油库安全管理自动化系统的可靠性分析与冗余设计

文　馨　韩济阳（中国航空油料有限责任公司甘肃分公司，甘肃　兰州　730300）

摘　要：在全球能源格局变革及我国油库仓储规模扩大的背景下，油库安全管理自动化系统的可靠性成为关键。本文构建了包含现场感知层、边缘控制层、云端管理层的系统架构，基于ISO与国标确立硬件、功能安全及数据传输可靠性指标，运用FMEA方法识别传感器与通信环节高风险点。针对可靠性需求，设计硬件双重化配置、通信多层冗余、软件“三取二表决”机制及能源多级保障等冗余技术，并通过标准化接口集成与分阶段测试验证系统。工程案例表明，改造后系统可用度提升至99.92%，经济效益显著。研究为油库自动化系统的可靠性提升提供了技术路径与实践参考。

关键词：油库安全；自动化系统；可靠性分析；冗余设计；故障模式分析

中图分类号：TE972　　**文献标识码：**A　　**文章编号：**1674-5167（2025）033-0154-03

Reliability analysis and redundancy design of oil depot safety management automation system

Wen xin, Han Jiyang (China Aviation Fuel Co., Ltd. Gansu Branch, Lanzhou Gansu 730300, China)

Abstract: under the background of the global energy pattern reform and the expansion of China's oil depot storage scale, the reliability of the oil depot safety management automation system has become the key. This paper constructs a system architecture including the field perception layer, edge control layer and cloud management layer, establishes hardware, functional safety and data transmission reliability indicators based on ISO and national standards, and uses FMEA method to identify high-risk points in sensors and communication links. For reliability requirements, redundancy technologies such as hardware dual configuration, multi-layer redundancy of communication, software "two out of three voting" mechanism and multi-level energy guarantee are designed, and the system is verified through standardized interface integration and phased testing. The engineering case shows that the system availability is increased to 99.92% after the transformation, and the economic benefit is remarkable. The research provides a technical path and practical reference for the reliability improvement of oil depot automation system.

Key words: oil depot safety; Automation system; Reliability analysis; Redundancy design; Failure mode analysis

据中国石油流通协会数据，全国主要石油仓储总库容达6.8亿m^3，单库平均库容较2012年增长45%至11.6万m^3。油库储存介质具有高危特性（汽油爆炸极限1.4% ~ 7.6%VOL），涉及18—22个专业子系统协同作业。应急管理部2023年报告显示，近五年28.5%的油库事故源于自动化系统故障，其中传感器故障（42%）、控制系统异常（33%）为主因。目前中石油、中石化等企业已完成90%在营油库自动化改造，事故率较改造前下降37%。传统油库自动化系统各子系统独立运行，存在“孤岛化”现象，缺乏系统性可靠性设计。随着物联网、边缘计算、数字孪生等技术的发展，构建高可靠、自冗余的自动化系统成为必然选择。

1 油库安全管理自动化系统可靠性分析体系构建

1.1 系统组成与功能架构解析

油库安全管理自动化系统作为典型的分布式工业控制系统（DCS），其架构具有清晰的分层特性，各层协同工作以保障油库的安全稳定运行。现场感知层宛如系统的“触角”，由智能传感器与执行机构构成。例如，光纤光栅温度传感器凭借其高精度，能够以±0.5℃的精度采集罐区温度，红外对射探测器则时刻警惕非法入侵。执行机构中的电动阀可精准执行控制指令，消防泵在关键时刻迅速响应。此类设备数量众多，占比高达60% ~ 70%，但由于其直接暴露于复杂的现场环境，成为故障高发区域。

边缘控制层犹如系统的“中转站”，是基于工业级PLC等边缘计算节点构建而成的，它肩负着数据预处理的关键要点，借助滤波算法可有效地去除高达95%的噪声，以此来保证数据的准确性。在逻辑控制方面，它可以实现200ms级别的联锁响应，保障系统在紧急状况下可快速动作。它还拥有本地存储功能，这样在通信出现异常时数据就不会丢失，该层借助Modbus等协议与现场设备以及云端进行稳定的通信，保证数据可顺畅地传输。

云端管理层堪称系统的“大脑”，部署在中控室或者数据中心，其中的数据中台有强大的数据处理能力，处理速度每天可达10TB，可对海量数据展开高效分析。视频监控平台支持200路高清视频解码，为

管理人员提供清晰的现场画面，应急指挥系统集成了30余种应急预案模型，凭借大数据分析与数字孪生技术，达成对油库全局态势的精准感知，帮助管理者做出科学决策。

1.2 可靠性关键指标体系

参考ISO26262以及GB/T3836等国际国内有权威性的标准，去构建全面又科学的可靠性指标体系是很关键的，在硬件可靠性指标这一方面，平均故障间隔时间也就是MTBF，它是衡量设备稳定性的关键参数。比如说，传感器的MTBF需要达到大于等于50000h，而控制器的MTBF则要达到大于等于100000h，这就说明设备在长时间运行的时候出现故障的概率是非常低的。平均修复时间也就是MTTR，它反映出了设备维修的便捷程度以及效率，现场设备的MTTR需要小于等于2h，以此来保证设备出现故障之后可快速恢复到正常运行状态，失效率也就是λ，它同样是关键的指标，像传感器的失效率小于等于2×10^{-5}/h，其在单位时间内发生故障的可能性是极小的。

