调度与变电站一体化系统远程维护安全防护设计

易 强，万书鹏，彭 晖，张 凯
(国电南瑞科技股份有限公司，江苏 南京 211106)

摘 要：安全防护是调度与变电站一体化系统的关键技术。针对调变一体化系统中存在的安全隐患，以远程维护为例介绍了调度与变电站一体化的安全防护关键技术，提出了安全远程维护的解决方案，即通过一体化双因子登录技术进行安全登录，通过一体化签名认证技术实现安全通信，通过一体化权限管理技术进行细粒度的权限管理和认证。提高了调变一体化系统远程维护抵御风险的能力，有效保障了调度与变电站系统一体化运行、一体化维护的安全性。

关键词：调度与变电站一体化系统；远程维护；双因子；数字证书；权限管理
中图分类号：TM76 **文献标志码**：A **文章编号**：1009-0665(2015)01-0040-03

智能电网调度技术支持系统在调度主站已经广泛应用[1]，智能变电站技术也日趋成熟并得到全面推广，但是传统模式下，调度与变电站松散的交互方式已越来越难以满足电网安全稳定运行和精细化管理的要求，智能电网建设迫切需要将调度与变电站统筹设计，形成综合型、平台化调度与变电站一体化系统[2-4](以下简称调变一体化系统)。调度和变电站广域分布，其一体化运行、一体化维护的安全防护是必须解决的问题。调变一体化系统安全技术遵循以“安全分区、网络专用、横向隔离、纵向认证”为核心的二次安全防护标准规范。目前，无人值守智能变电站已经开始逐步替代了传统变电站，当调度中心显示屏上出现遥信状态异常、通信中断等故障时，调度中心往往无法立即判断具体的故障原因，错失排除故障的最佳时机，因此远程维护[5-7]在无人值守变电站中得到了广泛的应用。国内已有学者对调度与变电站间的远程维护的安全做过研究，但是研究内容仅局限于采用纵向加密装置进行边界安全防护，未见用户双因子登录、系统内通信安全以及人员权限认证保护等方面的内容。文中以远程维护为例，提出了一种基于调变一体化系统的远程维护安全策略，采用双因子登录技术保障用户的登录安全，通过对发送数据的数字签名实现全过程的安全通信，通过平台一体化进行细粒度的有限认证。

1 远程维护安全需求

1.1 登录验证

调度中心对变电站进行远程维护，需要在调度中心进行登录。目前调度中心登录方式一般采用用户名与口令相结合的方法，未采用高安全等级的安全访问控制机制。一旦维护人员口令泄露，系统就可能被恶意登录，进而导致信息泄露，甚至威胁电网安全。

1.2 通信安全

目前调度中心和变电站之间的数据通信安全主要通过纵向加密装置保证，这种方式考虑了调度数据网传输的安全性，未考虑调度和变电站自动化系统内自身通信的安全性。智能变电站中基于 IEC 61850 标准的各厂家互操作未考虑安全认证问题，支持任意客户端的连接。如果远程维护数据在系统内被篡改或被重置，将无法被发现。

1.3 权限管理和维护

无论调度中心还是变电站自动化系统内都有一套完整的用户权限管理机制，能为每个用户定义各自独立的访问控制权限。但是调度自动化系统与变电站自动化系统间的远程维护缺乏有效的权限管理机制，而且无法灵活地为不同的维护人员配置不同的访问控制权限。

2 远程维护安全总体设计

基于集成平台的调变一体化系统采用面向服务的体系结构(SOA 架构)，如图 1 所示，将调度中心和变电站的信息进行统一维护，实现调度中心和变电站的信息共享和各种一体化应用。

