



国家电网  
STATE GRID

国网信通产业集团北京智芯微电子科技有限公司  
BEIJING SMARTCHIP MICROELECTRONICS TECHNOLOGY COMPANY LIMITED  
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

# 基于面向对象协议的 智能电能表安全模块 产品手册

版本号: V1.1.6

# 目录

版本历史 .....	1
1. 芯片简介 .....	4
1.1 概述 .....	4
1.2 产品特点 .....	4
1.3 结构框图 .....	5
2. 引脚分配及典型电路 .....	5
2.1 引脚分配 .....	5
2.2 参考电路 .....	6
2.2.1 连接标识说明 .....	6
2.2.2 参考电路设计要点 .....	6
3. 电气特性及时序参数 .....	7
3.1 直流参数 .....	7
3.1.1 直流特性 (DC3V) (-40℃至 +85℃) .....	7
3.1.2 直流特性 (DC5V) (-40℃至 +85℃) .....	7
3.2 交流参数 (3V/5V 电源) (-40℃至 +85℃) .....	8
3.3 绝对最大额定值 .....	8
4. 信息交换 .....	9
4.1 SPI 通信接口 .....	9
4.2 SPI 通信协议描述 .....	9
4.3 SPI 通信流程 .....	10
4.4 设计要点 .....	11
4.5 SPI 通信时序 .....	11
4.5.1 SPI 通讯时序说明 .....	11
4.5.2 SSN 时序要求 .....	11
4.5.2 SPI 通信时序要求 .....	14
4.5.3 参考逻辑 .....	15
4.6 命令的结构和处理 .....	15
4.6.1 发送数据结构 .....	16
4.6.2 接收数据结构 .....	16
4.6.3 状态字节 .....	16
4.7 数据重发机制 .....	17
4.7.1 发送数据错误 .....	17
4.7.2 接收数据错误 .....	17
5. 交互指令流程 .....	17
5.1 远程操作流程 .....	17
5.1.1 读取 (获取 ESAM 信息、读取钱包) .....	17

5.1.2 建立应用连接（会话密钥协商） .....	18
5.1.3 安全传输数据处理（主站到电能表） .....	19
5.1.4 安全传输数据处理（电能表到主站） .....	22
5.1.5 终端抄读电能表 .....	22
5.1.6 文件传输（软件比对） .....	23
5.1.7 红外查询 .....	24
5.1.8 红外认证 .....	24
5.2 本地操作指令流程 .....	24
5.2.1 本地身份认证 .....	24
5.2.2 用户卡 .....	25
5.2.3 参数预置卡 .....	28
5.3 通用指令说明 .....	29
<b>6. 文件结构 .....</b>	<b>30</b>
6.1 ESAM 文件结构 .....	30
6.1.1 文件目录 .....	30
6.1.2 表号文件 .....	30
6.1.3 钱包文件 .....	30
6.1.4 安全标识文件 .....	30
6.1.5 参数信息文件 .....	31
6.1.6 当前套电价文件 .....	32
6.1.7 备用套电价文件 .....	32
6.1.8 运行信息文件 .....	33
6.2 参数预置卡文件结构 .....	33
6.2.1 文件目录 .....	33
6.2.2 指令信息文件 .....	34
6.2.3 钱包文件 .....	34
6.2.4 当前套电价文件 .....	34
6.2.5 备用套电价文件 .....	35
6.3 用户卡文件结构 .....	36
6.3.1 文件目录 .....	36
6.3.2 参数信息文件 .....	36
6.3.3 钱包文件 .....	36
6.3.4 当前套电价文件 .....	37
6.3.5 备用套电价文件 .....	37
6.3.6 返写信息文件 .....	38
<b>7. 封装尺寸及联系方式 .....</b>	<b>39</b>
7.1 封装尺寸说明 .....	39
7.2 订货联系方式 .....	40

## 版本历史

版本号	修改日期	修改内容
V1.0.0	2016.8.29	初稿
V1.1.0	2016.10.25	<p>1、第 6.1.1 节 ESAM 文件目录增加安全文件标识，增加 6.1.4 节安全文件标识结构。</p> <p>2、修改 6.1.5ESAM 当前套电价文件结构。</p> <p>3、修改 6.1.6ESAM 备用套电价文件中备用套阶梯电价长度，修改保留字节长度。</p> <p>4、修改钱包操作，将初始化、开户/充值、退费合并为一个流程。</p> <p>5、术语统一，增加软件比对流程。</p>
V1.1.1	2016.11.21	<p>1、5.1.5 章节将“电表序列号”改为“电表表号”</p> <p>2、按照 13 标准修改 ESAM、用户卡、参数预置卡的文件结构，只是修改文件内容，文件的 FID 不变。</p> <p>3、修改本地交互流程，用户卡客户编号的偏移改动</p> <p>4、设置 ESAM 参数时，需要将 Data 区的 0AD+LEN 删除后组帧发给芯片，表号设置除</p>

		外
V1.1.2	2017.1.13	1、修改状态字节。
V1.1.3	2017.1.24	1、新增 VCC 电源供电纹波限制。
V1.1.4	2017.2.8	<p>1、本地交互操作指令流程中，用户卡和参数预置卡的流程增加写电表 ESAM 参数信息文件内容。</p> <p>2、ESAM 文件更新描述中增加参数信息文件</p> <p>3、用户卡交互流程中的更新钱包文件指令长度“0C”改为“000C”</p>
V1.1.5	2017.5.24	<p>1、对 2.2.2 章节增加芯片上电相关说明；</p> <p>2、对 5.1.3 章节修改第 5 步骤、第 6 步骤描述</p> <p>3、增加 5.1.7 红外查询和 5.1.8 红外认证章节</p> <p>4、对 6.1.5、6.1.6、6.1.7、6.2.2、6.2.4、6.2.5、6.3.2、6.3.4、6.3.5 章节修改字段名称，将“两套分时费率切换时间”修改为“备用套分时费率切换时间”。将“年第 n 结算日”修改为“阶梯第 n 结算日”。将“两套阶梯切换时间”修改为</p>

		“备用套阶梯切换时间”。
V1.1.6	2017.8.11	1、对 2.2.2 章节增加芯片上电相关说明； 2、修改软件比对中数据项内容，与 698.45 协议对应。

北京智芯微电子科技有限公司

## 1. 芯片简介

### 1.1 概述

智能电能表安全模块，简称电表 ESAM (Embedded Secure Access Module, 嵌入式安全控制模块)，具有普遍安全应用价值的嵌入式数据安全产品。硬件具有 SM1 国密算法、硬件随机数发生器、电压和频率检测等多种安全性保护机制，可有效保证传输数据的机密性和完整性。

### 1.2 产品特点

- 支持 SPI 通信接口。
- 支持 SM1 国密算法。
- 支持电压检测、频率检测等安全防护机制。
- 具有真随机数发生器。
- 具有存储器数据加密和总线加扰机制。
- 数据存储区容量:32Kbytes。
- 数据保存时间不低于 10 年，数据存储区擦写次数不低于 50 万次。
- SPI 通信速率支持 1~10MHz，推荐使用 4MHz。
- 工作电压：2.7V~5.5V。
- 工作温度：-40℃~+85℃。

## 1.3 结构框图

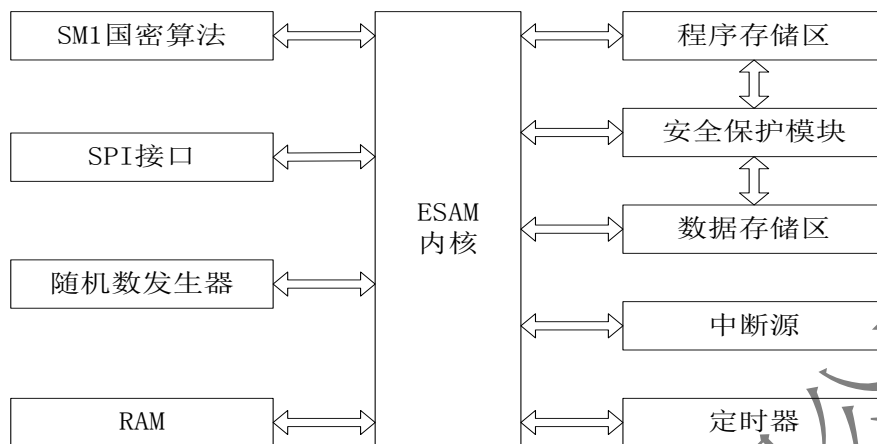


图 1ESAM 结构框图

## 2. 引脚分配及典型电路

### 2.1 引脚分配

ESAM 的引脚分配如下图所示：

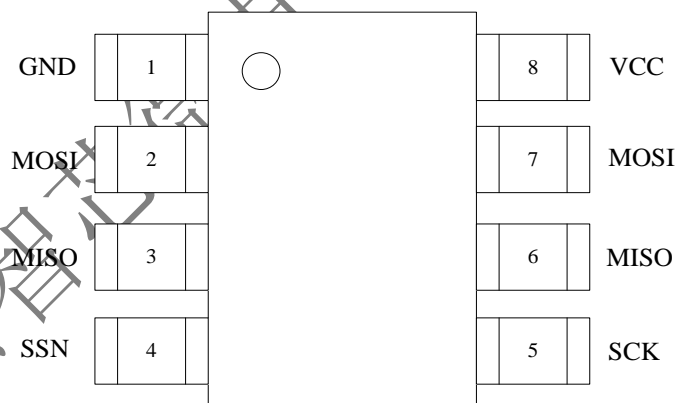


图 2ESAM 引脚分配图

引脚描述如下表所示：

表 1 引脚描述列表

引脚号	引脚名	功能描述
1	GND	地
2、7	MOSI	主出从入，引脚 2 与 7 需外部短接
3、6	MISO	主入从出，引脚 3 与 6 需外部短接
4	SSN	片选



