



## 关键词

- TX522CT 读卡模块
- Mifare 1 S50, S70
- 扇区 密钥
- 一卡多用 一卡通
- 非接触式 智能卡
- RS485

## 摘要

TX522 系列模块是基于 13.56MHz 频率的 Mifare 卡读写模块,符合 ISO14443A 标准,可支持 Mifare1 S50、Mifare1 S70、Mifare Light、Mifare UltraLight、Mifare Pro。TX522 系列 Mifare 读写模块具有易用、高可靠、多种接口、体积小等特点,可帮助用户方便、快捷地将当今最流行的非接触式 IC 卡技术融入到系统中,提高产品的档次。

本文详细介绍了 TX522CT 模块的基于 51 单片机的 C51 库函数的使用方法。

## 目 录

1. 适用范围.....	4
2. TX522CT 简介 .....	5
2.1 技术参数.....	5
2.2 极限参数.....	5
2.3 直流特性.....	5
3. TX522CT 读卡模块数据传输协议 .....	7
3.1 物理层.....	7
3.2 UART 设置.....	7
3.3 数据帧描述.....	7
3.4 网络层通信协议.....	9
3.5 应用层通信协议.....	9
4. TX522CT 的函数（应用层命令） .....	10
5. 函数描述.....	12
5.1 协议控制类命令（CmdType = 0x00） .....	12
5.1.1 获取设备序列号—Get_DvcSnr（Cmd = ‘A’） .....	12
5.1.2 设置设备地址—Set_SlvAddr（Cmd = ‘B’） .....	12
5.1.3 获取设备地址—Get_SlvAddr（Cmd = ‘C’） .....	13
5.1.4 设置波特率—Set_Baud（Cmd = ‘D’） .....	14
5.1.5 搜索从机设置—Find_Slv（Cmd = ‘E’） .....	14
5.2 设备控制类命令（CmdType = 0x01） .....	15
5.2.1 获取信息—Get Info（Cmd = ‘A’） .....	15
5.2.2 配置—Config（Cmd = ‘B’） .....	16
5.2.3 关闭—Close（Cmd = ‘C’） .....	17
5.2.4 关闭—Load_Key（Cmd = ‘E’） .....	17
5.3 ISO14443A 类命令（CmdType = 0x02） .....	18
5.3.1 激活卡片并获取卡号—Get_CardSnr（Cmd = ‘M’） .....	18
5.3.2 直接密码证实—Auth_Key（Cmd = ‘F’） .....	19
5.3.3 证实 2—Auth2（Cmd = ‘E’） .....	20
5.3.4 读—Read（Cmd = ‘G’） .....	20
5.3.5 写—Write（Cmd = ‘H’） .....	21
5.3.6 带内部自动传送的值操作 1—Value（Cmd = ‘J’） .....	22
5.3.7 复位—Reset（Cmd = ‘L’） .....	22

5.3.8 挂起卡片—Halt (Cmd = 'D') .....	23
6. 免责声明.....	24
7. 修订历史.....	25
8. 销售信息.....	25

## 1. 适用范围

本文对 TX522CT Mifare 卡读写模块在 51 单片机下的 C51 库函数做了详细的讲解，使用 51 系列单片机与 TX522CT 进行通讯的用户参考本文提供的各函数，可以非常容易的编写操作 Mifare 卡的应用程序。不使用 51 系列单片机，而使用其它处理器的用户，也可以参考本文所描述提供的通讯格式和函数，将本文提供的函数很容易的移植到其它处理器上。

对于 C51 函数的调用，用户可不必关心数据块格式，只要理解函数的功能，输入、输出参数即可。当用户自己编写函数（包括非 C51 下的函数）时，就需了解数据块格式，必须按照数据块的格式来编写函数。

## 2. TX522CT 简介

**TX522CT 是 RS485 接口的读写模块，可组成 RS485 网络。**

用户主机通过 RS485 总线向 TX522CT 模块发送命令来对 TX522CT 进行读写控制。本应用指南将重点描述 TX522CT 与主机之间的通信协议和命令。

### 2.1 技术参数

表 1 TX522CT 模块技术参数表

产品型号	TX522CT 系列
功耗	25 毫安/直流 5V(读卡); 3 毫安/直流 5V (不读卡);
工作频率	13.56 兆赫兹
读卡距离	30~60 毫米 (mifare1 卡)
接口方式	RS485
数据传输速率	9600~230400bit/s
支持卡类型	mifare1 S50、mifare1 S70、mifare Pro
尺寸	50mm×38mm×12mm

### 2.2 极限参数

每个管脚的对地电压 .....-0.5~+5.5V  
 Vcc 对地的电压 .....-0.3~+12.0V  
 每个管脚的最大 I<sub>OL</sub> .....20mA  
 湿度 (相对湿度) .....5%~95

超出“绝对最大额定值”列出的值的条件下工作会造成器件的永久损坏。以上列出的是器件正常工作的额定值，并未涉及器件在这些条件或超出这些条件下的功能操作。器件不能长时间工作在绝对最大额定值条件下，否则会影响其可靠性。

### 2.3 直流特性

VCC=+5.0V，器件都工作在建议的温度范围-30~85℃条件下，除非特别说明。

表 2 TX522 模块的直流特性

符号	参数	测试条件	最小值	典型值 <sup>(1)</sup>	最大值	单位
VCC	工作电压		+4	+5.0	+12	V
T <sub>OK</sub>	上电后稳定工作时间		5			ms
I <sub>CC</sub>	电流消耗	读卡芯片配置成功		25		mA
V <sub>IL</sub>	输入低电平		0.7	1.3	-	V
V <sub>IH</sub>	输入高电平		-	2	2.3	V
V <sub>OL</sub>	输出低电平	I <sub>OL</sub> =20mA		0.6	1.0	V
		I <sub>OL</sub> =3.2mA		0.2	0.3	V
V <sub>OH</sub>	输出高电平	I <sub>OH</sub> =-20uA	3	3.1		V
I <sub>IL</sub>	逻辑低电平输入电流	V <sub>pin</sub> =0.4V			-80	μA
I <sub>TL</sub>	逻辑1到0变化电流	V <sub>pin</sub> =2V	-30		-450	μA

