·技术探讨·

基于双重隔离的电力通用安全接入区设计与实现

曹翔，胡绍谦，张阳，林青，汤震宇，张春合
（南京南瑞继保电气有限公司，江苏 南京 211102）

摘　要：为了解决现有安全接入区在设计和实现上困难、通用性差、传输效率低、安全性不足等问题，提出了基于双重隔离的电力通用安全接入区设计。该设计主要包含加密认证装置、正反向隔离装置和通用接入设备。在对现有安全接入区结构和原理分析的基础上，指出了其在实现上的不足。提出的安全接入区采用通用接入设备简化了安全接入区的设计，实现了通信双方的无感接入以及安全接入区的双重隔离和基于国密算法的加密和认证。测试及验证结果证明了该设计的可行性并给出了关键通信和安全参数的测试结果。与现有方案相比，该设计在通用性、性能和安全性上都得到了提高，具有较好的实用性。

关键词：安全接入区；通用；隔离；加密；认证
中图分类号：TP939　　**文献标志码：**A　　**文章编号：**2096-3203(2019)02-0152-07

0　引言

随着国家电网加强智能电网的全面建设和推进，配电自动化业务和技术迅速发展，配电自动化系统中的配电终端通常需要通过无线或公网与主站系统通信[1—4]，保证主站侧配电终端的安全接入成为急需解决的问题。另一方面，一些新能源厂站或低电压等级的电厂由于地形复杂、通信基础薄弱等原因，无法采用调度数据网方式或专线方式接入主站，要采用无线通道的方式接入主站[5—8]。厂站侧生产控制大区的边界安全也需要得到保障。

为适应新形式下电力业务的安全需求，根据国家发改委14号令附件的要求，当生产控制大区需要在纵向联接中使用无线通信网或其他外部公用数据网而其安全防护水平低于生产控制大区内其他系统时，需要设立安全接入区[9—10]。安全接入区与生产控制大区中其他部分的联接处必须设置经国家指定部门检测认证的横向单向安全隔离装置。该要求仅对特定场景下的接入进行了安全接入区设立的要求，并未细化安全接入区本身的实现。

目前国内对安全接入区的研究主要包括：文献[11]提出了基于安全代理的数据交换，但是仅针对安全代理的若干关键技术进行研究，并未从整体上给出解决方案；文献[12]提出了针对电力长期演进技术(long term evolution，LTE)无线接入专网的安全防护解决方案，重点解决了涉及无线通信的安全接入、安全传输及身份认证等问题，但在安全接入区的设计上仅给出了其组成和功能说明，未给出详细设计且不具备通用性；文献[13]给出了电力行业工控终端设备安全接入系统的设计与实现方案，解决了配电网调度自动化系统和配网终端双向身份鉴别和报文加密传输问题，但其安全接入系统中并未采用正反向隔离装置；文献[14]提出了电力移动终端安全接入系统的研究与实现，但其安全接入区的侧重点在移动终端身份的合法性验证和监控接入终端的行为上，未对安全接入区的整体结构和实现效率进行讨论。

文中首先给出了现有实施环境中安全接入区的设计，并提出了其安全接入区本身在通用性、性能和安全性上的不足，然后给出了基于双重隔离的通用安全接入区的设计与实现，并针对该设计的安全性进行了讨论，最后给出了验证、总结和展望。

1　现有安全接入区的设计

1.1　主站侧安全接入区设计

图1为某配网自动化主站安全接入区结构图[15]，此处为了强调安全接入区仅给出了主站的生产控制大区而未给出主站的信息管理大区。主站需要实现对配电终端的实时数据采集与控制命令下发。其中配电终端通过无线或公网方式接入，在生产控制大区通过设立安全接入区来实现配电终端的安全接入。配电安全接入网关主要采用国产商用非对称密码算法实现配电安全接入网关与配电终端的双向身份认证。专网采集服务器对下用于实现与配电终端的应用层规约通信，对上需要在报文和文件之间进行转化以实现采集信息通过正反向隔离装置到达主站前置服务器的目的。主站前置服务器侧的配电加密认证装置用于实现第二重身份认证和报文的加解密。配电终端自身带有

