文章类型：论文|刊号（ISSN）：2529-7821 /（中图刊号）：868GL002

电力监控系统网络安全应用实践——基于网络安全管理平台

谢娟
新疆维吾尔自治区乌鲁瓦提水利枢纽管理局
DOI:10.12238/hwr.v5i11.4057

[摘　要] 在时代不断进步的过程中我国电力事业发展更加突飞猛进,而现阶段电力的网络系统应用越来越成熟,但同时人们对其安全运行也提出更高的要求。结合网络安全管理平台建设及日常监控中的应用,分别从功能介绍、典型设备接入以及网络安全技术应用三个方面开展研究,着力解决电力监控系统网络空间有序,规范业务访问流量,为地区电力监控系统安全稳定运行提供了可靠技术保障。
[关键词] 电力监控系统；网络安全；网络安全管理平台
中图分类号：TN915.08　文献标识码：A

Application Practice of Network Security in Electric Power Monitoring System —— Based on Network Security Management Platform

Juan Xie
Uluwati Water Conservancy Control Project Management Bureau, Xinjiang Uygur Autonomous Region
[Abstract] In the process of continuous progress of the times, the development of my country's electric power industry is advancing by leaps and bounds. At this stage, the application of electric power network systems is becoming more and more mature, but at the same time, people also put forward higher requirements for its safe operation. Combined with the construction of network security management platform and its application in daily monitoring, the research is carried out from three aspects: function introduction, typical equipment access and network security technology application. Efforts will be made to solve the problem of orderly network space of electric power monitoring system, standardize business access flow, and provide reliable technical guarantee for safe and stable operation of regional electric power monitoring system.
[Key words] power monitoring system; network security; network security management platform

引言

电力和铁路、民航、银行等一起被列为我国的主要系统,电力监控系统每种业务的组织,全方位提升电力系统的安全性、稳定性、生产效率和服务质量。电力监控系统的安全运行与社会的稳定、发展和人民的生活有关,电力系统的网络安全是电力调度业务自动化与信息化的主要保证,和电力生产有紧密关系。网络安全即网络系统的硬件、软件和系统中数据受到保护,防止被损坏,网络安全最重要的是信息安全,和信息的保密性、完整性可控性有关。

1 概述

电力监控系统是指用于监视和控制电力生产及供应过程、基于计算机及网络技术的业务系统及智能设备,以及作为基础支撑的通信及数据网络。木桶理论决定了整体安全防护水平是由系统中最薄弱环节的水准决定的。对电力监控进行体系化的安全保护十分必要,为了防止黑客利用噪声系统漏洞和对企业系统后门的恶意入侵,并防止使用计算机病毒或恶意代码实施的破坏和攻击,从而导致电力监控系统被劫持或沦陷,造成对电力系统生产安全运行的危害。我国电力监控系统安全防护在十数载不断地强化完善过程中,已经实现了从静态布防到动态管控的转变。电力监控系统从安全防护技术,应急备用措施和全面安全管理三个方面构建了三维立体的安全防护体系。

2 电力监控系统网络安全防护的原则

在电力控制系统安全防护活动开展过程中,要结合国家信息安全等级保护制度,高效落实相应的安全防护工作。通过加强黑客、恶意代码等对电力监控系统所造成的攻击侵害的防范,避免引发电力系统事故,要坚持相应的工作原则,保障相应工作能够高效落实到位,保障通信高效有序的开展。因而在发电场电力监控系统安全防护工作开展过程中,首先要结合计算机和网络技术的业务系统,完成生产控制大区和管理信息大区的划分,将相应的工作进行有效划分,进而明确相应的职责,做好安全分区等相应工作,使得网络安全防护工作能够更

加高效稳定的开展。在生产大区的划分过程中,还可以根据其实际需要划分为控制区和非控制区等不同的区域。在管理信息大区的划分过程中,要充分满足安全防护的总体原则,根据业务系统的实际情况,简化安全区的设置工作,避免形成不同安全区纵横交叉连接的现象。通过采用网络专用的形式,有效提高信息传输的安全性和稳定性。而通过实现不同强度的横向安全隔离,在提高数据信息处理能力的同时,为发电的生产管理提供有效决策,全面加强管理信息,调度生产管理等相关工作。在纵向上加强安全认证,有效提高整体的工作质量和水平。

