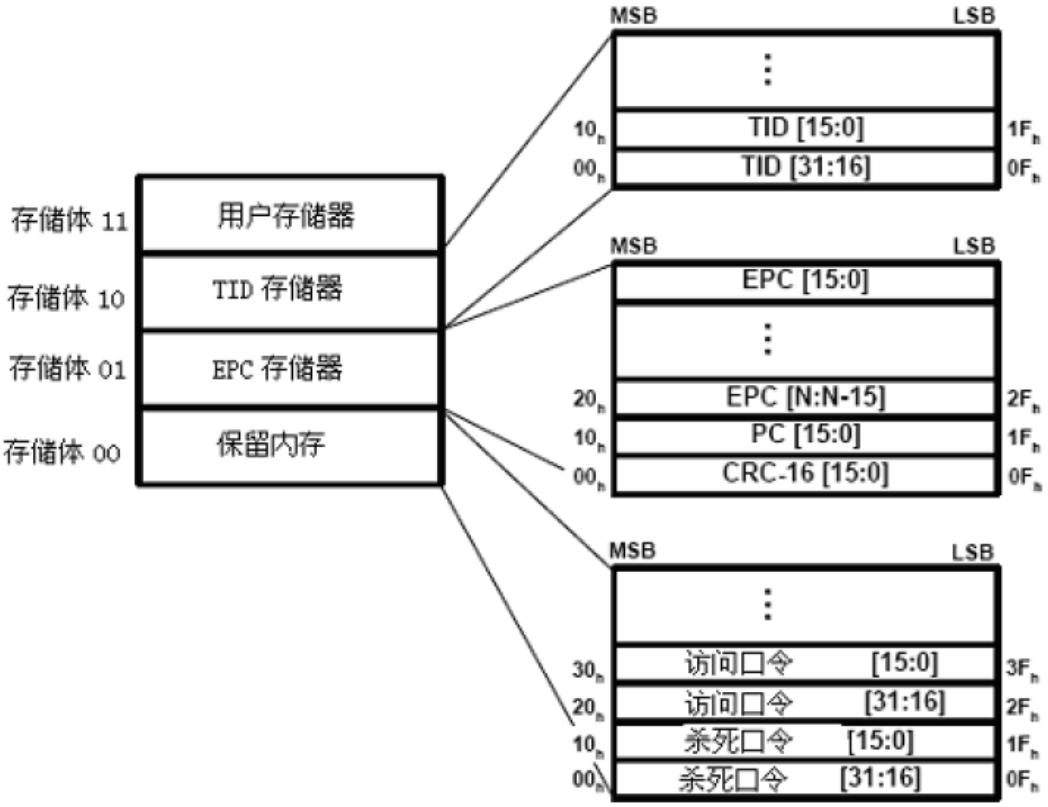
数据传输速率：读写器与标签之间交换数据，有高/低两种传输速率。对于一般的厂商提供的标签，我们都首先选择高速数据传输速率。

2.2 电子标签的存贮器结构

对于每个厂商生产的电子标签，其存贮器的结构是相同的，但会存在存贮器容量大小的差别。

2.2.1 电子标签存贮器

从逻辑上来说，一个电子标签被分为四个存贮体，每个存储体可以由一个或一个以上的存储器字（2 个字节）组成。其存贮逻辑图为：



从以上结构图中可以看到，一个电子标签的存贮器分成四个存贮体，分别是：

存贮体 0：保留内存（Reserver）

存贮体 1：EPC 存贮器（EPC）

存贮体 2：TID 存贮器（TID）

存贮体 3：用户存贮器（User）

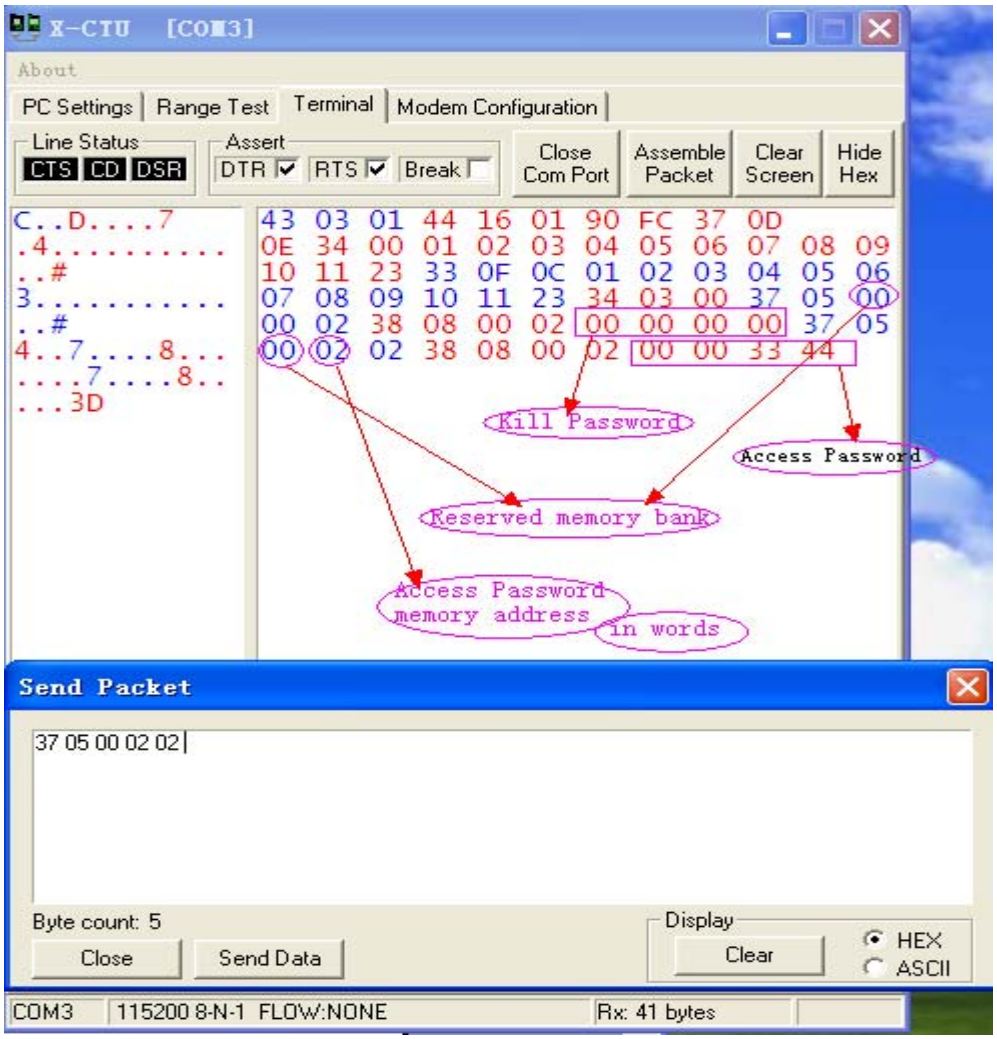
这四个存储体的定义是：

a） 保留内存 保留内存为电子标签存贮密码（口令）的部份。包括灭活口令（Kill Password）和访问口令(Access Password)。

灭活口令和访问口令都为 4 个字节。

其中： 灭活口令的地址为 00H—03H（以字节为单位）；

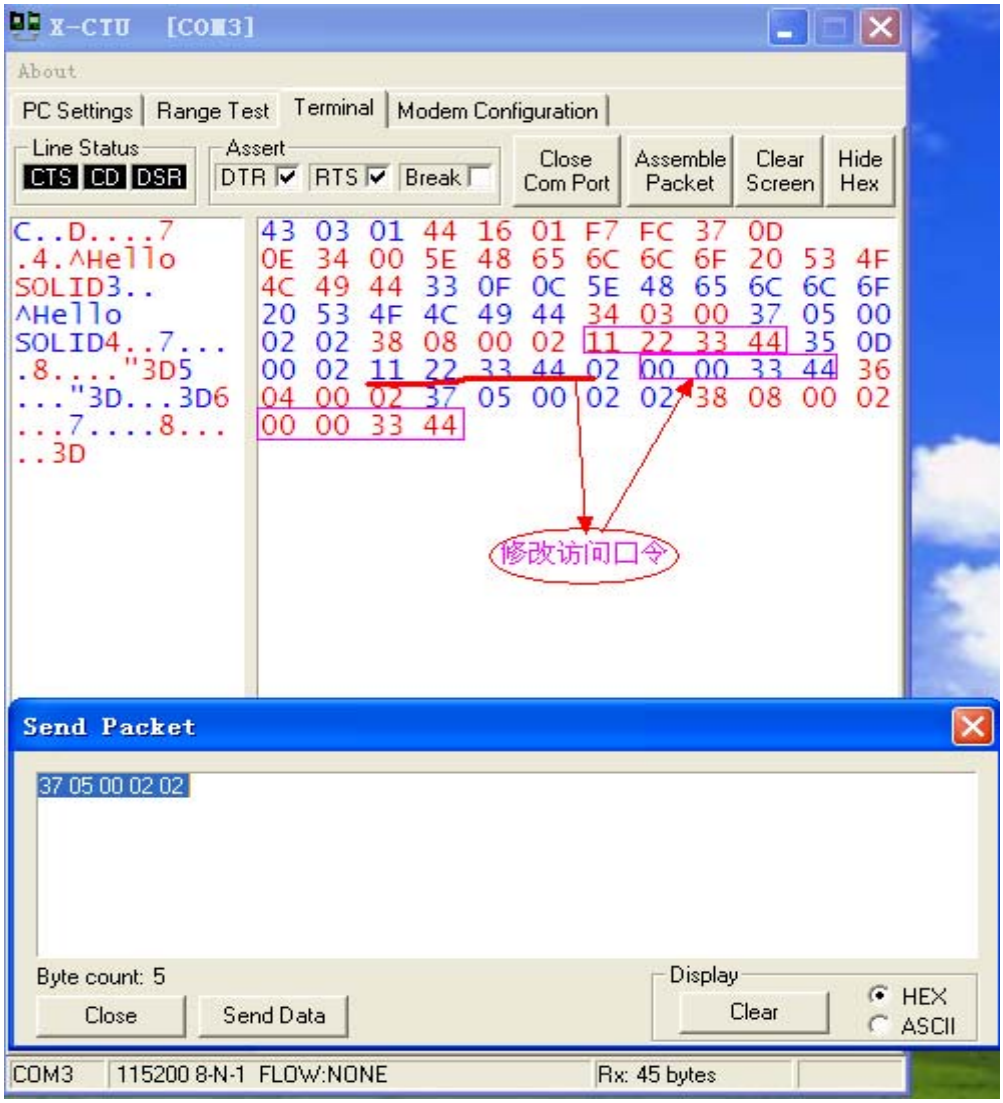
访问口令的地址为 04H—07H。



通常标签的初始访问口令默认为：00 00 00 00，在写标签时会需要这个口令。

你可以根据需要修改访问口令，如

将访问口令 11 22 33 44 改成 00 00 33 44



b) EPC 存储器 EPC 存储器用于存贮电子标签的 EPC 编号、PC（协议-控制字）以及本存贮块数据的 CRC—16 校验码。

其中：CRC—16：存贮地址为 00—01H，2 个字节，CRC-16 为本存贮体中存贮数据的 CRC 校验码。

PC：电子标签的协议-控制字，存贮地址为 02—03H，2 个字节。

PC 是指本电子标签的控制信息，包括如下内容：

PC 为 2 个字节，16 位，其每位的定义为：

00-04 位：电子标签的 EPC 号的数据长度.

