水电厂监控系统信息安全防护优化研究

李 鹏
(大唐雅安电力开发有限公司,四川雅安 625500)

摘 要:针对水电厂监控系统在信息安全领域存在的问题,提出解决这些问题的优化设计方案,包括网络系统的防火墙优化、提升监控系统的物理隔离水准、加快网络数据传输的防护优化进程以及监控系统防护入侵策略的优化等,对于水电厂监控系统而言,可以有效提高水电厂监控系统的安全性,为水电厂的生产和运营提供重要的保障。

关键词:水电厂;监控系统;信息安全;网络通信;防护优化
中图分类号:[TM622];X924.3;S605+.3 **文献标识码**: B **文章编号**:1001-2184(2023)04-0085-05

Research on Information Security Protection Optimization of Hydropower Plant Monitoring System

LI Peng
(Datang Ya'an Electric Power Development Co., Ltd., Ya'an Sichuan 625500)

Abstract: Aiming at the problems in the field of information security of the hydropower monitoring system, this paper proposes the optimization design schemes, including the firewall optimization of network system, the physical isolation level of monitoring system, the acceleration of the protection optimization process of network data transmission, and the optimization of intrusion protection strategy of monitoring system. The optimal design scheme proposed in this paper can effectively improve the safety of the monitoring system and provide an important guarantee for the production and operation of hydropower plants.

Keywords: Hydropower plant; Monitoring system; Information security; Network communication; Protection optimization

0 引 言

随着社会的不断发展和进步,水电厂的生产运营已经逐渐向着智能化、自动化方向发展。水电厂监控信息系统作为水电厂的中枢神经系统,起到整个生产运营流程的关键作用。然而,随着信息技术的不断发展,网络攻击技术也愈来愈成熟和高级。因此,水电厂监控信息系统的安全问题已经日益引起人们的重视。安全一旦出现问题,不仅会造成生产经济上的巨大损失,还会对社会稳定和人民生命财产安全造成巨大威胁。

针对水电厂监控系统在信息安全领域存在的问题,必须对网络系统的防火墙进行优化,提升监控系统的物理隔离水准,加快网络数据传输的防护进程,同时还要对监控系统防护入侵策略进行优化,才能保证水电厂监控信息系统更加安全可靠,降低潜在风险,增强对水电厂生产运营的保障力度。

收稿日期:2023-06-29

1 水电厂监控系统概述

水电厂作为国民经济的重要组成部分,其生产运营的自动化程度不断提高,监控信息系统也在随之发展。水电厂监控系统是水电厂自动化控制系统的核心部分,是水电厂操作者获取和控制水电厂信息的重要工具。它的主要功能是对水电厂的运行参数进行实时监测、收集和存储,并对这些数据进行自动化处理,依据预设好的算法规律采取必要的措施,保障水电厂的正常运行。

水电厂监控系统主要由硬件设备与软件系统构成,硬件设备包括传感器、控制器、执行器等,而软件系统则包括操作系统、数据库、应用软件等。

在实际应用中,水电厂监控系统一般包含人机界面(HMI)、数据采集与处理、数字信号处理与控制、通信管理、远程操作等功能模块[1]。其中,人机界面 HMI 是水电厂操作者与监控系统之间的桥梁,负责人机交互,显示现场实时数据的状态和控制命令的结果。数据采集与处理模块是水电厂监控系统的核心部分,主要负责对各种传感器和设备的数据进行采集、处理、分析和计算,并控制执行器对系统进行调整、控制和优化。数字信号处理与控制模块则负责对数据进行数字化编码,进行数据流的传输、分析和处理。通信管理模块是监控系统与其他设备或系统之间的数据通信的重要部分,提供数据传输的环节。远程操作模块则允许操作者通过互联网远程获取水电厂运行数据及进行远程控制。

