电力系统一体化设计中信息安全防护体系研究

刘静芳[1],陈赤培[1,2],樊江涛[1]
(1. 华东交通大学 电气与电子工程学院,江西 南昌 330013;
2. 江西电力设计院,江西 南昌 330006)

摘要:建设电力系统集成环境已成为实现全电网信息共享的自动化系统的基础建设。然而,信息安全问题也是威胁电力系统的安全、稳定、经济、优质运行的重大问题。介绍了一体化的电力系统及特点;阐述了电力系统一体化信息安全的主要内容(保密性、完整性、有效性);几种安全技术(防火墙、虚拟专用网、认证中心、入侵检测系统等);以及一体化信息安全防护体系的设计原则、系数设计、管理上的安全策略。该系统安全方案已应用于地区电网自动化系统,效果良好。

关键词:电力系统;一体化设计;信息安全;安全防护
中图分类号:TM 73;TP 393.08 **文献标识码**:A **文章编号**:1006-6047(2005)02-0083-03

1 一体化的电力系统介绍

1.1 一体化的电力系统及特点

一体化的电力系统是包括各级电网调度自动化系统、变电站自动化系统、配电网自动化系统、水调自动化系统和水电梯级调度自动化系统、电能量计量计费系统、实时电力市场的辅助控制系统等在内的自动化系统总称。它具有可靠性、安全性、完整性、一致性、及时性等特点[1]。

1.2 电力系统一体化的信息安全

电力系统一体化的信息安全问题成为电力企业生产、经营和管理的重要组成部分。结合电力工业的特点,要保障信息安全,不仅要进行信息的安全保护,还要重视提高系统的入侵检测能力、系统的事件反应能力及系统遭受破坏后的快速恢复能力。除了加密[2]、身份认证、访问控制[3]、防火墙[4]、安全路由等安全技术,还强调信息系统整个生命周期的防御和恢复。电力自动化系统一体化的信息安全就是要保护系统内的信息和计算资源不被未授权访问、篡改和拒绝服务攻击,防止病毒入侵、黑客入侵、操作错误等带来的系统威胁,主要包括以下几方面内容:

a. 保密性是防止系统内信息的非法泄漏;

b. 完整性是防止系统内软件与数据被非法删改和破坏;

c. 有效性是要求信息和系统资源可以保持有效。

1.3 设计中普遍应用的几种安全技术

当前流行的安全产品很多,如防火墙、虚拟专用网(VPN)、认证中心(CA)以及入侵检测系统[5](IDS)等,其各有特点,可根据实际情况应用于不同网络层次和不同安全程度的电力自动化网络中。

1.3.1 防火墙

防火墙是一种古老而又有着很大发挥余地的网络安全构件,在企业网络和不安全网络之间设置障碍,阻止对信息资源的非法访问,可使用防火墙阻止专利信息从公司网络上被非法输出。目前,防火墙系统大多指“硬件防火墙”,它一般由防火墙硬件卡和防火墙策略服务器软件组成。应用时需要服务器和工作站上安装防火墙硬件卡,在服务器上安装对应的防火墙策略服务器软件,并通过这个策略服务器软件对整个网络系统中的防火墙进行配置、管理。防火墙适用于相对独立的、与外部网络互连途径有限、服务种类相对集中的单一网络,可有效地保护局域网。

1.3.2 虚拟专用网 VPN

VPN 是利用基于公共基础设施建设的公开网络的数据传输能力,借助相关安全技术和手段实现的,能够提供安全、可靠、可控的保密数据通信的一条安全通道。确切来说,VPN 是利用不可靠的公用互联网络作为信息传输媒介,通过附加的安全隧道、用户认证和访问控制等技术实现与专用网络相类似的安全性能,从而实现对重要信息的安全传输。VPN 引入电力系统既可以大大降低电力网络的生产投入,又可以摆脱部分繁重的网络升级和维护工作量。在 VPN 的支持下,电力网络的可扩展性大为提高,并且可以灵活调整电力系统各部门间的协调关系,对电力系统各部门参与一些突发事件的处理提供高效的网络支持,降低协调办公的费用。隧道技术是 VPN 的核心,它是一种基于网络层协议的规范,用于确保两点之间或两端之间数据传输隧道的建立和拆除。VPN 的实现依赖于网络设备及固化于网络设备上的控制软件,现在交换式VPN 的核心设