系统功能安全指标也不能被忽视，安全完整性等级也就是SIL，它规定了系统在特定条件之下执行安全功能的能力，核心控制模块需要达到SIL2级，消防联动系统作为保障油库安全的关键部分，是要达到SIL3级。这样才能保证在火灾等紧急情况发生的时候可可靠运行，诊断覆盖率也就是DC，它对于及时发现设备故障是很关键的，关键传感器的诊断覆盖率需要大于等于99%，可最大程度地检测出潜在故障，防止故障扩大。

数据传输可靠性指标直接对系统的实时性以及准确性产生影响，通信误码率在有线传输的时候需要小于等于1×10^{-9}，以此来保证数据在传输过程中的准确性。对于实时控制数据，数据丢包率需要小于等于0.1%，保障控制指令可准确无误地传达到执行机构，避免因为数据丢失而导致控制失误。

1.3 故障模式与影响分析（FMEA）

以某油库储罐监控子系统为研究对象，采用FMEA方法可对系统中的潜在故障进行量化评估，从而有效识别风险。例如，温度传感器误报问题，经分析发现是由光纤连接器污染导致。此故障影响等级高，因为温度数据的不准确可能引发错误的控制决策，影响油库的安全运行。现有控制措施为每季度清洁，但仍存在风险，其风险优先数（RPN）达120。为进一步降低风险，建议增加自校准算法，使传感器能够实时自我检测与校准，提高数据的准确性。

液位计卡滞问题由机械部件磨损引起，RPN为75。机械部件在长期使用过程中，由于摩擦等原因容易出现磨损，进而导致液位计卡滞，影响液位检测的准确性。针对这一问题，可升级为非接触式雷达液位计，避免机械部件的磨损，提高液位监测的可靠性。

2 油库自动化系统冗余设计关键技术

2.1 硬件冗余技术

硬件冗余是提高系统可靠性的重要手段。关键设备采用“主－主”双重化配置，以储罐液位计为例，两台设备同时运行并同步数据。当一台设备出现故障时，系统能够在＜50ms的极短时间内完成故障切换，确保液位监测的连续性与准确性。某油库在进行此项改造后，液位计误报警率大幅下降82%，显著提升了液位监测系统的可靠性。

通信网络运用多层次冗余设计，自物理层直至应用层全方位保障通信稳定性，物理层搭建双光纤环网，其自愈时间小于20ms，于光纤出现故障之际可快速切换链路，以此保证通信不中断，配备无线Mesh网络作为备用手段，在关键区域部署冗余AP，使得信号覆盖率达到99.9%，保证通信实现全面覆盖。协议层叠加心跳检测机制，连续3次心跳丢失便会自动切换链路，可及时察觉并处理通信链路故障，应用层针对关键指令采用CRC-32校验与双签名确认方式，借助校验码验证数据完整性，依靠双签名确认保证指令准确性，以此保证传输正确率大于等于99.99%。

2.2 软件冗余技术

软件冗余技术从控制逻辑和数据存储两方面保障系统的可靠性。控制逻辑采用“三取二表决”机制，三台控制器并行运行，各自独立处理数据并输出控制信号。输出结果经多数表决器仲裁，只有当至少两台控制器输出一致时，才执行相应的控制指令。这种机制可将随机硬件故障影响降低至1/1000，极大提高了控制逻辑的可靠性。

数据存储采用本地与云端冗余的方式。边缘节点配置SSD与NAND闪存双存储介质，实时数据同步写入，即使一种存储介质出现故障，另一种仍能保存数据。云端采用分布式存储系统，数据在三个物理节点备份，确保数据的安全性。在数据恢复方面，恢复点目标（RPO）≤5min，意味着数据丢失最多不超过5min；恢复时间目标（RTO）≤1h，能够在1h内完成数据恢复，保障系统在出现故障后能快速恢复正常运行。

3 基于可靠性的系统集成与验证

3.1 集成实施路径

系统集成的关键环节之一便是标准化接口设计。《油库自动化系统接口技术规范》的制定，将传感器、控制器以及管理平台的接口协议与数据格式进行

统一，这一举措能切实降低因协议转换而引发的故障。据了解，这类故障在以往系统运行中所占比例高达 15%。借助标准化接口，不同的设备和系统之间得以实现无缝衔接，数据传输更为流畅，进而降低了系统集成的复杂程度以及故障发生概率。

