

自动化仪表与系统的安全防护研究

巩鹏飞

宁夏宝丰能源集团股份有限公司 宁夏 银川 750000

摘要: 随着工业自动化程度不断提升,自动化仪表与系统在工业生产中占据关键地位。其安全运行直接关系到生产效率、产品质量及人员安全。研究表明,自动化仪表与系统面临网络攻击、物理环境不稳定、人为操作失误等多种安全风险。通过加强网络安全防护、优化物理环境条件、强化人为操作与管理以及建立应急响应机制等措施,可有效降低风险,保障系统稳定运行,为工业自动化的可持续发展提供有力支撑。

关键词: 自动化仪表; 系统; 安全防护

引言

在工业4.0与智能制造蓬勃发展的时代背景下,自动化仪表与系统已深度融入工业生产全流程。然而,复杂的网络环境、多变的物理条件以及人为因素,使自动化仪表与系统面临诸多安全隐患,一旦出现安全问题,可能引发生产中断、经济损失甚至安全事故。对自动化仪表与系统安全防护的研究具有重要的现实意义。本文将深入分析其面临的安全风险,并针对性提出防护措施,为保障工业自动化系统安全运行提供参考。

1 自动化仪表与系统概述

1.1 自动化仪表

自动化仪表作为工业生产过程中实现检测、控制、调节等功能的核心设备,通过将物理量、化学量等非电信号转换为便于处理和传输的电信号,为生产过程的精确监控与控制提供数据支撑。其涵盖了检测仪表、显示仪表、调节仪表等多种类型。检测仪表利用敏感元件感知温度、压力、流量、物位等参数变化,例如热电阻传感器基于金属导体电阻随温度变化的特性,将温度信号转化为电阻值,进而转换为电信号输出。显示仪表则将检测仪表输出的信号以数字、模拟指针等形式直观呈现,方便操作人员实时获取生产数据。调节仪表依据设定值与检测值的偏差,通过PID等控制算法自动调节输出信号,驱动执行机构动作,使生产过程参数维持在目标范围内。各类自动化仪表凭借高精度的传感技术、稳定的信号处理能力,在化工、电力、冶金等工业领域中保障生产过程的稳定、高效运行。

1.2 自动化系统

自动化系统是由多个自动化仪表及控制装置相互关联、协同工作构成的有机整体,旨在实现对工业生产过程的全面自动化控制与管理。其通过传感器采集现场数据,经信号传输网络将数据传送至控制器,控制器运

用预设控制策略对数据进行分析处理,再将控制指令发送至执行机构,形成完整的闭环控制回路。以集散控制系统(DCS)为例,其将控制功能分散到各个现场控制站,实现对多个生产过程的分布式控制,同时通过中央操作站实现集中监控与管理,既保证了系统的可靠性,又便于操作与维护。先进过程控制系统(APC)则利用模型预测控制等先进算法,针对复杂工业过程的非线性、时变性等特性,优化控制策略,提升产品质量与生产效率。自动化系统通过高度集成化与智能化的架构设计,在提升工业生产自动化水平的同时,降低人工干预,减少人为操作误差,为工业生产的连续稳定运行与精细化管理提供了强有力的技术保障。

2 自动化仪表与系统面临的安全风险分析

2.1 网络安全风险

随着自动化仪表与系统的智能化、网络化程度不断提高,其网络安全风险日益突出。自动化仪表与系统采用的Modbus、Profibus等通信协议,设计时侧重通信便捷性与效率,安全性考量不足。例如Modbus协议在部分场景下未加密,攻击者可通过中间人攻击截取、篡改数据,如修改工业关键控制指令,导致生产偏差甚至事故。系统为实现远程监控、数据共享等功能,需接入企业内网及互联网,由此面临外部网络威胁。黑客可能利用系统漏洞植入恶意软件,一旦成功,可能控制仪表设备,造成数据泄露、设备失控,甚至破坏整个工业生产。美国某能源企业曾因此遭入侵,关键数据被盗,承受巨额经济损失并陷入运营危机。系统还可能遭遇DDoS攻击,大量恶意请求占用带宽导致系统瘫痪,中断生产流程。设备层面,因身份认证机制不完善,非法设备易接入网络并伪装成合法设备通信,干扰生产秩序。设备间数据传输的完整性与保密性缺乏保障,数据可能被窃取或篡改,而接收方难以察觉,直接影响生产决策准确

性。自动化仪表与系统内设备众多,设备间的通信安全至关重要。若设备身份认证机制不完善,非法设备便可能轻易接入网络,伪装成合法设备进行通信,干扰正常生产秩序。在设备通信过程中,数据传输的完整性与保密性也易遭受威胁,数据可能在传输途中被窃取或篡改,而接收方却难以察觉,最终影响生产决策的准确性^[1]。

