化工自动化仪表中安全仪表系统的设计与可靠性分析

高如意
山西焦化集团有限公司　山西　临汾　041606

摘　要：在现代化工生产过程中，安全是不可逾越的红线。安全仪表系统（Safety Instrumented System, SIS）作为抵御灾难性事故的最后一道自动化防线，其设计的科学性与运行的可靠性直接关系到人员、资产及环境的安全。本文旨在深入探讨化工自动化仪表领域中SIS的设计原则与可靠性保障机制。文章首先阐述了SIS的基本概念、功能；随后，从安全完整性等级（SIL）定级、系统架构、硬件选型、软件开发及人机界面等维度，系统论述了SIS的设计方法论；最后，重点剖析了SIS可靠性的内涵，详细介绍了基于IEC 61508/61511标准的可靠性建模、定量分析、验证以及贯穿全生命周期的维护策略。通过本文的探讨，旨在为化工行业SIS的工程实践提供理论参考，强调以标准化、系统化的方法构建高可靠性的安全保障体系。

关键词：安全仪表系统（SIS）；安全完整性等级（SIL）；可靠性

引言

化工生产具有高温、高压、易燃、易爆、有毒及强腐蚀等高风险特征，装置大型化与流程复杂化进一步加剧了潜在危险。DCS系统在极端工况下安全裕度不足，难以有效防控重大事故。为此，独立于DCS系统的安全仪表系统（SIS）成为现代化工安全体系的核心。SIS依据IEC 61508/61511等国际功能安全标准设计，旨在当温度、压力、液位等关键参数超限时，以高置信度自动执行紧急停车、切断物料等安全动作，将工艺带入安全状态。其有效性依赖两大支柱：一是设计正确性，包括系统架构、组件选型与逻辑功能满足安全目标；二是运行可靠性，即在数十年服役期内，按需正确执行安全功能的概率须持续达标。系统研究SIS的设计与可靠性，对提升化工本质安全水平具有重要意义。在国内市场，浙大中控的TCS-900系统凭借其高可靠性和成熟的工程应用，已成为众多大型化工企业的首选。该系统采用三重化（2oo3）冗余架构，支持SIL3等级的安全功能，并集成了先进的在线诊断和部分行程测试（PST）技术，能有效降低平均要求时失效概率（PFDavg），显著提升了整个安全回路的可靠性。

1 安全仪表系统（SIS）概述

一个完整的SIS通常由三个基本部分协同工作来实现其保护功能。首先是传感器，它负责实时监测关键的过程变量，例如温度、压力、液位或流量，并将这些物理量精确地转换为可供后续处理的电信号。其次是逻辑控制器，它扮演着SIS“大脑”的角色，持续接收来自传感器的信号流，并依据预先设定的安全逻辑程序进行实时判断；一旦检测到过程状态已进入危险区域，逻辑控制器便会立即向最终执行元件发出明确的指令。最终执行元件，通常是具备快速响应能力的切断阀或电机驱动器等设备，其任务是忠实执行逻辑控制器的命令，通过改变阀门的开闭状态或启停关键设备等物理动作，强制性地将整个工艺过程带入一个预设的安全状态。这三个环节环环相扣，共同构成了一个或多个独立的安全仪表功能（SIF）回路，每个回路都针对特定的危险场景提供专门的保护。

2 安全仪表系统（SIS）的设计原则与方法

2.1 基于SIL等级的系统架构设计

IEC 61508标准通过“结构约束”这一概念，将SIL等级与系统的硬件容错能力紧密绑定。为了满足不同SIL等级对硬件故障裕度（HFT）的要求，冗余设计成为SIS工程中的普遍实践。例如，对于低风险的应用，可能采用单一通道的1oo1架构；而对于需要更高安全性的场合，则倾向于使用双通道的1oo2架构，该架构下任一通道检测到危险即可触发安全动作，虽然这会略微增加误停车的可能性，但极大地提升了安全性[1]。在化工行业主流的SIL2和SIL3应用中，三重化的2oo3架构因其卓越的平衡性而被广泛采纳，它要求三个并行通道中至少有两个同时确认危险状态才会执行安全动作，这种设计既能有效抑制随机硬件故障带来的风险，又能通过表决机制避免单点故障导致的非计划停车，从而在安全性和可用性之间取得了最佳的折衷方案。这种冗余思想不仅适用于逻辑控制器，也同样应用于传感器和最终执行元件，以构建端到端的高完整性安全回路。