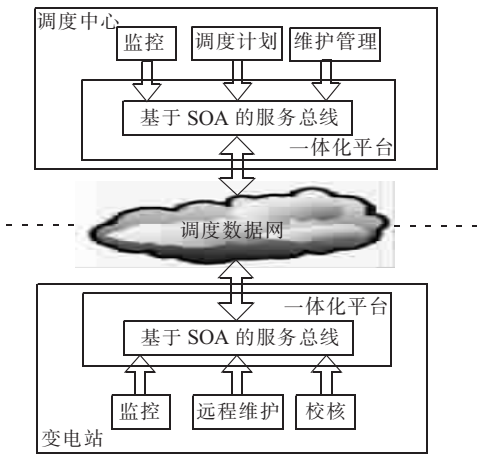

图 1 基于 SOA 服务总线的一体化系统架构

调变一体化系统基于 SOA 架构的服务总线跨越

收稿日期：2014-07-25；修回日期：2014-09-18

调度系统和变电站监控系统，在调度中心的操作就可实现对变电站的远程维护。调度中心侧运行远程维护界面程序,变电站侧启动远程维护的相应服务,两者之间通过服务总线进行远程通信。

如图 2 所示,结合目前远程维护的安全需求,在原有纵向加密装置进行边界安全防护基础上，进行了如下几方面的安全强化设计。

(1) 一体化双因子登录技术。系统管理员登录远程维护界面时需要进行双因子登录，系统将通过数据库认证人员身份以及查询用户权限信息表，判断登录用户是否具有远程维护权限。

(2)一体化签名认证技术。进行数据远程通信时,调度中心侧的服务总线会对请求数据进行数字签名,变电站侧的服务总线负责使用公钥证书进行验签。

(3) 一体化权限管理技术。变电站侧的远程维护服务最终会从请求数据中获取远程维护请求者的用户名，并根据自己本地定义的权限信息判断该用户是否具有具体的访问权限。

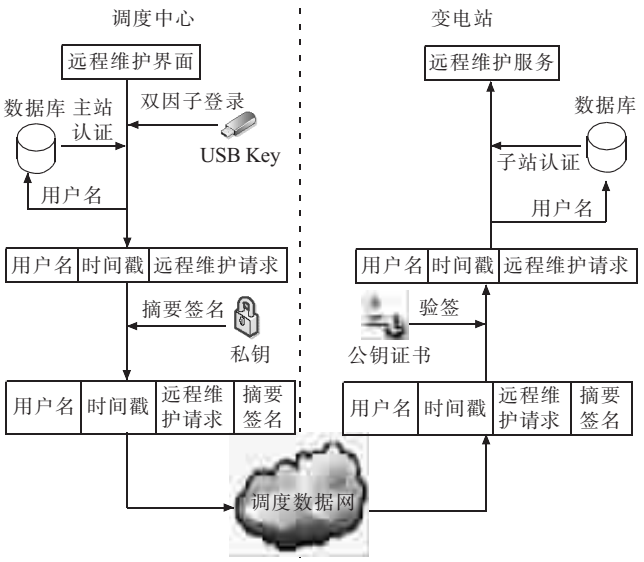

图 2 调变一体化系统远程维护安全认证流程

3 远程维护安全防护关键技术

3.1 一体化双因子登录技术

在调度中心，用户登录远程维护界面的过程采用一体化双因子登录技术。一体化双因子登录技术是依托电力调度数字证书系统，将电力调度数字证书与用户口令结合的高安全等级的认证方式。登录过程包括 2 个环节，一是用户需要插入电力调度专用移动数字证书(USBKey)进行身份认证。我国电力调度证书系统采用了分布式结构[8,9],电力调度系统的数字证书由本级别拥有电力调度根证书的证书签发机构统一签发，电力调度系统的数字证书采用电力调度专用的 USBKey 作为载体。USBKey 签发后,每个调度员都拥有一个与其身份相对应的 USBKey。USBKey 携带方便,能够做到调度人员人手一个,需要下发调度指令时插入 USBKey,能唯一地识别调度员身份。USBKey 登录时，弹出个人识别密码（PIN 码）框需要输入的 USBKey 的 PIN 码,PIN 码类似于 USBKey 的密码，PIN 码保护功能还能防止 USBKey 丢失后被他人使用。只有 PIN 码输入正确，系统才会继续对 USBKey 中的身份信息进行验证,否则,将会直接登录失败。系统中通过调度数字证书签名的信息将发送到站，并经过站端系统的验证。