$=00001_2$：EPC 为一个字,16 位

$=00010_2$：EPC 为两个字,32 位

$=00011_2$：EPC 为三个字,48 位

$=11111_2$：EPC 为 31 个字，496 位

05--07 位：RFU=000

08—0F 位：$=00000000_2$

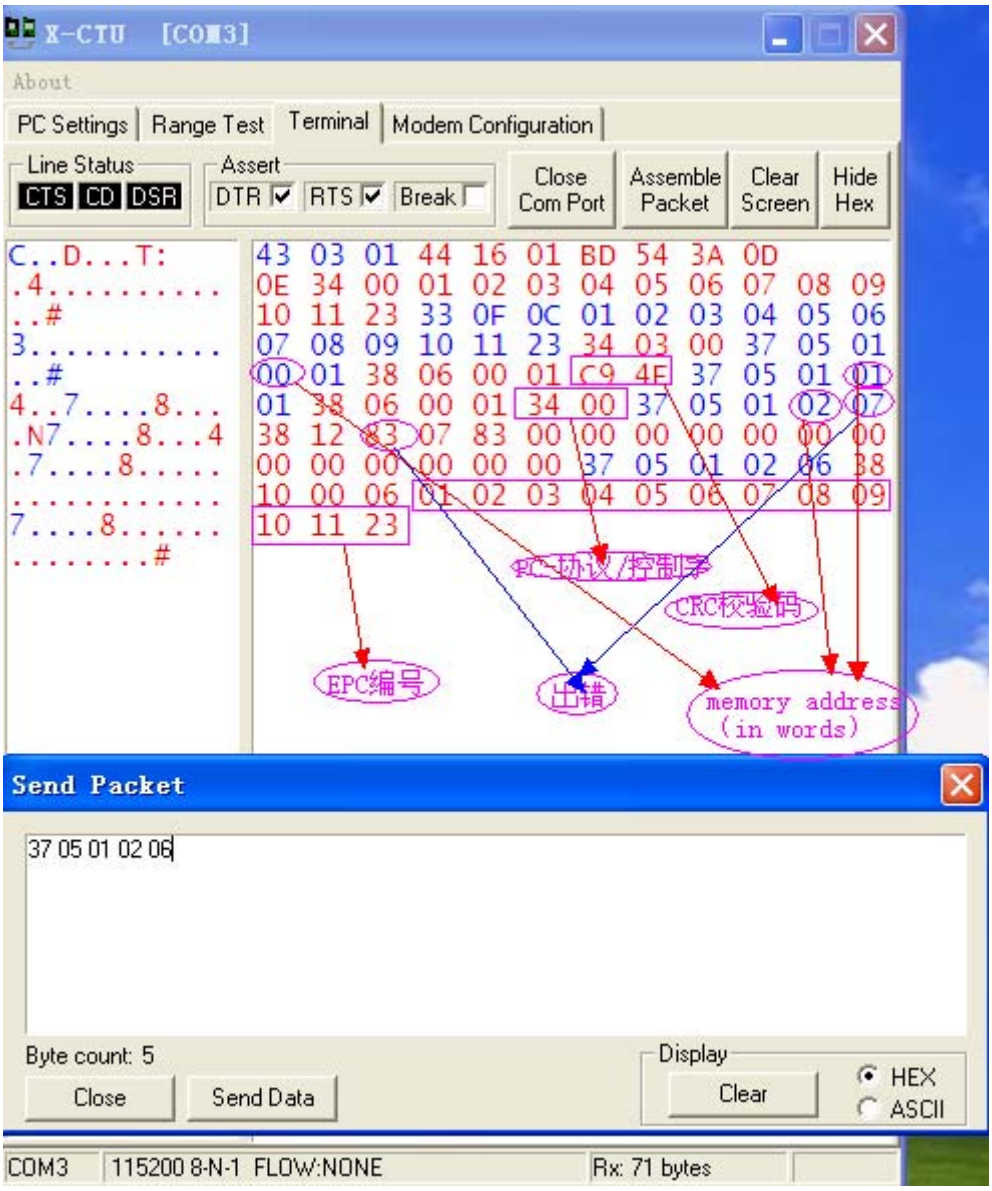
EPC 编号：若干个字,由 PC 的值来指定。

EPC 为本标签的编码。EPC 存储在以 04h 字节存储地址开始的 EPC 存储器内，MSB 优先。每类电子标签(不同厂商或不同型号)的 EPC 号长度可能会不同。

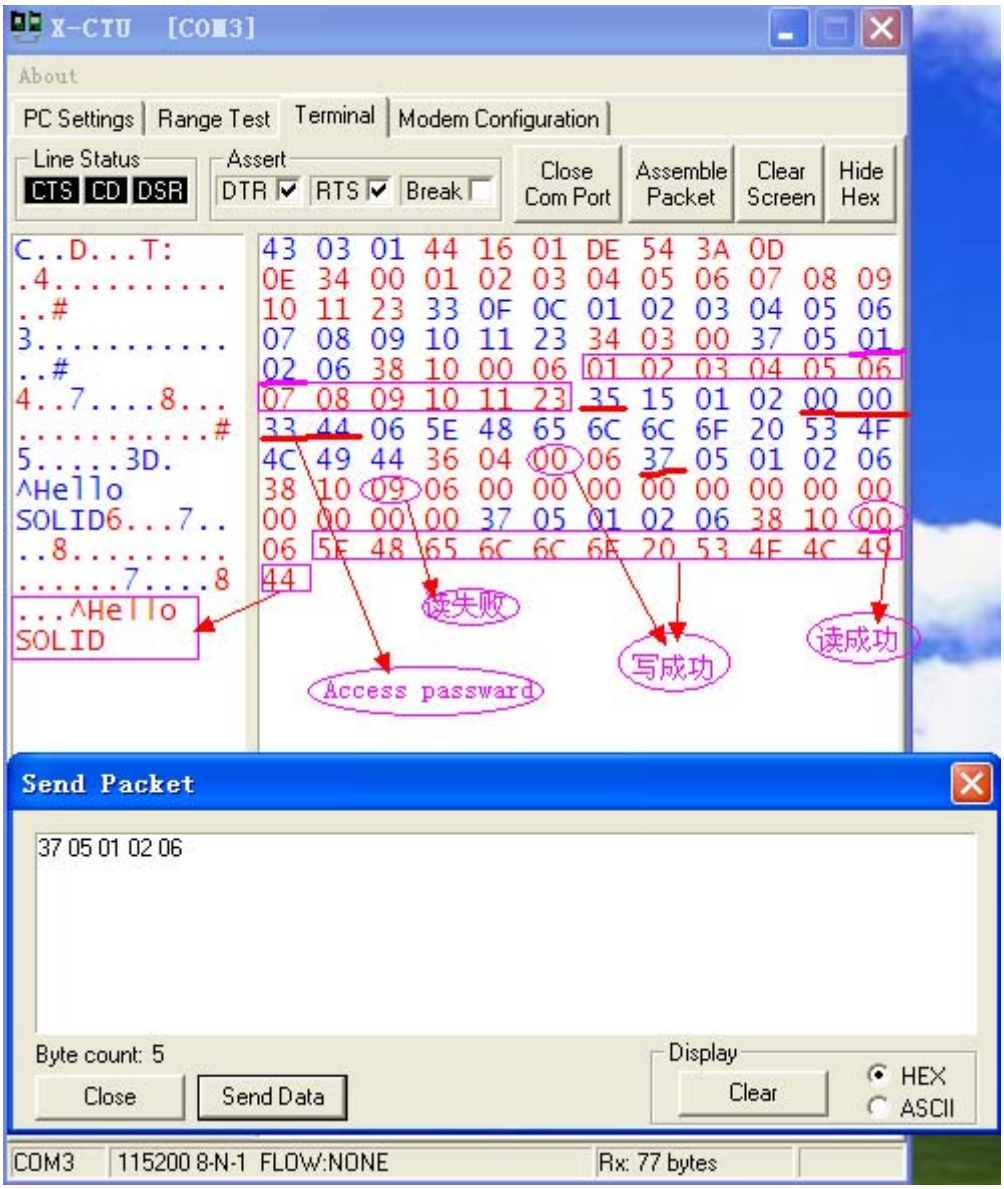
用户通过读该存贮器内容命令读取 EPC 号。

在发行标签时，可通过改写 EPC 编号，使该值在系统中唯一，以标明每个商品的 ID 号。

一般地，EPC 号为 96 位，12 个字节。



修改 EPC，用写标签指令：

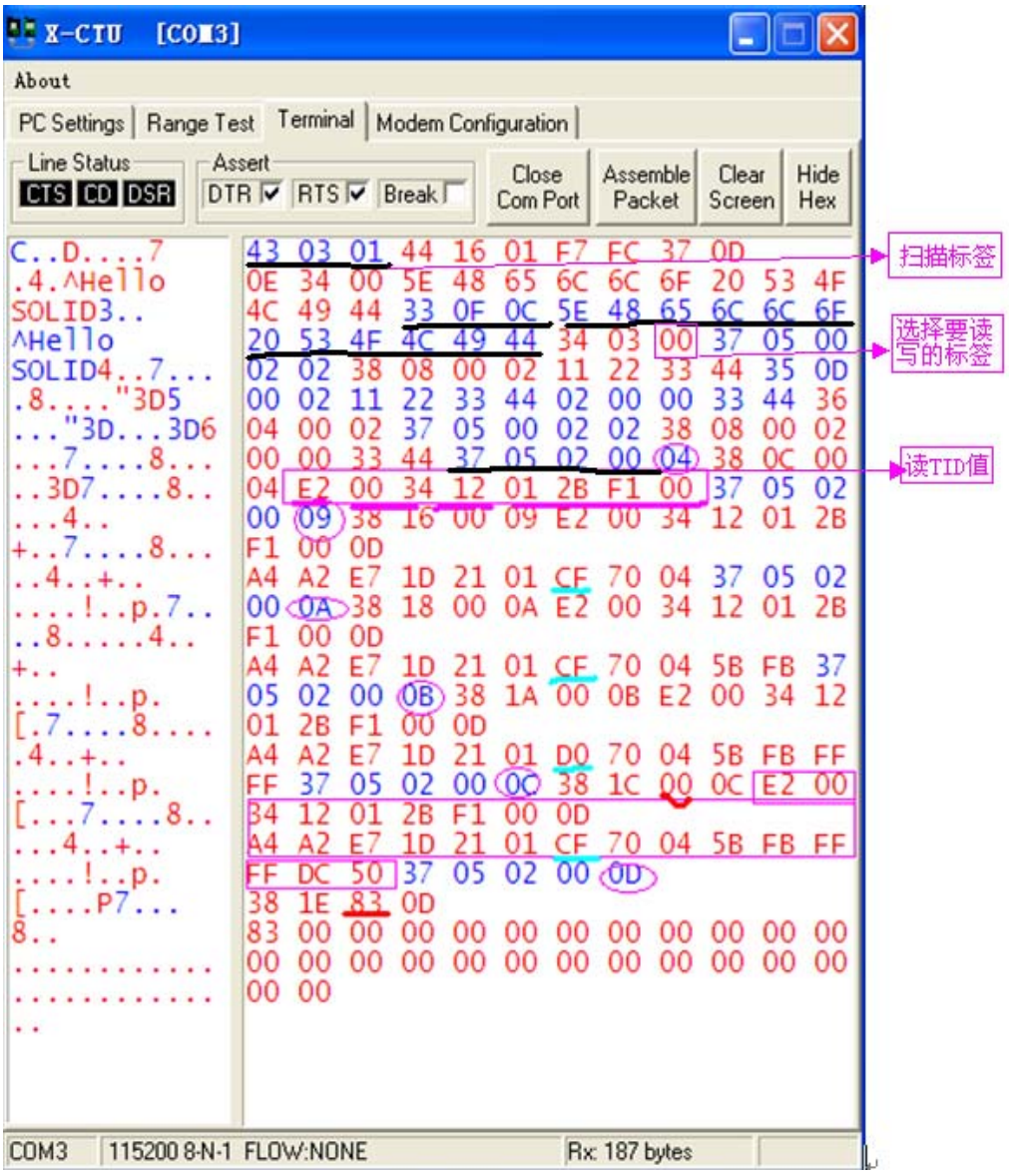


c） TID 存储器 该存贮器是指电子标签的产品类识别号，每个生产厂商的 TID 号都会不同。标签生产厂商会在该存贮区中存贮其自身的产品分类数据及产品供应商的信息。

一般来说，TID 存贮区的长度为 4 个字，8 个字节。但有些电子标签的生产厂商提供的 TID 区会为 2 个字或 5 个字。

该 TID 值在标签出厂时，往往是由厂商写好，用户无法再作修改。

用户在使用时，需根据自己的需要选用相关厂商的产品。



d) 用户存储器 该存贮区用于存贮用户自定义的数据。用户可以对该存贮区进行读、写操作。

该存贮器的长度由各个电子标签的生产厂商确定。每个生产厂商提供的电子标签，其用户存贮区的容量会不同。存贮容量大的电子标签会贵一些。用户应根据自身应用的需要，来选择符合要求的电子标签，以减低标签的成本。

许多电子标签为低成本的，可能会不包括该用户存贮器。

2.2.2 存贮器的操作

在电子标签的应用场合，由电子标签供应商提供的标签为空白标签，用户首先会在电子标签的发行时，通过读写器将相关数据写入到电子标签中（被称为已发行标签）。然后在标签的流通使用过程中，通过读取标签存贮器的相关信息，或将某状态信息写入到电子标签中得以完成数据的交换和传递。

对于电子标签的四个存贮区，读写器提供的存贮命令都能支持对它们的读写操作。但有些电子标签在出厂时就已由供应商设定为只读的，而不能由用户自行改写，这点在选购电子标签时需特别注意。