2.2 硬件选型与认证

在硬件选型阶段，所有用于SIS的关键设备，包括

传感器、逻辑控制器的I/O及处理模块、以及阀门和执行机构等，都必须选用那些已经获得权威第三方机构（如TÜV、Exida等）颁发的功能安全认证的产品。这些认证不仅仅是市场准入的标签，更重要的是，它们证明了产品在设计上已经满足了IEC 61508标准对相应SIL等级所规定的硬件安全完整性和系统性能力要求。此外，认证过程还会产生进行SIL验证所必需的关键失效数据，例如安全失效分数（SFF）、诊断覆盖率（DC）以及各类失效率（λ）等。这些数据是后续进行可靠性定量计算不可或缺的输入。除了关注产品的SIL认证等级外，工程师还必须综合考虑其在实际工厂环境中的适应性，包括工作温度范围、防爆等级、防护等级（IP代码）、电磁兼容性（EMC）性能以及与现有控制系统的接口兼容性等因素，以确保所选设备能够在严苛的工业现场长期稳定可靠地工作。

2.3 软件开发与V模型

随着可编程电子技术的普及，现代SIS的逻辑控制器内部运行着复杂的嵌入式软件，其可靠性对整个系统的安全性能有着决定性影响。IEC 61508标准对安全相关软件的开发提出了极为严格的要求，并推荐采用V模型作为其开发流程。V模型的核心思想在于强调开发活动与验证活动的同步性和对应性。在模型的左侧，开发工作从顶层的系统安全需求开始，逐层向下分解为软件架构设计、模块设计，直至最底层的详细代码实现[2]。与此同时，在模型的右侧，验证工作则自下而上进行，从针对最小代码单元的单元测试，到模块间的集成测试，再到整个软件系统的全面测试，最终完成与硬件结合的系统验收测试。这种一一对应的结构确保了在开发的每一个层级上产生的输出物，都能立即得到相应层级测试活动的检验和确认。通过这种方式，软件缺陷得以在生命周期的早期被发现和修复，从而最大限度地降低了将错误带入最终产品的风险，为SIS软件的高可靠性提供了坚实的流程保障。

2.4 人机界面（HMI）与辅助设施设计

SIS的人机界面（HMI）设计主要目的并非用于日常的过程操控，而是要在任何时刻，尤其是紧急情况下，向操作员提供关于SIS自身状态的即时、准确且易于理解的信息。这包括系统是处于正常的待命状态，还是已被人为旁路，或是内部发生了故障，抑或已经成功触发了安全动作。为了达到这一目标，HMI设计应极力避免使用复杂的动态图形、闪烁动画或过多的颜色，而应采用标准化的、高对比度的静态显示，并配以简洁明了的文字说明。通常，红色被用来表示危险状态或已执行的动作，绿色则代表系统健康和正常。此外，SIS的可靠性还依赖于一系列高质量的辅助设施。其供电系统必须配备不间断电源（UPS）和冗余配置，以抵御电网波动或中断；接地系统需精心设计，以消除共模干扰和地电位差；信号线路应采取有效的隔离和屏蔽措施，防止来自DCS系统或其他强电设备的噪声耦合；同时，完善的防雷和浪涌保护装置也是必不可少的，它们共同构成了SIS抵御外部恶劣电气环境的坚固屏障，确保其核心功能不受干扰。

