SAM9260 地铁用非接触 IC 卡大读卡机使用说明书

版本 1.16

2014 年 4 月 2 日

苏州市永兴电子有限公司

目录

1. 产品概要

- 本读卡机通过 RS232 或 USB 通讯协议与上位计算机进行通信，可对满足 ISO14443A 协议的非接触 IC 卡和上海模式卡进行读写等操作，与上位机通信协议简便稳定.
- 本读卡机基于 ARM9 处理器，最大时钟频率达到 210MHz，并且拥有大量的外部 Flash 和 SDRAM 扩展，非常适合使用嵌入式操作系统完成复杂的功能.

2. 读卡机规格

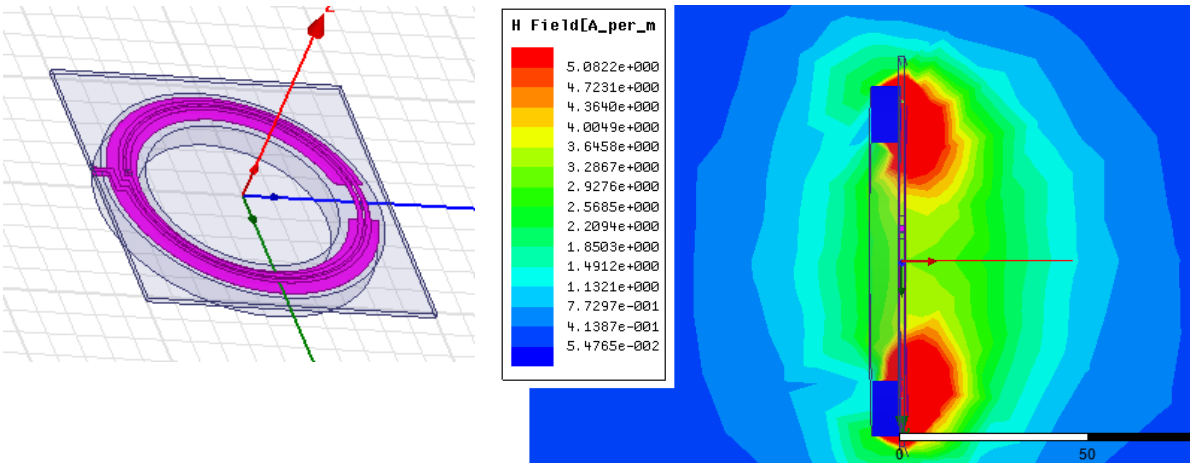
2.1 读卡机参数

读卡机硬件参数	
读卡机处理器	AT91SAM9260 ARM9 内核
处理器最大频率	210MHz
处理器内部 ROM	32Kbytes
处理器内部 RAM	8Kbytes
扩展并行 Flash	并行 NAND Flash(用于存储操作系统镜像和文件系统),标准尺寸为 256Mbits，最大可扩展至 2Gbits.
扩展串行 Flash	2 片串行 NOR Flash(用于存储用户自定义数据,如交易记录,黑名单等信息), 每片 Flash 标准尺寸为 128Mbits，最大可扩展至 2Gbits.
扩展 RAM	采用 SDRAM，标准尺寸为 256Mbits，最大可扩展至 512Mbits.
扩展 EEROM	内置 3KBytes DataFlash，可扩展 EEROM 或 FRAM 最大至 512Kbytes
操作系统支持	支持 Linux，WinCE 等操作系统
读卡机辅助处理器	NUC120LE3AN ARM CortexM0
实时时钟功能(RTC)	有,需要添加纽扣电池
RS232 / RS485 串口	有两个 DB9 插座(一个用于和上位机通信，另一个既可以和上位机通信，又可以连接到手机读写模块. 请参考 3.1 节和 4.3 节) 插座 J4 为通信串口，支持 RS232 或 RS485 插座 J6 为手机模块串口，支持 TTL 电平或 RS232
USB	3 个(两个 USB A 型插座,一个为 USB2.0 全速主机.另一个 USB2.0 全速设备. 另有一个 USB MiniB 插座,为 USB2.0 全速 HID 设备)
外接 SAM 卡插座	有,读卡机电路板上有两个 10pin 插座，可以连接到 SAM 卡板. SAM 卡板最多能插入 8 个 SAM 卡. 支持 ISO/IEC7816-1/2 标准 PPS 协议,可支持 9600—115200 的 SAM 卡
射频通道	2 个(如果增加一个射频开关，可以增至 3 通道)

SD 卡接口	有(标准 SD 或 MicroSD 卡插座, 支持 MMC 卡 3.11 标准和 SD 存储卡 1.0 标准)
以太网接口	有(RJ45 插座, 10/100M 以太网)
扩展通用 IO 插座	2 个,最大可扩展 10 个 GPIO 引脚,请参考 3.7 节
LED 状态显示	3 个,一个电源指示灯,两个用户可编程状态指示灯
蜂鸣器	有
机械参数	
读卡机主板尺寸	长 141.7mm*宽 90mm*高 15mm
读卡机主板定位孔	定位孔直径 3.5mm, 使用标准 M3 平头螺丝安装. 定位孔距板边沿 4mm
SAM 卡扩展板尺寸	长 74.5mm*宽 56.7mm*高 7mm
电气参数	
工作温度	-20℃~70℃
工作湿度	≤90%
电源电压	DC12V±10%
静态电流	220mA@12.0V
绝对最大电压	DC15V
最大功率损耗	4W
通信参数	
10/100M 以太网	10/100Mbps
USB 标准	USB2.0 Full Speed
USB 数据速率	12Mb/s or 1.5Mb/s
通信串口波特率	默认为 115200bps, 用户可自定义
辅助处理器 串口(UART2)波特率	默认为 38400bps 可设置为 9600,19200,57600,115200,230400,460800
辅助处理器 串口(UART2)参数	8 位数据位,1 位停止位,无奇偶校验
SD 传输速率	支持 4 位宽总线, 默认速度模式最大数据传输速率为 12.5Mb/s 高速模式下最大数据传输速率为 25Mb/s
射频参数	
射频协议	ISO14443 及 ISO/IEC18000-Part3
射频载波频率	13.56MHz
射频信号通讯速率	106 Kbps 可支持 212Kbps,424Kbps
近场磁场强度	天线表面磁场强度≤7.5A/m rms，5cm 处磁场强度≥1.5A/m rms
IC 卡标准	支持 NXP 的 Mifare Classic 系列（M1S50,M1S70,Ultralight）非接触 IC 卡 支持符合 ISO/IEC14443 TYPE A 标准的上海模式 Mifare 系列非接触 IC 卡 支持符合 ISO/IEC14443 TYPE A 标准的 CPU 卡 支持符合 ISO/IEC14443 TYPE B 标准的非接触 IC 卡

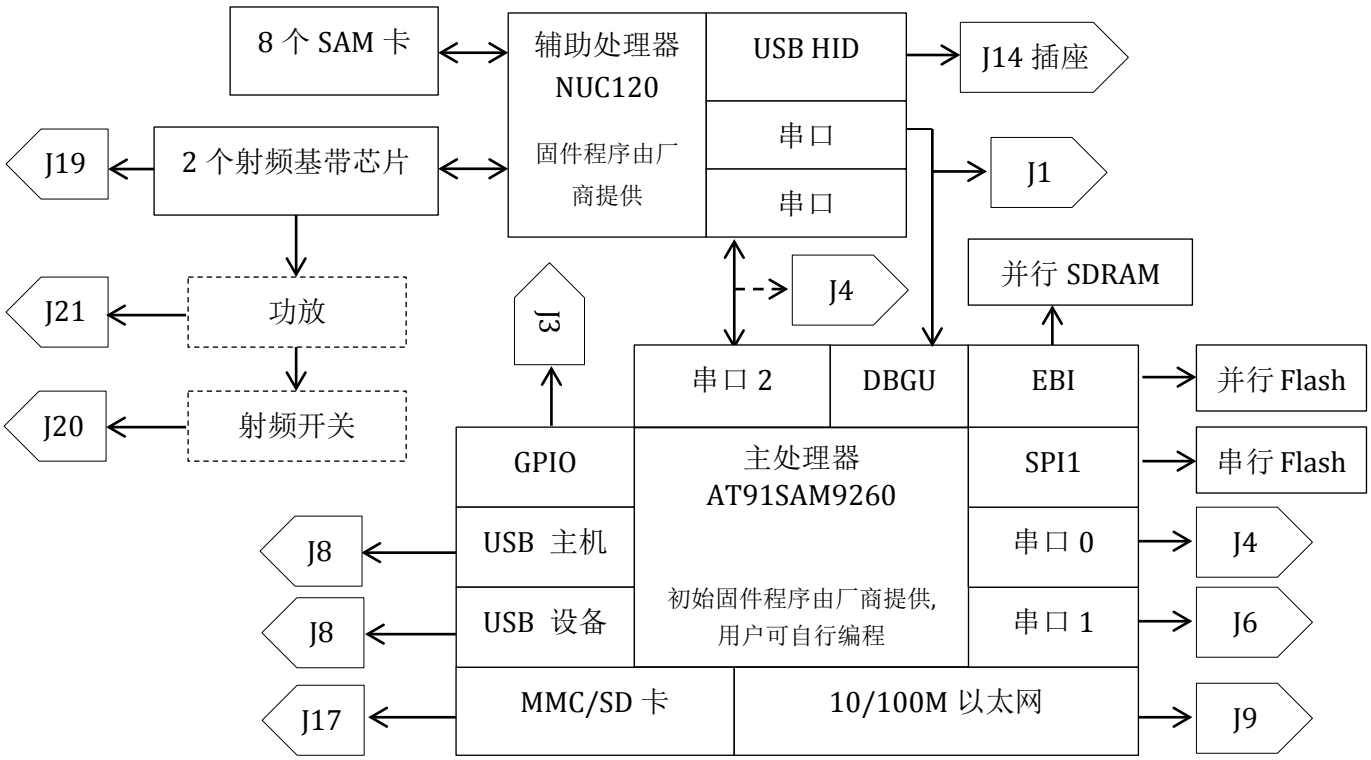
2.2　近场天线参数

本读卡机使用近场环状天线，经过阻抗匹配网络匹配至 50 欧姆．按照 ISO14443 标准，天线表面磁场强度应小于 7.5A/m 均方根，5cm 处磁场强度应大于 1.5A/m 均方根．仿真结果显示本产品天线表面磁场强度为 5.08A/m，5cm 处磁场强度为 1.85A/m，符合标准要求.

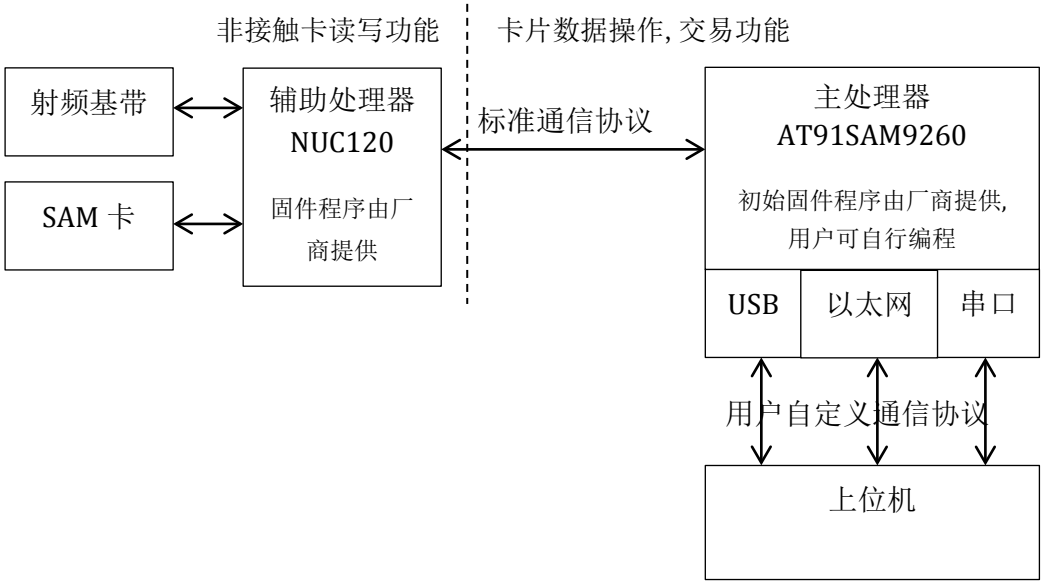


对于标准 Mifare 卡，本产品典型读卡距离为 8cm，最大读卡距离为 10cm.

2.3　读卡机原理框图



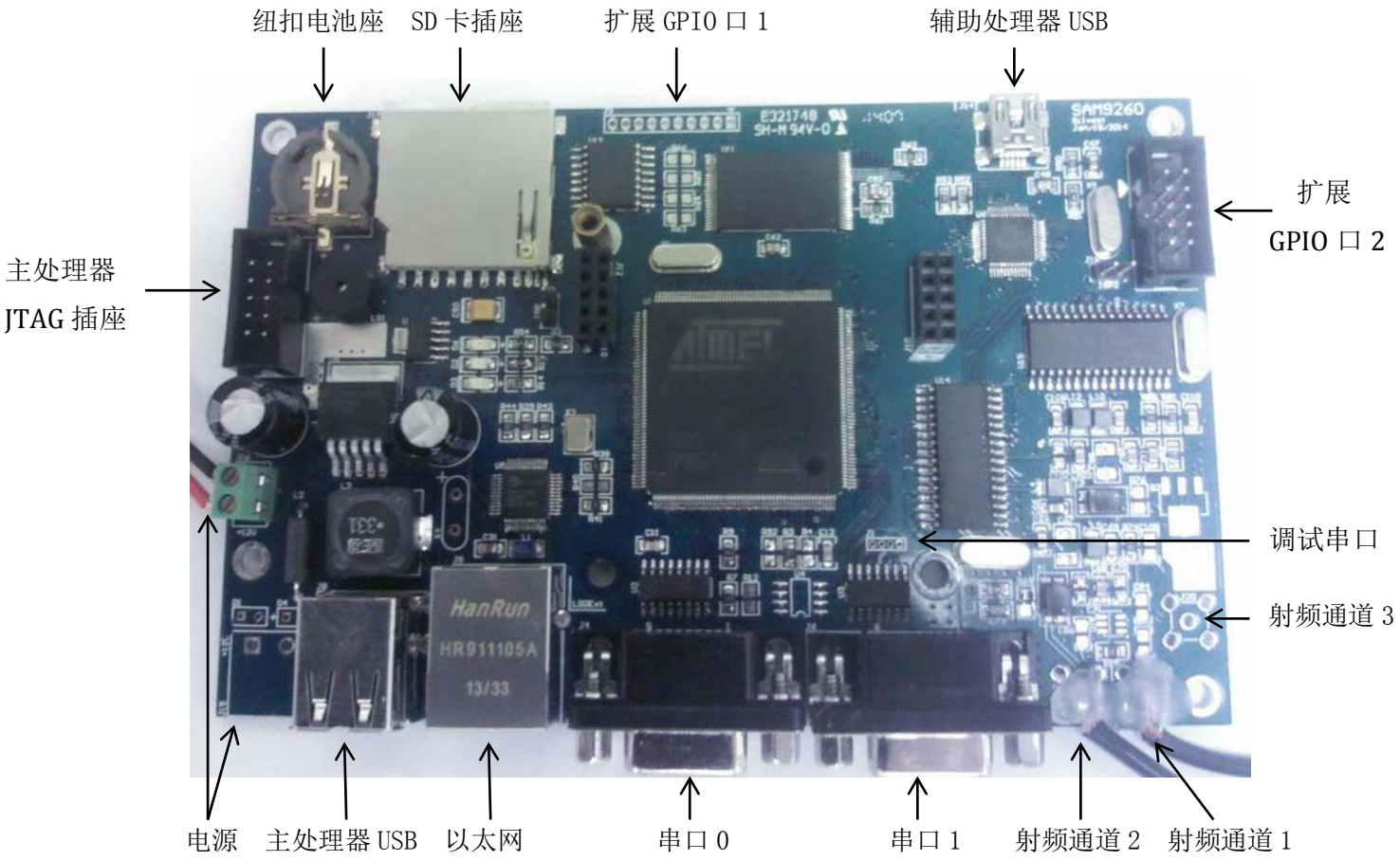
2.4 读卡机操作模型

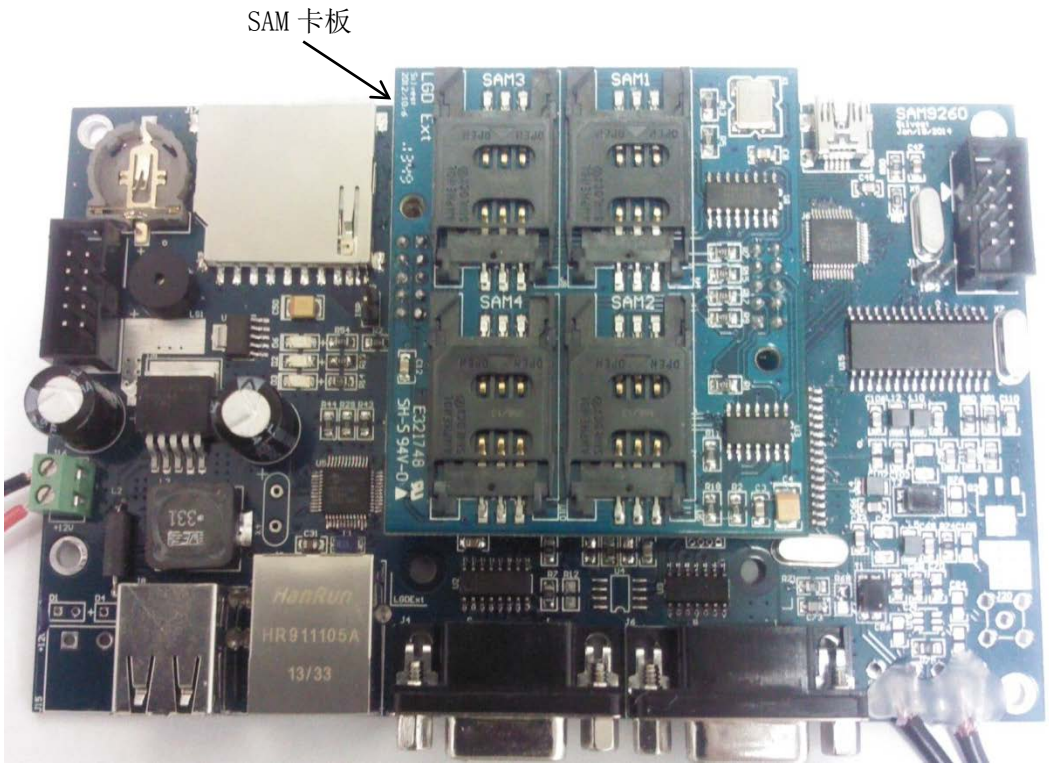


上图中，辅助处理器的程序由厂商提供，主要完成对射频基带和 SAM 卡的操作．与主处理器采用标准通信协议进行通信(请参考第 7 章)，此时主处理器就相当于它的上位机．用户可以自行给主处理器编程，以实现卡片的数据操作和交易功能．于此同时，主处理器程序通过操作 USB,以太网及串口与上位机进行通信.用户还可以自定义与上位机的通信协议.

