电力调度自动化系统中物理隔离技术的研究与应用

程碧祥
(四川乐山电业局,四川 乐山 614000)

摘 要:主要阐述了物理隔离技术的原理、装置的实现以及在电力监控系统局域网中的应用情况。指出在应用物理隔离装置时的几个误区和需要注意的问题。

关键词:物理隔离;安全防护;调度自动化系统(SCADA)

Abstract: The principle of physical isolation technique, the realization of its devices and its application to local area network of supervisory control and data acquisition system are mainly described. And several mistaking understandings during using physical isolation devices are pointed out as well as the points needing attention.

Key words: physical isolation; safety protection; dispatching automation system

中图分类号:TM734 **文献标识码**:A **文章编号**:1003-6954(2008)01-0073-03

电力系统的MIS系统是集用电营业管理、生产技术管理、财务管理、人事劳资管理、档案管理等多项管理功能于一体的局域网络系统,它是电力企业实现信息资源共享、无纸化办公的基础。而调度自动化SCADA系统是集变电所端设备RTU与调度主站端设备于一体的数据采集处理系统,这个系统主要是为监视电网的运行、指挥变电所的倒闸操作及事故处理、保障电网的安全服务的。可见,MIS系统与调度自动化SCADA系统的服务对象、网络安全、及软硬件结构都不大相同,但为了实现资源共享、减少投资,MIS系统又应该能够调用调度自动化网的实时数据,这就涉及到MIS系统(简称MIS网)与SCADA系统的安全接口问题,中国十分重视电力系统的安全问题,为了防范对电网和电厂计算机监控系统及调度数据网络的攻击侵害及由此引起的电力系统事故,国家经贸委在2002年发布了30号令《电网和电厂计算机监控系统及调度数据网络安全防护的规定》,该规定要求两个隔离:各电力监控系统必须与办公自动化系统(MIS)实行有效(物理)隔离措施;电力调度数据专用网络必须与综合信息网络及因特网实行物理隔离[1]。

因为TCP/IP是冷战时期的产物,目标是要保证通达,保证传输的粗旷性。通过来回确认来保证数据的完整性,不确认则要重传。而TCP/IP没有内在的控制机制,来支持源地址的鉴别,证实IP从哪儿来。这就是TCP/IP漏洞的根本原因。黑客利用TCP/IP这个漏洞,致使能够通过监听或窜改网络上传送的数据、破解密码或者发送蓄意制造的数据来获得机密信息或伤害他人,大多数安全问题都是这个原因[2]。

网络安全的主要内容是如何保护网络数据的安全和维持系统的正常运行,人们为了保证网络安全,基本上是使用防火墙。但是传统的防火墙只能在一定程度上保护网络安全,也很难解决内部网的安全问题,而据权威部门统计结果表明,网络上的安全攻击事件有70%左右来自网络内部的攻击[2]。另外,防火墙难于管理和配置,容易造成安全漏洞,防火墙管理员必须对网络安全攻击的手段及其与系统配置的关系有相当深刻的了解。根据美国财经杂志统计资料表明,30%的入侵发生在有防火墙的情况下[3]。

结合目前国内电力调度自动化系统的实际情况,下面从系统安全防护的角度论述了地区电网控制中心自动化系统建设中要着重考虑的物理隔离和安全防护技术的发展及其应用情况,以期为新一代调度自动化系统的规划和设计提供技术上的支持和建议。

1 电力系统的安全防护需求分析

1.1 安全区之间的划分

根据国家电力公司的《电力二次系统安全防护方案(第7稿)》文件,电力二次系统安全防护方案根据电力系统的特点及各相关业务系统的重要程度、数据流程、目前状况和安全要求,将整个电力二次系统分为四个安全区:Ⅰ实时控制区、Ⅱ非控制生产区、Ⅲ生产管理区、Ⅳ管理信息区。对不同的安全区确定了不同的安全防护要求,从而决定了需要实现不同的安全等级和防护水平、隔离强度。其中安全区Ⅰ的安全等级最高,安全区Ⅱ次之,其余依次类推。电力二次系

统网络隔离目标是确保电力实时闭环监控系统及调度数据网络的安全，抵御黑客、病毒、恶意代码等通过各种形式对系统发起的恶意破坏和攻击，特别是能够抵御集团式攻击，防止由此导致一次系统事故或大面积停电事故，及二次系统的崩溃或瘫痪。