5	SCK	时钟
8	VCC	电源

## 2.2 参考电路

为了能更安全有效地使用 ESAM 芯片，推荐使用如下参考电路图：

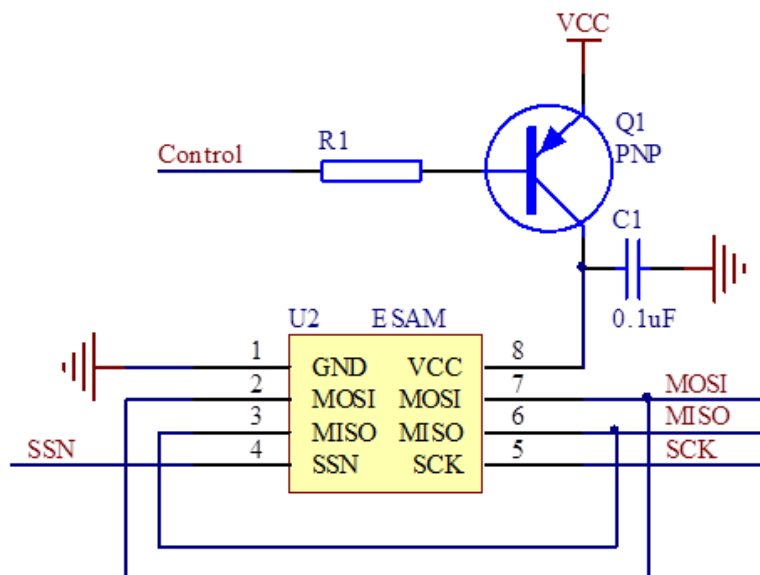


图 3ESAM 参考电路

### 2.2.1 连接标识说明

- Control: 用于控制 ESAM 电源的端口，与微控制器连接。
- MISO: ESAM 的输出端口。
- MOSI: ESAM 的输入端口。
- SCK: 时钟端口。
- SSN: ESAM 片选端口。

注：引脚 2 与 7 需外部短接，引脚 3 与 6 需外部短接。

### 2.2.2 参考电路设计要点

- 保证 ESAM 的 VCC 引脚电压从 0V 升至稳定工作电压的时间小于 100us。
- 保证 ESAM 在正常工作期间的 VCC 的纹波维持在工作电压 $\pm 100\text{mV}$  以内。
- 器件 Q1 可以是三极管或 PMOS 管，提供的最大电流保证大于 100mA。
- 当对 ESAM 进行主动断电再重新上电时：在给 ESAM 的 VCC 管脚断电过程中，应保证 MISO、MOSI、SSN、SCK 等管脚均处于低电平或高阻态，VCC 管脚保持低

电平持续时间大于 2ms，然后再给 ESAM 上电；ESAM 的 VCC 上电稳定后，先进行 SPI 模式配置，然后持续时间大于 5ms，再给 ESAM 发送指令。

- 当电能表和 ESAM 交互过程中发生断电时，给 ESAM 的 VCC 稳定上电后，先进行 SPI 模式配置，然后持续时间大于 100ms，再给 ESAM 发送指令。

### 3. 电气特性及时序参数

#### 3.1 直流参数

##### 3.1.1 直流特性 (DC3V) (-40℃至 +85℃)

表 2 直流特性 (DC3V)

参数	符号	最小值	典型值	最大值	单位
电源电压	VCC	2.7	3	3.3	V
电源电流	I <sub>CC</sub>	—	—	30	mA
电源峰值电流	I <sub>peak</sub>	—	—	60	mA
SCK	V <sub>IH</sub>	0.7×VCC	—	VCC	V
	V <sub>IL</sub>	0	—	0.6	V
MISO	V <sub>OH</sub>	0.7×VCC	—	VCC	V
	V <sub>OL</sub>	0	—	0.3×VCC	V
MOSI	V <sub>IH</sub>	0.7×VCC	—	VCC	V
	V <sub>IL</sub>	0	—	0.6	V
SSN	V <sub>IH</sub>	0.7×VCC	—	VCC	V
	V <sub>IL</sub>	0	—	0.6	V

##### 3.1.2 直流特性 (DC5V) (-40℃至 +85℃)

表 3 直流参数 (DC5V)

参数	符号	最小值	典型值	最大值	单位
电源电压	VCC	4.5	5	5.5	V
电源电流	I <sub>CC</sub>	—	—	30	mA
电源峰值电流	I <sub>peak</sub>	—	—	80	mA
SCK	V <sub>IH</sub>	0.7×VCC	—	VCC	V
	V <sub>IL</sub>	0	—	0.6	V
MISO	V <sub>OH</sub>	0.7×VCC	—	VCC	V

参数	符号	最小值	典型值	最大值	单位
	$V_{OL}$	0	—	$0.3 \times VCC$	V
MOSI	$V_{IH}$	$0.7 \times VCC$	—	VCC	V
	$V_{IL}$	0	—	0.6	V
SSN	$V_{IH}$	$0.7 \times VCC$	—	VCC	V
	$V_{IL}$	0	—	0.6	V

### 3.2 交流参数（3V/5V 电源）（-40℃至 +85℃）

表 4 交流特性

参数	符号	最小值	典型值	最大值	单位	条件
MOSI						
沿变时间	$t_R, t_F$	—	5, 5	—	ns	
MISO						
沿变时间	$t_R, t_F$	—	5, 5	—	ns	
SSN						
沿变时间	$t_R, t_F$	—	5, 5	—	ns	
SCK						
频率	$f_{SCK}$	—	4	—	MHz	
沿变时间	$t_R, t_F$	—	5, 5	—	ns	
占空比	—	—	50%	—		

### 3.3 绝对最大额定值

表 5 绝对最大额定值

参数	符号	最小值	典型值	最大值	单位
电源电压	VCC	2.7	—	5.5	V
输入电压	VIN	2.7	—	5.5	V
工作温度	TA	-40	—	+85	℃
存储温度	TS	-40	+25	+125	℃
抗瞬变脉冲群电压	VESD	2	6	—	KV
焊接温度	—	—	—	+260	℃
焊接时间	—	—	—	9	S

## 4. 信息交换

### 4.1 SPI 通信接口

表 6 SPI 通信接口

接口信号	芯片方向
SSN	IN
SCK	IN
MISO	OUT
MOSI	IN

### 4.2 SPI 通信协议描述

SPI 工作方式采用 MODE 3，时钟极性 (CPOL=1)，串行同步时钟的空闲状态为高电平，时钟相位 (CPHA=1)，在串行同步时钟的下降沿转换数据，上升沿采样数据。

主设备发送数据，ESAM 接收数据：

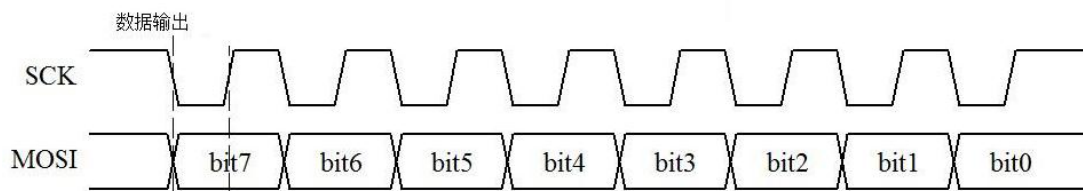


图 4ESAM 接收数据信号图

注：主设备在发送数据时，MISO 引脚需保持接收态，MISO 引脚上的数据为无效数据，主设备无需做处理，直接舍弃或不接收。

主设备接收数据，ESAM 发送数据：

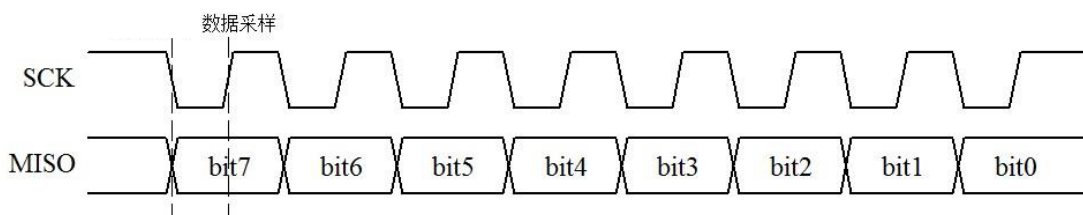


图 5ESAM 发送数据信号图

注：主设备在接收数据时，MOSI 引脚应始终保持低电平。

### 4.3 SPI 通信流程



图 6SPI 通信流程

## 4.4 设计要点

- SSN=0: 将 SSN 置低; SSN=1: 将 SSN 置高。
- Len1 代表长度的高字节, Len2 代表长度的低字节。
- LRC1 的计算方法: 对 CLA INS P1 P2 Len1 Len2 DATA 数据, 每个字节的异或值, 再取反。
- LRC2 的计算方法: 对 SW1 SW2 Len1 Len2 DATA 数据, 每个字节的异或值, 再取反。
- Len1 Len2 代表 DATA 域的长度, 不包括 LRC1 或 LRC2。

