DOI: 10.7667/PSPC151345

自主可控的安全 RTU 设计与实现

南亚希[1]，展 巍[2]，裴后宣[3]

(1. 山西国际电力集团有限公司，山西 太原 030002；2. 北京泰豪电力科技有限公司，北京 100176；
3. 中国电子信息产业集团有限公司第六研究所，北京 100083)

摘要：工业控制系统广泛应用于电力行业，成为维护电力系统安全、平稳运行的基础。为改进电力工业控制系统在电力设备信息安全技术上的不足，介绍了一种具有自主知识产权的配电自动化远方终端(RTU)的设计与实现方法。安全 RTU 采用自主可控的国产芯片作为核心处理器，通过外扩电能计量芯片提高采样精度，简化设计。基于国产加密算法的安全机制能实现数据在 VPN 隧道密文传输和用户认证访问。在实验室模拟工业现场测试表明该方法可以有效防止信息泄露以及木马病毒的攻击。

关键词：信息安全；远方终端；国产芯片；国密算法；加密认证

Design and implementation of a self-control secure RTU

NAN Yaxi[1], ZHAN Wei[2], PEI Houxuan[3]

(1. Shanxi International Electricity Group Limited Company, Taiyuan 030002, China; 2. Beijing Tellhow Power Technology Limited Company, Beijing 100176, China; 3. The 6th Research Institute of China Electronics Corporation, Beijing 100083, China)

Abstract: Industrial control system is widely used in power industry, which has become the base of maintaining power system running safely and steadily. To improve the deficiency of power industry control system in power equipment information security technology, this paper introduces a design and implementation method of distribution automation remote terminal (RTU) which is based on independent intellectual property rights. Secure RTU chooses a self-control homebred chip as the core processor, an energy measurement chip is extended to improve the acquisition accuracy and simplify the design. The security mechanism based on homebred encryption algorithm allows the cryptograph transfer in the VPN channel and credentials access. Test in the laboratory shows that this method can prevent information leakage and the Trojans virus.

This work is supported by National Information safety Foundation of the National Development and Reform Commission.

Key words: information security; RTU; homebred chip; homebred encryption algorithm; encryption and authentication

0 引言

随着计算机技术和网络通信技术应用于工业控制系统，出现了工业控制网络的诸多安全问题。2010 年，席卷全球工业界的震网(Stuxnet)蠕虫，已感染了全球超过 45 000 个网络，伊朗遭到的攻击最为严重，60%的个人电脑感染了这种病毒[1]。震网事件表明工业控制系统在信息安全的防护上存在较大漏洞，一旦被攻击，将对社会稳定和经济安全造成重大影响。电力工业控制系统信息安全问题同样不容忽视，电力设备是保证电力控制系统安全稳定运行的基础，配电自动化远方终端(RTU)用于柱上负荷开关、断路器、重合器等配电设备上，负责采集各个开关量及测量量，实现线路的故障识别、定位、隔离。按照约定的通信协议报告给上级主站或子站，并接受上级下达的命令。是电力自动化系统中的一个重要装置。目前国内外厂商生产的 RTU 在功能实现上能够基本满足用户需求，但在信息安全防护方面的研究仍处于空白，增强电力设备通信的安全性和可靠性，能有效防止电力系统重要信息的泄漏，