2.5 读卡机机械结构

2.6 读卡机电路板结构


纽扣电池座
SD 卡插座
扩展 GPIO 口 1
辅助处理器 USB
扩展
GPIO 口 2
主处理器
JTAG 插座
调试串口
射频通道 3
电源
主处理器 USB
以太网
串口 0
串口 1
射频通道 2
射频通道 1

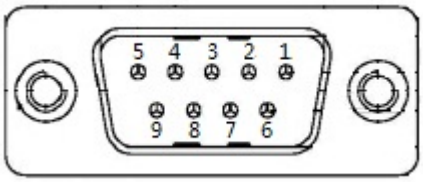

SAM 卡板
SAM3
SAM1
SAM4
SAM2
SAM9260
HanRun
HR911105A
13/33

3. 系统接口定义

本章定义了读卡机系统的硬件接口,包括插座引脚定义等.

3.1 RS232 串口定义

读卡机的串口使用标准 DB9 插座, 可以很方便地和计算机串口连接. 读卡机有两个 Female(孔)串口插座, 串口 0 用于和上位机通信, 插座编号为 J4, 引脚 9 通过一个 0.4A 自恢复保险丝接到 5V, 用于对外提供电源. 如有需要, 该串口还兼容 RS422/485 标准. 默认情况下带有一个 120 欧姆终端负载电阻, 该终端电阻可以根据用户需要改变. 具体引脚定义如下:



串口 0 信号	引脚	引脚说明	方向
TXD	2	读卡机→上位机	OUT
RXD	3	读卡机←上位机	IN
GND	5	地线	N/A
VCC	9	5V 电源	N/A
RS485_B(可选)	1	RS485 标准差分数据线	N/A
RS485_A(可选)	8		N/A

串口 1 既可以用于和上位机通信, 也可以与手机模块进行通信, 并支持 3.3V LVCMOS 电平. 插座编号为 J6, 引脚 9 通过一个 0.4A 自恢复保险丝接到 5V, 用于对外提供电源.引脚 4, 8 为从读卡机到手机模块的控制线.

- 与上位机通信时, R87,R88,R9 各有一个 0 欧电阻, 引脚如下:

串口 1 信号	引脚	引脚说明	方向
TXD	2	读卡机→上位机	OUT
RXD	3	读卡机←上位机	IN
OUT1	4	读卡机→手机模块	OUT
OUT0	8	读卡机→手机模块	OUT
GND	5	地线	N/A
VCC	9	5V 电源	N/A

- 与手机模块用 232 电平通信时，R19,R22,R9 各有一个 0 欧电阻，引脚如下：

串口 1 信号	引脚	引脚说明	方向
RXD	2	读卡机←上位机	IN
TXD	3	读卡机→上位机	OUT
OUT1	4	读卡机→手机模块	OUT
OUT0	8	读卡机→手机模块	OUT
GND	5	地线	N/A
VCC	9	5V 电源	N/A

- 与手机模块用 LVCMOS 电平通信时，R21,R22,R11 各有一个 0 欧电阻，引脚如下：

串口 1 信号	引脚	引脚说明	方向
RXD	2	读卡机←上位机(LVCMOS)	IN
TXD	3	读卡机→上位机(LVCMOS)	OUT
OUT1	4	读卡机→手机模块	OUT
OUT0	8	读卡机→手机模块	OUT
GND	5	地线	N/A
VCC	9	5V 电源	N/A

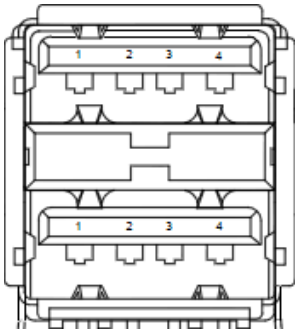
3.2 电源插座定义

读卡机的电压插座使用 4 芯航空插座，插座编号为 J15，插入时请注意方向和缺口．读卡机内部带有反接保护电路，在电源和地接反时，读卡机并不会损坏．但是，请注意输入电源电压，最大不能超过 15V．读卡机最低能在大约 8V 时工作，过低的电源电源会影响功放电路的正常工作，进而影响读卡机功能.

电源座引脚	定义	说明
1	DC12V	12V 正电源
2	DC12V	12V 正电源
3	GND	地
4	GND	地

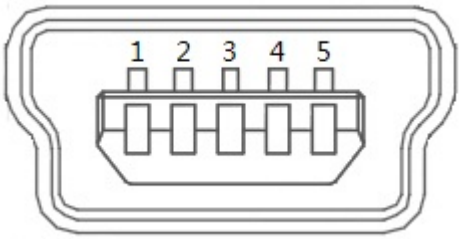
3.3 USB 插座定义

本读卡机有两个的 USB 插座. 插座编号为 J8 的双层 USB A 型插座连接到主处理器.其上面的插座为 USB2.0 全速主机, 电源能够提供 0.4A 电流. 下面的插座为 USB2.0 全速设备, 用于和上位机连接. 具体信息请参考 USB2.0 标准第 6 章.



双排 A 座引脚	定义	说明
上层 1	主机 VBUS	USB 5V 电源, 对外最大提供 0.4A 电流
上层 2	主机 D-	负数据线
上层 3	主机 D+	正数据线
上层 4	主机 GND	地
下层 1	设备 VBUS	必须由主机提供一个 5V 电源, 消耗电流不大于 10mA
下层 2	设备 D-	负数据线
下层 3	设备 D+	正数据线
下层 4	设备 GND	地

插座编号为 J14 的标准 USB Mini-B 插座连接到辅助处理器, 为 USB2.0 全速 HID 设备, 用于调试和与上位机通信.



Mini-B 座引脚	定义	说明
1	VBUS	USB 5V 电源
2	D-	负数据线
3	D+	正数据线
4	ID	未连接
5	GND	地

3.4 射频插座定义

读卡机的射频插座使用 SMA 90 度弯角母座，特征阻抗 50 欧姆. 插座编号分别为 J19 和 J21. 当用户需要时，可以添加一个射频开关，使得射频通道增加到 3 通道. 新增加的插座编号为 J20. J21 对应射频通道 1，J19 对应射频通道 2，J20 对应射频通道 3.

3.5 调试串口定义

调试串口连接到主处理器 AT91SAM9260 的 DBGU 上，用于调试程序. 该串口没有外部插座，插座编号为 J1，用户需要自行连接电荷泵芯片(例如 MAX3232)以连接到上位机. **注意：该调试串口的电平为 3.3V LVCMOS，请勿直接连接到串口使用的+3 至+15V 和 -3 至-15V RS232 电平. 否则会损坏芯片.**

调试串口引脚	定义	说明
1(方型过孔)	VDD3.3	3.3V 电源,无过流保护
2	DTXD	读卡机→上位机
3	DRXD	读卡机←上位机
4	GND	数字地

3.6 ISP 引脚定义

ISP 引脚用于在 RFIDBootstrapEx 进行系统引导时确保进入 SAM-BA Monitor，以便开始在系统编程(ISP). ISP 插座编号为 J2，连接到主处理器 AT91SAM9260 的 PB25 脚，Pin168 上. 在 RFIDBootstrapEx 中会检查 PB25 脚，如果该脚为低电平，则系统正常启动. 如果该脚为高电平，则进入 ISP 过程. PB25 脚默认为下拉，当短路该插座后，PB25 脚的状态为高电平. 有关 RFIDBootstrapEx 的详细信息,请参考 SAM9260 编程手册.

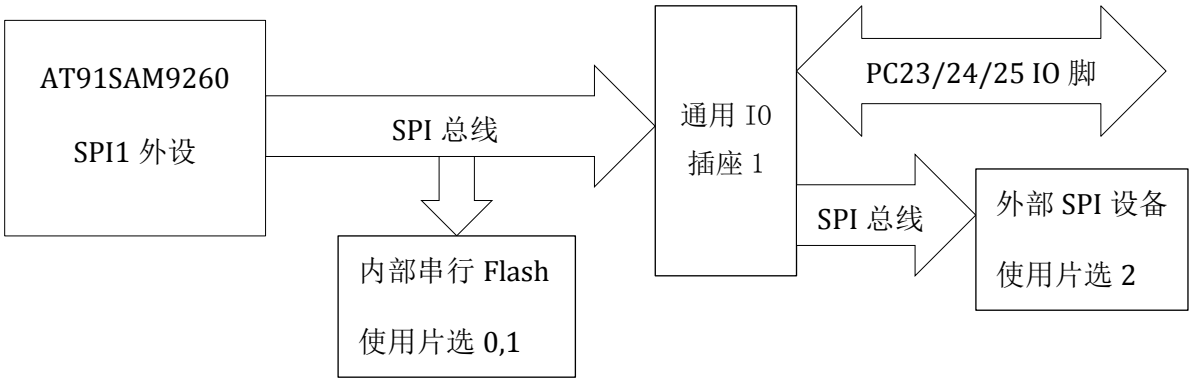
ISP 引脚	定义	说明
1(方型过孔)	PB25	PB25,GPIO 输入脚,有一个 4.7K 下拉电阻
2	VDD3.3	3.3V 电源

3.7 通用 IO 插座定义

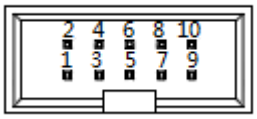
本读卡机共有两个通用 IO 插座，插座 1 编号为 J3，是 2mm 间距，10pin 单排直插插针插座.其引脚定义如下:

通用 IO 插座 1 引脚	定义	说明
1	VDD3.3	3.3V 电源,无过流保护
2	PC18/ SPI1_NPCS1	通用 IO 脚或 SPI1 片选脚
3	PC19/ SPI1_NPCS2	通用 IO 脚或 SPI1 片选脚
4	PC23	通用 IO 脚
5	PC24	通用 IO 脚
6	PC25	通用 IO 脚
7	SPI1_MISO	SPI1 外设主机输入脚
8	SPI1_CLK	SPI1 外设主机时钟脚
9	SPI1_MOSI	SPI1 外设主机输出脚
10	GND	数字地

注意到通用 IO 插座 1 的 2,3 脚既可以作为 GPIO 脚，也可以作为 SPI 总线的片选脚. 而 SPI1 总线还连接到读卡机内部的串行 Flash 芯片，**如果用户不需要连接到外部 SPI 设备，引脚 7,8,9 必须为不连接(NC)**.典型的通用 IO 插座 1 应用如下图所示.

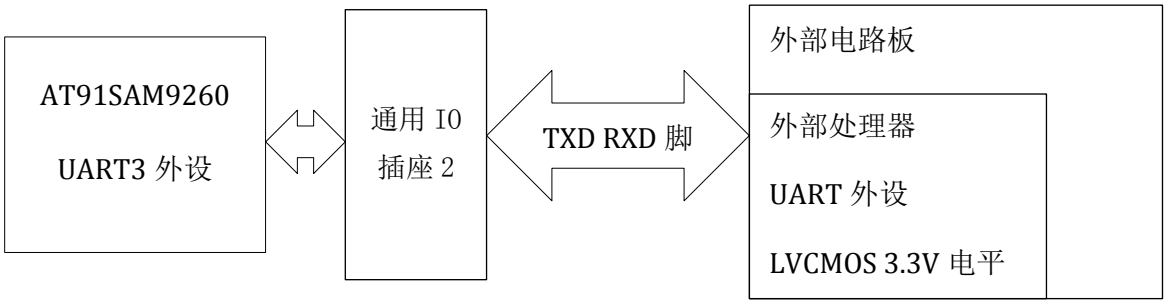


插座 2 编号为 J13，是 DC3 2.54mm 间距，10pin 双排直插插针插座．其引脚定义如下：



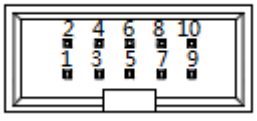
通用 IO 插座 2 引脚	定义	说明
1	GND	数字地
2	GND	数字地
3	NC	内部上拉，用户不得使用此脚
4	IO1/TXD3	通用 IO 脚/外设 UART3 的 TXD
5	NC	内部上拉，用户不得使用此脚
6	IO2/RXD3	通用 IO 脚/外设 UART3 的 RXD
7	NC	内部上拉，用户不得使用此脚
8	IO3	通用 IO 脚
9	NC	无连接
10	VDD3.3	3.3V 电源,无过流保护

通用 IO 插座 2 的 3,5,7 脚为读卡机内部使用，默认状态为上拉至 3.3V.用户不能连接任何信号到这 3 个引脚．第 4,6 脚既可以作为 GPIO 脚，也可以作为主处理器的 UART3 外设的 TXD 和 RXD 脚．**注意：第 4,6 脚的电平为 3.3V LVCMOS，请勿直接连接到串口使用的+3 至+15V 和 -3 至-15V RS232 电平．否则会损坏芯片．**典型的通用 IO 插座 2 应用如下图所示．



3.8 JTAG 插座定义

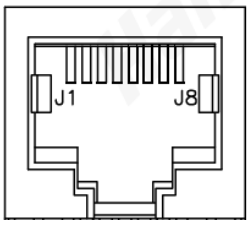
JTAG 插座编号为 J7，是 DC3 2.54mm 间距，10pin 双排直插插针插座．其引脚定义如下：



JTAG 插座引脚	定义	说明
1	TMS	JTAG 的 TMS 引脚
2	TCK	JTAG 的 TCK 引脚
3	RTCK	JTAG 的 RTCK 引脚
4	TDO	JTAG 的 TDO 引脚
5	nRST	读卡机系统复位引脚
6	VDD3.3	3.3V 电源,无过流保护
7	nTRST	JTAG 的复位引脚
8	TDI	JTAG 的 TDI 引脚
9	GND	数字地
10	GND	数字地

3.9 以太网插座定义

以太网插座使用 RJ45 插座，连接器为 8J8C 类型，详细描述请参考 ISO/IEC 15018 和 ISO/IEC 11801 标准. 插座编号为 J9，其引脚定义如下:



以太网插座引脚	定义
J1	TX+
J2	TX-
J3	RX+
J4	SHIELD
J5	SHIELD
J6	RX-
J7	SHIELD
J8	SHIELD

4. 外设连接

4.1 内存映射

本节定义了主处理器AT91SAM9260的内部内存映射，该芯片的BMS引脚连接到VDD3.3，因此在硬件复位时，总是引导到片内ROM. 如果软件复位,且MATRIX_MRCR寄存器的RCB位均为1，则REMAP=1，引导到片内SRAM中.该芯片的片选1连接到外部SDRAM，片选3连接到外部NAND Flash. 因此EBI_CSA寄存器的状态应设置为0x0001000A.

起始地址	中止地址	尺寸	描述
0x00000000	0x00100000	32K或4K字节	引导内存映射
0x00100000	0x00108000	32K字节	内部ROM
0x00200000	0x00201000	4K字节	内部SRAM0
0x00300000	0x00301000	4K字节	内部SRAM1
0x00500000	0x00504000	16K字节	USB主机寄存器映射
0x20000000	0x24000000	16M至64M字节	扩展SDRAM
0x40000000	0x4FFFFFFF	32M至256M字节	扩展NAND Flash
0xF0000000	0xFFFFFFFF	N/A	系统和外设寄存器映射

4.2 引脚描述

本节定义了主处理器AT91SAM9260的引脚定义. 该芯片的PIO_PSR寄存器用于设置GPIO引脚的功能，如果为1则作为IO脚，如果为0则作为外设引脚. PIO_OSR寄存器用于设置IO引脚的方向，如果为1则作为输出脚.PIO_ABSR寄存器用于设置外设引脚的功能,如果为0,则连接到外设A. 在下表中，寄存器设置依次为PIO_PSR,PIO_OSR和PIO_ABSR的对应位，如果为0/0/1，就是指该引脚设置为外设引脚，连接到外设B.