## 4.5 SPI 通信时序

### 4.5.1 SPI 通讯时序说明

- 图中紫色为 MOSI、黄色为 SSN、绿色为 CLK、红色为 MISO。SPI 通讯可分为下图中的三个过程: 发送、查询、接收。

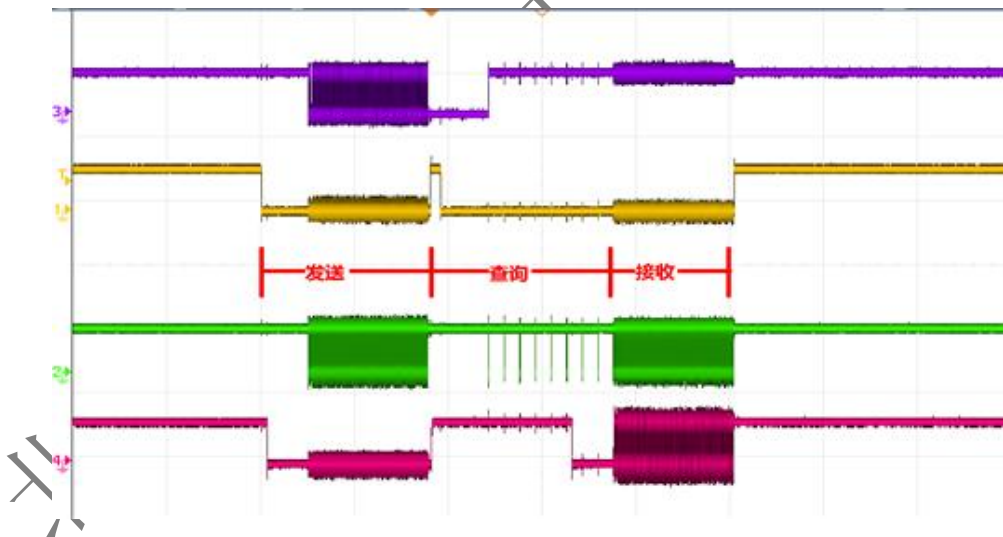


图 7 SPI 通信过程

### 4.5.2 SSN 时序要求

- SSN 每次拉低以后需要等待一段时间以后才可以进行 SPI 通讯, 该等待时间  $T_{cs1} > 50\mu s$ 。

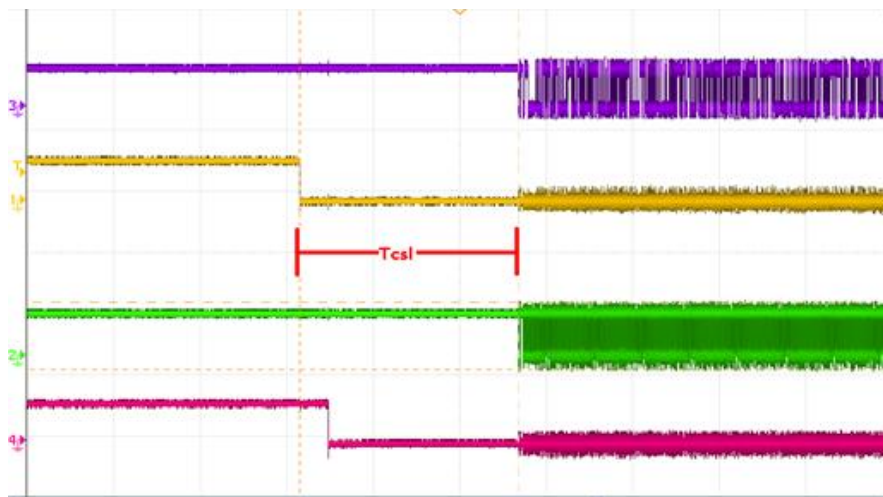


图 8 SSN 拉低时序

- 每次 SPI 通讯结束后，需等待一段时间才可以将 SSN 拉高，该等待时间  $T_{csd} > 3\mu s$ 。

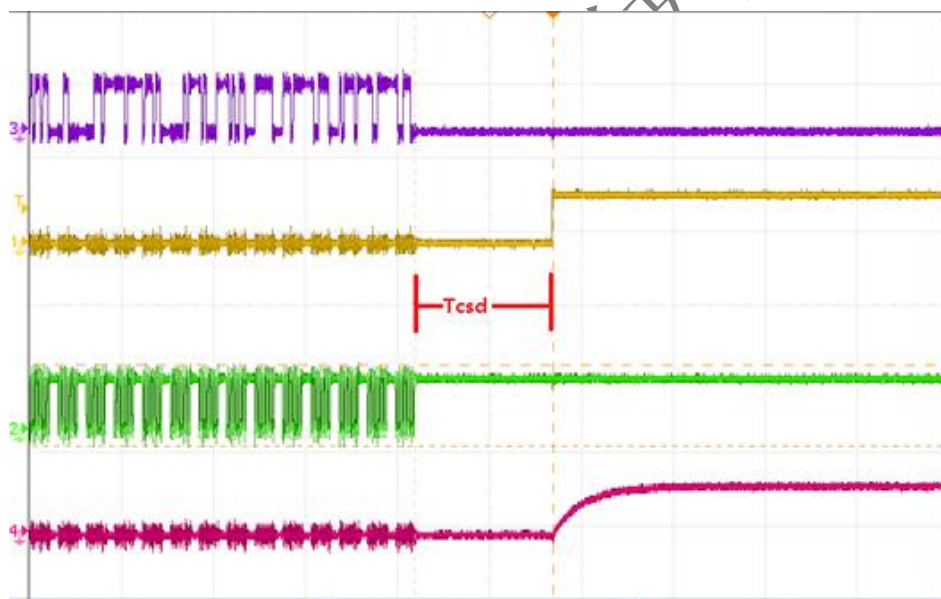


图 9 通信结束 SSN 时序

- SSN 每次拉高必须维持一定的时间， $T_{csh} > 10\mu s$ 。

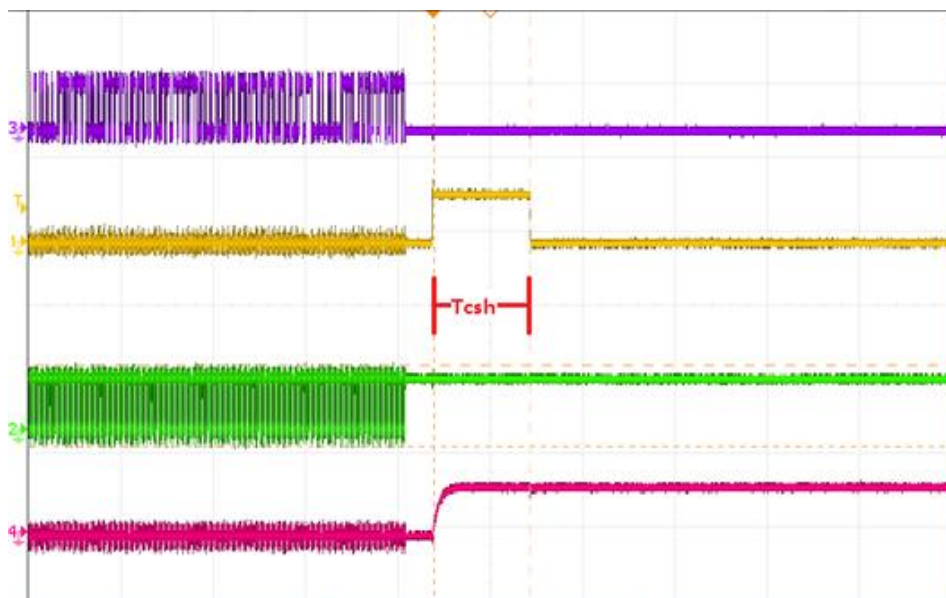


图 10 SSN 拉高时序

- SPI 频率与字符间隔

SPI 频率最大支持 10MHz， $T_{clk} > 100\text{ns}$ ；字节有效传输时间  $T_b > 1.5\mu\text{s}$ 。

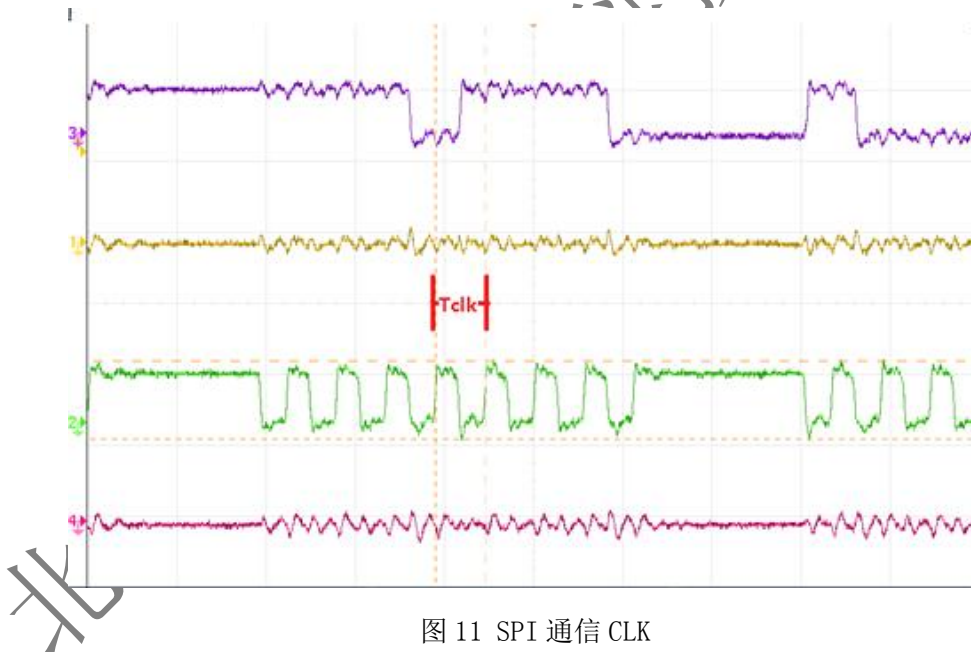


图 11 SPI 通信 CLK



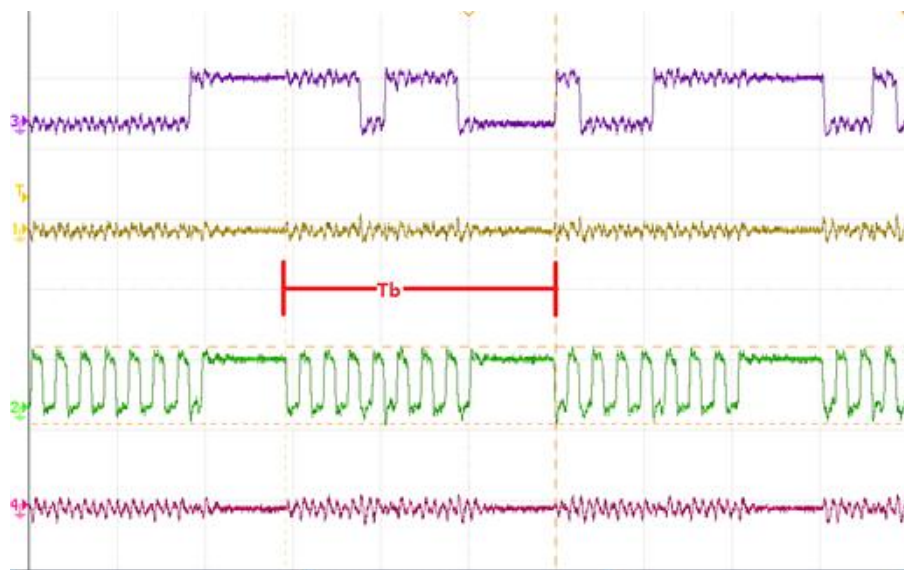


图 12 字符传输

#### ● SPI 查询

该过程用于查询 ESAM 指令是否执行完成，当收到 0x55 时，即可接收后续执行结果。查询时，SPI 主设备每隔一段时间接收一个数据，并判断是否为 0x55，该间隔时间  $T_q > 15\mu s$ 。为了防止 ESAM 异常导致系统挂死，总的查询时间  $T_{tq} < 3s$ 。

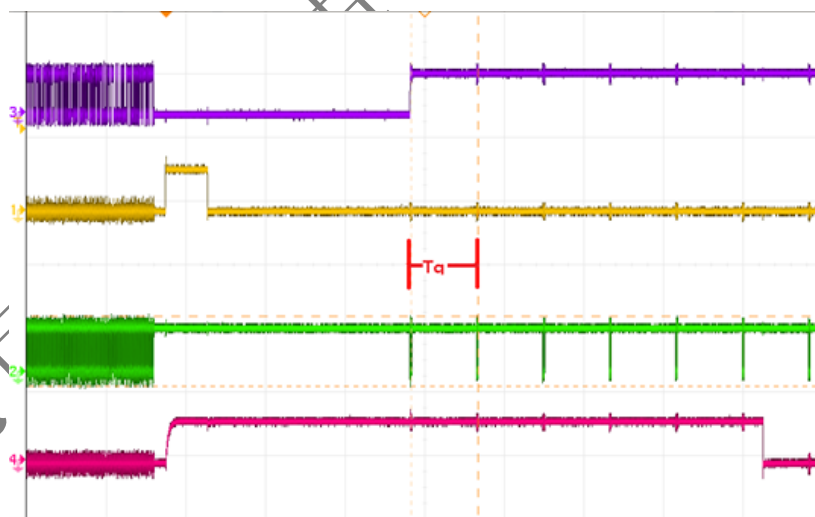


图 13 查询时间

#### 4.5.2 SPI 通信时序要求

表 7 SPI 通信时序要求

标识	最小值	最大值	推荐值	说明