$I_{OL}$	低电平时的灌电流				-20	mA
$I_{OH}$	高电平时的拉电流				20	$\mu$ A
$C_{IO}$	管脚输入电容				15	pF
$T_{OP}$	工作温度(I)		-30		+85	$^{\circ}$ C
$T_{STR}$	存储温度		-55		+125	$^{\circ}$ C

(1) 典型值是难以保证的，这个值是在常温条件下测试得到。

(2) 模块上电后，必须等待 5ms 以上时间才能稳定工作。

### 3. TX522CT 读卡模块数据传输协议

#### 3.1 物理层

TX522CT 支持 RS485。

#### 3.2 UART 设置

UART 为 8 位数据位，无校验位，1 停止位。

出厂默认通信参数是：地址为 1，波特率为 9600。在下列任何一种情况下，采用默认通信参数：

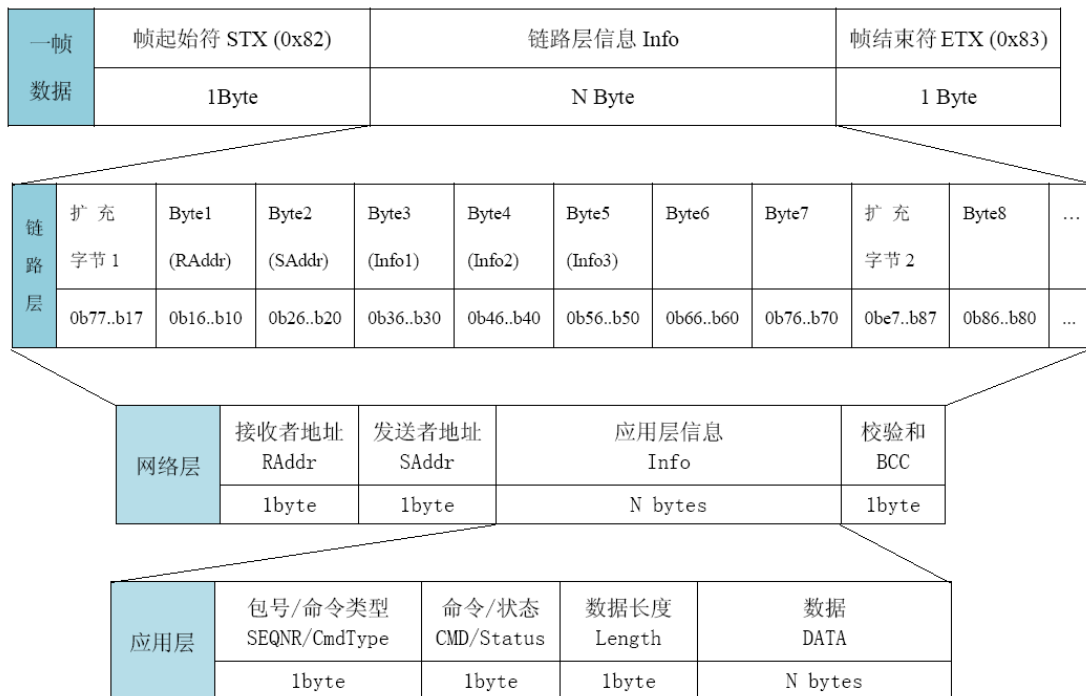
1、上电时，若模块上的模式短接点短接。模块地址和波特率恢复为默认值（1、9600）。但不改变非易失性存储器内的通信参数；

2、出厂时。

在使用时，可以对模块的地址和波特率进行设置，请看通信协议，模块支持的地址范围为 0~255，支持的波特率有：9600，19200，28800，38400，57600，115200，172800，230400，波特率号分别为 0、1、2、3、4、5、6、7。

#### 3.3 数据帧描述

在 RS485 总线上，数据总是以一帧为单位进行通信。数据帧的结构如下图所示。



一帧数据的起始符为STX（0x82），结束符为ETX（0x83），最高位都为1。

数据帧中最高层为应用层，应用层数据加上接收者地址（RAddr）、发送者地址（SAddr）、以及所有字节的校验和BCC构成网络层数据。

在一帧数据中，为了与STX 和ETX 区分开来，链路层数据信息的每个字节的最高位必须为0，而高层数据信息的每个字节的取值可为0x00~0xff。网络层的数据必须通过数据处

理（扩充）才能成为数据链路层。

链路层数据处理方法如下：将高层数据每7字节分为一组，在每组前面插入一个字节，该字节的最高位bit7为0，后面7位bit6~bit0 依次为后面7个字节的最高位。如下图所示：

网络层数据 (7 字节一组)	Byte1	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7
	0b17..b10	0b27..b20	0b37..b30	0b47..b40	0b57..b50	0b67..b60	0b77..b70

转换为下面数据：

链路层 (8 字节)	扩充字节	Byte1	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7
	0b77..b17	0b16..b10	0b26..20	0b36..b30	0b46..b40	0b56..b50	0b66..b60	0b76..b70

举例如下：

第 1 组							第二组		
Byte1	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7	Byte8	Byte9	Byte10
0x00	0x01	0x00	0x00	0x04	0xff	0x80	0x00	0x01	0x84

转换为链路层为：

扩充 1	Byte1	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7	扩充 2	Byte8	Byte9	Byte10
0x60	0x00	0x01	0x00	0x00	0x04	0x7f	0x00	0x04	0x00	0x01	0x04

数据链路层接收规则：

1. 任何时候，接收到STX，表示一帧开始，继续接收内容（下一字节实际上是地址）。
2. 若接收到的地址字段与本机地址相符，则继续接收数据信息，否则丢弃后面的数据。
3. 数据链路层只管把数据接收下来并不验证数据，验证数据的正确性必须通过上层协议来完成。
4. 接收相邻两字节的间隔时间不得超过5ms 若超时则本帧数据无效。重新接收下一个STX。