2　水电厂监控信息系统的网络安全问题

2.1　网络数据传输问题

水电厂监控信息系统中的网络数据传输是个重要环节。传统的网络通信方式采用明文传输,存在数据被窃听和篡改的可能性,并且这些安全威胁会对水电厂的运行和生产带来巨大损失。因此,保障网络数据传输的安全非常关键。为了解决这个问题,可采用数据加密技术,对传输的数据进行加密处理。一般来说,对于需要保护的数据,可以采用对称加密算法或非对称加密算法进行加密,加密后的数据在传输过程中即使被截取,攻击者也无法利用这些数据进行攻击[2]。而对于数据的完整性保护,则可以通过数字签名技术来实现,保证接收方能够验证所收到数据的真实性和完整性,从而防止数据被篡改。此外,对于对数据加密解密进行重复操作的情况,可以采用密钥协商技术,确保密钥的安全性。在实际应用中,为了更好地保障网络数据传输的安全,还需要做好网络拓扑结构设计、提升网络通信速度和稳定性、规范网络访问流程等工作。同时,还需要不断增强网络安全防御能力,包括制定安全策略、建立安全监控机制、加强网络安全培训等措施,提高网络安全防护水平。

根据电力监控系统安全防护总体方案指导,锅浪跷水电站地调数据网内已划分两个 VPN,分别是实时控制 VPN 和非控制生产 VPN,分别供安全区 I(实时控制区)、安全区 Ⅱ(非控制生产区)数据上传。站内调度数据网作为数据采集中心,由调度数据网接入地调骨干接点,实现公司的调度自动化信息经过调度数据网向地调传送。

远动装置经三层交换机(实时交换机)——实时纵向加密装置——地调路由器设备接入地调。电能量采集、保信子站数据经三层交换机(非实时交换机)——非实时纵向加密装置——地调路由器向地调传输。

2.2　网络通信安全问题

水电厂监控信息系统中的网络通信安全问题,是指数据在网络中传输过程中可能会被窃听、篡改、伪造等,影响水电厂的生产和运营。在现代化的水电厂系统中,网络已经成为各个子系统之间协同工作的基础,也成了水电厂安全的最大的威胁源。因此,如何保证水电厂网络通信的安全,保障系统的稳定运行,是一项必须着重考虑的重要问题。为了加强水电厂网络通信的安全,应建立完善的网络安全管理制度,按照“谁主管谁负责,谁运营谁负责”原则,制定《计算机监控系统管理制度》《计算机网络管理制度》《监控系统管理制度》《防病毒管理制度》《数据库系统管理制度》。定期按要求更新密码,采用禁止外网连接、权限登录、加强宣贯培训、封闭闲置的 USB 接口、应急预案演练等方式,确保系统安全稳定运行。此外,在网络通信中,进一步加强数据传输的安全性也是很重要的。一种方法是采用虚拟专用网络技术(VPN)来保证网络通信的安全性,使得数据在从发源端到目的端的过程中不被窃听、篡改或截获;另一种方法是采用身份验证和访问控制技术来防止非法用户访问网络资源。在此基础上,还应该增强系统的日志管理和审计功能,及时发现并处理网络安全事件[3]。

2.3　系统防火墙问题

系统防火墙是现代化水电厂监控信息系统中网络安全的第一道防线,在网络系统与互联网连接处起着至关重要的作用,主要用于防止非法入侵和攻击,保护系统的数据和应用等资源安全。为了提高系统防火墙的安全功能,可以从以下方面着手:

(1)采用合理的网络拓扑结构设计,将不同功能的子网放置在各自的子网中,并设置网络边界,保证不同区域之间的流量只能通过防火墙进行通

信。同时,采用虚拟专用网(VPN)等技术,将内部网络与外部网络隔离开来,有效减少系统被攻击的风险。

(2)在防火墙上设置规则,对进出网络的流量进行过滤和限制,设置合理的防火墙功能,可有效降低网络被攻击的危险性。此外,对具体的站点、IP 地址、协议、端口等进行深入细致的管理,增强网络安全保护能力。

(3)设置检测和过滤规则,通过分析和屏蔽恶意程序、垃圾邮件、病毒和木马等有害信息,保证通信内容的安全可靠。同时,也应该对内网与外网之间的通信进行监控,及时发现异常情况,做出相应的处理。

(4)防火墙应该设置安全日志记录功能,记录所有进出网络流量以及阻拦流量的详细信息。及时分析和处理日志数据,可以有效地提高系统对于攻击事件的应对能力,并为后续的网络安全分析和处理提供有用的数据支持。