Tcs1	50us	100us	60us	SSN 拉低持续时间

Tcsd	3us	10us	5us	通讯结束，SSN 拉低持续时间
Tcsh	10us	50us	10us	SSN 每次拉高持续时间
Tclk	100ns	1us	250ns	对应 SPI 频率，1MHz~10MHz
Tb	1.5us	10us	3us	SPI 有效通讯时间
Tq	15us	100us	20us	指令查询间隔时间
Ttq	1s	3s	2s	指令查询总时间

### 4.5.3 参考逻辑

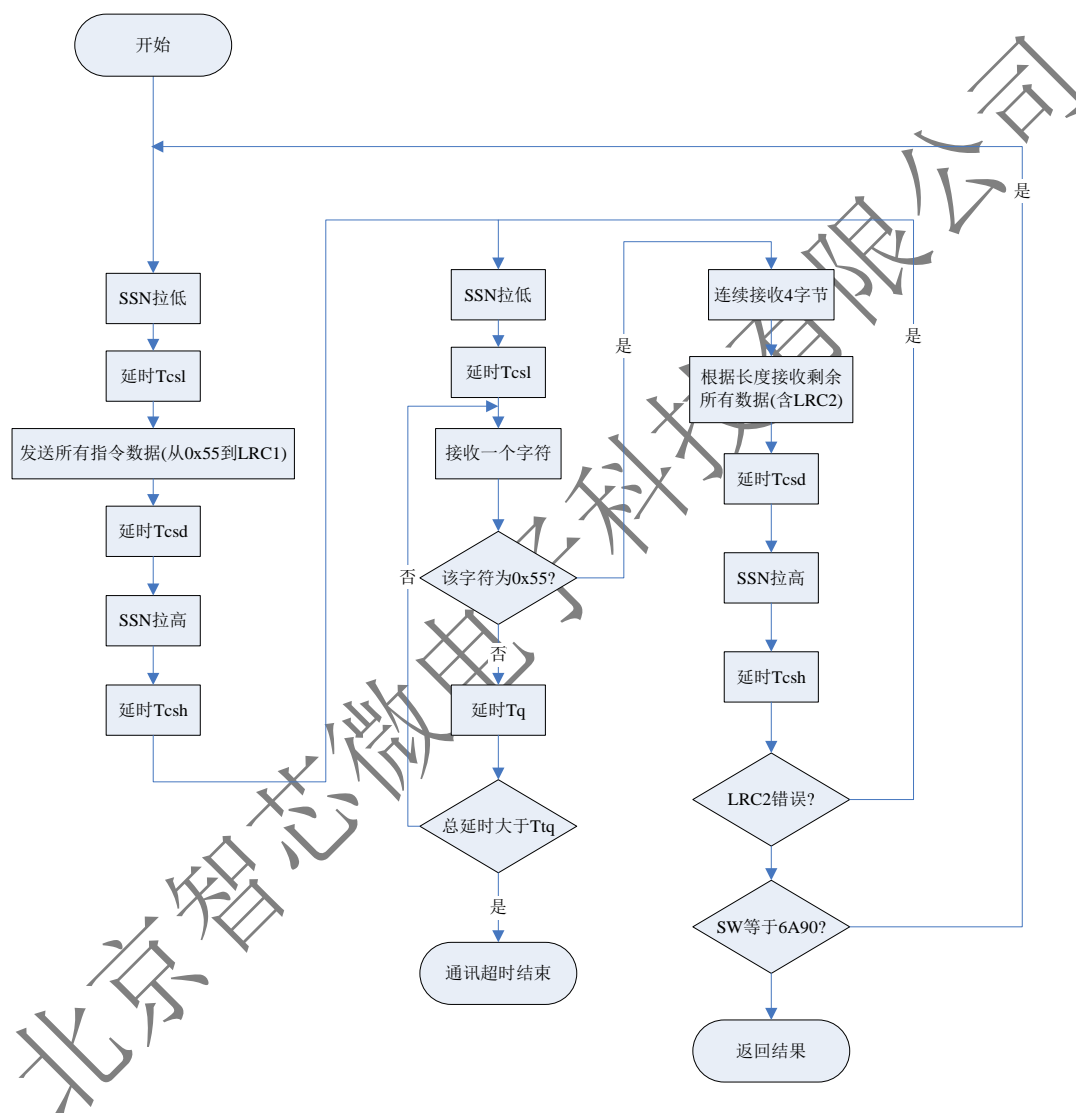


图 14 逻辑图

## 4.6 命令的结构和处理

命令由接口设备发起，ESAM 应答。

注：若无特殊说明，本章节默认数字采用 16 进制表示。

#### 4.6.1 发送数据结构

发送数据的结构为：55 CLA INS P1 P2 Len1 Len2 DATA LRC1，其中：

- 55 为发送命令结构的命令头；
- CLA 是命令类别；
- INS 是命令类别中的指令代码；
- P1、P2 是一个完成指令代码的参考符号；
- Len1 Len2 是后续 DATA 的长度，不包含 LRC1，由两字节表示；
- DATA 是由 ESAM 来处理的输入数据；
- LRC1 是发送数据的校验值，计算方法见 SPI 通信流程说明。

#### 4.6.2 接收数据结构

接收数据的结构为：SW1 SW2 Len1 Len2 DATA LRC2，其中：

- SW1 SW2 是指令执行完毕后，从设备返回的状态字；
- Len1 Len2 是后续 DATA 的长度，不包含 LRC2，由两字节表示；
- DATA 是 ESAM 处理数据完毕后，返回的输出数据；
- LRC2 是接收数据的校验值，计算方法见 SPI 通信流程说明；

#### 4.6.3 状态字节

SW1、SW2 构成接收数据的起始序列，起始序列在命令的起始指示芯片的状态。SW1 SW2= ‘9000’ 表示正常响应。

表 8 状态字信息表

SW1	SW2	含义
90	00	成功
6A	86	P1P2 不正确
67	00	LC 长度错误
69	01	计数器不正确
69	03	随机数无效
69	04	外部认证错误
69	07	TIMER 超时
69	82	会话未建立
69	85	使用条件不满足
69	88	计算错误
69	89	MAC 校验错

