电力行业网络安全风险评估体系构建研究

刘晋兵
大唐山西电力工程有限公司，中国·山西 太原 030032

摘　要：伴随信息技术的迅猛发展，作为国家关键基础设施，其网络安全的风险日益显著暴露，论文归纳了电力行业网络安全风险的不同类型，涉及技术、管理和法律三个层面范畴，又对电力行业的特点加以分析，搭建起电力行业网络安全风险评估的指标体系，明确指标体系构建的原则及所含内容，包含技术、管理与法律范畴指标，且对指标权重分配及量化途径进行了相关探讨，借助论文展开的探究，意在为电力行业网络安全风险的评估与管理提供科学且系统的参考支撑，以保证电力系统的安稳可靠运行。

关键词：电力行业；网络安全风险；评估指标体系；技术指标；管理指标；法律指标

Research on the Construction of Network Security Risk Assessment System in the Power Industry

Jinbing Liu
Datang Shanxi Electric Power Engineering Co., Ltd., Taiyuan, Shanxi, 030032, China

Abstract: With the rapid development of information technology, as a key infrastructure of the country, the risks of network security are increasingly exposed. This paper summarizes the different types of network security risks in the power industry, involving three levels of technology, management, and law. It also analyzes the characteristics of the power industry, establishes an indicator system for network security risk assessment in the power industry, clarifies the principles and contents of the indicator system construction, including technical, management, and legal indicators, and explores the allocation and quantification of indicator weights. With the help of the exploration in this paper, it aims to provide scientific and systematic reference support for the assessment and management of network security risks in the power industry, in order to ensure the stable and reliable operation of the power system.

Keywords: power industry; network security risks; evaluation index system; technical indicators; management indicators; legal indicators

0 前言

面对数字化时代这样的背景，电力行业身为国家关键基础设施的重要一环，其网络安全问题得到了空前的重视，国家安全和社会稳定，同电力系统的稳定运行紧密相连，对电力行业网络安全风险进行深度钻研意义重大。

1 电力行业网络安全风险概述

1.1 网络安全风险类型

面临数字化浪潮的汹涌席卷，电力行业所面临的网络安全风险愈发复杂又严峻，网络攻击属于极为普遍且极具危险性的风险类型，黑客或许会借助恶意软件、网络钓鱼之类的手段，企图突破大唐发电企业的网络壁垒，妄图窃取关键电力生产数据、客户详情及商业机密。以精心炮制的网络钓鱼邮件，哄骗企业员工点击不良链接，继而在企业内部网络植入相关木马，实现对系统的远程支配及数据盗取，恶意软件同样构成了一大隐患，譬如勒索病毒，若企业的计算机系统遭感染，会把重要数据进行加密处理，进而向企业敲诈高额赎金，极大影响了电力生产的正常有序运行，甚至有引发生产中断的风险。拒绝服务攻击（DoS）与分布式拒绝服务攻击（DDoS）不可忽视，该类攻击向大唐发电企业的网络服务器发送数量庞大的请求，难以正常开展服务工作，进而对电力调度、交易等关键业务的开展产生干扰，网络通信为电力行业所高度倚重，不法分子也许会利用通信网络存在的安全漏洞，擅自篡改电力传输命令，对电力系统稳定运行造成干扰，对电力供应可靠性产生极大负面影响。

1.2 电力行业特点

大唐发电涉及的电力行业展现出不少鲜明特质，从经济规模层面看，电力行业的资产规模极为庞大，在国民经济体系里起着关键作用，身为行业重要参与者的大唐发电，其生产经营的状态直接和区域乃至全国的电力供应与经济发展挂钩，电力生产体现同步运作和不可贮存的属性，瞬间完成电能的生产、传输、分配与消费工作，这要求大唐发电企业的各生产环节应紧密配合、高效实施作业，若有一个环节出现故障，皆可能诱发连锁状况，危及电力的稳定供应状态。电力行业呈现出高度的集中特性，大唐发电企业需依照统一调度及管理标准开展工作，为保障电网的安全稳定运转，从服务这个维度，电力行业服务对象涵盖面广，牵扯全社会各个范畴、各类人群，大唐发电企业给出的电能质量、电价

