 DOI: https://doi.org/10.12345/dlynyqy.v3i4.26468

Information security strategy for large-scale power engineering data interaction platform

Zhenfang Wang

Henan Jiacheng Electric Co., Ltd., Zhengzhou, Henan, 450000, China

Abstract

With the acceleration of digital transformation in the power industry, the data interaction platform for power engineering is improving operational efficiency while also facing increasingly prominent information security threats. This paper focuses on the security risks of the data interaction platform for power engineering and constructs a multi-level security protection system from three dimensions: technology, management, and operations. It analyzes in detail the application paths of key technologies such as data encryption, access control mechanisms, intrusion detection, and defense systems, using specific power engineering cases. The paper summarizes the actual application effects and delves into strategies for information security management and operations, including establishing a safety management system, strengthening emergency response mechanisms, and continuously optimizing the security operation and maintenance system. By applying these technologies and implementing management strategies, the security protection capabilities of the data interaction platform for power engineering can be effectively enhanced, ensuring the stable operation of the power system.

Keywords

power engineering; data interaction platform; information security

面向大规模电力工程数据交互平台的信息安全策略

王振方

河南佳程电气有限公司，中国 · 河南 长葛 461500

摘　要

随着电力行业数字化转型的加速，电力工程数据交互平台在改善运营效率之际，也承受着日益凸显的信息安全威胁。本文立足于电力工程数据交互平台的安全风险，按照技术、管理和运维三个维度搭建多层次安全防护体系，结合具体电力工程案例着重剖析了数据加密技术、访问控制机制、入侵检测与防御系统等关键技术的应用途径，总结了实际应用效果。并深入剖析了建设安全管理制度、强化应急响应机制以及持续优化安全运维体系等信息安全管理与运维策略。通过应用上述技术及落实管理策略，可有效增进电力工程数据交互平台的安全防护能力，实现电力系统的稳定运转。

关键词

电力工程；数据交互平台；信息安全

1 引言

伴随智能电网建设的逐步深入及电力行业数字化转型的加速，大规模电力工程数据交互平台已成为电力系统运行不可或缺的组成部分，这些平台达成了发电、输电、配电、用电各环节数据的实时采集、转送与处理，为电力系统的智能化决策提供数据作为支撑。平台规模的拓展与数据交互频次的提升同样引发了严峻的信息安全难题，电力系统作为国家核心基础配套设施，其信息安全直接关联到国民经济及社会稳定，针对电力系统的网络攻击事件不断涌现，对电力安全带来了极大威胁，本文聚焦于研究面向大规模电力工程数据交互平台的信息安全策略，在维持平台功能完整性的同时，核心提升其安全防护实力。

【作者简介】王振方（1990–），男，中国河南长葛人，本科，技术总工，从事电力工程研究。

2 电力工程数据交互平台的安全风险分析

2.1 技术风险

作为电力系统的神经中枢，那便是电力工程数据交互平台，面临着多样化的安全隐患，站在技术层面审视，平台在数据的传输、存储与处理阶段，易受到中间人攻击、数据篡改、拒绝服务攻击等威胁，攻击者可能将网络协议的漏洞、加密算法的弱点及系统配置的缺陷作为进攻的突破口，尤其是在呈现广域分布的电力监控系统内，数据传输一般要跨越多个网络节点，大幅增添了数据泄露以及被篡改的风险 [1]。

2.2 管理风险

就管理层面加以分析，电力企业普遍显现出安全意识薄弱、安全管理制度不规范等问题，员工安全操作规范不足、权限管理混乱不堪、第三方接入管控不严格等情形时有显

现，和技术漏洞相比，这些管理漏洞更易被人利用，而且造成的后果一样惨重，伴随电力系统跟其他行业互联互通规模的增长，数据共享时，安全责任的界定及管控面临新的挑战。

2.3 运维风险

运维相关的风险同样不可漠然视之，系统日志分析未能及时开展、安全事件响应迟缓、补丁更新滞后等，均会降低平台整体安全防护能力，由电力系统连续运行特性可知，安全运维要实现实时性及高效性，任何延误都或许会造成严重后果，伴着新型攻击手段陆续涌现，传统的安全防护举措可能无法及时招架，这要求安全运维务必要有快速适应及升级的能力。

3 信息安全技术防护策略

3.1 数据加密技术

作为保障电力工程数据交互平台安全的基础措施，是数据加密技术，就传输中的数据而言，可运用如 AES - 256 这类高强度加密算法，并结合 SSL/TLS 协议，使数据在传输阶段不被窃取或任意篡改，针对数据存储的情形，除了进行全盘加密处理外，也应采用字段级加密办法，对敏感数据给予额外庇护，加密系统的核心是做好密钥管理，需构建完善的密钥生成、分发、轮换及销毁的机制，推荐借助硬件安全模块 (HSM) 保障密钥安全 [2]。