基金项目：国家发改委信息安全专项资金

维护电力系统的安全。同时随着智能电网建设的不断加快，物联网、大数据等新的理念不断出现，使得电力系统设备朝着智能化的方向发展[2]。

1　安全 RTU 总体设计方案

1.1 总体设计方案

安全 RTU 分为电力采集计算、主控单元、安全防护三个部分。总体设计框架如图 1 所示。

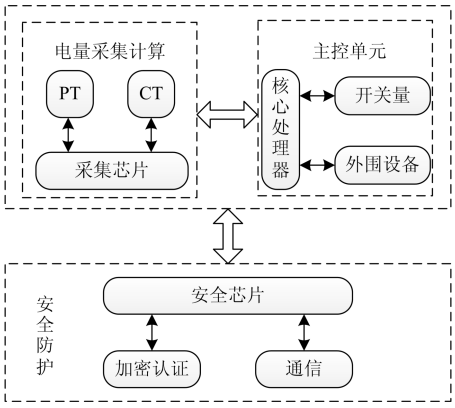

图 1 安全 RTU 总体设计框图

Fig. 1 Overall design diagram of the secure RTU

ATT7022 采集芯片首先通过 6 通道 16 位 ADC 模数转换电路来对输入电流和电压信号进行采样，转换后的数字量再经过 24 位 DSP 数字信号处理模块以完成全部三相电能参数的运算，同时将结果保存在相应的寄存器中并通过 SPI 口与 MCU 进行数据交换，DSP 模块同时还生成有功、无功电能脉冲输出 CF1、CF2，可用于现场校表。主控单元接收电量参数、开关量状态以及其他信息并存储，等待上级的命令发送相应数据。安全防护部分与主控单元相连，所有与上级通信的信息均通过安全芯片进行加密，保证数据以密文在 VPN 隧道传输。

1.2 自主可控的国产芯片

半导体芯片广泛应用于手机、电脑以及水利、交通、电力等设备和军事设备上，已经成为经济发展和国家安全的命脉。我国巨大的经济总量导致了对芯片极大的需求量，每年进口需要消耗 2000 多亿美元外汇。长期依赖国外芯片将会造成较大安全隐患，一些芯片厂商可以在芯片的某一个程序上植入木马程序获取商业信息甚至国家机密，或者通过病毒、恶意软件操作控制系统，致使系统瘫痪引发安全事故。目前，关键领域的计算机、移动终端等设备多采用国外的芯片，在安全可控性方面有较大的隐患，发展自主可控国产化芯片已成为半导体发展的必然趋势。近年来，我国不断增加对半导体芯片自主研发的力度，努力提高国产芯片的技术水平和市场占有率，摆脱芯片长期“受制于人”的局面。

(1) 龙芯 1B 核心处理器

龙芯 1B 芯片由中科院计算所研发，是一款 32 位 SoC 芯片，能够满足超低价位云终端、工业控制、数据采集、网络设备、消费类电子等领域的需求。目前龙芯系列芯片在军事设备上得到了较好的应用。主要技术指标如表 1 所示。

表 1 龙芯 1B 芯片主要参数

Table 1 Main parameters of LongXin 1B chip

主频	200 MHz	工艺	130 nmCMOS
指令集	MIPS32	封装	17×17 mmBGA
流水线结构	5 级	引脚数	256
浮点运算	64 位加、乘法	功耗	<0.5 W
执行结构	双发射乱序	控制器	DDR2
Cache	8 kB		

(2) 申威安全 SoC 芯片

申威安全 SOC 芯片是应用于 VPN 管理、IKE 协商、安全终端等安全领域的安全、可靠、高性能的 SoC 芯片。芯片采用 0.13 μm 工艺设计，工作频率 400 MHz，片内采用多级 AMBA 总线互联，集成了国内自主知识产权的 64 位高性能嵌入式微处理器，内置国家密码管理局指定安全算法模块，实现对安全模块配置管理、密钥协商、协议栈解析处理等功能；集成 DDR2 SDRAM 控制器、多种高速通信接口，可以方便实现数据通信；芯片整体处理能力强，安全性高，接口丰富。

(3) 采集芯片

ATT7022 是珠海炬力集成电路设计有限公司生产的一款高精度三相电能计量芯片，该芯片对有功功率、无功功率的测量精度分别达到 0.2 s 和 0.5 s，可测量的电参数包括有功、无功、视在功率、双向有功和四角限无功电能；电压和电流有效值；相位、频率等。ATT7022 具有计量参数齐全、校表功率完善等优点，简化了软件设计，缩短了软件开发周期。软件校表功能可提高校表精度、简化硬件设计、降低设计成本，为三相多功能计量装置提供了功能更加齐全、设计更加简单的应用方案。

