

基于可靠性分析的安全仪表系统（SIS）优化策略

张 冰

国家管网集团北京管道有限公司 内蒙古 鄂尔多斯 017200

摘 要：安全仪表系统（SIS）作为工业过程与设施安全的关键保障，其可靠性直接关系到生产过程的安全性和稳定性。本文基于可靠性分析，深入探讨SIS系统的优化策略，旨在提高SIS系统的可靠性，降低故障率，确保工业过程的安全运行。通过文献综述、案例分析等方法，本文提出了包括冗余设计、故障检测与诊断、生命周期管理、独立性原则遵循以及人员培训在内的优化策略，为SIS系统的优化提供了参考。

关键词：安全仪表系统；可靠性分析；优化策略；冗余设计；生命周期管理

引言

随着工业自动化的不断发展，安全仪表系统（SIS）在石油、化工、电力等流程工业领域得到了广泛应用。SIS系统通过实时监测工艺参数，并在异常情况出现时迅速作出反应，有效预防事故的发生，保障人员、资产和环境的整体安全。然而，SIS系统的可靠性问题一直是工业界关注的重点。一旦SIS系统失效，可能导致严重的安全事故和经济损失。因此，基于可靠性分析对SIS系统进行优化显得尤为重要。

1 SIS 系统可靠性分析

1.1 SIS系统组成与功能

SIS（安全仪表系统）是工业过程控制中至关重要的一部分，它通常由传感器、逻辑运算器和执行元件三大核心组件构成，这些组件协同工作，以实现一个或多个安全仪表功能（SIF）。传感器作为SIS系统的“眼睛”，负责实时监测工艺过程中的各种关键参数，如温度、压力、流量等。这些参数是判断系统是否处于安全状态的重要依据。传感器将监测到的信号转换为电信号，并传递给逻辑运算器。逻辑运算器是SIS系统的“大脑”，它接收来自传感器的信号，并根据预设的安全逻辑进行判断和处理。当逻辑运算器检测到某个参数超出安全范围或系统出现异常状态时，它会立即触发相应的安全动作。执行元件则是SIS系统的“手脚”，它根据逻辑运算器的指令，迅速采取措施，如关闭阀门、启动紧急停车程序等，以防止危险事件的发生或减轻其后果^[1]。SIF（安全仪表功能）是SIS系统的核心，它是为了防止和减少危险事件的发生而设计的。每个SIF都具有特定的安全完整性等级（SIL），这是衡量SIS系统对特定危险事件保护能力的重要指标。SIL等级越高，表示SIS系统对该危险事件的保护能力越强。SIS系统在生产装置的开车、停车、运行以及维护期间都发挥着重要作用。它不仅能够

够确保生产过程的顺利进行，还能在异常情况下迅速采取措施，保护人员健康、装置设备及环境的安全。

1.2 可靠性评估方法

为了确保SIS系统的可靠性，需要对其进行全面的评估。目前，常用的SIS系统可靠性评估方法主要包括故障树分析（FTA）、失效模式与影响分析（FMEA）以及安全完整性等级（SIL）评估等。故障树分析（FTA）是一种逻辑分析方法，它通过分析系统故障事件的原因和结果，建立故障树模型。故障树模型以系统故障为顶事件，以导致系统故障的基本原因为底事件，通过逻辑门连接顶事件和底事件，形成树状结构。通过计算故障树模型中各底事件的发生概率，可以推导出顶事件的发生概率，即系统的故障概率。FTA方法能够直观地展示系统故障的传递路径，帮助工程师识别系统中的薄弱环节，并采取相应的改进措施。失效模式与影响分析（FMEA）是一种系统化的分析方法，它通过识别系统各组成部分的潜在失效模式及其影响，评估系统的可靠性。FMEA方法首先列出系统各组成部分的所有可能失效模式，然后分析每种失效模式对系统功能的影响程度，以及失效模式发生的可能性和可检测性。通过综合考虑这些因素，可以对系统的可靠性进行全面评估，并确定需要优先关注的失效模式。安全完整性等级（SIL）评估则是根据SIS系统对特定危险事件的保护能力，确定其所需的安全完整性等级。SIL评估过程包括危险事件识别、风险评估、目标SIL确定以及SIL验证等步骤。通过SIL评估，可以确保SIS系统具备足够的安全保护能力，以满足工业生产过程的安全需求。

