

工业自动化机电系统中PLC程序安全可靠运行保障措施

孙 莉

浙江晨欧机电工程有限公司 浙江杭州 310000

摘要：本文聚焦于工业自动化机电系统中PLC程序的安全可靠运行问题。首先阐述了PLC程序在工业自动化机电系统中的重要性，接着分析了影响PLC程序安全可靠运行的多种因素，包括硬件故障、软件漏洞、电磁干扰等。在此基础上，从硬件保障、软件设计优化、运行环境管理、人员培训等多个方面详细探讨了保障PLC程序安全可靠运行的具体措施，旨在为工业自动化生产的稳定、高效进行提供有力支持。

关键词：工业自动化；机电系统；PLC程序；安全可靠运行

引言

在工业自动化的快速发展进程中，可编程逻辑控制器（PLC）作为机电系统的核心控制部件，发挥着至关重要的作用。PLC程序通过精确控制机电设备的运行，实现了生产过程的自动化、智能化和高效化。然而，PLC程序的安全可靠运行面临着诸多挑战，一旦出现故障，可能导致生产中断、设备损坏甚至引发安全事故，给企业带来巨大的经济损失。因此，深入研究工业自动化机电系统中PLC程序安全可靠运行的保障措施具有重要的现实意义。

一、影响PLC程序安全可靠运行的因素

（一）硬件故障问题

PLC硬件系统作为程序运行的物理载体和基础平台，其稳定性和可靠性直接决定了程序能否正常执行。在实际运行过程中，硬件故障是导致PLC系统失效的主要原因之一。常见的硬件故障类型包括：电源供应系统故障、中央处理器（CPU）模块故障、输入输出（I/O）接口模块故障等^[1]。其中，电源故障可能表现为电压波动、电源短路或完全断电等情况，这些都会导致PLC系统突然断电，使正在运行的程序被迫中断；CPU作为PLC的核心处理单元，其故障会严重影响程序的运算处理能力，可能导致控制指令无法准确生成和传输；而输入输出模块的故障则会造成现场设备信号与PLC内部信号之间的传输异常，使得实际设备动作与程序控制指令产生严重偏差。

（二）软件系统漏洞

PLC程序在软件开发、调试和维护过程中可能存在

多种类型的软件缺陷和漏洞。这些软件问题主要包括程序设计逻辑错误、内存管理异常、资源分配不当等。逻辑错误会导致程序执行流程与预期设计不符，产生错误的控制输出，进而影响被控设备的正常运行状态；内存泄漏问题会使系统可用资源持续减少，最终可能导致程序运行速度下降甚至系统崩溃。此外，随着工业控制系统网络化程度的提高，PLC程序还面临着日益严峻的网络安全威胁。黑客可能利用软件中存在的安全漏洞实施网络攻击，通过非法手段入侵控制系统，篡改或破坏程序代码，这将造成严重的安全事故和生产损失。

（三）电磁干扰影响

在典型的工业现场环境中，存在着多种强电磁干扰源，包括大功率电动机、高压变压器、电焊设备、变频器等。这些设备产生的电磁干扰会通过空间辐射、电源线传导、信号线耦合等多种途径影响PLC控制系统的正常运行。电磁干扰可能导致PLC出现程序误动作、通信中断、数据丢失或损坏等异常情况。具体而言，强电磁干扰可能使输入输出信号波形发生畸变，导致PLC接收到错误的现场信号，进而产生错误的控制决策和输出指令。在某些极端情况下，持续的强电磁干扰甚至可能造成PLC硬件设备的永久性损坏。

（四）运行环境条件

PLC控制系统对其工作环境有着严格的技术要求，包括环境温度、空气湿度、粉尘浓度、振动强度等多个方面。当运行环境条件超出PLC设备的允许范围时，会显著影响其工作性能和设备寿命^[2]。高温环境会加速电子元器件的老化过程，降低系统可靠性；高湿度环境可能导致电路板结露或短路故障；粉尘积聚不仅会影响设

备的散热效果，还可能造成电路接触不良；而机械振动则可能导致连接件松动或元器件脱焊。所有这些环境因素都会不同程度地威胁PLC程序的稳定运行。

（五）人为操作因素

操作维护人员的技术水平和操作规范程度也是影响PLC程序可靠运行的重要因素。由于对PLC系统不熟悉或操作失误，可能导致程序被意外修改、参数设置错误等问题。例如，在程序调试过程中，错误的强制I/O操作可能会引发设备误动作；不恰当的参数修改可能导致控制回路失调；而未经充分测试的程序变更可能引入新的系统缺陷。此外，在设备维护和检修作业中，如果操作人员不遵守安全操作规程，使用不当的工具或方法，不仅可能损坏PLC硬件设备，还可能造成系统软件故障，给生产运行带来安全隐患。

