智能电气自动化系统中的数据安全与隐私保护研究

姚云飞

410181198605157577

摘要：随着工业 4.0 的深度推进，智能电气自动化系统已成为现代工业生产与能源管理的核心支撑。该系统通过海量数据的采集、传输、存储与分析实现智能化决策，但数据在全生命周期中面临的泄露、篡改、窃取等安全风险，以及用户隐私信息泄露的隐患，严重制约了系统的健康发展。本文基于智能电气自动化系统的架构特性，深入剖析数据安全与隐私保护的核心痛点，梳理当前主流的防护技术，提出涵盖数据全生命周期的一体化防护策略，为提升智能电气自动化系统的数据安全防护能力提供理论参考与实践指引。

关键词：智能电气自动化；数据安全；隐私保护

DOI：10.69979/3060-8767.26.02.013

引言

在数字化转型浪潮下，智能电气自动化系统融合先进技术，广泛应用于关键领域。该系统打破传统信息孤岛，实现设备互联互通与协同调度，通过挖掘多维度数据提升生产效率等。但数据作为核心资产，在全生命周期面临诸多安全威胁，如工业控制系统受攻击、隐私信息泄露等。数据安全与隐私保护成行业焦点，虽学者有大量研究，但因系统架构复杂等因素，现有防护方案存在不足。因此，深入研究相关技术、构建防护体系意义重大。本文将从系统架构与数据特性出发，分析风险，梳理技术，提出策略并展望未来。

1 智能电气自动化系统架构与数据特性

1.1 系统架构

智能电气自动化系统采用分层架构设计，通常可分为感知层、网络层、平台层与应用层。感知层作为数据采集的前端，主要由各类传感器、智能仪表、控制器等终端设备组成，负责采集设备运行参数、环境数据、能源消耗数据等海量实时数据；网络层承担数据传输的核心功能，通过工业以太网、无线传感网络、5G 等通信技术，实现感知层与平台层、应用层之间的数据交互；平台层是系统的数据处理与存储中心，通过云计算、边缘计算等技术对采集到的数据进行清洗、整合、分析与存储，为上层应用提供数据支撑；应用层则根据不同的业务需求，实现智能监控、故障诊断、优化调度、能耗管理等具体应用功能。各层级之间紧密关联、数据交互频繁，形成了一个复杂的有机整体。

1.2 数据特性

智能电气自动化系统的数据具有显著的行业特殊性，主要体现在以下几个方面：一是海量性，系统中大量终端设备实时采集数据，数据规模呈指数级增长，形成了海量的工业大数据；二是实时性，为保障系统的精准控制与高效调度，数据的采集、传输与处理需满足严格的实时性要求，尤其是在电力调度、智能制造等关键场景中，数据延迟可能导致严重后果；三是异构性，数据来源广泛，涵盖结构化数据（如设备参数）、半结构化数据（如日志文件）与非结构化数据（如监控图像），数据格式与类型复杂多样；四是敏感性，数据中包含大量敏感信息，既包括企业的生产工艺、设备运行状态等商业机密，也包括用户的用电习惯、身份信息等个人隐私，一旦泄露将造成严重损失；五是关联性，各层级、各设备产生的数据之间存在紧密的关联关系，数据的完整性与一致性对系统决策的准确性至关重要。

2 智能电气自动化系统数据安全与隐私保护风险分析

2.1 感知层风险

感知层是系统数据采集的源头，其安全风险主要源于终端设备的脆弱性与部署环境的开放性。一方面，部分智能终端设备（如传感器、智能仪表）由于成本限制，硬件配置较低，缺乏完善的安全防护机制，容易遭受恶意入侵、篡改与控制。例如，攻击者可通过伪造传感器数据，导致系统做出错误的控制决策；另一方面，感知层设备多部署在户外或工业现场等开放环境中，物理防护不足，设备易被窃取、破坏或替换，造成数据采集中断或虚假数据注入。此外，终端设备之间的通信多采用传统的工业通信协议（如 Modbus、DNP3），这些协议缺乏加密与身份认证机制，数据传输过程中易被监听与窃取，泄露敏感信息。

2.2 网络层风险

网络层作为数据传输的核心通道，面临着数据泄露、篡改、拦截与拒绝服务攻击等多重风险。随着智能电气自动化系统与互联网的融合，网络边界逐渐模糊，外部攻击向量显著增加。攻击者可利用网络漏洞侵入系统网络，拦截传输中的数据，如企业的生产调度数据、用户的用电数据等；通过篡改数据内容，破坏数据的完整性，影响系统的正常运行；发起拒绝服务攻击，占用网络带宽与系统资源，导致数据传输中断，系统瘫痪。此外，网络层中存在的网络拓扑混乱、访问控制策略不完善等问题，也为攻击者提供了可乘之机，进一步加剧了数据安全风险。