通信描述：

1. RS485总线上，从机读卡模块可以有多个，而主机控制器只能有一个。只有主机才能主动发送命令或控制数据给从机，从机只能对主机的命令做出响应。
2. 主机发送完命令数据后，等待从机响应，若在100ms内从机未响应，则重发命令，再次等待从机响应，若连续发三次从机均未响应，则停止重发且向调用程序报告错误。
3. 从机只对与自身地址相符的命令帧做出响应. 如果接收到一个错误的的数据或地址不符则不做出任何响应。
4. 当主机以广播方式下发指令时，所有从机都接收这帧数据，但只有以下两种情况下从机才对广播命令进行应答。第1：数据中包含有与从机设备相符的设备序列号；第2：搜索命令允许每个从机在某个时间片内分别作出应答。



### 3.4 网络层通信协议

网络层可以保证数据的有效性和完整性。网络层有 4 个字段。数据格式如下所示：

网络层	接收者地址 RAddr	发送者地址 SAddr	应用层信息 Info	校验和 BCC
	1byte	1byte	N bytes	1byte

各字段说明如下：

字段	说 明
RAddr	数据接收者地址, 多机通信时是必需的参数, 只有当从机地址和该地址值相等时, 从机才处理所接收的数据。0xff是广播地址, 所有从机都接受这个地址。
SAddr	数据发送者地址
Info	应用层数据信息
BCC	从Addr 开始至应用层信息Info 的最后一字节相异或后取反。

### 3.5 应用层通信协议

应用层数据格式如下：

应用层	包号/命令类型 SEQNR/CmdType	命令/状态 CMD/Status	数据长度 Length	数据 DATA
	1byte	1byte	1byte	N bytes

各字段说明如下：

字段	长度	说明	补充
SEQNR/ CmdType	1	Bit7-4: 该数据帧包序号, 从 0 到 15 循环。可以用来作为通信间的错误检查, 从机(模块)接收到主机发来的信息, 在应答信息中发出一个同样的 SEQ 信息, 主机可以通过此信息检查是否发生的“包丢失”的错误。第一个包的 SEQ 可为任意值。 Bit3-0: 命令类型。 0x00: 协议控制类命令, 如设置从机地址, 读产品序列号等 0x01: 设备控制类命令, 如读产品信息等 0x02: ISO14443-A 命令 其它值保留。 注意: 从机返回相同的 CmdType	该字段主机发送和接收的应该相同
Cmd /Status	1	主机——从机: 命令 Command 从机——主机: 状态 Status	
Length	1	该帧所带数据信息长度 若模块返回状态不为 0 (OK), 则 Length=0。	
DATA	Length	数据信息, 长度等于 Length	

## 4. TX522CT 的函数（应用层命令）

表 3 TX522CT 提供的串行通讯库函数列表

命令类型	命令	函数名	输入参数(发送)	输出参数(接收)	功能描述
协议控制类 0x00	'A'	Get_DvcSnr	--	*DvcSnr	读设备序列号
	'B'	Set_SlvAddr	*DvcSnr,NewAddr	--	设置从机地址
	'C'	Get_SlvAddr	*DvcSnr	*Addr	读取从机地址
	'D'	Set_Baud	NewBaud	--	设置波特率
	'E'	Find_Slv	MinAddr, MaxAddr	*SlvNum, *SlvBfr	搜索从机
设备控制类 0x01	'A'	Get_Info	--	*Info	读取模块信息
	'B'	Config	--	--	复位且配置模块
	'C'	Close	--	--	关闭模块
	'E'	Load_Key	KeyAB,Sector,*Key	--	改变存贮在模块内密钥区中的密钥
TYPE A 0x02	'D'	Halt	--	--	将卡置于挂起模式
	'E'	Auth2	KeyAB,*SNR, Key_Sector,Block	--	使用模块内部密钥区中的密码对指定的卡的扇区 Sector 进行验证
	'F'	Auth_Key	KeyAB,*SNR,*Key,Block	--	直接密码验证
	'G'	Read	Block	*Data	从卡中指定块中读出一个 16 字节的块
	'H'	Write	Block,*Data	--	向卡中指定块写入一 16 字节的数据块
	'J'	Value	ValueMode,Block,*Value, Trans_Block	--	包含加、减、恢复函数，并可进行不同块之间的自动传送
	'L'	Reset	Msec	--	关闭天线输出数 ms，使卡复位
	'M'	Get_CardSnr	ReqCode	*TagType, *Sak,*SnrLen, *Snr	激活卡片并获取卡号

表 3 所有函数的返回值都是该函数执行后的状态结果，具体返回值请查看各函数说明。如果各函数有返回数据，则都是以指针的形式返回。

表 4 TX522 库函数的用到的状态值列表

名称	值	描述
OK, COMM_OK	0	函数调用成功
NO_TAG_ERR	1	在有效区域内没有卡
CRC_ERR	2	从卡中接收到了错误的 CRC 校验和
EMPTY	3	值溢出
AUTH_ERR	4	不能验证
PARITY_ERR	5	从卡中接收到了错误的校验位
CODE_ERR	6	通信错误
SENDR_ERR	8	在防冲突时读到了错误的串行码
KEY_ERR	9	证实密码错
NOT_AUTH_ERR	10	卡没有验证
BIT_COUNT_ERR	11	从卡中接收到了错误数量的位
BYTE_COUNT_ERR	12	从卡中接收到了错误数量的字节
TRANS_ERR	14	调用 Transfer 函数出错
WRITE_ERR	15	调用 Write 函数出错

INCR_ERR	16	调用 Increment 函数出错
DECR_ERR	17	调用 Decrment 函数出错
READ_ERR	18	调用 Read 函数出错
COLL_ERR	24	冲突错
ACCESS_TIMEOUT	27	访问超时
QUIT	30	上一次了送命令时被打断
CHK_WR_OK	0	Check Write 正确
CHK_WR_FAILED	1	Check Write 出错
CHK_WR_COMP_ERR	2	Check Write:写出错（比较出错）
COMM_ERR	255	串行通信错误
MI_WRONG_VALUE	123	值块格式错误