读写器对电子标签的访问操作，包括轮询标签（循环扫描标签）、唤醒标签、读标签数据、写标签数据、灭活标签、锁定标签、休眠标签等操作。

2.3 一些重要的 EPC 标签的概念说明

用户在实际应用电子标签时，需要对其相关的使用和相关概念，以有效地进行系统的设计及应用。包括如下部份：

1） 标签的存贮结构
2） 标签的工作状态及其转换
3） 标签的操作及命令说明
4） 标签的使用步骤

2.3.1 标签的存贮结构

见《2.2.1 电子标签存贮器》的说明。

2.3.2 电子标签的应用概念及说明

以下描述在使用 EPC G2 电子标签时会遇到的一些重要的概念。用户需详细了解这些概念，完整的说明，请参考《EPC G2 UHF》的国际标准资料或国家标准文档。

2.3.2.1 电子标签的操作命令集

在对于电子标签的操作中，有三组命令集，用于完成对电子标签的访问。这三组命令分别是：选择、盘存及访问，他们分别由一个或多个命令组成。

1） 选择（SELECT）

由一条命令组成。读写器对电子标签的进行访问操作前，需应用选择（SELECT）命令，选择符合用户定义的标签。使符合用户定义的标签进入相应的工作就绪状态，而其他不符合用户定义的标签仍处于非活动状态，这样可有效地先将所有的标签按各自的应用分成几个不同的类，以利于进一步的标签操作命令。

主机——>读写器

字节 0	字节 1	字节 2	字节 3	字节 n+4	字节 n+5…字节 63
帧头 0x33	字节长度	EPC 编号字节长度 n+1	EPC 字节 0	EPC 字节 n	保留位

读写器——>主机

字节 0	字节 1	字节 2
帧头 0x34	字节长度	错误字节

例如，要选中 EPC 为 01 02 03 04 05 06 07 08 09 10 11 23 的标签

发送：33 0F 0C 01 02 03 04 05 06 07 08 09 10 11 23

接收：34 03 09　　表示此标签无法读写

34 03 00　　表示可以读写此标签了（Error byte 为 0x00 表示 No error）

2） 轮询（盘存，INVENTORY）

由多条命令组成。轮询是将所有符合选择（SELECT）条件的标签循环扫描一遍，标签将分别返回其 EPC 号。用户利用该操作可以首先将所有符合条件的标签的 EPC 号读出来。

盘存操作中有许多参数，并且是一个循环的扫描的过程，在一个盘存扫描中，会组合应用到几条不同的盘存命令，故一个盘存又被称为一个盘存周期或轮询周期。我们模块的盘存周期最小为 50ms，轮询间隔时间也可调整。

因为读写器与标签之间对于盘存命令的数据交换的时间响应有严格的要求，故读写器会将一个盘存周期操作设计成一个盘存循环命令，提供给用户使用。而不需要用户去自己设计盘存算法及盘

存步骤。

一般读写器会为各种不同的盘存需求设计几个优化的盘存算法命令，供用户使用。

下面是两种盘存指令：

✧ Command Inventory

主机——>读写器

字节 0	字节 1	字节 2
帧头 0x31	字节长度	开始盘存 0x01

读写器——>主机

字节 0	字节 1	字节 2	字节 3	字节 4…字节 xx	字节 xx+1…字节 63
帧头 0x32	字节长度	找到的标签数目	EPC 字节长度	EPC 1…x	保留位

例如，发送：31 03 01

接收：32 04 00 00 表示未识别到标签

32 12 01 0E 34 00 01 02 03 04 05 06 07 08 09 10 11 23 表示识别到标签，EPC：01 02 03 04 05 06 07 08 09 10 11 23

✧ Command Inventory with RSSI :

主机——>读写器

字节 0	字节 1	字节 2
帧头 0x43	字节长度	开始盘存 0x01

读写器——>主机

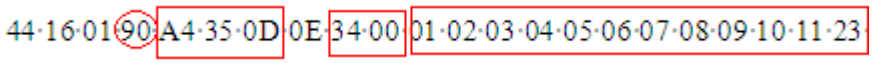
字节 0	字节 1	字节 2	字节 3	字节 4~字节 6	字节 7	字节 8~字节 21
帧头 0x44	字节长度	找到的标签数目	RSSI	工作频率	EPC 和 PC 字节长度	PC+EPC

例如，发送：43 03 01

接收：44 05 00 00 00 表示未识别到标签

44 16 01 90 A4 35 0D 0E 34 00 01 02 03 04 05 06 07 08 09 10 11 23

表示识别到标签，EPC：01 02 03 04 05 06 07 08 09 10 11 23



注：

90——RSSI

A4 35 0D——工作频率 0D<<16 | 35<<08 | A4 = 0xD35A4=865700KHz=865.7MHz（欧洲频率）

34 00——PC，电子标签的协议-控制字

3） 访问操作（ACCESS）

用户使用该组命令完成对电子标签的各个存贮器内容的读取或写入操作。

读写器可对标签进行如下的读写访问：

- .密码校验（即访问标签的保留区:灭活口令和访问口令）
- .读标签

主机——>读写器

字节 0	字节 1	字节 2	字节 3	字节 4	字节 5~8
ID 0x37	字节长度	存贮体	标签内存字地址	数据字长	保留位

读写器——>主机

字节 0	字节 1	字节 2	字节 3	字节 4~n
ID 0x38	字节长度	错误显示	读出数据字长	数据

➢ .写标签

主机——>读写器

字节 0	字节 1	字节 2	字节 3	字节 4~7	字节 8	字节[9]~[9+2*n]
ID 0x35	字节长度	存贮体	标签内存字地址	访问口令	数据字长 n	数据

读写器——>主机

字节 0	字节 1	字节 2	字节 3
ID 0x36	字节长度	错误显示	写入数据字长

➢ .锁定标签

主机——>读写器

字节 0	字节 1	字节 2	字节 3	字节 4~7
ID 0x3B	字节长度	锁定状态	内存区	访问指令

字节 2 的锁定状态选择：

value	Description
0x00	Unlock
0x01	Lock
0x02	Permalock
0x03	Lock&Permalock

锁定的内存区选择-字节 3：

Value	Memory space
0x00	Kill password
0x01	Access password
0x02	EPC
0x03	TID
0x04	User

读写器——>主机

字节 0	字节 1	字节 2
ID 0x3C	字节长度	错误显示

注：被锁定的内存区内容将不可读。

➢ .灭活标签

主机——>读写器

字节 0	字节 1	字节 2~5	字节 6
ID 0x3D	字节长度	灭活指令[0…32]	保留位

读写器——>主机

字节 0	字节 1	字节 2
ID 0x3E	字节长度	错误显示

注：被灭活的标签将废掉，无法使用和再激活。

2.3.2.2 盘存部分的相关概念

本部份将详细描述标签盘存过程中的相关概念,用户在初步使用时,可不需要考虑这些参数,但复杂应用中则需要设定这些参数。我们建议用户在这部份需要详细参考国际标准的相关定义，以免我们在理解时出现问题而误导用户的使用。

2.3.2.2.1 通话（SESSION）和已盘标记（INVENTORIED FLAG）

◆ 通话（SESSION）的概念

电子标签可处于 4 个工作区域下工作，称为 4 个通话（S0，S1，S2，S3），一个标签在一个盘存周期中只能处于其中的一个通话中。例如我们可以用 SELECT 选择命令，使某个应用的标签群进入 S0 通话（我们称之为工作区域），再用另一个 SELECT 选择命令，使另一个应用的标签群进入 S1 通话。这就相当于我们首先将标签群按其不同的应用分在不同的工作区域中。然而我们可以分别在各个的工作区域中，应用盘存命令将标签进行进一步的盘存操作或其他读写操作。

◆ 已盘标记的概念

对于一个标签，当其处于某个通话（工作区域）时，用户可以应用盘存命令对其进行盘存，标签会返回其 EPC 值，并且为其自身设置一个已盘标记。这样对于今后的盘存，如果其参数中与标签的已盘标记不符，标签就不会再响应该盘存命令。这样可以避免一个标签被反复多次盘存。

电子标签的已盘标记值为： A 或 B。

用户在应用 SELECT 命令中，会有一个参数，确定符合选择条件的标签在进入一个通话后，其初始的已盘标记。当一个标签被盘存后，标签会按照用户的盘存命令中的参数要求，更改其已盘标记。

例如，对于一张标签，在应用 SELECT 命令后，其已盘标志为 A，当其被盘存后，其已盘标志变为 B，这样，当下一个盘存命令时，由于该盘存命令是盘存“A”标志的标签，故不会再盘存到该标签。

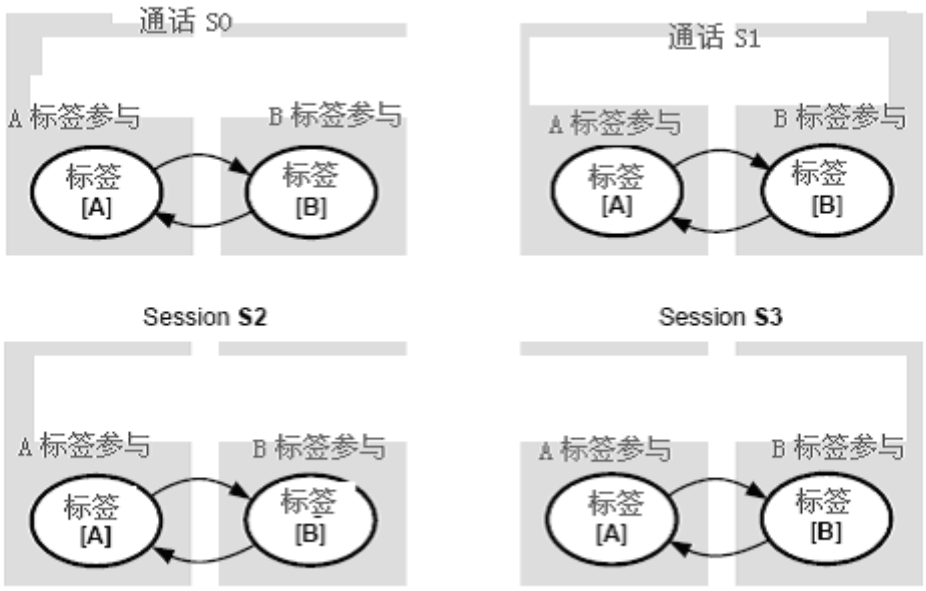
以下举例说明了两个读写器如何利用通话和已盘标记独立交错地盘存共用标签群：

打开读写器#1电源，然后启动一个盘存周期，使通话S2中的标签从A设到B。
关闭电源
打开询问机#2电源，然后
启动一个盘存周期，使通话S3中的标签从B单化为A。
关闭电源

反复操作本过程直至读写器#1 将通话 S2 中的所有标签均盘存到 B，然后，将通话 S2 的标签从 B 盘存为 A。同样，反复操作本过程直至读写器#2 将通话 S3 的所有标签放入 A，然后再将通话 S3 的标签从 A 盘存为 B。通过这种多级程序，各读写器可以独立地将所有标签盘存到它的字段中，无论其已盘标记是否处于初始状态。

- S0 已盘标记应设置为A。
- S1 已盘标记应设置为A或B，视其存储数值而定，如果以前设置的已盘标记比其持续时间要长，则标签应将其S1 已盘标记设置为A打开电源。由于S1已盘标记不是自动刷新，因此可以从B回复到A，即使在标签上电时也可以如此。
- S2 已盘标记应设置为A或B，视其存储的数值而定，若标签断电时间超过其持续时间，则可以将S2 已盘标记设置到A，打开标签。
- S3 已盘标记应设置为A或B，视其存储的数值而定，若标签断电时间超过其持续时间，则

可以将S3已盘标记设置到A，打开标签。



无论初始标记值是多少，标签应能够在 2 毫秒或 2 毫秒以下的时间将其已盘标记设置为 A 或 B。标签应在上电时更新其 S2 和 S3 标记，这意味着每次标签断开电源，其 S2 和 S3 已盘标记的持续时间如图所示。当标签正参与某一盘存周期时，标签不应让其 S1 已盘标记失去其持续性。相反，标签应维持此标记值直至下一个 Query 命令，此时，标记可以不再维持其连续性(除非该标记在盘存周期期间更新，在这种情况下标记应采用新值，并保持新的持续性)。

标签标记和持续值	
标记	应持续时间
S0 已盘标记	通电标签：不确定　　未通电标签：无
S1 已盘标记	通电标签： 标称温度范围：500 毫秒＜持续时间＜5 秒 延长温度范围：未规定 未通电标签： 标称温度范围：500 毫秒＜持续时间＜5 秒 延长温度范围：未规定
S2 已盘标记	通电标签：不确定 未通电标签： 标称温度范围：2 毫秒＜持续时间 延长温度范围：未规定
S3 已盘标记	通电标签：不确定 未通电标签： 标称温度范围：2 毫秒＜持续时间 延长温度范围：未规定

