

电力调度自动化网络的策略分析

王为鹏¹ 徐援军²

1.烟台金建冶金科技有限公司 山东烟台 264000; 2.金建工程设计有限公司 山东烟台 264000

摘要: 对于电力调度和自动化系统而言,保障网络安全至关重要,其目的就是为了确保电力调度和自动化系统能够稳定地正常运行。基于此,相关政府和部门仍然给予国电力调度和自动化网络安全的高度重视,促使其所有存在的价值与功能效用都可以在电力工程行业的发展中得到充分地挖掘和利用,为促进我国的社会和经济健康可持续发展做好保障。本文对电力调度自动化网络的策略进行分析。

关键词: 电力调度; 自动化网络; 系统安全

一、电力调度自动化的网络分析

电力调度自动化网络显然本质上是全球能源互联网的组成部分,但显然它与普通的互联网存在典型区别,电力调度自动化网络在智能电网中,承担主要的电力自动化调度指令传输与反馈的功能,是实现能源传输、资源配置、信息交互、智能控制的重要通信平台。信息通信技术是其关键技术手段,在电力自动调度中用以辅助电力生产,实现对电网、微电网、分布式电源的智能调控,在信息通信技术基础上将电网、微电网、分布式电源等纳入一个电力局域网当中,进而精准辨识全网负荷,用以科学调度,信息通信技术提供的调度控制支撑平台,实现更为高效的能源传输,将用户实时变更需要,线路状况等信息汇总后上传至供电公司的数据中心,为决策提供更为有效的数据支撑,同时前端智能化控制装备通过网络连接实现对电网的高效控制。

二、电力调度自动化的特点

严密监控电网的正常运行。电网系统在进行常规运行操作时,通过调度仪和技术人员对电网的各种参数和指标进行了控制和监测;以及对于供暖系统的供暖、位置条件情况以及给水等各个方面在工作中的运行状态进行了统计和分析,让其能够达到所有规定和具体要求,确保了供水系统的用电质量和使用者合理地计划供水。积极促进我电网通信运营商的管理。在对我国电网电力资源利用进行安全有效管理和远程监控的必要性和前提下,通过同时采取有效调度和实现资源利用自动化的两种手段方式来有效调度和不断优化我国电网的利用经济,以真正达到少资源耗能、多资源利用和节电的发展目标^[1]。

三、电力调度管理自动化系统中的安全问题

系统问题。该问题主要是由于系统未及时升级或者是未从手机下载的系统安全补丁来对系统进行了加固,让整个系统本身产生了安全性的漏洞。防火墙的安全性和防护措施由于设置得不合理,未对网络拓扑的结构和方式变化做出适当的调整,没有在第一个时间内做出防

护。另外还有一个原因是Web服务器上的协议和通信服务并没有及时被关闭。这样就让电力调度自动模糊系统本身所收集得到的大量数据错误,势必会严重影响自动风机的控制,继而导致电厂在工作中受到影响,无法正常运行,虽然电网已经能够维持正常工作,其也很容易导致电路发生安全事故^[2]。

1.内网用户问题

这主要是由于一些我国的用户由于自己欠缺的网络安全意识而造成,让外部的公网服务器直接进入一些系统的电脑和 workstation,导致整个系统的网络安全遭到严重威胁,或者部分用户的网络安全操作出现失误,又或者部分维修人员在对系统开始时进行日常维护和编程的过程中可能出现的一些失误,上述这些均将会直接造成我国的用电力调度机构和自动化系统都遭到了影响,无法安全稳定地正常运行。操作中应用的口令比较简便,不定期的修改和轮换也容易造成网络安全的问题,导致操作中的越权等状况时有发生,这对于电力调度机械自动化系统的完全正常运行非常不利。

2.外部网用户问题

远程诊断的拨号都是一直接通,并且欠缺相应的安全保障防护手段,即只有没有授权的无线网络用户才能直接进入至自动化的系统中。并且由于电子邮件的实际使用仍然欠缺有效的制约,病毒只能通过电子邮件的各种方式来传播、感染,电力调度机构自动化的系统也同时还会存在被网络黑客攻击和侵略的危害,因而存在很多的安全隐患内。电力调度和自动化管理系统制定相应的风险处置办法和解决措施。电力调度和计算机自动化系统中的所有数据的风险,会直接导致系统无法正常运行和工作^[3]。