高低等，跟大量电力用户的利益紧密挂钩。电力行业呈现先行属性，成为国民经济发展的基石与动力源头，大唐发电企业发展的步伐需跟经济增长需求相吻合，甚至要适度超前一步，方可为经济社会的发展筑牢坚实后盾，电力行业体现出技术密集型，持续的技术革新与升级，是大唐发电企业提升生产效益、保障电力可靠、实现可持续发展的核心驱动力。

2 电力行业网络安全风险评估指标体系构建

2.1 指标体系构建原则

构建电力行业网络安全风险评估指标体系，对大唐发电企业维持电力系统安全稳定运转意义重大，需依从以下原则，最初采用科学性原则，选取指标应参照电力行业网络安全的客观规律与大唐发电企业实际运营情形，保证评估结果切实可靠，精准呈现网络安全风险情形。根据系统性原则，需全面覆盖网络安全风险的层面，涉及网络攻击、通信漏洞、数据安全等范畴，同时考量大唐发电企业电力生产、传输、分配及消费全流程间的网络安全关联，杜绝指标遗漏现象，可操作性原则表明，指标的数据获取要方便，量化计算应简易，与大唐发电企业现有的技术水准和管理能力相契合，保证评估工作实现高效开展。动态性原则因网络安全环境持续更迭而设，指标体系要跟上时代节奏，及时增添新型风险要素，符合大唐发电企业网络安全防护的动态需求形势，针对性原则要求紧密围绕大唐发电企业于电力行业的特殊地位及业务特点来实施，着重体现与企业资产规模宏大、生产同时性及不可存储特性相关的风险指标，为企业定制贴合实际的网络安全风险评估方案，助力大唐发电企业增进网络安全防护实力。以先前所述原则为基础，也需遵循指标彼此独立原则，各指标之间应杜绝信息的重叠现象，要让每个指标都能独自反映特定维度的网络安全风险，增进评估的准确性及有效性，重要性原则同样不可或缺其意义，要按照风险发生的概率与可能造成的损失量级，为指标划分权重比例，突显关键的风险成分，使企业可集中资源优先处理高风险部分，依据兼容性原则，指标体系需与大唐发电企业当下的管理体系、技术标准和安全规范相契合，有利于和其他安全管理工作协同实施，实现网络安全风险评估与企业整体安全管理的和谐相融，着实增强企业网络安全防护实力。

2.2 指标体系内容

2.2.1 技术指标

从终端接入这一维度，企业的发电设备种类五花八门，如各类别的传感器、智能电表等，且数量达到庞大规模，部分老旧的终端防护能力不达标，易沦为网络攻击的进攻缺口，故而应着重考察终端加密认证机制有效性，实现接入的安全保障，系统及设备漏洞相关事宜，发电控制、监测系统及服务器等或许存在高危漏洞，恰似操作系统未做到及时更新补丁，极易被黑客钻空子，应当设置漏洞检测及持续更新相关检测指标。数据传输安全同样不可掉以轻心，发电进程中牵扯到大量实时数据传输，诸如电量、电压的关键数据，若数据出现泄露或被恶意篡改，将对发电生产造成重大冲击，所以得评价数据加密传输、完整性校验等举措是否实施恰当，在通信安全这个维度，碰到诸如 DDoS 攻击、虚假数据注入这般的威胁，能引起通信中断以及指令错误，需设定针对此类攻击的防护指标。恶意与勒索软件的防护也是核心点，应搭建完备的勒索软件清单库，实施数据的分级访问、备份及加密操作，防范数据被窃取和加密之虞，以此全面构建技术范畴的网络安全风险评估指标，维持发电业务稳定进行，就终端安全防护这一领域而言，需留意终端设备抵御恶意代码侵害的能力，查验是否拥有有效的病毒查杀及恶意进程拦截本领，抵御恶意软件对控制系统的入侵。就网络边界防护事宜，要对防火墙、入侵检测与防御系统的部署及配置情况展开评估，判定其是否可精确识别并阻挡非法的网络访问，就身份与访问管理这一工作，要设置如多因素认证强度、权限最小化分配等相关指标，保证只有得到授权的人员和设备可访问敏感资源，为应对突然降临的安全事件，还应设定应急响应相关指标，审视安全事件应急预案的完整性、演练频率以及响应的时间效果，保证遭受网络攻击后可迅速让系统恢复运行，进一步夯实技术指标体系的全面性和有效性根基。