选定(SL)标记	通电标签：不确定 未通电标签： 标称温度范围：2 毫秒＜持续时间 延长温度范围：未规定	

注 1：对于随机选择的足够大的标签群，95%的标签持续时间应符合持续要求，应达到 90%的置信区间。

2.3.2.2.2 选定标记（SL）

标签具有选定标记（SL），读写器可以利用Select命令予以设置或取消。

Query命令中的Sel参数使读写器对具有SL标记或非SL标记（～SL)的标签进行盘存，或者忽略该标记和盘存标签。

SL与任何通话无关，SL适用于所有标签，无论是哪个通话。

标签的 SL 标记的持续时间如表所示。标签应以其被设置的或取消的 SL 标记开启电源，视所存储的具体数值而定，无论标签断电时间是否大于其 SL 标记持续时间。若标签断电时间超过 SL 持续时间，标签应以其被取消确认的 SL 标记开启电源(设置到～SL)。标签应能够在 2 毫秒或 2 毫秒以下的时间内确认或取消确认其 SL 标记，无论其初始标记值如何。打开电源时，标签应刷新其 SL 标记，这意味着每次标签电源断开，其 SL 标记的持续时间均如表 2 所示。

2.4 标签状态及其转换

标签在使用过程中，会根据读写器发出的命令处于不同的工作状态，在各个状态下，可以完成各自不同的操作。即标签只有在相关的工作状态下才能完成相应的操作。标签亦响应读写器命令，使其标签从一个状态转换到下一个工作状态。

标签的工作状态包括：就绪状态
仲裁状态
应答状态
确认状态
开放状态
保护状态
灭活状态

1） 就绪状态

在进入读写器天线有效激励射频场后，任一个未灭活的标签就进入就绪状态。

在此状态下。标签等待选择（SELECT）命令，并按照其参数进入相应的工作区域（SESSION），并设置其初始已盘标记（A、B、SL 或~SL），然后等待进一步的盘存命令，当一个盘存命令中的参数符合当前标签所处在于工作区域（通话）和已盘标记，则匹配的标签就进入了一个盘存周期。标签会从其随机数发生器中抽出 Q 位数(参见槽计数器)，将该数字载入标签的槽计数器内，若该数字不等于 0 时，则标签转换到仲裁状态，若该数字等于零，则标签转换到应答状态。

对于掉电后的标签，当其电源恢复后，亦进入就绪状态。

2） 仲裁状态

在一个盘存周期中，各个标签的槽计数器值是不同的。所有标签会根据当前盘存扫描周期中的命令，完成其计数器的减一（-1）。当某个标签的槽计数器减一后等于零时，该标签就进入应答状态。

而其他的标签则仍然会处于仲裁状态中。通过这种方式就会分别使所有的标签进入应答状态，从而完成对所有标签的更进一步的操作。

3） 应答状态

标签进入应答状态后，标签会向读写器返回（实际上是反向散射，但为叙述简便，我们在今后的描述中会说成是标签的响应或发射）一个16位的随机数RN16。读写器在收到标签返回的RN16后，会向该标签发送一条含有该RN16的ACK命令。若标签收到有效的ACK的命令，则该标签会转换到确认状态，并发射标签自身的PC、EPC和CRC-16值。

若标签未能接收到 ACK，或收到无效 ACK，则应返回仲裁状态。

4） 确认状态

标签进入确认状态后，读写器可以发出访问命令使标签进入以后的开放状态或保护状态。

5） 开放状态

如果该标签的访问口令不等于零，标签在读写器发出访问命令后，会进入开放状态。

在此状态下，读写器需进一步发出访问口令的校验命令，当该命令有效时，标签进入保护状态。

6） 保护状态

如果标签的访问口令等于零，则标签在确认状态下，接收到访口命令后，即进入保护状态。

如果标签的访问口令不等于零，标签在开放状态下，接受到读写器的校验访问口令的命令后，如果该命令有效，则标签进入保护状态。

标签在保护状态下，读写器可以完成对标签的各项访问操作，包括：读标签、写标签、锁定标签和灭活标签等。

7） 灭活状态

标签在开放状态或保护状态下，接受到读写器的灭活标签命令，会使其进入灭活状态。表明该标签已被杀灭，而不能再被使用。

灭活操作具有不可逆性。即一个标签被灭活后即不能再用。

2.5 槽计数器（SLOT COUNTER）

每个标签中都含有一个 15 位的槽计数器，标签在就绪状态下，收到盘存命令后，该盘存命令中含有一个参数 Q，标签会根据该 Q 值，由自身的随机数产生器，产生一个 0--2^Q-1 之间的数值，载入标签的槽计数器。随后，该槽计数器的值会在一个盘存周期中随着盘存命令而减一，当其值为零时，标签就自动进入应答状态。而其他不为零的标签仍然处于仲裁状态中。

2.6 标签随机或伪随机数发生器

标签自身含有一个16位的随机数或伪随机数发生器(RNG)。会产生16位随机数RN16，以作为响应读写器命令中的参数用。

2.7 标签的操作步骤

为简便起见，我们在读写器的设计中，为用户提供的操作命令，是有效地包含了对标签的所有操作。有些命令实际上是对标签操作的几条命令的组合。这样可以更进一减少用户对标签的操作过程的理解。使用户在使用过程更为简单明了。

读写器提供了三大类命令：

1） 盘存标签

2） 唤醒标签/休眠标签

唤醒标签：只使一张标签处于开放状态或保护状态，在此状态下，该标签可以执行进一步的访问操作，而对其他标签的访问无效。

休眠标签：使一张被唤醒的标签处于休眠状态。

在此说明的是：实际上标签在标准规范中并没有休眠状态，而是我们在使用过程中为方便用户的操作，人为地增加了一个唤醒状态，而与其对应地增加了一个休眠状态。

3） 访问标签：包括对标签的读、写、锁定、灭活等操作

在下一节，我们将详细描述读写器对标签的各项操作以及其相关的参数。

2.8 标签的访问命令集

读写器与电子标签之间数据交换是由读写器先发出命令，标签根据自己的状态响应该命令，如该命令有效，标签在执行完该命令后，向读写器反向散射返回数据，并转换到其下一个工作状态。

读写器对标签的操作包括如下三大类命令：

1） 盘存标签（Inventory）

2） 唤醒标签/休眠标签 (Select/Isolate)

唤醒标签：只使一张标签处于开放状态或保护状态，在此状态下，该标签可以执行进一步的访问操作，而对其他标签的访问无效。

休眠标签：使一张被唤醒的标签处于休眠状态。

在此说明的是：实际上标签在使用过程中并没有休眠状态，而是我们在使用过程中为方便用户的操作，人为地增加了一个唤醒状态，而与其对应地增加了一个休眠状态。

3） 访问标签：包括对标签的读、写、锁定、灭活等操作

注： 本章所包括的命令并没有完整的描述《EPC G2 UHF》标准中所含的所有命令集，只是从用户的实用出发，说明了读写器提供给用户的操作命令。实际上，读写器提供给用户操作命令是几个基础命令的组合。因为对标签的基本命令集，用户不需要也不可能直接在读写器的上层来直接完成。

2.8.1 盘存命令

该命令用于启动一个盘存周期，对当前读写器天线有效范围内的标签进行扫描。并将扫描的EPC号全部记录下来。供用户读取。

有关盘存命令的参数包括两个部份：

第一部份为SELECT命令的参数，第二部份为INVENTORY命令的参数，用户可以参照以后部份的轮询命令来理解这些参数的意义。

第一部份的SELECT的参数包括：

目标（TARGET）：值为0—4，分别表示：

0—通话S0
1—通话S1
2—通话S2
3—通话S3
4—选择标记SL

该参数表示应用选择命令后，将使符合用户需要的标签进入哪一个工作区域（通话）中。

动作（ACTION）：值为0—7，分别表示：

标签对动作参数的响应		
动作	匹配	不匹配
0	设 SL 标志或已盘标志→ A	取消 SL 标志或已盘标志→ B
1	设 SL 标志或已盘标志→ A	无作为

10	无作为	取消 SL 标志或已盘标志→ B
11	~SL 标志 or (A → B, B → A)	无作为
100	取消 SL 标志或已盘标志→ B	设 SL 标志或已盘标志→ A
101	取消 SL 标志或已盘标志→ B	无作为
110	无作为	设 SL 标志或已盘标志→ A
111	无作为	~SL 标志或(A → B, B → A)

该参数表明对于被选择的符合条件的标签，设定其已盘标记为A或B或~SL，SL。

存贮体：0-3，分别表示，

0---RFU ； 未用

1---EPC ： EPC存贮体

2---TID ： TID存贮区

3---User ： 用户存贮区

该参数与以下的参数组合在一起，构成一个掩膜值，用于选择符合掩膜值内容的电子标签。

指针： 1个字节

该参数说明掩膜数据是起始地址。以位为单位。

长度：1个字节

该参数说明掩膜数据的数据长度。以位为单位。

掩摸数据：若干字节

该参数表示掩膜数据。

掩膜数据的意义是：

当SELECT命令设置了有效的掩膜值后，表示符合该掩膜值的标签才算是本次选择的有效匹配标签，而其他的标签为未匹配标签。对于有效匹配的标签，则作相应的已盘标记动作（ACTION），并进入SELECT命令中设定的通话（工作区域中）。

对于无效的标签也会按照ACTION参数的要求进入相应的动作和相应的工作区域。

第二部份INVENTORY的命令参数为：

INVENTORY参数：

1） SEL：值为：

0：全部

1：全部

2：~SL

3：SL 该参数与SELECT参数中的“目标”参数相对应，表明本盘存周期只针对相应的选定标签，而对其它标签无效。

2） 通话：值为：

0：S0

1：S1

2：S2

3：S3

该参数与SELECT参数中的“目标”参数相对应，表明本盘存周期只针对相应工作区域的选定标签，而对其它标签无效。

3） 目标：1个字节

0： A

1： B

该参数表明是对于已盘标签为A或B进行盘存。

4） Q值：1个字节

0—15

该参数表明盘存命令的Q值，其解释参见《2.4 槽计数器》的说明。

5） 盘存算法：

对于各种不同的盘存需要，一般读写器会提供用户几种不同的盘存算法，供用户在不同的盘存情况下使用，用户可以根据自己的要求选择相应的算法，以达到效率最高。

6） 盘存次数

该参数表明在一个盘存周期中执行几次的盘存命令。

2.8.2 唤醒标签/休眠标签

唤醒标签用于使一张符合条件的标签处于开放状态或保护状态下，从而用户可以对该标签作进一步的访问操作。

唤醒命令的参数定义与盘存命令中的SELECT部份命令相同。请参考上一节的说明。

休眠标签：使原被唤醒的标签返回到仲裁状态。

2.8.3 访问命令

本命令集用于对已被唤醒的标签进行进一步的读、写操作。本部份的操作只对已被唤醒的标签有效。

访问命令集包括如下命令：

1） 设置访问口令、灭活口令
2） 校验访问口令
3） 读标签数据
4） 写标签数据
5） 锁定标签数据
6） 灭活标签
7） 块写入数据
8） 块擦除数据

2.8.3.1 设置访问口令、灭活口令

该命令用于将32位的访问口令以及32位的灭活口令设置在读写器中，以用于今后对标签进行进一步的校验和灭活操作。

访问口令：4个字节

灭活口令：4个字节

2.8.3.2 校验访问口令

该命令用于对某个已被唤醒的标签进行访问口令的校验，如果校验正确，标签会进入保护状态，读写器则进一步对标签进行读、写等操作。

2.8.3.3 读操作

本命令用于读取标签的某个存贮块的数据。

其中参数包括：

存贮体：

0—保留内存
1—EPC存贮体
2—TID存贮体
3—用户自定义存贮体

该参数表明待读取的标签存贮器。
字指针： 该参数表明待读取的起始地址
字计数： 该参数表明待读取的标签的数据字的大小。
注意： 该参数是以字为单位（2个字节）。
对于标签成功地执行完该命令后，会将相关数据返回到读写器中。
在此需特别说明的是：如果以上参数指定的数据块不存在、字指针或字计数越界，都会返回错误信息。

2.8.3.4 写标签命令

本命令用于将某个字的数据写入到标签中。
其中的参数包括：
存贮体：
0—保留内存
1—EPC存贮体
2—TID存贮体
3—用户自定义存贮体
该参数表明待写入数据的标签存贮体。
字指针： 该参数表明待写入的起始地址
字计数： 该参数表明待写入的标签的数据字的大小。
注意： 该参数是以字为单位（2个字节）。
数据：待写入的数据组。

2.8.3.5 锁定命令

该命令用于将标签的各个存贮器的读/写控制位进行锁定。对于已被锁定的标签，则只有在符合锁定状态的条件下，其相应存贮器内容才能被访问，否则会提示出错。
对于锁定，共分为5个存贮区：访问密码、灭活密码、EPC区、TID区、USER区。
其中：访问密码、灭活密码可以设置“读/写控制”位及“永久锁定控制”位。
EPC区、TID区、USER区可以设置为“写控制”位及“永久控制”位。
即对于每个区，我们设定了二个锁定操作，一个是“读/写锁定（写锁定）”，另一个是“永久锁定”。
对于“读/写锁定（写锁定）”可以解除锁定。

