

自动化仪表与系统的安全防护对策分析

杨 超

赛迈科先进材料（宁夏）有限公司 宁夏 银川 750001

摘 要：自动化仪表与系统在工业生产中承担数据采集、逻辑运算与指令输出的关键职能，设备运行过程中面临硬件衰减、程序缺陷、网络入侵与人为误操作等多重安全威胁。本文围绕设备硬件、现场控制、软件程序、数据传输及运维操作五个维度，系统梳理安全风险成因与传导路径，提出涵盖硬件防护优化、通信链路加密、访问权限分级、故障预判处置及人员能力建设等方面的防护策略，为构建多层次、全流程的安全防护体系提供参考。

关键词：自动化仪表；安全防护；硬件加固；网络隔离；运维管控

引言：在工业自动化程度持续加深的背景下，仪表与控制系统承担着数据采集、信号处理与指令输出等关键职能，系统运行安全性直接关乎生产连续性与设备可靠性。然而，设备长期运行带来的硬件老化、程序冗余累积、网络边界模糊以及运维操作不规范等问题，正逐步成为威胁系统安全运行的主要隐患。深入剖析各层面风险成因并构建系统化防护对策，已成为保障自动化仪表与系统稳定运行的现实需要。

1 自动化仪表与系统安全风险成因分析

1.1 设备硬件层面风险诱因

自动化仪表与配套硬件设备长期处于连续运行状态，各类精密传感元件、采集模块及配套硬件组件会随运行时长增加出现性能衰减。工业生产场景中的环境因素会持续对硬件设备产生影响，温度波动、湿度变化以及粉尘堆积都会逐步干扰设备运行精度^[1]。硬件生产加工过程中的工艺偏差会潜藏隐性缺陷，这类缺陷不会在设备投入使用初期显现，会在长期运行过程中逐步引发设备运行异常。硬件设备老化会逐步降低数据采集与信号输出的稳定性，造成仪表数据偏差或设备短暂停机。

1.2 系统运行层面风险诱因

自动化控制系统搭载的程序模块会依托固定逻辑完成数据运算与指令输出，系统程序长期运行会产生冗余数据与无效缓存，持续堆积的冗余内容会占用系统运行资源，降低系统运行流畅度。系统内置程序版本未得到及时更新，会保留原有程序漏洞与运行缺陷，无法适配设备持续运行的实际需求。系统运行过程中的资源分配不均衡，会导致部分控制模块负载过高，其余模块处于闲置状态，整体运行架构的稳定性持续下降。系统内置防护机制存在覆盖盲区，无法对非常规运行状态进行有效管控，异常运行状态持续存在会逐步引发系统运行故障，威胁自动化系统整体运行安全。

1.3 网络传输层面风险诱因

自动化仪表与控制系统的数据交互依托网络链路完成，工业网络长期对外开放数据传输通道，会提升外部未知数据侵入的可能性。网络传输信道长期使用会出现传输稳定性下降的问题，数据传输过程中容易出现数据丢失、数据错乱等各类异常情况。网络防护配置存在不完善的情况，防护规则覆盖范围有限，无法全面抵御各类非正常数据传输行为。数据传输过程中的加密等级不足，传输数据容易出现泄露或被篡改的情况，失真数据传入控制系统后，会误导系统完成错误指令输出，引发设备运行偏差与安全隐患。网络拓扑结构规划不合理，会造成数据传输路径混乱，降低整套系统数据传输的安全性与稳定性。

1.4 运维操作层面风险诱因

自动化仪表与系统的运维工作具备较强的专业性，运维人员专业能力不足会导致日常运维工作落实不细致，无法及时识别设备与系统的隐性运行问题。运维工作缺乏规范化的执行标准支撑，不同运维人员的操作方式存在差异，整体运维工作的统一性难以保障。日常运维排查工作覆盖范围不全面，部分隐蔽性运行问题无法得到及时处理，问题持续累积会逐步转化为安全风险。运维人员对新型设备与升级后系统的熟悉程度不足，实际操作过程中容易出现操作偏差，不合理的操作行为会干扰系统与设备的正常运行节奏，持续影响自动化仪表与系统的运行安全性。

2 自动化仪表与系统硬件安全防护策略

2.1 仪表前端采集设备防护优化

前端采集设备承担工业现场数据捕捉与信号采集的核心职能，设备运行状态直接决定整套自动化系统的数据基准精度^[2]。针对现场复杂的工业环境，需要对采集设备外部防护结构进行优化升级，强化设备抵御外界环