## 5. 函数描述

下面是 C51 函数声明，包含在头文件“TX\_C.h”中，写应用程序时，将其包含在应用函数中即可。对于 C51 函数的调用，用户可不必关心数据块格式，只要理解函数的功能，输入、输出参数即可。当用户自己编写函数（包括非 C51 下的函数）时，就需了解数据块格式，必须按照数据块的格式来编写函数。

### 5.1 协议控制类命令（CmdType = 0x00）

#### 5.1.1 获取设备序列号—Get\_DvcSnr（Cmd = 'A'）

函数原型：uchar TX\_Get\_DvcSnr (uchar idata \* DvcSnr);

输入参数：无

输出参数：DvcSnr，DvcSnr 为模块序列号的首地址。

函数返回：执行命令后的状态，可能的状态值如下：OK，QUIT，COMM\_ERR。

功能描述：获取 TX522CT 模块的序列号信息。每个模块都有一个唯一的设备序列号。

主机→TX522 命令模式：

例如：地址为 0x00 的主机读取地址为 0x01 从机的设备信息的数据帧。（以后所有例子都假设主机地址为 0x00，从机为 0x01）

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x00	0x41	0x00	none	0xBF

假设所有例子的包序号 SEQ 都为 0。

数据链路层数据帧(黄色方框为数据链路层加上的STX、扩展数据和ETX):

0x82	0x20	0x01 0x00 0x00 0x41 0x00 0x3f				0x83
------	------	-------------------------------	--	--	--	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x00	0x00	0x04	0x09 0x23 0x00 0x02	0xD2

数据链路层数据帧：

0x82	0x00	0x00 0x01 0x00 0x00 0x04 0x09 0x23	0x00	0x00 0x02 0x52	0x83
------	------	------------------------------------	------	----------------	------

#### 5.1.2 设置设备地址—Set\_SlvAddr（Cmd = 'B'）

函数原型：uchar TX\_Set\_SlvAddr(uchar idata \*DvcSnr, uchar NewAddr);

输入参数：\*DvcSnr 为保存模块序列号的首地址

NewAddr：需要设置的新的地址 0~255

输出参数：NewAddr：设置好的新的地址。

函数返回：执行命令后的状态，可能的状态值如下：OK，QUIT，COMM\_ERR。

功能描述：设置模块的地址信息。每个模块都应设置不相同的地址。该命令发送广播地

址 0xff，所有从机接收到该命令后，将设备序列号与本身的进行比较，如果相同则修改自己的地址，并保存，然后返回应答数据。若序列号不相同则退出。

主机→TX522 命令模式：

例如：设置设备序号好为 0x09 0x23 0x00 0x02 的从机的地址为 0x02

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0xff	0x00	0x00	0x42	0x05	0x09 0x23 0x00 0x02 0x02	0x6d

数据链路层数据帧：

0x82	0x01	0x7f 0x00 0x00 0x42 0x05 0x09 0x23	0x00	0x00 0x02 0x02 0x6d	0x83
------	------	------------------------------------	------	---------------------	------

TX522→主机（响应模式）：

例如：设置好地址为 0x02 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x02	0x00	0x00	0x01	0x02	0xFE

数据链路层数据帧：

0x82	0x40	0x00 0x02 0x00 0x00 0x01 0x02 0x7e	0x83
------	------	------------------------------------	------

### 5.1.3 获取设备地址—Get\_SlvAddr (Cmd = 'C')

函数原型：uchar TX\_Get\_SlvAddr(uchar idata \*DvcSnr, uchar idata \*Addr);

输入参数：\*DvcSnr 为保存模块序列号的首地址

输出参数：Addr：设备地址。

函数返回：执行命令后的状态，可能的状态值如下：OK，QUIT，COMM\_ERR。

功能描述：**设置模块的地址信息。每个模块都应设置不相同的地址。**

该命令发送广播地址 0xff，所有从机接收到该命令后，将设备序列号与本身的进行比较，如果相同则返回自己的地址。若序列号不相同则不返回、退出。

主机→TX522 命令模式：

例如：读设备序号好为 0x09 0x23 0x00 0x02 的从机的地址

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0xff	0x00	0x00	0x43	0x04	0x09 0x23 0x00 0x02	0x6f

数据链路层数据帧：

0x82	0x01	0x7f 0x00 0x00 0x43 0x04 0x09 0x23	0x00	0x00 0x02 0x6f	0x83
------	------	------------------------------------	------	----------------	------

TX522→主机（响应模式）：

例如：设置好地址为 0x02 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x02	0x00	0x00	0x01	0x02	0xFE

数据链路层数据帧：

0x82	0x40	0x00 0x02 0x00 0x00 0x01 0x02 0x7e	0x83
------	------	------------------------------------	------

### 5.1.4 设置波特率—Set\_Baud (Cmd = 'D')

函数原型: uchar TX\_Set\_Baud( uchar NewBaud);

输入参数: NewBaud:波特率号。支持的波特率有: 9600, 19200, 28800, 38400, 57600, 115200, 172800, 230400, 波特率号分别为 0、1、2、3、4、5、6、7。

输出参数: 无。

函数返回: 执行命令后的状态, 可能的状态值如下: OK, QUIT, COMM\_ERR。

功能描述: 设置模块的波特率。每个模块都应设置相同的波特率。

该命令发送广播地址 0xff, 所有从机接收到该命令后, 修改本设备的波特率, 并保存。不做任何应答。

主机→TX522 命令模式:

例如: 设置所有从机的波特率为 19200 (0x01)

网络层数据:

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0xff	0x00	0x00	0x44	0x01	0x01	0x44

数据链路层数据帧:

0x82	0x01	0x7f 0x00 0x00 0x44 0x01 0x01 0x44	0x83
------	------	------------------------------------	------