双因子登录的另一个环节需要用户输入正确的用户名和对应的密码。程序能够验证用户名和 USBKey 中身份证书的一致性，防止用户名和密码泄露导致的安全隐患。采用双因子登录的同时,程序还将验证用户是否具有远程维护权限，保证只有维护人员才能成功登录远程维护界面。

3.2 一体化签名认证技术

为了保证调度中心发送给变电站的远程维护信息的通信安全，采用一体化数字签名技术对远程维护请求进行加密。在加密时,将把用户名和时间戳包含到报文中。在远程维护操作信息中加入用户名,可用于后续在子站验证远程维护操作的权限;加入时间戳,既能保证每次报文内容不相同，又能用于对报文进行时效性验证，防止报文被重置。超过时间阈值的远程维护信息,被视为不安全的信息,变电站将会断开此次与调度中心的会话连接,远程维护操作将不被执行。

如图 3 所示,在调度中心将用户名、时间戳和远程维护请求三部分信息作为需要进行签名的内容（以下称作 Message),首先对 Message 进行摘要操作得到摘要内容 Dmsg，再使用私钥对摘要结果 Dmsg 进行加密,得到摘要签名 Smsg。最后将内容 Message 和摘要签名 Smsg 组成远程维护安全报文发给变电站。

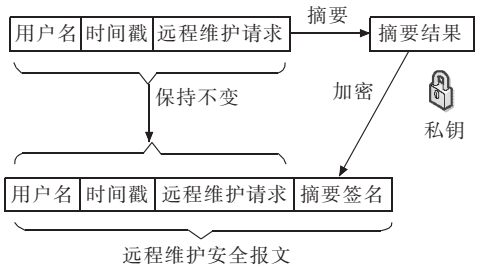

图 3 远程维护报文数字签名流程

变电站收到主站的请求后，将进行验证报文安全性和有效性的操作,一体化验签过程如图 4 所示。取出用户名、时间戳和远程维护请求三部分的内容作为 Message，对 Message 进行摘要算法的计算，得到 Dmsg_in。取出远程维护安全报文的摘要签名部分 Smsg,使用公钥对摘要签名 Smsg 进行解密,得到需要

验证的摘要 Dmsg_out。然后比较原摘要 Dmsg_in 和需要验证的摘要 Dmsg_out 是否相同，如果 Dmsg_in 和 Dmsg_out 相同，则说明远程维护安全报文内容没有改变，才会进行后续的权限验证。如果 Dmsg_in 和 Dmsg_out 不同，则说明远程维护安全报文内容被改变，该报文不应该被继续处理，服务连接断开。

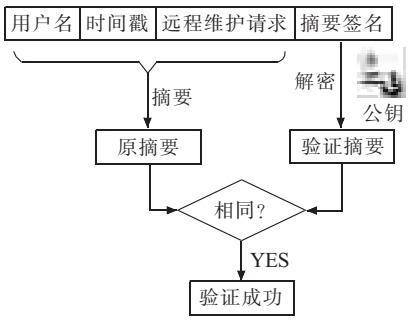

图 4 远程维护报文验签流程

远程维护请求信息验证通过后，还需要验证时间戳。在正常情况下，操作报文由调度中心发往变电站，时间花费应该很短。当变电站收到的远程维护安全报文的时间戳与本地的系统时间相差大于阈值时，变电站侧一体化系统会认为该报文存在被非法复制的可能，将断开会话连接。只有安全报文的时间戳与本地的系统时间之差小于有效时间阈值时，才会继续处理远程维护报文。