收稿日期：2018-09-21；修回日期：2018-10-27

安全芯片以实现和主站侧装置的身份认证及报文加解密。

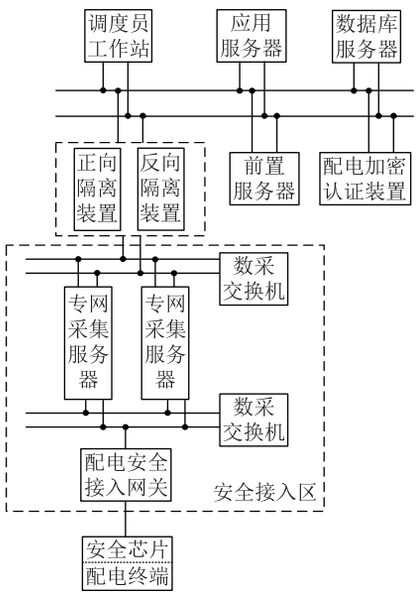


图 1 配网自动化主站安全接入区结构

Fig.1 Structure of security access zone in distribution network automation control center

在上述方案中,安全接入区的设计主要包含了配电安全接入网关和专网采集服务器。该方案可视为一个典型的安全接入区设计,主要有如下缺点。

(1) 专网采集服务器需要针对配电终端开发特殊的通信规约。若配电终端为 IEC104 服务器端,则专网采集服务器需要开发相应的客户端规约,而在传统的不含安全接入区的主站结构中,与终端通信的程序直接由前置服务器完成。这主要是由于正反向隔离装置的引入阻断了前置服务器和终端之间的 TCP 连接。按照这种方式搭建的安全接入区,若主子站之间的通信规约发生变化,则需要重新开发相应的专网采集服务器通信程序,不仅开发工作量大,而且增加了后期运维的复杂度。

(2) 主站前置服务器的对下采集需要重新开发。增加安全接入区后,前置服务器需要通过正反向隔离装置获得采集数据,采集方式的变化导致其程序开发的工作量增加。

(3) 报文传输延迟增大。正反向隔离装置的引入导致了两侧通信要通过文件进行摆渡,报文和文件之间的转换以及正反向隔离装置的周期扫描文件传送都大大增加了报文的传输延迟。这对于时间敏感的功率平衡或遥控操作存在额外的影响。

1.2 厂站侧安全接入区设计

图 2 为某新能源厂站的安全接入区结构图,该厂站需要将站内的二遥数据送到调度主站,但是尚不具备调度数据网的接入条件。在生产控制大区通过无线专网接入主站时,设立安全接入区。安全接入区由正向隔离装置、厂站前置和加密认证装置组成。二遥数据的传输首先由厂站采集装置将二遥数据存为公用数据模型 E 语言(common information model E language,CIME)文件,然后文件经正向隔离装置发往厂站前置,厂站前置接收到文件后,根据和主站协商的通信规约将文件中的二遥数据送到主站。加密认证装置在通信过程中起到了身份认证和数据加密的作用。

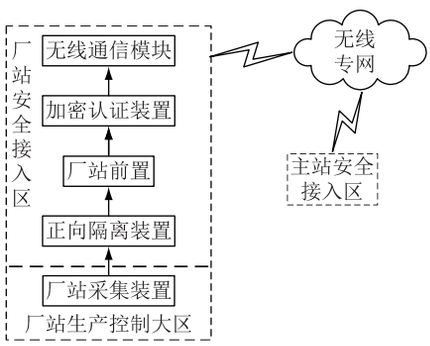


图 2 新能源厂站安全接入区结构

Fig.2 Structure of security access zone in new energy plant station

通过对通信过程的分析可以看到,主站侧安全接入区存在的问题在厂站侧安全接入区同样存在。即使有些主子站之间采用通用规约安全文件传输协议(secure file transfer protocol,SFTP)直接传输文件,则子站的厂站前置不必专门为通信开发规约,但是通过正向隔离装置导致的数据传输延迟依旧存在。此外,在该安全接入区中,还存在着数据保密性(即明文传输)的问题。