SW1	SW2	含义
6A	80	不正确的数据域
6A	90	LRC 校验错误
90	86	验签错误

## 4.7 数据重发机制

SPI 传输层支持错误重发机制。当出现 SPI 数据传输数据错时，允许重新发送。支持错误重发次数为 3 次。

### 4.7.1 发送数据错误

电表发送数据，如果 ESAM 返回的错误码为 6A90，表明数据在传输时出现错误，此时电表可以重发指令。

### 4.7.2 接收数据错误

电表收到数据后，需校验从 ESAM 接收的 LRC 与接收数据计算的 LRC 是否一致，如果不一致，说明 ESAM 数据在传输过程中出现错误，此时电表可以重新启动接收流程（将 SSN 置高，高电平保持时间至少 10us 以上，再将 SSN 置低，保持 MOSI 置高(低)，进入指令查询和接收流程。

## 5. 交互指令流程

注：若无特殊说明，本章节默认数字采用 16 进制表示。

### 5.1 远程操作流程

#### 5.1.1 读取（获取 ESAM 信息、读取钱包）

步骤	主站	电表和 ESAM	备注
1	主站下发获取 ESAM 信息命令		
2		发送：803600FF0000 返回：9000+LEN+Data1	批量获取电表安全芯片全部信息： Data1： ESAM 版本号（5B）、 ESAM 序列号（8B）、 保留（1B）

			<p>对称密钥版本 (16B)、 会话时效门限 (4B)、 会话时效剩余时间 1 (4B)、 当前计数器 (ASCTR: 单地址应用协商计数器 (4B)、 AMRCTR: 电表主动上报计数器 (4B) AGSEQ: 应用广播通信序列号 (4B)) ESAM 发行信息 (40B)</p>
3		<p>发送: 803600P20000 返回: 9000+LEN+ Data2</p>	<p>单项获取电表安全芯片信息: P2: 01: ESAM 版本号 (5B) 02: ESAM 序列号 (8B) 03: 保留 (1B) 04: 对称密钥版本 (16B)、 05: 会话时效门限 (4B)、 会话时效剩余时间 1 (4B)、 06: 当前计数器 (ASCTR: 单地址应用协商计数器 (4B)、 AMRCTR: 电表主动上报计数器 (4B) AGSEQ: 应用广播通信序列号 (4B)) 07: ESAM 发行信息 (40B)</p>
4		<p>发送: 80480000000100 返回: 9000+000E+Data3</p>	<p>读取钱包 Data3: 包含 4 字节购电金额 +4 字节购电次数+6 字节客户编号</p>

#### 5.1.2 建立应用连接 (会话密钥协商)

步骤	主站	电表和 ESAM	备注
1	主站建立应用连接下发电表会话协商数据, 包含 SessionData1 密文 1 和 MAC1 客户机签名 1		SessionData1:32 字节 MAC1:4 字节
2		<p>发送: 810200000024+ SessionData1+ MAC1 返回: 9000+0034+ SessionData2+MAC2</p>	<p>SessionData2: 服务器随机数, 48 字节 MAC2:服务器签名信息, 4 字节</p>
3		电表上传 SessionData2、	

		MAC2	
4	主站获得 SessionData2、MAC2 进行校验		

### 5.1.3 安全传输数据处理（主站到电能表）

步骤	主站	电表和 ESAM	备注
1	建立应用连接		读取电能表数据、广播操作可不需要建立应用连接
2	主站发送任务数据，包含应用数据单元 Data, 数据验证信息		使用应用会话密钥对数据进行计算 MAC Data: 明文应用数据单元或者密文应用数据单元 数据验证信息: SID_MAC 或 RN 或 RN_MAC 或 SID SID: 包含 4 字节标识+附加数据 AttachData
3		广播说明: 电表收到数据后判断组地址或广播地址、标识的前 4 个字节是否正确 标识: 8016480X	当组地址或广播地址最后一位有效位 为 1 时 X=1; 为 2 时 X=2; 为 3 时 X=3; 为 4 时 X=4; 为 5 时 X=5; 为 6 时 X=6; 为 7 时 X=7; 为 8 时 X=8; 为 9 时 X=9; 为 0 或 A 时 X=A;
4		若数据验证信息为随机数 RN, 则跳第 5 步;  若数据验证信息为 SID_MAC, 发送: 4 字节标识+附加数据 AttachData+Data+ MAC 返回: 9000+LEN+Data2  若数据验证信息为 SID, 发送: 4 字节标识+附加数据 AttachData+Data 返回: 9000+LEN+Data2	SID: 包含 4 字节标识+附加数据 AttachData
5		执行相应的应用层协议处理	读取（读取电能表数据）、 设置（二类参数设置）、 操作（远程控制、电表清零、事件/需量清零） ESAM 相关操作 （具体见后续步骤说明）
6		将 Data2 组织数据得到返	广播业务不需要返回帧给主

步骤	主站	电表和 ESAM	备注
		回帧 Data3	站  读取电能表数据时，根据 5.1.3.1 流程执行，跳到第 8 步骤进行验证  ESAM 相关操作需要根据 5.1.3.2 相关流程执行
7		发送：811C00+P2+Lc+ Data3 返回：9000+LEN+ Data4	Data3：数据返回帧 Data4：包含应用数据单元（和数据验证信息） 由电表按照下述规则组织各个数据项。 P2： 明文+MAC 方式：11 密文：A6 密文+MAC：A7
8	主站验证，获得确认帧或否认帧		

#### 5.1.3.1 读取（抄读电能表数据）

步骤	主站/掌机	电表和 ESAM	备注
1	根据 5.1.3 的第 2 步骤获得应用数据单元 Data, 数据验证信息，		Data：明文应用数据单元 数据验证信息：RN
2		发送：800E4002+LC+ Data1 返回：9000+0004+MAC	电表计算明文+MAC LC:Data1 长度，2 字节 Data1: RN+PlainData
3		发送：800A4002+LC+ Data1 返回：9000+Len+Data2	电表计算密文 LC:Data1 长度，2 字节 Data1：包含 RN+抄读数据 PlainData Data2：密文应用数据单元
4		发送：80104002+LC+ Data1 返回：9000+Len+Data2 +MAC	电表计算密文+MAC LC:Data1 长度，2 字节 Data1：包含 RN+抄读数据 PlainData Len: Data2 和 MAC 长度 Data2：密文应用数据单元 数据验证信息：MAC
5		组织数据返回主站	明文应用数据单元：抄读数据 PlainData 数据验证信息包含 MAC
6	验证 MAC 数据		主站验证抄读数据

### 5.1.3.2 ESAM 相关操作

#### (1)操作（ESAM 操作读取 ESAM 文件内容）

步骤	主站/掌机	电表和 ESAM	备注
1	根据 5.1.3 的 1、2、4 步骤获得 Data2		Data2: 包含 ESAM 操作信息 数据验证码 SID (包含标识、 附加数据 AttachData)
2		发送: 4 字节标识+附加数据 AttachData 返回: 9000+LEN+Data1+MAC	明文+MAC 方式读取文件 Data1: 文件内容
3	根据 5.1.3 的 6、7、8 步骤返回主站		

#### (2) 数据更新（更新 ESAM 文件内容：安全标识文件、表号、参数信息、备用套电价）

步骤	主站	电表和 ESAM	备注
1	根据 5.1.3 的 1、2、4 步骤获得 Data2		Data2 包含数据更新信息，参数内容 D1、数据验证码 SID_MAC (包含标识、附加数据 AttachData，数据 MAC)
2		发送: 4 字节标识+附加数据 AttachData+D1 +数据 MAC 返回: 9000+0000	向芯片发送指令时，D1 的内容需要删除 OAD+LEN，5 字节的内容后再组帧发给芯片，表号设置除外。
3	根据 5.1.3 的 6、7、8 步骤返回主站		

#### (3) 密钥更新（电能表对称密钥更新）

步骤	主站	电表和 ESAM	备注
1	根据 5.1.3 的 1、2、4 步骤获得 Data2		Data2: 包含密钥密文 (Endata1)、数据验证码 SID_MAC (包含标识、附加数据 AttachData、数据 MAC)
2		电能表判断标识为 812E0000	
3		发送: 标识+附加数据 AttachData+ Endata1+ MAC 返回: 9000+0000	
4	根据 5.1.3 的 6、7、8 步骤返回主站		

#### (4) 钱包操作（初始化/远程开户/充值/退费）

步骤	主站	电表和 ESAM	备注
1	根据 5.1.3 的 1、2、4 步骤获得 Data2		Data2: 包含钱包操作信息 D1: 包含操作类型、购电金额、购电次数、客户编号、数据验证码 SID_MAC，表号



2		发送：标识+附加数据 AttachData+Data3+MAC 返回：9000+0000	Data3: 购电金额 4 字节+购电次数 4 字节+客户编号 6 字节
3	根据 5.1.3 的 6、7、8 步骤返回主站		

(5)操作（更新安全模式、会话时效门限、电价切换时间、费率时段、对时任务等）

步骤	主站	电表和 ESAM	备注
1	根据 5.1.3 的 1、2、4 步骤获得 Data2		Data2 包含数据更新信息，参数内容 Data1、数据验证码 SID_MAC（包含标识、附加数据 AttachData，数据 MAC）
2		发送：4 字节标识+附加数据 AttachData+Data1 + 数据 MAC 返回：9000+0000	
3	根据 5.1.3 的 6、7、8 步骤返回主站		