2　电力参数采样算法与实现

2.1 采样算法

电力系统中的电量采样方法分为直流采样和交流采样。直流采样是将交流电压、电流信号转换成 0~5 V 的直流信号，这种测量方法软件设计简单，计算方便，但是由于变送器使用的电子元器件多、

电路复杂，而且电子元器件的性能不稳定、失效率高。交流采样是把交流量转化为±5 V 或±10 V 的交流电压进行采集。其理论基础是奈奎斯特采样定理，即以高于待测信号最高频率 2 倍的采样频率进行采样，以保持原有信号的基本特征[3-6]。主要优点是实时性好，相位失真小，投资少、便于维护；其缺点是算法复杂，精度难以提高，对 A/D 转换速度要求较高。随着半导体芯片技术的发展，交流采样逐渐成为电力系统主要的采样方式。安全 RTU 采用基于傅立叶变换的交流采样算法。

设 $u(t)$为周期函数，并且满足狄里赫利条件，则可展开级数

$$u(t)=\frac{U_{ao}}{2}+\sum_{n=1}^{N}(u_{an}\cos n\omega t+u_{bn}\sin n\omega t) \tag{1}$$

式中，

$$u_{an}=\frac{2}{T}\int_{o}^{T}u(t)\cos n\omega t\mathrm{d}t \quad (n=1,2,3,\cdots) \tag{2}$$

$$u_{bn}=\frac{2}{T}\int_{0}^{T}u(t)\sin \omega t\mathrm{d}t \quad (n=1,2,3,\cdots) \tag{3}$$

离散化得

$$u_{an}=\frac{2}{N}\sum_{k=1}^{N}u_k\cos n\frac{2\pi k}{N} \tag{4}$$

$$u_{bn}=\frac{2}{N}\sum_{k=1}^{N}u_k\sin n\frac{2\pi k}{N} \tag{5}$$

基波电压幅值

$$U_m=\sqrt{u_{a1}^2+u_{b1}^2} \tag{6}$$

这样可求出第 k 次谐波电压的振幅、相角、有效值，

振幅

$$U_{mk}=\sqrt{u_{ak}^2+u_{bk}^2} \tag{7}$$

相角

$$\varphi_n=\mathrm{arctg}\frac{u_{bk}}{u_{ak}} \tag{8}$$

有效值

$$U_k=\sqrt{\frac{U_{mk}}{2}}=\sqrt{\frac{(u_{ak}^2+u_{bk}^2)}{2}} \tag{9}$$

基波功率

$$u_{a1}i_{a1}+u_{b1}i_{b1}=U_m\cos\psi I_m\cos(\psi-\varphi)+U_m\sin\psi I_m\sin(\psi-\varphi)=U_mI_m(\cos^2\psi\cos\varphi+\sin^2\psi\cos\varphi)=U_mI_m\cos\varphi=2P \tag{10}$$

同理，

$$u_{b1}i_{a1}-u_{a1}i_{b1}=2Q \tag{11}$$

2.2 信号调理电路

在电力系统中，电压电流信号分别经过电压互感器 PT 和电流互感器 CT 转换成交流小信号，再经过信号调理电路处理后，供 ADC 模数转换器采样并计算[7]。信号调理电路的设计如图 2 所示。