3 优化电力监控系统网络安全防护技术

3.1加强外设管理

发电、供电公司在电力监控系统的日常管理活动中,应当努力强化网络安全防护方面的管控力度,面向安全区域中所涵盖的所有外部设施设备,特别是对于那些需要连接生产控制区的设施而言,一定要完全满足我国有关设施投入生产使用的相关规定和要求,并且还要求具备质监部门签署的质量认证书,全方位的满足防护工作的安全需求,严谨使用任何未经质量认证抑或是具有安全风险的外部设施。此外,在监控系统的网络之中,对于那些非安全区域所连接的子系统而言,是不可以同外部网络加以连接的,每个主机上配置的USB软盘与光盘驱动接口都要按照要求及时断开,一旦发生违章问题则需要立刻告知电力监控部门来予以调整处理。

3.2安全数据资源化及建模分析

在对内外部数据源进行统一采集、初筛和存储的基础上,通过流式数据的实时分析和历史数据的离线分析相结合的方式,将数量庞大、类型多样、独立价值低的数据(包括II型监测装置、Agent类信息、安防设备信息、网络设备信息、数据库、业务应用类信息等)进行模型化、范式化处理,形成可被逐级分析利用的数据资源。将上述资源化数据进行整合,根据电力监控系统实际安全防护需求,通过运用关联分析、多阶段组合关联分析、攻击场景关联分析等,进行静态设备模型、动态运行模型、风险分析模型、网络异常检测模型、安全审计模型、自动化应急处置等建模,形成全局式的网络安全态势分析。

3.3延长安全监控范围,拓展多单位合作制度

从开始部分实施准确监督,单位迅速反应完全运用分配自动的网络安全管控平台针对每个站网络安全管理设备中的网络安全事情和远程体系异常信息进完成准确的监管,让调度自动化的职业人员完成技术选择,而且经过网络安全值班和分配监管人员随时告知运行维修部门的有关负责人员完成设置。视频监测体系互相结合,全方位明确网络事物完全运用变电站视频监测体系随时监测和历史查看功能,根据网络安全事物的消息信息,针对整个站点完成全方位的评判。从多个层面、立体化的检测事情出现过程中有关人员的进出情况。运用安置在变电站的每个地方的录像机针对生产设施与氛围安全完成监测,而且把检测事件的动态图像传送到监测中心,监控中心能够对于摄像机完成管控与摄像。

3.4强化入侵检测技术,加强电力系统网络安全性

入侵检测技术简单来说就是指对电力监控系统中的各项重要信息和数据进行日常分析和检查的技术,在分析研究的过程中,就会发现电力系统有没有异常情况或者其中有没有恶意代码。入侵检测技术的最大作用就是发现电力监控系统中出现的各种异常情况并向工作人员发出警报。这也同防火墙一样,是一项有效提升网络安全的手段。入侵检测技术共有两种,一个是对主机进行检测,一个是对网络进行检测。应用入侵检测技术,可以明确电力监控系统主机的具体情况,查看信息数据有没有受到入侵。另外,检测网络安全情况的相关技术是比较简单方便的,只需要检测登录、审计等环节,就可以了解到网络安全情况。入侵检测技术同其它安全检测技术是有一定差别的,属于主动进行安全防护的技术。完整的入侵检测技术打造出来的入侵检测系统,是依据各种入侵行为的实际特点,所制定的对策,实时监控网络安全运行情况,一旦发现网络安全遭到破坏,会以最快的速度发出警报。

3.5让网络安全总体的预防能力变强

每个相关的单位都需要逐渐加大网络安全监管以及应急管控的强度,把有关看到的网络安全事件、处理与以后的维护工作处理完善,使得很多互联网安全问题能够有关的解决。需要主动探究与运用新型技术,网络方面如果存在安全问题需要随时处理。

4 结语

总之,加强电力发展能够有效缓解能源紧张问题,在为社会经济发展提供的同时,有效保障电力安全,推动电力发展。在网络安全防护活动开展过程中,要做到安全分区,网络专用,横向隔离,纵向认证。通过更加完善的工作流程,保障相应工作能够高效稳定落实,并且能够做好安全防护问题整改等相关工作,全面加强电力安全防护,运行管理等,有效维护电力监控系统网络安全。

[参考文献]

[1]李伟.电力监控系统网络安全管理平台设计[J].电子世界,2020,(22):176-177.

[2]汤超.浅析电力监控系统网络安全监视体系建设[J].机电信息,2020,(32):142-143.

[3]江志东.电力监控系统网络安全防护探究[J].网络安全技术与应用,2020,(03):99-100.

[4]张涛,赵东艳,薛峰,等.电力系统智能终端信息安全防护技术研究框架[J].电力系统自动化,2019,43(19):1-8+67.