电力监控自动化系统中信息安全防护的设计与应用

刘静芳[1], 陈赤培[1,2], 罗 杰[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: 电力监控自动化系统的发展使得电力网络信息资源高度共享,然而一体化、网络化的发展使信息安全问题也更为突出。依据电力监控自动化系统中各应用系统的特点和安全要求,提出了一种新的信息安全防护系统设计方案,从系统网络架构上对系统进行有效的安全分区,应用各种网络安全技术实现系统横向和纵向的信息安全。最后阐述了该方案在某地区电网自动化系统设计中的整体安全防护的实际应用。

关键词: 电力监控自动化系统; 信息安全; 安全防护

中图分类号: TM764 **文献标识码**: A **文章编号**: 1003-4897(2004)20-0033-03

0 引言

在IT技术的迅速发展支持下,国内外电力企业和技术标准组织普遍提出统一筹划电力监控自动化系统的建设发展规划来实现各配套自动化系统的信息资源和环境共享。然而,电力自动化系统一体化、网络化的发展必然使信息安全问题成为威胁到电力系统的安全、稳定、经济、优质运行的重大问题。防范对网络的攻击侵害及由此引起的事故,建立完善的安全防护体系成为一体化电力监控自动化系统设计中的重要部分。

1 一体化的电力监控自动化系统

电力监控自动化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、电能量计量计费系统等在内的自动化系统总称,具有可靠性、安全性、完整性、及时性及一致性等特点。要保障其信息安全,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以及系统遭受破坏后的快速恢复能力。除了加密、身份认证、访问控制、防火墙、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。当前流行的安全产品很多,如防火墙、VPN、CA以及入侵检测系统(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强度的电力自动化网络中。

2 信息安全防护系统的设计与应用

2.1 设计原则

电力监控自动化系统集成了SCADA、PAS、DMIS、TMR等自动化系统。它们对数据的实时性、安全性等要求不同,电网运行实时控制系统是电力二次系统安全保护的重点和核心。电力监控自动化系统的设计原则: ①必须确定实时控制系统的所有连接,去掉其不必要连接,巩固和加强网络中任何保留的实时控制系统的连接; ②不依赖拥有协议方来保护系统安全; ③由设备和系统的卖方提供执行系统的特征; ④通过实现内部和外部的IDS实现全天突发事件监测; ⑤引入物理安全审查,评定所有接入系统网络的远方位置,确定涉及的安全关系; ⑥全系统应该与防火墙、防病毒软件、IP-sec、入侵侦测等防护措施的策略互动执行。

Economic operation analysis of special modes about three sets of three-winding transformers

LIN Li[1], HU Jing-sheng[2]

(1. North China Electric Power University, Beijing 102206, China;
2. Transformer Economic Operation Institute of Shenyang, Shenyang 110000, China)

Abstract: There are six loads in mid-voltage and low-voltage sides of three sets of splitting three-winding transformers, whose loads can be regulated mutually. So totaled 289 kinds of operation modes are presented, such as load adjusting, splitting, parallel and different sets combination etc, among the three transformers. The economic operation of the 289 kinds of modes are analyzed and accounted. The economic effects on energy consumption are demonstrated with examples.

Key words: three-winding transformers; operation mode; splitting operation; parallel operation; economic operation

© 1994-2007 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2.2 系统架构

所有应用系统的安全可靠运行首先必须建立在安全可靠的网络系统基础之上。电力控制系统必须与办公自动化系统实行有效安全隔离;控制系统所用网络必须与公共信息网络及因特网等实行有效安全隔离。

调度 SCADA/ PAS 系统、配电 DMS 系统主要服务于电网运行生产的实时监视控制和调度,对数据有很高的实时性要求和安全性要求。电能量计量 TMR 系统,电力市场交易系统等是面向生产和交易业务的准实时性系统。DMIS 系统是基于 SCADA/ PAS、DMS、TMR 自动化系统采集的电网实时数据开展的电网运行调度管理而建设的,主要是服务于电网调度生产管理/ 办公。按照各系统安全等级的不同进行安全分区,如表 1 所示。

根据各区的特点和安全要求不同在各区之间设置不同的防范措施:

1) 在安全 I区与安全 II区之间通过逻辑隔离,设置硬防火墙设备。安全 I区/ 安全 II区主要是面对电网运行现场建立数据通信。安全 I区/ 安全 II区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。

表 1 电力监控系统安全分区

Tab. 1 Safety divisions of power supervision and control automatic system

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

2) 安全 III区与安全 I区/ 安全 II区之间,由于通过 DMIS 部分与本局 MIS 系统互连向企业管理部门提供电网生产数据,考虑到 MIS 系统具有 Internet 出口,所以安全 III区与安全 I区/ 安全 II区之间必须设立物理隔离设备。在安全 III区中的 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。

3) 从网络结构安全的角度考虑,把安全 I区和 II区视为电力监控自动化系统内部网络,把安全 III区视为电力监控自动化系统外部网络。在电力监控自动化系统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。IDS 按照时间策略设置运行。IDS 设置点可以分别考虑数据库、网络和桌面。全系统整体安全防护措施配置图请见图 1。

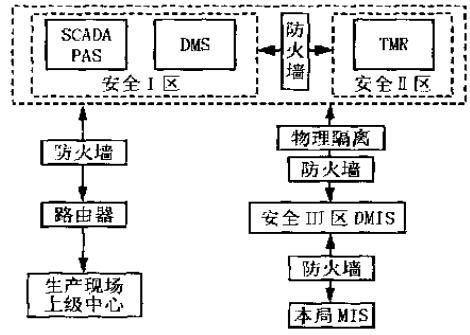

图 1 全系统安全防护措施整体部署图

Fig. 1 Holistic configuration of the whole system's safety protection measures

2.3 管理上的安全策略

网络入侵不仅来自于网络外部,也来自于网络内部,并且大多数的安全缺口来自于内部。在系统网络安全设计的同时,也要考虑从多方面加强安全管理,如: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,实现特定人员在特定节点可对特定对象的操作权限管理;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配套注册工具,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等等。