端口	引脚	功能	寄存器设置(依次为PIO_PSR,PIO_OSR和PIO_ABSR的对应位)	描述
PA0	179	MCDB0	0/0/1	连接到SD卡. SD_DETECT为GPIO输入脚,用于检测是否存在SD卡. 当该引脚为低电平时，存在SD卡.
PA1	180	MCCDB	0/0/1	
PA3	182	MCDB3	0/0/1	
PA4	183	MCDB2	0/0/1	
PA5	184	MCDB1	0/0/1	
PA8	189	MCCK	0/0/0	
PB27	172	SD_DETECT	1/0/0	

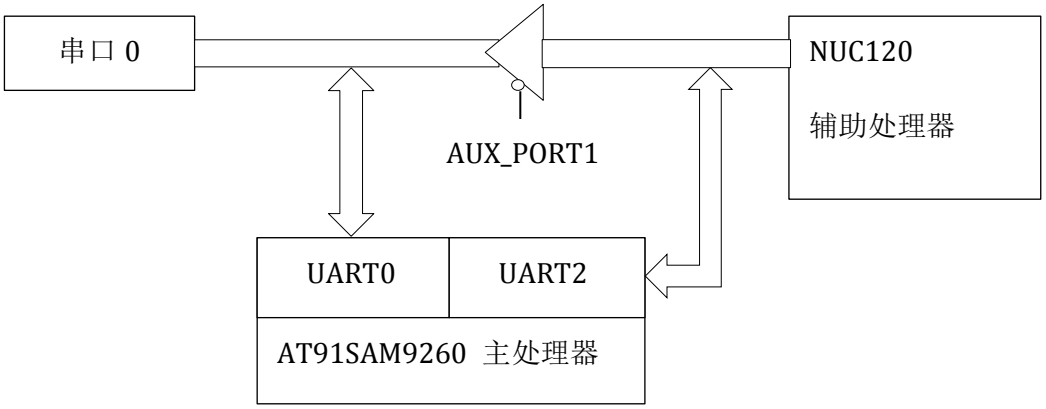
PA7	186	ETH_MDINT	1/0/0	连接到以太网物理层芯片. ETH_MDINT 为 GPIO 输入脚,当状态改变时,该引脚为低电平, 触发一个中断.
PA10	191	ETX2	0/0/1	
PA11	192	ETX3	0/0/1	
PA12	193	ETX0	0/0/0	
PA13	194	ETX1	0/0/0	
PA14	195	ERX0	0/0/0	
PA15	196	ERX1	0/0/0	
PA16	197	ETXEN	0/0/0	
PA17	198	ERXDV	0/0/0	
PA18	201	ERXER	0/0/0	
PA19	202	ETXCK	0/0/0	
PA20	205	EMDC	0/0/0	
PA21	206	EMDIO	0/0/0	
PA22	207	ETXER	0/0/1	
PA25	2	ERX2	0/0/1	
PA26	3	ERX3	0/0/1	
PA27	4	ERXCK	0/0/1	
PA28	7	ECRS	0/0/1	
PA29	8	ECOL	0/0/1	
PA23	208	TWD	0/0/0	连接到 I^2C 总线
PA24	1	TWCK	0/0/0	
PB0	9	SPI1_MISO	0/0/0	连接到SPI总线, 片选 0 连接到串行 Flash
PB1	10	SPI1_MOSI	0/0/0	
PB2	11	SPI1_SPCK	0/0/0	
PB3	12	SPI1_NPCS0	0/0/0	
PB4	15	TXD0	0/0/0	连接到串口 0, 插座编号为 J4
PB5	16	RXD0	0/0/0	
PB6	17	TXD1	0/0/0	连接到串口 1, 插座编号为 J6
PB7	18	RXD1	0/0/0	
PC9	60	OUT0	1/1/0	
PC8	61	OUT1	1/1/0	
PB8	19	TXD2	0/0/0	连接到辅助处理器串口
PB9	20	RXD2	0/0/0	
PB14	21	DRXD	0/0/0	连接到调试串口, 插座编号为 J1
PB15	22	DTXD	0/0/0	
PB10	161	IO1 或 TXD3	1/X/0 或 0/0/0	连接到通用 IO 插座 2, 插座编号为 J13
PB11	162	IO2 或 RXD3	1/X/0 或 0/0/0	
PB20	163	IO3	1/X/0	
PC5	67	USB_CNX	1/0/0	连接到 USB 设备,用于检测是否有主机连接
PC13	56	nBUSY	1/0/0	连接到 NAND Flash, 用于判定Flash芯片操作是否完成和片选.
PC14	59	NCS3/NANDCS	0/0/0	

PC23	137	PC23	1/X/0	连接到通用 IO 插座 1, 插座编号为 J3. 如果存在第二片 SPI Flash, 则 PC18 连接到该芯片的片选
PC24	138	PC24	1/X/0	
PC25	139	PC25	1/X/0	
PC18	130	PC18/SPI1_NPCS1	1/X/0 或 0/0/1	
PC19	131	PC19/SPI1_NPCS2	1/X/0 或 0/0/1	
PB29	176	LED_CTRL1	1/1/0	分别连接到 LED 的 D1, D2 和 D3, D4. 引脚为高电平时, LED 点亮
PB30	177	LED_CTRL2	1/1/0	
PC28	142	nWP	1/1/0	连接到 NAND Flash, 该引脚电平如果为低, 则 Flash 处在写保护状态
PC29	143	nWP2	1/1/0	连接到串行 Flash, 如果 nWP2 引脚电平为低, 则处在写保护状态. 如果 SPI_HOLD 引脚电平为低, 则 SPI 总线处在停止状态.
PC26	140	SPI_HOLD	1/1/0	
PA6	185	WP3	1/1/0	连接到 EEROM, 该引脚电平如果为高, 则 EEROM 处在写保护状态
PB19	28	AUX_PORT1	1/1/0	用于控制串口 0 的连接, 请参考 4.3.1 节
PC11	57	RS485_TXEN	1/1/0	如果使用 RS485 总线, 这两个引脚则用于控制输入和输出使能.
PC10	58	RS485_RXEN	1/1/0	
PB21	164	BEEP	1/1/0	连接到蜂鸣器. 当该引脚为高电平时, 蜂鸣器响.

4.3 外设描述

4.3.1 串口 0 连接

串口 0 不仅可以连接到 AT91SAM9260 的外设 UART0, 也可以连接到辅助处理器. 当串口 0 连接到辅助处理器时, 用户可以对辅助处理器通过通信协议直接进行操作. 其结构如下:



当 AUX_PORT1 引脚为高电平时，外设 UART0 连接到串口 0，外设 UART2 连接到辅助处理器. 然而当 AUX_PORT1 引脚为低电平时，用户需要关闭 UART0，UART2 外设，将引脚设置成输入 IO 脚. 此时，辅助处理器的 UART 就会和串口 0 相连. AUX_PORT1 引脚有上拉电阻，默认为高电平.

AUX_PORT1	串口 0	辅助处理器串口
1	连接到外设 UART0	连接到外设 UART2
0	PB4,PB5,PB8,PB9 引脚置为输入状态.	辅助处理器串口连接到串口 0

4.3.2 RS485 连接

如果串口 0 使用 RS485，而非 RS232 标准，则用户可以使用引脚 RS485_TXEN 和引脚 RS485_RXEN 来控制 485 电荷泵芯片的输入输出使能. 这两个引脚的逻辑如下表所示. 当 RS485_RXEN 为高，而 RS485_TXEN 为低电平时，485 芯片进入低功耗状态.当串口 0 使用 RS485 标准时，R12 有一个 0 欧电阻.

引脚	状态	485 芯片功能
RS485_TXEN	0	Rs485 输出禁用
	1	Rs485 输出使能
RS485_RXEN	0	Rs485 输入使能
	1	Rs485 输入禁用

注意到，电阻 R10 为一个 120 欧姆终端负载电阻. 根据 RS485 总线标准，在两个总线终端需要加入该负载电阻. 但是不处在终端的设备不能带有该电阻，否则会造成双绞线阻抗不匹配. 默认情况下，本读卡机作为一个 RS485 总线终端，这个电阻是存在的. 如果用户需要去除该电阻，需要在生产之前告知厂商.

4.3.3 串口 1 连接

下表显示了串口 1 在不同状态下，电阻连接情况.

状态	R9	R11	R19	R21	R22	R87	R88
与上位机通信,使用 RS232 电平	√					√	√
与手机模块通信,使用 RS232 电平	√		√		√		
与手机模块通信，使用 LVCMOS 电平		√		√	√		

5. 系统引导

系统复位后，AT91SAM9260 会开始执行片上 ROM 的代码，试图寻找有效的程序并将程序载入片上 SRAM. 一旦完成程序载入，会将 SRAM 映射到地址 0x00000000，并从 0x00000000 开始运行. 关于 ROM 引导程序，请参考 AT91SAM9260 数据手册 第 13 章.

5.1 标准引导

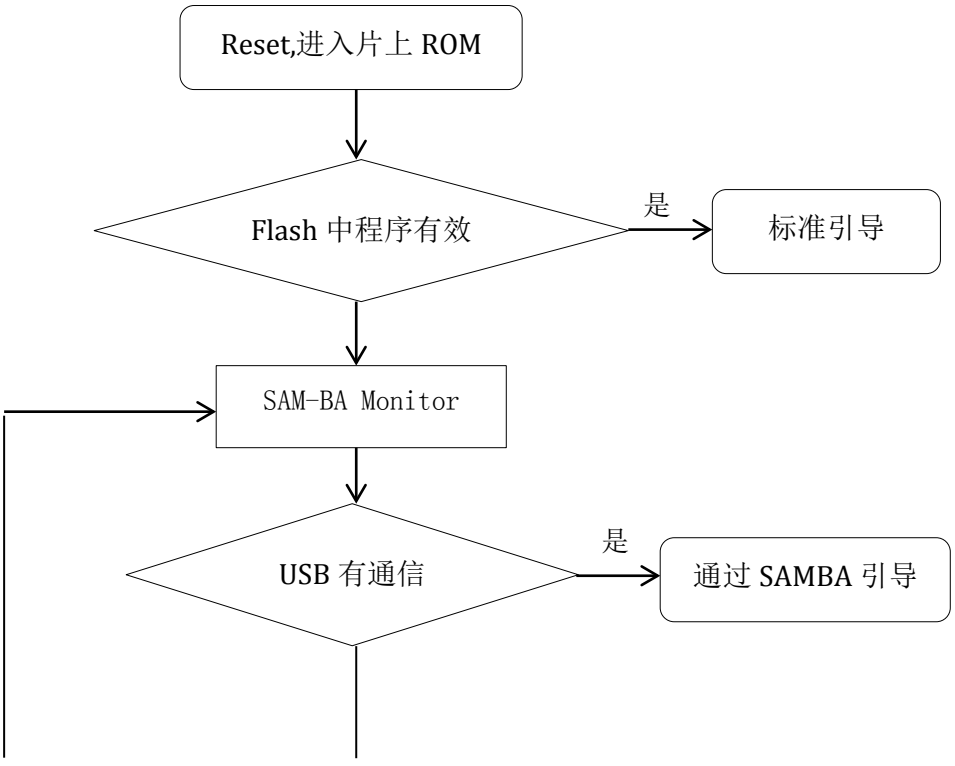
当 NAND Flash 中有自定义 RFIDBootstrapEx 启动程序时，进入该引导过程. 通常情况下，RFIDBootstrapEx 会将 U-Boot 载入 SDRAM，并在 SDRAM 中运行程序. 而 U-Boot 则负责载入 Linux 操作系统. 详细信息请参考 SAM9260 编程手册.

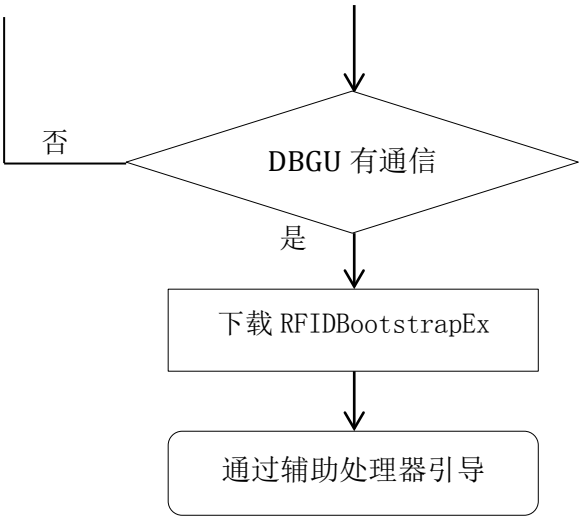
5.2 通过 SAM-BA 引导

当 NAND Flash 中并没有 RFIDBootstrapEx 启动程序时. ROM 中的 Loader 会进入 SAM-BA Monitor，检查调试串口和 USB 设备是否有信号. 此时如果用户通过 USB 或串口连接到板子上，则可以通过 SAM-BA 程序下载并运行的程序. 关于使用 SAM-BA，请参考 SAM Boot Assistant (SAM-BA) User Guide.

5.3 通过辅助处理器引导

当 NAND Flash 中并没有 RFIDBootstrapEx 启动程序时. ROM 中的 Loader 会进入 SAM-BA Monitor，此时辅助处理器可以通过 DBGU 调试口和 ROM 中的 Loader 通信，下载一个 RFIDBootstrapEx，再通过这个 RFIDBootstrapEx 从调试口将要运行的程序下载到 SDRAM 中,如下图所示.





一个典型的通过辅助处理器引导流程发生在出厂自检阶段. 一小段用于测试 AT91SAM9260 芯片的程序被放置在辅助处理器的 Flash 中. 当辅助处理器执行自检命令时, 它首先将 RFIDBootstrapEx 通过 ROM 中的 SAM-BA Monitor 下载入 SRAM 中. 再与 RFIDBootstrapEx 通信, 将这段测试程序下载到 SDRAM 中, 并跳转到 SDRAM 执行测试.

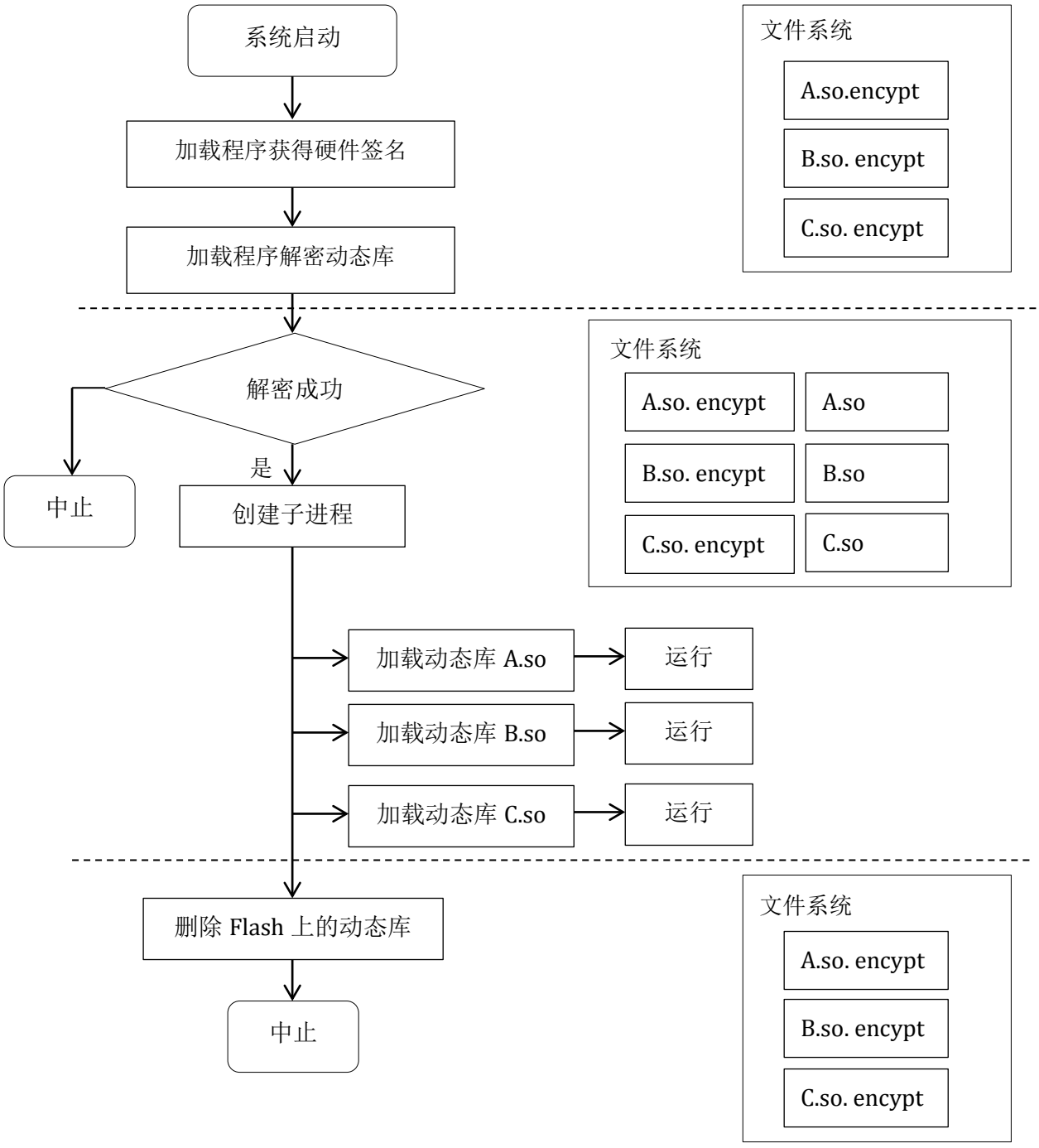
6. 程序加密与验证

运行操作系统的嵌入式系统并不特别适合加密, 主要原因是操作系统和文件系统都被放置在外部 Flash 中, 而外部 Flash 并不是加密的. 例如在某些 Linux 项目中, 系统要运行的程序被直接放在根目录下, 使用启动脚本在开机后运行. 这样根本毫无保密性可言, 只需要连接 Linux 调试串口即可下载程序. 本系统提供了一些加密与验证的解决方案.

6.1 硬件签名

辅助处理器提供一个硬件签名命令, 该命令会返回一个 16 字节硬件签名, 这个签名对每一台读卡机都是唯一的. 辅助处理器在初始化过程中会检查该签名的有效性, 如果签名无效, 辅助处理器会停止运行. 辅助处理器的 Flash 是经过加密的, 即使有人进行了解密, 将辅助处理器的固件程序烧写入另一台读卡机的辅助处理器, 由于硬件签名不同, 辅助处理器不会正常工作, 这样就保证了固件程序的安全性.请参考 8.40 节.

