电力监控系统网络安全监测的改进与优化

邵春林
浙江浙能华光潭水力发电有限公司　浙江　杭州　311300

摘　要：随着生产管理信息化、移动化建设发展，为提高生产管理便捷性，同时部分信息需要在互联网进行发布，用户通过互联网进行查看，访问内部特定资源，需要与互联网进行数据信息交互。内外网之间需要有严格的安全防护措施，防止内部网络遭受来自外部互联网的网络攻击，部署在互联网上的外网应用也应具备防御来自互联网攻击的能力。

关键词：电力监控系统；网络安全；监测优化

引言

电力设施在基础设施中占据着重要地位。通过计算机对电力系统进行监控，对于维护动力系统的安全平稳运转意义重要。受诸多因素影响，电力监控系统存在运行不畅的不良状况，无法对安全防护软件进行有效安装，甚至难以对各项操作系统進行更新升级，极易导致安全隐患。对此，电力企业要剖析电力监控系统网络安全监测现状，采取有效的改进措施，规避各类安全隐患，从而确保了电力系统的正常安全工作。

1 电力监控系统的含义及其重要性

1.1 电力监控系统

为了保证电网控制系统的平稳工作，以通讯设施、计算机和检测与管理仪器为依据，研制和实现的一个监控装置。该平台减少了检测与管理成本，大大提高了能量转换的效能，同时有助于电网中减少能量孤岛，为获取与远程控制电力设施和供电系统的运行信息创造一个基本平台。

1.2 该系统网络安全方面的重要性

因为用电监控系统对电能产品的稳定性和品质都有直接影响，其工作的稳定性也对于供电方而言逐渐变得更为重要[1]。电网监控系统装置中的通信与装置形成了统一网络，其网络的稳定性直接制约着其监视与管理的精度，也可能造成电网信息系统的安全性下降。为避免此类现象在实际工作中存在，所以要加大电网监管体系和安全监测体系的建立工作。

2 电力监控系统网络安防原则

国家对电力监控安防系统提出的总体方案中明确指出，电力监控安防系统应按照安全分区的原则，实行联网专用，确保横向隔离，强化纵向认证。当前，国家电力企业越来越注重和逐步强化网络安全保护，网络与安全的工作行稳致远。为防止出现网络与安全事件，维护安全良好的供电和正常安全的电力供应，必须做好供电监控系统网络安全，具体要遵循如下原则：（1）对电力监控安防系统进行良好构建电力企业应契合自身实际，综合考虑信息安全需要，对电力监控安防系统进行良好构建，加强网络安全防护，并实施一体化的监督管理。调度部门要对网络安全防护的具体实施方案进行严格审查，并在正式投运电力监控系统前，对各项环节进行严格验收，保障系统运行后保持稳定高效的运行效果。另外，要优化联网，与工厂实现协同工作，提升联防工作水平。(2)对现有装置做好全面自查，修补系统漏洞。电力企业应遵循相关法律法规，通过确保安全防护设施对电厂进行安全覆盖，并经常对现有设施进行全面自查，对系统出现的缺陷作出及时合理的补救。

3 网络安全监测的主要功能

3.1 监测对象与监测方式

根据中国电力行业的安全防范工作按照"安全分区、网络专用、横向隔离、纵向认证"的原则，目前安全检测设备最主要的检测对象是服务器、工作站、数据库系统、网络设备、防火墙、正反方向的隔离设备、纵向加密、反病毒攻击侦测系统，同时还能够对除资产设备以外的所有监控范围进行信息收集，还能够对企业自身的内部数据进行监控[2]。控制方法是:通过与主机、工作站等设备通讯并使用消息总线以及基于TCP的私有协议，完成对上述装置的数据收集和命令管理，并通过本地图形化用户界面对网络安全控制设备实施管理。

3.2 数据采集

网络安全监控设备主要用于对服务器、工作站、网络设备、网络安全保护设备等的监控数据进行信息收集，主要包含:（1）服务器、工作站:客户注册信息、使用行为信息、网络信息、系统配置信息、用户变更信息、系统设置信息、系统运行信息、操作系统运行信

息、外设连接信息、系统核查指令信息。（2）网络设备:局域网内交换机设备、连接交换机的活跃设备等网络设备拓扑信息、在线时长、CPU利用率、内存利用率、网口状态、网络连接情况等网络设备运行信息。（3）安全设备:有关设备及自身策略的安全事件、设置情况、及操作数据、设备运行资料。