2.2.2 管理指标

管理指标对大唐发电企业网络安全保障起着关键支撑作用，就安全管理制度相关方面，必须拥有完备的网络安全策略、人员权限管理规定以及应急处理预案等，就像明确不同岗位人员在发电数据上的访问权限，防止权限滥用引发的数据泄露现象，人员安全意识及培训举足轻重，员工成为网络安全的第一道防护壁垒，定期实施网络安全培训工作，提高员工对于钓鱼邮件、社交工程攻击等常见网络威胁的辨别能力，降低因人员粗心带来的安全事故概率。平时开展运维管理的时候，须打造严格的设备巡检体系，定期对发电设备与网络设备开展检查维护工作，及时揪出潜藏的安全隐患；与此同时规范运维操作的流程，防止因操作出错影响系统安全性，安全审计及监控绝不可缺，依靠部署审计系统，实时开展对网络活动、用户操作的监控与记录，以能及时察觉异常活动并追查根源，若监测到异常的数据访问请求，迅速触发告警机制。就供应商管理而言，应对涉及发电设备与软件系统等的供应商实施严格评估，保证其产品及服务具备安全特性，防止带入安全威胁，于管理各环节强化企业网络安全防护水平，在漏洞管理范畴，应建立常态化的漏洞扫描及修复体系，用专业工具对系统、设备开展全面的检测，若发现漏洞，要及时评估风险等级然后制定修复举措，保证漏洞管理实现闭环流程，灾难恢复管理同样不可忽视掉，要定期实施数据备份及恢复演练，维护发电业务数据的完整性及可用性，遇到重大安全事件时可迅速让系统恢复运行，从多个维度筑牢网络安全管理的基础。

2.2.3 法律指标

法律指标给大唐发电企业网络安全运营划出了合规边界，在落实合规制度方面，企业需严格依照国家出台的诸如《电力行业网络安全等级保护管理办法》等相关法规形式，按规定对发电网络的安全等级作出评定，进而落实对应的防护办法，数据保护及隐私法规的执行极为关键，发电企业掌握大量用户数据以及生产运营的关键敏感数据，应依照《中华人民共和国网络安全法》等法规的要求，将数据进行妥善的存储、传输与运用，阻止数据泄露对用户隐私的侵害。从知识产权保护这个层面看，企业靠自身研发的发电控制软件、监测系统等涉及知识产权范畴，应当根据法律规定实施有效保护，防止软件出现非法复制盗用现象，就法律责任与处罚的应对而言，企业要弄清楚违反网络安全相关法律的责任后果是啥，清晰掌握内部人员违规操作、外部侵权行为等可能面对的法律处罚情形，然后制定恰当的应对方式，紧盯法律法规的更新变化点，迅速对企业网络安全管理策略及措施进行调整，保证企业长久在法律框架里稳健发展，规避违法违规引发经济损失和声誉方面的损害。

