

电气自动化安全控制探讨

岳秀峰 董宇斌

内蒙古华电锡林浩特新能源有限公司 内蒙古 锡林浩特 026000

摘要：电气自动化安全控制是保障工业生产稳定运行的关键环节。本文深入探讨电气自动化安全控制，分析其重要性，指出其对设备稳定运行、生产安全以及企业效益的重要意义。研究影响安全控制的因素，涵盖硬件设备故障、软件系统漏洞、复杂环境干扰及人为操作失误等方面。针对上述问题，提出优化自动化控制系统架构、设计多层次安全保护措施、加强运维人员管理等策略，旨在提升电气自动化系统的安全性与可靠性，为相关领域的安全管理和技术改进提供参考。

关键词：电气自动化；安全控制；探讨

引言：在工业智能化快速发展的当下，电气自动化技术广泛应用于能源、制造、交通等多个领域，极大提升了生产效率与管理水平。然而，电气自动化系统运行中面临诸多安全隐患，硬件设备的老化、软件系统的脆弱性、恶劣环境的影响以及人为操作不当等，都可能导致系统故障甚至安全事故，造成重大经济损失与人员伤亡。因此，深入研究电气自动化安全控制，分析影响因素并提出有效策略，对于保障系统稳定运行、推动工业可持续发展具有重要的现实意义。

1 电气自动化安全控制的重要性

1.1 保障生产安全

在工业生产场景中，电气自动化设备广泛应用于各类生产线。这些设备运行时涉及高电压、大电流以及复杂的机械运动，倘若缺乏有效的安全控制，一旦发生故障，极易引发严重事故。以某化工企业为例，由于电气自动化设备的线路老化未及时察觉与维护，致使短路产生电火花，进而引发了易燃易爆化学品的爆炸，造成了人员伤亡和巨额财产损失。安全控制措施可从多方面保障生产安全，如安装漏电保护装置，能在设备发生漏电时迅速切断电源，防止操作人员触电；设置紧急制动按钮，当出现紧急状况时，工作人员可及时停止设备运行，避免事故恶化。

1.2 确保系统稳定运行

电气自动化系统由众多电气设备、控制系统及通信网络构成，任何一个环节出现问题都可能影响整体运行。稳定运行的电气自动化系统是企业高效生产的基石。比如汽车制造企业的自动化生产线，从零部件的搬运、加工到整车装配，高度依赖电气自动化系统。若系统因设备故障、软件漏洞或外界干扰等因素出现停机，不仅会导致生产停滞，还会使在制品积压，增加生产成本。安全控制能够通

过实时监测设备运行状态，及时发现潜在故障隐患，如利用智能传感器监测设备温度、振动等参数，一旦参数异常便发出预警，以便维修人员及时处理；定期对系统进行维护保养，包括设备清洁、软件升级等，确保系统各部分正常工作，从而维持电气自动化系统的稳定运行，保障生产活动的连续性与高效性。

1.3 促进电气自动化技术发展

安全控制对电气自动化技术发展起到积极推动作用。一方面，随着安全需求的不断提升，促使科研人员和企业投入更多资源用于研发更先进的安全技术与设备。例如为满足对电气设备更高精度的故障检测需求，研发出基于人工智能的故障诊断系统，通过对设备运行数据的深度学习，能够快速、准确地识别故障类型与位置。另一方面，安全控制标准的日益严格，使得电气自动化技术在设计、生产和应用等各个环节都更加注重安全性与可靠性。这促使企业在产品设计阶段就将安全因素融入其中，采用更优质的材料和更合理的电路设计，提升产品的整体质量^[1]。

2 影响电气自动化安全控制的因素

2.1 硬件设备因素

2.1.1 设备质量

硬件设备的质量直接影响电气自动化系统的安全性能。低质量的设备可能存在设计缺陷、制造工艺粗糙等问题，导致设备在运行过程中容易出现故障。例如，一些质量不佳的传感器可能无法准确感知物理量，导致控制系统接收到的数据不准确，从而影响系统的正常运行。此外，低质量的电气元件可能存在绝缘性能差、耐压能力不足等问题，容易引发电气故障，甚至引发火灾等安全事故。

2.1.2 设备老化

随着使用时间的增加，电气自动化设备会出现老化

现象。设备的老化会导致其性能下降,可靠性降低。例如,电缆在长期使用过程中,绝缘层可能会逐渐老化、破损,导致漏电现象的发生;接触器、继电器等电器元件的触点可能会磨损、氧化,导致接触不良,影响系统的控制精度和稳定性。设备老化还可能引发设备的突然故障,给生产带来严重的安全隐患。