5.1.4 安全传输数据处理（电能表到主站）

5.1.4.1 上报（电能表主动上报）

步骤	主站	电表和 ESAM	备注
1		发送：80140103+LC+Data1 返回：9000+LEN+Data2+4 字节 MAC	LC: Data1 长度，2 字节 Data1: 明文数据 Data2: 12 字节 RN_MAC, 包含 12 字节 Data2 和 4 字节 MAC
2		电表上传数据 Data1、RN_MAC 给主站	
3	主站对上报数据进行验证，并保存数据，下发应答帧		
4		发送：800E4081+LC+Data2+00000000+Data3+MAC 返回：9000+0000	Data3 接收主站下发应答帧数据

5.1.5 终端抄读电能表

步骤	终端和 TESAM	电表和 ESAM	备注
1	发送：800400100000 返回：9000+LEN+ RN 下发随机数到电表，包含应用数据单元 Data, 数据验证信息		Data: 明文应用数据单元 数据验证信息： RN

步骤	终端和 TESAM	电表和 ESAM	备注
2		电能表根据安全模式要求按照第 3 或者第 4 或者第 5 步骤进行	
3		发送: 800E4002+LC+Data1 返回: 9000+0004+MAC	电表计算明文+MAC LC:Data1 长度, 2 字节 Data1: 包含 RN+抄读数据 PlainData
4		发送: 800A4002+LC+Data1 返回: 9000+Len+Data2	电表计算密文 LC:Data1 长度, 2 字节 Data1: 包含 RN+抄读数据 PlainData Data2: 密文应用数据单元
5		发送: 80104002+LC+Data1 返回: 9000+Len+Data2+MAC	电表计算密文+MAC LC:Data1 长度, 2 字节 Data1: 包含 RN+抄读数据 PlainData Len: Data2 和 MAC 长度 Data2: 密文应用数据单元 数据验证信息: MAC
6		组织数据返回终端	
7	终端根据接收数据格式, 分别对应安全模式进行验证		
8	发送: 800E4887+LC+电表表号+ RN + PlainData+MAC 返回: 9000+0000		终端明文+MAC 方式验证抄读数据
9	发送: 800C4807+LC+电表表号+ RN + Data2 返回: 9000+ Len+Data3		终端密文方式验证抄读数据 Data3:明文数据
10	发送: 80124807+LC+电表表号+RN+ Data2+MAC 返回: 9000+ Len+Data3		终端密文+MAC 方式验证抄读数据 Data3:明文数据

#### 5.1.6 文件传输（软件比对）

步骤	主站	电表和 ESAM	备注
1	主站下发软件比对参数		密钥索引: 09~0D
2		发送: 800A48P2+LC+ 分散因子+随机数+ Data1 返回: 9000+Len+Data2	电表计算密文 P2: 为密钥索引, 09~0D LC:后续数据长度, 2 字节

			分散因子：对应 698.45 协议附录 E.1.2.b 中的分散因子。 随机数：对应 698.45 协议附录 E.1.2.c 中的随机数。 Data1：对应 698.45 协议附录 E.1.2.d 中的加密数据。 Data2：对应 698.45 协议附录 E.1.2.e 中的加密后数据。
3		电表返回软件比对信息	
4	主站验证软件比对信息		

### 5.1.7 红外查询

步骤	掌机对 ESAM 操作	电表和 ESAM	备注
1	掌机 ESAM 取随机数 RN, 下发红外查询命令和随机数到电表, 包含应用数据单元 Data, 数据验证信息 RN1		操作此步骤之前先按照 5.1.1 步骤获取芯片 ESAM 序列号, 通过 5.1.3.2 章节第 (1) 小结方法获得表号; 数据验证信息: RN1;
2		发送: 800808030010+0000+表号+RN1 返回: 9000+0008+Endata1	
3		发送: 800400080000 返回: 9000+0008+RN2	
4	根据 5.1.3 的 6、7、8 步骤返回主站		

### 5.1.8 红外认证

步骤	掌机对 ESAM 操作	电表和 ESAM	备注
1	掌机通过 ESAM 根据 RN2 计算得到密文 2, 下发红外认证命令到电表, 包含应用数据单元密文 2;		密文 2: 8 字节
2		发送: 800600010008+密文 2 返回: 9000+0000	
3	根据 5.1.3 的 6、7、8 步骤返回主站		

## 5.2 本地操作指令流程

### 5.2.1 本地身份认证

步骤	电能表对 CPU 卡操作	电能表对 ESAM 操作	说明
----	--------------	--------------	----

步骤	电能表对 CPU 卡操作	电能表对 ESAM 操作	说明
1	发送: Reset 返回: 3BXXXXXXXX+CardReset8		CPU 卡复位
2	发送: 00a40000023F00 返回: 61XX 或 9000		CPU 卡选择 3F00 主文件
3	发送: 00a4000002DF01 返回: 61XX 或 9000		CPU 卡选择 DF01 目录
4		发送: 800400080000 返回: 9000 数据: 9000+0008+Rand8	ESAM 取随机数
5		发送: 80080801+0010+CardReset8+Rand8 返回: 9000+0008+随机数密文 K1	根据 CPU 卡复位信息后 8 字节分散, 加密
6	发送: 0088000108+Rand8 返回: 6108 发送: 00C0000008 返回: 随机数密文 K2+9000		CPU 卡加密随机数, 得到随机数密文 K2
7			比较 K1 与 K2, 如果相同则身份认证通过

### 5.2.2 用户卡

步骤	电能表对 CPU 卡操作	电能表对 ESAM 操作	解释	说明
1		本地身份认证		身份认证
2	发送: 00B08100LC 返回: DATA+9000		明文读取用户卡参数信息文件, LC: DATA 长度	
3	发送: 00B085P2 (起始地址) LC 返回: 返写信息+9000		读用户卡返写信息文件, LC: 返写信息长度	读用户卡返写信息文件
4	发送: 0084000008 返回: Rand8+9000		取用户卡随机数	
5		发送: 80080802+0010+CardReset8+Rand8 返回: 9000+0008+ 随机数密文 K3	用户卡复位信息后 8 字节作为分散因子, 分散得到临时密钥。用临时密钥加密随机数, 得到随机数密文 K3	用户卡返写权限认证

步骤	电能表对 CPU 卡操作	电能表对 ESAM 操作	解释	说明
6	发送: 0082000208+ K3 返回: 9000		用户卡进行返写权限认证	
7		发送: 800400040000 返回: 9000+0004+Rand4	取 ESAM 随机数用于 MAC 计算	取随机数
8	发送: 04B0820009+ Rand4+804200000C 返回: 610C 发送: 00C000000C 返回: DATA+MAC+9000		明文+MAC 方式读取用户卡钱包文件 DATA: 4 字节购电金额+4 字节购电次数	更新 ESAM 钱包文件
9		发送: 80420000+000C+ DATA+MAC 返回: 9000+新余额+交易金额	ESAM 进行钱包充值	
10	发送: 04B0812409+ Rand4+832A8F060A 返回: 610A 发送: 00C000000A 返回: DATA+MAC+9000		明文+MAC 方式读取客户编号	更新客户编号
11		发送: 832A8F06000A+ DATA+MAC 返回: 9000+0000	明文+MAC 方式写入客户编号	
12	发送: 04B081P2 (起始) 09+Rand4+832A84+P2+LC 返回: 61XX 发送: 00C00000LC 返回: DATA+MAC+61XX		明文+MAC 方式读取用户卡参数信息文件 LC: DATA 长度+MAC 长度(DATA 长度为用户卡电价文件中有有效数据指定长度) P2: 文件偏移地址, 1 字节	更新 ESAM 参数信息文件
13		发送: 832A84+P2+LC+ DATA+MAC 返回: 9000+0000	明文+MAC 方式写入 ESAM 参数信息文件 LC: 后续数据长度, 2 字节	
14	发送: 04B083P2 (起始) 09+Rand4+832A85+P2+LC 返回: 61XX 发送: 00C00000LC 返回: DATA+MAC+61XX		明文+MAC 方式读取用户卡当前套电价文件 LC: DATA 长度+MAC 长度(DATA 长度为用户卡电价文件中有有效数据指定长度) P2: 文件偏移地址, 1 字节	更新 ESAM 当前套电价文件 (P2 起始地址要保持一致)

步骤	电能表对 CPU 卡操作	电能表对 ESAM 操作	解释	说明
15		发送: 832A85+P2+LC+DATA+MAC 返回: 9000+0000	明文+MAC 方式写入 ESAM 当前套电价文件 LC: 后续数据长度, 2 字节	
16	发送: 04B084P2 (起始) 09+Rand4+832A86+P2+LC 返回: 61XX 发送: 00C00000LC 返回: DATA+MAC+9000		明文+MAC 方式读取用户卡备用套电价文件 LC: DATA 长度+MAC 长度(DATA 长度为用户卡电价文件中有有效数据指定长度) P2: 文件偏移地址, 1 字节	更新 ESAM 备用套电价文件 (P2 起始地址要保持一致)
17		发送: 832A86+P2+LC+DATA+MAC 返回: 9000+0000	明文+MAC 方式写入备用套电价文件 LC: 后续数据长度, 2 字节 P2: 文件偏移地址, 1 字节	
18	发送: 0084000004 返回: 用户卡随机数 Rand5+9000			
19		发送: 832C0007+LC1+48+CardReset8+Rand5+P3+LEN +04D685P2+LC 返回: 9000+DATA+MAC	明文+MAC 方式读取 ESAM 运行信息文件, LC: DATA 长度+MAC 长度(DATA 长度为写入用户卡数据的长度) LC1: 后续数据长度, 2 字节 P3: 偏移地址, 2 字节 LEN: 将要读取的数据, 2 字节	更新用户卡返写信息文件
	04D685 P2 (起始) +LC+DATA+MAC 返回: 9000		明文+MAC 方式写入用户卡返写信息文件 P2: 偏移地址, 1 字节	

