

调度自动化系统及数据网络的安全防护

王益民, 辛耀中, 向 力, 卢长燕, 邹国辉, 彭清卿

(国家电力调度通信中心, 北京 100761)

摘要: 分析了调度自动化系统的不同应用对安全性、可靠性、实时性、保密性的不同特殊要求。提出了建立调度自动化系统的安全防护体系, 在技术体制方面, 应该在通道层建立调度专用数据网络; 在防护措施方面, 应该采取必要的技术手段, 并建立严格的安全管理规章制度, 以确保调度自动化系统的安全。

关键词: 调度自动化系统; 数据网络; 安全防护

中图分类号: TM 734; TP 393

0 引言

目前数据网络在电力系统中的应用日益广泛, 已经成为不可或缺的基础设施。国家电力数据网一级网从 1992 年 2 月一期工程开始规划建设, 到 1997 年 7 月二期工程开通运行, 迄今已有近 10 年的发展历史。目前国家电力数据网同时承载着实时、准实时控制业务及管理信息业务, 虽然网络利用率较高, 但安全级别较低、实时性要求较低的业务与安全级别较高、实时性要求较高的业务在一起混用, 级别较低的业务严重影响级别较高的业务, 存在较多的安全隐患。随着信息与网络技术的发展, 计算机违法犯罪行为在不断增加^[1], 信息安全问题已经引起了政府部门和企业的高度重视。因此, 根据调度自动化系统中各种应用的不同特点, 优化电力调度数据网, 建立调度系统的安全防护体系, 具有十分重要的意义。

1 电力系统中各类网络应用的特点

电力系统中网络应用的分类方法有许多种, 根据业务类型、实时等级、安全等级等因素, 电力系统的网络应用主要可分为生产数据传输和管理信息传输两大类。另外, 其他的应用还包括话音视频传输和对外服务等。不同的应用系统对安全有不同的要求, 如图 1 所示。

生产控制类中的基于 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; 与计费相关的电力市场业务^[2]对安全性有特殊要求, 不仅要求可靠, 原始数据还要求保密。从应

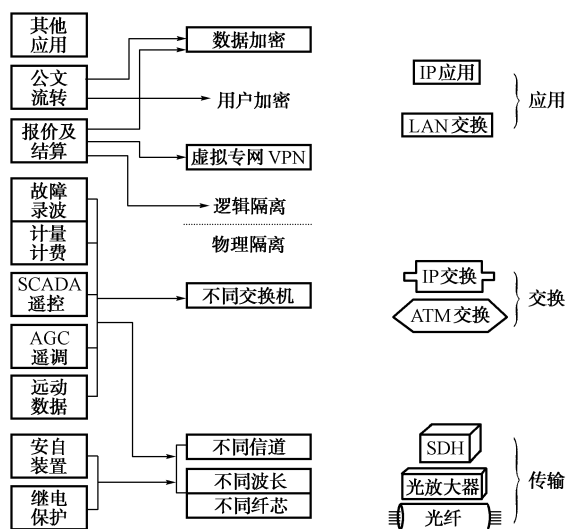


图 1 基于数据网络的应用系统对安全性的要求
Fig. 1 Security required by applications based on digital network

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。

管理信息类业务突发性很强, 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。

话音视频类业务是指建立在 IP 平台上的电话及会议电视, 对实时性要求较高, 安全可靠无特殊要求, 目前其质量还有待提高。对外服务类业务是指根据市场的需要而建立的数据网络。

2 调度自动化系统的安全防护

2.1 制定调度自动化系统安全防护策略的重要性

近年来调度自动化系统的内涵有了较广的延伸, 由原来单一的 EMS 扩展为 EMS, DMS, TMS,

以及厂站自动化、水调自动化、雷电监视、故障录波远传、功角遥测、电力市场技术支持和调度生产管理等系统。数据网络是支持调度自动化系统的重要技术平台,一般要求数据网络安全可靠,实时性要求在秒级,其中发电报价、市场信息发布等电力市场信息系统由于需要与公网连接,因而还要求做加密及隔离处理。