四、电力调度自动化网络安全技术的应用

1.网络安全体系

要想实现电力调度自动化,网络安全就需要进一步的提高网络安全的体系,相关人员要构建一个完整的网

络安全体系, 这样在进行管理的过程中才更加的容易。同时, 该体系的总体构建能够把整个网络安全性能划分在一起, 再遇到黑客攻击时, 可以全面进行反击。

2. 物理层安全的技术

在进行电力调度自动化网络安全发展的过程中, 也一定要实现物理层的安全技术, 这样它能够确切地保护这些网络设备的安全性, 因为物理层, 它是包含着网络的所有硬件设备, 所以说在进行运作的过程中, 网络的硬件设备可以有效地抵御病毒的入侵。并且根据物理层的一些特点可以对电力调度自动化网络安全的一些调整, 这样能够多方面的保护电力系统的网络安全性。(1) 一定要做好网络设备的保护措施, 因为有的时候网络设备的运行可能会受到一些自然灾害的影响, 例如, 突发的泥石流台风, 龙卷风等一些自然灾害都会对网络设备的运行产生巨大的影响。(2) 在电力系统安全防护方面, 还要设置一些网络备份, 这样能够防止网络设备的丢失, 提前做好防范工作。(3) 对于网络设备的运行环境也要进行关注。因为在使用过程中会发现有一些设备并没有授权就进入, 从而导致了整个系统的崩溃, 有些设备存在一些不安全因素。而且在发展的过程中, 还要将电力调配的网络与分支网络进行相应的隔离, 从而防止一些黑客进行恶意的攻击。并且因为网络它是处于一个独立性的, 这样就不会对电力调控的运行造成影响, 能够使得网络安全性能更加的有保障^[4]。

3. 网络层安全的技术

在网络层管理过程中, 网络的设备其实是非常重要的, 所以说在进行安全决策的过程中, 一定要与网络安全形成密切的联系, 这样能够从根本上保护网络层的安全。所以说, 为了更好地保护网络层的安全, 就需要做到以下措施:(1) 不是授权的人员, 不能与网络层有相应的接触, 因为网络层是非常重要的, 一旦被其他人员接触, 那么就很可能被一些人员进行篡改。因此在进行设备管理的过程中, 一定要禁止非授权人员进入。(2) 还要对网络的路由协议进行完善, 及时的补休那些协议中所存在的一些漏洞, 其实不法分子他们大部分都是利用一些漏洞对网络进行全面的攻击, 从而造成网络的瘫痪以及数据的丢失。因此, 在进行发展过程中, 一定要完善网络路由协议, 这样才能够从根本上阻挡不法分子的入侵^[5]。(3) 针对专用的网络, 要采取一定的访问控制技术, 这样它能够应用物理隔断的技术来阻挡病毒的侵入, 并且还可以更好地提高数据传输的一些安全性, 保证数据能够不被病毒所入侵, 这样在一定程度上可以使得数据更加的安全性, 同时也能够防止一些重要的数据在输入的过程中被窃取^[6]。

4. 系统层安全的技术

对于系统安全层的管理, 是由专门的网络技术员,

他们负责面对网络所出现的问题, 及时的进行清理和排查。定期对软件进行升级, 以及内部系统的垃圾清理, 这样可以更好地提高网络的运行速度。要想真正的提高网络的安全, 就必须加强防火墙和一些杀毒软件技术的运用, 通过防火墙, 它能够阻挡不法分子的入侵, 并且即使当有不法分子入侵时, 防火墙会自动进行预警, 可以保护内网里面的数据信息使数据信息自动的保存^[7]。然而, 防火墙对于不法分子进行内部攻击却束手无策, 这时就需要把防火墙与其他一些新的技术进行连接, 更好地保证内网和外网的安全性, 而杀毒软件顾名思义, 就是用来杀毒的, 其实许多网络中会含有大量的病毒, 而这些病毒对于网络数据也会进行侵入, 从而销毁一些重要的信息内容, 对于网络病毒, 就需要专业的人士去鉴别病毒的类型, 从而升级一些杀毒软件, 能够把这些病毒全部剔除, 还需要相关人员能够定期对网络进行清理和更新, 这样能够提高整个网络运行的安全性, 更好的保障人们的日常用电。因此, 在今后的发展过程中, 相关人员还要不断地提高自己的专业技术以及素质, 这样才能够更好地应对各种各样的病毒软件^[8]。

五、结束语

对于一些大型电力电网调度系统自动化管理系统来说, 会出现一些来自电力电网调度系统数据库的信息被一些用户随意地非法窃取或者随意修改, 从而极大地有可能甚至或许会在近期内可能引发很多的重大电网安全事。因此, 各大中型电力设备公司必须根据实际工作情况, 加强对我国电力设备调度系统机械和电力自动化管理系统设备安全性的分析研究, 以此来作为主要基础作用来不断维护它们的安全和稳定地正常运行。

参考文献:

- [1]焦伟.电力调度自动化网络安全防护系统的研究与实现[D].河北:华北电力大学, 2014.
- [2]李耀庭.电力调度自动化网络的安全与实现[J].科技创新导报, 2010(02): 33-34.
- [3]王喜贺.电力调度自动化网络安全与实现[D].山东:山东大学, 2009.
- [4]江茂森.电力调度自动化网络安全防护系统的研究与实现[J].山东工业技术, 2018(23): 220.
- [5]王谦, 李烽.电力调度的自动化网络安全分析及实现[J].电子技术与软件工程, 2017(21): 116.
- [6]王雅婷.电力调度自动化网络安全与实现技术[J].中国设备工程, 2020(22): 202-204.
- [7]侯红梅.浅谈电力调度自动化运行中的网络安全问题及解决对策[J].中国高新技术企业, 2017(01): 141-142.
- [8]王桂兰.电力调度自动化系统的应用现状与发展趋势[J].科技信息, 2011(28): 330.