电气及其自动化系统的信息安全与防护策略

刘晓峰

江西省人力资源有限公司（江西科能工程建设咨询监理有限公司），江西南昌，330000；

摘要：工业 4.0 与“双碳”目标推动下，电气及其自动化系统已从传统孤立模式转向高度互联的智能化形态，成为工业生产与社会基建的核心。互联互通带来效率提升的同时，也使系统面临严峻信息安全风险，设备劫持、数据泄露等问题直接影响生产安全与公共利益。本文结合电气及其自动化系统的技术特性，分析当前信息安全领域的隐患与风险成因，引入系统全生命周期管理理念，从技术、管理、应急等维度探索防护策略。研究旨在为构建可靠且安全的现代化电气自动化系统提供参考，助力解决数字化转型中的安全瓶颈，保障关键基础设施稳定运行。

关键词：电气及其自动化系统；信息安全；防护策略；风险识别；智能防护

DOI：10.64216/3080-1508.25.12.088

引言

物联网、大数据技术在工业领域的深度应用，推动电气及其自动化系统实现全流程数字化管控，其应用已覆盖电力、制造、交通等关键行业。系统稳定运行直接决定产业效能与社会秩序，但信息安全防护发展滞后于技术升级。传统物理隔离的防护方式，难以应对跨域攻击、恶意代码注入等新型威胁，信息安全事件导致的生产中断、设备损坏问题屡有发生。精准把握系统信息安全痛点，构建科学防护体系，是工业数字化转型的必然要求，也是保障关键基础设施安全的重要举措，具有鲜明的现实意义。

1 核心内涵与时代价值

1.1 定义与边界

电气及其自动化系统的信息安全以数据完整性、设备可控性、运行连续性为核心指标，覆盖从感知层数据采集到应用层指令下发的完整链路。其安全边界具有双重属性，既包括硬件设备的物理安全，如设备防篡改、防盗窃等基础要求，也涵盖软件系统的逻辑安全与数据传输的通信安全。在实际防护中，技术层面的防护措施需与管理层面的规范制度相结合，形成协同防护模式。只有明确安全边界与核心目标，才能针对性构建防护体系，避免出现安全防护的漏洞与盲区，为系统稳定运行提供基础保障。

1.2 核心价值

信息安全是电气及其自动化系统发挥应有效能的前提条件，直接关联工业生产的稳定性与安全性。可靠的安全防护体系能够有效抵御恶意攻击，避免生产线停机、电力供应中断等严重事故，从而降低企业经济损失与社会影响。同时，完善的防护措施可保障生产数据与运营信息的安全，防止核心数据被窃取或篡改。对于企业而言，生产数据与运营信息是重要的无形资产，其安全性直接关系企业核心利益。在行业层面，数据安全能够维护行业数据隐私，避免因数据泄露引发的行业恶性竞争，推动行业健康有序发展，凸显信息安全的重要价值。

1.3 安全独特性

与普通信息系统相比，电气及其自动化系统的信息安全具有显著独特性。首先是实时性要求极高，系统在保障安全的同时，必须满足设备控制的毫秒级响应需求，避免安全防护措施影响系统控制精度。其次是设备多样性带来的防护难度，系统中既有传统继电器等老旧设备，也有智能 PLC 等先进设备，技术架构差异大，需要适配多元防护方案。最后是影响的延伸性，安全事件的影响会从网络空间直接延伸至物理世界，可能引发设备损坏、生产事故等实体危害，这与普通信息系统的安全影响有本质区别。

2 安全风险与成因

2.1 架构固有风险

架构层面的固有风险是电气及其自动化系统安全的重要隐患。部分老旧系统设计于网络安全意识薄弱的时期，未融入网络安全考量，缺乏基础的访问控制与数据加密模块，轻易成为攻击者的突破口。在系统集成过程中，这一问题更为突出。不同厂商的设备采用各自的通信协议，存在协议兼容性问题，导致安全防护措施无

法有效衔接，形成安全防护“断层”。这种“断层”使得全链路防护体系难以构建，部分环节成为安全短板。随着系统运行时间增长，架构固有风险会逐渐凸显，对系统安全构成持续威胁，需引起足够重视。