建立调度自动化系统的安全防护体系,首先要制定安全防护策略^[3]。应用系统的安全策略位于安全防范的最高一级,是决定系统的安全要素。从大的方面讲,安全策略决定了一个系统要达到的安全级别及可以付出的代价;从小的方面讲,安全策略的具体规则用于说明哪些行为是允许的,哪些行为是禁止的。系统是否安全,很大程度上依赖于最初设计时制定的安全策略,因为今后的安全措施都围绕这一策略来选择和使用,如果在安全策略上出了问题,将会给今后的应用系统带来安全隐患,从而使将来的安全建设处于十分被动的局面。因此,考虑调度自动化系统的安全,应首先根据系统对安全性、可靠性、实时性、保密性等方面不同的特殊要求,按照国家有关部门的规定^[4],从应用系统的各个层面出发,制定完善的安全防护策略。

2.2 信息系统的安全分层理论

一个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。调度自动化系统的安全防护体系应包含上述 5 个层面的所有内容。

物理安全主要包含主机硬件和物理线路的安全问题,如自然灾害、硬件故障、盗用、偷窃等,以及由此类隐患而导致的重要数据、口令及账号的丢失。

网络安全是指网络层面的安全,即联网计算机可能被网上任何一台主机攻击,而网络安全措施不到位而导致的安全问题。

系统安全是指主机操作系统层面的安全,包括系统存取授权设置、账号口令设置、安全管理设置等安全问题,如未授权存取、越权使用、泄密、用户拒绝系统管理、损害系统完整性等。

应用安全是指主机系统上应用软件层面的安全,如 Web 服务器、Proxy 服务器、数据库等的安全问题。

人员管理是指如何防止内部人员对网络和系统的攻击及误用等。

2.3 国家对网络及信息安全问题的有关政策和法规

国家有关部门对安全问题的有关政策和法规,对制定电力调度控制系统的安全策略起到了指导性

的作用。

公安部是党政机关、企事业单位安全及公共安全的主管部门,已经颁布了安全防护方面的一系列文件,正在制定安全保密和保护的等级,规定各部门应根据具体情况决定自己的安全等级,实行国家强制标准。公安部规定,从安全保密角度看,政府办公网应与外部因特网物理隔离,并认为自动控制系统应与外部网络绝对物理隔离,可根据业务的需要建立专用数据网络。

国家保密局是党政机关、企事业单位保密方面的主管部门,1998 年以来颁布了一系列安全保密方面的文件。规定:涉及国家机密的通信、办公自动化和计算机信息系统的建设,必须与保密设施的建设同步进行,系统集成方案和信息保密方案不可混淆,应从整体考虑;涉及国家机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他公共信息网络相连接,必须实行物理隔离。

电力生产事关国计民生,电力系统的安全和保密都很重要,电力自动化系统要求可靠、安全、实时,而电力信息系统要求完整、保密。两种业务应该隔离,特别是电力调度控制业务是电力系统的命脉,一定要与其他业务有效、安全地隔离。

2.4 调度自动化系统数据网络的安全防护策略

2.4.1 数据网络的技术体制

规划数据网络技术体制和电力系统安全防护体系,应根据电力生产业务对数据网络安全性、可靠性、实时性方面的特殊要求,并遵照国家对涉密单位和重要设施在网络安全方面的有关规定。首先应根据网络的规模、目的、服务对象、实时程度、安全级别等综合考虑,确定最基本的网络技术体制^[5]。

从应用和连接方式来看,企业内部网络有两类,一类是与公网完全隔离、在链路层上建立的企业内部网络,一般称为专用网络;另一类是连接于公网、并利用公网作为通道的企业内部网。第 1 类网络除了面临来自物理层面的安全问题外,主要面临内部的计算机犯罪问题,如违规或越权使用某些业务、查看修改机密文件或数据库等,以及从内部发起的对计算机系统或网络的恶意攻击;第 2 类网络除了具有上述安全问题外,还要承受来自公网的攻击和威胁,由于公网上黑客、病毒盛行,网络安全的攻击与反攻击比较集中地体现在公网上。