境干扰的基础能力。针对温湿度波动、粉尘堆积等环境影响因素,可通过升级密封结构、优化防护外壳材质的方式,削弱外界环境对传感采集组件的侵蚀作用。定期对采集探头、传感组件进行清洁与校准处理,维持设备稳定的采集性能,减少数据采集偏差问题。结合现场工况调整设备安装位置,规避强干扰区域对采集工作的影响,持续保障前端数据采集的真实性与稳定性。

2.2 现场控制单元安全防护设置

现场控制单元作为自动化系统的核心硬件载体,承担数据处理与现场指令输出的关键职能,需要落实全方位的安全防护设置。针对控制单元的运行环境制定专属防护方案,做好运行空间的防尘、防潮与温控处理,维持硬件组件稳定的运行工况。对控制单元的硬件访问权限进行严格管控,杜绝非授权人员接触硬件设备造成的运行异常。优化控制单元硬件运行负载配置,根据现场运行需求合理调配硬件运行资源,规避高负载运行状态引发的硬件损耗。定期检测控制单元内部电路板、接口组件的运行状态,及时排查硬件接触不良、组件老化等潜在问题。

2.3 配套供电与辅助设备防护管控

供电设备与各类辅助设备为自动化硬件系统提供运行支撑,设备运行稳定性直接影响整套系统的安全运行水平。完善供电系统的稳压与防雷防护配置,削弱电压波动、瞬时电流冲击对仪表硬件的损伤。对供电线路进行常态化检查与养护,及时更换老化破损线路,规避线路故障引发的设备停机问题。规范辅助设备的运行调试标准,统一设备启停与工况调节的操作规范,维持辅助系统运行状态的稳定性。细化辅助设备的运行监测内容,针对性把控冷却、通风等配套设备的运行状态,保障硬件系统整体运行环境达标。

2.4 硬件设备常态化防护管控机制

常态化管控体系是维持自动化硬件设备长期安全运行的重要保障,需要搭建贴合工业运行场景的硬件防护管理模式。结合不同硬件设备的运行属性与损耗规律,制定差异化的周期性检修养护方案,精准把控设备运行状态变化。细化硬件设备检修养护的工作内容,覆盖设备清洁、性能校准、组件检测、线路排查等多个核心环节。搭建硬件设备运行台账,完整记录设备检修、更换、调试的相关信息,实现硬件运行状态的可追溯管理^[3]。持续优化硬件防护管理流程,结合设备升级迭代与工况变化调整防护内容,稳步提升硬件系统整体安全防护水平。

3 自动化仪表与系统软件及网络安全防护策略

3.1 系统程序与组态软件安全加固

自动化运行依托程序代码与组态软件实现工况调控与数据处理,软件运行质量直接决定系统控制精度与运行稳定性。针对工业控制系统常用的组态软件,需要定期开展程序漏洞扫描与代码检测工作,及时修复程序运行过程中暴露的缺陷。对系统后台程序进行精简优化,清理长期运行累积的无效代码与冗余数据,缩减程序运行资源占用空间,提升程序运行效率。针对软件版本迭代更新建立固定管理模式,及时完成老旧程序版本替换,适配现场设备运行的最新工况需求。对组态逻辑进行规范化梳理,修正不合理的程序逻辑设定,减少软件运行过程中出现的指令错乱与运算异常问题,夯实软件层面的运行基础。

3.2 数据传输链路安全防护搭建

工业仪表与控制系统的交互数据需要依托传输链路完成双向流转,链路安全建设可以有效规避数据交互过程中的各类安全问题。针对工业专用传输协议开展安全强化处理,升级传输协议的加密标准,提升数据传输过程中的保密等级。对整体传输链路进行分区规划,划分专属数据传输通道,隔离不同类型的生产数据,规避数据交叉干扰引发的传输异常。针对链路传输过程中的数据篡改与窃取隐患,部署针对性的传输防护机制,对流转数据进行全程校验筛查。持续优化链路传输架构,提升数据传输的稳定程度,减少数据丢失与传输延迟等问题对系统运行造成的负面影响。

3.3 系统访问与权限安全管控

系统访问行为的规范管理能够有效规避人为操作带来的软件与网络安全隐患,构建严谨的访问管控体系尤为重要。根据岗位工作内容划分梯度化的系统操作权限,匹配对应层级的系统操作与数据查看范围,杜绝超范围操作系统的行为出现。完善系统访问校验机制,增设多重身份核验方式,拦截非合规访问行为。定期清理系统内部闲置访问账号,及时注销离岗人员操作权限,缩减非法访问的可行渠道。对系统操作日志进行持续留存与筛查,记录各类访问与操作行为,实现系统操作行为的全程可追溯管理。

