能源电站信息采集控制系统中的数据隐私保护机制

陈小姿[1] 牟 昊[2]
1. 中晟智慧能源科技（浙江）有限公司 浙江 杭州 310000
2. 猎日集团有限公司 浙江 台州 318000

摘 要：随着全球能源产业的飞速发展，能源电站作为能源供应的关键枢纽，其信息采集控制系统的重要性日益凸显。能源电站信息采集控制系统收集了大量设备运行、用户用能等多方面的数据，这些数据不仅关系到电站的高效运行，也涉及到诸多隐私信息。然而，当前能源电站信息采集控制系统在数据隐私保护方面存在明显问题。一方面，数据在采集、传输、存储和处理的各个环节缺乏有效的安全防护措施，容易导致数据泄露；另一方面，对于数据的访问控制和权限管理不够严格，使得敏感数据面临被非法获取和滥用的风险。基于此，本文针对能源电站信息采集控制系统中的数据隐私保护机制展开深入分析。综合运用密码学、访问控制等技术理论，结合能源电站数据的特点和实际运行需求，设计全面且有效的数据隐私保护机制。涵盖数据采集、传输、存储与处理等各个阶段，构建合理的评估指标体系对保护机制进行评估，并提出改进措施。本文以期达到切实保护能源电站数据隐私，提升系统安全性和可靠性，为能源电站的稳定运行和能源产业的健康发展提供有力保障的目的。

关键词：能源电站；信息采集控制系统；数据隐私保护；安全机制；访问控制

1 引言

在全球能源格局深刻变革、能源数字化进程加速推进的大背景下，能源电站作为能源生产与转换的核心场所，其信息采集控制系统发挥着至关重要的作用。该系统能够实时收集设备运行状态、能源生产与消耗数据等大量信息，为电站的智能化管理和高效运行提供有力支撑。然而，随着能源电站信息化程度的不断提高，数据隐私保护问题日益凸显。能源电站的数据不仅包含设备运行的关键参数，还涉及用户的能源使用习惯、地理位置等敏感隐私信息。一旦这些数据遭到泄露或非法使用，不仅会对用户的个人权益造成侵害，还可能影响能源电站的正常运营，甚至威胁到国家能源安全。目前，尽管在数据保护领域已取得一定进展，但针对能源电站信息采集控制系统的数据隐私保护仍存在诸多不足。现有的保护措施难以满足复杂多变的安全需求，数据隐私保护机制亟待完善。因此，深入研究能源电站信息采集控制系统的数据隐私保护机制，对于保障能源行业的安全稳定发展具有重要的现实意义。

2 能源电站信息采集控制系统数据特点分析

2.1 数据类型与来源

能源电站信息采集控制系统的数据类型丰富多样。从设备运行数据来看，包含发电设备的电压、电流、功率、温度、压力等参数，这些数据由安装在设备上的各类传感器实时采集，用于监测设备的工作状态和性能。输电线路数据则涵盖线路的电流、电压损耗、负载情况等，依靠线路上的监测装置获取。此外，还有能源消耗数据，涉及不同区域、不同用户的用能情况，通过智能电表等设备收集。环境数据如温度、湿度、风速等，对电站的运行和能源生产有影响，由环境监测设备提供。用户信息数据包括用户身份、联系方式、用能习惯等，来源于用户注册和用能过程中的记录[1]。这些不同类型的数据从多个渠道汇聚到信息采集控制系统中，共同为电站的运行管理提供支撑。

2.2 数据的重要性与敏感性分级

能源电站的数据具有不同的重要性和敏感性。关键设备的运行参数，如发电机组的核心性能数据，对于电站的安全稳定运行至关重要，一旦出现错误或丢失，可能导致设备故障甚至停机，影响能源供应，属于高度重要数据。同时，这些数据也涉及电站的核心技术和运营机密，敏感性极高。用户的个人身份信息、用能习惯等数据，关系到用户的隐私权益，敏感性也很强，若泄露可能导致用户权益受损。而一些环境数据和一般性的设备运行辅助数据，虽然对电站运行有一定参考作用，但重要性和敏感性相对较低。合理对数据进行重要性和敏感性分级，有助于针对性地制定数据隐私保护策略，确保关键和敏感数据得到有效保护。

2.3 数据在系统中的流动与处理过程

在能源电站信息采集控制系统中，数据从采集端开始流动。传感器等设备采集到原始数据后，通过网络传输至数据采集模块，该模块对数据进行初步的筛选、

过滤和格式转换。随后，数据被传输到数据处理中心，在这里进行深度分析和计算，如设备运行状态的评估、能源消耗的预测等。处理后的数据一部分存储在数据库中，用于历史数据查询和分析，另一部分根据不同的需求反馈给控制系统，用于设备的调节和控制，或者提供给管理人员进行决策支持。在整个数据流动和处理过程中，涉及多个环节和不同的系统组件，每个环节都存在数据泄露和被篡改的风险，因此需要对数据的全生命周期进行严格的隐私保护和安全管理。