### 5.1.5 搜索从机设置—Find\_Slv (Cmd = 'E')

函数原型: uchar TX\_Find\_Slv(uchar MinAddr, uchar MaxAddr, uchar idata \*SlvNum, uchar idata \* SlvBfr);

输入参数: MinAddr 需要搜索的最小地址

MaxAddr: 需要搜索的最大地址

输出参数: SlvNum: 搜索到的从机数量

SlvBfr: 搜索到的从机地址的保存的首地址

函数返回: 执行命令后的状态, 可能的状态值如下: OK, QUIT, COMM\_ERR。

功能描述: 搜索指定地址范围内的从机地址。该命令发送广播地址 0xff, 所有从机接收到该命令后, 将搜索范围地址本身的进行比较, 如果在搜索范围内, 返回应答数据。

只有不小于搜索地址且不大于最大搜索地址的从机才在自己的时间片内返回应答。如果主机在一个时间片内没有接收到应答, 则可以认为与这个时间片对于的从机不存在。

以上命令的正确执行需要满足下面几个条件:

1. 总线上所有从机的波特率必须相同。
2. 总线上所有从机的地址互不相同。
3. 总机发送命令后, 必须等待至少 (最大搜索地址-最小搜索地址 + 2) 个时间片的时间, 才能继续发送下一条命令。

所有从机在接收到此命令后, 根据自身地址在不同的时间片内进行应答, 时间片的长短和波特率有关。时间片和波特率的关系为:

( (11位×9字节) / 波特率 ) + 5ms (冗余时间)

波特率	波特率号	时间片大小 (ms)
9600	0	15
19200	1	10
28800	2	10

38400	3	10
57600	4	5
115200	5	5
172800	6	5
230400	7	5

主机→TX522 命令模式：

例如：搜索地址范围 0-0xfe 的从机

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0xff	0x00	0x00	0x45	0x02	0x00 0xfe	0xb9

数据链路层数据帧：

0x82	0x41	0x7f 0x00 0x00 0x45 0x02 0x00 0x7e	0x01	0x39	0x83
------	------	------------------------------------	------	------	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机应答（收到命令后立即应答）

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x00	0x00	0x00		0xFE

数据链路层数据帧：

0x82	0x20	0x00 0x01 0x00 0x00 0x00 0x7e	0x83
------	------	-------------------------------	------

例如：地址为 0x02 的从机在自己的时间片发送的应答

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x02	0x00	0x00	0x00		0xFD

数据链路层数据帧：

0x82	0x20	0x00 0x02 0x00 0x00 0x00 0x7D	0x83
------	------	-------------------------------	------

例如：地址为 0xFE 的从机在自己的时间片发送的应答

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0xfe	0x00	0x00	0x00		0x01

数据链路层数据帧：

0x82	0x02	0x00 0xfe 0x00 0x00 0x00 0x01	0x83
------	------	-------------------------------	------

## 5.2 设备控制类命令（CmdType = 0x01）

### 5.2.1 获取信息—Get Info（Cmd = 'A'）

函数原型：uchar TX\_Get\_Info(uchar idata \*Info);

输入参数：无

输出参数：模块的信息\*Info，Info 为保存信息空间的首地址。Info[0]~Info[4]为模块类型标识，依次为 '5'，'2'，'2'，'D'，0，Info[5]~Info[8]为模块的唯一序列号，Info[9]为固件版本号，高四位为版本号的整数，取值从 1 到 15，低四位为版本号的小数，取值从 0

到 9。

函数返回：执行命令后的状态，可能的状态值如下：OK, QUIT, COMM\_ERR。

功能描述：获取 TX522CT 模块的信息。

主机→TX522 命令模式：

例如：地址为 0x00 的主机读取地址为 0x01 从机的设备信息的数据帧

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x01	0x41	0x00	none	0xBE

数据链路层数据帧：

0x82	0x20	0x01 0x00 0x01 0x41 0x00 0x3e					0x83
------	------	-------------------------------	--	--	--	--	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x01	0x00	0x0a	0x35 0x32 0x32 0x43 0x00 0x09 0x23 0x00 0x02 0x10	0xBB

数据链路层数据帧：

0x82	0x00	0x00 0x01 0x01 0x00 0x0a 0x35 0x32	0x00	0x32 0x43 0x00 0x09 0x23 0x00 0x02	0x02	0x10 0x3B	0x83
------	------	---------------------------------------	------	---------------------------------------	------	-----------	------

### 5.2.2 配置—Config（Cmd = 'B'）

函数原型：uchar TX\_Config(void);

输入参数：无

输出参数：无

函数返回：TX522CT 执行命令后的状态，可能的状态值如下：OK, QUIT, COMM\_ERR。

功能描述：对模块进行初始化，初始化成功后，此时天线发射载波信号，任何进入天线感应区的卡可得电进入 IDLE 状态，可使用任一函数对卡进行操作。此时读卡芯片完全被激活，所消耗的电流最大。

建议每次对卡片操作完成后都调用 TX\_Close 关闭射频场以降低模块功耗，每次对卡片操作前都调用 Config 打开射频卡。

主机→TX522 命令模式：

例如：配置地址为 0x01 的从机

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x01	0x42	0x00	none	0xBD

数据链路层数据帧：

0x82	0x20	0x01 0x00 0x01 0x42 0x00 0x3e					0x83
------	------	-------------------------------	--	--	--	--	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：



RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x01	0x00	0x00		0xff

数据链路层数据帧:

0x82	0x20	0x00 0x01 0x01 0x00 0x00 0x7f				0x83
------	------	-------------------------------	--	--	--	------

### 5.2.3 关闭—Close (Cmd = 'C')

函数原型: uchar TX\_Close(void);

输入参数: 无

输出参数: 无

函数返回: 执行命令后的状态, 可能的状态值如下: OK, COMM\_ERR。

功能描述: 此函数将关闭 TX522CT 模块, 天线不发送载波信号, 模块消耗的电流最小, 在此状态在, 模块不能使用。当发送请求或者获取卡号命令时, 模块会重新自动调用 Config() 函数对 TX522CT 重新进行配置。

