

[手持终端]

内置T-ESAM安全单元的计量现场手持终端设计

文/内蒙古电力营销服务与运营管理中心 尹卿 肖斌 王建强 谭富贵

通过对手持终端软硬件平台及工作流程的研究，提出了终端的硬件结构和软件实施方案，该终端为电力用户现场服务提供了安全有效的技术手段。

随着智能电网建设的逐步推进，在智能电表推广应用过程中，迫切需要一款支持计量现场作业的移动手持终端。安装到计量现场手持终端的安全模块（以下简称T-ESAM安全模块）。该模块能够实现密钥存储、加解密流程控制，在手持终端与管理系统、电能表和采集终端通信时，完成身份认证及数据信息加解密操作。

系统结构设计

本文中CPU采用基于ARM926EJ-S的AT91SAM9G45，集成了常用的和具有高传输速率的硬件接口，AT91SAM9G45支持用于存储程序和数据的数据的DDR2和NAND Flash存储器接口。

1. 通用接口设计

这里采用SPI及ISO7816接口分别与RFID及T-ESAM模块连接；10位ADC用来检查电池电量、16位PWM用来生成38KB载波信号用作红外载波信号；UART口分别连接安全单元、抄表模块及GPS模块接口；两组高速存储卡控制器支持SD卡操作；设计过程中因USB接口模块较多且需要主从切换，采用USB扩展口分别连接相应模块。设计中采用模块化思路，根据《计量现场手持设备技术规范》中硬件配置V型要求，设计了全功能型手持终端，包含所有模块的插接口，可

根据业务现场实际需求进行减配。

2. USB专用接口设计

USB系统包含三类硬件设备：USB主机（USB HOST）、USB设备（USB DEVICE）和USB集线器（USB HUB）。USB HOST管理USB系统，每毫秒产生一帧数据，发送配置请求对设置进行配置操作，对总线上的错误进行管理；USB DEVICE接收总线数据包并判断地址确认是否响应USB HOST；USB HUB用作设备扩展连接，所有USB DEVICE都连接在USB HUB端口上。

设计中因USB接口模块较多且需要主从切换，所以采用USB2514进行USB口扩展分别连接摄像头、条码扫描模块、蓝牙及WIFI模块。

软件方案

采用开源的Linux操作系统开发嵌入式产品是当前一个新的技术热点，配合一款合适的图形用户界面能够使产品和用户进行友好便捷的交互。本方案采用Linux3.6进行内核及驱动等底层开发，Linux图形用户界面支持系统MiniGUI3.0.12进行终端应用开发。MiniGUI提供了完备的多窗口机制、开发中所需的对话框控件和预定义控件类、采用消息传递机制、支持多种汉字输入法、支持常见图像文件等，库

文件小巧可根据项目需求定制配置和编译，可移植性好。通过将开发中所需的MiniGUI核心库及依赖库进行GCC交叉编译后移植到ARM9平台指定路径下，可执行程序运行时链接到相应的库即可。

1. 驱动设计

设备驱动的作用是驱使硬件设备工作。驱动与底层硬件直接打交道，按照硬件设备的具体工作方式，读写设备的寄存器，完成设备的轮询、中断处理和DMA通信，进行物理内存向虚拟内存的映射等，最终让通信设备能收发数据，让显示设备能显示文字和画面，让存储设备能记录文件和数据。设备驱动充当了硬件和应用软件之间的纽带，它使得应用软件只需要系统软件的应用编程接口（API）就可以让硬件去完成要求的工作。

2. 应用及业务流程

终端软件架构层级含：数据存储层、数据访问层、基础操作类、协议层及UI层。MiniGUI是一个典型的消息驱动的GUI系统，UI层输入交互信号后，窗口响应消息，加入消息队列，通过消息循环执行窗口过程，通过UI界面可执行系统配置、任务同步及任务执行等功能。

为确保任务上传、下载及执行过程安全可靠，手持终端内置T-ESAM能够在设备内部完成密钥存储、加解密流程控制等。安全单元装有操作员卡和业务员卡，当计量现场手持设备与管理系统、智能电表和采集终端通信时，根据安全单元通信协议完成身份认证及数据信息加解密操作。

信息安全防护设计

1. 安全单元

终端内置安全单元（T-ESAM），作为设备的安全认证模块，提供加解密服务的硬件平台。内置了SM1、SM2、SM3及SM7等算法，可以实现数据的加密、解密、签名、验签、身份认证、访问权限控制和通信线路保护等多种功能，保证了计量现场作业终端数据存储、传输与交互的安全性。具有嵌入式安全操作系统，具备防检测、抗攻击和安全文件管理等特性。

2. 安全交互流程

（1）终端MCU与安全单元交互流程设计

计量手持终端与安全单元采用串行方式通

信，实现数据的加密、解密、签名、验签和身份认证等功能。由现场服务终端的控制单元发送命名启动帧，由安全单元发送响应帧结束。

（2）终端与主站交互流程设计

系统安全防护设计主站和终端，双方交互流程如下图所示。



图 手持终端与主站安全交互流程

1) 终端与主站之间基于数字证书技术，进行双向身份认证。

2) 终端与主站之间的双向身份认证通过后，双方建立安全通道。

3) 终端发起与主站的双向身份认证。

4) 认证成功后，主站读取终端的芯片序列号和密钥版本等信息。

5) 终端和主站之间开始进行业务交互。

结束语

本文设计了一款基于T-ESAM安全模块的计量现场手持终端设备，根据设备实际功能及性能需求，采用ARM9平台及Linux下MiniGUI图像界面系统嵌入T-ESAM安全单元的方案进行终端软硬件设计。设计中采用模块化思路，配备全功能型模块接口，可根据业务现场实际需求进行减配。通过与国网计量中心后台主站及内置T-ESAM芯片的智能电表进行身份认证、数据交互和任务下载执行等操作，终端功能满足规范技术要求，为电力用户现场服务提供了安全有效的技术手段。EA

（收稿日期：2018.09.18）

（编辑：白文亭）