Lock 动作—字段功能		
写入口令	永久锁定	描述
0	0	在开放状态或保护状态下可以写入相关存储体。
0	1	在开放状态或保护状态可以永久写入相关存储体，或者可以永远不锁定相关存储体。
1	0	在保护状态下可以写入相关存储体但在开放状态下不行。
1	1	在任何状态下都不可以写入相关存储体。
读取、写入口令	永久锁定	描述
0	0	在开放状态或保护状态下可以读取和写入相关口令位置。
0	1	在开放状态或保护状态下可以永久读取和写入相关口令位置，并可以永远不锁定相关口令位置。
1	0	在保护状态下可以读取和写入相关口令位置但在开放状态下不行。

1	1	在任何状态下都不可以读取或写入相关口令位置。

2.8.3.6 灭活标签

本操作命令将灭活标签，使符合条件的标签不再可用。

在执行灭活命令前，必须先将灭活口令设置到读写器中。

2.8.3.7 块数据输入

本命令是将一个数据块一次性写入到标签中。

其中的参数包括：

存贮体：

0—保留内存

1—EPC存贮体

2—TID存贮体

3—用户自定义存贮体

该参数表明待写入的标签存贮体。

字指针： 该参数表明待写入的标签的起始地址

字计数：1个字节 该参数表明待写入的标签的数据字的大小。

注意： 该参数是以字为单位（2个字节）。

数据：待写入的数据组。

2.8.3.8 块数据擦除

本命令用于一次性擦除标签中的某个数据块。

其参数的定义是：

存贮体：

0—保留内存

1—EPC存贮体

2—TID存贮体

3—用户自定义存贮体

该参数表明待擦除的标签存贮体。

字指针：1个字节 该参数表明待擦除的标签的起始地址

字计数：1个字节 该参数表明待擦除的标签的数据字的数目。

注意： 该参数是以字为单位（2个字节）。

2.9 标签的返回错误码

对标签的访问操作，如果命令码不正确或其他一些错误出现，标签将无法有效地执行相关的操作，标签会返回出错信息，用户可以利用这些信息判别出错的原因：

标签错误代码			
错误代码支持	错误代码	错误代码名称	错误描述
特定错误代码	1000 0000	其它错误	全部捕捉未被其它代码覆盖的错误
	11	存储器超限或不被支持的 PC 值	规定存储位置不存在或标签不支持 PC 值
	100	存储器锁定	规定存储位置锁定和/或永久锁定，且不可写入。

	1011	电源不足	标签电源不足，无法执行存储写入操作
非特定错误代码	1111	非特定错误	标签不支持特定错误代码

第三章 AS399x读写模块操作命令集

AS399x读写模块/读写器是一种被动式的工作方式，即它接收由用户发出的操作命令，并执行。最后将执行的结果返回给操作者。

AS399x读写模块/读写器是采用USB通信方式与PC机或用户的主控机进行通信的，RFID系列读写模块提供了多种与用户系统的通信方式，以方便用户构成自己的系统。

AS399x读写模块/读写器提供用户完整地对标签的操作命令，主要包括如下三个部分：

1） 读写器参数设定命令：完成对读写器工作参数的设定，
包括：工作频率、接收灵敏度、盘存周期、GEN2参数设置。

2） 标签操作的基础指令集：提供与国际标准相一致的对标签操作的基础指令集，
包括：轮询标签、密码校验、读标签、写标签、锁定标签及灭活标签等。

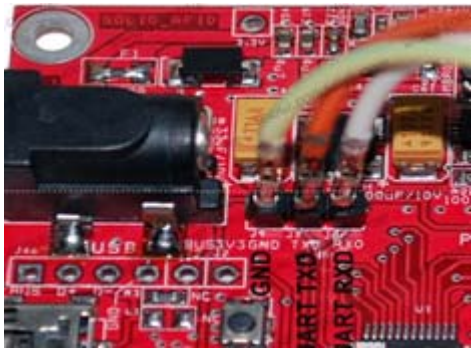
3） 标签操作的高级指令集：为进一步方便用户的操作，我们在基础指令集的基础上，提供了对标签操作的高级指令级，它的每条命令是由几条基础指令集组合而成，用户应用这些命令会使操作更为简明。
包括：读标签、写标签、锁定标签及灭活标签。

本章将详细述RFID读写模块与用户主系统的连接方式，RFID读写器与PC机的通信以及各个命令的相关内容。

3.1 通信接口定义

AS399x读写模块有二个外部接口，分别提供与外部主机的通信接口和外部输入/输出信号（I/O）。其接口定义为：

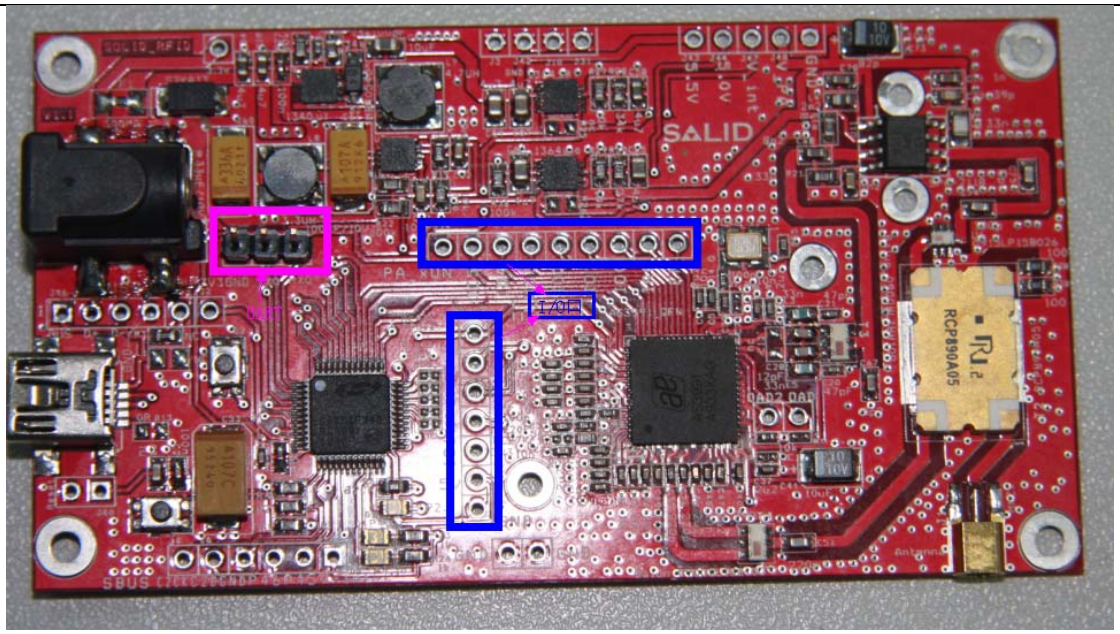
CN1：外部的通信接口（TTL UART）



J9——GND J7——TX0 J8——RX0

CN2：外部输入/输出信号接口（I/O接口）

RFID读写模块一组输入输出引脚，用户可以应用这些外部的输入输出接口来完成对外部设备的控制，或者由外部的MCU来控制AS399x芯片工作。



使能引脚：EN
中断信号引脚：IRQ
时钟信号引脚：CLK
数据输入输出引脚：IO0—IO7
电源引脚：3V3、5V、GND

3.2 通信方式

RFID读写模块可根据用户的需要设置成不同的与主机通信模式，用户在订货时需说明自己需要的通信方式，我们会按你的要求生产相应的模块。否则，您需要自己烧写我们提供的固件，以满足你的通信要求。

我们的RFID读写模块提供两种通信协议：

- TTL电平UART通信协议
- USB通信协议

所提供的通信波特率有：115200dps, 9600dps

3.3 通信命令格式

主机与AS399x读写模块的通信模式是主动式，即由主机向RFID读写器/模块发出命令，读写器/模块执行完该命令后将相关的结果或数据返回到主机中。

主机与RFID读写模块之间的通信数据是以字节为单位来传送的。每条命令由多个字节组成。

3.3.1 通信命令的格式

主机向AS399x读写模块发送的命令与读写器返回的数据格式是相同的：

命令体包括：命令码+命令字节长度+命令数据

返回数据的命令码是对发送数据命令码的回答。

3.4 RFID读写模块的操作指令集

AS399x读写模块提供了对RFID标签的完整的操作命令，这些命令可以通过RFID模块与用户主控方

之间的通信，由主控方发出，完成用户对RFID标签的操作。

读写器提供的操作命令分为两个部分：

✧ 读写器系统参数设置命令：提供了对RFID读写器/模块的系统参数进行设置。

✧ RFID标签访问命令集：提供对电子标签的轮询和访问命令集。

以下详细描述各个命令的功能及命令格式。

3.4.1 读写器/模块系统参数设置命令集

3.4.1.1 读取读写器的固件版本和硬件版本号（ID）

功能说明：本命令用于将读写模块的固件和硬件ID号读出，也可用来检测RFID模块与主控机是否通信正常。

发送命令：

命令码：0x10

命令字节长度：0x03

命令数据：0x00——Firmware/0x01——Hardware

返回数据：

命令码：0x11

命令字节长度：0x23

得到的数据：String

例. Software version indentify command

Send: 10 03 00

Receive: 11 23 41 53 33 39 39 31 20 4D 69 6E 69 20 52 65 61 64 65 72 20 46 69 72 6D 77 61 72 65 20 31 2E 35 2E 31（ASCII码显示） (select the Show Hex)

Or receive: 0x11_AS3991 Mini Reader Firmware 1.5.1 (not select the Show Hex)

Hardware version indentify command

Send: 10 03 01

Receive: 11 22 41 53 33 39 39 31 20 52 4F 47 45 52 20 52 65 61 64 65 72 20 48 61 72 64 77 61 72 65 20 31 2E 32（ASCII码显示）

Or receive: 0x11_AS3991 ROGER Reader Hardware 1.2

3.4.1.2 天线功率开关命令

功能说明：开、关天线功率，关掉后读写模块将不能读写。

发送命令：

命令码：0x18

命令字节长度：0x03

命令数据：天线功率选择字节

字节 3 的值	天线功率
0x00	关功率
0x01 – 0xFE	保留，用于在其他版本中改变天线功率大小
0xFF	开功率

注：保留处在此命令中不起作用，改变功率大小要在寄存器中设置。

返回数据：

命令码：0x19

命令字节长度：0x03

得到数据：0x00

例. Send: 18 03 00

Receive: 19 03 00

此时读写器将不能读写标签。

3.4.1.3 写AS399x寄存器命令

功能说明：直接操作AS399x寄存器。

发送命令：

命令码：0x1A

命令字节长度：0x04/0x05/0x06

寄存器地址：（查看AS399x datasheet）

写入的数据：1/2/3个字节

返回数据：

命令码：0x1B

命令字节长度：0x03

错误提示字节：0x00表示写入正确，其他返回值见错误字节表

例. Send: 1A 04 08 00

Receive: 1B 03 00 No error

RX Wait Time (08)

Bit	Signal Name	Function	Comments
B7	Rxw7	RX wait time	Defines the time during which the RX input is ignored. It starts from the end of TX. RX wait range is 6.4µs to 1632µs (1..255), Step size 6.4µs, 00: receiver enabled immediately after TX. ISO 1800-6C(Gen2) Gen2: T1min=11.28µs…262us, ISO 1800 - 6A: 150…1150µs ISO 1800 - 6B: 85…460µs
B6	Rxw6		
B5	Rxw5		
B4	Rxw4		
B3	Rxw3		
B2	Rxw2		
B1	Rxw1		
B0	Rxw0		

1. Defines the time after TX when the RX input is disregarded.

Notes:

1. Preset at por=H or EN=L and at each write to 'Protocol control' register
2. Gen2: 07(44.8µs < 54.25µs…84.5µs – LF:160kHz)

3.4.1.4 读AS399x寄存器值命令

功能说明：直接读取AS399x寄存器值

发送命令：

命令码：0x1C

命令字节长度：0x03

寄存器地址:

返回数据：

命令码：0x1D

命令字节长度：0x06
读取的数据：Data

例. Read the RX Wait Time register,

Send: 1C 03 08 Receive: 1D 06 00 00 00 00
Write to it,
Send: 1A 04 08 07 Receive: 1B 03 00
Read again,
Send: 1C 03 08 Receive: 1D 06 07 00 00 00

3.4.1.5 改变读写器工作频率命令

功能说明：改变读写器的工作频率、得到发射功率值或者RSSI值

发送命令：

命令码：0x41
命令字节长度：0x07/0x08
选择项：MASK（见下面）
频率地位字节（单位：KHz）
频率中位字节
频率高位字节
RSSI值(单位：dBm)

Mask 0x01: RSSI值扫描
Mask 0x02: 反射功率扫描
Mask 0x04: 开跳跃模式; - 增加频率值到频率单上
Mask 0x08: 关跳跃模式，删除频率单上的频率
Mask 0x10: 设置LBT参数,用于跳跃模式

Byte 0/ID	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8
0x41	Frame length	0x10	listening Time low	listening Time high	max SendingTime low	max SendingTime high	idle Time low	idle Time high

不同的MASK选择，返回数据也不一样。
最常用的是开、关跳跃模式，设置读写器工作频率
不同国家的读写器频率标准见下表：

Profile	Start freq [khz]	End freq [khz]	Increment [khz]	RSSI Threshold [dBm]	Listen Time [ms]	Idle Time [ms]	Max. Allocation [ms]
Europe	865,700 0x0d35a4	867,500 0x0d3cac	600 0x0258	-40 0xd8	1	0	10000
Japan	952,400	952,600	200	-87	10	100	4000
USA	902,750 0x0dc65e	927,250 0x0e2612	500 0x01f4	-40 0xd8	1	0	400

China 920.625	920,625	924,375	750	-40	1	0	10000
China 840.125	840,125	844,875	250	-40	1	0	10000
Korea	917,300	920,300	600	-40	1	0	10000

我们的读写模块默认的是欧洲频率标准，有4个频点，

865700 khz	866300 khz	866900 khz	867500 khz
0x0d35a4	0x0d37fc	0x0d3a54	0x0d3cac

例. Send: 41 08 08 AC 3C 0D D8 01

Receive: 42 40 FE FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Value	Meaning
0x41	命令码
0x08	字节长度
0x08	关跳跃模式并清除频率单
0xAC 0x3C 0x0D	设置成 867.5Mhz 工作频率
0xD8	RSSI 阈值-40 dBm
0x01	Profile No.