2.2 双重威胁影响

电气及其自动化系统面临外部攻击与内部操作的双重威胁，安全形势复杂。外部网络中，针对工业控制系统的恶意代码、钓鱼攻击数量不断增加，攻击者利用系统漏洞实现远程控制，手段隐蔽且破坏力强。内部威胁同样不可忽视，内部人员的误操作可能导致系统参数异常，影响系统正常运行。部分人员违规接入外部设备，如私自连接 U 盘、手机等，为病毒传播提供途径，破坏系统安全平衡。与外部攻击相比，内部威胁具有更强的隐蔽性，难以被及时发现与防范，给系统安全带来极大挑战，需要建立全面的防控机制。

2.3 协同失衡问题

安全管理与技术更新的协同失衡，进一步放大了系统安全风险。部分企业存在重功能升级、轻安全防护的误区，将资金与精力集中在系统功能提升上，对安全防护建设投入不足。这导致防护设备更新与系统升级不同步，防护技术落后于系统发展，无法有效应对新型安全威胁。同时，专业安全管理团队的缺失与管理制度的不完善，使得安全隐患无法被及时发现与处置。日常运维中，缺乏规范的安全操作流程，部分安全制度流于形式，无法落实到实际工作中。这种协同失衡从管理与技术两方面削弱了系统防护能力，需尽快加以解决。

3 技术支撑体系

3.1 感知与网络防护

感知层与网络层是系统安全防护的前沿阵地，其防护效果直接影响整体安全水平。在感知层，应部署具备身份认证功能的智能传感器，对接入设备进行严格的权限管控，只有通过认证的设备才能接入系统，从源头阻止非法设备入侵。网络层需构建深度防御网络，采用工业防火墙、入侵检测系统等专业设备，对网络流量进行实时监测与过滤。同时，运用虚拟专用网络技术对数据传输进行加密处理，保障数据传输的加密性与独立性，防止数据在传输过程中被窃取或篡改。通过感知层与网络层的协同防护，构建系统安全的第一道防线，有效抵御外部攻击。

3.2 数据与应用加固

数据层与应用层的安全加固是系统防护的核心环节。数据层应采用数据加密、脱敏等技术手段，对采集数据、指令数据等进行全面保护，保障数据的完整性与保密性。建立数据全生命周期安全管理机制，从数据产生、传输、存储到销毁的各个环节，都制定明确的安全规范，确保数据安全可控。应用层需定期对软件系统进行漏洞扫描，及时发现并修复安全漏洞，同时做好补丁更新工作，提升系统抗攻击能力。引入最小权限原则优化访问控制策略，根据岗位需求分配相应权限，避免权限滥用导致的安全风险，实现数据与应用的全方位防护。

3.3 智能防护融合

智能防护技术的融合应用是提升系统防护能力的重要方向。引入人工智能与大数据分析技术，构建系统安全态势感知平台，该平台能够对系统运行中的异常流量、异常操作进行实时监测，实现智能预警。通过机器学习算法对历史攻击数据进行深入分析，挖掘攻击行为规律与特征，使防护系统能够提前预判潜在攻击风险，做好防御准备。这种从“被动响应”到“主动预判”的转变，大幅提升了系统的主动防御能力。智能防护技术与传统防护手段相结合，形成多层次、智能化的防护体系，有效应对日益复杂的安全威胁，为系统安全提供先进技术支撑。

4 管理保障机制

4.1 全流程管理制度

构建全流程安全管理制度是保障系统安全的基础保障。制度应覆盖系统规划、建设、运行、维护的全生命周期，明确各环节的安全责任主体，细化操作规范与安全要求。在系统规划阶段，需进行安全风险评估，将安全理念融入规划设计；建设阶段要严格把控设备选型与软件开发的安全标准；运行阶段制定日常安全巡检制度；维护阶段规范维护流程与应急处理措施。同时，制定设备接入审批流程、数据访问权限管理办法等专项制度，将安全管理要求贯穿于日常运营的每一个环节，确保安全管理有章可循、落到实处。例如，在设备选型时，应优先选择通过安全认证的产品，并对其安全性能进行严格测试；在软件开发中，采用安全开发生命周期（SDL）方法，确保代码的安全性。

4.2 人员能力提升

人员是系统安全管理的核心要素，强化人员安全意识与专业能力至关重要。应定期开展针对不同岗位人员的信息安全培训，培训内容需结合岗位实际，普及安全

操作规范、风险识别技巧与应急处置方法。对于一线操作人员，重点培训设备安全操作与异常情况处理；对于技术人员，侧重安全技术更新与漏洞修复能力提升。同时，建立专业的信息安全团队，负责系统安全防护的日常运维、定期风险评估与安全事件应急处置。通过持续培训与团队建设，提升相关人员的安全素养与技术储备，增强系统安全的人为保障。例如，定期组织模拟安全事件演练，让员工在实践中提升应急处置能力；为技术人员提供参加安全技术研讨会的机会，使其及时了解最新的安全技术和趋势。