2.2 物理环境风险

自动化仪表与系统的运行对物理环境要求较为严苛,温度、湿度等环境因素的变化,都可能对其性能产生显著影响。在高温环境下,仪表内部电子元件的性能会下降,导致测量精度降低,甚至可能引发元件损坏。例如,化工生产中的一些温度传感器,若长期处于高温环境,其测量误差会逐渐增大,影响对生产过程温度的精确控制。湿度方面,湿度过高可能使仪表内部出现结露现象,造成电路短路,损坏设备;湿度过低则可能产生静电,干扰仪表正常工作,严重时同样会损坏设备。自动化仪表与系统多应用于复杂工业环境,可能受到各种电磁干扰。工厂中的大型电机、变压器等设备在运行时会产生强电磁场,这些电磁场会干扰仪表信号传输,导致测量数据出现偏差。如在钢铁生产车间,电磁干扰较为严重,自动化仪表若未采取有效屏蔽措施,其测量结果的准确性将大打折扣,进而影响生产过程的稳定性与产品质量。雷击产生的瞬间强电磁脉冲,也可能对自动化仪表与系统造成毁灭性打击,损坏设备,甚至导致整个生产系统停机。自动化仪表与系统的正常运行依赖稳定的供电系统,若供电出现故障,如电压波动、停电等,会对系统产生严重影响。电压波动可能使仪表工作不稳定,测量数据异常,长期处于电压波动环境下,还会缩短仪表使用寿命。突然停电,若系统未配备不间断电源(UPS)或所配备的UPS容量不足,那么在遭遇停电时,正在运行的数据极有可能因断电而丢失,控制系统也难以正常切换运行模式,甚至会因突然断电而损坏设备。恢复供电后重启系统也需耗费大量时间与人力,严重影响生产效率。

2.3 人为操作与管理风险

自动化仪表与系统的操作需要专业知识与技能,若操作人员对系统不熟悉、操作不当,极易引发安全问题。参数设置错误会直接导致测量与控制偏差,如化工反应釜的温度、压力等关键参数误设,可能引发反应失控;维护检修流程违规可能造成设备损坏或安全事故。企业管理层面的风险同样突出。安全管理制度不完善,设备缺乏定期巡检、维护与更新,会因老化、故障未及时处理而增加运行风险;人员安全培训不足导致安

全意识淡薄,易出现违规操作,如随意接入外部存储设备可能引入病毒。内部权限划分不清会引发越权操作,造成关键数据篡改、删除;数据管理疏漏,包括备份不及时、存储设备安全性差、共享管控不严等,可能导致数据丢失、窃取、泄露,如对外合作中核心生产数据未经严格审核泄露,将损害企业市场竞争力。自动化仪表与系统在运行过程中会产生大量数据,数据管理至关重要。若数据备份不及时、不完整,一旦设备出现故障或遭受攻击,数据丢失将给企业带来巨大损失。数据存储安全也存在风险,若存储设备安全性差,数据可能被窃取、篡改。对数据的使用与共享缺乏有效管理,可能导致数据泄露,损害企业利益。例如,某些企业在与外部合作时,未对共享数据进行严格审核与管控,致使企业核心生产数据泄露,在市场竞争中处于不利地位^[2]。

3 自动化仪表与系统的安全防护措施

3.1 加强网络安全防护

(1) 网络边界防护。部署多层次防火墙,依据预设访问控制策略对进出网络的数据包进行深度检测与过滤;结合入侵检测与防御系统(IDS/IPS),实时监测网络异常行为和攻击迹象,发现威胁后立即采取阻断、隔离等措施。其实施目的是抵御外部网络攻击,拦截非法访问请求和恶意流量,将安全风险降至最低,适用于自动化仪表与系统连接企业内部网络、互联网的场景,如远程监控、数据共享时。(2) 数据传输加密。对仪表与控制系统间、系统与外部设备间的数据传输采用高强度加密算法加密;对生产参数、控制指令等关键数据使用数字签名技术。实施目的是防止数据在传输过程中被窃取、篡改,确保数据的完整性和真实性,适用于所有涉及数据传输的环节,尤其是关键控制指令和敏感生产数据的传输。(3) 漏洞管理与监控。利用专业漏洞扫描工具定期检测网络设备、服务器、操作系统和应用程序的安全漏洞,及时更新补丁;建立网络安全监控平台,实时监控和分析网络流量、设备运行状态,及时处理安全事件。实施目的是消除潜在安全隐患,保障网络环境的安全性和稳定性,适用于系统日常运行过程中,定期执行及实时监控。