某大型电力公司采用了基于 AES（也就是 Advanced Encryption Standard，基于高级加密标准算法的数据加密办法，对电力工程数据采取加密保护手段，当数据开展交互的时候，借助 SSL/TLS（Secure Sockets Layer/Transport Layer Security，以安全套接字层 / 传输层安全协议对数据传输做加密处理，保障数据在传输阶段的安全。在进行数据存储阶段，采用 AES 加密方法处理电力工程数据，由硬件安全模块（HSM）来开展密钥管理工作，守护数据于存储阶段的安全，针对用户的不同层级，采用角色基访问控制（RBAC）这一技术手段，限定用户针对数据的访问权限，阻止非法的访问行径。

某智能电网数据交互平台采用的一种是基于 RSA（Rivest - Shamir - Adleman，采用 RSA（Rivest - Shamir - Adleman）公钥加密算法实施的数据加密技术，实现电力工程数据的安全传送与存储。在数据传送期间，采用 RSA 公钥加密法对数据加密，保证数据传输过程中的安全系数，在数据存储这一环节，采用 AES 算法对电力工程数据做加密处理，依靠 HSM 管理密钥，保障数据在存储期间的安全性，按照用户的不同层级，采纳基于属性的访问控制（ABAC）技术，将用户属性、资源属性及操作属性相结合，实现细微化的访问管制。

依靠以上案例考察，采用一系列加密算法，比如 AES、RSA 之类，保障数据在传输与存储环节的安全性，把 SSL/TLS、HSM 等安全技术跟设备联合起来，增强数据加密的安全水平，采用访问限制控制技术，限定用户针对数据的访问权限，防范非正当访问，着眼不同档次的用户及资源，实现精细度高的访问管控，提高数据安全保障水平。

3.2 访问控制机制

访问控制机制是阻止未授权访问的重要技术手段，基于角色的访问控制（RBAC）模型贴合电力工程数据交互平台的组织结构特点，可按照岗位工作责任分配权限，属性基访问控制（ABAC）模型若有更细的粒度，就能结合用户属性、资源属性、环境因素等进行动态权限判断，多因素认证（MFA）宜作为平台访问的标准设置，尤其是针对关键操作以及管理功能，像 VLAN 划分、防火墙策略配置等网络隔离技术，可切实限制横向移动，减少受攻击的范畴 [3]。

某大型电力工程的相关数据交互平台采用 B/S 架构，分为前端显示层、业务逻辑层、数据访问层，前端展示层承担展示用户界面的工作；业务逻辑层承担处理用户请求的工作，达成数据彼此的交互；数据访问层承担着数据的存储与读取工作，平台采纳基于角色的访问控制（RBAC）模式，用户需借助用户名和密码完成认证。待认证成功实现后，系统依据用户角色赋予合适的权限，平台把用户按不同角色归类，若如管理员、工程师、监理等角色，各角色对应着不一样的权限，诸如数据查看、数据更新、数据去除等，管理员握有顶级的权限，具备管理所有用户及角色的权限，平台对用户操作做审计检查，记录用户登录、操作时间以及操作类型等内容，若出现异常操作情况，系统即刻自动发出警报，利于管理员及时发觉与处置。

该平台进行权限分配操作中，未充分顾及实际业务需求，造成部分用户权限超出正常水平，存有安全相关的潜在隐患，平台仅仅采用用户名和密码实施认证，安全系数偏低，平台仅对操作时间、操作类型等相关信息做记录，未对操作前后的数据变化加以记录，阻碍了问题追踪的进行。相关人员按照实际业务情形，对用户权限做进一步细化，实现最小权限的相关原则，工程师角色可查看、编辑相关数据，可无法进行数据删除操作，引入多要素认证机制，诸如短信验证码、动态认证令牌等，增强用户认证的安全水平，记载操作前后的数据变动，涵盖数据内容、操作时刻、操作主体等详情，利于开展问题的追踪溯源，利用第三方的安全审计手段，定期对平台开展安全检查，及时探知并消除安全弊病，经由优化权限分发、引入多因子验证、完善操作审计等途径，有效增强了平台的安全性级，推动电力工程数据交互顺利实施。

3.3 入侵检测与防御系统

平台安全监测依靠的重要技术手段有入侵检测与防御系统（IDS/IPS），基于特征的检测可鉴别出已知攻击模式，而基于异常的检测能辅助发现新型攻击，处于电力工程的环境里，提议布置专门针对工业控制协议的深度包检测引擎，安全信息和事件管理（SIEM）系统能实现日志集中收集、