电网二次系统安全防护体系分为三层：第一层为实时系统，第二层为生产管理系统，第三层为电力信息系统。这三层反映了各层中各系统的不同重要性。

在层中按安全等级的不同又区分为安全工作区。第一层被认为是一个独立的安全区Ⅰ，而第二层根据所连接的外部边界通信网络为省调度数据网 FJPDnet 和不连 FJPDnet 的二部分。因而前者为安全区Ⅱ，后者为安全区Ⅲ。第三层电力信息系统，目前暂设为一个安全区，或者说对电力信息系统的安全区的划分在本框架中不作规定。

第一层是安全保护的核心，调度中心实时监控系统即调度自动化系统。它是调度决策系统，面向调度员，其数据实时性为秒级，原则上实时监控均需经过调度自动化系统。其外部边界的通信，传统的远动通道的通信可以认为不存在网络安全问题。其它外部边界通信网边界为电力数据通信网。

第二层生产管理系统层，调度中心生产管理系统即调度生产管理系统。在调度生产管理系统中属于安全区Ⅱ的典型系统包括电量计量系统、故障信息系统等。其面向的使用者为运行方式、运行计划工作人员及电力市场交易员等。数据的实时性是分级、小时级、日、月甚至年。该区的其它外部边界通信网边界为调度数据通信网 FJPDnet－VPN2。

安全区Ⅲ是调度生产管理系统中经电力信息网互联的区域。该层中典型的系统为调度 MIS 系统和相关系统的 WEB 发布等。在该区中是公共数据库内的数据可提供运行管理人员的 web 浏览。

安全区Ⅳ是指包括办公自动化系统或办公管理信息系统，经电力信息网 PInet 互连。

调度中心中各系统分置于三层四安全区的安全防护体系的原则：根据该系统的主要业务特点及面向使用者决定其置于调度自动化系统层、调度生产管理系统层安全区Ⅱ/安全区Ⅲ、还是电力信息系统层。进行实时控制或未来可能为实时控制的均需经调度自动化系统。

某些系统的次要业务或与外部通信所需的外部边界通信网络相匹配的安全区与按前述原则所选定的安全区不一致，可采用以下两法之一：系统分为若干子系统。其主要子系统仍在所选定的安全区中，其他子系统也相应在各安全区中，在层间通信能保证满足其时延要求的条件下，经过层间通信来构成整个系统。整个系统置于由次要业务或与外部通信所需的外部边界通信网络相匹配的安全区中，通过把用户终端设备直接接到用户处。

1.2 安全区之间的隔离

在各安全区之间均需选择适当安全强度的隔离装置。具体隔离装置的选择不仅需要考虑网络安全的要求，还需要考虑带宽及实时性的要求。安全区之间隔离装置必须是国产并经过国家或电力系统有关部门认证。