3.3 一体化权限管理技术

远程维护中，用户虽然是在调度中心登录，但是调度中心只进行用户是否具有远程维护权限的粗粒度认证，具体的权限认证是由远程变电站的对应服务根据自身需要进行认证。

和传统的远程维护访问控制需要单独架设权限认证服务器不同[10]，在调变一体化系统中，对调度中心维护人员权限的认证可以直接使用变电站系统中的权限服务。已有的调变一体化系统中的权限管理为服务使用者提供了丰富的控制手段，是各类应用实现数据安全访问控制的重要机制。通过已有的权限管理工具，可以很灵活地为远程维护人员配置不同的权限，既可以进行基于对象(模型表、图形、报表、流程等)的权限控制，也可以进行基于物理节点(工作站、服务器等)的权限控制。通过这种在变电站进行细粒度的权限认证，使得同一个调度中心的远程维护人员可以在不同的变电站拥有不同的维护权限，而这些权限是由变电站的管理人员控制的。这就保证了调度中心的远程维护人员必须经过变电站的授权才能进行远程维护，从而保证了变电站自身的安全。

4 结束语

针对调度中心远程维护变电站时可能存在的安全隐患，以调变一体化系统为基础，通过 USBKey 数字证书和用户名密码认证，实现了调度人员的一体化双因子登录；通过一体化数字签名认证技术，将用户名和时间戳结合到远程维护报文中进行数字签名，解决了远程维护报文通信的安全问题，有效防止了远程维护报文被篡改和重置的可能性；使用维护人员的登录用户名在变电站上进行权限对比，实现了细粒度的权限认证和主子站的一体化权限管理。结合本文提出的安全防护技术，已开发出了调变一体化系统安全远程维护功能。采用安全防护关键技术的调变一体化系统远程维护功能已经在江苏省电力调度中心进行了测试，满足设计要求。江苏省电力调度中心试运行的结果表明，各项安全指标满足实用化验收的安全标准。调变一体化安全防护技术使得远程维护的安全性得到有效提高，有效保障了调度中心和变电站一体化运行、一体化维护的安全防护要求。

参考文献：

[1] 彭 晖，赵家庆，王昌频，等. 大型地区电网调度控制系统海量历史数据处理技术[J]. 江苏电机工程，2014，33(5)：11-14.

[2] YANG Z H , ZHANG H B, ZHAI M Y ,et al. Study on Control Center and Substation Integrated Monitor and Control System in Smart Grid [C]// 2012 GIGRE Canada Conference:Technology and Innovation for the Erolving Power Gird,Moteral Canada , 2012：24-26.

[3] 万书鹏，雷宝龙，翟明玉. 调度与变电站一体化系统链路状态监测与 TCP 通信方案[J]. 电力系统自动化，2014，38(1)：92-96.

[4] 史金伟，杨启京，肖艳炜，等. 异构系统间数据远程调阅的方法与实现 [J]. 江苏电机工程，2014，33(2)：44-47.

[5] 梁运华，沈梦甜. 500 kV 变电站自动化系统实时远程维护实现 [J] .电力系统保护与控制，2010，38(14)：165-168.

[6] 詹成国，钟 昀，徐 敏. 一种基于 P2P 技术的远程维护工具的实现[J]. 电力系统自动化，2011，31(10)：131-133.

[7] 高 卓，罗 毅，涂光瑜. 基于分布式对象技术的变电站远程维护系统[J]. 电力系统自动化，2002，26(16)：66-70.

[8] 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(S)：71-75.

[9] 王 文，鲁玉华，陶静娜，等. 电力调度证书系统的特点及应用 [J]. 电网技术，2007，31(12)：23-27.

[10] 段 斌，刘 念，王 键，等. 基于 PKI/PMI 的变电站自动化系统访问安全管理[J]. 电力系统自动化，2005，29(23)：58-63.