2.4　工作人员安全意识问题

工作人员安全意识问题是企业信息安全管理中非常重要的一环。随着互联网技术的发展,网络安全威胁日益增多,企业面临着越来越复杂的安全挑战。而工作人员作为企业信息系统的重要组成部分,其安全意识和安全行为直接影响着企业的安全状况[4],因此,需要加强对工作人员安全意识问题的培训和教育。

首先,在工程师站计算机管理中,其有权限进入锅浪跷水电站微机防误系统的操作人员,应严格按变电运行规定及规程要求在微机防误系统下,模拟操作及填写、上传、打印操作票。查看、填写当日发电日报表、月报表及相关数据,必须经当值值班长同意或授权,禁止打开、移动、删除计算机目录下的所有文件夹及文件,未经系统管理员批准,禁止进行数据拷贝或外来磁盘、光盘的插入和操作,严禁进行与工作无关的任何操作。

其次,在使用办公用计算机时,必须经当值值班长或系统管理员同意,并且详细登记后方可使用。自己所建文件或文档必须归类到各自所属磁盘的文件夹内,不准将文档、文件或文件夹乱摆乱放,不得随意打开、移除、更改与自己无关的程序及文件。除上网向国电公司上传报表数据外,未经系统管理员同意或授权,不得上网做与国电公司报表无关的事。严禁更改计算机的所有设置、安装和删除所有程序,严禁更改、删除、移动计算机内所有文件夹及文件,严禁外来磁盘以及光盘的插入和操作。通过此类措施,能够大大提高员工的应急反应能力和相应的处理能力,更好地保障企业信息安全[5]。

3　水电厂监控系统安全防护优化设计

3.1　网络系统的防火墙优化

网络系统的防火墙优化是保障水电厂监控系统安全性的重要措施。防火墙是网络系统的第一道防线,可有效地预防和阻拦恶意攻击,保护系统的数据和应用等资源安全。

3.1.1　升级改进现有防火墙

对现有防火墙进行评估,了解其安全漏洞和弱点,并根据情况进行升级和改进。例如,使用最新的防火墙设备和软件,增强网络对攻击、恶意代码和病毒等威胁的防御能力,保证系统的稳定性和安全性。

3.1.2　对防火墙的规则进行优化

设置合理的防火墙规则,对进出网络的流量进行过滤和限制,加强对不同网络层次之间的通信管控。同时,针对常见攻击方式和流量进行规则修订,例如 IP 地址、协议、端口等进行逐一筛查管理,增强对违规访问或不明威胁的阻止。

3.1.3　采取虚拟专用网(VPN)等技术措施

将内部网络与外部网络隔离开来,减少系统被攻击的风险。采用可信安全防护设备和自主研发的安全软件对防火墙和网络设备进行加固和加密,提高系统的安全性和稳定性。防火墙还应该设置日志记录功能,及时记录所有进入或离开网络的信息流量,并对恶意攻击等安全事件及时处理。

3.2　提升监控系统的物理隔离水准

随着科技的发展,监控系统在水电厂中得到广泛应用。然而,如何保障监控系统的安全性和稳定性,是值得考虑的问题。提升监控系统的物理隔离水准是保障系统安全的重要措施。

3.2.1　对监控系统合理布局

对监控系统进行合理的规划布局,合理分区并设置限制与控制。如果监控系统正在运行敏感的信息或应用程序,需要采取更严格的控制措施。例如,将具有相同密级和其他安全特征的信息或

应用程序放置在独立的区域内,并采取设置门禁、刷卡等物理隔离访问控制措施,以确保系统的安全可靠。

3.2.2　选择高品质的监控设备

增加摄像头的数量及其安装位置,采用高清晰度的监控摄像头,增加系统的可靠性和受控性,以及有效监测攻击和操作活动。

3.2.3　加固系统硬件和软件安全

更换安全性能更强的存储设备,增强对数据的保护;对监控系统中的软件、驱动等进行管理与升级,及时修补安全漏洞,防止黑客攻击。

3.2.4　宣传物理隔离的重要性

向所有工作人员宣传物理隔离的重要性和方法,引导员工自觉遵守企业安全管理规定,增强员工的安全意识和应急反应能力。

3.3　加快网络数据传输的防护优化进程

网络数据传输的高效、稳定和安全是保障网络正常运行以及信息安全的必要条件。然而,在日益增多的网络攻击、病毒、恶意软件等黑客攻击下,如何加快网络数据传输的防护优化进程变得尤为重要。