1) 安全区Ⅰ与安全区Ⅱ之间的隔离要求：采用硬件防火墙可使安全区之间逻辑隔离。禁止跨越安全区Ⅰ与安全区Ⅱ的 E－MAIL、WEB、telnet、rlogin。

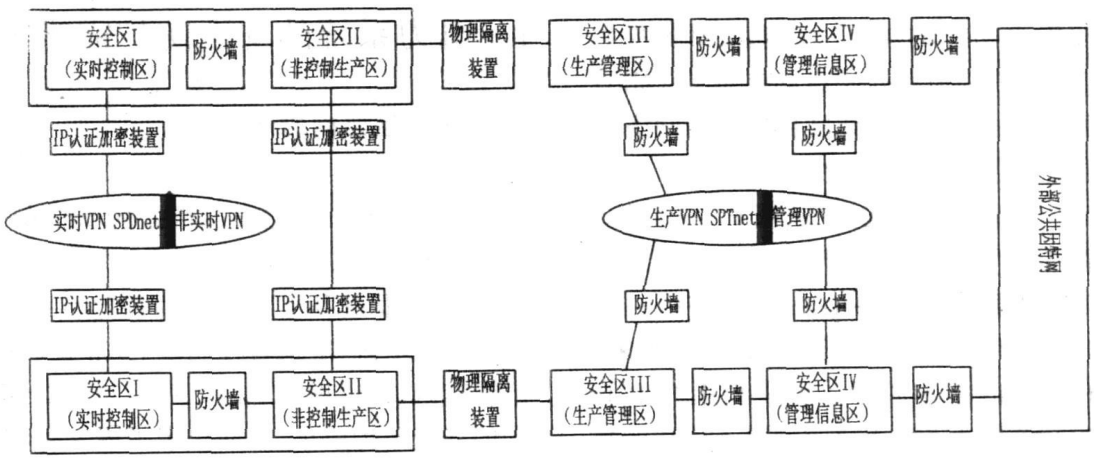

图 1 二次系统安全区划分框图

2) 安全区Ⅰ/Ⅱ与安全区Ⅲ/Ⅳ之间的隔离要求:采用物理隔离装置可使安全区之间物理隔离。禁止跨越安全区Ⅰ/Ⅱ与安全区Ⅲ/Ⅳ的非数据应用穿透。物理隔离装置安全防护强度适应由安全区Ⅰ/Ⅱ向安全区Ⅲ/Ⅳ的单向数据传输。由安全区Ⅲ/Ⅳ向安全区Ⅰ/Ⅱ的数据传输必须首先经安全区Ⅰ/Ⅱ内的进程发起联接,然后通过建立的链路进行数据传输。

3) 同一安全区间纵向防护与隔离:同一安全区间纵向联络使用VPN网络进行连接,安全区Ⅰ/Ⅱ分别使用SPDnet的实时VPN与非实时VPN,安全区Ⅲ/Ⅳ分别使用电力数据网的VPN。

2 目前物理隔离设备的应用现状

目前国内电力系统应用的定向式物理隔离装置主要有两种,按照数据传输方向的不同分为正向式物理隔离装置和反向式物理隔离装置,分别应用于安全区Ⅲ/Ⅳ到安全区Ⅰ/Ⅱ的单向数据传递。

应用的产品包括北京科东电力控制系统有限责任公司的StoneWall－2000系列网络安全隔离装置,南瑞信息系统分公司SysKeeper－2000网络安全隔离装置;珠海鸿瑞公司的电力系统专用网络隔离仪等。

多数用户参照"三层四区"的安全防护原则将物理隔离装置使用在安全区Ⅲ/Ⅳ到安全区Ⅰ/Ⅱ的单向数据传递上,其中Ems系统一般都使用正向式物理隔离装置,而电量系统多采用反向式物理隔离装置。

3 物理隔离设备的安全技术分析[3]

物理隔离技术架构在隔离上,物理隔离的一个特征,就是内网与外网不连接,内网和外网在同一时间最多只有一个同隔离设备建立数据连接。

3.1 隔断网络之间的连接,保证内网不被入侵

除了定义的数据流,从外网不能访问内网,即使外网被入侵,内网不会有任何破坏。实际的数据和服务都放在内网,外网只是一个应用代理系统,修复外网系统非常容易。物理隔离技术解决了系统本身受攻击的问题。防火墙可以定义安全政策控制数据流,但是本身如果被攻击和入侵,就不能起到任何防护作用。比如防火墙的操作系统,网络协议的实现,都有可能存在漏洞。

3.2 保护内部服务

物理隔离不但能够保证内部系统不会被入侵和篡改,也能保证内部系统开放的服务不会遭到IP炸弹的DOS/DDOS攻击。当前最流行、最有效的攻击是DOS/DDOS攻击,这是建立在TCP/IP网络协议的漏洞上的。

3.3 内容检查

内容检查是最高安全性的要求。这是在防火墙技术发展过程中被认识到的。物理隔离技术的内容检查是建立在应用代理上的。所不同的是,物理隔离系统是隔离的双系统,每个系统都采取应用代理,内容检查建立在可信任的内部系统的应用代理上,这样保证了真正的安全。内容检查,包括应用协议检查、命令检查、内容过滤、杀病毒等。

所以,物理隔离技术是建立在首先保证自身安全基础上的,能够屏蔽网络协议攻击和进行内容检查和过滤的安全技术,比防火墙安全。但是与应用协议相关,速度和带宽会比防火墙稍低,所以其应用范围是数据交换形式简单,但是安全性要求特别高的场合,一般是隔断局域网。防火墙一般与应用协议无关,高速度高带宽,可以用于骨干网之间的连接。

4 应用物理隔离需要注意的几个问题

4.1 使用国产物理隔离设备的必要性

由于目前的很多防火墙和路由器也具备将某一个或者几个端口设置为只允许数据单向流通。但考虑到目前多数的防火墙和路由器均由国外厂商提供,在设计时也经常会因为考虑不周而留有"后门"等安全隐患,所以不能一味依赖国外设备,必须使用国产物理隔离设备做为安全防护的最终屏障。

4.2 支持双机热备

由于物理隔离设备直接联系着内网与外网,在实际应用中,可以设置有双机备份,一台工作在主机位置,一台工作于备用位置,两台机器时刻进行通信并进行信息备份,一旦一台隔离设备出现故障时,或者处于看门狗复位阶段,备机可以承担起主机的工作,以避免重要数据的丢失。结合物理隔离设备的荣誉,系统的MIS服务器也可以规划为冗余配置,提高系统的可靠性和可行性。

