Universe Scientific Publishing
Hydropower and Water Resources 水电水利
第 2 卷◆第 12 期◆版本 1.0◆2018 年 12 月
文章类型：论文|刊号（ISSN）：2529-7821

电网调度自动化系统主要安全防护技术

王平荔　钟志萍　向恺
国网江西省电力有限公司萍乡供电分公司
DOI:10.32629/hwr.v2i12.1757

[摘　要] 伴随着我国电力行业电网调度自动化系统的不断发展和提升,数据控制的多样性和混杂性日趋复杂,这样在很大程度上要求我国电网调度自动化系统进行持续的发展。在电网调度自动化系统运行的过程中,有效的保障电网调度自动化系统的安全运行就在很大程度上稳定了我国电力系统的正常运行,保障了我国电力系统的发展,因此电力系统中的电网调度自动化系统安全防护工作需要给予足够的重视和关注。
[关键词] 电网调度自动化系统；安全防护；技术；措施

在电网调度自动化系统的发展下,计算机网络技术成为确保电力系统稳定运行的重要技术。为了能够更好的发挥出电网调度自动化系统运行发展,需要相关人员加快打造电网调度自动化信息系统平台,在平台上获取重要信息资源,实现对各类资源的合理利用,加强各个局域网的连接,不断优化调度数据网。为了实现这一目标,保证电网稳定运行,文章就电网调度自动化系统主要安全防护技术问题展开探究。

1 电网调度自动化系统运行存在的问题

1.1 设备管理问题。

现阶段,电网调度自动化网络通讯设备管理存在一些问题,而这些问题出现的主要原因是电网调度工作人员对角色分工不明确,在工作中没有做好自己的本职工作,在操作中忽视了对设备的管理,无法保证电网调度自动化网络通信系统的安全。

1.2 安全管理问题。

能量管理系统、电力应用软件、调度防误操作是电网调度自动化网络通信系统的重要组成,在实际应用中,电网调度自动化网络通信需要借助这三个系统来构建,但是从实际发展情况来看,电网调度自动化通信操作过程中没有有效协调各个系统的配合,在无形中降低了电网调度自动化网络通信系统的应用安全。

2 电网调度自动化系统业务和特点

电网调度自动化系统也被人们称作是能量管理系统,在实际工作操作中主要是对各类数据信息的采集、监控,为了完成这项工作,相关人员借助电网调度自动化系统进一步加强了供电站、配电系统、电力用户、电力企业之间的关联。电网调度自动化系统大体可以分为两类,一类是生产数据传输系统,另外一个是管理信息传输系统。在实际应用中,电网系统中的生产控制类业务对数据信息的传输率要求不高,无法保证数据信息的安全、稳定。另外,对于电网调度自动化管理系统来讲,在应用的时候面临较多的突发性问题,由此对电网调度自动化系统信息处理速率提出了更高的要求。

3 我国电力行业中电网调度自动化系统在运行过程中存在的主要安全风险

电网企业、发电企业内部的电网调度自动化系统,原则上划分为生产控制大区（安全Ⅰ区、安全Ⅱ区）和管理信息大区（安全Ⅲ区、安全Ⅳ区）,不同的安全区之间以及处于不同层级的相同安全区之间会存在不同规模和速率的数据交互。例如,在地区调度电网调度自动化系统中,地级调度同省级调度、县级调度、地区所辖变电站、发电企业及用户等电力控制、生产、传输及分配的区域都存在着相互之间的数据传输。又如,电力调度实时监视与控制子系统的服务器所处的安全Ⅰ区与 WEB 子系统服务器所处的安全Ⅲ区之间也会存在不同方向的数据传送。这种在不同安全区之间,以及不同层级的相同安全区之间的数据交互机制,不仅能够最大限度地提升电力系统运行中的监管和控制的效果,也很大程度上为电力公司中各个运行部门和职能科室的日常工作提供了便捷的数据服务。与此同时,需要特别注意的是,不同的安全等级以及不同的安全分区之间的运行系统的相互连接意味着对电力调度数据网络的跨区域应用,这导致接触到电力运行专业系统的非专业人员越来越多,给电网调度自动化系统的安全带来巨大隐患。网络黑客的恶意攻击、网络恶意代码的侵犯等都严重危害我国电力行业的电网调度自动化系统的安全运行。

4 我国电力行业中电网调度自动化系统在安全防护技术中的常见措施

4.1 电网调度自动化系统安全防护技术中的网络设备安全配置

不使用默认路由,网络边界路由器关闭 OSPF 路由功能,采用安全增强的 SNMPv2 及以上版本的网管协议,记录设备日志,设置 8 位以上符合复杂度要求的密码并定期进行修改,对访问控制列表进行配置,封闭空闲的网络端口等。

4.2 电网调度自动化系统安全防护技术中的横向隔离安全技术

正向横向安全隔离装置用于生产控制大区到管理信息大区的单向数据传送,实现两个安全分区之间的非网络方式的数据传输,比如地调调度生产管理功能在管理信息大区部署网关机,该功能模块与生产控制大区的数据通信必须采用

Copyright © This word is licensed under a Commons Attibution-Non Commercial 4.0 International License.