二、保障PLC程序安全可靠运行的措施

（一）硬件保障措施

在选用优质硬件设备时，我们必须把符合工业级标准的PLC产品作为优先选项。工业环境复杂，车间内电机、变频器等设备会产生大量电磁辐射，这对PLC设备的稳定性是巨大挑战。因此，所选PLC产品的电磁兼容性能需严格满足EN61000-6-2标准，抗干扰度要不低于10V/m。例如在某汽车生产线中，选用了西门子S7-1200系列PLC，它通过内置隔离电路，将共模干扰抑制比提升到80dB，大大降低了信号失真的风险^[3]。这就好比给PLC设备穿上了一层强大的“电磁防护服”，使其能在恶劣的电磁环境中稳定工作。

冗余设计是确保关键部件无缝切换的重要手段。双电源系统配备自动切换模块，切换时间不超过5ms，这样在主电源突发故障时，备用电源能立即无缝接入，保证设备持续供电。冗余CPU则通过高速同步总线（速率不低于100Mbps）实时同步程序与数据，主备切换时间不超过10ms。某化工生产线上冗余系统采用这种设计后，实现了连续18个月无停机运行，极大地提高了生产的稳定性和连续性。

定期维护需要制定精细化计划。每季度要对硬件进行全面检测，测量电源电压波动（允许范围在±5%）、CPU温度（不高于60℃）、I/O模块接触电阻（不高于10mΩ）等关键参数。每年要更换主板锂电池，防止数据丢失，同时更换散热风扇，避免设备过热。某食品加工厂实施该维护机制后，硬件故障率从8%降至2%，显著提高了设备的可靠性。

（二）软件设计优化措施

严格的程序开发流程要贯穿软件的全生命周期。在需求分析阶段，采用SRS（软件需求规格说明书）明确控制逻辑，覆盖率必须达到100%，确保软件功能的完整性和准确性。设计阶段采用模块化编程，将每个功能模块独立封装，如逻辑控制、数据采集、报警处理模块等，这样便于单独测试与维护。测试阶段实施“三级验证”，单元测试要求模块通过率达到100%，集成测试要求接口兼容性达到100%，现场测试要求连续72小时满负荷运行无异常。某智能仓储项目通过该流程，使程序漏洞率降低了60%，提高了软件的稳定性和可靠性^[4]。

软件加密采用AES-256算法对程序代码进行加密，密钥每90天自动轮换，只有授权人员可通过加密狗或指纹认证进行解密。备份策略实行“双重存储”，每日凌晨自动备份至本地服务器，每月底离线备份至加密U盘，并将U盘存放于防火柜中。某冶金企业通过这种方式，在硬盘故障时15分钟内就恢复了程序，没有造成生产中断，保障了生产的连续性。

软件更新需遵循“测试-过渡-切换”三步法。先在仿真环境验证新版本兼容性，测试时长不少于48小时，确保新版本与现有系统兼容。再在非生产时段进行局部设备过渡运行，覆盖30%负载，观察系统的运行情况。最终全系统切换。某水处理厂通过该方法成功升级程序，避免了因版本冲突导致的阀门误动作，保证了生产的安全稳定。

（三）运行环境管理措施

电磁屏蔽需构建“多层次防护”。PLC控制柜采用1.5mm冷轧钢板制作，屏蔽效能不低于80dB，柜门与柜体通过导电胶条密封，接触电阻不高于50mΩ，有效屏蔽外界电磁干扰。内部电缆分类敷设，动力电缆（如电机线）与信号电缆（如传感器线）间距不小于30cm，交叉处采用垂直穿越方式，减少电缆之间的电磁干扰。某机床车间通过该设计，使信号传输误差从5%降至0.5%，提高了信号传输的准确性。

环境控制需维持稳定参数。控制柜内安装智能温控系统，将温度控制在0-55℃，波动范围不超过±2℃，湿度控制在30%-70%RH，超出范围自动启动除湿/加湿设备。空气过滤器每30天更换一次，过滤精度不低于99%，能拦截0.3μm以上粉尘。某半导体工厂通过该措施，使PLC内部积尘量减少80%，主板寿命延长至8年以上，降低了设备的维护成本和故障率。