注：此命令设置后，读写模块/器将工作在所设置的单一频率下。

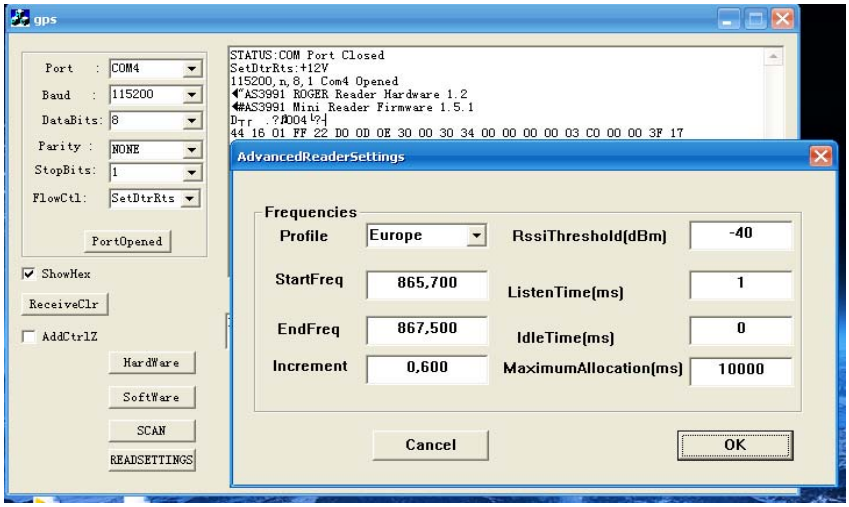
Send: 41 08 04 54 3A 0D D8 01

Receive: 42 40 FC FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

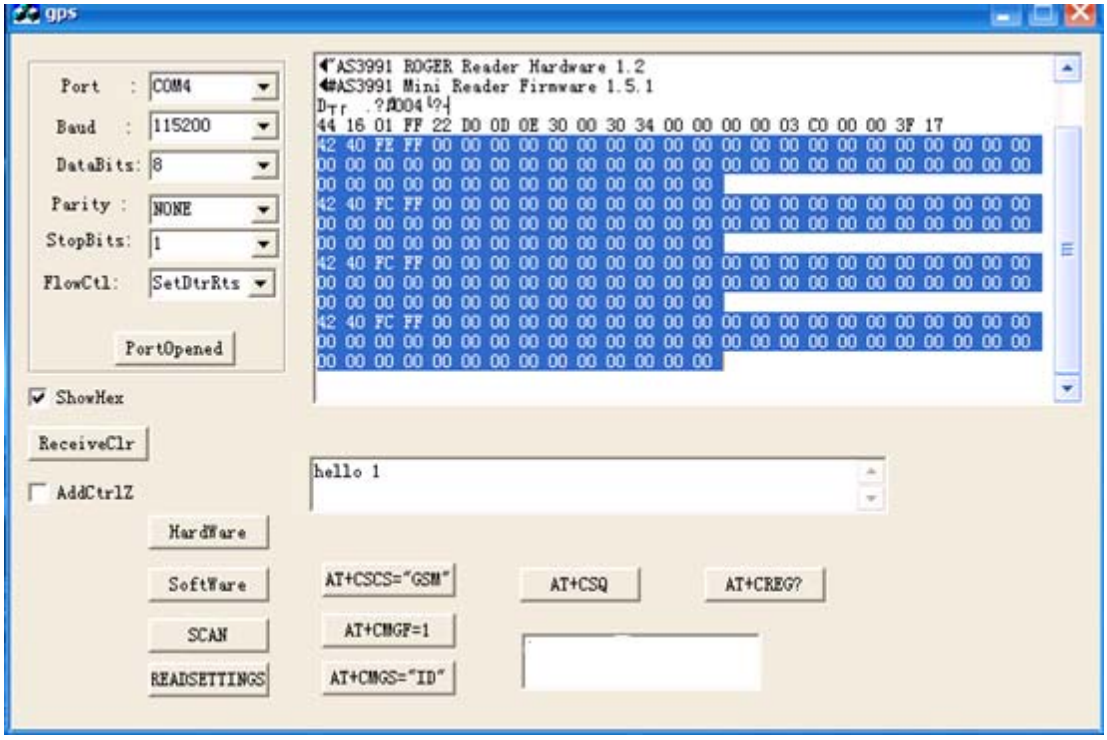
Value	Meaning
0x41	命令码
0x08	字节长度
0x04	开跳跃模式，增加频率值
0x54 0x3A 0x0D	你在频率单上增加的频率值,866.9Mhz
0xD8	RSSI Level,-40 dBm
0x01	相当于频率单号
0x42	对命令码 0x41 的回答
0xFE	关跳跃模式的返回值
0XFC	开跳跃模式的返回值

注：在这个命令后，读写器将工作在跳跃模式，如现在以867.5Mhz和866.9Mhz频点工作，重复切换。当然你可以用上面第二个开跳跃模式指令继续添加频率值。不过要在国家标准内。

你也可以使用我们做的上位机软件来设置，



如，设置成欧洲频率，即有4个频点，返回数据就有四组，见下图



设置成美国（USA）频率，就会有50个频点，即50组返回值。

3.4.1.6 设置GEN2参数

功能说明：设置 GEN2 相关参数

发送命令：

命令码：0x59

命令字节长度：按实际需要

需要设置的参数：字节地址+设置值

链接频率（linkfrequency）

盘存算法选择（miller）

通话区域选择（session）

Pilot tone（trext）
初始可用槽数值 2^q（qbegin）

参数选择可有如下：

- • linkfrequency: 0=40kHz, 3=80kHZ, 6=160kHz,8=213kHz,9=256kHz,12=320kHz,15=640kHz
- miller: 0=FM0, 2=Miller2, 2=Miller4, 3=Miller8
- session: 0=S0, 1= S1, 2=S2, 3=S3, 4=S4
- • trext: 1 use long pilot tone, 0: don’t
- qbegin: Start value for q when doing inventory rounds. The first round will have 2^q slots

此命令执行后将返回所有设置的值。

3.4.1.7 AS399x 寄存器值

功能说明：读取 AS399x 所有寄存器的现值

发送命令：

命令码：0x57

命令字节长度：0x02

例. Send: 57 02

Receive: 58 2D 02 06 F0 62 35 05 00 07 07 01 08 02 00 37 0B 10 98 02 0C 40 00 38 83 84 0A 06 3F 20 06 41 E4 46 18 01 00 87 00 00 00 00 00 00 00

3.4.2 RFID 读写模块/器的标签操作的基础命令集

这部分命令完成微处理器和标签之间的通信，因此需要天线输出功率使能，天线的读写区域内至少有 1 个标签。

读写器与电子标签之间数据交换是由读写器先发出命令，标签根据自己的状态响应该命令，如该命令有效，标签在执行完该命令后，向读写器反向散射返回数据，并转换到其下一个工作状态。

读写器对标签的操作包括如下三大类命令：

1） 盘存标签

2） 唤醒标签/休眠标签

唤醒标签：只使一张标签处于开放状态或保护状态，在此状态下，该标签可以执行进一步的访问操作，而对其他标签的访问无效。

休眠标签：使一张被唤醒的标签处于休眠状态。

在此说明的是：实际上标签在使用过程中并没有休眠状态，而是我们在使用过程中为方便用户的操作，人为地增加了一个唤醒状态，而与其对应地增加了一个休眠状态。

3） 访问标签：包括对标签的读、写、锁定、灭活等操作。

注： 本章所包括的命令并没有完整的描述《EPC Gen-2》标准中所含的所有命令集，只是从用户的实用出发，说明了读写器提供给用户的操作命令。实际上，读写器提供给用户操作命令是几个基础命令的组合。因为对标签的基本命令集，用户不需要也不可能直接在读写器的上层来直接完成。

3.4.2.1 盘存命令

功能说明：该命令用于启动一个盘存周期，对当前读写器天线有效范围内的标签进行扫描，并将扫描的 EPC 号全部记录下来，供用户读取。

发送命令：

命令码：0x31
命令字节长度：0x03
开始新的一轮盘存：0x01
返回数据：
回复命令码：0x32
返回数据字节长度：0x12
还未读到的标签数，即还需调用盘存命令的次数：
PC 和 EPC 的字节长度：0x0E
EPC 数据
注：每发送盘存命令后，读取一个标签 EPC，字节 2 显示了要得到所有已识别到的标签信息还要调用几次盘存命令。在这个过程中盘存的标签信息是不会被删除的。一个完整的命令长度是 64 字节，用 USB 口通信时会发现返回数据均是 64 字节的。
例. Send: 31 03 01
Receive: 32 12 01 0E 30 00 01 02 03 04 05 06 07 08 09 10 6A 0F

Value	Meaning
0x32	回应 0x31
0x12	返回数据字节长度,0x12=18
0x01	识别到一个标签
0x0E	PC+EPC 字节长度
0X30 0X00	PC
0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x6A 0x0F	EPC

3.4.2.2 带有 RSSI 值的盘存命令
功能说明：该命令用于启动一个盘存周期，对当前读写器天线有效范围内的标签进行扫描，并将扫描的 RSSI 值、工作频率和 EPC 号全部记录下来，供用户读取。读写标签存贮体时需要首先执行这个命令，否则会读写不成功。
发送命令：
命令码：0x43
命令字节长度：0x03
开始新的一轮盘存周期
返回数据：
回应命令码 0x43：0x44
返回数据字节长度：
还需调用盘存命令的次数
RSSI 值
这一时刻的工作频率
PC 和 EPC 字节长度

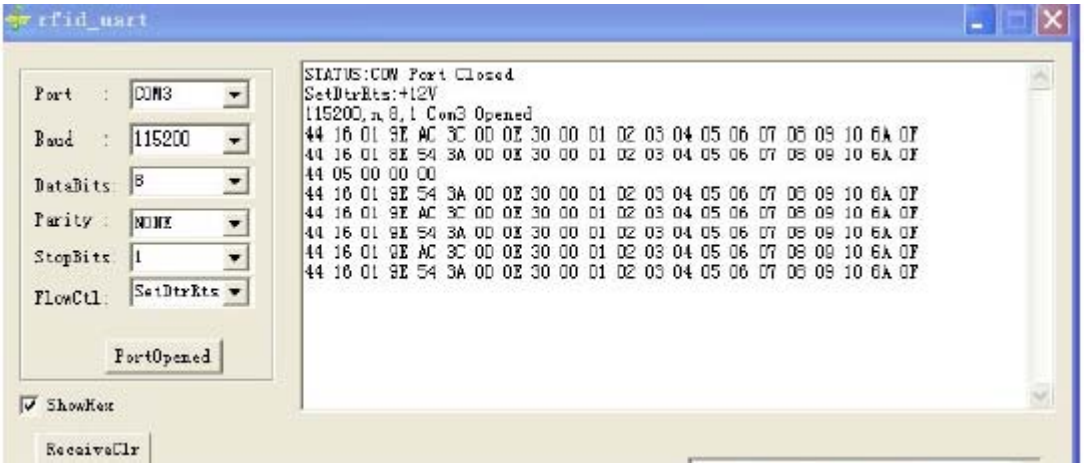
PC 和 EPC 数据

例. Send: 43 03 01

Receive: 44 16 01 9E AC 3C 0D 0E 30 00 01 02 03 04 05 06 07 08 09 10 6A 0F

Value	Meaning
0x44	回应 0x43
0x16	字节长度
0x01	标签数
0x9E	代表 Q 和 I 值; Signal strength of signal Q =(0x9E>>4)*2=18 Signal strength of signal I =(0x9E&0x0F)*2=28
0xAC 0x3C 0x0D	频率 866900kz，可由下计算得 0D<<16 | 3C<<8 | AC = 0x0D3CAC=867500kz=867.5M=865.7+0.6+0.6+0.6M; 这是欧洲标准频率; 例如，欧洲频率表单: Europe,865.7,867.5,0.6,-40,1,0,10000
0x0E	PC 和 EPC 字节数
0x30 0x00	PC
0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x6A 0x0F	EPC