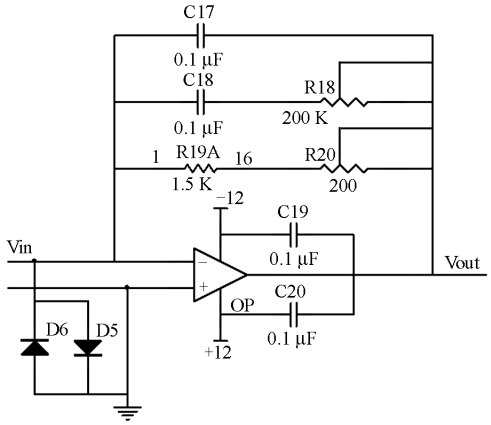

图 2 信号调理电路

Fig. 2 Signal conditioning circuit

由于互感器输出的是电流信号，可通过调节图中的反馈电阻 R19、R20 转换成所需要的电压信号。1.5K 的电阻 R19 串联一个 200 Ω的可调节电阻 R20 进行微调，以达到所要求的电压精度。为了补偿相移即相位差，需采用补偿电容 C18，因为电容不能微调，所以通过补偿电阻 R18 补偿互感器的固有相移。两个反接的二极管是起到保护运算放大器的作用。为了测试验证信号调理电路的性能，本文采用 Multisim 电路设计仿真软件对电路进行仿真测试。设置函数发生器的参数，其中频率为 50 Hz，振幅为 10 vP。运行仿真，从示波器可以得到经过信号调理电路处理后的波形。如图 3 所示。

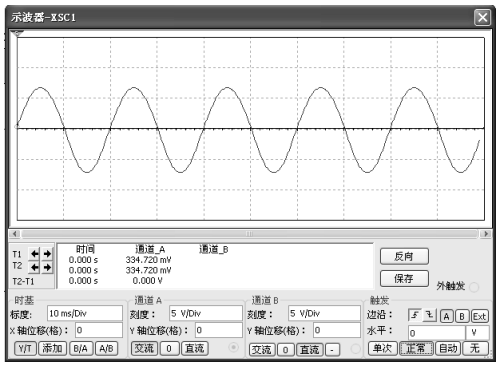

图 3 信号调理电路仿真

Fig. 3 Signal conditioning circuit simulation

3 通信接口设计

3.1 串口通信

在工业控制、电力通信、仪器仪表等领域，串

口通信是普遍采用的通信方式。RS232 与 RS485 是两种常见的接口，安全 RTU 采用 RS485 接口作为通信方式，与 RS232 相比，RS485 有以下主要特点：

(1) 采用差分信号，可以抑制共模干扰；

(2) 通信速率快，最大传输速度可以达到 10 Mb/s 以上；

(3) 传输距离最远可以达到 1 200 km 左右；

(4) 可以在总线上进行联网实现多机通信，总线上允许挂多个收发器。

Modbus 通信协议是应用于电子控制器上的一种通用语言。通过此协议，控制器与控制器之间，控制器经由网络可以和其他设备进行通信。Modbus RTU 串口通信技术成熟可靠、应用方便、实用性强，可以很容易地实现不同控制系统之间的数据通信，在工控系统中被广泛应用[8]。本文采用 Modbus 通信协议下的 RTU 模式。其数据帧格式如表 2 所示。

表 2 RTU 数据帧

Table 2 Data frame of RTU

起始位	设备地址	功能代码	数据	CRC 校验	结束符
T>4 字节	8 Bit	8 Bit	*n* 个 8 Bit	16 Bit	*T*>4 字节

(1) 起始位与结束符

每个 RTU 数据帧的起始位和结束符没有数据，表示时间间隔不小于 4 个字节的时间。这是因为 Modbus 协议规定两条数据帧的间隔时间不小于 4 个字节的通信时间，以此来判断一条数据帧是否发送完。

(2) 设备地址

设备地址是 RTU 数据帧第一个有意义的数据，设备接收到一帧数据后，首先将设备地址信息与自己的地址比较，如果两者相同，则继续接受数据并执行功能码相应的命令；如果两者不同，则不做响应。

(3) 功能代码

Modbus 通信规约定义的功能号为 1 到 127，当设备检测到数据帧的设备地址与自己的地址相同后，继续检测功能代码中的功能号，根据其数值来做出相应的功能处理。