防雷接地系统需满足双重标准。外部防雷采用三级避雷器，响应时间不超过25ns，将直击雷电流泄放至接地网。设备接地采用独立接地板，接地电阻不高于 4Ω ，柜体与接地板通过 6mm^2 铜缆连接，确保阻抗不高于 0.1Ω 。某户外光伏电站通过该设计成功抵御3次雷击，PLC设备无损坏，保障了设备的安全运行。

（四）人员培训和管理措施

专业培训需覆盖“理论+实操+应急”全场景。理论培训不少于40小时，内容包括PLC指令原理、程序架构、通信协议（如Modbus、Profinet）等，让操作人员具备扎实的理论基础。实操培训不少于20小时，要求学员独立完成程序编写、故障排查（如I/O点诊断、通信中断处理）等任务，提高实际操作能力。应急培训模拟10类典型故障（如程序跑飞、模块离线），考核通过率需达到100%，使操作人员在面对突发故障时能够迅速应对。某汽车零部件厂通过培训，使操作人员故障处理效率提升50%，提高了生产效率。

操作规程需明确“双人复核”机制。关键操作（如程序下载、参数修改）需由操作员与工程师共同确认，操作记录实时上传至管理系统，留存不少于3年，确保操作的准确性和可追溯性。设备启停需遵循“三步确认法”，即检查状态指示灯、核对参数设定、测试输出信号。某药厂通过该规程，杜绝了因误操作导致的批次报废事故，保障了生产质量。

权限管理采用“三级分级”模式。一级权限（操作工）仅可监控运行状态，二级权限（技术员）可进行参数调整，三级权限（工程师）可修改程序，权限变更需经部门主管审批并记录日志^[5]。某自动化车间通过该机制，2年内未发生非授权操作事件，保障了系统的安全性。

（五）监控和预警措施

实时监控系统需实现“全要素感知”。通过SCADA软件（采样频率100ms/次）采集PLC的I/O状态、寄存器数据、通信状态等128项参数，设置异常阈值（如CPU负载 $>80\%$ 、通信中断 $>5\text{s}$ ），一旦触发则声光报警，报警响应时间不超过10秒。监控界面采用“红黄绿”三色动态标识（绿：正常，黄：预警，红：故障），使操作人员能够直观地了解系统运行状态。某物流分拣线通过该系统，使异常发现时间从30分钟缩短至2分钟，提高了故障处理的及时性。

故障诊断系统融合“规则+数据”双驱动。基于规则库（含500+典型故障特征）实时匹配异常模式，如“输入信号跳变频繁→传感器接线松动”，能快速定位故障原因。结合历史数据（留存不少于3年）训练预警模型，对潜在故障（如模块老化导致的响应延迟）预警准确率不低于90%。某钢铁厂通过该系统提前72小时预测到PLC电源模块故障，避免了计划外停机（单次停机损失约5万元），减少了经济损失。

通过上述措施的协同实施，PLC程序的安全可靠运行得到全方位保障。某综合工厂的实践显示，其程序故障率从12%降至1.5%，平均无故障运行时间（MTBF）从1500小时提升至8000小时，为工业自动化的稳定运行奠定了坚实基础，有力地推动了工业生产的高效、安全发展。

结论

工业自动化机电系统中PLC程序的安全可靠运行是保障工业生产稳定、高效进行的关键。本文分析了影响PLC程序安全可靠运行的多种因素，包括硬件故障、软件漏洞、电磁干扰、运行环境恶劣和人员操作不当等。并从硬件保障、软件设计优化、运行环境管理、人员培训和管理、监控和预警等多个方面提出了具体的保障措施。通过综合应用这些措施，可以有效提高PLC程序的安全可靠性，降低故障发生率，为工业自动化生产的发展提供有力保障。在未来的研究中，还需要不断探索新的技术和方法，进一步提高PLC程序的安全可靠运行水平。

参考文献

- [1] 冯洪高. PLC技术在机电控制系统中的合理应用研究——评《机电控制与可编程控制器技术》[J]. 有色金属工程, 2021, 11 (12): I0004-I0004.
- [2] 李新宇. 工业自动化中计算机控制技术的应用 [J]. 现代工业经济和信息化, 2022, 12 (9): 304-306.
- [3] 张金辉, 张晨蕾. 工业自动化生产过程中PLC控制系统的应用 [J]. 装备维修技术, 2020 (3): 10-10.
- [4] 于俊朋. PLC在工业自动化控制中的有效运用分析 [J]. 中国战略新兴产业, 2020, 000 (2020年2期): 97.
- [5] 林星翰. 机械手PLC自动控制系统在恶劣环境中的应用 [J]. 环境工程, 2022 (9): 357-357.