用户在操作系统的程序可以通过该硬件签名进行加密, 以保证安全性. 以一个需要运行 3 个程序的基于 Linux 系统的读卡机为例. 在 Linux 启动后, 在初始化脚本中, 运行一个加载程序. 这个加载程序首先读取硬件签名, 用它将需要运行的程序或动态库解密. 如果解密正确,这个加载程序调用 fork 创建出 3 个子进程. 在这 3 个子进程中延迟链接动态库, 并调用动态库中的代码. 加载程序则删除位于 Flash 上的动态库, 因为此时 RAM 上已经有了这三个动态库的副本.注意到由于硬件签名被用来给文件加密, 在不同读卡机上的 encrypt 文件内容都是不同的.

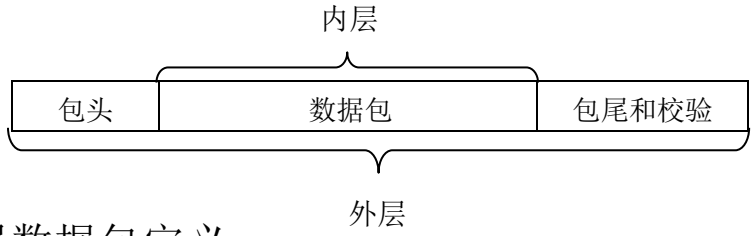


6.2 验证引导

另一种保证代码安全性的方法是验证引导，即在引导进入操作系统之前进行验证．如果验证失败则不能进入操作系统．一个典型的方案就是修改 UBoot，在其中加入验证代码．这样 UBoot 在启动时首先需要验证硬件签名，验证成功后才允许将 Linux 系统镜像复制到 SDRAM 中并执行．如果验证失败，则系统不能成功引导．有关 UBoot 移植的详细信息，请参考 SAM9260 编程手册．

7. 通信协议

本通信协议适用于辅助处理器的通信，包括串口和USB HID设备. 串口的通信波特率为38400, 8位数据位, 1位停止位, 无奇偶校验. HID设备的VID为0x0532, PID为0x5201. 通信协议分为两层，内层为数据包定义，外层为通信协议. 外层的通信协议封装了内层的数据包. 其中4.1节描述内层数据包的结构，4.2至4.3节描述两种不同的外层数据包格式.



7.1 内层数据包定义

数据包格式:

选择命令	命令	长度段1	长度段2	数据段	帧分隔符
CmdSel	Command	Length1	Length2	Data	FS
1Byte	1Byte	1Byte	3 Bytes	Variable	1Byte

选择命令

选择命令字节(CmdSel)指示了整个数据包的格式.

Bit#	Name	Description
7	Request	0: Request数据包为0 1: Response数据包为1
6	Length Enable	0: 长度段1和2均不存在 1: 长度段存在
5	Response Flag	0: 选择命令字节CmdSel的bit7始终为0 1: 选择命令字节CmdSel的bit7有意义
4	NFS	0: 数据包末尾的帧分隔符有效, FS为0x1C 1: 帧分隔符不存在
3-0	Parameter	可以被用作范围在0x00至0x0F的一个参数.

命令代码

命令字节(Command)指示了该数据包将执行的命令，0x7F以下某些保留命令为读卡机内部测试使用，用户不应使用这些命令. 0x80至0xFF是保留命令，用于未来扩展. 任何对被锁定命令或是非法命令的操作都会返回NACK应答包.

命令	命令代码	命令	命令代码	命令	命令代码
保留	0x00	SAM 卡复位	0x21	读取内存字节	0x37
延时写入 M1 卡	0x01	SAM 卡 APDU 命令	0x22	保留	0x38-0x40
延时读取 M1 卡	0x02	辅助处理器引导	0x23	写入调制芯片 EEROM	0x41
读取状态	0x04	设置 USB 模式	0x24	读取调制芯片 EEROM	0x42
立即写入 M1 卡	0x05	写入 USB 数据包	0x25	M1 卡初始化钱包	0x43
立即读取 M1 卡	0x06	读取 USB 数据包	0x26	M1 卡读钱包	0x44
写入 DataFlash	0x07	设置调制模式	0x27	M1 卡钱包充值	0x45
读取 DataFlash	0x08	寻卡	0x28	M1 卡钱包扣款	0x46
关闭射频	0x09	CPU 卡初始化	0x29	M1 卡备份钱包	0x47
保留	0x10	CPU 卡 APDU 命令	0x2A	UltraLight 卡写块	0x48
立即写入 M1 卡,无保护	0x11	M1 卡写入块	0x2B	UltraLight 卡读块	0x49
立即读取 M1 卡,无保护	0x12	M1 卡读取块	0x2C	M1 卡写入块,无密钥保护	0x4A
保留	0x13-0x19	M1 卡写入扇区	0x2D	M1 卡读取块,无密钥保护	0x4B
芯片重置	0x1A	M1 卡读取扇区	0x2E	读取硬件签名	0x4C
电路检测	0x1B	休眠 ISO14443 卡	0x2F	引导编程	0x4D
保留	0x1C-0x1D	保留	0x30-0x32	保留	0x4E-0xFF
查询串口参数	0x1E	写入内存	0x33		
设置串口参数	0x1F	读取内存	0x34		
保留	0x20	写入内存字节	0x36		

长度段

长度段分为两个部分，表示后面的数据段实际长度. 如果选择命令字节(CmdSel)的 bit6 为 0，则长度段不存在. 如果长度段 1(Length1)不为 0xFF，则 3 字节的长度段 2(Length2)不存在. 反之，数据部分实际长度取决于 Length2.

长度段例子:

选择命令	长度段 1	长度段 2	实际长度
Length Enable=0	N/A	N/A	可变
Length Enable=1	0x04	N/A	4 字节
	0x10	N/A	16 字节
	0xFF	0x000010	16 字节
	0xFF	0x000110	272 字节

帧分隔符段

有两种情况帧分隔符段为空，NFS=1 或是精简可变长包. 当接收到精简可变长包时，帧分隔符段始终为空并且在返回数据包中 CmdSel 的 NFS 位始终为 0. 当接收到基础可变长包时，帧分隔符段的存在与否取决于选择命令字节 CmdSel 的 NFS 位.

7.2 基础可变长包通信协议

报文字符

STX 用于报文的起始位置, ETX 用于报文的结束. DLE 用于报文内出现特殊字符时的转义. ENQ 用于询问是否可以发送一个命令. ACK 和 NAK 用于确认数据包发送是否正确.
正转义指的是 STX、ETX 两个字符的前面必须插入 DLE, 而数据中出现的 STX 和 ETX 则不需要插入. 报文控制字符遵循 JIS-X-0211 标准, 具体如下:

报文控制字符	编码
STX (Start of Text)	0x02
ETX(End of Text)	0x03
DLE(Data link escape)	0x10
ENQ(Enquiry)	0x05
ACK(Acknowledge)	0x06
NAK(Negative acknowledge)	0x15
FS(File Separator)	0x1C
BUSY(Busy)	0x14

数据包格式

数据包格式为正转义,校验值可以为前置或后置, 下位机程序在收到请求数据包时,会动态判断其格式,返回相对应的数据包.校验值的前置和后置取决于数据长度的最高 4 位.
传输的数据为大尾端格式.

正转义, 校验值前置:

STX	数据长度	内层数据包	校验值	ETX
0x1002	2Byte	可变长	可变长	0x1003

正转义, 校验值后置:

STX	数据长度	内层数据包	ETX	校验值
0x1002	2Byte	可变长	0x1003	可变长

数据长度

数据长度为两个字节, 表示内层数据包的实际长度, 不包括校验值. 其最高四位指示了校验值的类型, 如下表所示. 下位机支持这 8 种校验算法的任意一种, 用户在上位机编程时可根据需要选择任意一种即可.

Bit 15-12	指示校验值的类型(见下表)
Bit 11-0	内层数据包的长度

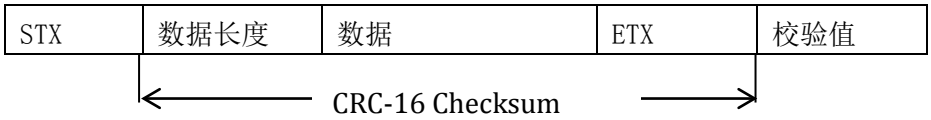
校验值的类型:

校验值编码(Binary)	校验值类型	长度
0000	CRC-16 校验值后置，不包含包头	2Bytes
0001	CRC-16 校验值后置，包含包头	2Bytes
0010	CRC-16 校验值前置，不包含包头	2Bytes
0011	CRC-16 校验值前置，包含包头	2Bytes
0100	XOR 校验，异或 0xFF	1Byte
0101	XOR 校验，不异或 0xFF	1Byte
0110	模为 8 位的加法校验	1Byte
0111	模为 16 位的加法校验	2Bytes

校验值

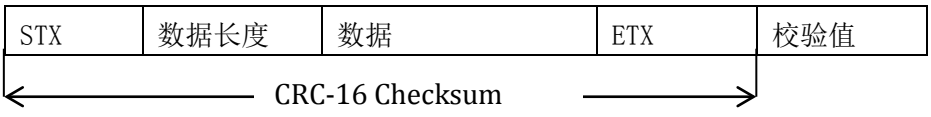
在基础可变长包的协议中，校验范围包含转义字符 DLE.例如在正转义，校验值编码为 b0000 时，协议使用 CRC-16 校验值后置，不包含包头(如下图 a 所示)．其中 CRC 校验范围包含了 ETX．由于是正转义,ETX 为 0x1003，此时校验值也包括 0x10 (DLE).

a) CRC-16 校验值后置，不包含包头

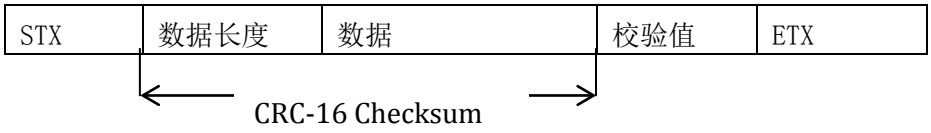


CRC16 使用 CRC-16-CCITT 标准，冗余校验多项式为 x^16+x^12+x^5+x^1．以 MSB 优先代码表示为 0x1021，又称 Kermit 算法 或 CRC-16/CCITT-TRUE．请注意，该 CRC16 校验和 USB 中使用的 CRC-16-ANSI 多项式不同，因此校验结果也不同．CRC16 的算法较多，请勿将此校验算法和其他 CRC-16 算法混淆.

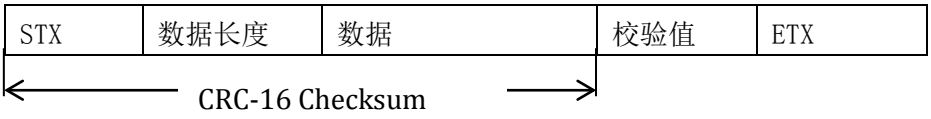
b) CRC-16 校验值后置，包含包头



c） CRC-16 校验值前置，不包含包头



d） CRC-16 校验值前置，包含包头



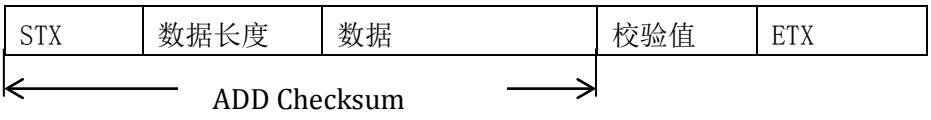
e） XOR 校验，异或 0xFF

使用异或校验时，校验值前置．具体校验值为 0xFF 逐字节异或从包头 STX 开始的数据，直到内层数据包的结束．初始值为 0xFF.

f） XOR 校验，不异或 0xFF

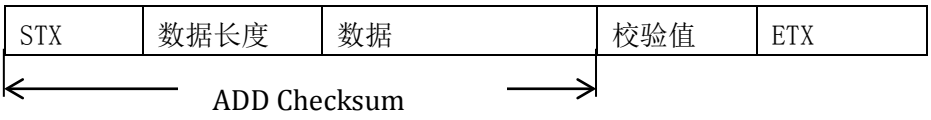
使用异或校验时，校验值前置．具体校验值为 0x00 逐字节异或从包头 STX 开始的数据，直到内层数据包的结束．初始值为 0x00.

g） 模为 8 位的加法校验



使用加法校验时，校验值前置．具体校验值为逐字节从包头 STX 开始的数据，一直加到数据段的结束．加法计算的结果取 8 位模，即位与上 0xFF.

h） 模为 16 位的加法校验



使用加法校验时，校验值前置．具体校验值为逐字节从包头 STX 开始的数据，一直加到数据段的结束．加法计算的结果取 16 位模，即位与上 0xFFFF.

7.3 精简可变长包通信协议

精简可变长包通信协议在上位机发送完命令包后，下位机并不返回应答包(除了发送包的绝对长度为 0，即如果发送包为 0x0203，返回 NACK 应答包 0x1015)，而是直接返回命令响应包．精简可变长包协议的内层数据包略有不同，其内层数据包如下:

命令代码	命令重发序号	命令参数
Command	Resend Index	Data
1Byte	1Byte	可变长

这相当于没有了选择命令字节(CmdSel)，也没有长度段和帧分隔符．但是增加了命令重发序号，该值表示该命令重发的次数，初次发送为 0x00，每次重发该值均加一．如果设备在发出命令报文后的一段时间内没有收到应答报文，则可以进行重试，重试时应重发相同的命令报文，并在命令重发序号中指明重发报文的重发序号。读写器收到后，如确认该命令报文确实与最近收到的命令报文相同，除发送与上一次相同的应答报文（但重发序号为当前报文中的值）外，不进行任何操作。

精简可变长包通信协议的外层数据包使用负转义，校验值前置．但是数据长度只有 1 个字节，不包含插入的转义字符．负转义指如果在报文中出现诸如 0x02、0x03、0x10 数据而非 STX、ETX、DLE 时，必须插入 DLE．所有插入的 DLE 字符应在接收处理过程中去除且不增加报文长度。负转义仅对 STX,ETX 和 DLE 三个报文控制字符有效.

精简可变长包通信协议使用模为 8 位的加法校验．校验的范围不包含插入的转义字符 DLE,校验范围从数据长度字节到数据区，不包含 STX 和 ETX．校验值如果为 STX, ETX 或是 DLE,则需要进行转义，如下所示.

STX	数据长度	数据	Add 校验值	ETX
0x02	1Byte	可变长	1Byte	0x03

例如，内层数据包为两个字节 0x0100 时，数据长度的值为 0x02，需要转义．校验值为数据长度加上每个数据字节(不包含 DLE)，于是校验值为 0x03，需要转义.

STX	数据长度	数据	Add 校验值	ETX
0x02	0x1002	0x0100	0x1003	0x03

7.4 通信方式与询问

本节主要描述协议的通信方式，适用于基础可变长包．精简可变长包协议只能使用下文中提到的命令模式，不支持询问． 精简可变长包协议也不会发送应答包.

7.4.1 应答和询问

通信方式主要以主从模式为主，通常情况下，上位机为 master，下位机为 slave．上位机为命令的发起者，即发送一个命令包，下位机则返回一个应答包，如果命令执行成功还返回一个响应命令包．不管是使用正转义还是负转义，返回的应答包都包含 DLE(0x10).

标准应答包和询问包:

ACK 应答包	0x10	0x06
NACK 应答包	0x10	0x15
Busy 应答包	0x10	0x14
ENQ 询问包	0x10	0x05

数据包分为 4 类:

命令包	从上位机到下位机的一个命令包
响应命令包	执行上位机的命令后，下位机用于响应的包
询问包	询问对方是否空闲，只有 ENQ 一种
应答包	应答包用于回应命令包，响应命令包或是询问包，以指示当前状态．包括 ACK，NACK 和 Busy 三种

询问包是可选的，其目的主要是询问对方是否可以接收数据包，如果对方返回 Busy，则需要等待一段时间再询问．在带有询问包时，上位机对下位机的任何数据包(包括 ENQ 包)都需要进行响应，即返回 ACK，NACK，或是 Busy 包．但是在不带询问包时，下位机不会主动发送询问包，且上位机不响应 ACK，请参考 7.4.3 节.

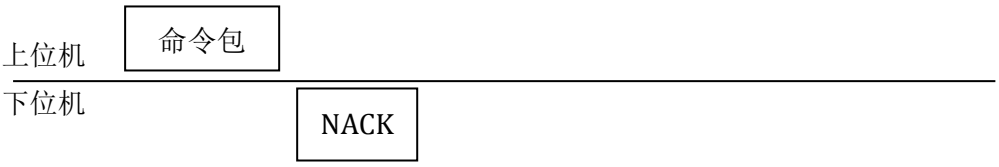
7.4.2 命令模式和自主模式

下位机有两种模式，命令模式和自主模式．命令模式指的是上位机发送一个命令，而下位机则返回一个响应命令包．在此模式下，下位机处在死循环中，一直等待上位机命令.而自主模式指的是下位机始终处在忙碌状态，在工作的间隙读取上位机命令并可能将工作结果放在响应命令包中发给上位机．有两种方式中止自主模式，第一种是上位机在收到下位机 ENQ 包之后，返回一个 NACK，第二种就是通过执行命令，中止自主模式.