由于电力调度数据网的服务对象、网络规模相对固定,并且主要满足自动化系统对安全性、可靠性、实时性的特殊需求,为调度自动化系统提供端到端的服务,符合建设专网的所有特征,所以电力调度数据网宜在通道层面上建立专网,以实现该网与其

他网的有效、安全隔离。

目前国家电力数据网同时承载着调度控制业务和管理信息业务,应当在将来通道资源允许的条件下,将现有电力调度数据网上的信息业务逐步分离出去,改造成为实时控制业务专用的数据网络。

电力系统中的光纤通信网络正在加紧建设,采用光纤+SDH+IP 模式容易实现对不同 IP 应用业务之间的物理隔离,具有较高的传输效率,能满足控制、保护等电力系统关键业务的要求,便于调度部门对网络进行有效监控,并有利于通信部门对外出租带宽。因此,用光纤+SDH+IP 模式建立调度数据专网是一个适当的选择,可以很好地满足电力系统的下列要求:

- a. 数据传输的实时性(继电保护毫秒级,自动化秒级),要求网络层次简化;
- b. 传输的连续性,通信负荷基本恒定,需要恒定带宽;
- c. 远方控制的可靠性(遥控、遥调、AGC 等),要求有效隔离;
- d. 因特网时代的安全防护体系(防黑客、防病毒、防破坏等);
- e. 网络拓扑结构必须覆盖远离城市的电厂、变电站;
- f. 充分利用 SPDnet 的现有设备,节约大量资金,便于平滑过渡。

2.4.2 调度专用数据网络的安全防护措施

调度专用数据网除了传送 EMS 数据外,还要传送电能量计量计费、水调自动化、电力市场信息和调度生产信息(工作票和操作票、发电计划和交易计划、负荷预报、调度报表、运行考核等)。应根据各类应用的不同特点,采用不同的安全防护措施,如 EMS 等实时控制业务具有较高的优先级,应该优先保证,生产信息的优先级次之,而电力市场信息须进行加密处理等。

采用调度专用网络体制使数据网络在网络层的安全得到最大程度的保证,但也不能保证百分之百的安全,对调度数据专用网络还必须做到技术措施和管理制度双管齐下,才有可能从根本上保障信息和控制系统的安全。在管理制度方面,要做到:

- a. 对全网实施监管,所有与电力调度数据网连接的节点都必须在有效的管理范围内,保障安全的系统性和全局性。
- b. 加强人员管理,建立一支高素质的网络管理队伍,防止来自内部的攻击、越权、误用及泄密。
- c. 加强运行管理,建立、健全运行管理及安全规章制度,建立安全联防制度,将网络及系统安全作

为经常性的工作。

- d. 聘请网络安全顾问,跟踪网络安全技术。

在技术措施方面^[6],要做到:

a. 在网络传输层,既要保证数据网络的安全,又能向外传输必要的信息,必须坚持调度控制系统与调度生产系统之间、调度生产管理系统与企业办公自动化系统(OA/MIS)之间有效、安全地隔离,它们之间的信息传输只能采用单向传输的方式。常采用的措施包括防火墙、专用网关(单向门)、网段选择器等进行有效隔离。另外在调度数据专用网络的广域网和局域网上,根据不同的业务系统,还可采取以下技术手段:①网络安全访问控制技术。通过对特定网段和服务建立访问控制体系,可以将绝大多数攻击阻止在到达攻击目标之前。可实施的安全措施有:防火墙、VPN 设备、VLAN 划分、访问控制列表、用户授权管理、TCP 同步攻击拦截、路由欺骗防范、实时入侵检测技术等。②加密通信技术。该措施主要用于防止重要或敏感信息被泄密或篡改。该项技术的核心是加密算法,其加密方法主要有:对称型加密、不对称型加密、不可逆加密等。③身份认证技术。该项技术广泛用于广域网、局域网、拨号网络等网络结构。用于网络设备和远程用户的身份认证,防止非授权使用网络资源。④备份和恢复技术。对于网络关键资源如路由器、交换机等做到双机备份,以便出现故障时能及时恢复。

b. 在系统和应用层面,包括计算机防病毒技术、采用安全的操作系统(达 B2 级)、应用系统的关键软硬件及关键数据的热备份和冷备份等。防病毒技术和备份措施是通常采用的传统安全技术,而安全的操作系统是一个新的发展趋势。