关联分析及即时警报，支持安全团队迅速发现与响应安全事件，与威胁情报平台相结合，可预先对潜在攻击告警，强化主动防御水平 [4]。

某大型电力工程牵涉多个地区，频繁进行数据交互，对数据安全性与可靠性要求达到极高水平，为守护电力工程数据交互平台的安全防线，该公司选择采用入侵检测与防御系统（Intrusion Detection and Prevention System，简称为 IDPS）以抵御潜在安全威胁。对电力工程数据交互平台的关键节点实施 IDPS 部署，做到实时监控与攻击行为甄别，基于已有的 IDPS 基础，实施 IPS 部署，对恶意流量实施实时拦截，结合电力工程数据交互平台的特性，制定契合的安全策略，好比采取访问控制、采取数据加密等，按时为 IDPS 和 IPS 的病毒库及恶意代码库进行更新，增强抵御实力，对员工进行安全意识相关培训，培养员工对安全问题的觉察，降低人为差错造成的安全风险。

采用 IDPS 和 IPS 进行部署，攻击检测率急剧攀升，切实降低了攻击行为对数据交互平台造成的影响，采用多层次的安全防护办法，数据安全性实现有效防护，未产生数据泄露方面的事故，实施安全加固措施后，系统稳定性得到进一步提高，运行阶段未出现因安全漏洞引起的问题，采用安全意识培训方式，员工对安全问题的认识得到了强化，减少了人为差错引发的安全风险，依靠部署入侵检测及防御系统，该大型电力工程数据交互平台的信息安全得到有效守护，为电力工程搭建了稳定、可靠的数据交互环境基础。

4 信息安全管理与运维策略

4.1 完善安全管理制度

成熟的安全管理制度是技术措施有效推进的基础后盾，电力企业需设立覆盖数据全生命周期的安全管理规程，弄清各类数据的分类分级标准及相应保护要求，制订严格的身份认证及权限管理规程，保证最小权限原则顺利落实，必须特别重视第三方接入管理事宜，构建供应商安全评估体系与合同约束条例，厘清安全责任的边界范围，按期开展安全意识教导，把信息安全融入员工绩效考核体系，造就全员普遍参与的安全文化。

4.2 建立应急响应机制

应急响应机制的搭建对及时控制安全事件的影响意义重大，电力企业要制订细致的应急预案，厘清不同级别安全事件的处置流程及责任人，设立 7×24 小时持续值守的安全监控及响应团队，配置必要的技术工具，赋予相关处置权限，按计划开展应急演练，评判预案的可操作性强弱，不断精进响应流程，跟行业监管部门、其余电力企业与专业安全机构建立起信息共享和协作机制，提升整体应对水平，事件结束后需开展深度调查与剖析，总结经验跟教训，优化防护手段 [5]。

4.3 持续优化安全运维体系

安全运维体系不断优化是维系长期安全的关键，创建系统化的漏洞处理流程，按时开展安全评估及渗透检测，迅速找出并排除安全的隐患点，补丁管理得平衡安全需求跟系统稳定性，关键系统补丁必须充分测试后及时付诸应用，配置管理数据库（CMDB）须维持数据精确并及时更新，为安全决策给出可靠参考，运维操作应全程留下痕迹，做到可追溯效果，伴随新技术与新应用的引入，应迅速调整安全运维策略，保证适应新的安全情形。

5 结论

传统安全措施无法有效应对电力系统面临的复杂安全威胁，应采用综合治理的思路，技术手段是安全防护的根基，但有效实施它离不开完善的管理制度的保障，电力企业要结合自身禀赋，恰当分配资源，设立恰当的安全防护体系，伴着 5G、物联网、人工智能等新技术在电力系统的大量应用，数据交互平台将面临更错综的安全环境挑战，安全策略需不断推陈出新，符合新技术引起的变化，探索应用零信任架构、自适应安全模型等新理念于电力工程数据交互平台是值得的，为智能电网建设构建坚实的安全壁垒。

参考文献

[1] 谭澍林.“互联网+大数据”助力电力工程安全管理水平提升[J].现代职业安全,2024,(12):33-35.

[2] 赵雨塑.基于蚁群算法的电力工程数据管理控制方法研究[J].电气技术与经济,2024,(11):81-83.

[3] 杨鸿.大数据时代电力工程电子档案安全管理措施[J].办公室业务,2024,(18):93-95.

[4] 王楠,周鑫,周云浩,等.基于改进SVM算法的电力工程异常数据检测方法设计[J].电子设计工程,2024,32(04):162-166.

[5] 罗仲达,李容嵩,彭凌烟,等.基于区块链和CP-ABE的电力工程检测数据安全共享方法[J].电力信息与通信技术,2023,21(03):80-86.