3 数据隐私保护相关理论与技术基础

3.1 数据隐私保护的基本概念与原则

数据隐私保护旨在确保数据所有者的信息不被未经授权的访问、使用或披露。基本概念涵盖了个人隐私数据，如用户身份信息、健康记录、财务数据等，以及企业或组织的敏感数据，如商业机密、技术专利等。其核心原则包括保密性，即通过加密等手段防止数据泄露给非授权方；完整性，保证数据在传输和存储过程中不被篡改，维持数据的准确性和一致性；可用性，确保授权用户在需要时能够及时、可靠地访问数据[2]。此外，还有最小必要原则，即仅收集和处理为实现特定目的所必需的数据，避免过度收集导致的隐私风险。遵循这些概念和原则，能有效保障数据在各个环节的隐私安全，平衡数据利用和隐私保护之间的关系。

3.2 密码学技术在数据隐私保护中的应用

密码学技术是数据隐私保护的重要手段。对称加密算法，如AES（高级加密标准），加密和解密使用相同的密钥，运算速度快，适用于大量数据的加密存储和传输。非对称加密算法，像RSA算法，使用公钥加密、私钥解密，解决了密钥传输的安全性问题，常用于数字签名和密钥交换。哈希函数则能将任意长度的数据映射为固定长度的哈希值，常用于数据完整性验证，如文件的哈希校验可判断文件是否被篡改。同态加密技术允许在密文上进行计算，计算结果解密后与在明文上计算的结果相同，在不泄露数据内容的情况下实现数据处理，为数据隐私保护提供了更高级别的安全保障。

3.3 访问控制与权限管理理论

访问控制是保障数据隐私的关键机制，它规定了哪些主体（用户、程序等）可以对哪些客体（数据、资源等）进行何种操作。自主访问控制（DAC）允许数据所有者自主决定其他主体对其数据的访问权限，但存在权限滥用风险。强制访问控制（MAC）基于主体和客体的安全级别进行访问控制，更具严格性和安全性，常用于对安全要求极高的系统。基于角色的访问控制（RBAC）则根据用户在组织中的角色分配权限，简化了权限管理。权限管理理论强调对权限的精细划分、动态调整和审计，确保只有授权用户能访问相应数据，防止越权访问和权限泄露，有效保护数据隐私，维护系统安全稳定运行[3]。

4 能源电站数据隐私保护机制设计

4.1 数据采集阶段的隐私保护措施

在能源电站数据采集阶段，需采取多方面措施保护数据隐私。首先，对传感器等采集设备进行安全加固。通过设置强密码、定期更新固件等方式，防止设备被恶意入侵，避免采集数据被窃取或篡改。对于采集的数据，进行初步的匿名化处理。例如，在采集用户用电数据时，可将用户的身份标识用加密的随机代码代替，确保在数据采集源头就降低隐私泄露风险。同时，严格规范数据采集的范围和目的。依据最小必要原则，仅采集与电站运行管理直接相关的数据，避免过度采集用户的敏感信息。对采集设备的访问权限进行严格管理，只有经过授权的人员才能访问和配置采集设备，防止未经授权的人员获取采集数据。此外，建立数据采集日志记录机制，详细记录每次数据采集的时间、操作人员、采集数据的类型等信息，以便后续审计和追溯。

4.2 数据传输过程中的安全保障机制

数据在传输过程中面临着多种安全威胁，因此要构建完善的安全保障机制。采用加密传输协议，如SSL/TLS协议，对传输的数据进行加密处理，确保数据在传输过程中即使被截获也无法被读取。对于重要的数据，可采用多重加密的方式进一步增强安全性。设置安全的传输通道，对传输网络进行安全防护，如部署防火墙、入侵检测系统等，防止外部网络攻击和非法访问。在数据传输前，对数据进行完整性校验，生成校验码并随数据一同传输，接收端通过校验码验证数据的完整性，若发现数据被篡改则拒绝接收并重新请求传输[4]。同时，对传输过程中的数据流量进行监控，及时发现异常流量并采取相应措施，保障数据传输的安全稳定。