如果要对功耗进行控制, 在每次对卡片进行完所有操作后, 应该发送该命令以关闭模块。

主机→TX522 命令模式:

例如: 关闭地址为 0x01 从机

网络层数据:

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x01	0x43	0x00	none	0xBc

数据链路层数据帧:

0x82	0x20	0x01 0x00 0x01 0x43 0x00 0x3c				0x83
------	------	-------------------------------	--	--	--	------

TX522→主机 (响应模式):

例如: 地址为 0x01 的从机响应地址为 0x00 主机

网络层数据:

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x01	0x00	0x00		0xff

数据链路层数据帧:

0x82	0x20	0x00 0x01 0x01 0x00 0x00 0x7f				0x83
------	------	-------------------------------	--	--	--	------

### 5.2.4 关闭—Load\_Key (Cmd = 'E')

函数原型: uchar TX\_Load\_Key(uchar KeyAB,uchar Key\_Sector,uchar idata \*Key)

输入参数: KeyAB: 密钥类型 (1 字节)。可取值为 KeyAB=0x60 (KEYA) —密钥 A, 或 KeyAB=0x61 (KEYB) —密钥 B。

Key\_Sector: 模块内的密钥区号 (1 字节): 取值范围 0~3

\*Key: 需要装载到模块内密钥区的密钥 (6 字节)

输出参数: 无

函数返回: 执行命令后的状态。

功能描述: 此函数的作用是将指定的密码 (\*Key) 装载到模块内 E2PROM 指定的密钥区 (Key\_Sector), 并非改变 Mifare1 卡内扇区的密码。本函数只对模块进行操作, 模块与卡之间没有数据传输。装载的密钥掉电不丢失, 因此只用装载一次就可以。考虑到系统安全性,

装载密钥过程可单独进行，用户程序中可不出现该命令。

模块内有 4 个密码区(区号 0—3)，称它为密钥区号 Key\_Sector。每个区分密钥 A(0x60)和密钥 B (0x61) 两个，总共 8 个密码。装载成功后，可用该密钥对 Mifare1 卡进行验证。

在 M1 卡中有 16 个存储区，称它为扇区号 Sector。若要改变 Mifare1 卡内的密钥，可在用原密码验证通过后，直接用写块数据 TX\_Write()函数，将密码块改写。Mifare 卡出厂后的初始密钥为 6 个 FFH，A 和 B 密钥都一样。

主机→TX522 命令模式：

例如：往密钥 0 区装载密钥 A：0xff 0xff 0xff 0xff 0xff 0xff 的数据帧

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x01	0x45	0x08	0x60 0x00 0xff 0xff 0xff 0xff 0xff 0xff	0x52

数据链路层数据帧：

0x82	0x00	0x01 0x00 0x01 0x45 0x08 0x60 0x00	0x7f	0x7f 0x7f 0x7f 0x7f 0x7f 0x7f 0x52	0x83
------	------	------------------------------------	------	---------------------------------------	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x01	0x00	0x00		0xff

数据链路层数据帧：

0x82	0x20	0x00 0x01 0x01 0x00 0x00 0x7f	0x83
------	------	-------------------------------	------

### 5.3 ISO14443A 类命令（CmdType = 0x02）

#### 5.3.1 激活卡片并获取卡号—Get\_CardSnr（Cmd = 'M'）

函数原型：uchar TX\_Get\_CardSnr(uchar ReqCode, uchar idata \*TagType, uchar idata \*Sak, uchar idata \*SnrLen, uchar idata \*Snr);

输入参数：ReqCode：请求模式 ReqCode 取值为 1 或 0

ReqCode=0x26（IDLE），请求天线范围内 IDLE 状态的卡（HALT 状态的除外）

ReqCode=0x52（ALL），请求天线范围内的所有卡。

输出参数：

- (1) \*TagType：请求应答：2 个字节的卡片类型。
- (2) \*Sak：最后一级选择应答的应答。
- (3) \*SnrLen：返回卡片序列号的长度。
- (4) \*Snr：返回卡片的序列号。

函数返回：执行命令后的状态，可能的状态值如下：OK，QUIT，COMM\_ERR 中的某一个。

功能描述：该命令为请求、防碰撞和选择三条命令的组合。成功执行该命令后即可进行验证及后续操作。

主机→TX522 命令模式：

例如：以请求所有的方式获取地址为 0x01 从机的天线区域的卡片信息。

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x02	0x4d	0x01	0x52	0xe2

数据链路层数据帧：

0x82	0x40	0x01 0x00 0x02 0x4d 0x01 0x52 0x62					0x83
------	------	------------------------------------	--	--	--	--	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机出卡号为 0x007e0a42 的 Mifare1 S50 卡的响应

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x02	0x00	0x08	0x04 0x00 0x08 0x04 0x42 0x0A 0x7E 0x00	0xca

数据链路层数据帧：

0x82	0x00	0x00 0x01 0x02 0x00 0x08 0x04 0x00	0x20	0x08 0x04 0x42 0x0A 0x7E 0x00 0x4a	0x83
------	------	------------------------------------	------	------------------------------------	------

该命令返回数据的长度随卡片类型而不同，LENGTH= 4 字节+序列号的长度，Mifare1 S50、S70、Light 卡卡号长度 4 字节，共 8 字节，Mifare0 UltraLight 和 Mifare3 Desfire 卡卡号 7 字节，共 11 字节。

### 5.3.2 直接密码证实—Auth\_Key (Cmd = 'F')

函数原型：uchar TX\_Auth\_Key (uchar KeyAB, uchar Sector, uchar idata \*Key);

输入参数：KeyAB：密钥类型（1 字节）。可取值为 KeyAB=0x60 (KEYA)，利用密钥 A 进行验证，或 KeyAB=0x61 (KEYB)，利用密钥 B 进行验证。