2 SIS 系统优化策略

2.1 冗余设计

冗余设计是提高SIS系统可靠性的核心策略之一，其核心理念在于通过增加系统组件或子系统的数量，确保

即使部分组件发生故障,整个系统仍能维持其功能的完整性,从而显著提升系统的容错能力和稳定性。在硬件冗余方面,常见的冗余设计架构包括1oo2(一取二)、2oo3(二取三)等投票制系统。以1oo2系统为例,它意味着对于每一个关键的安全仪表功能(SIF),都采用两个独立的传感器或控制器来执行。当且仅当两个传感器或控制器都检测到异常信号时,系统才会触发安全动作。这种设计有效避免了单一组件故障导致的系统误动或拒动,提高了系统的可靠性。2oo3系统则是一种更为高级的冗余设计,它采用三个独立的传感器或控制器来执行同一个SIF。系统会根据三个组件的输出信号进行投票,只有当至少两个组件输出异常信号时,系统才会触发安全动作。这种设计不仅提高了系统的容错能力,还进一步降低了因组件故障导致的系统误动率^[2]。除了硬件冗余外,软件冗余也是提高SIS系统可靠性的重要手段。软件冗余通常通过在不同的处理器或计算机上运行相同的软件程序来实现。当主处理器或计算机发生故障时,备用处理器或计算机将立即接管控制,确保系统的连续运行。软件冗余还可以包括算法冗余,即采用多种不同的算法来计算同一个安全参数,以提高计算的准确性和可靠性。冗余设计的实施需要考虑多个因素,包括组件的可靠性、系统的复杂性、成本以及维护的便利性等。在实际应用中,需要根据系统的具体需求和约束条件,选择合适的冗余设计架构和组件。此外,冗余设计还需要与系统的故障检测与诊断机制紧密结合。通过实时监测和分析系统组件的运行状态,可以及时发现并处理潜在故障,确保冗余组件的可靠性和可用性。同时,定期的系统测试和验证也是确保冗余设计有效性的重要手段。

2.2 故障检测与诊断

故障检测与诊断是确保SIS(安全仪表系统)可靠性的至关重要环节。在工业生产过程中,SIS系统承担着防止和减轻危险事件的重要职责,因此,其运行状态的稳定性和可靠性直接关系到生产安全。通过实时监测SIS系统的运行状态,及时发现并处理故障,可以有效降低故障率,提高系统的整体可靠性。故障检测与诊断技术涵盖了SIS系统的各个组成部分,包括传感器、逻辑控制器以及执行元件等。在传感器故障诊断方面,由于传感器是SIS系统获取现场数据的关键设备,其准确性直接影响到系统对工艺过程的监控能力。因此,对传感器进行故障检测与诊断显得尤为重要。这通常包括监测传感器的输出信号是否稳定、是否存在异常波动或漂移,以及传感器与系统的通信是否正常等。一旦发现传感器故障,系统应能迅速识别并采取相应的替代措施或报警,以确

保数据的准确性和系统的连续性。逻辑控制器故障诊断则是确保SIS系统逻辑判断准确性的关键。逻辑控制器负责根据传感器的输入信号进行逻辑运算,并决定是否触发安全动作^[3]。因此,对逻辑控制器的故障检测与诊断需要关注其运算过程的正确性、逻辑规则的完整性以及与其他系统组件的通信状态等。通过定期的逻辑测试、模拟故障注入以及在线监测等手段,可以及时发现并处理逻辑控制器的潜在故障,确保系统的逻辑判断准确无误。执行元件故障诊断则是确保SIS系统能够迅速、准确地执行安全动作的重要保障。执行元件如阀门、紧急停车装置等,是SIS系统直接作用于工艺过程的关键设备。对其故障检测与诊断需要关注其动作是否迅速、准确,是否存在卡滞、泄漏或损坏等问题。通过定期的执行元件测试、在线监测以及维护检查等手段,可以及时发现并处理执行元件的故障,确保系统能够在紧急情况下迅速响应并执行安全动作。

2.3 生命周期管理

SIS(安全仪表系统)的生命周期管理是一个全面、系统的过程,它涵盖了从设计、制造、安装、调试到运行、维护、升级直至停用的每一个阶段。通过实施严格的生命周期管理,可以确保SIS系统在持续运行的过程中始终维持其应有的安全防护功能,为工业生产提供坚实的安全保障。在设计阶段,生命周期管理着重于确保SIS系统的设计满足特定的安全需求和标准。这包括确定系统的安全完整性等级(SIL)、选择合适的硬件和软件组件、设计合理的系统架构以及制定详细的系统规范等。设计阶段的工作为SIS系统的后续制造、安装和调试奠定了坚实的基础。在制造阶段,生命周期管理关注于确保SIS系统的硬件和软件组件按照设计要求进行生产和测试。这包括对传感器、逻辑控制器和执行元件等关键组件的严格质量控制,以及对系统软件的详细测试和验证。制造阶段的工作确保了SIS系统的组件具有高度的可靠性和稳定性。安装和调试阶段是SIS系统生命周期中的关键环节。在这个阶段,需要确保系统的所有组件都按照设计要求正确安装,并且系统能够正常运行。调试过程包括对系统的功能测试、性能测试和安全性测试等,以确保系统能够满足预期的安全防护要求。在运行阶段,生命周期管理着重于确保SIS系统的持续可靠运行。这包括定期验证测试、预防性维护、实时监控和故障处理等。定期验证测试可以确保系统的功能和诊断能力符合设计要求,及时发现并处理潜在问题。预防性维护则通过定期检查、清洁和更换易损件等措施,延长系统的使用寿命并减少故障发生的可能性。系统升级和设备更