收稿日期:2004-02-21;修回日期:2004-12-07

备就是VPN交换机,它用隧道交换可以将访问直接导向相应的隧道终端,使不同的网络用户可以进入不同的网段。

1.3.3 入侵检测系统IDS

入侵检测是用于检测任何损害或企图损害系统的保密性、完整性或可用性行为的一种网络技术,是一个全新的、迅速发展的领域。IDS通过实时的检测,检查特定的攻击模式、系统配置、系统漏洞、存在缺陷的版本及系统或用户的行为模式,监控与安全有关的活动。IDS由网络探测代理、数据管理服务器组成。网络探测代理是运行在一个专门的主机上监视网络上流过的所有数据包,当发现受到攻击时将信息发送到数据管理服务器,同时服务器上的数据库记录这些信息。

2 一体化信息安全防护体系设计及应用

2.1 设计原则

由于电力系统集成了监控和数据采集系统(SCADA)、电力系统应用软件(PAS)、调度管理信息系统(DMIS)、电能量计量系统(TMR)等自动化系统,不仅包括电网运行实时控制系统、电力营销系统,还有支持企业经营、管理、运营的管理信息系统。各应用系统对数据的实时性、安全性等要求不同。电力系统的一体化设计必须遵从以下原则。

a. 为了保证实时监控系统的安全必须确定实时控制系统的所有连接,去掉不必要连接,巩固和加强网络中任何保留的实时控制系统的连接,排除和取消不必要的服务以加固实时控制系统。

b. 不依赖拥有协议方来保护系统安全。有些SCADA系统使用厂家特有的协议进行通信,显然系统安全就取决于这些协议,这时就不能依赖厂家默认的设置保护系统;另外,还要求厂家告之任何可能威胁系统安全的后门并提供相应保护措施。

c. 由设备和系统的卖方提供执行系统的特性。目前,大多数SCADA系统没有任何安全特性,所以需要卖方以产品补丁或升级的形式提供安全特性,同时要设置这些特性以达到最大的系统安全水平。

d. 通过实现内部和外部的IDS,实现全天24小时突发事件监测。为了能有效地响应网络入侵,需要建立一种入侵探测策略(包括对内部或外部恶意行为作反应的告警网络管理员),入侵探测系统可以通过一个寻呼机建立起来。

e. 引入物理安全审查,评定所有接入系统网络的远方位置评估他们的安全,执行电力监控系统设备和网络,以及任何其他连接的网络的技术审查,确定涉及的安全关系。

f. 全系统所有的系统运行策略设置应该与防火墙、防病毒软件、网络协议安全(IP-sec)、入侵侦测等防护措施的策略互动执行。

结合电力系统中各应用系统的特点和安全等级,在以上设计原则的基础上,主要从设计的系统架构和安全管理的过程和政策上探讨系统的安全防范。

2.2 系统设计

根据电力系统中各种应用的不同特点和安全等级要求,通过安全分组的方法提高系统的安全。按照各系统安全等级的不同进行安全分组,如表1所示。

表1 电力系统安全分组

Tab.1 Security group of power system

安全组	系统功能部分	数据实时性要求	对应生产现场控制区
Ⅰ组	SCADA/PAS/DMS部分	高实时性	面对生产实时控制区
Ⅱ组	TMR部分	准实时性	面对生产非实时控制区
Ⅲ组	DMIS部分	非实时性	面对生产管理区

在安全Ⅰ组与安全Ⅱ组(面对电网运行现场建立数据通信)间设置硬防火墙设备,应该杜绝与电网外部的公共通信链路或者电网内部的公共信息通道链路直接相连接。考虑到MIS系统具有Internet出口,所以安全Ⅲ组与安全Ⅰ组/安全Ⅱ组之间必须设立物理隔离设备。在安全Ⅲ组中的DMIS应该杜绝与电网外部的公共通信链路或者电网内部的公共信息通道链路直接相连接。从网络结构安全的角度考虑,把安全Ⅰ组和Ⅱ组视为一体化系统内部网络,安全Ⅲ组视为外部网络。在内部网络和外部网络同时设置IDS系统,以防范来自系统内部和外部的入侵攻击及病毒。系统整体安全防护配置图见图1。

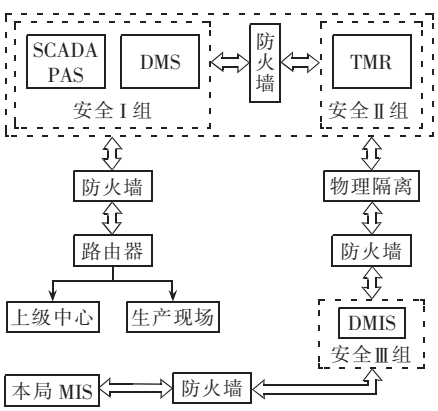

图1 系统整体安全防护配置图

Fig.1 System-wide security protection configuration

2.3 管理上的安全策略

管理上的安全策略主要可从以下方面进行安全策略的管理。

a. 明确定义计算机安全的任务、责任以及管理员、系统管理员、普通用户的职权。通过定义节点权限和操作员权限,对自动化系统内部对象(如开关)的安全级进行定义,可以实现特定人员在特定节点可对特定对象的操作权限管理。对用户权限定义4级:第1级为系统维护员,即对硬件系统、网络、数据库、节点配置的维护;第2级为维护员,即对数据、图形的编辑维护;第3级为操作员,即对SCADA运