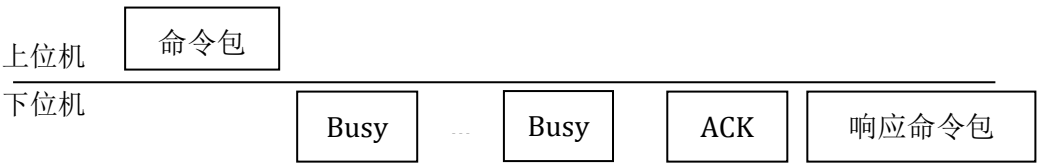
7.4.3 通信方式示例

a) 不带询问包，正常通信

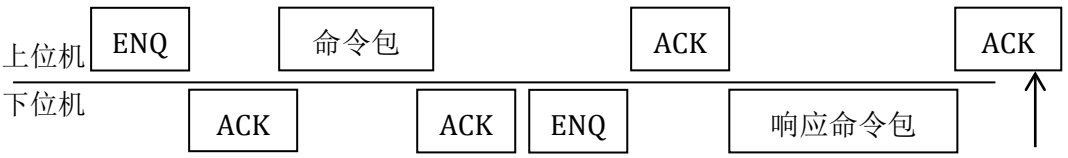
b) 不带询问包，命令包格式错误



c) 不带询问包，长时间命令，需要返回 Busy 包

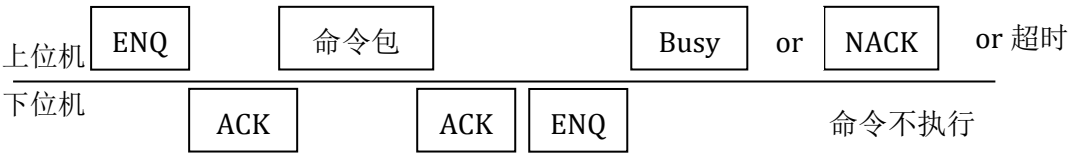


d) 带询问包，正常通信

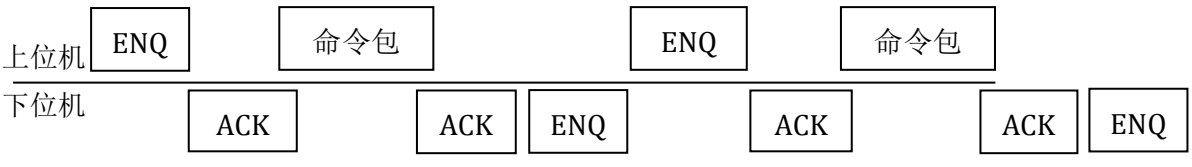


这个数据包并不重要，下位机会舍弃这个包. 因此即使是 NACK, Busy 或是接收超时，下位机都不会响应. 但不能是一个错包

e) 带询问包，上位机忙碌

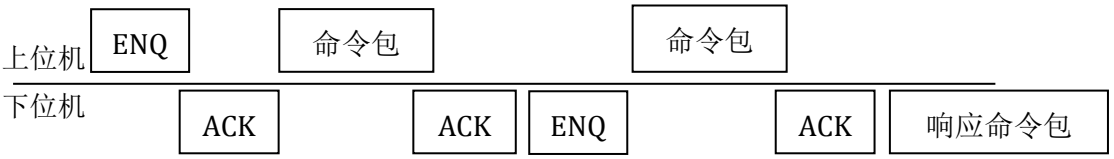


f) 带询问包，上位机开始执行新的命令



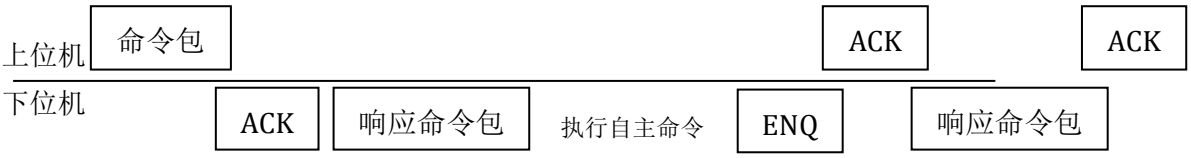
不执行旧命令

g） 带询问包，上位机开始执行新的命令



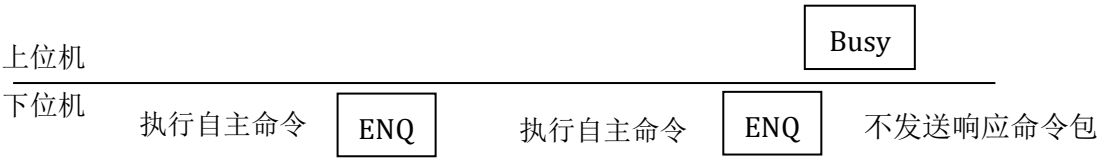
不执行旧命令

h） 进入自主模式

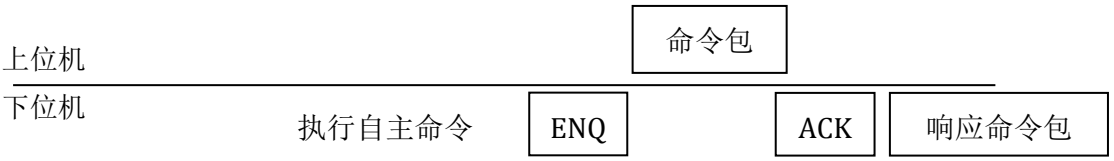


进入自主模式

i） 处在自主模式，上位机无响应

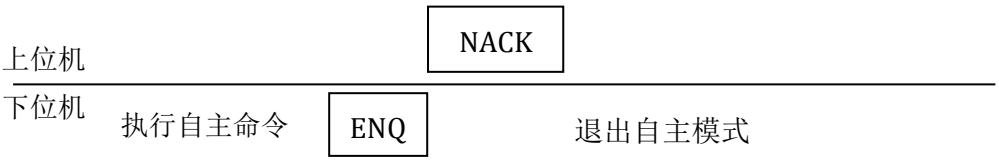


j） 处在自主模式，上位机开始执行新的命令



k） 处在自主模式，阻塞其他命令

l） 退出自主模式

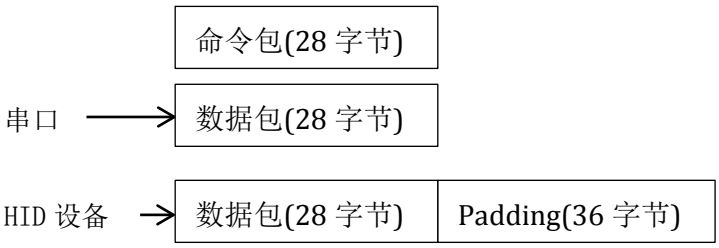


7.5 流通信与块通信

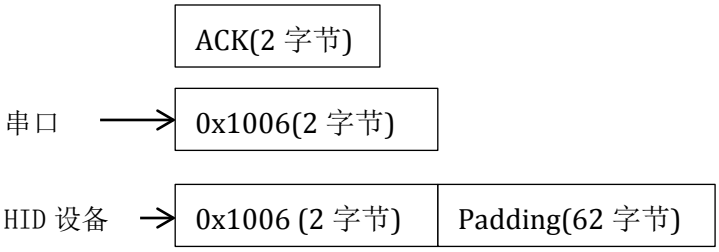
上位机与下位机通信方式有两种：流通信和块通信．流通信指的是数据以流的形式传输，例如串口通信．而块通信指的是数据以数据块的形式传输，例如 USB 的人机接口设备(HID)．HID 在发送和接收数据时都是以 64 字节数据包为一个发送单元．在上位机与下位机进行块通信时，数据长度被补充成数据块的整数倍．不足的数据用 padding 0x00 填充．下面是两个流通信和块通信的例子：

a) 数据包长度小于 64 字节

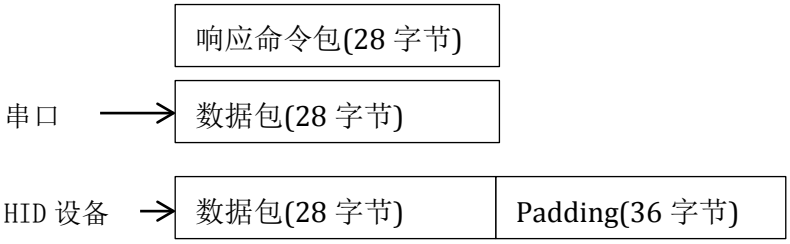
上位机发送命令包



下位机响应 ACK 应答包

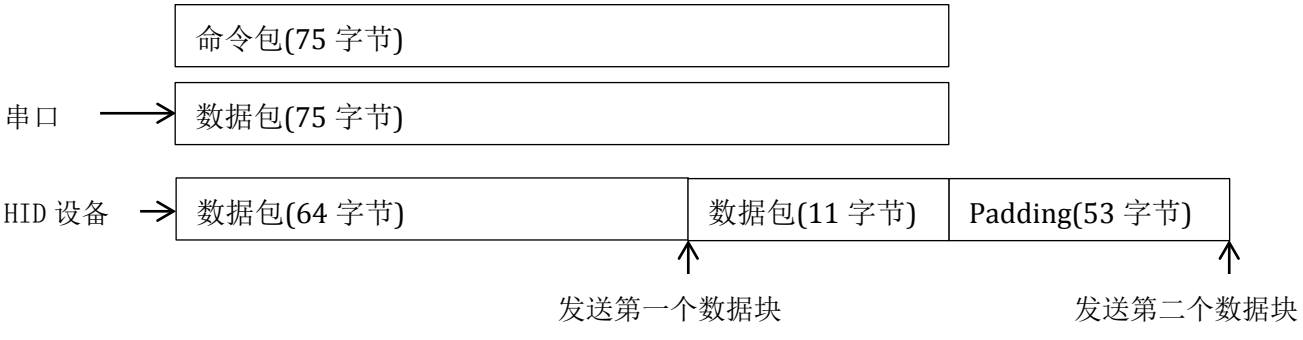


下位机响应命令包

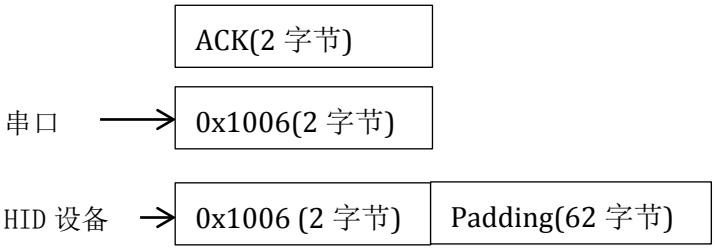


b) 数据包长度大于 64 字节

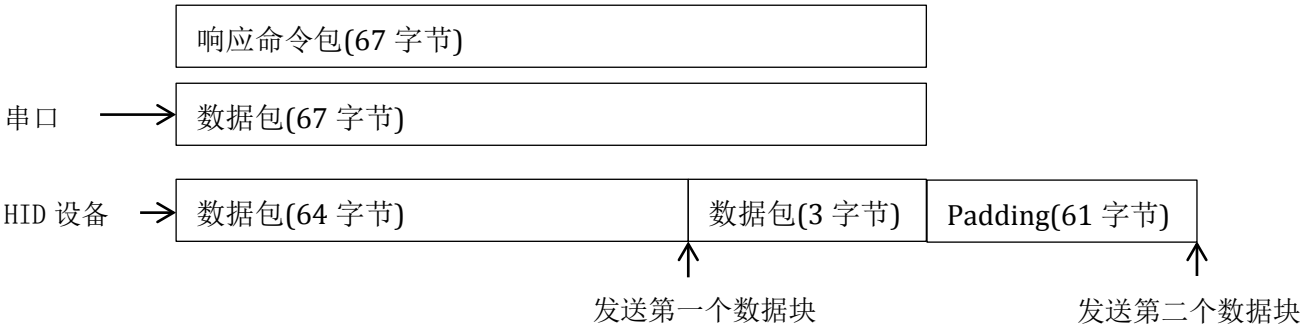
上位机发送命令包



下位机响应 ACK 应答包



下位机响应命令包



下位机的接收和发送缓冲区长度为 512 字节，在此情况下，发送的内层数据包最大长度为 495 字节. 请注意, 由于协议限制，精简可变长包最大发送内层数据包长度为 252 字节. 同时，内层数据包的长度段不能为长度段 1，因为长度段 1 只适用于长度小于 250 字节的情况.

8. 读卡机命令

8.1 读取状态

命令: 0x04

接收数据段: 1 字节是否包含其他状态数据, 为 1 时返回数据段包含其他状态数据

Has Other Status
1 Byte

返回数据段: 4 字节主程序版本, 4 字节 Loader 版本, 4 字节制造日期, 可变长度其他状态数据.

Main Version	Loader Version	Manufacture time	Other Status
4 Bytes	4 Bytes	4 Bytes	Variable

在本读卡机中, 其他状态数据内容如下:

Modulator mode	SAM channel	SAM data rate
2 Bytes	1 Byte	8 Bytes

Modulator mode 指的是当前读卡机射频调制芯片的模式, 最低位(LSB)如果为 0,表示使用 ISO14443-A 类型协议, 如果为 1, 则使用 ISO14443-B 类协议. 次低位(LSB+1)表示当前 Mifare 卡使用的传输密钥集. 如果为 0, 表示使用 Philips 定义的标准密钥集, 如果为 1, 表示使用上海传输密钥集.

SAM channel 指的是当前选择的 SAM 通道, 在 SAM 卡扩展板上一共可以插入 8 个 SAM 卡, 对应着通道 0 到通道 7. SAM data rate 指的是 SAM 卡当前的通信速率, 8 个字节分别对应着 8 个通道.请参考 8.18 节

8.2 芯片重置

命令: 0x1A

软件复位芯片, 该命令用于错误恢复, 或是烧写程序.

接收数据段: 1 字节复位位置, 0x00 表示复位到主程序, 0x01 表示复位到 Loader

Reset Location
1 Byte

返回数据段: 1 字节复位结果, 0xAA 表示复位成功

Reset Result
1 Byte

8.3 电路检测

命令：0x1B

该命令用于检测硬件电路是否正常工作.，参数为 12 字节的 0xFF. 在调用此命令之前，必须先执行辅助处理器引导命令，使主处理器进入检测模式.

接收数据段：12 字节 0xFF

Parameter (0xFF)
12 Bytes

返回数据段：共 5 字节检测结果,全部为 0x00 表示检测成功,其他表示硬件检测失败.

Test Result	Parameter (0x00)
4 Byte	1 Byte

Test Result	错误原因	Test Result	错误原因
0x00000000	无错误	0x00000040	射频调制芯片 1 出错
0x00000001	SDRAM 读写出错	0x00000080	射频调制芯片 2 出错
0x00000002	串行 Flash0 读写出错	0x00000100	SAM 卡 0 出错
0x00000004	串行 Flash1 读写出错	0x80000000	其他错误
0x00000008	并行 Flash 读写出错		
0x00000010	EEROM 读写出错		
0x00000020	以太网芯片出错		

8.4 写入内存

命令：0x33

将数据写入辅助处理器内存映射的某个位置.具体内存映射信息请参考第 9 节. 内存地址必须为 4 字节对齐，即地址的末两位必须为 0. 有些内存地址是只读的，使用该命令会返回失败结果. 读取和写入的 4 字节均为大尾端格式.

接收数据段：4 字节内存映射地址，4 字节数据.

Mapping Address	Data
4 Bytes	4 Bytes

返回数据段：1 字节写操作结果，0xAA 表示写入成功. 其他返回值表示写入失败.

Write Result
1 Byte

8.5 读取内存

命令：0x34

从辅助处理器内存映射的某个位置读取数据.具体内存映射信息请参考第 9 节. 内存地址必须为 4 字节对齐，即地址的末两位必须为 0. 有些内存地址是只写的，使用该命令会返回失败结果.

接收数据段：4 字节内存映射地址.

Mapping Address
4 Bytes

返回数据段：1 字节读操作结果，0xAA 表示读取成功，4 字节数据. 其他返回值表示读取失败.

Read Result	Data
1 Byte	4 Bytes

8.6 延时写入 MIFARE 系列卡

命令：0x01

该命令将 16 字节的数据写入 Mifare 1K 系列卡片的一个数据块(Block)中，写入的数据块地址不能为卡片的第一个数据块和密钥块.即写入的块地址不能为 0x00 或块地址的末两位不能为 0x03. 如果读写范围内没有卡或是卡片类型不是 Mifare 卡,读卡机将在 0.25 秒内继续尝试寻卡，当该段时间结束后仍然没有卡片，读卡器将返回一个出错状态. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

注意：本函数和 8.7 至 8.11 节描述的 Mifare 卡操作函数只能操作标准 Mifare 卡，且块地址的范围为 0x00 至 0xFF. 并假设前 32 个扇区(Sector)有 4 个 Block，第 33 至 40 扇区有 16 个 Block. 例如,块地址参数为 0x7E，它表示扇区 31 的第 3 个块. 块地址参数为 0xFF,则表示扇区 39 的第 16 个块，即典型 4K 卡的最后一个扇区最后一个 Block.

接收数据段：1 字节射频通道，1 字节块地址，2 字节密钥信息，16 字节写入数据.

Channels	Block Address	Key	Data
1 Byte	1 Byte	2 Bytes	16 Bytes

返回数据段：1 字节写操作结果.

Write Result
1 Byte

操作结果	错误原因
0x00	操作正常
0x01	读取 Block 出错
0x02	写入 Block 出错
0x03	通道参数出错
0x04	卡认证出错
0x05	选卡出错
0x06	非法 Block 地址
0x07	寻卡出错

2 字节密钥信息的最高位如果为 0,表示这个扇区的密钥在内存映射对应的 Mifare 密钥区中.0x0000 表示使用密钥 A, 0x0001 表示使用密钥 B. 最高位如果为 1, 则后 9 位表示密钥在 EEROM 中的地址.此时,次高位(MSB-1)为 0 表示密钥 A,为 1 表示密钥 B.

例如, 0xC110 表示密钥为以 0x0110 地址的起始的调制芯片的 EEROM 中, 一共 6 个字节, 密钥类型为密钥 B.

0x0001 表示密钥在内存映射的 Mifare 密钥区中,为密钥 B. 在调用该命令之前, 用户需要执行写入内存字节命令, 写入地址为 0x00011050 或 0x00021050, 先将密钥写入密钥区.