(4) 数据

数据域的大小是由功能代码确定的，可以是需要设备回馈的信息或者执行的动作。包括数字量输入、输出，模拟量输入、输出，寄存器值等。

(5) CRC 校验

CRC 校验将一帧数据中除去最后两个字节的信息进行算法计算，将生成的信息作为校验码放到这一帧数据的最后，当这一帧数据被接收后，程序首先采用同样的算法对数据中除去最后两个字节的信息计算，并和发送过来的校验码比较，若检验码相同则数据正常，若不相同则作为错误信息丢弃。

表 3 和表 4 为举例说明读取 4 路开关量状态输入(遥信)。

表 3 上位机发送

Table 3 Data from upper computer

设备地址	01	设备地址为 01
功能代码	02	读开关量输入状态
数据长度	01	一个字节
开关量状态	0C	1、2 路状态为“0”，3、4 路状态为“1”
CRC 校验码	E04F	

表 4 设备回应

Table 4 Response data

设备地址	01	设备地址为 01
功能代码	02	读开关量输入状态
起始 BIT 位	0000	起始 BIT 地址 0000
读数据长度	0004	读取 4 路开关量输入状态
CRC 校验码	79C9	

3.2 以太网通信

对工业自动化而言，大量的智能设备可以通过各种途径连到 Internet 上，通过网络相互传递信息和数据，实现智能化现场设备的功能自治性、系统结构的高度分散性以及监管控一体化。网络通信具有兼容性、可扩展性以及适合处理突发事件的异步工作方式，工业以太网在电力自动化系统发展中作用越来越明显[9-11]。安全 RTU 设计了以太网通信接口，以满足不同需求对数据传输速度、距离、稳定性的要求。

Modbus/TCP 协议采用以太网的物理层和数据链路层，可以连接不同的网络，适应大部分底层的通信技术。本文采用的工业以太网 TCP 协议基于 IEC60870-5-103 规约[12]。Modbus/TCP 报文采用了客户端/服务器的模式。基于四种类型的报文：Modbus 请求、Modbus 确认、Modbus 指示、Modbus 响应。

与 Modbus 串口通信协议相比，Modbus/TCP 协议去掉了从机地址、校验码。在底层的 TCP 协议已经确定了端到端的连接，通过 TCP 协议的校验可以保证传输信息的正确性。

4 安全防护设计

4.1 国产加密算法

加解密技术是指将一个信息经过加密钥匙及加密函数转换变成无意义的密文，而接收方则将此

密文经过解密函数、解密钥匙还原成明文[13]。密码学中应用最为广泛的三类算法包括对称算法、非对称算法、杂凑算法。对称算法包括 DES、3DES、AES 等；非对称算法有 RSA、DSA、DH、ECC 等；杂凑算法又称 hash 函数，杂凑函数主要用于完整性校验和提高数字签名的有效性。

为了保障商用密码安全，国家商用密码管理办公室制定了一系列密码标准，包括 SSF33、SM1(SCB2)、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等。国密算法是一套完全具有自主知识产权的加密算法。其中 SM1、SM3 等算法的原理仍保密，与国际通用的加密算法相比，国密算法密钥长度、算法强度更大、安全性更好。

4.2 可信密码模块(TCM)

TCM 模块可以有效构建基于国产安全平台的可信安全防护系统，防御各类计算机平台的非法入侵，实现计算机自身的安全稳定运行。图 4 为 TCM 结构图。

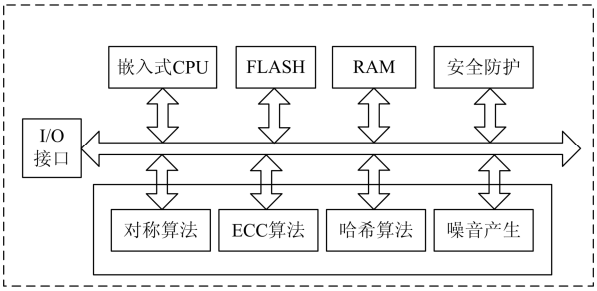

图 4 TCM 结构图

Fig. 4 Structure of TCM

可信安全防护系统由可信密码支撑子系统和基于可信支撑的安全应用子系统组成。系统以可信计算模块(TCM)为可信根，采用可信度量、存储和报告机制，保证平台身份以及系统环境的安全、可信，同时结合安全控制机制，从硬件架构、可信引导、网络接入、外设接入、用户认证、软件安全等多方面进行安全性设计，采用主动防御手段，保障计算机系统的安全可信。

