《电力安全》编辑部

地址：苏州市西环路1788号
邮编：215004
电话：
0512-68602709(主编室)
0512-68602711(编辑部)
0512-68603420(广告部)
传真：
0512-68602711(编辑部)
0512-68602312(广告部)
E-Mail：
editor@csest.com(编辑部)
sale@csest.com(广告部)

热门文章 HOTS

- 综论电气误操作事故的
- 现场培训的探讨与分析
- 对安全生产中的几个不
- 对违章的思考(续1)
- 影响无人值班变电站运
- 500kV变电站3/
- 供电企业变电检修管理

电网监控系统与其它信息系统的网络隔离（2005年第1期）

作者：谢宇明(蕉岭县供电局，广东 蕉岭 514100) 点击：199

〔摘　要〕 分析了电网监控系统对安全性、可靠性、实时性的特殊要求,提出了在电力网络安全的体系中，应该采取必要的措施，使电网监控系统与其它信息系统进行网络隔离，并就相关技术手段进行了探讨，为建立严格的安全管理规章制度创造条件，确保电网监控系统和电力系统的安全.

〔关键词〕 电网监控系统；信息系统；网络隔离

引　言

随着Internet的迅速发展，信息安全问题面临新的挑战。电力系统信息安全问题已威胁到电力系统的安全、稳定、经济、优质运行，影响着“数字电力系统”的实现进程。开发相应的应用系统、制定电力系统信息遭受外部攻击时的防范与系统恢复措施等信息安全战略是当前信息化工作的重要内容。电力系统信息安全已经成为电力企业生产、经营和管理的重要组成部分，是电力系统安全运行和对社会可靠供电的保障。

电力系统信息安全是一项涉及电网调度自动化、继电保护及安自装置、厂站自动化、配电网自动化、电力负荷控制、电力市场交易、电力营销、信息网络系统等有关生产、经营和管理方面复杂的多领域大型系统工程。建立电力系统信息安全体系的一个关键问题是怎样实施实时监控系统(简称监控系统)与其它信息系统的联网。针对监控系统与其它信息系统互联而设计的“电力系统专用网络隔离装置”，对提高监控系统对有可能导致电网安全事故的攻击、病毒、泄密等的防御水平，消除绝大部分的安全隐患，为电力系统信息安全、电网安全运行把好最重要的关口，具有重大的意义。

1　网络环境

1.1　监控系统与其它信息系统的特点

监控系统是指电网运行控制系统，它包括各级调度自动化系统，对水、火电厂机组自动发电控制的电网AGC系统，继电保护，故障录波，安全自动装置，火电机组DCS系统，水电厂计算机实时监控系统，电力系统光纤、数字微波、模拟微波等通信系统等。监控系统类中的基于TCP/IP的数据业务，速率要求不高，数据流基本恒定，但业务实时性较强，其中遥控遥调更与电网安全直接相关，可靠性要求较高；从应用范围来看，生产控制类业务分布在各网省调及大量发电厂和变电站，属于较特殊的一类窄带业务。

其它信息系统是指以电力信息主干网络为中心，辐射各发、供电、施工、修造等单位的计算机信息网络系统。其它信息系统类业务突发性很强，速率要求较高，实时性不强，保密性要求较高，覆盖除生产控制类以外的所有数据业务，其网络布局集中于行政办公中心，一般要求为宽带网络。

1.2　监控系统与其它信息系统互联情况

近年来监控系统的内涵有了较大的延伸，其它信息系统的发展也很快。系统互联是生产管理的必然需要。目前主要有串行口联接和网关连接2种方式，按串行口联接基本不会带来攻击或病毒，但数据交互很不方便。因此，当前的监控系统与其它信息系统大多分不同网段通过网关联接，但是其它信息系统安全性不够，对实时监控系统会带来一些安全隐患(如攻击、病毒、泄密等)，导致电网安全事故。