8.7 延时读取 MIFARE 系列卡

命令: 0x02

该命令从 Mifare 1K 系列卡片的一个数据块(Block)中读取 16 字节的数据, 读取的数据块地址不能为密钥块. 即块地址的末两位不能为 0x03. 如果读写范围内没有卡或是卡片类型不是 Mifare 卡,读卡机将在 0.25 秒内继续尝试寻卡, 当该段时间结束后仍然没有卡片,读卡器将返回一个出错状态.密钥信息请参考 8.6 节.

接收数据段: 1 字节射频通道, 1 字节块地址, 2 字节密钥信息.

Channels	Block Address	Key
1 Byte	1 Byte	2 Bytes

返回数据段: 1 字节操作结果, 参考 8.6 节. 当返回读取成功时, 16 字节数据有效 . 如果读取结果不成功, 数据段无效.

Read Result	Data
1 Byte	16 Bytes

8.8 立即写入 MIFARE 系列卡

命令: 0x05

该命令将 16 字节的数据写入 Mifare 1K 系列卡片的一个数据块(Block)中, 写入的数据块地址不能为卡片的第一个数据块和密钥块.即写入的块地址不能为 0x00 或块地址的末两位不能为 0x03. 如果读写范围内没有卡或是卡片类型不是 Mifare 卡,读卡器将立刻返回一个出错状态. 射频通道的范围从 1 到 3, 请参考 SAM9260 编程手册 1.4 节. 关于密钥信息,请参考 8.6 节.

接收数据段: 1 字节射频通道, 1 字节块地址, 2 字节密钥信息, 16 字节写入数据.

Channels	Block Address	Key	Data
1 Byte	1 Byte	2 Bytes	16 Bytes

返回数据段: 1 字节写操作结果, 参考 8.6 节.

Write Result
1 Byte

8.9 立即读取 MIFARE 系列卡

命令: 0x06

该命令从 Mifare 1K 系列卡片的一个数据块(Block)中读取 16 字节的数据, 读取的数据块地址不能为密钥块. 即块地址的末两位不能为 0x03. 如果读写范围内没有卡或是卡片类型不是 Mifare 卡,读卡器将立即返回一个出错状态. 密钥信息请参考 8.6 节.

接收数据段: 1 字节射频通道, 1 字节块地址, 2 字节密钥信息.

Channels	Block Address	Key
1 Byte	1 Byte	2 Bytes

返回数据段: 1 字节操作结果, 参考 8.6 节. 当返回读取成功时, 16 字节数据有效 . 如果读取结果不成功, 数据段无效.

Read Result	Data
1 Byte	16 Bytes

8.10 立即写入 MIFARE 系列卡,无密钥区保护

命令: 0x11

该命令将 16 字节的数据写入 Mifare 1K 系列卡片的一个数据块(Block)中, 写入的数据块地址不能为卡片的第一个数据块, 但可以是密钥块.即写入的块地址不能为 0x00, 但块地

址的末两位可以为 0x03. 如果读写范围内没有卡或是卡片类型不是 Mifare 卡,读卡器将立刻返回一个出错状态. 射频通道的范围从 1 到 3, 请参考 SAM9260 编程手册 1.4 节. 关于密钥信息,请参考 8.6 节.

接收数据段: 1 字节射频通道, 1 字节块地址, 2 字节密钥信息, 16 字节写入数据.

Channels	Block Address	Key	Data
1 Byte	1 Byte	2 Bytes	16 Bytes

返回数据段: 1 字节写操作结果, 参考 8.6 节.

Write Result
1 Byte

8.11 立即读取 MIFARE 系列卡,无密钥区保护

命令: 0x12

该命令从 Mifare 1K 系列卡片的一个数据块(Block)中读取 16 字节的数据, 读取的数据块地址可以为密钥块. 即块地址的末两位可以为 0x03. 如果读写范围内没有卡或是卡片类型不是 Mifare 卡,读卡器将立即返回一个出错状态. 密钥信息请参考 8.6 节.

接收数据段: 1 字节射频通道, 1 字节块地址, 2 字节密钥信息.

Channels	Block Address	Key
1 Byte	1 Byte	2 Bytes

返回数据段: 1 字节操作结果, 参考 8.6 节. 当返回读取成功时, 16 字节数据有效 . 如果读取结果不成功, 数据段无效.

Read Result	Data
1 Byte	16 Bytes

8.12 写入 DATAFLASH

命令: 0x07

辅助处理器内部为用户提供了 3K 字节长度,用于存储数据的 DataFlash 区. 用户可以使用该命令, 或是内存映射对 DataFlash 进行写入操作. 操作类型为 0x00 时, 该命令将数据写入 DataFlash. 当操作类型为 0x01 时, 该命令将擦除整个 DataFlash, 且地址和数据字节无效. 地址从 0x00000000 到 0x00000BFF.读取和写入必须 4 字节对齐.

接收数据段：1 字节操作类型，4 字节数据地址，4 字节数据.

Operation	Data Address	Data
1Byte	4 Bytes	4 Bytes

返回数据段：1 字节操作结果，如果结果为 0x00，则写入 Flash 成功.

Operation Result
1 Byte

8.13 读取 DATAFLASH

命令：0x08

该命令用于读取 DataFlash 内的数据.

接收数据段：4 字节数据地址.

Data Address
4 Bytes

返回数据段：1 字节操作结果，如果结果为 0x00，则读取 Flash 成功，数据段有效. 否则数据段无效.

Operation Result	Data
1 Byte	4 Bytes

8.14 辅助处理器引导

命令：0x23

该命令将从辅助处理器引导 AT91SAM9260 芯片，在调用该命令之前，AT91SAM9260 芯片必须处在 SAMBA monitor 状态. 该命令将首先向主处理器的内部 SRAM 写入一个 Bootstrap，即 RFIDBootstrapEx. 然后通过 DBU 串口与 Bootstrap 通信，将 NAND Flash 的第一个 Block 中的数据擦除. 然后向 NAND Flash 的起始地址写入 RFIDBootstrapEx. 在调用该命令之后，用户才可以调用电路检测命令和引导编程命令.

接收数据段：1 字节 Flash 操作，如果为 0，则在执行此命令时不擦除 Flash，如果为 1，则擦除第一个 Block，并向 NAND Flash 的起始写入 4K 的 AT91BootstrapEx. 如果为 2，则还向 Flash 地址 0x00020000 写入一个测试程序.

Flash Operation
1 Byte

返回数据段：1 字节操作结果，如果结果为 0x00,则操作成功.注意:该命令执行时间较长.

Operation Result
1 Byte

8.15 设置 USB 模式

命令：0x24

辅助处理器的 USB 通常用于辅助处理器与上位机的通信，这个 USB 被配置成 HID 设备，其 VID 为 0x0532，PID 为 0x5201. 但是用户可以占用这个 USB，让主处理器直接与上位机进行通信.每次发送和接收数据包的长度为 64 字节，通过内存映射进行访问.

接收数据段：1 字节 USB 模式，如果为 0，则辅助处理器的 USB 数据包将作为上位机发送给辅助处理器的命令进行处理. 如果为 1，则辅助处理器的 USB 发送和接收的数据由主处理器负责.

USB Mode
1 Byte

返回数据段：1 字节操作结果，如果结果为 0x00，则操作成功.

Operation Result
1 Byte

8.16 写入 USB 数据包

命令：0x25

通过辅助处理器的 USB 数据包向上位机发送数据，在调用此函数之前，用户需要向辅助处理器内存映射的 HID 设备发送缓冲区写入数据.

接收数据段：1 字节 USB 发送数据包长度，长度不能超过 64 字节，如果发送长度小于 64 字节，数据包将用 0x00 填充.

Package Length
1 Byte

返回数据段：1 字节操作结果，如果结果为 0x00，则操作成功.

Operation Result
1 Byte

8.17 读取 USB 数据包

命令：0x26

通过辅助处理器的 USB 数据包从上位机接收数据，调用该函数后，辅助处理器将一直等待上位机发送返回数据包,或超时后才返回. 在此函数返回后，用户可以通过辅助处理器内存映射的 HID 设备接收缓冲区读取数据.

接收数据段：2 字节超时参数. 超时参数的单位为 0.01 秒，例如 0x000A 表示在 0.1 秒内接收到整个数据包. 如果该参数为 0xFFFF，则无限超时等待.

Timeout
2 Bytes

返回数据段：1 字节操作结果，如果结果为 0x00，则操作成功.

Operation Result
1 Byte

8.18 SAM 卡复位

命令：0x21

该命令复位 SAM 卡槽中的 SAM 卡，获得其 ATR. 并执行 PTS，设置通信的数据传输速率. 在调用完该函数后，如果复位成功，用户可以通过内存映射获取 SAM 返回的历史字节信息.如果该命令成功，用户可以调用发送 APDU 命令与 SAM 卡进行通信.

接收数据段：1 字节通道号，范围从 0 到 7 对应着 SAM 卡板上的 8 个 SAM 卡槽. 1 字节复位波特率指的是卡片在 ATR 时使用的波特率. 按照 ISO7816 协议，这个参数为 9600. 但是国内大量使用的一些 SAM 卡,如建设部 SAM，在复位时即为 38400 波特率. 用户需要根据不同的卡片设置该参数. 1 字节 PTS 波特率指的是卡片执行 PTS 命令，调整通信使用的波特率的参数. 该参数如果为 0x00，则不执行 PTS.

Channel	Reset Baudrate	PTS Baudrate
1 Byte	1 Byte	1 Byte

返回数据段：1 字节通道号,1 字节操作结果，如果结果为 0x00，则操作成功,且 ATR 有效，后面有 1 字节 ATR 数据长度和复位返回数据. 一个典型的复位返回数据为 0x3b 9d 18 00 01 13 03 07 fa ed 57 13 e6 d8 89 da 16. 指 SAM 卡传输为正向编码，TA1=0x18，TD1=0x00 并且有 13 个历史字节.

Channel	Operation Result	ATR Length	ATR Data
1 Byte	1 Byte	1 Byte	ATR Length Bytes

波特率参数	SAM 卡实际波特率
0x01	9600
0x02	19200
0x03	38400
0x04	56000
0x05	115200

8.19 SAM 卡发送 APDU 命令

命令：0x22

该命令向 SAM 卡发送 APDU 命令，并接受卡的返回数据. SAM 卡的 APDU 命令由 ISO7816 标准定义，并使用半双工字符传输模式(T=0). SAM 卡命令缓冲区长度为 512 字节，这意味着用户最大可以发送的 APDU 命令长度或返回 APDU 响应长度为 489 字节.

接收数据段：1 字节通道号，4 字节 APDU 长度，定义后面 APDU 命令的发送长度.可变长度 APDU 命令，格式由 ISO7816 协议定义.

Channel	APDU Length	APDU Command
1 Byte	4 Bytes	Variable

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功. 4 字节 APDU 响应长度，定义后面 APDU 响应的发送长度. 可变长度 APDU 响应.

Channel	Operation Result	APDU Response Length	APDU Response
1 Byte	1 Byte	4 Bytes	Variable

8.20 设置调制模式

命令：0x27

该命令设置射频调制芯片的调制模式，可以选择当前读卡机使用 ISO14443 标准定义的 Type A 还是 Type B.注意到调制模式参数在通道 1 和通道 3 是相同的，因为通道 1 和通道 3 使用同一个调制芯片. 且该参数与通道 2 独立.

接收数据段：1 字节射频通道，范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.1 字节调制模式，最低位(LSB)如果为 0,表示使用 ISO14443-A 类型协议，如果为 1，则使用 ISO14443-B 类协议. 次低位(LSB+1)表示当前 Mifare 卡使用的传输密钥集. 如果为 0，表示使用 Philips 定义的标准密钥集,如果为 1，表示使用上海传输密钥集.例如，如果我们需要读写基于 FM11RF08SH 的非接触卡，需要使用上海传输密钥集.用户需要将调制模式设置为 0x02，才能进行正常的三重认证.如果需要读写基于 MF1S50 的非接触卡，调制模式应设置为 0x00. 2 字节自动关断射频时间，请参考 8.45 节.

Channel	Modulator Mode	AutoSleep Time
1 Byte	1 Byte	2 Bytes

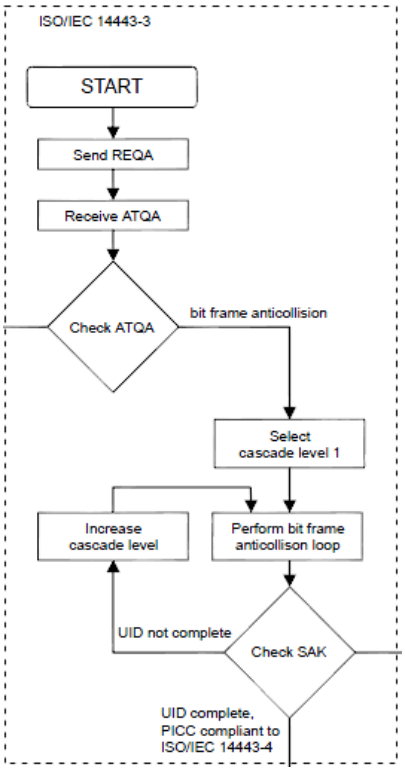
返回数据段：1 字节射频通道，1 字节操作结果，如果结果为 0x00，则操作成功.

Channel	Operation Result
1 Byte	1 Byte

8.21 寻卡

命令：0x28

该命令会自动查询某射频通道是否有卡存在，如果有卡，则该命令返回成功，用户通过卡片返回的 SAK 和 UID 等信息来判断下面的操作.该命令执行由 ISO14443-3 定义的寻卡和防重叠环的操作. 其流程图如下.



如果寻卡次数大于 1，该命令将定时开启射频进行寻卡，如果没有寻到，则关闭射频等待下一次寻卡. 如果寻卡成功，该命令则自动中止，即使寻卡剩余次数大于 0. 如果寻卡次数大于 1，该命令将进入自主模式.在此模式下，会向主处理器发送 ENQ 数据包，如果主处理器返回 ACK，则将整个数据包发送给主处理器. 请参考 7.4.2 节.

接收数据段：1 字节射频通道，范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节. 4 字节寻卡次数，该参数定义了后续寻卡进行的次数，如果为 0，则在一次寻卡完成后就不再继续寻卡. 如果为 0xFFFFFFFF,则无限寻卡. 2 字节寻卡间隙时间，间隙参数的单位为 0.01 秒，例如 0x0032 表示每隔 0.5 秒进行一次寻卡.考虑到 280ms 的寻卡超时，在未读到卡时，实际接收命令间隔大约为 0.8 秒. 1 字节寻卡模式，最低位(LSB)如果为 0 表示是否每次寻卡都向上位机报告，即使寻卡失败. 如果为 1 则表示只在寻卡成功时向上位机报告. 次低位(LSB+1)表示是否阻塞其他命令，如果为 0，则不阻塞，其他命令(除了读写卡操作)仍可以正常执行. 1 字节寻所有卡，如果为 1,则执行 WUPA(0x52)命令，否则执行 REQA(0x26)

Channel	Request Times	Request Interval	Request Mode	Request All
1 Byte	4 Bytes	2 Bytes	1 Byte	1 Byte

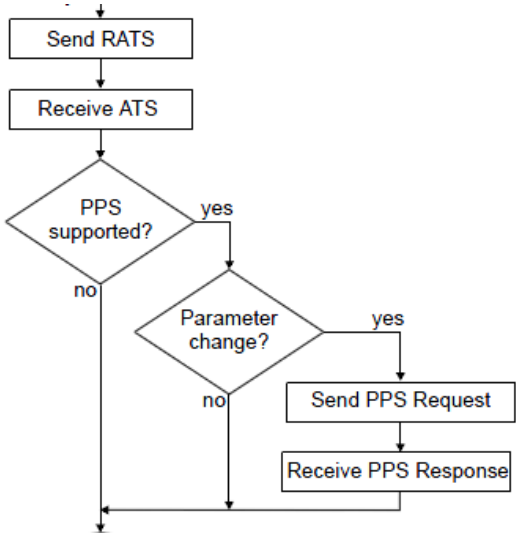
返回数据段：1 字节射频通道，4 字节已寻卡次数，1 字节操作结果，如果结果为 0x00，则寻卡成功，后续字节有效．ATQA 为卡片响应 REQA 或 WUPA 命令返回的 2 字节数据，SAK 为卡片响应选卡命令返回的 1 字节数据，UID 为卡片内部 ID 号．这三个参数的定义请参考 ISO14443 标准．1 字节卡片状态，其最高位如果为 1 表示该卡支持 ISO14443-4 标准，末尾 4 位表示 UID 的长度，可以为 0x04，0x07 或 0x0A．

Channel	Elapsed Request Times	Operation Result	ATQA	SAK	TagStatus	UID
1 Byte	4 Bytes	1 Byte	2 Bytes	1 Byte	1 Byte	10 Bytes

8.22 CPU 卡初始化

命令：0x29

该命令进行 CPU 卡的初始化，主要执行由 ISO14443-4 标准定义的 RATS 和 PPS 两个命令．在 CPU 卡初始化之后，用户就可以通过 APDU 命令与卡进行通信．其流程图如下．



接收数据段：1 字节射频通道，范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节．1 字节期望 CPU 卡数据速率，其末尾 2 位(LSB,LSB+1)为 DRI，即从 FM1715 到卡片的 bit 传输速率．第 2-3 位(LSB+2,LSB+3)为 DSI，即从卡片到 FM1715 的 bit 传输速率．如果值为 00，速率为 1；01 速率为 2；10 速率为 4；11 速率为 8．分别对应着 106Kbps，212Kbps，424Kbps 和 848Kbps 传输速率．最高位如果为 1，则不执行 PPS．例如，0x05 表示期望上行和下行传输速率均为 212KBps．0x80 表示不进行 PPS．

注意：该参数仅仅是期望使用的速率，CPU 卡在 ATS 的 TA(1)字节指示了当前卡支持的速率，读卡机会根据卡支持速率自动选择最接近的值．例如如果用户期望上行和下行传输速率均为 212KBps，但卡片只支持 106KBps，则读卡机会选择 106KBps 作为 PPS 命令参数．

Channel	Expected CPUTag Data Rate
1 Byte	1 Byte

返回数据段：1 字节射频通道，1 字节操作结果，如果结果为 0x00，则初始化成功，后续字节有效．1 字节当前数据速率．64 字节 ATS,为卡片响应 RATS 返回的数据，其实际长度由第一个字节定义，具体 ATS 数据结构,请参考 ISO14443-4 标准，5.2 节.