主要功能如下：

(1) 主动度量，TCM 作为可信根，可有效实现 BMC、BIOS、操作系统、应用系统的度量；

(2) I/O 控制，根据 TCM 硬件保护的安全策略，实现 I/O 的使能控制；

(3) 系统状态显示，提供 TCM 和系统可信的状态显示；

(4) 可信密码支撑，提供可信度量、存储、报告机制，提供密码服务；

(5) 提供密码服务，具有加/解密、签名/验签、密钥管理等密码运算功能；

(6) 支持数据安全存储；

(7) 支持内部资源的授权访问；

(8) 具有带电和不带电销毁功能。

4.3 国密算法性能测试

对于安全 RTU 的密码子系统部分，通过国家密码局密码性能检测系统，对加解密算法，密钥生成速率做了检测，结果表 5~表 7。

表 5 加密性能测试

Table 5 Encryption performance test

加密数据	运算时间/s			平均时间/s	平均速度/Mps
	第一次	第二次	第三次		
128 KB	0.012	0.012	0.013	0.013	80.659

表 6 解密性能测试

Table 6 Decryption performance test

解密数据	运算时间/s			平均时间/s	平均速度/Mps
	第一次	第二次	第三次		
128 KB	0.012	0.012	0.013	0.013	80.659

表 7 密钥生成速率

Table 7 Key generation rate

密钥对组数	运算时间/s			平均时间/s	平均速度(对/s)
	第一次	第二次	第三次		
1 000	3.419	3.414	3.414	3.415	293

5 结论

(1) 采用自主可控的国产芯片，以龙芯 1B 为核心处理器，外扩电量采集芯片可以分担 CPU 的部分工作，弥补 CPU 在性能上的不足，测试结果表明，电量参数可以控制在相关标准的误差范围内。

(2) 针对电力设备缺少信息安全防护机制的缺点，设计了 TCM 模块，采用国产加密算法，对信源加密，使数据在 VPN 隧道以密文传输，通过密钥可以解析出伪 IP 数据包，隔离病毒、木马以及其他攻击，提高了 RTU 的安全性。

参考文献

[1] 朱世顺, 董钰, 刘行. 电力工业控制系统信息安全测评体系研究[J]. 电力信息化, 2012, 10(4): 16-19.
ZHU Shishun, DONG Yu, LIU Xing. Research of information security evaluation system for power industrial control systems[J]. Electric Power Information Technology, 2012, 10(4): 16-19.

[2] 王建华, 张国刚, 耿英三, 等. 智能电器最新技术研究及应用发展前景[J]. 电工技术学报, 2015, 30(9): 1-11.

WANG Jianhua, ZHANG Guogang, GENG Yingsan, et al. The latest technology research and application prospects of the intelligent electrical apparatus[J]. Transactions of China Electrotechnical Society, 2015, 30(9): 1-11.

[3] 李科, 向中凡, 黄磊, 等. 基于 DSP2812 的交流信号实时采样系统[J]. 西华大学学报(自然科学版), 2014, 33(6): 33-36.
LI Ke, XIANG Zhongfan, HUANG Lei, et al. AC real-time sampling system based on DSP2812[J]. Journal of Xihua University (Natural Science), 2014, 33(6): 33-36.

[4] 李明, 项新建. 基于改进交流采样算法的电气火灾监控系统研制[J]. 工业控制计算机, 2012, 23(4): 1-3.
LI Ming, XIANG Xinjian. Control system for electric fire prevention based on improved AC sampling algorithm[J]. Industrial Control Computer, 2012, 23(4): 1-3.