2.3 平台层风险

平台层集中了大量的数据存储与处理设备，是数据安全与隐私保护的核心环节，其风险主要体现在数据存储安全与数据处理安全两个方面。在数据存储方面，若存储设备缺乏完善的加密保护机制，或访问控制策略不严格，攻击者可通过非法访问存储系统，窃取或篡改海量敏感数据；存储设备的硬件故障、软件漏洞也可能导致数据丢失或损坏。在数据处理方面，平台层采用的云计算、大数据分析等技术涉及多用户数据的共享与协同处理，若缺乏有效的数据隔离机制，可能导致不同用户之间的数据泄露；数据处理过程中产生的中间数据若未得到妥善管理，也可能成为隐私泄露的源头。此外，平台层的管理权限混乱、日志审计不完善等问题，可能导致安全事件发生后无法及时追溯，增加了安全风险的管控难度。

2.4 应用层风险

应用层直接面向用户与业务场景，其风险主要源于应用程序漏洞、用户操作不当与隐私保护机制缺失。部分应用程序在开发过程中未严格遵循安全开发规范，存在代码漏洞、权限管理不严等问题，攻击者可利用这些漏洞侵入应用系统，窃取用户隐私信息或篡改业务数据；用户操作不当，如弱密码、密码泄露、随意授权等行为，也会为攻击者提供非法访问的机会；此外，部分应用在服务过程中过度收集用户数据，或未对用户数据进行脱敏处理就进行共享与使用，严重侵犯了用户的隐私权益。例如，智能用电系统若未对用户的用电数据进行有效保护，可能导致用户的生活习惯、居住规律等隐私信息泄露。

3 智能电气自动化系统数据安全与隐私保护主流技术

3.1 数据加密技术

数据加密技术是保障数据安全的核心技术之一，通过对数据进行加密处理，可确保数据在传输与存储过程中即使被窃取，攻击者也无法获取有效信息。根据加密场景的不同，数据加密技术可分为传输加密与存储加密。传输加密主要用于保障网络层数据传输的安全性，常用技术包括对称加密（如 AES、DES）与非对称加密（如 RSA、ECC）。对称加密具有加密效率高、运算速度快的特点，适用于海量实时数据的传输加密；非对称加密具有密钥管理便捷、安全性高的优势，常用于密钥交换与身份认证。在智能电气自动化系统中，可采用对称加密与非对称加密相结合的方式，既保障数据传输的效率，又提升加密的安全性。存储加密则用于保障平台层数据存储的安全性，常用技术包括文件加密、数据库加密等。通过对存储的数据进行加密处理，可防止非法访问存储设备导致的数据泄露。

3.2 身份认证与访问控制技术

身份认证与访问控制技术用于规范系统访问行为，防止非法用户与设备侵入系统，是保障系统安全的第一道防线。身份认证技术通过验证用户或设备的身份信息，确保其合法性，常用技术包括密码认证、生物特征认证（如指纹、人脸）、密钥认证、多因素认证等。在智能电气自动化系统中，针对不同的访问主体，可采用不同的身份认证方式。例如，对管理员采用多因素认证（密码+U 盾+生物特征），提升身份认证的安全性；对终端设备采用密钥认证，确保设备接入的合法性。访问控制技术则在身份认证通过后，根据预设的访问策略，限制用户或设备对系统资源的访问权限，常用技术包括基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）等。RBAC 通过将用户分配到不同的角色，根据角色赋予相应的访问权限，具有易于管理、灵活性高的特点，适用于用户类型相对固定的场景；ABAC 则根据用户、资源、环境等多维度属性动态判断访问权限，适用于智能电气自动化系统中异构设备多、访问场景复杂的需求。

3.3 数据脱敏技术

数据脱敏技术是保护用户隐私的关键技术，通过对敏感数据进行处理，使其在保留数据可用性的同时，无法识别原始信息，从而防止隐私信息泄露。常用的数据脱敏技术包括屏蔽、替换、加密、匿名化等。屏蔽技术通过隐藏敏感数据的部分字段（如将身份证号的中间几位替换为*），实现数据脱敏；替换技术将敏感数据替换为虚构的非敏感数据，确保数据格式与原有数据一致，