3 结语

电力调度数据网络是调度自动化系统的支撑平台,网络安全是系统安全的保障,专用数据网络是整体安全防护体系的基础,专网的特点体现在网络互联、网络边界、网络用户的可管性和可控性。目前,国际上正在制定相应的自动化系统网络安全标准,国内也开始进行相关课题的研究。对于调度自动化系统及数据网络的安全防护措施,首先应在网络技术体制方面,采用光纤+SDH+IP 的数据专网模式,在全系统实现电力调度专用数据网络与其他公用信息网络、电力生产控制系统与办公自动化系统等的安全隔离,同时在调度专用数据网及各相关应用系统上采取必要的安全防护技术手段,建立严密的安全管理措施,以确保电力调度系统和电力系统的安全。

参考文献

- 1 余建斌(Yu Jianbin). 黑客的攻击手段及用户对策 (Hacker's Attack Measures and User's Countermeasures). 北京:人民邮电出版社(Beijing: People's Posts and Telecommunications Publishing House), 1998
- 2 赵遵廉(Zhao Zunlian). 电力市场运营系统(Electricity Market Operation System), 北京:中国电力出版社(Beijing: China Electric Power Press), 2001
- 3 Othmar Kyas. 网络安全技术——风险分析、策略与防火墙 (Network Security Technology: Risk Analysis, Strategy and Firewall). 王 霞, 铁满霞, 陈希南, 等译 (Wang Xia, Tie Manxia, Chen Xinan, et al, Trans). 北京: 中国水利水电出版社 (Beijing: Hydraulic Power Publishing Company), 1998
- 4 计算机信息系统安全法规汇编 (Laws and Rules on Security of Computer Information System). 中国电力信息中心 (China Electric Information Center), 2000
- 5 辛耀中, 卢长燕 (Xin Yaozhong, Lu Changyan). 电力系统数据网络技术体制分析 (Analysis of Data Network Technology Architecture for Power Systems). 电力系统自动化 (Automation of Electric Power Systems), 2000, 24(21): 1~6
- 6 肖 康 (Xiao Kang). 建立和完善企业 IP 网络安全体系 (Establish and Perfect Enterprise's IP Network Security System). 计算机世界—网络与通信 (China Computerworld Network and Telecommunication), 2000, 10(39): 31~32

王益民, 男, 高级工程师, 副主任, 长期从事通信、电网调度自动化等领域的研究及管理工作。

辛耀中, 男, 教授级高级工程师, 总工程师, 从事电力系统调度自动化建设与管理工作。

向 力, 男, 教授级高级工程师, 处长, 从事电网调度自动化运行和管理工作的。

SECURITY AND PROTECTION OF DISPATCHING AUTOMATION SYSTEMS AND DIGITAL NETWORKS

Wang Yimin, Xin Yaozhong, Xiang Li, Lu Changyan, Zou Guohui, Peng Qingqing
(National Electric Power Dispatching & Communication Center, Beijing 100761, China)

Abstract: Special requirements of security, reliability, real-time and privacy for dispatching automation system's different application are analyzed. In this paper, security protection system is raised to set up to assure the safety of dispatching automation system, which includes two aspects: (I) dispatching dedicated network should be constructed directly on physical link circuit at the aspect of network technology architecture. (II) Necessary technological measures should be taken via practical means and strict network security management rules should be laid down.

Keywords: dispatching automation system; digital network; security protection