[5] 陈先中, 温建澎, 陈宁. 一种应用于电网参数检测的小波消噪交流采样新算法[J]. 传感技术学报, 2007, 20(3): 640-643.
CHEN Xianzhong, WEN Jianpeng, CHEN Ning. A new AC sampling algorithm using wavelet denoising to measure the parameters of power network[J]. Chinese Journal of Sensors and Actuators, 2007, 20(3): 640-643.

[6] 杜玉宇, 于群, 史青禾, 等. 基于 C8051F020 多通道交流采样电路设计[J]. 电气技术, 2012(8): 95-97.
DU Yuyu, YU Qun, SHI Qinghe, et al. Design of multi-channel AC sampling circuit based on C8051F020[J]. Electrical Engineering, 2012(8): 95-97.

[7] 王玲, 冯宇, 邱进, 等. 电压互感器谐波特性测量用可控谐波电压源的构建[J]. 电力系统保护与控制, 2015, 43(16): 106-111.
WANG Ling, FENG Yu, QIU Jin, et al. Construction of controllable harmonic voltage source for harmonic characteristic measurement[J]. Power System Protection and Control, 2015, 43(16): 106-111.

[8] 沈林晖. Modbus RTU 串口通信在工业自动化系统中的应用[J]. 化工自动化及仪表, 2014, 41(2): 207-211.
SHEN Linhui. Application of Modbus RTU serial communication application in industrial automation system[J]. Control and Instruments in Chemical Industry, 2014, 41(2): 207-211.

[9] 刘颖, 陈立. 工业以太网技术在变电站自动化系统中的应用[J]. 电力系统保护与控制, 2008, 36(23): 65-68.
LIU Ying, CHEN Li. Application of industrial Ethernet in substation automation system[J]. Power System Protection and Control, 2008, 36(23): 65-68.

[10] 汪强, 徐小兰, 葛光胜, 等. 智能变电站专用通信设备的关键技术[J]. 电力系统保护与控制, 2014, 42(7): 150-154.
WANG Qiang, XU Xiaolan, GE Guangsheng, et al. Key technologies of special communication device in smart substation[J]. Power System Protection and Control, 2014, 42(7): 150-154.

[11] 刘建, 赵树仁, 张小庆. 中国配电自动化的进展及若干建议[J]. 电力系统自动化, 2012, 36(19): 6-10.
LIU Jian, ZHAO Shuren, ZHANG Xiaoqing. Development of distribution automation in China and some suggestions[J]. Automation of Electric Power Systems, 2012, 36(19): 6-10.

[12] 张磊, 陈宏君, 吴相楠, 等. 基于扩展 103 规约的保护装置通信与调试系统设计[J]. 电力系统保护与控制, 2015, 42(21): 126-130.
ZHANG Lei, CHEN Hongjun, WU Xiangnan, et al. Design of communication and debugging system for protection device based on extended 103 protocol[J]. Power System Protection and Control, 2015, 42(21): 126-130.

[13] 赵昊, 李英韬, 王春才. 基于国密算法的数据加解密技术在油井作业现场的应用[J]. 长春理工大学学报(自然科学版), 2014, 37(2): 108-113.
ZHAO Hao, LI Yingdao, WANG Chuncai. Application of code technique in oil well site based on the SM1 and SM2 cryptographic algorithm[J]. Journal of Changchun University of Science and Technology (Natural Science Edition), 2014, 37(2): 108-113.

收稿日期：2015-08-03；　修回日期：2015-11-25

作者简介：

南亚希(1960-)，男，本科，高级工程师，研究方向为电力系统及其自动化；Email: nanxi7890@163.com

展　巍(1975-)，男，硕士，高级工程师，研究方向为电力自动化软件系统；Email: zhanwi@163.com

裴后宣(1988-)，男，通信作者，硕士，工程师，研究方向为电力工业控制系统信息安全。Email: pei320322@163.com

(编辑　姜新丽)