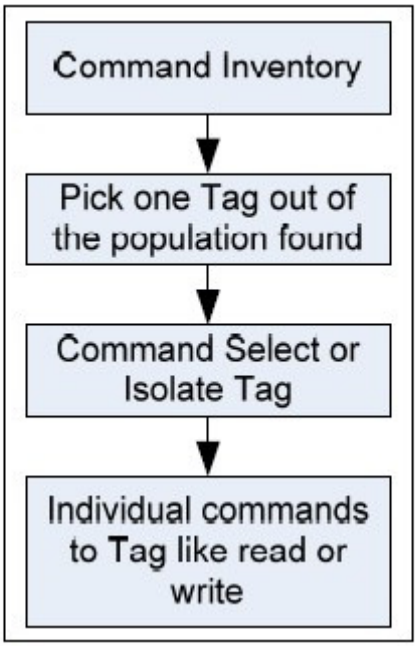
下图工具上的 SCAN 按键等同于这个命令，



3.4.2.3 选择标签

功能说明：读写器对电子标签的进行访问操作前，需应用选择（SELECT）命令，选择符合用户定义的标签。使符合用户定义的标签进入相应的工作就绪状态，而其他不符合用户定义的标签仍处于非活动状态，这样可有效地先将所有的标签按各自的应用分成几个不同的
类。以利于进一步的标签操作命令。

正确的操作顺序如下：



主机需要发送完整的EPC给读写模块控制器，不管EPC多长，来确保工作正常。完整的命令字节长度是64字节，在上位机软件中需要注意。

发送命令：

命令码：0x33

命令字节长度：

EPC字节长度：

EPC数据

例. Send: 33 0F 0C 01 02 03 04 05 06 07 08 09 10 6A 0F

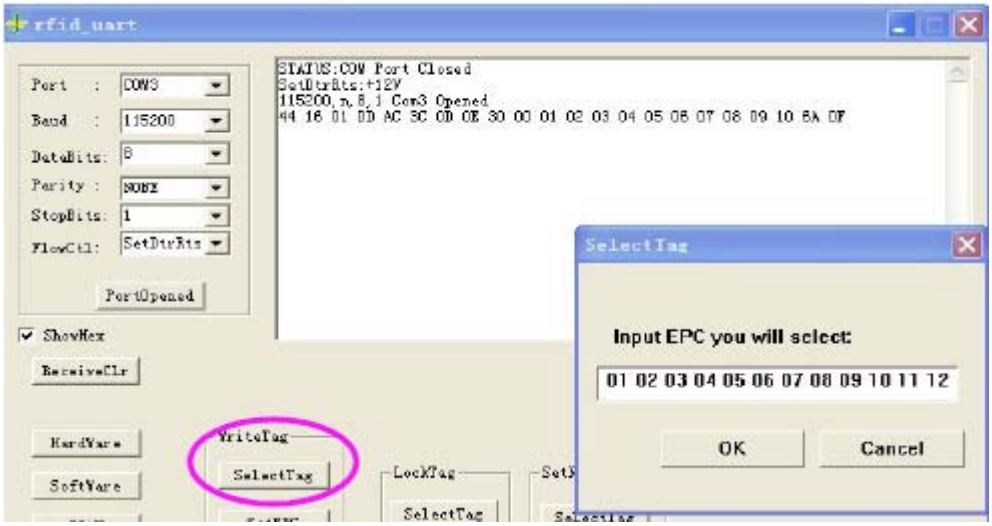
Receive: 34 03 00

选中标签 - 01 02 03 04 05 06 07 08 09 10 6A 0F

If receive: 34 03 09

未找到标签。.

下面软件工具上“SelectTag”按键如此命令:



3.4.2.4 写标签数据

功能说明：本命令是将一个数据块一次性写入到标签中。

建议用户在使用时，先应用轮询标签命令读取所有的EPC号，然后应用选择标签命令指定EPC号，然后完成对特定标签的读写。

其中的参数包括：

存贮体：

0—保留内存

1—EPC存贮体

2—TID存贮体

3—用户自定义存贮体

该参数表明待写入的标签存贮体。

字指针： 该参数表明待写入的标签的起始地址

访问口令：4个字节

字计数：1个字节，该参数表明待写入的标签的数据字的大小。

注意： 该参数是以字为单位（2 个字节）。

数据：待写入的数据组。

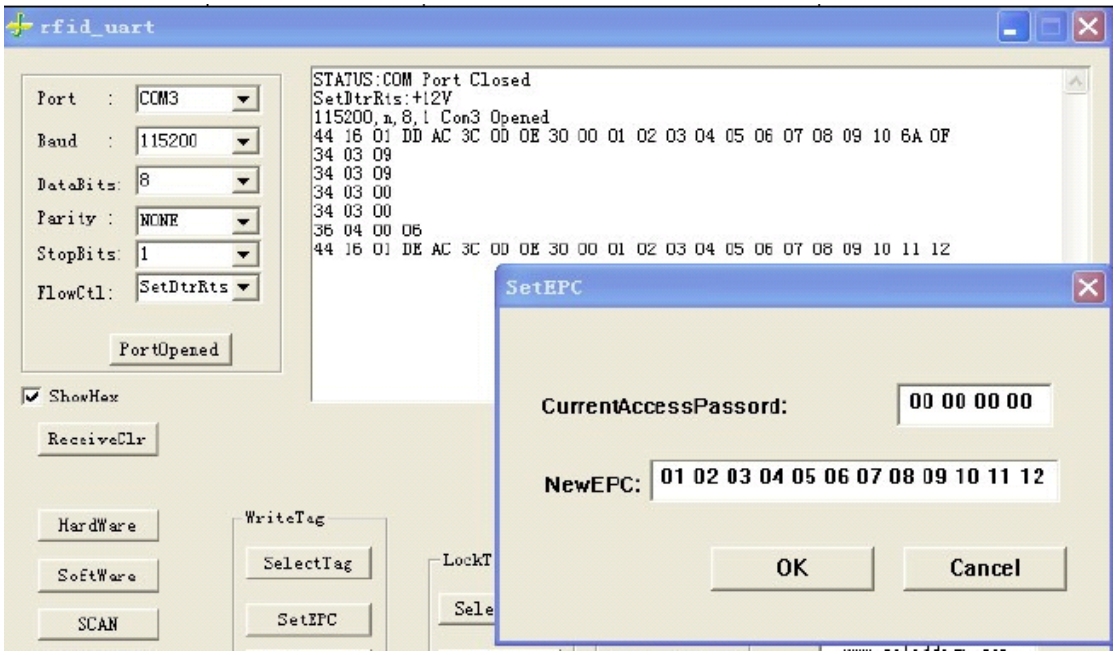
例. Send: 35 15 01 02 00 00 00 00 06 01 02 03 04 05 06 07 08 09 10 11 12

Receive: 36 04 00 06 表示写入成功，字节3是错误码字节

注：对标签的访问操作，如果命令码不正确或其他一些错误出现，标签将无法有效地执行相关的操作，标签会返回出错信息，用户可以利用这些信息判别出错的原因：

标签错误代码

错误代码支持	错误代码（二进制）	错误代码名称	错误描述
特定错误代码	1000 0000	其它错误	全部捕捉未被其它代码覆盖的错误
	1000 0011	存储器超限或不被支持的 PC 值	规定存储位置不存在或标签不支持 PC 值
	1000 0100	存储器锁定	规定存储位置锁定和/或永久锁定，且不可写入。
	1000 1011	电源不足	标签电源不足，无法执行存储写入操作
非特定错误代码	1000 1111	非特定错误	标签不支持特定错误代码



通过此命令也可以设置访问口令和灭后口令，该命令用于将32位的访问口令以及32位的灭活口令设置在读写器中，以用于今后对标签进行进一步的校验和灭活操作。

访问口令：4个字节

灭活口令：4个字节

3.4.2.5 读标签命令

功能说明：本命令用于读取标签的某个存贮块的数据。

建议用户在使用时，先应用轮询标签命令读取所有的EPC号，然后应用选择标签命令指定EPC号，然后完成对特定标签的读写。

其中参数包括：

存贮体：

0—保留内存

1—EPC存贮体
2—TID存贮体
3—用户自定义存贮体

该参数表明待读取的标签存贮器。

字指针：
该参数表明待读取的起始地址
字计数：
该参数表明待读取的标签的数据字的大小。
注意： 该参数是以字为单位（2个字节）。

对于标签成功地执行完该命令后，会将相关数据返回到读写器中。

在此需特别说明的是：如果以上参数指定的数据块不存在、字指针或字计数越界，都会返回错误信息。

例. Send: 37 05 01 02 06
Receive: 38 10 00 06 01 02 03 04 05 06 07 08 09 10 11 12

3.4.2.6 锁定命令

功能说明：该命令用于将标签的各个存贮器的读/写控制位进行锁定。对于已被锁定的标签，则只有在符合锁定状态的条件下，其相应存贮器内容才能被访问，否则会提示出错。

对于锁定，共分为5个存贮区：访问密码、灭活密码、EPC区、TID区、USER区。

建议用户在使用时，先应用轮询标签命令读取所有的EPC号，然后应用选择标签命令指定EPC号，然后完成对特定标签的锁定。

其中：访问密码、灭活密码可以设置“读/写控制”位及“永久锁定控制”位。EPC区、TID区、USER区可以设置为“写控制”位及“永久控制”位。即对于每个区，我们设定了二个锁定操作，一个是“读/写锁定（写锁定）”，另一个是“永久锁定”。对于“读/写锁定（写锁定）”可以解除锁定。

Lock 动作—字段功能		
写入口令	永久锁定	描述
0	0	在开放状态或保护状态下可以写入相关存储体。
0	1	在开放状态或保护状态可以永久写入相关存储体，或者可以永远不锁定相关存储体。
1	0	在保护状态下可以写入相关存储体但在开放状态下不行。
1	1	在任何状态下都不可以写入相关存储体。
读取、写入口令	永久锁定	描述
0	0	在开放状态或保护状态下可以读取和写入相关口令位置。
0	1	在开放状态或保护状态下可以永久读取和写入相关口令位置，并可以永远不锁定相关口令位置。
1	0	在保护状态下可以读取和写入相关口令位置但在开放状态下不行。
1	1	在任何状态下都不可以读取或写入相关口令位置。

发送命令：

命令码：0x3B

命令字节长度：0x08

选项：锁定/不锁定

内存区选择：

访问口令：4个字节

字节 2 的锁定状态选择：

value	Description
0x00	Unlock
0x01	Lock
0x02	Permalock
0x03	Lock&Permalock

要锁定的内存区选择：

Value	Memory space
0x00	Kill password
0x01	Access password
0x02	EPC
0x03	TID
0x04	User

返回数据：0x3C 0x03 错误码字节

例. Send: 3B 08 01 02 11 22 33 44

Receive: 3C 04 00 00 锁定成功。.