2.2 软件系统因素

2.2.1 软件漏洞

电气自动化系统的软件系统是实现自动化控制的核心,但软件中可能存在漏洞。这些漏洞可能被黑客利用,导致系统遭受攻击,从而影响系统的安全运行。例如,黑客可能通过网络入侵电气自动化系统,篡改控制程序,导致设备运行异常;或者窃取系统中的重要数据,给企业带来经济损失。此外,软件漏洞还可能导致系统出现死机、崩溃等问题,影响生产的连续性。

2.2.2 软件兼容性

电气自动化系统通常由多个软件模块组成,不同模块之间的兼容性也会影响系统的安全性能。如果软件模块之间存在兼容性问题,可能会导致数据传输错误、控制指令执行异常等问题。例如,在某些系统中,由于不同厂家的软件模块之间兼容性不佳,导致系统在升级过程中出现故障,影响了生产的正常进行。

2.3 环境因素

2.3.1 气候条件

气候条件对电气自动化系统的运行安全有着重要影响。例如,在高温环境下,设备的散热性能会受到影响,可能导致设备过热,影响其性能和寿命。在低温环境下,设备的某些部件可能会出现脆化现象,降低其可靠性。此外,高湿度环境可能导致设备内部出现凝露现象,引发电气短路等故障。

2.3.2 机械作用

电气自动化系统在运行过程中会受到各种机械作用力的影响,如振动、冲击等。这些机械作用力可能会导致设备的零部件松动、损坏,影响系统的正常运行。例如,在振动较大的工业生产环境中,电气设备的固定螺丝可能会松动,导致设备接触不良;冲击力可能会导致设备的内部元件损坏,引发系统故障。

2.4 人为因素

3.4.1 操作失误

运维人员的操作失误是导致电气自动化系统安全事故的重要原因之一。例如,操作人员进行设备调试、维护过程中,如果操作不当,可能会导致设备损坏或系统故障。在启动设备时,未按照正确的操作顺序进行操

作,可能会导致设备过载,引发电气火灾等事故。

2.4.2 管理不善

企业安全管理不到位也会影响电气自动化系统的安全控制。例如,缺乏完善的安全管理制度和操作规程,导致运维人员在工作过程中无章可循;对运维人员的培训不足,使其缺乏必要的安全知识和操作技能,无法及时发现和处理系统中的安全隐患^[2]。

3 电气自动化安全控制的策略

3.1 优化自动化控制系统架构

3.1.1 合理选择控制器

控制器作为电气自动化系统的核心,其性能与适配性直接决定系统运行的稳定性与安全性。在选型时,需综合考量系统规模、控制精度、响应速度及环境适应性等因素。对于复杂工业场景,应优先选用运算能力强、抗干扰性高的可编程逻辑控制器(PLC),或结合分布式控制系统(DCS)实现分级管控,避免单点故障引发系统崩溃。同时,需评估控制器的冗余设计能力,通过主备切换机制保障关键控制环节持续运行。

3.1.2 完善运行监控系统

完善的运行监控系统是实现电气自动化安全控制的重要保障。通过部署高精度传感器实时采集设备运行数据,如电流、电压、温度、振动等参数,利用大数据分析 with 人工智能算法对数据进行深度挖掘,可提前预判设备异常趋势。同时,建立可视化监控平台,将系统运行状态以图表、动画等直观形式呈现,便于运维人员快速定位故障点。此外,设置多级阈值报警机制,当监测数据超出安全范围时,系统立即发出声光报警,并通过短信、邮件等方式通知相关人员。定期对监控系统进行校准与维护,确保数据采集的准确性和实时性,实现对系统运行状态的全流程、动态化安全管控。

3.1.3 强化网络接入安全

随着电气自动化系统与工业互联网的深度融合,网络安全威胁日益严峻。强化网络接入安全需从多维度入手:一方面,采用虚拟专用网络(VPN)、防火墙等技术,对外部访问进行严格身份认证与权限管理,限制非授权设备接入系统;另一方面,对传输数据进行加密处理,防止数据在网络传输过程中被窃取或篡改。定期开展网络安全漏洞扫描与渗透测试,及时修复系统漏洞,更新安全补丁。此外,建立网络攻击实时监测与阻断机制,一旦发现异常网络行为,迅速切断连接并启动应急响应程序,保障电气自动化系统网络环境的安全性与稳定性。

3.2 设计多层次安全保护措施

3.2.1 安全隔离

安全隔离是防止电气自动化系统受到外部干扰和恶意攻击的重要手段。在物理层面,通过设置专用的电气控制柜、隔离变压器等设备,将自动化系统与其他非相关系统进行物理分隔,避免电气信号干扰和电气火灾等安全隐患的蔓延。在网络层面,采用网闸、物理隔离装置等技术,实现生产控制网络与办公网络、互联网的隔离,防止外部网络攻击渗透到关键控制系统。此外,对不同功能区域的子系统进行逻辑隔离,利用 VLAN(虚拟局域网)技术划分网络段,限制数据的非法访问与传输,确保各系统在独立安全的环境下运行,降低安全风险的扩散概率。

