

# 电力监控系统网络安全防护技术应用探析

苑金龙

国网天津市电力公司高压分公司 天津 300232

**[摘要]**随着电力系统的发展和计算机通信技术的革新,火电企业自动化、数字化和智能化程度越来越高,发电企业电力监控系统网络之间的信息交互也越来越复杂,在日益严峻的工控安全形势下,必须有一个完善的电力监控系统安全防护技术,来保障机组的安全稳定运行。基于此,本文介绍了提升电力监控系统网络安全的具体要求,分析了电力监控系统中已经出现的网络安全疏漏,并探讨了电力监控系统网络安全防护技术的具体应用,仅供参考。

**[关键词]**电力监控系统;网络安全;防护技术;应用

**[DOI]** 10.12252/j.issn.2096-627X.2021.10.034

## 引言

我国电网规模世界第一,发电量世界第一,电力生产的发、输、变、配、用各个环节是动态平衡的过程,信息技术支撑各环节有序运转。电力监控系统用于监视和控制电力生产及供应的过程,故保障电力监控系统安全是保障电力安全生产的关键,也是国家安全的基础保障。据统计,近年来,电力工控系统信息安全事件呈现低频率但高威胁的特点,因此保障电力监控系统网络的安全性,利用网络关键技术加强安全防护十分重要。

### 一、提升电力监控系统网络安全的具体要求

在整个电力监控系统中存在多种多样的问题,网络安全防护是非常重要的问题之一。若要切实保障电力监控系统的网络安全,那么就必须按照相关要求进行网络安全防护工作。实际上,电力监控系统网络安全防护工作就是必须保证相关数据资料不被侵犯或者盗取,保证所有重要的资料信息都被完好无损的保存下来。管理人员必须提前制定好电力监控系统网络安全防护方案,防范黑客或者不法分子的入侵,利用一系列防护技术保障电力监控系统的安全。

### 二、电力监控系统中已经出现的网络安全疏漏

#### (一)网络安全方面

网络设备是否配置合理的参数,会关系到网络设备能否安全、稳定地运作。在涉密机构的核心控制系统方面,考虑到一般防火墙是依靠逻辑实体,其自身也可能受到外界操控,所以在安全控制效果上十分有限,并且对于各类专用的通信协议与规则不太适用,所以不能有效满足高层次的数据安全需要。对于规模相对较大的网络,若是未设置专门的网络管理设施与网络故障侦察设施,则一旦网络内部出现问题,网络管理人员便需要花费很多的时间来进行处理,特别是当网络发生严重故障时,就可能会导致办公系统整体上的正常运作都受到影响。

#### (二)网络安全防护工作实施效率低

首先,大部分进行相关工作的工作人员,不会更改系统中自带的比较容易记住的口令,而且经常以远程操作的方式进行一系列工作,导致很多口令和密码都被泄漏出去,进而使得电力监控系统出现严重的安全隐患。电力监控系统在运行过程中需要大量的工作人员,如果不严格监管,那么很容易将口令密码泄漏出去。其次,现在很多电力网络系统仍存在系统风险,比如实际设备和系统台账连接失误,导致机密外泄,监管力度不到位,工作人员并没有担负起自己应尽的责任,最终导致电力监控系统出现非常多的网络安全问题。

### 三、电力监控系统网络安全防护技术的具体应用

#### (一)建立安全架构

电网运行是一个十分庞大的系统,必须建立足够安全的架构才能够保证运行的稳定性,更好地应对信息风险安全问题。技术人员应当明确电网运行的基本脉络和原理,在计算机网络安全管理过程当中并入电网的基本特征,以信息安全倒推电网系统管理办法,保证做好安全架构和信息防护工作。电网员工有时不能掌握计算机信息安全的相关技术,在日常操作过程中可能会因为误触病毒或其他原因而引发电网信息安全问题。且应当对基层员工进行基础的培训,提升在

长工作当中的信息安全防护意识。在员工入职之前,还需要签署保密协议明确日常行为和个人职位权限,杜绝因为人为原因造成的信息泄漏问题。有一些网络科技发展较为成熟的企业,电网也可以与其合作共同开发电网运行专有的网络安全架构体系,借助更加成熟先进的计算机手段,做好信息保障工作。

#### (二)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。入侵检测技术同其他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。

#### (三)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证书,全方位满足防护工作的安全需求,严禁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。

#### 结束语

总之,加强对于电力系统信息网络的风险分析和安防防护,是提高电力系统供电效率和供电品质的关键。电力企业应该建立安全架构、强化入侵检测技术、加强外设管理,以更加全面的角度来对电力系统信息网络提供保障,进一步促进我国电力行业信息技术的发展。

#### 参考文献

- [1]杨浩,陈宝靖,李燕.电力监控系统网络安全防护技术应用研究[J].电子世界,2021(1):2.
- [2]张同伟,刘永琦.电力系统信息网络安全防护及措施研究[J].网络安全技术与应用,2020, No.240(12):137-138.
- [3]孟庆东,李满坡,安天瑜,等.电力监控系统网络安全管理平台设计与实现[J].实验技术与管理,2020,37(7):6.