2　网络隔离

2.1　网络安全

信息系统的安全主要包含5个层面，即物理安全、网络安全、系统安全、应用安全、人员管理。其中网络安全即网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，以免遭到破坏、更改、泄露，使系统连续可靠地正常运行，网络服务不中断。广义来说，凡是涉及到网络上

信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。

2.2　网络隔离

国家保密局颁布的“计算机信息系统国际联网保密管理规定”确定，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行物理隔离。电力生产事关国计民生，电力系统的安全非常重要，监控系统要求可靠、安全、实时，而其它信息系统要求完整、保密。两种业务应该有效安全隔离。

目前各级电力信息系统通常在企业Internet出口侧设普通防火墙，承担的是普通的网络隔断任务。在此基础上对网络进行分层，能增强系统的可靠性，具体实施是在监控系统与其它信息系统唯一接入点设置专用隔离装置，从物理上分为两级，以保证监控系统的安全，结构如图1所示。

图1　电力系统专用网络隔离防火墙接入配置

专用隔离装置提供了2个网络接口。除了监控系统LAN接口、其它信息系统LAN接口，还专门有一个控制口用来连接一台专用管理机，用于对装置进行配置、管理。

监控系统LAN区是不对外开放的区域，它只对其它信息系统LAN区提供部分服务，所以外部Internet用户检测不到它的IP地址，无法对它进行攻击。

其它信息系统LAN区可以对外提供服务，系统开放的信息都放在该区，由于它的开放性，就有可能成为黑客攻击的对象，但由于与监控系统是隔离开的，即使受到了攻击也不会危及监控系统。

3　技术平台

网络隔离装置的安全等级应高于防火墙，因此应选用目前国内通用的Linux为基础进行大幅整改的专用网络安全操作系统。

通用的Linux操作系统尽管能提供多种多样的功能，但由于其开放性和本身含有安全漏洞,因此极易受到攻击,直接导致了受其保护的网络的安全危机，而且这种通用操作系统的漏洞是不断被发现的，一经发现网上就会公布，相应的攻击办法也跟着公布，致使最终用户和制造厂商无法应付。因此对通用Linux应作如下方面的修改：

取消危险的系统调用或者截获系统调用,限制命令执行权限,取消IP转发功能,检查每个分组的接口,采用随机连接序号,驻留分组过滤模块,取消动态路由功能,采用多个安全内核等。

通过以上设计方法和实现技术，基于独立开发的专用网络安全操作系统之上，网络隔离装置的运行效率很高，安全性能优越。

4　应用介绍

网络隔离装置软件包含如下模块：内核模块，隔离模块(含状态检测模块),NAT模块,带宽管理模块,通信协议模块,图形用户界面模块(或者Web界面模块),透明代理模块(属于NAT模块),透明模式模块(包括ARP代理子模块、路由转发子模块等),各电力系统应用代理模块(包括过滤模块),流量统计模块，审计模块，其它模块(如MAC、IP地址绑定模块、简单的IDS、自我保护)等。

网络联接要求：监控网中主机(地址为10.43.10.233)可以单方向对其它信息系统DMIS前置主机(地址为192.168.2.66)传输层按TCP协议、端口为9000、应用层为用户自定义的通讯规约提供服务，而从管理角度其它所有的服务均不提供。

根据上述要求拟定网络隔离规则，对单个非特权端口、协议、单方向、监视定义帧头等联合安全策略控制，实现网络隔离。隔离装置将监控系统的安全性统一到其本身，网络安全性是在隔离装置系统上得到加固，而不是分布在监控系统网络的所有节点上，简化了监控系统安全管理。从而实现网络隔离装置的基本目标即作为一个中心“遏制点”，将监控系统的安全管理集中起来，屏蔽非法请求，防止跨权限访问，并产生安全报警。

电网监控系统与其它信息系统进行网络隔离是电力系统网络安全的重要核心，使用专用安全操作系统的网络隔离装置已势在必行，同时也要建立严密的安全管理措施相配合，以确保电网监控系统和电力系统的安全。

(收稿日期:2004-05-12)