2 基于双重隔离的通用安全接入区设计和实现

鉴于现有安全接入区存在开发工作量大、性能受限、通用性差等问题,文中提出了基于双重隔离的通用安全接入区设计(以下简称本设计)。从前面的分析可以看到,目前安全接入区的这几个问题主要是由于正反向隔离装置的引入,导致了传输控制协议(transmission control protocol,TCP)连接被阻断。

文中提出的安全接入区设计,是在充分了解正反向隔离装置工作原理的基础上,通过增加一种通用接入设备,来实现正反向隔离装置两侧通信主机的无感接入。同时在原有正反向隔离装的基础上增加了一层协议隔离,并实现了加密和认证功能,从而大大提高安全接入区的通用性、安全性、传输效率并有效减少了相关的开发工作量。

2.1 整体设计

图 3 给出了文中设计的整体结构图，简化了安全接入区使用的环境，重点突出安全接入区本身的结构，同时将安全接入区两侧的通信模拟为内网主机和外网主机，内网主机或外网主机在实际应用中可以表示服务器、嵌入式装置或任何能承载传输规约的智能设备。其中，内网区可以理解为变电站或调度主站的生产控制大区，外网区可以理解为公网或无线网络。从图 3 可以看到，本设计的安全接入区包含加密认证装置、通用接入设备与正反向隔离装置。与现有安全接入区不同的是，其中并没有服务器设备，取而代之的是通用接入设备，通用接入设备的引入将极大地通用化安全接入区的设计并在开发量、性能、安全性、易于维护性、稳定性等方面取得更优的结果。

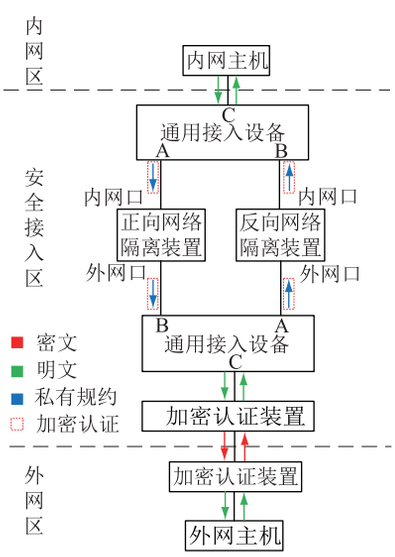


图 3 基于双重隔离的安全接入区设计

Fig.3 Design of security access zone based on dual isolation

内外网主机的通信流程如下：

（1）外网主机将明文发送给加密认证装置，加密认证装置在已经与对侧加密认证装置完成身份认证并建立隧道的情况下，将明文加密后发送到对侧；

（2）安全接入区中作为边界防护的加密认证装置在收到密文后进行解密并将明文传给通用接入设备；

（3）通用接入设备在 C 口收到明文后，首先进行合法性判断，判断为合法链路后进行网络协议剥离，然后进行加密及签名操作，并转换为正反向隔离装置的私有规约，最后从 A 口转出私有规约报文；

（4）私有规约报文通过反向隔离装置；

（5）对侧通用接入设备在 B 口收到报文后，首先进行合法性判断，判断为合法链路后对私有协议进行剥离，然后进行认证和解密操作，最后进行网络协议封装并从 C 口发给内网主机；