3.3 数据分析

（1）对收集到的CPU使用率、存储器使用量、网口数量、用户注册情况等数据进行分类整理，依据结果判断能否产生新的上报情况。（2）对网络设备日志信息进行分析处理，提取出需要的事件信息。（3）生成外设接入事件、用户注册事件、危险操作事件、系统异常事件和上传事务。

3.4 服务代理

（1）远程调阅采集数据、上传事件信息等的数据功能，并能够通过时间时段、设备类别、事件级别、事件信息数量等的过滤手段进行调阅数据功能。（2）对被监测系统内的资产进行远程管理，包括资产信息的添加、删除、修改、查看等。（3）参数配置的远程管理，包括系统参数、通信参数及事件处理参数。（4）通过代理方式实现对服务器、工作站等设备基线核查、设备主动断网命令的调用。（5）采用代理方法完成对主机、工作站等系统的关键数据列表、危险操作设置参数、周期性的上报时间等数据的加载、撤销、更改、检测[3]。

4 电力监控系统结构

大多数的电力监控系统当中包含现场控制层、网络通讯层以及系统管理层，进而在每一部分当中都能够实现不同功能的应用效果，进而对整体电力系统形成集中的优化完善效果。但是如若达到最佳的电力能源应用效率的优化，则需要能够对现有结构进行优化，尤其是针对于管理层面当中的现场监控以及网络通讯等，需要进行全面的分层管理。这主要是基于在电力监控系统当中，网络通讯层整体处于承上启下的作用，能够在电力能源的运行过程当中将系统与现场之间进行紧密连接，保障相关信息数据能够实现更加良好的衔接传输。而在现场监控的分层当中，主要是基于显示功能的存在，能够对现场进行连接管理。系统管理层能够对整体电力监控系统进行全面的监管，并能够对其中存在的各项数据内容进行处理加工，一般多用于主控机下的软件数据等相关内容的处理。

5 电力通信系统对电网安全运行的主要作用

5.1 为自动化调度与实时监控提供了信息通道

目前，中国电网向智能化调度和实施监控等方面的发展，已是一种趋势。而智能化调度系统中一旦需要对电网的运营状况实施调节工作，就需要借助监测系统来对电网当前的运营状况做出掌握与分析，而在实时监测和智能化调度系统之间的信号传输，又需要依赖于电力通信控制系统来实现。电力通信技术为自动调度系统和实时监测系统创造了双向通道的数据交换途径，这样可以促进自动调度对电网的安全稳定工作作出更为准确的评估。

5.2 提供高质量、高可靠性的保护传输通道

对继电器系统来说，关系其操作安全性最关键的方面便是对继电保护系统的正确操作和快速切断，而这些正确操作和快速切断都是需要以用电数据作为操作基础的，这就导致了用电数据传递和继电器保护装置系统的安全变成了一个关键课题，而电力通信设备所提供的通信通道则恰好可以保证为继电器系统创造一条高质量、高可靠性的安全数据传输路径[4]。

5.3 紧急情况下电力通信系统保证了通信通道的可靠性

对供电系统来说其发生紧急情况的几率是很大的，但在以往许多时候情况下不但会导致电力供应停止还会导致通讯系统发生故障，这将导致事件处置人员和供电调度指挥之间的信息沟通存在问题，很可能会耽误事件的处置时机，而且在中国的供电发展史上因为通讯中断还出现了对整个供电体系的稳定性产生负面影响，或者是供电体系直接瓦解的重大事故。

6 电力监控系统网络安全监测的改进措施

6.1 对网络信息安全加强体系建设和组织管理

电力企业应针对网络信息安全加强体系建设和组织管理。电力企业要加深对信息安全的认识，并高度重视信息安全工作，剖析企业现状和潜在风险，加强企业的组织领导，遵循相关法律，严格落实专项经费使用，强化网络信息安全管理，将其作为评估考核生产安全的重要内容，保障对相关责任的有效落实。另外，电力企业应根据相关防护规定、评估规范，遵循上级的统一部署，契合自身实际情况，对安全防护方案进行科学制定，实现对安全防护的有效加强。

6.2 对安防系统实施规范管理并加强安全等级保护

电力企业对生产安全系统实施标准化管理并做好安全等级防护，具体可从以下方面着手：从整体上对安防机制进行加强，以防止因生产保护系统漏洞而引发的重大安全风险；在生产管理大区上要对外部访问严格限制，以确保内部数据的机密性与完整性；对上网用户加强了身份核实，并禁止一个服务器同时对不同网络段地

址进行布置；对各安全区相应的数据段进行了横向分隔，并据此对电力调度网涉及的数据传输设备和其他系统功能进行了物理分隔，将安全分隔功能重点安排在企业管理和经营的安全大区，并采用了正向型和反向型二种网络分隔方法，对各种分离功能加以了划分。