### 5.2.3 参数预置卡

步骤	电能表对 CPU 卡操作	电能表对 ESAM 操作	解释	说明
1	本地身份认证			
2	发送: 00B08100LC 返回: DATA+9000		明文读取参数预置卡指令信息文件, LC: DATA 长度	读取指令信息
3		发送: 800400040000 返回: 9000+0004+Rand4	取 ESAM 随机数, 用于 MAC 计算	取 ESAM 随机数
4	发送: 04B081P2 (起始) 09+Rand4+832A84+P2+LC 返回: 61XX 发送: 00C00000LC 返回: DATA+MAC+61XX		明文+MAC 方式读取用户卡参数信息文件 LC: DATA 长度+MAC 长度 (DATA 长度为用户卡电价文件中有效数据指定长度) P2: 文件偏移地址, 1 字节	更新 ESAM 参数信息文件
5		发送: 832A84+P2+LC+DATA+MAC 返回: 9000+0000	明文+MAC 方式写入 ESAM 参数信息文件 LC: 后续数据长度, 2 字节 P2: 写文件偏移地址, 1 字节	
6	发送: 04B0820009+Rand4+833E000008 返回: 6108 发送: 00C0000008 返回: 初始化金额+MAC+9000		明文+MAC 方式读取参数预置卡钱包文件的 4 字节购电金额	更新 ESAM 钱包文件
7		发送: 833E00000008+DATA+MAC 返回: 9000+0000	明文+MAC 方式写入 DATA : 4 字节 ESAM 初始化钱包预置金额	
8	发送: 04B083P2 (起始) 09+ Rand4+832A85+P2+LC 返回: 61XX 发送: 00C00000LC 返回: DATA+MAC+9000		明文+MAC 方式读取参数预置卡当前套电价文件, LC: DATA 长度+MAC 长度 P2: 写文件偏移地址, 1 字节	更新 ESAM 当前套电价文件 (P2 起始地址要保持一致)
9		发送: 832A85+P2+LC+DATA+MAC 返回: 9000+0000	明文+MAC 方式写入 ESAM 当前套电价文件	

步骤	电能表对 CPU 卡操作	电能表对 ESAM 操作	解释	说明
			LC: 后续数据长度, 2 字节 P2: 写文件偏移地址, 1 字节	
10	发送: 04B084P2 (起始 09+ Rand4+832A86+P2+LC 返回: 61XX 发送: 00C00000LC 返回: DATA+MAC+9000		明文+MAC 方式读取参数预置卡备用套电价文件, LC: DATA 长度+MAC 长度	更新 ESAM 备用套电价文件 (P2 起始地址要保持一致)
11		发送: 832A86+P2+LC+DATA+MAC 返回: 9000+0000	明文+MAC 方式写入 ESAM 备用套电价文件 LC: 后续数据长度, 2 字节 P2: 写文件偏移地址, 1 字节	

### 5.3 通用指令说明

序号	电能表对 ESAM 操作	说明
1	发送: 804600000004+ Data1 返回: 9000+0008+Data2	明文扣款 Data1: 扣款金额, 4 字节 Data2: 包含 4 字节剩余金额+4 字节交易金额
2	发送: 802C+FID+000500+Data1 返回: 9000+LEN+Data3	读取 ESAM 文件信息 FID: 文件标识, 2 字节 Data1: 2 字节偏移地址+2 字节读取长度
3	发送: 80480000000100 返回: 9000+000E+Data4	读取钱包 Data4: 包含 4 字节购电金额+4 字节购电次数+6 字节客户编号
4	发送: 800400+P2+0000 返回: 9000+LEN+Rand	取随机数 P2: 取随机数长度, 04/08/10
5	返送: 802A0007+LC+00+偏移地址 2 字节+Data 返回: 9000+0000	写 ESAM 运行信息文件 LC: Data 长度+3, 为 2 字节;



## 6. 文件结构

### 6.1 ESAM 文件结构

#### 6.1.1 文件目录

附表 1ESAM 文件目录

文件	内容说明	标识
EF01	表号文件	0001
EF01	钱包文件	0001
EF03	安全标识文件	0003
EF04	参数信息文件	0004
EF05	当前套电价文件	0005
EF06	备用套电价文件	0006
EF07	运行信息文件	0007

#### 6.1.2 表号文件

附表 2 表号文件

序号	数据项	长度	格式	备 注
1	表号对象标识	4	HEX	40020200
2	表号长度	1	HEX	08
3	表号	8	BCD	0000000000000000

#### 6.1.3 钱包文件

附表 3 钱包文件

序号	数据项	长度	格式	备 注
1	购电金额	4	HEX	00000000
2	购电次数	4	HEX	00000000
3	客户编号	6	HEX	000000000000

#### 6.1.4 安全标识文件

附表 4 安全标识文件

序号	数据项	长度	格式	备 注
1	电价存储标志	1	HEX	默认 0，表示一类参数不存储 ESAM，按照二类参数更新流程进行密文+MAC 更新 1：一类参数存储 ESAM,明文+MAC 方

				式更新
--	--	--	--	-----

## 6.1.5 参数信息文件

附表 5 参数信息文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	
4	保留	1	HEX	
5	参数更新标志位	1	HEX	
6	保留	4	HEX	000000000000
7	备用套分时费率切换时间	5	BCD	年月日时分
8	保留	1	HEX	
9	报警金额 1	4	BCD	XXXXXX.XX
10	报警金额 2	4	BCD	XXXXXX.XX
11	电流互感器变比	3	BCD	XXXXXX
12	电压互感器变比	3	BCD	XXXXXX
13	表号	6	HEX	
14	客户编号	6	BCD	
15	电卡类型	1	BCD	
16	身份认证时效性	2	BCD	分钟
17	校验和	1	HEX	
18	结束码	1	HEX	0x16

## 6.1.6 当前套电价文件

附表 6 当前套电价文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	0xFC
4	费率 1	4	BCD	XXXX. XXXX
5	.....	...	.....	.....
6	费率 32	4	BCD	XXXX. XXXX
7	阶梯值 1	4	BCD	XXXXXX. XX
8	.....	...	...	.....
9	阶梯值 6	4	BCD	XXXXXX. XX
10	阶梯电价 1	4	BCD	XXXX. XXXX
11	.....	...	...	.....
12	阶梯电价 7	4	BCD	XXXX. XXXX
13	阶梯第 1 结算日	3	BCD	月日時
14	阶梯第 2 结算日	3	BCD	月日時
15	阶梯第 3 结算日	3	BCD	月日時
16	阶梯第 4 结算日	3	BCD	月日時
17	保留	60	HEX	默认为全 00
18	校验和	1	HEX	
19	结束码	1	HEX	0x16

## 6.1.7 备用套电价文件

附表 7 备用套电价文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	0xFC
4	费率 1	4	BCD	XXXX. XXXX
5	.....	...	.....	.....
6	费率 32	4	BCD	XXXX. XXXX
7	阶梯值 1	4	BCD	XXXXXX. XX
8	.....	...	...	.....
9	阶梯值 6	4	BCD	XXXXXX. XX
10	阶梯电价 1	4	BCD	XXXX. XXXX
11	.....	...	...	.....
12	阶梯电价 7	4	BCD	XXXX. XXXX
13	阶梯第 1 结算日	3	BCD	月日時

14	阶梯第 2 结算日	3	BCD	月日时
15	阶梯第 3 结算日	3	BCD	月日时
16	阶梯第 4 结算日	3	BCD	月日时
17	备用套阶梯切换时间	5	BCD	年月日时分
18	保留	55	HEX	默认为全 00
19	校验和	1	HEX	
20	结束码	1	HEX	0x16

## 6.1.8 运行信息文件

附表 8 运行信息文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x11
3	数据长度	2	HEX	
4	保留	1	HEX	
5	电流互感器变比	3	BCD	XXXXXXXX
6	电压互感器变比	3	BCD	XXXXXXXX
7	表号	6	BCD	XXXXXXXXXXXXXXXX
8	客户编号	6	BCD	
9	剩余金额	4	HEX	
10	购电次数	4	HEX	
11	透支金额	4	BCD	XXXXXX. XX
12	保留	4	HEX	默认 00000000
13	非法卡插入次数	3	BCD	
14	返写日期时间	5	BCD	年月日时分
15	校验和	1	HEX	
16	结束码	1	HEX	0x16

## 6.2 参数预置卡文件结构

### 6.2.1 文件目录

附表 9 参数预置卡文件目录

文件	内容说明	标识
MF	主文件	3F00
EF19	复位信息文件	0019
DF01	电表应用目录文件	DF01

EF01	指令信息文件	0001
EF02	钱包文件	0002
EF03	当前套电价文件	0003
EF04	备用套电价文件	0004

## 6.2.2 指令信息文件

附表 10 指令信息文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x06
3	长度	2	HEX	
4	保留	1	HEX	
5	参数更新标志位	1	HEX	
6	保留	4	HEX	000000000000
7	备用套分时费率切换时间	5	BCD	年月日时分
8	保留	1	HEX	
9	报警金额 1	4	BCD	XXXXXX.XX
10	报警金额 2	4	BCD	XXXXXX.XX
11	电流互感器变比	3	BCD	XXXXXX
12	电压互感器变比	3	BCD	XXXXXX
13	校验和	1	HEX	
14	结束码	1	HEX	0x16

## 6.2.3 钱包文件

附表 11 钱包文件

序号	数 据 项	长度	格式	备 注
1	预置金额	4	HEX	00000000

## 6.2.4 当前套电价文件

附表 12 当前套电价文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	0xFC
4	费率 1	4	BCD	XXXX. XXXX
5	.....	...	.....	.....
6	费率 32	4	BCD	XXXX. XXXX
7	阶梯值 1	4	BCD	XXXXXX. XX
8	.....	...	...	.....