4.3 正、反向物理隔离装置的混用

系统中可以同时使用正向和反向 (下转第83页)

烧助燃风。该助燃风:风压≥2 500 Pa,单只油燃烧器最大风量:约1 500 m^3/h。助燃风可直接利用原燃烧器中心风,在每路单独加装手动蝶阀,以方便调整助燃风参数,确保油燃烧效果达到最佳。

热工监控系统主要包括小油枪点火控制系统、图像火焰监视系统、一次风速在线监测系统、燃烧器壁温监测系统等。

4 锅炉采用小油枪技术后的运行效果与结论

1)小油枪能安全、稳定地点燃煤粉,有较高的燃烧效率,不爆燃、不发生二次燃烧。

2)小油枪能与机组启动曲线相适应,保证启动过程整台机组的安全。

3)在机组燃烧不稳定的情况下,快速地投入小油枪点火及助燃系统,通过改善单角燃烧器的燃烧情况进而改变整个锅炉的燃烧状况。

4)运行监视、操作和调整方便、灵活。

两台锅炉安装小油枪点火系统后,点火助燃阶段用油节约80%,低负荷稳燃用油节约70%。运行一年后,统计燃油实际消耗350 t,则节省燃油1 050 t,其直接节能经济效益达500万元/年。两台锅炉安装小油枪点火设备的初投资总共为240万元。

5 应用研究结果

通过国电深能四川华蓥山发电有限公司两台大型乏气送粉锅炉(1 025 t/h)采用小油枪点火节能技术的应用研究结果表明:小油枪点火技术在锅炉启动过程中能保证启动过程的安全,即安全稳定地点燃煤粉,不爆燃、不二次燃烧;投入功率能满足锅炉点火启动曲线的要求;在正常运行中,不影响主燃烧器的主要功能,不影响整体燃烧组织、不超温、不结渣,能满足锅炉检修周期的要求。该技术具有良好的经济效益与社会效益。

由于国内燃煤市场的变化,各个电厂在设计与实际运行中,燃煤变化都较大。特别对采用乏气送粉的锅炉机组,由于乏气送粉系统本身对煤种的适应能力较差,所以在燃用煤质变化较大,特别是高灰份、低挥发份、低发热量煤时,采用小油枪点火技术对同类电厂有很大借鉴作用。

(收稿日期:2007-11-15)

(上接第75页) 物理隔离装置。但是不能将其等同的视为一个实时的,双向的网络连接。只能通过时间和软件的配合(多种情况需要人工干预),才能完成文件和数据双向传输的要求。

4.4 物理隔离装置和其他安防措施的配合

首先,隔离装置不能取代防火墙,而是与防火墙相辅相成的。目前的做法是将普通防火墙安装在整个电力系统子网和Internet接口处,然后将隔离装置安装在监控系统与信息系统的接口处。这样,在保证监控系统的安全前提下。用户可以使用上网的功能。

同时,物理隔离装置对于系统内部只用防止病毒入侵的功能,并没有查毒杀毒的作用,所以系统依然需要配置杀毒软件和定期维护软件病毒库来防治计算机的病毒。

4.5 系统远程维护功能的使用

通过拨号线路进入系统进行系统的远程维护,方便设备调试,是系统维护的一种重要手段。但考虑到系统安全的要求,应进一步改良远程维护的方式,例如在远方采用模拟系统进行调试的方式,或者在图形监控系统支持下,现场直接操作的方式进一步保证系统的安全稳定。

5 电力系统安全防护的展望

目前还没有一种技术可以解决所有的安全问题,但是安全防护考虑得越周到,针对不同的安防需求制定的措施越得当,网络愈安全。物理隔离装置是目前能够较完备的实现网络安全深度防御的安全设备。

此外,只有不断的加强电力系统内部对信息系统的安全教育培训,根据自身的特点和要求,设计和应用更多具有自主知识产权和应用方便、使用安全的设备和系统,才能在更大的范围内推进电力系统信息化建设的进程。

参考文献

[1] Andrens·Tanenbaum Computer Networks[M]·American:prentice hall·

[2] 高志国,龙文辉编·反黑客教程[M]·北京:邮电出版社·

[3] 雷云,凌玉华,廖力清·物理隔离在电力系统中的实现[J]·微计算机信息,2004,(1):107-109.

(收稿日期:2007-12-09)