2.4 方案应用

以下描述某个地区电网自动化系统设计中的系统整体安全防护方案的实际应用。

1) 横向安全

①安全 I 区与安全 II 区

安全 I 区与安全 II 区之间设置明显可断开点,设有网络防火墙。

在安全 I 区内设有区内交换机,该区内各自动化系统均可接入该交换机与安全 II 区通信。

在安全 II 区内设有区内交换机,该区内各自动化系统均可接入该交换机与安全 I 区和与安全 III 区通信。

同样在安全 III区内设有区内交换机,该区内各自动化系统均可接入该交换机与安全 I 区/ 安全 II 区通信。

在各个安全区内所设置的区内交换机一方面是为了汇接区内各个自动化系统,构成一个网段。另一方面也是设置的一个可操作的断开点,并且该操作不会影响到系统的整体运行。

②安全 I 区/ II 区与安全 III 区

安全 I 区/ II 区与安全 III 区之间设置明显可断开点,并采用网络物理隔离装置。由安全 I 区/ II 区

© 1994-2007 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

向安全Ⅲ区启动连接的为正方向,由安全Ⅲ区向安全Ⅰ区/Ⅱ区启动连接的为反方向。

自动化系统主站内部的横向安全防护应用配置请参见图2。

2) 纵向安全

①调度中心安全Ⅰ区和安全Ⅱ区分别与厂站端对应的二次系统自动化设备的通信均设置认证加密装置。并且考虑配置两侧对称认证加密装置。

②在厂站端的二次系统设备装置的远方拨号服务通信均设置拨号认证装置。

自动化系统纵向安全防护应用配置请参见图3。

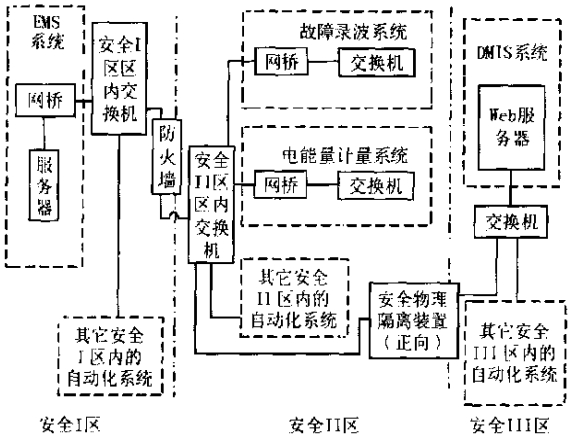

图2　横向安全防护应用配置

Fig. 2　Transverse application scheme of safety protection

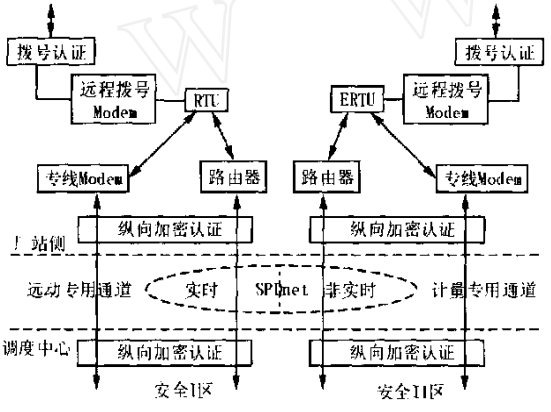

图3　纵向安全防护应用配置

Fig. 3　Longitudinal application scheme of safety protection

3　结语

由于电力监控自动化系统中包含了多个应用自动化系统的集成,所以电力监控自动化系统的安全防护,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(WANG Yi-ming, XIN Yao-zhong, XIANG Li, et al). 调度自动化系统及数据网络的安全防护(Security and Protection of Dispatching Automation Systems and Digital Networks)[J]. 电力系统自动化(Automation of Electric Power Systems),2001,25(21):5-8.

[2]　戴英侠,连一峰,王航(DAI Ying-xia, LIAN Yi-feng, WANG Hang). 系统安全与入侵检测(System Security and Intrusion Detection)[M]. 北京:清华大学出版社(Beijing: Tsinghua University Press),2002.

收稿日期:　2004-02-19;　　**修回日期**:　2004-06-07

作者简介:

刘静芳(1977-),女,硕士研究生,从事电力自动化系统的研究; E-mail: liujingfang@4y.com.cn

陈赤培(1954-),男,高级工程师,兼职教授,长期从事电网自动化系统工程设计和规划;

罗　杰(1978-),男,硕士研究生,从事电力自动化系统的研究和开发。

Design and application of information's security and protection in power supervision and control automatic system

LIU Jing-fang[1], CHEN Chi-pei[1,2], LUO Jie[1]

(1. School of Electrical and Electronic Engineering, East China Jiaotong University, Nanchang 330013, China;
2. Jiangxi Electric Power Design Institute, Nanchang 330006, China)

Abstract: Power supervision and control automatic system makes information resources in power network highly shared. And yet the integration and network raise higher demands on information security. According to those application system's characteristics and security demands, this paper gives a new design scheme which divides the system into several effective safty sections from the network configuration, and realizes transverse and longitudinal information security by using many techniques on network security. Finally, a practical application of this scheme in some power network automatic system is given.

Key words: power supervision and control automatic system; information security; security protection

© 1994-2007 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net