行监视控制功能的执行;第 4 级为一般用户,只能查看各种画面,不能进行任何控制操作。

b. 全系统的系统/功能/工具软件、所有人员进入系统的操作等均需要配套注册工具。可采用公钥技术或证书技术实现电力系统的纵向数据交换和操作的安全。

c. 建立基于深度防御理论的网络保护策略。深度防御必须在设计进程中予以考虑,要对与网络有关的任何技术的、决定性的方面进行综合性考虑,利用技术和管理上的控制尽可能地减小对网络各个层面的威胁;另外,每个层面的各个系统之间必须不受影响,例如,为防范内部威胁,要限制用户只访问与他工作有关的必需的那部分资源。

d. 建立有效的配置管理过程。配置管理需要覆盖硬件和软件配置,对硬件或软件的改变可能会引入一些威胁网络安全的因素,这时就要对任何改变进行评价和控制。

e. 建立系统备份和灾难恢复计划。该计划必须对任何紧急情况作出快速恢复,系统备份是任何安全防护体系的重要组成部分,有利于网络的快速重建,所有成员都要熟悉灾难恢复计划并根据实践中的经验教训对其做出合适的调整。

3　结语

本系统安全方案已经应用于江西宜春地区电网自动化系统。由于电力系统中包含了多个应用自动化系统的集成,所以其安全防护体系首先应在系统网络构架上安排合理,生产核心部分按照内部网络考虑安全等级设置,生产管理部分按照外部网络考虑安全等级设置。通过各应用自动化系统的横向有效安全隔离,应用各种网络安全技术切实保障整个电力网络的安全。

参考文献:

[1] 王益明,辛耀中,向　力,等. 调度自动化系统及数据网络的安全防护[J]. 电力系统自动化,2001,24(21):5-8.
WANG Yi-ming,XIN Yao-zhong,XIANG Li,*et al*. Security and protection of dispatching automation systems and digital networks[J]. **Automation of Electric Power Systems**,2001,24(21):5-8.

[2] 李　芳,黄毓瑜. MIS 系统安全登录中加密技术的应用研究[J]. 工程图学学报,2003,(1):37-43.
LI Fang,HUANG YU-yu. Application of encryption technique in security login of MIS system [J]. **Journal of Engineering Graphics**,2003,(1):37-43.

[3] 王怀伯, 李　林, 张申生. CORBA 中的安全机制及实现[J]. 上海交通大学学报,2000,7(34):983-986.
WANG Huai-bo,LI Lin,ZHANG Shen-sheng. Security mechanism in common object request broker architecture (CORBA) and its implementation[J]. **Journal of Shanghai Jiaotong University**,2000,7(34):983-986.

[4] 闵　君,龚晶莹. 入侵检测技术的研究[J]. 计算机应用研究,2002,(2):1-4.
MIN Jun,GONG Jing-ying. Research of technologies about intrusion detection[J]. **Computer Application Research**,2002,(2):1-4.

[5] 戴英侠,连一峰,王　航. 系统安全与入侵检测[M]. 北京:清华大学出版社,2002.

(**责任编辑**: 汪仪珍)

作者简介:

刘静芳(1977-),女,河北井陉人,硕士研究生,从事电力系统自动化的研究(**E-mail**:liujingfang@4y.com.cn);

陈赤培(1954-),男,北京人,教授级高级工程师,长期从事电网自动化系统工程设计和规划 (**E-mail**:chenchipei@vip.sina.com);

樊江涛(1979-),男,江西遂川人,硕士研究生,从事电力系统自动化的研究和开发。

Research of information security and protection architecture in integrative design of power system

LIU Jing-fang[1],CHEN Chi-pei[1,2],FAN Jiang-tao[1]

(1. East China Jiaotong University,Nanchang 330013,China;
2. Jiangxi Electric Power Design Institute,Nanchang 330006,China)

Abstract: Integrative environment construction is the base of automation system for information sharing within the whole power network. However,the information security becomes more important for the secure,stable,economic and superior operation of power system. The integrative power system and its features are introduced. The main contents of the integrative information security are expounded,inchuding secrecy,integrality and effectiveness. The security techniques such as fire wall,virtual network,authentication center and intrusion detection system are introduced. The design principle,system design and security strategy of integrative information security and protection architecture are discussed. The proposed scheme is applied in areal power network automation system with good effect.

Key words: power system; integrative design; information security; security protection