6.3 加强基础设施建设和人才队伍培养

电力企业要做好基础设施建设和管理人才队伍培训工作，储备网络安全管理的专业人才，对各种工作规定和有关操作细则加以规定，举办安全技术培训，从总体上提高职工的网络安全意识。要通过制定安全应急预案、科学编写和严格审核处理方案，定期组织员工开展安全应急演习，增强员工抵御信息安全入侵和恶意攻击的能力，确保对安全事件实施高效良好的应急处理[5]。要督促引导维护人员树立良好的安全意识，并增强责任心，在开展网络安全维护的实践过程中，要合理安排调遣专职技术人员和管理人员，严格落实执行各项技术和管理措施。电力企业要对维护人员组织定期培训和绩效考核，为改进网络安全监测提供强有力的人力资源支持。

6.4 完善体制

贯彻地方和国家标准有关等级防护的规定，应用安全评价标准，开展分类和归档的性能维修。开展电力监控系统的生命周期优化和系统安全控制的标准化，加强系统全过程控制，按照安全需求，经常对各种业务连接开展安全性检查。建立了考核制度，对电力系统保安实施闭环管理[1]。要强化保安系统装备的规范要求，对安全设备配置、内网控制设备的使用以及事故处置要求进行严格规范。

6.5 加大整治力度

鼓励企业积极开展并网工程启动审核前的质量安全自评与审查工作，加强对发电机组开工前的引导，并配备全新的或更新的性能检测系统。不断完善建设部门提交的信息内容，包括基础设施使用信息和基础设施安全性评价报告，运营和维修单位在连接互联网前要进行检测。明确规定和履行了技术监管责任，督促和引导并网作业人员严格依照国家安全规定进行具体工作。特别是审查国家安全防护工作的实施状况，健全督导检查和工作制度，及时发现潜在和已出现的问题，并按照实际状况、国家政策和行业管理规定，积极主动地提出整改计划。

6.6 管理设备入网接入

加强了准入安全扫描力度，有效防止不符合规定的装置和系统投入使用，从而有效提升了安全。为了使所有设备都连接到每个接入网络中，由系统的使用部门起草了连接请求，经信息中心审核通过并发出方式单，以便于防止审核失败[2]。对于优化安全设备的市场准入，尤其是垂直加密和隔离的技术设备，信息中心必须根据各个方面的情况，认真审核其操作和管理单位规定的市场准入要求。

6.7 制订安全防护方案

按照《关于发电企业电力监控系统安全防护工作要求的通知》，认真做好了发电企业的用电监测系统的安全保护管理工作。首先，项目在最前期的评估阶段，按照"安全分区，网络专用，横向隔离，纵向认证"的基本原则，要求发电公司在分区设置并接入了相应的加密验证设备、物理隔离装置、防火墙等关键的安全设备。第二，主厂站专门对该系统进行了联合测试，在运行结束后进行了现场测试验证，并严格限制完全通过的验证程序。三，配置侵入监测系统。所有系统的二级网络必须主动配置侵入监测系统，完成对数据网数据的全监测，及时发现侵入情况。并根据在其他领域需要建立的网络安全管理体系，确定网络安全控制措施和安全责任人，并建立网络安全事故应急预案，同时还必须开展定期的演练。

结语

随着现代科学技术的发展，电力监控系统的安全性也逐步得以改善，进而推动着中国电力工业现代化发展的步伐。由于电力监控系统的使用具有一些安全隐患，所以完善系统管理和提高安全质量十分关键。它也对动态不断的监视和管理，执行法规和确定的安全策略以及合理实施有关措施和法律必不可少。应根据整合管理基础知识、现代电力系统建设规范等的要求，与技术控制、安全监测系统的维护、技术训练与管理等一并进行，以适应现代供电建设需要。

参考文献

[1]赵志宏.电力监控系统网络安全防护探讨[J].科技风,2021 (13):195-196.

[2]李勤琴.电力监控系统网络安全防护探讨[J].数码设计(上), 2021,10(1):39-40.

[3]安树勇,冉德旺,袁玮佳.攻击视角下的电力监控系统终端安全防护[J].电力信息与通信技术,2021,19(7):40-46.

[4]陶文伟,梁志宏,吴金宇,等.等保2.0下的电力监控系统安全运行环境设计[J].电气自动化,2021,43(3):89-91+104.

[5]吴程楠,李曼,田茜.地区电力监控系统安全技术及其应用[J].电力与能源,2021,42(1):51-55.