3.3.1　保护网络设备的安全性

提高网络设备的防护性能,确保设备本身的安全,须选择符合标准的设备,加强对硬件和软件的安全管理,对其进行加密、认证和授权等技术手段,有效地保护网络设备的安全性。

3.3.2　设置合理的防火墙规则

采用严格的访问控制和鉴别技术,限制违规访问,防止未经授权的访问。配置成熟的防火墙软件,加强对流量的监管,自动发现并拦截恶意程序和异常流量,确保网络数据的安全传输。同时,还应加强加密技术的应用,通过使用各种加密算法,保护数据传输的隐私性和机密性。例如,SSL/TLS 协议、IPSec、SSH 等加密技术,均可以有效保护网络数据的安全传输。

3.3.3　定期进行安全漏洞扫描及人工检查

在安全漏洞扫描中,工作人员可以通过本地或远程扫描的方式检测系统的安全漏洞、网络结构、网络设备、服务器主机、数据、用户账号、口令等目标,是否存在的安全风险、漏洞和威胁。在安全扫描过程中,其主要需要注重系统安全漏洞、网络层安全漏洞和应用层安全漏三个层面的问题。其中系统安全漏洞主要包括操作系统本身不安全的因素和安全配置存在问题,网络层安全漏洞主要关注网络身份认证、网络资源访问控制、数据传输保密与完整性、远程接入、域名系统、路由系统的安全和入侵检测等,而应用层安全漏洞则考虑网络对用户提供服务的应用软件安全性,包括数据库软件、Web 服务、电子邮件系统、域名系统、交换与路由系统、防火墙及应用网管系统、业务应用软件及其他网络服务等。在进行人工检查时则需要检查操作系统的配置是否达到最优状态,以保证网络系统的正常运行。同时,确认操作系统自身的保护机制是否已经实现,以及相应的管理机制是否安全也是极为必要的。此外,工作人员还需要检查操作系统为网络提供的保护措施是否有效,并且这些措施是否被正确地配置。再者,工作人员还需要关注操作系统是否定期升级或更新,以保持其最新的安全补丁和修复程序。最后,需要注意检查操作系统是否存在漏洞或后门,并及时采取措施加以修复。这些人工检查内容能够有效地提升操作系统的安全性和稳定性,以满足信息安全体系的需求。

3.4　监控系统防护入侵策略的优化

3.4.1　入侵防御

监控系统在保障安全和维持运行方面具有重要作用,但是监控系统经常成为黑客攻击的目标。因此,确保监控系统免受入侵,防止数据泄露和操作失误,是至关重要的。为了优化监控系统的防护入侵策略,可以采取以下措施:

(1)建立健全的防火墙策略,设置合理的访问控制机制,对入侵者进行鉴别和隔离。合理分类不同的网络节点和数据流,设置不同的权限和安全性级别,最大程度限制入侵者的篡改破坏和窃取数据。

(2)加强系统日志和安全审计的监管和管理。记录用户访问、修改、删除等操作行为,完善管理制度,及时预警有可能出现的问题,并尽快采取相应的解决措施。加强设备的安全检测和修复工作,提高系统审核的精度和效果。

(3)定期开展安全培训和意识教育。通过多种途径向员工宣传安全防范知识,强化员工安全意识,并向员工介绍新的安全漏洞、病毒、攻击技

术等,引起员工对网络安全的高度重视。

(4)加强合作伙伴和供应商的监管。与合作伙伴和供应商建立严格的监管和管理制度,并要求其采取相应的安全保护措施,避免安全事件对本企业造成损失和影响。

3.4.2　防病毒措施

(1)防病毒软件应该支持多种操作系统平台,包括:Windows9x/Me/NT/2000/XP/2003、Unix、Linux 等。此外,还具备支持群件系统 Lotus Notes 和 MS Exchange 邮件服务器的实时监控和查杀毒。要求支持广泛操作系统平台的作用是将来可以比较容易地进行扩展。