分阶段测试验证属于保障系统可靠性的关键手段，于单元测试阶段之时，会针对设备开展为期 72 h 的连续运行测试，着重去验证设备的精度以及稳定性，保证设备在长时间运行进程里始终保持良好性能，联调测试囊括 95% 的业务场景，模拟实际运行期间的各类状况，借此检验系统各部分之间的协同运作能力。压力测试是模拟故障情形，对系统的容错能力加以验证，关键功能恢复时间需小于 10 s，保证系统在遭遇突发故障时可迅速恢复至正常运行状态。

3.2 工程应用案例

中国石油安徽销售分公司的阜阳油库，作为典型的水路型油库，其自动化系统改造工程有着突出的示范价值。阜阳油库的输油管线长达 12.6t，途径 3 个行政村、5 处农田保护区以及颍河大堤。在过去，传统的人工巡检模式暴露出响应迟缓，难以迅速察觉安全隐患等一系列问题。

在改造期间，项目团队运用光纤光栅传感技术搭建起管道监测网络，并与智能终端设备相配合，达成数据的实时采集与传输。改造过后，传感器的平均无故障时间（MTBF）从 35000h 跃升至 62000h，误报率也从每月 5 次锐减到 0.5 次，数据采集的可靠性得到大幅提升。

在通信系统领域，通过布置双链路冗余架构，数据传输延迟从 200ms 缩短至 80ms，年均通信中断次数由 4 次降为 0 次，系统可用度从 99.2% 提高到 99.92%。从经济效益角度来看，系统改造收获了颇为可观的收益。非计划停机时间减少了 85%，这使得油库年均运营损失降低了约 1200 万元。就拿 2023 年冬季寒潮期间来说，自动化系统提前 3h 检测到管道冻堵风险，通过自动开启伴热系统，成功避免了重大事故，减少直接经济损失超过 200 万元。不仅如此，人工巡检工作量减少了 60%，同时引入 AI 视觉识别技术辅助巡检，将人工巡检的准确率从 78% 提升至 95%。另外，经由系统优化，单批次油品周转效率提高 18%，年吞吐量增加约 15 万 t，进一步提高了油库的运营效益。

3.3 持续改进机制

中石化江苏盐城石油分公司上冈油库所搭建的“监测 – 分析 – 优化”闭环体系，为系统可靠性的不断增强给出了有效途径。此油库所布置的系统健康管理模块融合了多源数据融合技术，能实时收集设备振动、电流、温度等 12 类参数，接着借由 D – S 证据理论来对数据开展可信度评定。利用模糊综合评价法构建出的设备健康度模型，把设备状态划分成正常、预警、故障这三个级别，一旦设备健康指数低于设定阈值，就会自动启动预警机制。

在机器学习算法的运用上，上冈油库运用 LSTM 神经网络对过往数据进行训练，预测设备老化趋势的精准度能超 85%。比如在对消防泵的监测过程中，系统提前 30 天就预测到轴承出现磨损故障，还生成了涵盖更换时间、备件清单的维护方案。依据预测结果所制定的个性化维护计划，让传统的事后维修转变为预防性维护。借助这一机制，上冈油库的设备维护成本降低了 25%，备件库存周转率提升了 40%。

4 结语

该项研究聚焦于油库安全管理自动化系统可靠性的提升，搭建起一套囊括风险分析、冗余设计以及系统集成的完备技术体系，借助对分层架构可靠性指标的量化、对关键环节的 FMEA 风险识别以及多层次冗余技术的部署，成功化解了传统系统在传感器误报、通信中断等方面存在的核心难题。工程实践显示，冗余设计可有效提升系统的可用性、数据传输准确性以及故障响应效率，达成安全风险与运营成本的双重降低，未来有必要融合物联网边缘计算、数字孪生等新兴技术，深入推进预测性维护与智能决策功能，促使系统朝着“自感知 – 自修复 – 自优化”的智能化冗余模式发展，为能源仓储领域的本质安全提供更为前沿的技术支持，帮助行业在数字化转型进程中实现安全与效率的协同共进。

参考文献：

[1] 李驾 . 智慧化石油库建设与安全防护管理 [J]. 石油库与加油站 ,2025,34(1):38-40.

[2] 张正澔 . 物联网技术在油库安全管理中的应用 [J]. 现代盐化工 ,2024,51(1):95-97.

[3] 张国跃 . 现代安防技术在油库安全管理中的应用研究 [J]. 石化技术 ,2024,31(5):332-334.

[4] 苏哲 . 智能化油库安全管理与应急预案研究 [J]. 石油石化物资采购 ,2024(16):166-168.

[5] 李涛 , 敬一平 , 严龙云 , 刘飞 . 云边端协同的智能油库作业及调度监控平台建设实践 [J]. 石油化工自动化 ,2025,61(1):67-72+96.

作者简介：

文馨 (1996.1-), 女 , 汉族 , 河南新野人 , 研究生 , 助理工程师 , 研究方向：工业自动化 , 智能控制系统 , 故障诊断 , 信息化平台。