3.2.2 多级保护

多级保护机制通过构建多层防护屏障,提升系统的整体安全性。在电气系统中,从设备层、控制层到管理层设置不同级别的保护措施。设备层通过安装熔断器、断路器等保护装置,对过流、过压等异常情况进行快速切断;控制层采用冗余控制策略,当主控制器出现故障时,备用控制器立即接管控制任务,保证系统连续运行;管理层则通过权限分级管理,限制不同岗位人员对系统的操作权限,防止人为误操作或恶意篡改数据。

3.2.3 紧急停机

紧急停机系统是在电气自动化系统面临重大安全风险时的最后一道防线。通过在关键设备和操作区域设置紧急停机按钮,操作人员可在遇到设备故障、人身安全威胁等紧急情况时,一键触发停机指令。系统接收到指令后,将迅速切断设备电源、停止生产流程,并通过声光报警装置提示周边人员。同时,紧急停机系统与自动化控制系统深度集成,具备故障自诊断和状态记忆功能,在故障排除后,可安全、快速地恢复系统运行,避免因停机造成更大损失。

3.2.4 防火墙与网络安全

防火墙作为网络安全的重要屏障,在电气自动化系统中承担着过滤非法访问和阻断恶意攻击的关键作用。部署工业级防火墙时,需根据系统业务需求,精准配置访问控制策略,限制外部设备对系统内部资源的访问,只允许必要的通信协议和端口开放。同时,结合入侵检测与防御系统(IDS/IPS),实时监测网络流量,识别并拦截病毒、木马、DDoS攻击等网络威胁。

3.3 加强运维人员管理

3.3.1 提升运维人员技能

提升运维人员技能需构建系统化培养体系。企业应依据电气自动化系统的技术特点,制定分层分类的培训方案,课程内容覆盖电气原理、自动化控制技术、网

络安全防护等专业知识。培训过程采用理论教学与实操训练相结合的模式,通过模拟设备操作、故障模拟演练等方式,强化运维人员对设备调试、故障诊断及修复的实践能力。同时,鼓励员工参与行业技术研讨会,跟进电气自动化领域的前沿技术;支持员工考取专业资格证书,如 PLC 编程认证、工业控制系统安全工程师认证等,拓宽知识储备。

3.3.2 强化职业素养与责任意识

强化运维人员职业素养与责任意识,需从制度约束与文化培育双向发力。企业应制定严谨的岗位操作规范与安全管理制度,明确各岗位在系统运维中的权责边界,杜绝因操作随意性引发的安全隐患。通过定期开展安全知识讲座、职业操守培训,向员工传递安全第一的工作理念,深化其对安全运维重要性的认知。将安全责任落实到个人,建立安全绩效与薪酬、晋升挂钩的激励机制,对严格遵守规范、保障系统安全运行的员工给予物质奖励与精神表彰,树立责任意识标杆。

3.3.3 建立应急响应机制

建立高效应急响应机制是降低系统安全风险的关键。企业需结合电气自动化系统运行特性,制定涵盖故障分级、应急流程、人员分工的标准化应急预案。预案应明确不同类型故障(如设备故障、网络攻击、电力中断等)的处置流程与技术要求,确保响应操作有章可循。定期组织应急演练,模拟各类突发场景,检验预案可行性与人员协同能力,及时发现并优化预案漏洞。建立24小时应急值班制度,配备专业应急小组,确保突发状况下能第一时间响应;搭建跨部门应急联络平台,保障信息快速传递与资源调配^[3]。

结束语

电气自动化安全控制是保障工业生产稳定运行的关键,关乎设备安全、生产效益与人员生命财产。本文从硬件、软件、环境及人为因素剖析安全风险,针对性提出优化系统架构、设计多层次保护措施、加强运维人员管理等策略,构建了全方位安全控制体系。然而,随着工业互联网、人工智能等技术的深度融合,电气自动化系统面临的安全挑战将持续升级。

参考文献

- [1]张妍飞.电气自动化技术在儿童电动汽车安全控制中的应用[J].玩具世界,2024,(02):141-143.
- [2]房宝平.电气自动化系统中的质量控制与安全管理技术分析[J].电子技术,2023,52(10):167-169.
- [3]刘岩.基于计算机技术应用下的电气自动化控制系统设计分析[J].通讯世界,2021(14):174-175.