适用于数据测试、培训等场景；加密脱敏通过对敏感数据进行加密处理，需要时通过解密获取原始数据，兼顾了数据安全性与可用性；匿名化技术则通过删除或替换数据中的个人标识信息，使数据无法关联到具体的个人或企业，适用于数据共享与公开场景。在智能电气自动化系统中，针对用户的用电数据、企业的生产数据等敏感信息，可根据数据的使用场景，采用相应的数据脱敏技术，在保障数据应用价值的同时，保护隐私权益。

3.4 入侵检测与防御技术

入侵检测与防御技术用于实时监测系统中的恶意行为，及时发现并阻断攻击，保障系统的正常运行。入侵检测技术通过收集系统的日志数据、网络流量数据等，采用特征匹配、异常检测、机器学习等方法，识别系统中的入侵行为，并发出告警。根据检测范围的不同，可分为主机入侵检测系统（HIDS）与网络入侵检测系统（NIDS）。HIDS 部署在终端设备或服务器上，监测主机的运行状态与操作行为；NIDS 部署在网络节点上，监测网络流量中的异常行为。入侵防御技术则在入侵检测的基础上，具备主动阻断攻击的能力，通过对网络流量进行实时过滤、拦截恶意数据包，防止攻击行为对系统造成破坏。在智能电气自动化系统中，可构建分布式入侵检测与防御体系，覆盖感知层、网络层、平台层与应用层，实现对系统全链路的实时监测与防护，提升系统的抗攻击能力。

4 智能电气自动化系统数据安全与隐私保护一体化防护策略

在数据采集阶段，加强感知层终端设备安全防护，进行身份认证与加密配置，采用安全通信协议加密传输数据，确保数据真实完整、防监听窃取。数据传输阶段，构建安全网络通道，采用 VPN 等技术保障网络层传输安全，优化拓扑结构、加强访问控制，防非法数据流入流出。数据存储阶段，对存储设备加密保护，采用分布式存储等技术，建立严格访问控制策略，对敏感数据分级存储，加强审计管理。数据处理阶段，采用数据隔离等技术，加强处理平台防护、修复漏洞，防数据泄露。数据销毁阶段，采用安全销毁技术，确保数据彻底删除。结合分层架构，构建感知层、网络层、平台层、应用层防护的多层次体系。感知层加强终端物理防护与配置，定期检测升级；网络层部署安全设备，监测网络行为、阻断攻击；平台层加强核心设备防护，采用安全软件、建立审计机制；应用层加强程序安全开发测试、修复漏洞，规范用户访问。各层级协同形成防护网络，提升整体防护能力。

技术防护是基础，安全管理与制度建设是关键。一方面，健全管理制度，明确职责、规范流程，制定应急预案、开展演练。另一方面，加强人员管理，开展培训、提升技能，建立准入离岗制度、规范账号权限。此外，加强合规管理，遵守相关法律法规，保护隐私权益。

随着攻击技术升级，需推动技术创新与融合应用。加强新兴技术在数据安全领域研究，如用人工智能精准识别预测入侵，用区块链保障数据完整可追溯，用边缘计算减少传输量、降风险。加强产学研合作，推动成果转化，提升防护技术水平。

5 结论

智能电气自动化系统的数字化、智能化发展为工业生产与能源管理带来了巨大变革，但也使数据安全与隐私保护问题日益凸显。本文通过分析智能电气自动化系统的架构与数据特性，梳理了系统在感知层、网络层、平台层与应用层面临的各类数据安全与隐私保护风险，介绍了数据加密、身份认证与访问控制、数据脱敏、入侵检测与防御等主流防护技术，并提出了涵盖数据全生命周期的一体化防护策略。该策略通过完善数据全生命周期管控、构建多层次安全防护体系、加强安全管理与制度建设、推动技术创新与融合应用，可有效提升系统的数据安全与隐私保护能力，为系统的健康发展提供保障。

参考文献

[1]张秦萌.人工智能背景下电气自动化升级改造分析[J].黑龙江科学,2025,16(22):135-137.

[2]李松林,李明.电气工程自动化控制现状及智能化技术的有效应用分析[J].中国设备工程,2025,(22):28-30.

[3]陈阳.智能技术在电气工程自动化控制中的应用探讨[J].能源与节能,2025,(11):294-296+299.DOI:10.16643/j.cnki.14-1360/td.2025.11.088.

[4]曹建斌.基于人工智能技术的电气自动化控制策略探析[J].中国电子商情,2025,31(21):127-129.