Channel	Operation Result	Current CPUTag Data Rate	ATS
1 Byte	1 Byte	1 Byte	64 Bytes

8.23 CPU 卡发送 APDU 命令

命令：0x2A

在完成 CPU 卡初始化后，用户可以执行该命令向 CPU 卡发送 APDU 命令并接受 APDU 命令响应.传输协议使用 ISO14443-4 中定义的半双工块传输协议(T=1) ． CPU 卡的 APDU 命令格式由 ISO7816 标准定义，调制芯片的命令缓冲区长度为 512 字节，这意味着用户最大可以发送的 APDU 命令长度或返回 APDU 响应长度为 489 字节.

接收数据段：1 字节通道号，4 字节 APDU 长度，定义后面 APDU 命令的发送长度.可变长度 APDU 命令，格式由 ISO7816 协议定义.

Channel	APDU Length	APDU Command
1 Byte	4 Bytes	Variable

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功．4 字节 APDU 响应长度，定义后面 APDU 响应的发送长度．可变长度 APDU 响应.

Channel	Operation Result	APDU Response Length	APDU Response
1 Byte	1 Byte	4 Bytes	Variable

8.24 MIFARE 卡写入块

命令：0x2B

该命令向 Mifare 系列卡写入一个数据块，主要完成三重认证和写卡命令．写入的数据块地址不能为卡片的第一个数据块和密钥块．即当扇区地址为 0x00 时,写入的块地址不能为 0x00 或 0x03．当扇区地址在 0x01 至 0x1F 范围内时，写入块地址不能为 0x03．当扇区地址在 0x20 至 0x27 时，写入块地址不能为 0x0F．射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.该命令会比较上一个块操作扇区，如果扇区相同则不用再次进行三重认证，如果扇区不同，则需要重新进行三重认证.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM.1 字节块地址，范围从 0x00 至 0x15．2 字节扇区密钥，16 字节需要写入的数据.

Channel	Sector Address	Block Address	Key	Data
1 Byte	1 Byte	1 Byte	2 Bytes	16 Bytes

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因.

Channel	Write Result	Error Info
1 Byte	1 Byte	1 Byte

2 字节密钥信息的最高位如果为 0,表示这个扇区的密钥在内存映射对应的 Mifare 密钥区中.0x0000 表示使用密钥 A，0x0001 表示使用密钥 B. 最高位如果为 1，则后 9 位表示密钥在 EEROM 中的地址.此时,次高位(MSB-1)为 0 表示密钥 A,为 1 表示密钥 B.

例如，0xC110 表示密钥为以 0x0110 地址的起始的调制芯片的 EEROM 中，一共 6 个字节，密钥类型为密钥 B.

0x0001 表示密钥在内存映射的 Mifare 密钥区中,为密钥 B. 在调用该命令之前，用户需要执行写入内存字节命令，写入地址为 0x00011050 或 0x00021050，先将密钥写入密钥区.

8.25 MIFARE 卡读取块

命令：0x2C

该命令从 Mifare 系列卡中读取一个数据块，主要完成三重认证和读卡命令. 读取的数据块地址不能为卡片的密钥块. 即当扇区地址在 0x00 至 0x1F 范围内时，读取块地址不能为 0x03. 当扇区地址在 0x20 至 0x27 时，读取块地址不能为 0x0F. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.该命令会比较上一个块操作扇区，如果扇区相同则不用再次进行三重认证，如果扇区不同，则需要重新进行三重认证.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM. 1 字节块地址，范围从 0x00 至 0x15. 2 字节扇区密钥.

Channel	Sector Address	Block Address	Key
1 Byte	1 Byte	1 Byte	2 Bytes

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因. 16 字节读取的数据.

Channel	Read Result	Error Info	Data
1 Byte	1 Byte	1 Byte	16 Bytes

2 字节密钥信息的最高位如果为 0,表示这个扇区的密钥在内存映射对应的 Mifare 密钥区中.0x0000 表示使用密钥 A, 0x0001 表示使用密钥 B. 最高位如果为 1, 则后 9 位表示密钥在 EEROM 中的地址.此时,次高位(MSB-1)为 0 表示密钥 A,为 1 表示密钥 B.

例如, 0xC110 表示密钥为以 0x0110 地址的起始的 6 个字节,为密钥 B

0x0001 表示密钥在内存映射的 Mifare 密钥区中,为密钥 B. 在调用该命令之前, 用户需要执行写入内存命令, 先将密钥写入密钥区.

8.26 MIFARE 卡写入扇区

命令: 0x2D

该命令向 Mifare 系列卡写入一个扇区, 主要完成三重认证和写卡命令. 写入的数据块地址不能为卡片的第一个数据块和密钥块. 即当扇区地址为 0x00 时,写入的块地址不能包括 0x00 或 0x03. 当扇区地址在 0x01 至 0x1F 范围内时, 写入块地址不能包括 0x03. 当扇区地址在 0x20 至 0x27 时, 写入块地址不能包括 0x0F.射频通道的范围从 1 到 3, 射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段: 1 字节通道号, 1 字节扇区地址, 范围从 0x00 至 0x37, 支持最大 16Kbytes EEROM. 1 字节起始块地址, 范围从 0x00 至 0x15. 2 字节扇区密钥. 1 字节写入块数量 N,N 的范围从 1 到 16. 还有可变长度的需要写入的数据, 数据长度需要是 16 的 N 倍. 该命令将从块地址开始将数据写入 N 个数据块.例如将 64 字节的数据写入卡片 MF1S70 扇区 32, 块 2,3,4,5 中, 即为 Sector Address=0x20, Start Block Address=0x02, N=4.

Channel	Sector Address	Start Block Address	Key	N	Data
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	16 Bytes*N

返回数据段: 1 字节通道号, 1 字节操作结果, 如果结果为 0x00, 则操作成功,其定义请参考 8.6 节. 1 字节错误信息, 如果操作结果不为 0x00, 则错误信息有效, 定义了出错原因.

Channel	Write Result	Error Info
1 Byte	1 Byte	1 Byte

2 字节密钥信息的最高位如果为 0,表示这个扇区的密钥在内存映射对应的 Mifare 密钥区中.0x0000 表示使用密钥 A, 0x0001 表示使用密钥 B. 最高位如果为 1, 则后 9 位表示密钥在 EEROM 中的地址.此时,次高位(MSB-1)为 0 表示密钥 A,为 1 表示密钥 B.

例如, 0xC110 表示密钥为以 0x0110 地址的起始的 6 个字节,为密钥 B

0x0001 表示密钥在内存映射的 Mifare 密钥区中,为密钥 B. 在调用该命令之前, 用户需要执行写入内存命令, 先将密钥写入密钥区.

8.27 MIFARE 卡读取扇区

命令：0x2E

该命令从 Mifare 系列卡中读取一个扇区，主要完成三重认证和读卡命令. 读取的数据块地址不能包含卡片的密钥块. 即当扇区地址在 0x00 至 0x1F 范围内时，读取块地址不能包含 0x03. 当扇区地址在 0x20 至 0x27 时，读取块地址不能包含 0x0F. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM. 1 字节起始块地址，范围从 0x00 至 0x15. 2 字节扇区密钥. 1 字节写入块数量 N,N 的范围从 1 到 15. 该命令将从块地址开始读取 N 个数据块.例如需要从卡片 MF1S70 的扇区 32,块 2,3,4,5 中读取 64 字节的数据，即为 Sector Address=0x20，Start Block Address=0x02，N=4.

Channel	Sector Address	Start Block Address	Key	N
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因.可变长度的读取的数据，数据长度为 16 的 N 倍.

Channel	Read Result	Error Info	Data
1 Byte	1 Byte	1 Byte	16 Bytes*N

2 字节密钥信息的最高位如果为 0,表示这个扇区的密钥在内存映射对应的 Mifare 密钥区中.0x0000 表示使用密钥 A，0x0001 表示使用密钥 B. 最高位如果为 1，则后 9 位表示密钥在 EEROM 中的地址.此时,次高位(MSB-1)为 0 表示密钥 A,为 1 表示密钥 B.

例如，0xC110 表示密钥为以 0x0110 地址的起始的 6 个字节,为密钥 B

0x0001 表示密钥在内存映射的 Mifare 密钥区中,为密钥 B. 在调用该命令之前，用户需要执行写入内存命令，先将密钥写入密钥区.

8.28 休眠 ISO14443 卡

命令：0x2F

该命令将卡片置入 Halt 状态，如果当前卡为 Mifare 卡，则使用 HALT 命令. 如果当前卡为 CPU 卡，则使用 DESELECT 命令. 该命令还会关断当前通道的射频信号.

接收数据段：1 字节通道号，1 字节卡片类型.

Channel	Tag Type
1 Byte	1 Byte

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功.

Channel	Halt Result
1 Byte	1 Byte

卡片类型	条件
0x00	符合 ISO14443 TypeA，Mifare 卡
0x01	符合 ISO14443 TypeA，CPU 卡
0x02	符合 ISO14443 TypeB

8.29 写入调制芯片 EEROM

命令：0x41

该命令将普通数据或是密钥写入调制芯片的 EEROM 中，EEROM 的地址范围从 0x0000 到 0x01FF. 如果密钥字节为 0,则直接写入数据. 如果密钥字节为 1,则写入的数据长度必须为 6 字节. 读卡机会将这 6 字节密钥转换成 Crypto1 格式的密钥并写入. 例如，实际密钥 0xA0 A1 A2 A3 A4 A5 将会转换成 0x5A F0 5A E1 5A D2 5A C3 5A B4 5A A5. 注意到通道号选择 1 和 3 都对应着同一个调制芯片. 关于调制芯片 EEROM 映射和密钥格式，请参考 MFRC500 数据手册 6.1 节和 6.4 节.

接收数据段：1 字节通道号，2 字节写入地址,1 字节密钥字节. 1 字节数据长度，数据长度的范围在 1 到 16 字节. 可变长度写入 EEROM 数据.

Channel	Address	Key	Data Length	Data
1 Byte	2 Bytes	1 Byte	1 Byte	Variable

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功.

Channel	Operation Result
1 Byte	1 Byte

8.30 读取调制芯片 EEROM

命令：0x42

该命令将普通数据从调制芯片的 EEROM 中读取出来，EEROM 的地址范围从 0x0000 到 0x007F. 注意到通道号选择 1 和 3 都对应着同一个调制芯片.

接收数据段：1 字节通道号，1 字节数据长度，数据长度的范围在 1 到 16 字节.

Channel	Address	Data Length
1 Byte	2 Bytes	1 Byte

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功.

Channel	Operation Result	Data
1 Byte	1 Byte	Variable

8.31 MIFARE 卡初始化钱包

命令：0x43

将 Mifare 卡的一个块初始化为一个值块(Value Block)，其具体结构如下图所示.

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	value				value				value				adr	$\overline{adr}$	adr	$\overline{adr}$

写入的值块地址不能为卡片的第一个数据块和密钥块. 即当扇区地址为 0x00 时,写入的块地址不能为 0x00 或 0x03. 当扇区地址在 0x01 至 0x1F 范围内时，写入块地址不能为 0x03. 当扇区地址在 0x20 至 0x27 时，写入块地址不能为 0x0F. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM.1 字节块地址，范围从 0x00 至 0x15. 2 字节扇区密钥，4 字节有符号值和 1 字节地址.

Channel	Sector Address	Block Address	Key	Value	Adr
1 Byte	1 Byte	1 Byte	2 Bytes	4 Bytes	1 Byte

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因.

Channel	Write Result	Error Info
1 Byte	1 Byte	1 Byte

8.32 MIFARE 卡读钱包

命令：0x44

该命令从 Mifare 系列卡中读取一个值块(Value Block). 读取的值块地址不能为卡片的密钥块. 即当扇区地址在 0x00 至 0x1F 范围内时，读取块地址不能为 0x03. 当扇区地址在 0x20 至 0x27 时，读取块地址不能为 0x0F. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM. 1 字节块地址，范围从 0x00 至 0x15. 2 字节扇区密钥.

Channel	Sector Address	Block Address	Key
1 Byte	1 Byte	1 Byte	2 Bytes

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因. 4 字节有符号值和 1 字节地址.

Channel	Read Result	Error Info	Value	Adr
1 Byte	1 Byte	1 Byte	4 Bytes	1 Byte

8.33 MIFARE 卡钱包充值

命令：0x45

该命令向 Mifare 系列卡的某一个值块(Value Block)执行增值操作(INCREMENT)，并将增值的块写回这个块. 写入的数据块地址不能为卡片的第一个数据块和密钥块. 即当扇区地址为 0x00 时,写入的块地址不能为 0x00 或 0x03. 当扇区地址在 0x01 至 0x1F 范围内时,写入块地址不能为 0x03. 当扇区地址在 0x20 至 0x27 时，写入块地址不能为 0x0F. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM.1 字节块地址，范围从 0x00 至 0x15. 2 字节扇区密钥，4 字节需要增值的数据.

Channel	Sector Address	Block Address	Key	Value
1 Byte	1 Byte	1 Byte	2 Bytes	4 Bytes

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因.

Channel	Operation Result	Error Info
1 Byte	1 Byte	1 Byte

8.34 MIFARE 卡钱包扣款

命令：0x46

该命令向 Mifare 系列卡的某一个值块(Value Block)执行减值操作(DECREMENT)，并将减值的块写回这个块. 写入的数据块地址不能为卡片的第一个数据块和密钥块. 即当扇区地址为 0x00 时,写入的块地址不能为 0x00 或 0x03. 当扇区地址在 0x01 至 0x1F 范围内时,写入块地址不能为 0x03. 当扇区地址在 0x20 至 0x27 时，写入块地址不能为 0x0F. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM.1 字节块地址，范围从 0x00 至 0x15. 2 字节扇区密钥，4 字节需要减值的数据.

Channel	Sector Address	Block Address	Key	Value
1 Byte	1 Byte	1 Byte	2 Bytes	4 Bytes

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因.

Channel	Operation Result	Error Info
1 Byte	1 Byte	1 Byte

8.35 MIFARE 卡备份钱包

命令：0x47

该命令首先备份(RESTORE)Mifare 系列卡的某一个值块(Value Block)，并执行转移操作(TRANSFER),将备份的块写到别的块中. 写入的数据块地址不能为卡片的第一个数据块和密钥块. 即当扇区地址为 0x00 时,写入的块地址不能为 0x00 或 0x03. 当扇区地址在 0x01 至 0x1F 范围内时，写入块地址不能为 0x03. 当扇区地址在 0x20 至 0x27 时，写入块地址不能为 0x0F. 射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段：1 字节通道号，1 字节扇区地址，范围从 0x00 至 0x37，支持最大 16Kbytes EEROM.1 字节备份块地址，范围从 0x00 至 0x15. 1 字节转移块地址，范围从 0x00 至 0x15. 2 字节扇区密钥. 注意到转移的块和备份的块必须在同一个扇区.

Channel	Sector Address	Restore Block Address	Tran Block Addr	Key
1 Byte	1 Byte	1 Byte	1 Byte	2 Bytes

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因.

Channel	Operation Result	Error Info
1 Byte	1 Byte	1 Byte

8.36 ULTRALIGHT 卡写入块

命令：0x48

该命令写入 Ultralight 卡的某个 Page，射频通道的范围从 1 到 3，射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段：1 字节通道号，1 字节页地址，范围从 0x00 至 0x28，支持最大 40 个页. 1 字节认证标志，如果该标志为 1，则从卡片的 Block0 中读取 4 字节,再进行三重认证. 如果该标志为 0，则不进行三重认证. 2 字节三重认证密钥，密钥的格式参考 8.24 节.

1 字节 Ultralight 卡写命令. 如果该字节为 1, 则在写卡时使用命令 0xA2. 如果为 0, 则使用 0xA0 作为写命令. 4 字节写入数据.

Channel	Page Address	Authen	Key	UltralightCmd	Data
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	4 Bytes

返回数据段: 1 字节通道号, 1 字节操作结果, 如果结果为 0x00, 则操作成功,其定义请参考 8.6 节. 1 字节错误信息, 如果操作结果不为 0x00, 则错误信息有效, 定义了出错原因.

Channel	Write Result	Error Info
1 Byte	1 Byte	1 Byte

该命令兼容两种不同的 512bits 卡, 第一种卡为 MF0ICU1 型, UID 的长度为 7 字节, 选卡过程和 ISO14443 标准兼容. 在完成选卡后并不需要三重认证就能够直接读写. 操作这种卡时, Authen=0, Key=0, UltralightCmd=1. 另一种卡为 FM11RF005M 型, 卡片需要三重认证操作, 而写命令使用 0xA0. 操作这种卡时, Authen=1, UltralightCmd=0.Key 对应的 6 字节密钥必须为卡片第 8 个 Block 的 4 字节加上两个 0x00.

8.37 UltraLight 卡读取块

命令: 0x49
该命令读取 Ultralight 卡的 4 个 Page, 射频通道的范围从 1 到 3, 射频通道的定义请参考 SAM9260 编程手册 1.4 节.