（6）内网主机对报文进行处理；

（7）报文从内网主机发往外网主机的过程与上述过程相反。

上述通信过程中的合法性判断，是指根据通用接入设备中的配置对链路的协议、源 IP、源端口、目的 IP、目的端口进行判断。上述通信过程中私有协议的设计，主要考虑了正反向隔离装置对其传输报文的格式要求，由标志头、传输长度、传输内容、填充字节组成。从上述通信流程可以看到，在整个通信过程中，没有报文与文件的转换，也就没有了文件通过周期扫描任务通过正反向隔离装置，从而大大降低了传输的时延。且通用接入设备的引入，避免了复杂规约的开发，从通信过程的分析可以看到，本设计实现的关键是通用接入设备。

2.2 通用接入设备的设计与实现

通用接入设备在设计上是一个采用非 X86 架构 CPU 的嵌入式装置，主要用于通过协议隔离实现明文和私有规约的转换，并带有加密和认证功能。通过将 2 台通用接入设备与正反向隔离装置配套使用，可以实现两侧通信的无感接入。

通用接入设备的接口设计如图 4 所示，该装置在功能上有 A、B、C、D 4 个网口。在使用上，A 网口用于和正向隔离装置的内网口或反向隔离装置的外网口相连，B 网口用于和正向隔离装置的外网口或反向隔离装置的内网口相连，C 网口用于和两侧通信设备相连，D 网口用于装置的参数配置。下面对主要接口的作用及装置的工作原理进行分析。

图 4 通用接入设备接口设计

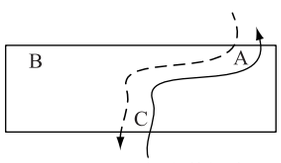
Fig.4 Interface design of universal access device

2.2.1 地址解析协议（address resolution protocol，ARP）报文处理

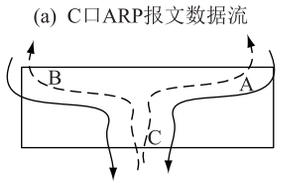
通信双方在建立连接前通常先通过 ARP 报文获取对方的介质访问控制（media access control，MAC）地址。通用接入设备的 C 网口收到 ARP 报文后首先进行合法性判断，判断合法后直接将报文从 A 网口送出，由正反向隔离装置对通信双方的 ARP 报文进行回复。ARP 回复的报文在通过合法

性判断后通过 C 口传回给通信双方。对于正反向隔离装置发出的 ARP 报文,通用接入设备同样在完成合法性判断后直接将其转发到 C 网口由通信双方主机进行处理。

具体的数据流示意如图 5 所示。其中实线表示 ARP 的查询报文,虚线表示 ARP 回复报文。



(a) C口ARP报文数据流



(b) A口或B口ARP报文数据流

图 5 通用接入设备的 ARP 报文数据流示意图

Fig.5 Diagram of ARP message dataflow

2.2.2 TCP/用户数据报协议(user datagram protocol,UDP)报文处理

TCP/UDP 报文的数据流示意如图 6 所示。通用接入设备在 C 口收到 TCP/UDP 报文后,首先进行合法性判断,判断为合法链路后在协议层对报文进行剥离,获得应用数据后进行加密和签名,然后重新封装成私有规约并从 A 口发出。同样的在 B 口收到私有规约的报文后,首先进行合法性判断,判断为合法链路后从私有规约中获得应用层数据,然后进行验签和解密,操作成功后重新封装成 IP 报文从 C 口发出。通用接入设备对报文的处理类似于隔离装置的过程,其本质是实现了协议的隔离和数据的摆渡。