换是生命周期管理中不可或缺的一部分。随着技术的不断进步和工业生产需求的变化, SIS系统可能需要进行升级或更换某些设备以保持其技术先进性和可靠性。系统升级可以包括硬件升级、软件升级或系统架构的优化等, 以提高系统的性能和安全性^[4]。

2.4 独立性原则遵循

SIS(安全仪表系统)必须严格遵循独立性原则, 与基本过程控制系统(BPCS)等其他控制系统保持独立。这种独立性是确保SIS能够在紧急情况下独立采取行动、迅速响应并有效防止事故扩大的关键。独立性不仅体现在物理层面的分隔, 如单独的硬件设备、独立的布线系统和隔离的通信网络, 更涵盖了电气和逻辑上的独立隔离。在电气隔离方面, SIS系统应采用独立的电源供电, 避免与BPCS等系统共享电源, 以减少因电源故障导致的系统失效风险。同时, SIS系统的接地系统也应与BPCS等系统分开, 确保电气信号的稳定性和可靠性。在逻辑隔离方面, SIS系统的控制逻辑应与BPCS等系统完全独立, 避免逻辑上的相互干扰和影响。这意味着SIS系统的输入输出信号、控制算法和决策逻辑都应独立设计, 确保其在任何情况下都能独立判断并采取正确的安全动作。通过遵循独立性原则, SIS系统能够有效降低因外部因素(如BPCS系统的故障、网络攻击或电磁干扰等)导致的失效风险, 提高系统的可靠性和安全性。同时, 独立性原则还要求SIS系统的维护、测试和验证工作也应独立进行, 确保系统的完整性和可靠性得到持续保障。

2.5 人员培训

操作人员作为SIS系统的直接使用者, 其专业水平和操作技能对系统的稳健性至关重要。因此, 必须建立周密的培训体系, 确保操作人员接受全面的专业培训。培训内容应涵盖SIS系统的基本功能、工作原理、操作界面、故障处理流程以及系统维护知识等。操作人员需要

熟知系统的各项功能, 能够熟练操作系统界面, 掌握故障排查和处理的方法, 以及了解系统维护的基本要求和流程。除了系统操作和维护知识的培训, 培训内容还应包括事故应急处理的模拟演练。通过模拟真实的事故场景, 让操作人员亲身体验应急处理过程, 提高其应对突发事件的能力和反应速度。同时, 模拟演练还可以检验操作系统的有效性和可操作性, 为实际应急处理提供有力的支持。此外, 培训内容还应包括对安全规范的定期学习。安全规范是确保SIS系统稳健运行的重要保障, 操作人员必须熟悉并严格遵守相关安全规范, 确保系统的安全性和可靠性。通过定期学习和考核, 可以促使操作人员不断更新安全知识, 提高安全意识, 为SIS系统的稳健运行提供有力的人员保障。

结束语

基于可靠性分析对SIS系统进行优化是提高工业生产安全性的重要手段。通过冗余设计、故障检测与诊断、生命周期管理、独立性原则遵循以及人员培训等措施的实施, 可以显著提高SIS系统的可靠性, 降低故障率, 确保工业过程的安全运行。未来, 随着工业自动化的不断发展, SIS系统的优化策略将不断完善和发展, 为工业生产提供更加可靠的安全保障。

参考文献

- [1]姜巍巍,李玉明,王春利,等.安全仪表系统安全完整性等级(SIL)评估技术应用[J].中国仪器仪表,2009(2):48-51.
- [2]许忠仪.安全仪表系统(SIS)的SIL评估[J].化工自动化及仪表(5):66-70.
- [3]张斌,阳宪惠,康荣学.安全仪表系统中参数满足某分布区间时的SIL评估方法[J].化工自动化及仪表,2008,35(5):33-37.
- [4]龙飞.安全仪表系统及其SIL评估技术在歧化装置中的应用[D].华东理工大学,2015.