接收数据段: 1 字节通道号, 1 字节页地址, 范围从 0x00 至 0x28, 支持最大 40 个页.
1 字节认证标志, 如果该标志为 1, 则从卡片的 Block0 中读取 4 字节,再进行三重认证. 如果该标志为 0, 则不进行三重认证. 2 字节三重认证密钥, 密钥的格式参考 8.24 节.

Channel	Page Address	Authen	Key
1 Byte	1 Byte	1 Byte	2 Bytes

返回数据段: 1 字节通道号, 1 字节操作结果, 如果结果为 0x00, 则操作成功,其定义请参考 8.6 节. 1 字节错误信息, 如果操作结果不为 0x00, 则错误信息有效, 定义了出错原因.1 字节读取长度, 16 字节读取数据, 实际长度取决于读取长度.

Channel	Read Result	Error Info	Read Length	Data
1 Byte	1 Byte	1 Byte	1 Byte	16 Bytes

该命令兼容两种不同的 512bits 卡, 第一种卡为 MF0ICU1 型, 操作这种卡时, Authen=0, Key=0, 读取的数据长度为 16 字节. 另一种卡为 FM11RF005M 型, 卡片需要三重认证操作, 操作这种卡时, Authen=1, Key 对应的 6 字节密钥必须为卡片第 8 个 Block 的 4 字节加上两个 0x00. 读取的数据长度为 4 字节.

8.38 MIFARE 卡写入块,无密钥区保护

命令: 0x4A

该命令向 Mifare 系列卡写入一个数据块, 主要完成三重认证和写卡命令. 写入的数据块地址不能为卡片的第一个数据块. 即当扇区地址为 0x00 时,写入的块地址不能为 0x00. 射频通道的范围从 1 到 3, 射频通道的定义请参考 SAM9260 编程手册 1.4 节.该命令总是重新进行三重认证.

接收数据段: 1 字节通道号, 1 字节扇区地址, 范围从 0x00 至 0x37, 支持最大 16Kbytes EEROM.1 字节块地址, 范围从 0x00 至 0x15. 2 字节扇区密钥, 16 字节需要写入的数据.

Channel	Sector Address	Block Address	Key	Data
1 Byte	1 Byte	1 Byte	2 Bytes	16 Bytes

返回数据段: 1 字节通道号, 1 字节操作结果, 如果结果为 0x00, 则操作成功,其定义请参考 8.6 节. 1 字节错误信息, 如果操作结果不为 0x00, 则错误信息有效, 定义了出错原因.

Channel	Write Result	Error Info
1 Byte	1 Byte	1 Byte

2 字节密钥信息的最高位如果为 0,表示这个扇区的密钥在内存映射对应的 Mifare 密钥区中.0x0000 表示使用密钥 A, 0x0001 表示使用密钥 B. 最高位如果为 1, 则后 9 位表示密钥在 EEROM 中的地址.此时,次高位(MSB-1)为 0 表示密钥 A,为 1 表示密钥 B.

例如, 0xC110 表示密钥为以 0x0110 地址的起始的 6 个字节,为密钥 B

0x0001 表示密钥在内存映射的 Mifare 密钥区中,为密钥 B. 在调用该命令之前, 用户需要执行写入内存命令, 先将密钥写入密钥区.

8.39 MIFARE 卡读取块,无密钥区保护

命令: 0x4B

该命令从 Mifare 系列卡中读取一个数据块, 主要完成三重认证和读卡命令. 读取的数据块地址可以为卡片的密钥块. 射频通道的范围从 1 到 3, 射频通道的定义请参考 SAM9260 编程手册 1.4 节.该命令总是重新进行三重认证.

接收数据段: 1 字节通道号, 1 字节扇区地址, 范围从 0x00 至 0x37, 支持最大 16Kbytes EEROM. 1 字节块地址, 范围从 0x00 至 0x15. 2 字节扇区密钥.

Channel	Sector Address	Block Address	Key
1 Byte	1 Byte	1 Byte	2 Bytes

返回数据段：1 字节通道号，1 字节操作结果，如果结果为 0x00，则操作成功,其定义请参考 8.6 节. 1 字节错误信息，如果操作结果不为 0x00，则错误信息有效，定义了出错原因. 16 字节读取的数据.

Channel	Read Result	Error Info	Data
1 Byte	1 Byte	1 Byte	16 Bytes

2 字节密钥信息的最高位如果为 0,表示这个扇区的密钥在内存映射对应的 Mifare 密钥区中.0x0000 表示使用密钥 A，0x0001 表示使用密钥 B. 最高位如果为 1，则后 9 位表示密钥在 EEROM 中的地址.此时,次高位(MSB-1)为 0 表示密钥 A,为 1 表示密钥 B.

例如，0xC110 表示密钥为以 0x0110 地址的起始的 6 个字节,为密钥 B

0x0001 表示密钥在内存映射的 Mifare 密钥区中,为密钥 B. 在调用该命令之前，用户需要执行写入内存命令，先将密钥写入密钥区.

8.40 读取硬件签名

命令：0x4C

该命令读取辅助处理器产生的 16 字节硬件签名和 16 字节伪随机数.

硬件签名由辅助处理器产生,包含如下信息：两个调制芯片的序列号，辅助处理器的硬件序列号和 AT91SAM9260 芯片 ID. 硬件签名由辅助处理器在出厂检测时生成，加密存放在辅助处理器的片上 EEROM 中. 辅助处理器在启动时检查该硬件签名的有效性. 如果硬件签名非法，则不再继续执行任何操作. 上位机发送的任何命令均响应 NACK.

硬件签名可以保证硬件的唯一性，例如即使有人将读卡机的 NAND Flash 数据读取出来,将辅助处理器破解并读取其源程序，并将这些数据烧写入一个新的读卡机中. 由于硬件签名的不同，程序将无法正常执行.

接收数据段：1 字节包含随机数，如果为 1，返回数据包含 16 字节的随机数，如果为 0,则不包含.

RandomAppend
1 Byte

返回数据段：16 字节硬件签名和 16 字节伪随机数.

Hardware Signature	Random
16 Bytes	16 Bytes

8.41 查询串口参数

命令：0x1E

该命令用于查询当前串口参数.

接收数据段：1 字节串口序号，为 0x00，1 字节参数类型，参数类型可以为 0x00 波特率，0x01 数据位个数，0x02 停止位个数，0x03 奇偶校验类型.

SerialIndex	SerialType
0x00	1 Byte

返回数据段：1 字节操作结果，如果结果为 0x00，则操作成功.1 字节参数结果. 如果为波特率参数,请参考 8.42 节.

Operation Result	Parameter
Operation Result	1 Byte

8.42 设置串口参数

命令：0x1F

该命令设置辅助处理器串口的参数.在电路复位后，辅助处理器串口的波特率一定为 38400，8N1. 用户可以调用此命令设置一个新波特率或其他参数. 新的波特率将在辅助处理器返回一个正确数据包后有效.**注意**：在进行固件下载前，用户必须将辅助处理器串口的波特率设置成 38400.否则固件下载将失败.

接收数据段：1 字节串口序号，为 0x00,1 字节参数类型，可以为 0x00 波特率，0x01 数据位个数，0x02 停止位个数，0x03 奇偶校验类型，1 字节参数数值.

SerialIndex	SerialType	SerialParameter
0x00	1 Byte	1 Byte

返回数据段：1 字节操作结果，如果结果为 0x00，则操作成功.

Operation Result
1 Byte

波特率参数	实际波特率
0x00	38400(默认)
0x02	9600
0x04	19200
0x05	38400
0x08	57600

0x09	115200
0x0B	230400
0x0D	460800

数据位参数	数据位个数
0x06	6
0x07	7
0x08	8

停止位参数	停止位个数
0x01	1
0x02	1.5
0x03	2

奇偶校验参数	奇偶校验类型
0x00	无校验
0x01	奇校验
0x02	偶校验

8.43 写入内存字节

命令：0x36

将数据写入辅助处理器内存映射的某个位置.具体内存映射信息请参考第 9 章.注意到有效内存映射的数据段地址必须为 4 字节对齐，这些地址不能使用该命令. 有些内存地址是只读的，使用该命令会返回失败结果.

接收数据段：4 字节内存映射地址，1 字节数据.

Mapping Address	Data
4 Bytes	1 Byte

返回数据段：1 字节写操作结果，0xAA 表示写入成功. 其他返回值表示写入失败.

Write Result
1 Byte

8.44 读取内存字节

命令：0x37

从辅助处理器内存映射的某个位置读取数据.具体内存映射信息请参考第 9 章. 注意到有效内存映射的数据段地址必须为 4 字节对齐，这些地址不能使用该命令. 有些内存地址是只写的，使用该命令会返回失败结果.

接收数据段：4 字节内存映射地址.

Mapping Address
4 Bytes

返回数据段：1 字节读操作结果，0xAA 表示读取成功，4 字节数据. 其他返回值表示读取失败.

Read Result	Data
1 Byte	1 Byte

8.45 关闭射频

命令：0x09

关闭辅助处理器某个通道的射频信号，以减小读卡机的功耗. 控制射频芯片的读卡机有定时功能，在某个通道寻卡成功后超过一定时间未关闭时，会自动关断射频信号. 该定时由参数 AutoSleepTime 决定，参数的单位为 0.1 秒，默认为 50(0x0032)，即 5 秒之后关断.设置调制模式命令可以修改这个参数. 如果该参数大于 0xFFF0，则禁用自动关断射频功能.

接收数据段：1 字节射频通道.

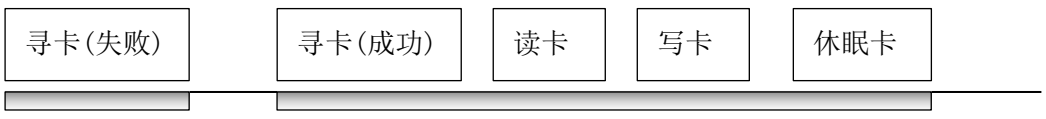
Channels
1 Bytes

返回数据段：1 字节关闭操作结果，0x00 表示操作成功.

Operation Result
1 Byte

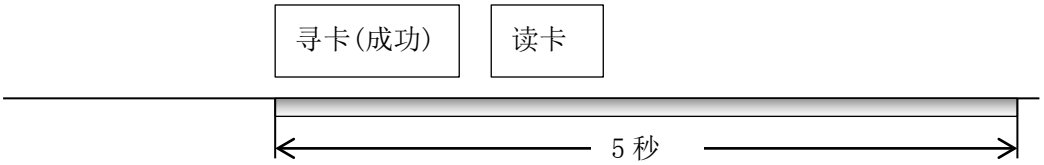
射频信号的开关流程如下：

- 用户调用休眠卡命令关断射频



- 用户调用关闭射频命令关断射频

- 自动关断射频



- 延时写入 Mifare 卡等内部寻卡命令(8.6 节至 8.11 节)

8.46 引导编程

命令: 0x4D

该命令对主处理器的 NAND Flash 进行编程操作. 在执行此命令之前, 用户必须先执行辅助处理器引导命令, 使得主处理器进入测试状态. 然后通过内存映射操作向内存映射区域 0x10000000 写入 16K 字节数据. 执行该命令后, 会将写入的 16K 数据烧写到 NAND Flash 中.

接收数据段: 2 字节写入 NAND Flash Block 号, 该参数的范围由 Flash 的尺寸决定, 对于 512Mb flash, 从 0x0000 至 0x1000, 对于 256Mb flash, 从 0x0000 至 0x0800. 每一个 Block 的尺寸为 16K 字节, 即如果该参数为 0x000A, 则实际写入 NAND Flash 的偏移量为 160K 字节, 对应地址为 0x00028000.

NAND Flash Block Index
2 Bytes

返回数据段: 1 字节编程操作结果, 0x00 表示成功.

Operation Result
1 Byte

9. 辅助处理器内存映射

本节描述了辅助处理器的内存映射，该功能有助于主处理器对读卡机进行深入操作. 用户可以通过该内存映射，直接操作射频调制芯片的寄存器，查看辅助处理器状态等.

起始地址	长度	读写权限	描述	单字节	4 字节
0x00000000	3K 字节	RW	辅助处理器内部对用户开放的 DataFlash 区,地址从 0x00000000 到 0x00000BFF.读取和写入必须 4 字节对齐.		√
0x00010000	64 字节	RW	射频通道 1 对应的调制芯片寄存器，从 0x00 到 0x3F	√	
0x00011000	1 字节	RO	射频通道 1 上一个操作芯片的 SAK 值.	√	√
0x00011002	10 字节	RO	射频通道 1 上一个操作芯片的 UID 值.	√	
0x0001100E	2 字节	RO	射频通道 1 上一个操作芯片的 ATQA 值.	√	
0x00011010	64 字节	RO	射频通道 1 上一个操作芯片的 ATS 值.	√	√
0x00011050	6 字节	WO	射频通道 1 的 Mifare 卡密钥区.	√	
0x00011060	1 字节	RW	射频通道 1 的延时命令允许出错次数	√	
0x00011061	1 字节	RW	射频通道 1 的延时命令延迟时间	√	
0x00012000	512 字节	RW	射频通道 1 的 EEROM 区		√
0x00020000	64 字节	RW	射频通道 2 对应的调制芯片寄存器，从 0x00 到 0x3F	√	
0x00021000	1 字节	RO	射频通道 2 上一个操作芯片的 SAK 值.	√	√
0x00021002	10 字节	RO	射频通道 2 上一个操作芯片的 UID 值.	√	
0x0002100E	2 字节	RO	射频通道 2 上一个操作芯片的 ATQA 值.	√	
0x00021010	64 字节	RO	射频通道 2 上一个操作芯片的 ATS 值.	√	√
0x00021050	6 字节	WO	射频通道 2 的 Mifare 卡密钥区.	√	
0x00021060	1 字节	RW	射频通道 2 的延时命令允许出错次数	√	
0x00021061	1 字节	RW	射频通道 2 的延时命令延迟时间	√	
0x00022000	512 字节	RW	射频通道 2 的 EEROM 区		√
0x00030000	1 字节	RW	当前选择使用的 SAM 卡槽	√	√
0x00030100	15 字节	RO	SAM 卡 0 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030110	1 字节	RW	SAM 卡 0 的波特率，参考 8.18 节	√	
0x00030120	5 字节	RW	SAM 卡 0 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030130	1 字节	RW	SAM 卡 0 的命令超时参数，参考编程手册 5.7 节	√	
0x00030131	1 字节	RW	SAM 卡 0 的 ATR 超时参数，参考编程手册 5.7 节	√	
0x00030200	15 字节	RO	SAM 卡 1 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030210	1 字节	RW	SAM 卡 1 的波特率，参考 8.18 节	√	
0x00030220	5 字节	RW	SAM 卡 1 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030230	1 字节	RW	SAM 卡 1 的命令超时参数，参考编程手册 5.7 节	√	
0x00030231	1 字节	RW	SAM 卡 1 的 ATR 超时参数，参考编程手册 5.7 节	√	

0x00030300	15 字节	RO	SAM 卡 2 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030310	1 字节	RW	SAM 卡 2 的波特率，参考 8.18 节	√	
0x00030320	5 字节	RW	SAM 卡 2 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030330	1 字节	RW	SAM 卡 2 的命令超时参数，参考编程手册 5.7 节	√	
0x00030331	1 字节	RW	SAM 卡 2 的 ATR 超时参数，参考编程手册 5.7 节	√	
0x00030400	15 字节	RO	SAM 卡 3 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030410	1 字节	RW	SAM 卡 3 的波特率，参考 8.18 节	√	
0x00030420	5 字节	RW	SAM 卡 3 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030430	1 字节	RW	SAM 卡 3 的命令超时参数，参考编程手册 5.7 节	√	
0x00030431	1 字节	RW	SAM 卡 3 的 ATR 超时参数，参考编程手册 5.7 节	√	
0x00030500	15 字节	RO	SAM 卡 4 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030510	1 字节	RW	SAM 卡 4 的波特率，参考 8.18 节	√	
0x00030520	5 字节	RW	SAM 卡 4 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030530	1 字节	RW	SAM 卡 4 的命令超时参数，参考编程手册 5.7 节	√	
0x00030531	1 字节	RW	SAM 卡 4 的 ATR 超时参数，参考编程手册 5.7 节	√	
0x00030600	15 字节	RO	SAM 卡 5 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030610	1 字节	RW	SAM 卡 5 的波特率，参考 8.18 节	√	
0x00030620	5 字节	RW	SAM 卡 5 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030630	1 字节	RW	SAM 卡 5 的命令超时参数，参考编程手册 5.7 节	√	
0x00030631	1 字节	RW	SAM 卡 5 的 ATR 超时参数，参考编程手册 5.7 节	√	
0x00030700	15 字节	RO	SAM 卡 6 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030710	1 字节	RW	SAM 卡 6 的波特率，参考 8.18 节	√	
0x00030720	5 字节	RW	SAM 卡 6 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030730	1 字节	RW	SAM 卡 6 的命令超时参数，参考编程手册 5.7 节	√	
0x00030731	1 字节	RW	SAM 卡 6 的 ATR 超时参数，参考编程手册 5.7 节	√	
0x00030800	15 字节	RO	SAM 卡 7 的历史字节，历史字节的最大长度为 15 字节.	√	
0x00030810	1 字节	RW	SAM 卡 7 的波特率，参考 8.18 节	√	
0x00030820	5 字节	RW	SAM 卡 7 的 Guard 延时参数，参考编程手册 5.7 节	√	
0x00030830	1 字节	RW	SAM 卡 7 的命令超时参数，参考编程手册 5.7 节	√	
0x00030831	1 字节	RW	SAM 卡 7 的 ATR 超时参数，参考编程手册 5.7 节	√	
0x00040000	64 字节	RW	辅助处理器 HID 设备的发送缓冲区	√	√
0x00040200	64 字节	RO	辅助处理器 HID 设备的接收缓冲区	√	√
0x10000000	16K 字节	WO	辅助处理器烧写 Flash 的 Block 缓冲区		√