9	阶梯值 6	4	BCD	XXXXXX. XX
10	阶梯电价 1	4	BCD	XXXX. XXXX
11	.....	...	...	.....
12	阶梯电价 7	4	BCD	XXXX. XXXX
13	阶梯第 1 结算日	3	BCD	月日時
14	阶梯第 2 结算日	3	BCD	月日時
15	阶梯第 3 结算日	3	BCD	月日時
16	阶梯第 4 结算日	3	BCD	月日時
17	保留	60	HEX	默认为全 00
18	校验和	1	HEX	
19	结束码	1	HEX	0x16

## 6.2.5 备用套电价文件

附表 13 备用套电价文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	0xFC
4	费率 1	4	BCD	XXXX. XXXX
5	.....	...	.....	.....
6	费率 32	4	BCD	XXXX. XXXX
7	阶梯值 1	4	BCD	XXXXXX. XX
8	.....	...	...	.....
9	阶梯值 6	4	BCD	XXXXXX. XX
10	阶梯电价 1	4	BCD	XXXX. XXXX
11	.....	...	...	.....
12	阶梯电价 7	4	BCD	XXXX. XXXX
13	阶梯第 1 结算日	3	BCD	月日時
14	阶梯第 2 结算日	3	BCD	月日時
15	阶梯第 3 结算日	3	BCD	月日時
16	阶梯第 4 结算日	3	BCD	月日時
17	备用套阶梯切换时间	5	BCD	年月日時分
18	保留	55	HEX	默认为全 00
19	校验和	1	HEX	
20	结束码	1	HEX	0x16

## 6.3 用户卡文件结构

### 6.3.1 文件目录

附表 14 用户卡文件目录

文件	内容说明	标识
MF	主文件	3F00
EF19	复位信息文件	0019
DF01	电表应用目录文件	DF01
EF01	参数信息文件	0001
EF02	钱包文件	0002
EF03	当前套电价文件	0003
EF04	备用套电价文件	0004
EF05	返写信息文件	0005

### 6.3.2 参数信息文件

附表 15 参数信息文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	
4	保留	1	HEX	
5	参数更新标志位	1	HEX	
6	保留	4	HEX	000000000000
7	备用套分时费率切换时间	5	BCD	年月日时分
8	保留	1	HEX	
9	报警金额 1	4	BCD	XXXXXX.XX
10	报警金额 2	4	BCD	XXXXXX.XX
11	电流互感器变比	3	BCD	XXXXXX
12	电压互感器变比	3	BCD	XXXXXX
13	表号	6	HEX	
14	客户编号	6	BCD	
15	电卡类型	1	BCD	
16	校验和	1	HEX	
17	结束码	1	HEX	0x16

### 6.3.3 钱包文件

附表 16 钱包文件

序号	数据项	长度	格式	备 注
1	购电金额	4	HEX	000000. 00

2	购电次数	4	HEX	00000000
---	------	---	-----	----------

#### 6.3.4 当前套电价文件

附表 17 当前套电价文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	0xFC
4	费率 1	4	BCD	XXXX. XXXX
5	.....	...	.....	.....
6	费率 32	4	BCD	XXXX. XXXX
7	阶梯值 1	4	BCD	XXXXXX. XX
8	.....	...	...	.....
9	阶梯值 6	4	BCD	XXXXXX. XX
10	阶梯电价 1	4	BCD	XXXX. XXXX
11	.....	...	...	.....
12	阶梯电价 7	4	BCD	XXXX. XXXX
13	阶梯第 1 结算日	3	BCD	月日時
14	阶梯第 2 结算日	3	BCD	月日時
15	阶梯第 3 结算日	3	BCD	月日時
16	阶梯第 4 结算日	3	BCD	月日時
17	保留	60	HEX	默认为全 00
18	校验和	1	HEX	
19	结束码	1	HEX	0x16

#### 6.3.5 备用套电价文件

附表 18 备用套电价文件

序号	数据项	长度	格式	备 注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x01
3	长度	2	HEX	0xFC
4	费率 1	4	BCD	XXXX. XXXX
5	.....	...	.....	.....
6	费率 32	4	BCD	XXXX. XXXX
7	阶梯值 1	4	BCD	XXXXXX. XX
8	.....	...	...	.....
9	阶梯值 6	4	BCD	XXXXXX. XX
10	阶梯电价 1	4	BCD	XXXX. XXXX
11	.....	...	...	.....
12	阶梯电价 7	4	BCD	XXXX. XXXX
13	阶梯第 1 结算日	3	BCD	月日時



14	阶梯第 2 结算日	3	BCD	月日時
15	阶梯第 3 结算日	3	BCD	月日時
16	阶梯第 4 结算日	3	BCD	月日時
17	备用套阶梯切换时间	5	BCD	年月日時分
18	保留	55	HEX	默认为全 00
19	校验和	1	HEX	
20	结束码	1	HEX	0x16

### 6.3.6 返写信息文件

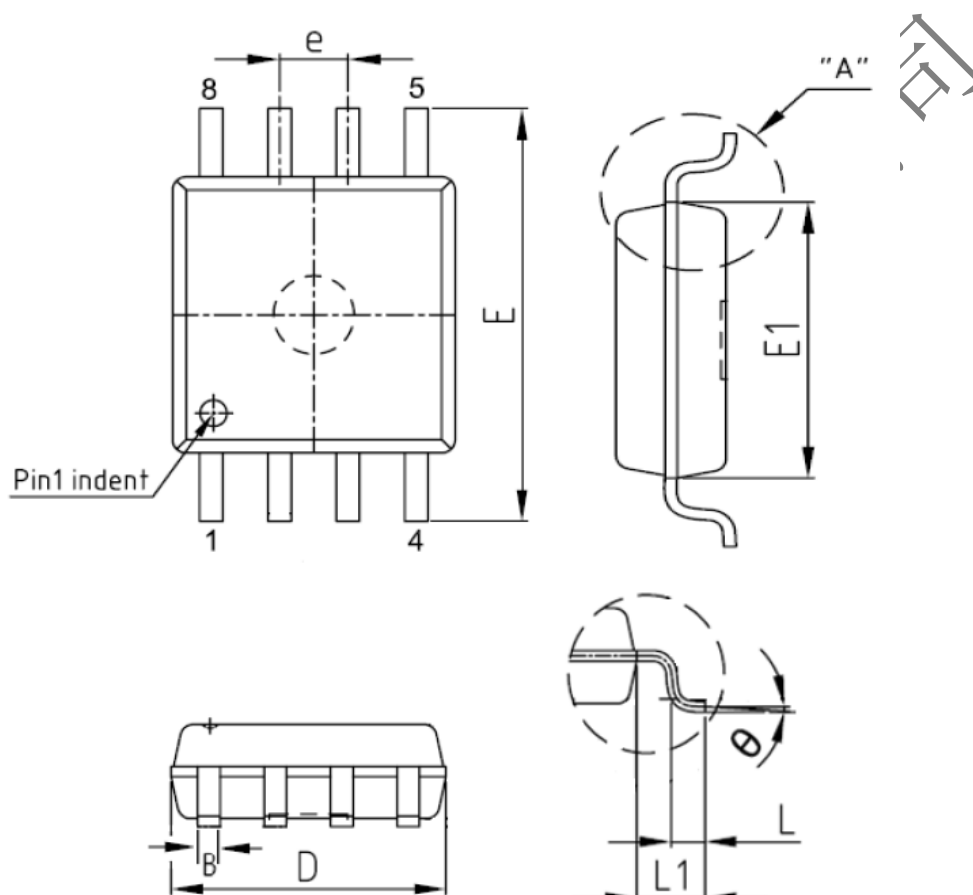
附表 19 返写信息文件

序号	数据项	长度	格式	备注
1	起始码	1	HEX	0x68
2	命令码	1	HEX	0x11
3	数据长度	2	HEX	
4	保留	1	HEX	
5	电流互感器变比	3	BCD	XXXXXX
6	电压互感器变比	3	BCD	XXXXXX
7	表号	6	BCD	XXXXXXXXXXXXXXXX
8	客户编号	6	BCD	
9	剩余金额	4	HEX	
10	购电次数	4	HEX	
11	透支金额	4	BCD	XXXXXX. XX
12	保留	4	HEX	
13	非法卡插入次数	3	BCD	
14	返写日期时间	5	BCD	年月日時分
15	校验和	1	HEX	
16	结束码	1	HEX	0x16

## 7. 封装尺寸及联系方式

### 7.1 封装尺寸说明

智能电能表安全模块采用 S0IC8 封装，外形尺寸图如下：



符号	尺寸 (单位: mm)		
	最小值	标准值	最大值
D	5.18	5.28	5.38
E	7.70	7.90	8.10
E1	5.18	5.28	5.38
e	----	1.27	----
B	0.31	0.41	0.51
L1	----	1.37	----
L	0.50	0.65	0.80
$\theta$	0°	----	8°

## 7.2 订货联系方式

销售电话：010-82156228-322

技术支持电话：010-57123291

地址：北京市海淀区西小口路 66 号东升科技园北领地 A-3

北京智芯微电子科技有限公司



**北京智芯微电子科技有限公司**  
BEIJING SMARTCHIP MICROELECTRONICS TECHNOLOGY COMPANY LIMITED

📍 地址：北京市海淀区西小口路66号中关村东升科技园A-3座

☎ 电话：010-82156080

📠 传真：010-82156090

✉ 邮编：100192