(2)应能监测引导型病毒、内存病毒、文件病毒、蠕虫、宏病毒、木马、恶意 Java 小程序和 ActiveX 代码等各种病毒,能自动回复病毒修改的注册表,自动删除特洛伊/木马程序。

(3)对 smtp、pop3 协议邮件进行实时监控保护,并且支持对 Lotus Notes 和 MS Exchange 邮件服务器的实时监控和查杀毒,对所有进出邮件服务器的邮件进行病毒扫描。

(4)具备实时检测病毒的功能,同时支持手动扫描。

(5)要求支持后台检测,采用低资源占用检测技术,对系统资源、网络带宽占用少。

(6)实时检测并清除各种常用压缩格式文件内部的病毒,查杀包括 arj、rar、cab、cml、jar 等多种格式的压缩文件。

(7)支持对病毒的多种处理方式。根据实际情况,可分别对染毒文件进行实时查杀、删除文件、重命名、只报告等方式,清除文件前可进行备份,对不能处理的病毒文件进行隔离。

(8)对于公共服务器的访问,提供带毒用户的隔离措施。一旦发现带毒用户访问或者上传染毒文件,自动阻止其连接,防止病毒通过公共服务器大范围传播。

(9)提供封锁文件访问的功能。通过封锁指定扩展名的方式,拒绝对所有该类型文件的访问,以此在特殊情况下保护关键文件。

(10)支持用户根据实际需要定制针对特定目标的定时扫描任务;可以根据用户的实际情况,排除不需要扫描的对象。

(11)要求采用双引擎技术,为查杀计算机病毒提供更全面的手段。

3.4.3　主机加固

3.4.3.1　防止程序非法终止

防止未经授权的超级用户非法终止重要进程及后台守护进程,保证服务器的正常运行,一些关键的进程如数据库守护进程、应用程序进程等应该一直运行,不应该被终止。提供对进程的保护,可以截取发向系统的进程结束信号。被保护的进程可以正常或异常退出,但不能被非授权的用户(包括超级用户)终止,这就保护了误操作造成的关键进程的异常终止,保障了系统的可靠性,只有通过认证的超级用户可以结束进程。

3.4.3.2　文件的访问控制权限

通过细化用户的文件访问权限规定,严格限制了用户对文件的访问权。例如可以设置保护的文件即使超级用户也只能读,不能进行修改,同时,还可以完整检查文件内容是否被修改过。除此而外,还可采取访问控制列表的方式确定用户对文件的访问权限,因此,每一个不同的用户都可以对文件有不同的权限,而不仅仅限于属主、同组者和其他用户三种情况,这就增加了控制的灵活性。

3.4.3.3　进程管理

通过管理控制台实时显示连接站点的进程状态,可以选择进程添加/删除访问控制和发送信号,可实时查看当前进程和进程设置防 kill 保护,还可以对进程发送多种信号,方便管理员管理维护系统,及时地停止可疑程序或进程。

3.4.3.4　主动的入侵防护及审计跟踪

当系统发生入侵行为或者违反安全的操作时,系统能利用自身功能对用户在网络层和系统内部对进行阻断,并且由系统向管理员进行报警,实现主动的入侵防御功能。

3.4.3.5　权限分离及最小特权实现

操作系统访问控制的最佳策略是权限分离和最小特权原则。通过严格分开系统管理员和安全管理员的权限,以控制超级用户的权限,可有效防止内部人员的越权访问和外部的攻击。

3.4.3.6　先进的程序自我保护

系统使用了全球领先的内核密封技术管理内

(下转第 113 页)

下开启闸门，可能会引发事故。

闸门自动控制系统对水电站的运行有百利而无一害，但需要技术人员在实践中解决这些.难题，才能保障系统稳定运行。

5　结　语

本文在通过对某电站的闸门参数、运行方式、运行原理、日常维护方式进行分析，并结合该电站闸门在历史运行过程出现的故障问题，得出该电站的闸门运行方式比较成熟可靠，装置集成化程度较高的结论。但是，对比国内某些尖端电站，在装置自动化、智能化上还存在比较大的差距，因此，该站要实现“关门运行”，还有很长的一段路要走。闸门控制系统要想真正从“人”手中交到“机器”手中，不仅要依赖精密程度高的可靠装置，更需要人工智能技术的结合，因为人工智能技术在今后水电站运行的发展中必将扮演重要的角色。

参考文献：

[1] 曹宁，温宁.水利闸门控制系统的研究进展[J].信息与电脑(理论版)，2015，(21)：96－99.