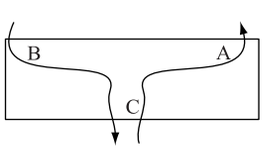


图 6 通用接入设备的 TCP/UDP 数据流示意图

Fig.6 Diagram of TCP/UDP message dataflow

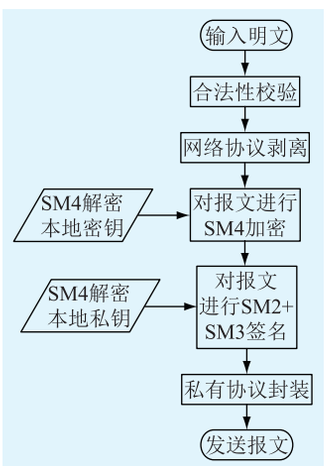
2.2.3 加密和认证功能

在 GB/T 22239—2008 信息系统安全等级保护基本要求中,对应用安全的三级要求通信的完整性、保密性和不可抵赖性。安全接入区作为生产控制大区的一部分,也应当能够满足等级保护三级的要求。通用接入设备支持对报文进行基于国密算法的加密和认证[16—18]功能。

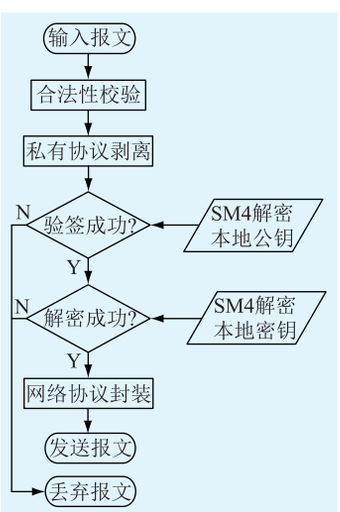
当通用接入设备配置对称加密密钥后,会对协议剥离后的报文数据进行基于 SM4 的对称加密,加密密钥从配置中获取。在对侧的通用接入设备上,配有同样的密钥用以实现报文的解密。加密密钥在装置本地加密保存,其使用可以保证通信过程的保密性。

同理,当通用接入设备配置认证公私钥对后,会对密文进行基于 SM2+SM3[19—20]的签名,签名所用的私钥从本地配置中获取,并将签名的结果放在密文之后进行封装。在对侧的通用接入设备上,配有对应的公钥用以实现报文的验签。公私钥在装置本地同样加保存,其使用可以保证通信过程的完整性和不可抵赖性。

通用接入设备上的 IP 报文加密和认证处理流程如图 7 所示。



(a) C口接收报文



(b) A、B口接收报文

图 7 通用接入设备上的 IP 报文加密和认证处理流程

Fig.7 Diagram of IP message encryption and authentication process

2.3 总体安全防护方案

本设计方案的安全防护,主要体现在如下 3 道防线:

（1）第一道防线是由加密认证装置实现安全接入区的边界防护。加密认证装置可以和待接入侧的加密认证装置配套使用，实现双向身份认证和报文加密。同时加密认证装置所具备的部分防火墙的功能也可以对通信链路的 IP 及端口等进行过滤。

（2）第二道防线是由正反向隔离装置实现的第一重隔离。正反向隔离装置本身就通过采用“双机+隔离岛”的物理结构，实现了 TCP 连接的阻断、协议隔离、信息流访问控制和内容过滤，隔离强度接近物理隔离。

（3）第三道防线是由通用接入设备所引入的协议隔离、报文加密和认证。通用接入设备通过采用连接方向控制、综合条件过滤、防穿透 TCP 连接设计、无协议栈设计和状态检测技术来实现第二重隔离。

3 测试与验证

根据图 3 所示的结构搭建了图 8 所示的测试与验证环境。该环境中省略了加密认证装置的搭建，主要是因为加密认证装置仅仅对报文进行了加密和对侧装置的认证，不影响整个设计的实现。其中通用接入设备采用 PowerPC 4 核 1 200 MHz CPU，内网主机作为服务器端（开启 9000 端口），外网主机作为客户端。IP_A 为内网主机的 IP 地址，IP_B 为外网主机的 IP 地址，MAC_N 为内网侧通用接入设备网口 C 的 MAC 地址，MAC_W 为外网侧通用接入设备网口 C 的 MAC 地址。表 1 给出了正反向网络隔离装置的参数配置。