作者简介：

易 强(1983)，男，江苏徐州人，工程师，从事电网调度自动化系统研发工作；

万书鹏(1982)，男，江苏南京人，工程师，从事电网调度自动化系统研发工作；

彭 晖(1974)，男，重庆人，高级工程师，从事电网调度自动化系统研发和管理工作；

张 凯(1986)，男，江苏徐州人，助理工程师，从事电网调度自动化系统研发工作。

(下转第 46 页)

网来提高全网设备的稳定性,保证数据的正确交换。

(3) 交换机流量控制。即便是千兆网络,也需要评估全部设备接入后交换机的流量状况, 保证交换机的负载不能过重。

(4) VLAN 确认。通过 VLAN 划分,减少接收设备无效数据的接收,也减少交换机内部数据转存,提高数据的有效流动。

(5) 交换机延时标记确认。为尽可能提高保护的动作速度, 对于网络上各级交换机的 SV 数据包的延时时间需要正确统计, 为网采需要设定采样回退时间的保护、测控等设备提供参数。

4 结束语

随着通信技术的发展,尤其是交换机技术的发展,三层一网的组网方式成为可能。文中研制的基于三层一网要求的保护装置, 在站域保护控制系统、110 kV 线路保护等多间隔保护等方面取得了应用。相关测试试验表明,装置的性能指标满足要求,在网络风暴的环境和时钟丢失的条件下,装置依然能够正常工作。随着智能变电站的发展, 三层一网的组网方式由于自身的优势也会得到推广应用, 基于三层一网的保护装置也会有广阔的应用前景。

参考文献:

[1] 陈 磊,张侃君,夏勇军,等. 智能变电站站域保护研究综述[J]. 华东电力,2013,41(5):0947-0952.

[2] 杜振华,王建勇,罗奕飞,等. 基于 MMS 与 GOOSE 网合一的数字化网络保护设计[J].电力系统保护与控制,2010,38(24):178-181.

[3] 和敬涵,李 倍,刘 琳,等. 基于分布式功能的站域保护[J]. 电力系统保护与控制,2014,42(6):26-32.

[4] 董新洲,丁 磊. 数字化集成保护与控制系统结构设计方案研究[J]. 电力系统保护与控制,2009,37(1):1-5.

[5] 高东学,智全中,朱丽均. 智能变电站保护配置方案研究[J]. 电力系统保护与控制,2012,40(1):68-71.

作者简介:

窦乘国(1974),男,湖南永州人,工程师,从事继电保护、智能变电站应用的相关研究工作;

张宏波(1975),男,吉林伊通人,高级工程师,从事嵌入式软件在电力系统内应用、智能变电站应用的相关研究工作;

陆征军(1973),男,江苏张家港人,高级工程师,从事继电保护、智能变电站应用的相关研究工作。

The Development of the New Protective Device Based on the Three-level-in-one-network Situation of Smart Substation

DOU Chengguo, ZHANG Hongbo, LU Zhengjun

(Shanghai SHR Electrical Power Technology Co. Ltd. Nanjing Branch, Nanjing 210012, China)

Abstract: The development of the communication technology makes it possible of integrating the sampled value (SV) network, generic object oriented substation events (GOOSE) network and manufacturing message specification (MMS) network for the bay level, the process level, and the station level (three-level-in-one-network). A new developed protective device for this integration can realize the grading and separate treatment of the network data. Meanwhile, this new device can network with the corresponding switch, which can solve the data synchronization problem under the three-level-in-one-network condition, thus the problem of the data reliability and availability of the protective device can be solved. Under the three-level-in-one-network structure, this device can meet the requirements of protection and control in the smart substation. The reliability of this new developed protective device already has been verified by relevant tests.

Key words: three-level-in-one-network; gateway; networking; point-to-point

(上接第 42 页)

Design of Security Protection for Remote Maintenance in Dispatch and Substation Integrated System

YI Qiang, WAN Shupeng, PENG Hui, ZHANG Kai

(NARI Technology Development Co. Ltd., Nanjing 211106, China)

Abstract: Security protection is a key technique of the dispatch and substation integrated system. From the point of view of security risks in dispatch and substation integrated system, taking remote maintenance as an example, a method based on double-factor login, digital certificate and right authentication for security protection has been designed. Firstly, login with a double-factor strategy makes sure its safety. Secondly, communication packet must be signed and verified. Finally, verifying user's access right in the substation. These measures enhance the system to resist risks in dispatch and substation integrated system.

Key words: dispatching and substation integration system; remote maintenance; double-factor; digital certificate; right management