4.3 评估改进机制

完善安全评估与持续改进机制，是提升系统防护能力的重要手段。定期组织第三方专业机构对电气及其自动化系统进行全面安全评估，第三方机构具有独立性与专业性，能够客观识别系统存在的潜在漏洞与管理缺陷。评估完成后，依据评估报告制定针对性的改进方案，明确改进目标、责任人与完成时限。建立安全防护体系的动态优化机制，根据系统升级情况、技术发展趋势与新型安全威胁，及时调整防护策略与措施。通过定期评估、整改优化的循环机制，确保防护能力与系统发展、威胁演变保持同步，持续提升系统安全水平。

5 应急响应与协同机制

5.1 分级应急预案

制定分级分类应急响应预案是应对安全事件的关键准备。结合系统应用场景与安全风险等级，划分安全事件级别，针对不同级别制定差异化的应急响应预案。明确各级别安全事件的响应流程、责任分工与处置措施，确保事件发生时能够快速启动、有序处置。针对设备故障、数据泄露、恶意攻击等典型场景，编制标准化的应急操作手册，细化操作步骤与注意事项。定期组织应急演练，让相关人员熟悉预案内容与操作流程，提升应急处置的实战能力。通过科学的预案制定与演练，降低安全事件造成的损失，保障系统尽快恢复正常运行。

5.2 应急处置平台

搭建高效应急处置技术平台，为安全事件处置提供有力技术支撑。平台应集成监测预警、应急指挥、故障恢复等功能模块，实现安全事件的快速定位与精准处置。监测预警模块实时采集系统运行数据，及时发现异常并发出预警；应急指挥模块整合各方资源，实现指挥调度的高效协同；故障恢复模块提供数据恢复、设备重启等技术支持。建立完善的系统备份与恢复机制，通过定期数据备份、设备冗余配置等手段，提升系统恢复能力。当安全事件发生时，依托平台快速开展处置工作，缩短事件持续时间，降低运行中断损失，提升应急处置效率与效果。

5.3 跨主体协同机制

建立跨主体协同防护机制，能够整合各方力量提升整体防护效能。积极推动企业、设备厂商、安全服务商之间的协同合作，建立安全威胁信息共享机制。企业及时反馈系统运行中的安全问题，设备厂商提供设备安全升级支持，安全服务商输出专业防护技术，实现攻击预警与防护经验的实时互通。加强与行业监管部门、应急管理机构的联动，主动接受监管指导，参与行业安全协同行动。通过构建企业、厂商、服务商、监管部门等多方参与的协同防护网络，打破信息壁垒与资源孤岛，形成防护合力，提升应对复杂安全威胁的能力，保障电气及其自动化系统的整体安全。

6 结论

电气及其自动化系统的信息安全是工业数字化转型过程中不可忽视的关键议题，直接关系生产安全与社会稳定。本文通过分析系统信息安全的核心内涵与时代价值，明确了安全防护的核心目标与独特要求。针对系统面临的架构固有风险、双重威胁影响与协同失衡问题，从技术、管理、应急三个维度构建了完善的防护体系。技术层面形成感知网络防护、数据应用加固与智能防护融合的支撑体系；管理层面建立全流程制度、人员提升与评估改进的保障机制；应急层面完善预案、平台与协同的响应体系。未来，需结合技术发展持续优化防护策略，实现安全与效能的协同提升，为系统稳定运行提供坚实保障，推动工业领域安全、高效发展。

参考文献

[1]汤孜冲.基于电力系统电气工程自动化的智能化应用[J].中国设备工程,2025,(20):246-248.
[2]温周项.基于自动化技术的变电站电气系统运行时钟同步方法[J].电气技术与经济,2025,(10):106-108.
[3]黄思齐,王岳珩.电气自动化智能建筑设备安装和质量控制要点[J].中国科技信息,2025,(20):64-66.
[4]付宝友.电力系统电气设备故障自动化智能监测技术探析[J].电力设备管理,2025,(18):102-104.
[5]王爱斌.电气自动化技术在电力系统生产运行中的应用[J].光源与照明,2025,(08):242-244.