4.3 数据存储与处理时的隐私防护策略

在数据存储方面，选择安全可靠的存储设备和存储系统。对存储的数据进行加密存储，可采用对称加密或非对称加密算法，确保数据在存储介质上以密文形式存在。对存储设备的访问权限进行严格控制，设置不同的访问级别，只有授权人员才能访问存储的数据。在数据处理阶段，采用隐私保护的数据处理技术。如差分隐私技术，在数据中添加适量的噪声来保护个体数据的隐私，同时不影响数据的整体统计特性。对于涉及用户隐

私的数据处理，遵循严格的审批流程，确保处理目的合法合规。建立数据备份和恢复机制，定期对重要数据进行备份，并确保备份数据的安全存储，以便在数据遭遇丢失或损坏时能够及时恢复，保障数据的可用性和隐私安全。

5 数据隐私保护机制的评估与改进

5.1 评估指标体系的构建

构建科学合理的评估指标体系是衡量能源电站数据隐私保护机制有效性的关键。从保密性角度，设置数据加密强度指标，评估加密算法的安全性以及密钥管理的规范性，如密钥的生成、存储和更新方式是否符合安全标准。同时考量未授权访问率，通过模拟攻击等方式检测数据被非法获取的概率。在完整性方面，关注数据篡改检测率，评估系统能否及时发现数据在传输和存储过程中是否被篡改。建立数据一致性指标，检查不同存储位置或处理环节的数据是否保持一致。对于可用性，衡量数据访问成功率，确保授权用户能够顺利获取所需数据。同时考虑系统恢复时间，即数据遭遇安全事件后恢复正常使用的时长。此外，纳入合规性指标，评估保护机制是否符合国家法律法规和行业标准，以及用户权益保障指标，如用户对数据使用的知情权和控制权是否得到满足。

5.2 评估方法与流程

评估方法采用定量与定性相结合。定量方法包括利用工具对数据加密算法的性能进行测试，统计未授权访问、数据篡改等事件的发生次数，计算各项指标的具体数值。定性方法则通过专家评审、问卷调查等方式，收集用户和专业人员对数据隐私保护机制的主观评价，如对隐私政策的理解程度、对数据处理透明度的满意度等。评估流程首先是制定详细的评估计划，明确评估目的、范围和时间安排。接着进行数据收集，包括系统运行日志、安全检测报告、用户反馈等[5]。然后运用选定的评估方法对数据进行分析处理，得出各项指标的评估结果。最后撰写评估报告，总结评估发现，提出改进建议和措施。

5.3 基于评估结果的改进方向与措施

若评估结果显示保密性存在问题，可考虑升级加密算法，加强密钥管理，如采用更高级别的加密标准和多重密钥机制。对于未授权访问率较高的情况，强化访问控制措施，增加身份验证方式，如多因素认证。若完整性指标不达标，优化数据校验和监测机制，引入更先进的哈希算法和实时监测工具，及时发现并纠正数据篡改。针对可用性问题，完善系统备份和恢复策略，增加冗余存储设备，缩短系统恢复时间。在合规性和用户权益方面，根据法律法规的更新及时调整隐私政策，加强用户教育和沟通，确保用户清楚了解数据的使用方式和自身权益。持续跟踪评估结果，不断调整改进措施，以提升能源电站数据隐私保护机制的整体效能。

6 结语

本文围绕能源电站信息采集控制系统的数据隐私保护机制展开深入研究。剖析了系统数据特点，阐述相关理论技术，设计涵盖采集、传输、存储处理阶段的保护机制，构建评估体系并明确改进方向。研究成果对保障能源电站数据隐私、提升系统安全性意义重大。通过实施保护机制，能有效降低数据泄露与滥用风险，维护用户权益，保障电站稳定运行。然而，研究存在局限。能源电站场景复杂多样，保护机制的普适性需进一步验证；技术发展迅速，新的安全威胁不断涌现，现有机制可能无法完全应对。未来，需持续关注技术动态，深化对复杂场景下数据隐私保护的研究，完善保护机制，加强跨学科合作，提升能源电站数据隐私保护水平，助力能源行业安全健康发展。

参考文献

[1]张华贵,张俊萌.医院信息系统中的数据安全与隐私保护[J].电脑知识与技术,2024,20(18):67-69.

[2]孟庆.区块链技术在信息化数据安全保护中的应用[J].计算机应用文摘,2024,40(22):81-83+86.

[3]张龙.基于物联网技术的电厂信息化智能化监测与控制系统设计[J].通信电源技术,2024,41(8):10-12.

[4]杜金瑞,苑新.物联网中的数据安全与隐私保护[J].通信电源技术,2025,42(1):156-158.

[5]哈斯沐沦.用户数据分析与隐私保护策略在智慧广电系统中的应用[J].移动信息,2024,46(12):204-206.