3.4 网络边界安全隔离与防护优化

工业生产网络与外部公共网络的交互场景会产生大量安全隐患,网络边界的防护建设可以阻断多数外部网络风险。部署专用网络隔离设备划分网络边界区域,实现工业内网与外网的有效隔离,阻断外部不明网络节点的侵入通道。优化网络边界防护规则,针对异常网络访问、恶意数据投递等行为设置自动拦截机制。定期更新网络边界防护数据库,适配新型网络风险的防护需求。

细化网络边界流量监测内容,对进出内网的各类数据流量进行甄别过滤,保障工业网络整体运行环境的纯净性与安全性。

4 自动化仪表与系统运维全流程安全防护体系构建

4.1 日常运维标准化防护规范搭建

日常运维工作是保障自动化仪表与系统长期稳定运行的核心环节,标准化规范能够统一运维执行标准,弱化人为因素带来的运行波动。结合自动化设备与系统的运行特性,梳理全流程运维作业内容,制定适配现场工况的标准化作业流程^[4]。明确各类运维作业的执行标准与技术要求,细化设备巡检、状态核查、性能检测等基础工作内容,填补运维作业中的管控空白。建立运维作业审核机制,对各项运维工作的落实质量进行把控,保证所有运维操作符合安全运行要求。持续结合设备运行状态更新规范内容,让运维标准适配系统长期运行与设备迭代的发展需求。

4.2 故障预判与应急防护处置机制

工业自动化系统长期连续运行难免出现各类运行异常,完善的故障处置机制可以降低异常问题带来的安全影响。结合设备运行规律与系统故障发生特征,搭建常态化故障预判模式,依托日常运行数据捕捉潜在异常征兆。细化不同类型运行故障的处置流程,针对仪表数据异常、系统程序卡顿、网络链路波动等问题制定专属处置方案。建立故障分级管控模式,依据异常影响范围划分处置优先级,保障重大运行隐患可以得到优先处理。完善故障处置后的复盘流程,积累运维处置经验,优化隐患防控与问题处理的整体流程。

4.3 系统迭代与升级过程安全防护

自动化仪表与系统会根据生产需求完成功能优化与版本迭代,升级改造阶段容易出现各类临时安全隐患。系统迭代前期需要完成全面的运行状态检测,排查设备、程序与网络的潜在问题,为升级工作营造稳定基础条件。严格把控系统升级的操作流程,规范程序更新、

参数调整、模块替换等关键作业步骤,规避升级操作不当引发的系统紊乱。升级完成后需要开展全方位运行校验,核查数据采集、指令传输、设备联动等功能的运行状态,保障系统升级后可以稳定投入运行。锁定升级后的系统参数,杜绝非授权改动造成的运行异常。

4.4 人员操作安全防护与管控体系

一线操作人员与运维人员的作业行为直接影响自动化系统的运行安全,完善人员管控体系可以从源头规避人为安全隐患。搭建系统化的人员技能培育模式,围绕仪表操作、系统调控、隐患识别等内容开展常态化培训,提升岗位作业专业素养。规范各类岗位作业行为准则,明确禁止性操作内容,减少不规范作业引发的系统故障。建立人员作业监督管理模式,对日常操作与运维作业进行全程管控,约束岗位操作行为。结合行业技术更新持续丰富培训内容,适配新型设备与升级系统的作业管控需求,筑牢人员层面的安全运行防线。

结束语

自动化仪表与系统的安全防护是一项贯穿设备全生命周期的系统工程,硬件防护、软件加固、网络隔离与运维管控缺一不可。任何单一环节的薄弱都可能成为安全链条的断裂点。只有将防护策略嵌入日常运行的每个节点,让硬件管理、程序维护、网络管控与人员培训形成协同联动,才能真正提升系统抵御各类风险的综合能力,为工业生产的连续稳定运行提供可靠保障。

参考文献

- [1]林泽群.基于化工仪表的自动化控制与安全防护[J].广州化工,2025,53(15):140-142.
- [2]马涛,张兴兵,吴超.电力配电网自动化系统网络安全风险及防护策略[J].消费电子,2025(18):92-94.
- [3]刘伟.化工自控仪表系统的网络安全防护策略探讨[J].建筑工程技术与设计,2022,10(27):115-117.
- [4]吴海霞.石油化工仪表中自动化控制技术的应用[J].中国石油和化工标准与质量,2025,45(24):157-159.