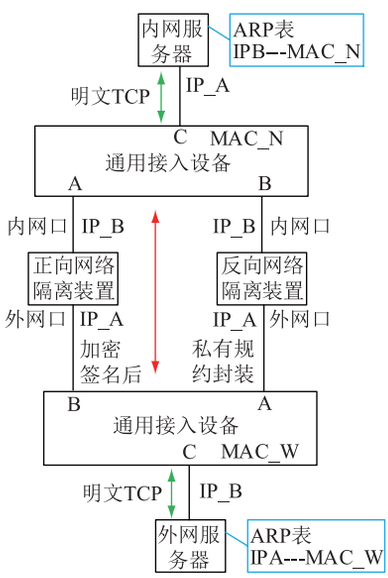


图 8 测试与验证环境

Fig.8 Test and verification environment

从图 8 可以看到，正反向隔离装置在内网侧或外网侧使用了相同的虚拟 IP 地址。这在常规站中是不允许的，因为常规站中正反向隔离装置同一侧的网口往往接在同一个交换机上，这种配置会造成 IP 冲突。但是在本设计中，针对同一个连接，正反向隔离装置在内外网侧的虚拟 IP 地址必须配置成相同的，这是由于通用接入设备可以接管整个链路的维护，并能很巧妙地处理 ARP 报文和 IP 报文。

表 1 正反向网络隔离装置配置

Table 1 Configuration of positive and reverse network isolator

参数	内网	外网
IP 地址	IP_A	IP_B
端口	9000	0
虚拟 IP	IP_A	IP_B

为了能够支持多个主机的接入，通用接入设备还需要在 C 口虚拟出一个 MAC 地址来代理正反向隔离装置在同一侧相同的虚拟 IP 地址所对应 MAC 地址。在本实例中，这个虚拟出来的 MAC 地址即 MAC_N 和 MAC_W。

经测试，本设计能实现通信双方的 TCP 通信，通信稳定，采用 IXIA PerfectStorm ONE 测试仪对其通信参数和安全性能测试结果如表 2 所示，其中 DOS 攻击包括 SYN/ICMP/UDP Flood 攻击，协议 FUZZER 测试针对常用的网络协议进行协议模糊测试，Stack Scrambler 主要针对报文在 IP 层，TCP 层或 UDP 层进行畸形变化后，测试系统协议处理能力的健壮性。

表 2 测试结果

Table 2 Test result

测试名称	测试结果
端到端延迟（明文）/ms	<2
端到端延迟（加密认证）/ms	<12
加解密速度/（μs·次$^{-1}$）	<100
签名速度/（ms·次$^{-1}$）	<10
系统带宽/kpbs	>200
DOS 攻击/80 Mbps	运行正常
协议 FUZZER 测试	运行正常
Stack Scrambler 测试	运行正常

注意通信带宽受限于系统中带宽最小的装置，通用接入设备在 1 024 字节长度报文测试下满负荷带宽不小于 60 Mbps，延迟小于 5 ms。正向隔离装置带宽为 180 Mpbs，延迟小于 5 ms。主要带宽限制为反向隔离装置。但该系统带宽已经足够正常的主子站通信系统使用（常规 IEC104 的单链路使用带宽通常不大于 20 kbps）。

4 结语

文中提出了一种基于双重隔离的电力专网通用安全接入区设计与实现。通过通用接入设备的引入,简化了现有安全接入区的结构,大大减少了安全接入区的开发工作量,提高了通用性,且传输效率大大提高,该设计还具备对报文的双重协议隔离,并能实现报文的加密和认证。经在现场实际环境中测试,该方案可行性高且运行稳定,具有较好的实用性。同时,该方案也能向工控领域推广。

参考文献:

[1] 周冬旭,张明,朱红,等. 新电改形势下智能配电网调度互动研究应用[J]. 电力工程技术,2018,37(2):89-94.
ZHOU Dongxu,ZHANG Ming,ZHU Hong,et al. Intelligent distribution network dispatching interactive practice exploration under the background of electric power system reformation [J]. Electric Power Engineering Technology,2018,37(3):89-94.