若返回: 3C 04 09 00 表示有错

3.4.2.7 灭活口令

功能说明：本操作命令将灭活标签，使符合条件的标签不再可用。

在执行灭活命令前，必须先将灭活口令设置到读写器中。

3.4.3 特殊命令

此是针对NXP标签用户设置的命令，主要有防盗系统（EAS）报警、读保护、校验。

发送命令：

命令码：0x45

命令字节：0x08

命名选择：见下表

位状态：0-reset，1-set

访问口令：

字节 3 用于命令选择可有：

value	Description
0x01	EAS Command Bit set/reset
0x02	Read Protect Bit set/reset
0x04	EAS Alarm execute
0x08	Calibrate execute

注：字节 3 对 EAS Alarm 和校验（calibrate）没有作用。

返回数据：0x46 0x03 错误码字节

例. Send: 45 08 02 01 11 22 33 44

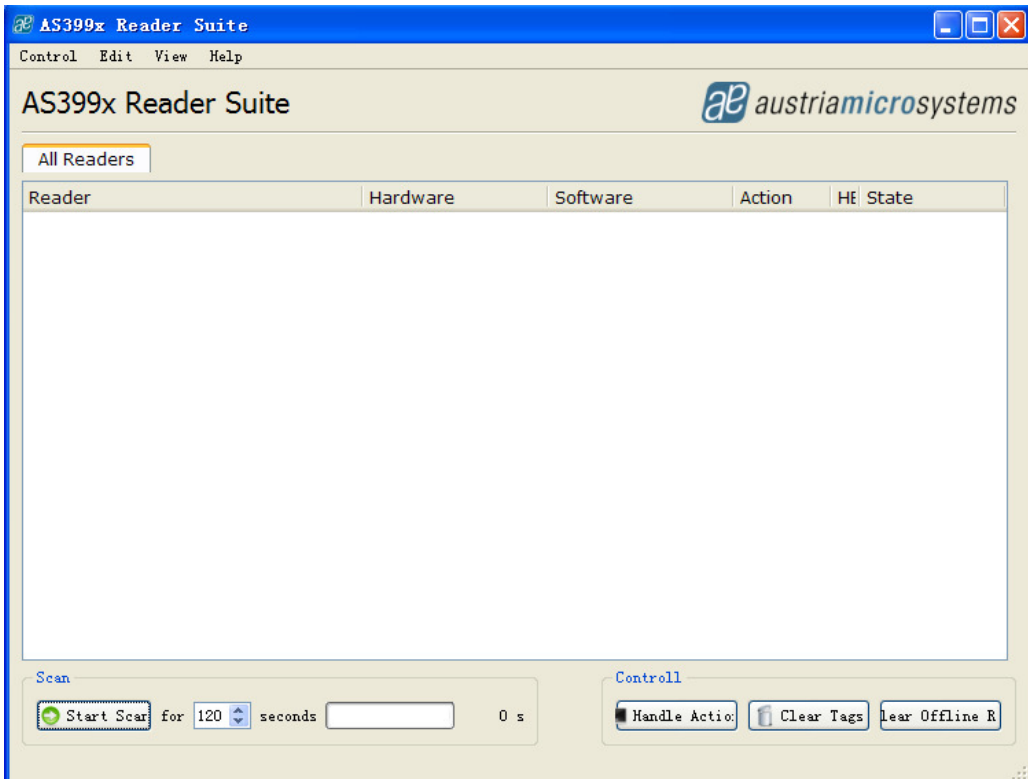
Receive: 46 05 00 00 00 No error.

Value	Meaning
0x02	读保护位 set/reset
0x01	置位
0x11 0x22 0x33 0x44	当前访问口令

第四章 可使用的上位机软件

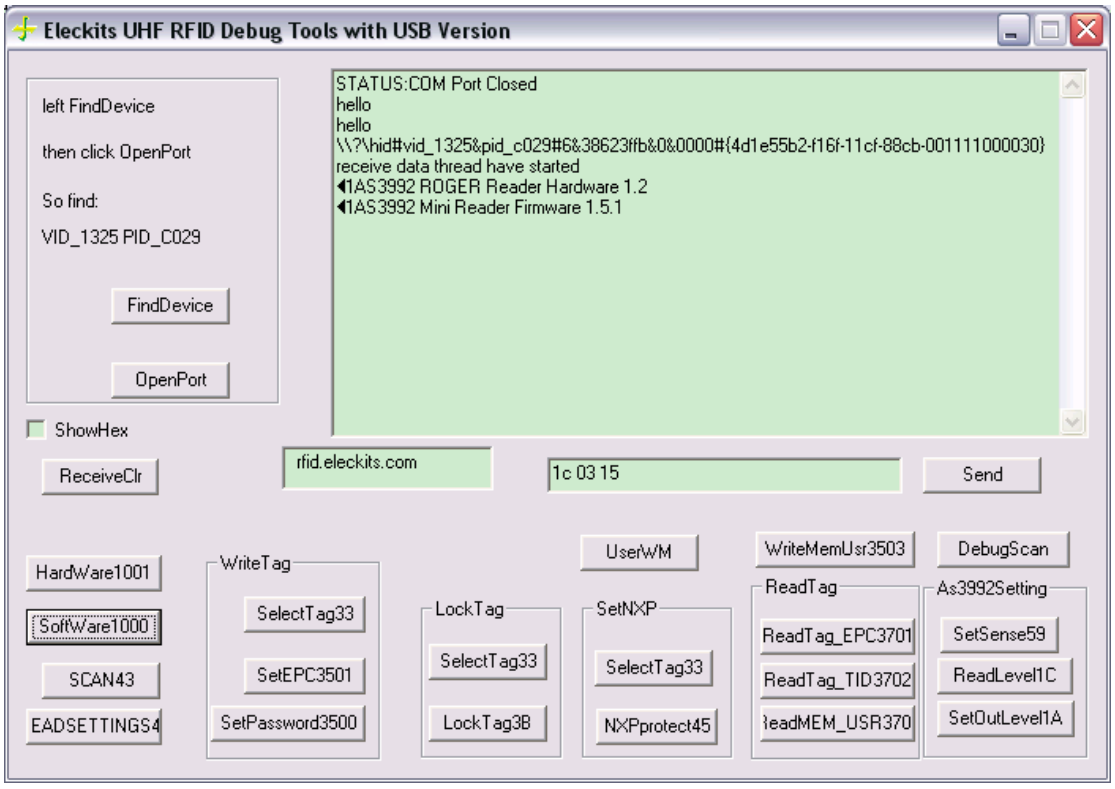
目前公司提供的可使用的软件有两种：

一是“AS399x Reader Suite v1.4.1”

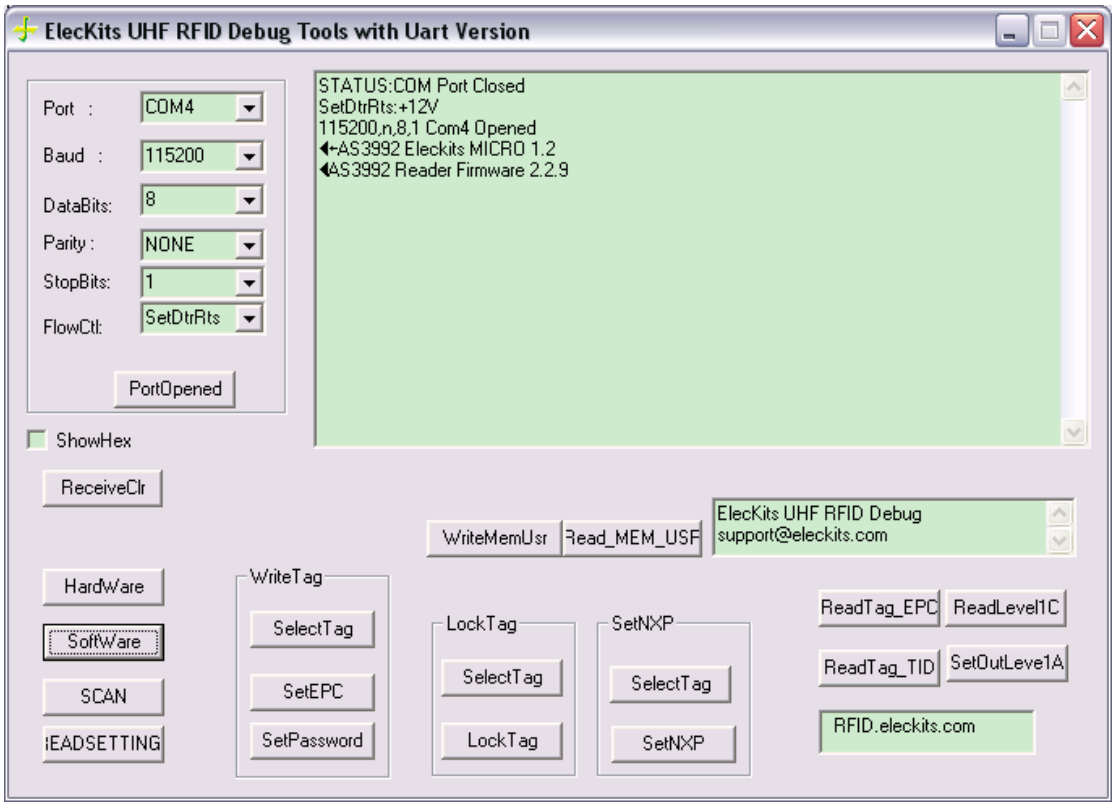


该上位机主要针对USB版本的UHF RFID，可进行参数设置和RSSI、EPC扫描。

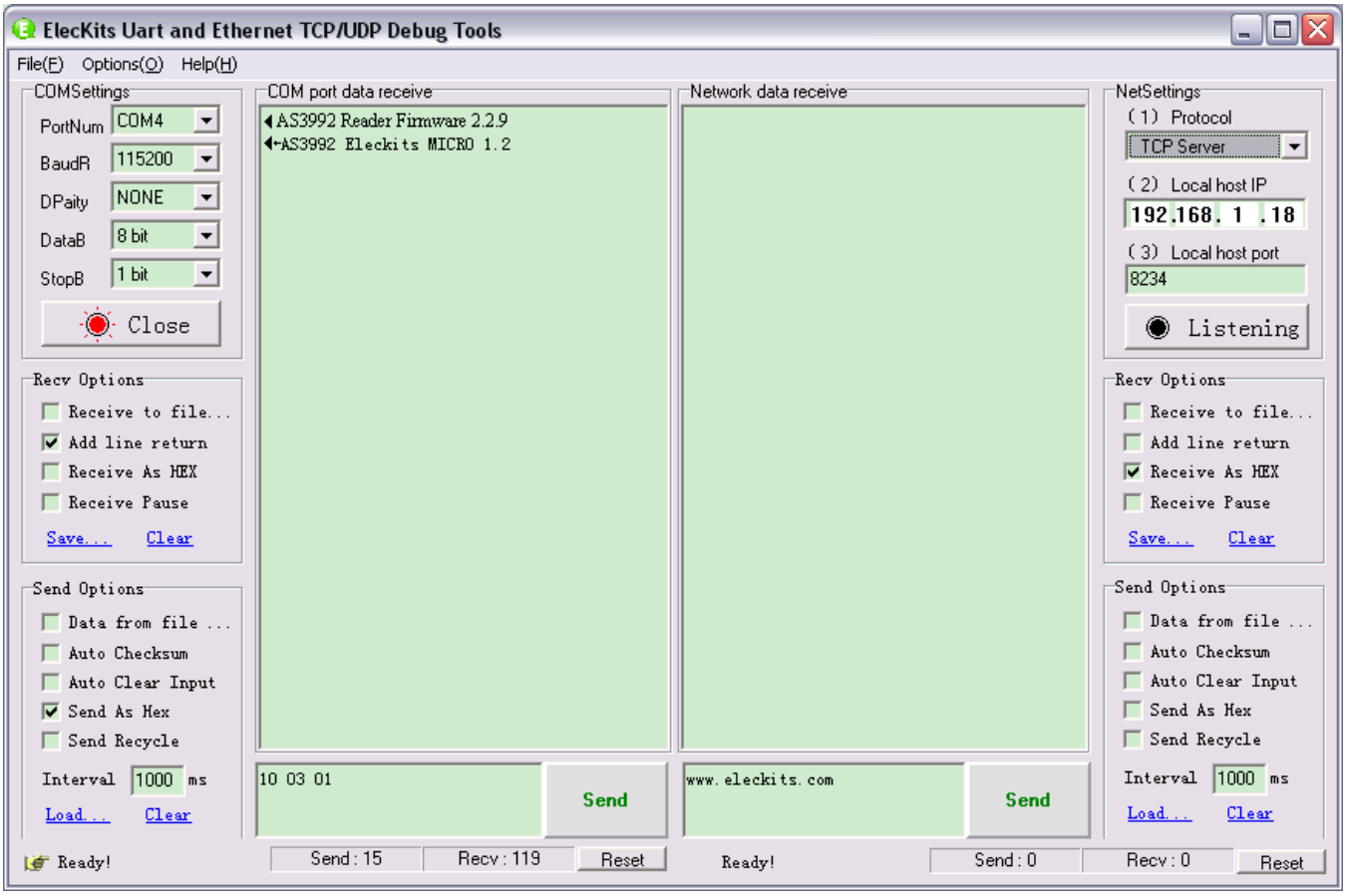
另一种是较简单的软件，可用于学习实验,有 UART 和 USB 两种版本：



上图为 USB 版本 debug 工具。



上图为 Uart 版本 debug 工具。
UART接口版本使用，当然你可以下载其他串口调试工具，自己发送命令查看。
工具的使用说明在上位机文件夹里，请参照使用。



ElecKits 串口及网络 TCP UDP 调试助手。

矽控电子（中远嵌入式）	
	
微信公众号『工控嵌入式 ARM』	智能硬件 QQ 群：273156182
http://iot.eleckits.com http://rfid.eleckits.com 高速 PCB Layout 与制板　　工控嵌入式 ARM 定制　　UHF RFID 与物联网	