Sector：所要验证的卡扇区号（也即将要访问的卡的扇区号），取值范围 0~39，能用于 S70 卡。

Key：用于证实的密码首地址，应在外部定义一个共 6 个字节的数组用于存放密码

输出参数：无

函数返回：执行命令后的状态。

功能描述：TX\_Auth\_Key 函数用 Key 指针所指向的 6 个字节密钥进行验证，也称为直接密码证实。若卡中的密钥与所传输的密码相匹配。则证实成功。

主机→TX522 命令模式：

例如：用密码 0xff 0xff 0xff 0xff 0xff 0xff 证实扇区 0。

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x02	0x46	0x08	0x60 0x00 0xff 0xff 0xff 0xff 0xff 0xff	0x52

数据链路层数据帧：

0x82	0x00	0x01 0x00 0x02 0x46 0x08 0x60 0x00	0x7f	0x7f 0x7f 0x7f 0x7f 0x7f 0x7f 0x52	0x83
------	------	------------------------------------	------	---------------------------------------	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x02	0x00	0x00		0xfc

数据链路层数据帧：

0x82	0x20	0x00 0x01 0x02 0x00 0x00 0x7c					0x83
------	------	-------------------------------	--	--	--	--	------

### 5.3.3 证实 2—Auth2 (Cmd = 'E')

函数原型：uchar TX\_Auth2(uchar KeyAB, uchar Sector, uchar Key\_Sector);

输入参数：KeyAB：密钥类型（1 字节）。可取值为 KeyAB=0x60（KEYA），利用密钥 A 进行验证，或 KeyAB=0x61（KEYB），利用密钥 B 进行验证。

Sector：所要验证的卡扇区号（也即将要访问的卡的扇区号），取值范围 0~39，能用于 S70 卡。

Key\_Sector：模块内的密钥区号（1 字节）：取值范围 0~3。

输出参数：无

函数返回：执行命令后的状态。

功能描述：使用模块内部密钥区中 Key\_Sector 中的密码对指定的卡的扇区 Sector 进行验证，若卡 Sector 区中的密码与存储在模块内 Key\_Sector 中的密码相同，则验证成功。

该函数依赖 TX\_Load\_Key 函数曾经成功执行过，因为模块内部密码区（Key\_Sector）中的密码要由 TX\_Load\_Key 函数事先装载。该函数适用于对于所有卡来说密码相同的应用，密钥的装载可以在一个安全的场合一次性装入。

主机→TX522 命令模式：

例如：用密钥 0 区的密钥 A 证实卡的扇区 0。

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x02	0x45	0x03	0x60 0x00 0x00	0xda

数据链路层数据帧：

0x82	0x00	0x01 0x00 0x02 0x45 0x03 0x60 0x00				0x02	0x00 0x5a	0x83
------	------	------------------------------------	--	--	--	------	-----------	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x02	0x00	0x00		0xfc

数据链路层数据帧：

0x82	0x20	0x00 0x01 0x02 0x00 0x00 0x7c					0x83
------	------	-------------------------------	--	--	--	--	------

### 5.3.4 读—Read (Cmd = 'G')

函数原型：uchar TX\_Read(uchar Block,uchar idata \*Data)

输入参数：Block：卡块号（1 字节）； S50：0~63； S70：0~255

输出参数：\*Data：Data 为读回 16 字节数据的首地址。

函数返回：执行命令后的状态。

功能描述：在验证成功后，使用该函数读 Mifare 卡中相应块的数据。Mifare 卡中一个块的数据是 16 字节，因此读写一次均是 16 个字节。

所读块号必须与之前所验证的块号在同一个扇区内，mifare1 卡从块号 0 开始按顺序每 4 个块 1 个扇区。密码数据不能被读取。

主机→TX522 命令模式：

例如：读取块 1 的数据的数据帧。

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x02	0x47	0x01	0x01	0xcb

数据链路层数据帧：

0x82	0x40	0x01 0x00 0x02 0x47 0x01 0x01 0x3b						0x83
------	------	------------------------------------	--	--	--	--	--	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x02	0x00	0x10	0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x11 0x12 0x13 0x14 0x15 0x16	0xfa

数据链路层数据帧：

0x82	0x00	0x00 0x01 0x02	0x00	0x03 0x04 0x05	0x00	0x10 0x11 0x12	0x01	0x7a	0x83
		0x00 0x10 0x01		0x06 0x07 0x08		0x13 0x14 0x15			
		0x02		0x09		0x16			

### 5.3.5 写—Write (Cmd = 'H')

函数原型：uchar TX\_Write(uchar Block,uchar idata \*Data)

输入参数：Block: 卡块号（1 字节）； S50: 1~63; S70: 1~255

\*Data: 16 字节数据指针，Data 为写入的 16 字节数据的首地址。

输出参数：无

函数返回：执行命令后的状态。

功能描述：对卡内某一块进行验证成功后，即可对同一扇区的各个块进行写操作（只要访问条件允许），其中包括位于扇区尾的密码块，这是更改密码的唯一方法。

Mifare 卡中一个块的数据是 16 字节，因此读写一次均是 16 个字节。所读块号必须与之前所验证的块号在同一个扇区内，mifare1 卡从块号 0 开始按顺序每 4 个块 1 个扇区。

主机→TX522 命令模式：

例如：往块 1 写入数据的数据帧。

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x02	0x00	0x11	0x01 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x11 0x12 0x13 0x14 0x15 0x16	0xb2

数据链路层数据帧：

0x82	0x00	0x01 0x00 0x02 0x48 0x11 0x01 0x01	0x00	0x02 0x03 0x04 0x05 0x06 0x07 0x08	0x00	0x09 0x10 0x11 0x12 0x13 0x14 0x15	0x02	0x16 0x32	0x83
------	------	--	------	--	------	--	------	--------------	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x02	0x00	0x00		0xfc

数据链路层数据帧：

0x82	0x20	0x00 0x01 0x02 0x00 0x00 0x7c	0x83
------	------	-------------------------------	------