[2] 郑宗强,韩冰,闪鑫,等. 输配电网高级应用协同运行关键技术分析[J]. 电力系统自动化,2017,41(6):122-128.
ZHENG Zongqiang,HAN Bing,SHAN Xin,et al. Analysis on key technologies for coordinated operation of advanced application software in transmission and distribution network[J]. Automation of Electric Power Systems,2017,41(6):122-128.

[3] 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.

[4] 李映雪,陆俊,徐志强,等. 多技术融合的智能配用电终端通信接入架构设计[J]. 电力系统自动化,2018,42(10):163-169.
LI Yingxue,LU Jun,XU Zhiqiang,et al. Design of terminal communication access architecture for smart power distribution and utilization based on integration of multiple technologies[J]. Automation of Electric Power Systems,2018,42(10):163-169.

[5] 曹晶,卞宇翔,冯宝,等. 电力无线专网通信终端接入工勘测试体系研究[J]. 电力工程技术,2018,37(3):97-101.
CAO Jing,BIAN Yuxiang,FENG Bao,et al. Research on access engineering exploration test system of power wireless private network communication terminal[J]. Electric Power Engineering Technology,2018,37(3):97-101.

[6] 王炫,李红,丛琳. 基于无线通信和光通信的高压输电线路监测系统[J]. 电网技术,2009,33(18):198-203.
WANG Xuan,LI Hong,CONG Lin. A novel monitoring system for high voltage transmission lines based on wireless and optical communication technologies [J]. Power System Technology, 2009,33(18):198-203.

[7] 魏访. TD-LTE 技术在智能电网无线通讯中的应用[J]. 青岛大学学报,2018,31 (1):128-132.
WEI Fang. The TD-LTE technology in smart grid for the application of wireless communications[J]. Journal of Qingdao University,2018,31 (1):128-132.

[8] 周浩,吴国庆,陆竑,等. TD-LTE 230 无线专网在嘉兴电力通信的应用[J]. 浙江电力,2018,37(5):16-21.
ZHOU Hao,WU Guoqing,LU Hong,et al. Application of TD-LTE 230 wireless private network in jiaxing power communication[J]. Zhejiang Electric Power,2018,37(5):16-21.

[9] 周金辉,盛晔,苏义荣,等. 含高比例光伏的配电网电压协调控制策略研究[J]. 浙江电力,2018,37(4):7-13.
ZHOU Jinhui,SHENG Ye,SU Yirong,et al. Research on coordinated distribution network voltage control strategy with high proportion photovoltaics [J]. Zhejiang Electric Power, 2018, 37 (4):7-13.

[10] 王海欧,白金泉,陈群锋,等. 基于无线传输技术的接地导通测试仪的研究与设计[J]. 浙江电力,2017,36(5):5-7.
WANG Haiou,BAI Jinquan,CHEN Qunfeng,et al. Research and design of grounding conduction tester based on wireless transmission technology[J]. Zhejiang Electric Power,2017,36 (5):5-7.

[11] 纪元,娄征. 基于安全代理的数据交换在电力系统中的研究与应用[J]. 通信技术,2017,50 (2):365-369.
JI Yuan,LOU Zheng. Application of security agent-based data exchange in power system[J]. Communications Technology, 2017,50(2):365-369.

[12] 韦磊,刘锐,高雪. 电力 LTE 无线专网安全防护方案研究[J]. 江苏电机工程,2016,35(3):29-33.
WEI Lei,LIU Rui,GAO Xue. Research on security protection solution to LTE power wireless private network[J]. Jiangsu Electrical Engineering,2016,35 (3):29-33.