[2] 代威.弧形闸门开度计算[J].山西水利科技，2014，(02)：18－20.

[3] 李作成.闸门启闭机自动化后的维修与保养[J].内蒙古水利，2011，(05)：91－92.

[4] 杨宏宇，刘婧，庞涛，等.闸门启闭机械维修保养技术[J].河南水利与南水北调，2016，(07)：91－93＋114.

[5] 杜亭，吴国栋，赵传啸，等.泄洪警报系统在官地水电站的应用[J].自动化应用，2019，(11)：148－149.

[6] 单江.水库闸门自动控制系统的安全性设计[J].中国水运(下半月)，2014，14(07)：168－171.

作者简介：

李承昊(1999-)，男，四川邛崃人，学士，助理工程师，从事水电运行方面工作；

赵　懿(1999-)，男，四川绵阳人，学士，助理工程师，从事水电运行方面工作；

胡玉芳(1998-)，女，四川攀枝花人，学士，从事水电运行方面工作.

(责任编辑：卓政昌)

(上接第 89 页)

核模块的加载/卸载，可阻断对内核的恶意攻击。系统还具有内核隐藏功能，它隐藏了安全内核，并自动保护自身系统程序目录和文件，可防止安全内核程序被删除，最大限度地降低了安全风险。

3.4.3.7　灵活的网络访问控制

系统提供了主机防火墙功能，系统管理员可以根据需要设计安全策略来控制基于网络的访问，可通过设置拒绝或允许的 IP 和服务管理系统的外部访问，也可对存在漏洞的连接进行控制，阻断外部非法访问，避免被入侵者利用。

3.4.3.8　日志管理

系统提供了对安全日志和系统日志进行详细的记录和保护，内容包括产品自身的安全配置和针对保护的目标所作的操作日志、违规日志等，提供细粒度的查询和检索，方便进行备份、保存、统计分析。

4　结　语

网络安全是当今社会中十分重要的一环，对于保障信息的安全和稳定具有至关重要的作用。在不断发展的互联网环境下，网络安全面临着越来越复杂和严峻的挑战，因此，需要采取相应的措施，加强网络安全保护。通过加强对硬件设备的防护、设置合理的防火墙、加强加密技术的应用等多种手段，可以有效地提高网络安全保障水平。同时，也应该注重人才的培养和引进，提高网络安全技能和素质，增强网络安全人才队伍力量，探索适合国情的网络安全发展模式。只有这样，才能确保网络的安全和稳定，为推动信息化建设和数字经济的快速发展提供保障和支撑。

参考文献：

[1] Shu, J., & Chen, X. (2021). Cybersecurity risk management in smart cities: State－of－the－art and research challenges. Journal of Cleaner Production, 305, 127687.

[2] Li, Y., Zhang, Q., Qi, L., & Chiu, D. M. (2019). A survey on internet of things security: Requirements, challenges, and solutions. Journal of Network and Computer Applications, 126, 46-70.

[3] Xu, Q., Yu, S., & Song, M. (2018). A survey of security and privacy issues in smart grids. IEEE Communications Surveys & Tutorials, 20(1), 556-576.

[4] 陈亚燕.水电厂信息网络安全防护策略探究[J].网络安全技术与应用，2021，(03)：103-104.

[5] 栾国强，张鹏.水电企业信息安全防护体系综合提升研究[C]//信息产业信息安全测评中心.2018 第七届全国安全等级保护技术大会论文集.2018 第七届全国安全等级保护技术大会论文集，2018：189-193.

作者简介：

李　鹏(1989-)，男，山东烟台人，工程师，学士学位，主要研究水电厂站通讯技术及网络安全管理.

(责任编辑：卓政昌)