专用横向单向安全隔离装置实现强隔离。通过正向横向单向隔离装置从生产控制大区向生产控制大区传输实时数据和交易信息等,通过反向横向单向隔离装置从管理信息大区向生产控制大区传输计划数据和气象信息等。

4.3 电网调度自动化系统安全防护技术中的安全备份及恢复技术

在电网调度自动化系统的安全防护技术中的备份及恢复技术就是要对系统中的关键运行数据进行定期的备份,这样才能够有效的保障在运行数据丢失或者是电力运行系统崩溃情况出现的情况下,有效并且准确快速的进行相关运行关键数据的恢复,最大限度的保障电力系统的有效运行及可用。备份及恢复技术能够有效的处理和规划电力系统关键运行服务器以及电力网络设备,电力运行电源关键模块部件,并且能够有效的规避由于系统运行过程中单点运行故障导致的电力系统的瘫痪。例如电力调度系统能够对数据服务器进行冗余相关配置,让数据服务器达到相关的技术要求以及安全标准要求。

4.4 电网调度自动化系统安全防护技术中的纵向加密保护技术

该技术主要通过使用纵向加密认证装置实现。它为本地生产控制大区提供一个网络防护,具有类似包过滤防火墙的功能。为生产控制大区各不同层级系统之间的通信提供认证和加密功能,实现各层级系统之间数据传输的保密性和完整性。

4.5 电网调度自动化系统安全防护技术中的防火墙技术

在电网调度自动化系统安全防护技术中的防火墙技术主要就是要控制访问的数据流量,只有达到防火墙的安全设置数据才能够有效的通过防火墙进行电力系统的访问,一旦出现不符合防火墙设置数据的访问就会遭到防火墙的控制和拒绝。同时利用防火墙进行电网调度自动化系统的安全防护不仅仅能够有效的关闭系统中不使用的网络端口,同时还能够有效的禁止外部对于特定网络端口的访问或者信息数据流出。在防火墙安全防护技术应用的过程中,最主要的技术有两种,首先是过滤防护技术,其次是代理服务应用技术。

4.6 电网调度自动化系统安全防护技术中的防恶意代码技术

在电网调度自动化系统的安全防护技术中的防恶意代码技术最主要的原理在于有效的部署恶意代码防御系统。在这一安全防护技术运行的过程中,防恶意代码系统要有效的覆盖在电力系统的每一个维护工作站以及应用服务器。需要注意的是在生产控制大区进行恶意代码防御系统的统一部署,在管理信息大区中进行恶意代码防御系统的统一部署。在系统运行过程中,要对恶意代码防御系统的恶意代码特征库进行定期的维护和升级,同时要针对应用服务器和维护工作站设置进行网络恶意代码的定期查找清除。需要重点注意的是升级恶意代码防御系统特征库的过程中严禁与外部网络进行连接。

4.7 电网调度自动化系统安全防护技术中的入侵检测技术

入侵检测安全防护技术主要的应用原理是对威胁电力系统网络安全的隐患进行主动的检查和排查。在部署入侵检查系统的过程中,我们能够有效的对计算机系统的关键数据以及关键点进行集中收集和检测,然后通过科学的分析和检测有效的分析出网络黑客的攻击手段以及入侵方法,能够对网络数据通信的安全性以及正常性进行检测,能够对电力系统出现的安全漏洞进行排查和修补。

4.8 电网调度自动化系统安全防护技术中的安全拨号技术

安全拨号技术主要就是通过在电力系统运行过程中部署相关的安全拨号装置来对拨号操作进行科学认证,以实现有效的安全拨号。安全拨号技术的组成分为两个部分,首先是安全拨号客户端,其次是服务端。拨号客户端用于进行网络内部数据的身份验证,验证通过之后采用专业的安全拨号运行软件同拨号服务端进行数据拨号的认证和交换。一般情况下,电网调度自动化系统安全运行的过程中会部署相关的加密卡,以保障系统安全。

5 结束语

综上所述,电网调度自动化系统是电力企业发展获取信息的重要关键,也是影响电力系统能否稳定运行的重要因素。为此,需要相关人员从技术措施和安全管理两个方面不断完善电网调度自动化系统,从而进一步提升电网调度自动化系统应用成效,促进电力事业发展。

[参考文献]

[1]曹茂,高伏英.电网调度自动化主站运行[M].北京：中国电力出版社,2011,(02):36.

[2]丁晓成.电网调度自动化系统主要安全防护技术阐析[J].中国新通信,2018,20(07):71.

[3]蒋业婷.电网调度自动化系统主要安全防护技术阐析[J].科技创新与应用,2017,(34):63.

[4]远方.电网调度自动化系统数据安全及安全防护体系设计[D].郑州大学,2010:35.

Copyright © This word is licensed under a Commons Attibution-Non Commercial 4.0 International License.