2.3 指标权重分配

在针对大唐发电企业的网络安全风险评估指标体系里，指标权重分配应充分结合企业生产运营特点以及网络安全风险核心，技术指标与发电设备、系统及数据的安全运行直接相关，对保障发电业务连贯运行意义非凡，由此赋予 40% 的权重值；管理指标从制度、人员、运维等维度给网络安全以支撑，是抵御风险的关键支撑，赋予 35% 的权重；法律指标为企业网络安全运营划定了合规的基本边界，规避因违法违规产生的重大损失，占 25% 的比重。在技术指标范畴之内，鉴于发电设备终端数量庞大，防护能力差，技术指标里，终端接入安全的权重占比是 30%；系统及设备的漏洞对核心系统安全构成威胁，赋予 25% 的权重；通信安全权重达 15%，数据传输及恶意软件防护权重分别是 20%、10%。就管理指标方面说，安全管理制度跟人员安全意识培训的权重各占 30%，日常运维管理占比 25%，安全审计与监控占据了 10% 的比重，5% 的比重归属于供应商管理，就法律指标这一领域，合规制度遵循的权重为 40 个百分点，执行数据保护和隐私法规占了 30% 的比重，知识产权保护占据 20% 的比重，法律责任及处罚应对占比 10%，由此搭建起科学合理的权重架构。

2.4 指标量化方法

对于大唐发电企业网络安全风险评估指标实施量化，要采用有针对性的途径确保评估无误，从技术指标量化这一维度，以终端加密认证机制通过率、未授权接入次数等检测数据来量化终端接入安全；以漏洞扫描工具找出的高、中、低危漏洞数及修复率为标准评估系统与设备漏洞；用数据加密算法强度、完整性校验准确率等对数据传输安全进行衡量；通信安全的量化借助抵御 DDoS 攻击成功次数、虚假数据注入拦截率等指标达成；恶意软件防护的评估采用勒索软件检测率和数据备份恢复成功率指标。实施管理指标量化操作时，安全管理制度的评定借助制度完备性与执行检查合格率；用培训覆盖率、考核通过率衡量人员的安全意识与培训水平；日常运维管理根据设备巡检完成率与故障修复及时率进行量化；评估安全审计与监控，采用异常行为发现及时率、事件追溯成功率；判定供应商管理情况，依据供应商安全评估得分与问题整改率。于法律指标量化工作中，采用等级保护达标率、法规符合项占比评估合规制度遵循与否；数据保护及隐私法规执行情况，用量化数据泄露事件次数、隐私合规检查合格率体现；采用侵权事件发生率、软件版权登记完成率衡量知识产权保护情况；法律责任与处罚应对的评估借助法律风险识别率和预案有效性，由此实现对网络安全风险的精准数据化呈现。

3 结语

总之，网络安全风险评估在电力行业是复杂且重大的课题，依靠搭建科学、合理的评估指标体系，可高效辨别和评价电力行业面临的网络安全风险，为制定契合的风险防控举措提供凭据，跟着技术的逐步发展与电力行业安全需求的日益高涨，应持续更新、完善电力行业网络安全风险评估体系，以适应新衍生的挑战，电力行业得强化网络安全相关意识，增进网络安全管理水平，让电力系统实现安全稳定运行，为国家经济进步和社会安定添砖加瓦。

参考文献：

[1] 向英,韩玄.电力行业人工智能技术应用的网络安全风险分析[J].信息安全与通信保密,2023(10):67-74.

[2] 高正刚,雷翔,左宇翔.大数据背景下的智能电网信息安全防护[J].网络安全技术与应用,2021(12):114-116.

[3] 于斌.浅议IPv6规模部署下电力行业网络安全风险[J].中国新通信,2020,22(3):132-133.

[4] 卢英佳.我国电力信息系统面临的网络安全风险及处置建议[J].中国信息安全,2019(11):97-99.

[5] 王云海.电力行业网络安全现状及解决方案探讨[J].网络安全技术与应用,2013(9):67-68.

作者简介：刘晋兵（1982-），男，中国山西太原人，本科，工程师，从事信息通信技术、网络安全研究。