补充说明：

注意：在将数据写到卡片上的某一扇区时，一定要小心。特别是每一个扇区的 Block3 中存放了该扇区的存取条件，包含有 KEYA, KEYB 及该扇区的控制字。Mifare 1 卡片出厂时的 Block3 有缺省值，为：“a0a1a2a3a4a5ff078069b0b1b2b3b4b5”，共 16 个 Bytes。

涉及 Mifare 1 卡片的存储结构等信息，请参考 Mifare 1 卡片数据手册。

程序员在使用 Mifare 1 卡片做应用时，一定要清清楚楚记住每一个扇区的 Block3 的数据，这样也就记住了扇区的密码和存取控制字。否则，扇区的存储空间将不执行 Read/Write 等操作而失效。

任何人试图用任何方式来读写不知密码的卡片或某一扇区都是徒劳无益的。

卡片应放在安全的地方，即不要放在离模块天线较近的地方。因为当模块对其它卡片执行某些指令时，有可能无意间对这一卡片进行了读/写等操作，从而操作卡片的失效。

### 5.3.6 带内部自动传送的值操作 1—Value (Cmd = 'J')

函数原型：uchar TX\_Value(uchar ValueMode, uchar Block, uchar idata \*Value, uchar Trans\_Block);

输入参数：ValueMode: 0xC0—减； 0xC1—加； 0xC2—恢复

Block: 卡内块地址，对该块进行值操作，取值范围：S50: 1~63; S70: 1~255

\*Value: 4 字节数据指针，用来存储减少值或增加值，当进行恢复操作时，该值为空值。

Value 是减少值或增加值存放的首地址，存放时，低地址存放高字节。

Trans\_Block: 传输块地址，取值范围：S50: 1~63; S70: 1~255。

输出参数：无

函数返回：执行命令后的状态。

功能描述：此函数对卡内的某一块进行加、减或数据备份，该块必须为值块格式，并支持自动传送。若卡块号与传输块号相同，则将操作后的结果写入原来的块内；若卡块号与传输块号不相同，则将操作后的结果写入传输块内，结果传输块内的数据被覆盖，原块内的值不变。当模式为“恢复”时，“值”无意义。

### 5.3.7 复位—Reset (Cmd = 'L')

函数原型：uchar TX\_Reset(uchar Msec);

输入参数：Msec: 取值 0~255，模块上射频电路关闭时间（以 ms 毫秒为单位），Msec = 0 时，一直关闭。

输出参数：无

函数返回：执行命令后的状态。

功能描述：该函数使模块上的射频电路关闭，关闭的时间由参数 Msec 指定，若 Msec=0，射频电路将一直处于关闭状态，一直到下一个 TX\_Request 命令到来。关闭射频电路能使天线内的所有卡复位。

### 5.3.8 挂起卡片—Halt (Cmd = 'D')

函数原型：uchar TX\_Halt(void)

输入参数：无

输出参数：无

函数返回：执行命令后的状态。

功能描述：将天线区所选择卡置为挂起状态。如果要进行重新选择，则应用 ALL 模式激活卡片。如果要进行重新激活,也可以将卡离开天线操作区再进入，或执行复位函数 TX\_Reset()。

主机→TX522 命令模式：

例如：挂起天线区域当前操作的卡片。

网络层数据：

RAddr	SAddr	CTYPE	CMD	Length	Info	BCC
0x01	0x00	0x02	0x44	0x00		0xb8

数据链路层数据帧：

0x82	0x20	0x01 0x00 0x02 0x44 0x00 0x38				0x83
------	------	-------------------------------	--	--	--	------

TX522→主机（响应模式）：

例如：地址为 0x01 的从机响应地址为 0x00 主机

网络层数据：

RAddr	SAddr	CTYPE	STATUS	Length	Info	BCC
0x00	0x01	0x02	0x00	0x00		0xfc

数据链路层数据帧：

0x82	0x20	0x00 0x01 0x02 0x00 0x00 0x7c				0x83
------	------	-------------------------------	--	--	--	------

## 6. 免责声明

- **开发预备知识**

TX®系列产品将提供尽可能全面的开发模板、驱动程序及其应用说明文档以方便用户使用，但也需要用户熟悉自己设计产品所采用的硬件平台及相关 C 语言的知识。

- **EMI 与 EMC**

TX®系列模块机械结构决定了其 EMI 性能必然与一体化电路设计有所差异。TX®系列模块的 EMI 能满足绝大部分应用场合，用户如有特殊要求，必须事先与我们协商。

TX®系列模块的 EMC 性能与用户底板的设计密切相关，尤其是电源电路、I/O 隔离、复位电路，用户在设计底板时必须充分考虑以上因素。我们将努力完善 TX®系列模块的电磁兼容特性，但不对用户最终应用产品 EMC 性能提供任何保证。

- **修改文档的权利**

东莞同欣智能保留任何时候在不事先声明的情况下对 TX®系列产品相关文档的修改权力。

- **ESD 静电放电保护**

TX®系列产品部分元器件内置 ESD 保护电路，但在使用环境恶劣的场合，依然建议用户在设计底板时提供 ESD 保护措施，特别是电源与 I/O 设计，以保证产品的稳定运行。安装 TX®系列产品，为确保安全请先将积累在身体上的静电释放，例如佩戴可靠接地的静电环，触摸接入大地的自来水管等。





## 7. 修订历史

版本	日期	原因
V1.00	2009/09/09	创建文档。
V1.1	2009/11/16	增加命令
V1.2	2011/04/01	增加指令

## 8. 销售信息

东莞市同欣智能科技有限公司

地 址：广东省东莞市石碣镇沙腰管理区林屋洲

邮 编：523292

销售电话：0769-86019851-168; 13652608930

技术支持：0769-86019851-138; 0769-86019853; 18666865339 QQ: 14754020

传 真：0769-86019852

网 址：[http:// www.TXRFID.com](http://www.TXRFID.com)

E-mail: [sales@TXRFID.com](mailto:sales@TXRFID.com) [support@TXRFID.com](mailto:support@TXRFID.com)