3.2 优化物理环境条件

(1) 机房环境建设。将自动化仪表与系统安装在专门设计的机房或控制室,采用密封性能良好的门窗和墙面材料,安装高效空气过滤设备;合理规划机房布局,保证设备有足够散热和操作空间。实施效果为具备良好的防尘、防潮、防腐蚀性能,减少环境因素对设备的影响,注意事项为定期清洁空气过滤设备,检查门窗和

墙面的密封性。(2) 电力供应保障。配置不间断电源(UPS), 在市电中断时瞬间切换并持续供电; 安装防雷装置, 对电源线路和信号线路进行防雷保护。实施效果为避免因断电导致数据丢失和设备损坏, 防止雷击浪涌电压对设备造成不可逆损害, 注意事项为定期检查UPS的电量和运行状态, 确保防雷装置有效。(3) 温湿度控制。安装精密空调系统, 将温度控制在18℃-25℃, 湿度保持在40%-60%; 定期监测和记录机房温湿度, 及时调整环境参数。实施效果为延长设备使用寿命, 提高系统可靠性, 满足仪表和系统的运行要求, 注意事项为根据季节变化调整空调运行参数, 确保温湿度稳定在适宜范围^[3]。

3.3 强化人为操作与管理

(1) 人员培训。开展系统化技术培训, 使操作人员熟练掌握仪表操作方法、系统运行原理和故障处理流程; 针对不同类型仪表和系统进行有针对性的实操训练; 培养操作人员的安全意识, 使其认识到操作不当的风险并自觉遵守规程。达成目标为提升操作人员专业技能和安全意识, 提高应对复杂情况的能力, 实施频率为新员工入职后进行系统培训, 老员工每季度进行一次技能巩固和安全意识强化培训。(2) 权限管理。根据岗位职责和工作需求分配不同操作权限; 对参数修改、系统启停等关键操作设置多重验证机制; 详细记录操作时间、人员、内容等信息, 便于事后审计和追溯。达成目标为确保只有授权人员进行关键操作, 及时发现和纠正违规行为, 保障系统安全稳定运行, 实施频率为适用于所有操作环节, 权限分配每年审核一次, 操作记录至少保存3年。(3) 巡检与维护。制定科学的巡检计划, 定期检查仪表运行状态、设备性能指标; 及时维修和更换发现的问题设备; 建立完善的设备维护档案, 记录维护历史、更换部件等信息。达成目标为及时发现故障隐患和异常情况, 确保仪表和系统处于良好运行状态, 为全生命周期管理提供数据支持, 实施频率为日常巡检每日一次, 全面检查每月一次, 设备维护档案实时更新。

3.4 建立应急响应机制

(1) 应急预案制定。针对仪表失灵、系统崩溃、网

络攻击等可能出现的故障和安全事件, 分别制定应急处置方案, 明确处置流程、各部门和人员职责分工、所需应急资源。其重要性为为突发事件提供处置依据, 确保应急救援工作迅速、有序开展, 实施方式为组织专业人员结合系统特点和过往案例制定, 每年修订一次。(2) 预案演练与评估。定期模拟真实故障场景进行应急预案演练, 检验预案可行性和有效性; 根据演练结果修订和完善预案, 总结经验提高应急处置人员的反应和协同能力。重要性为发现预案不足并改进, 提升应对实际突发情况的能力, 实施方式为每半年进行一次演练, 演练后及时召开评估会议。(3) 应急物资储备。建立应急物资储备库, 储备备用仪表、电源模块、通信设备等足够的应急设备、零部件和工具; 定期检查和维护应急物资, 与供应商建立良好合作关系以保障物资及时补充。重要性为为应急修复提供物资保障, 最大限度减少故障和安全事件对生产的影响, 实施方式为每月检查一次应急物资状态, 根据系统更新情况补充新的所需物资^[4]。

结语

综上所述, 自动化仪表与系统的安全防护是保障工业生产稳定运行的关键环节。面对网络安全、物理环境、人为操作等方面的风险, 通过采取一系列科学有效的防护措施, 能够显著提升系统的安全性与可靠性。未来, 随着工业自动化技术不断发展, 需持续深化安全防护研究, 动态调整防护策略, 以适应新的安全挑战, 为工业领域的安全发展筑牢防线。

参考文献

- [1]武刚.自动化仪表与系统的安全防护研究[J].百科论坛电子杂志,2020(13):52-53.
- [2]李岩,刘有琪.自动化仪表与系统的安全防护研究[J].数字通信世界,2020(4):266.
- [3]王兴军.自动化仪表与系统的安全防护研究[J].环球市场,2020(20):378.
- [4]崔旭.自动化仪表与系统的安全防护研究[J].百科论坛电子杂志,2020(6):110-111.