[13] 彭竹. 电力行业工控终端设备安全接入系统的设计与实现[D]. 北京:中国科学院大学,2015.
PENG Zhu. Design and implementation of industrial control terminal equipment of security access system in electric power industry[D]. Beijing: University of Chinese Academy of Sciences,2015.

[14] 孙红强. 电力移动终端安全接入系统研究与实现[D]. 河北:河北工业大学,2015.
SUN Hongqiang. Research and implementation of secure access system for power mobile terminal[D]. Hebei:Hebei university of technology,2015.

[15] 吕航. 诸暨市配电网自动化改造方案研究[D]. 北京:华北电力大学,2017.
LYU Hang. Study on automatic transformation scheme of distribution network in zhuji [D]. Beijing: North China electric power university,2017.

[16] 廖建容,段斌,谭步学,等. 基于口令的变电站数据与通信安全认证[J]. 电力系统自动化,2007,31(10):71-75.
LIAO Jianrong,DUAN Bin,TAN Buxue,el al. Authentication of substation automation data and communication security based on password[J]. Automation of Electric Power Systems, 2007,31(10):71-75.

[17] 刘刚,梁野,李毅松,等. 数字证书技术在电力二次系统中

的实现及应用[J]. 电网技术,2006,30:71-75.
LIU Gang,LIANG Ye,LI Yisong,et al. Realization and application of certificate in secondary part power system[J]. Power System Technology,2006,30:71-75.

[18] 赵兵,高欣,翟峰,等. 面向用电信息采集系统的双向认证协议[J]. 电网技术,2014,38(9):2328-2335.
ZHAO Bing,GAO Xin,ZHAI Feng,et al. Mutual authentication protocol for electricity consumption information acquisition system [J]. Power System Technology, 2014, 38 (9): 2328-2335.

[19] 骆钊,谢吉华,顾伟,等. SM2 加密体系在智能变电站站内通信中的应用[J]. 电力系统自动化, 2015, 39 (13): 116-123.
LUO Zhao,XIE Jihua,GU Wei,et al. Application of SM2 encrypted system in smart substation inner communication[J]. Automation of Electric Power Systems,2015,39(13):116-123.

[20] 骆钊,谢吉华,顾伟,等. 基于 SM2 密码体系的电网信息安全支撑平台开发[J]. 电力系统自动化,2014,38(6):68-74.
LUO Zhao,XIE Jihua,GU Wei,et al. SM2-cryptosystem based information security supporting platform in power grid[J]. Automation of Electric Power Systems,2014,38(6):68-74.

作者简介:


曹翔

曹翔(1986),男,硕士,工程师,从事电力系统安全产品研发工作(E-mail:caoxiang@nrec.com);

胡绍谦(1978),男,硕士,高级工程师,从事电力系统自动化、61850 规约研究工作;

张阳(1989),男,硕士,工程师,从事电力系统自动化,电力系统安全研发工作。

Design and implementation of power universal security access zone based on dual isolation

CAO Xiang, HU Shaoqian, ZHANG Yang, LIN Qing, TANG Zhenyu, ZHANG Chunhe
(NR Electric Co.,Ltd.,Nanjing 211102,China)

Abstract:In order to solve the problems in the design and implementation of current security access zone, such as poor universality, low transmission efficiency and lack of security, a design of power universal security access zone based on dual isolation is proposed. The design mainly includes the encryption and authentication device, the forward and reverse isolation devices and the universal access device. Based on the analysis of the structure and principle of the current security access zone, its shortcomings are given. By using universal access device, the design of security access zone is simplified, the no sense access of the two communication ends is realized, and the dual isolation of the security access zone and the encryption and authentication based on the state secret algorithm are realized. The results of test and verification prove the feasibility of the design and the test results of key communication and security parameters are given. Compared with the current schemes, the design has been improved in terms of universality, performance and security, and has good practicability.

Keywords:security access zone;universal;isolation;encryption;authentication

(编辑 钱悦)