3 安全仪表系统（SIS）的可靠性分析与保障

3.1 可靠性的内涵与度量

在功能安全的专业语境下，SIS的可靠性有着非常明确的定义，它特指系统在被需要时能够成功执行其预定安全功能的能力，而非传统意义上设备长时间无故障运行的可用性。这一核心概念通过一个关键的量化指标——平均要求时失效概率（PFDavg）来精确衡量。PFDavg代表了在SIS被工艺过程要求执行安全动作的那个关键时刻，系统由于自身存在未被检测到的危险故障而无法正确响应的平均概率。这是一个介于0和1之间的数值，越接近0，表示系统越可靠。国际标准IEC 61511为不同的安全完整性等级（SIL）设定了严格的PFDavg范围，例如，要达到SIL2等级，一个SIF回路的PFDavg计算值必须落在0.01至0.001的区间内。因此，SIS的设计与验证工作，本质上就是围绕如何将PFDavg控制在目标SIL所允许的上限之下而展开的。

3.2 可靠性建模与定量分析

为了科学地评估一个SIF回路是否能够满足其目标SIL所要求的PFDavg，必须对其进行严谨的可靠性建模和定量计算。可靠性框图法（RBD）是一种相对直观的方法，它将SIF回路中的传感器、逻辑解算器和最终元件等视为串联或并联的模块，利用概率论公式直接计算整个回路的PFDavg，适用于架构较为简单的系统。相比之下，故障树分析法（FTA）则是一种更为强大的演绎分析工具。它从“SIF未能正确执行”这一顶事件出发，自上而下地逐层剖析所有可能导致该失败的硬件随机失效、系统性失效以及共因失效等基本事件，并通过逻辑门（如“与门”、“或门”）建立起它们之间复杂的因果关系网络。FTA不仅能给出精确的PFDavg数值，还能通过重要度分析识别出对系统整体可靠性影响最大的薄弱环节，为设计优化提供极具价值的洞见[3]。对于包含复杂在线诊断、部分行程测试（PST）和维修策略的先进SIS，马尔可夫模型则能提供最高精度的分析结果。该方法将系统生命周期划分为一系列离散的状态，并通过建立状态转移方程来动态模拟故障的发生、检测和修复过程，从而得出

最为贴近实际的PFDavg值。无论采用何种方法，其分析的准确性都高度依赖于输入的组件失效数据的真实性和系统架构描述的完整性。

3.3 SIL验证与结构约束

SIL验证是SIS工程中承上启下的关键环节，其目的是确认已完成的设计方案确实能够满足SRS中规定的目标SIL要求。这一验证过程包含定量与定性两个不可分割的方面。定量验证即前述的PFDavg计算，通过数学模型证明系统的危险失效概率已降至可接受水平。然而，仅有计算达标是不够的，IEC 61508标准还设定了“结构约束”这一硬性门槛。结构约束规定了为达到某一SIL等级，系统硬件架构必须具备的最低容错能力（HFT）。这意味着，即使一个极其简单的1oo1单通道架构通过选用超高可靠性的元件使其PFDavg计算值进入了SIL2的范围，但由于其硬件故障裕度为零，不满足SIL2对HFT ≥ 1的结构性要求，该设计依然是无效的。因此，一个成功的SIL验证必须同时通过定量计算和定性结构的双重考验，确保SIS不仅在概率上可靠，在架构上也同样健壮。

3.4 运行维护与可靠性保障

必须建立一套系统化的运行维护策略。这首先包括按照SRS和设备制造商的建议，严格执行定期的检验与测试计划。测试可以是完全行程测试，即让阀门全关全开以验证其机械功能，也可以是更为先进的部分行程测试（PST），后者能在不影响生产的情况下检测阀门大部分的潜在故障。其次，随着技术的发展，遵循GB/T 44988-2024等新标准对SIS实施在线监视变得日益重要，通过对关键参数和诊断信息的实时采集与分析，可以实现对系统健康状况的连续评估和故障的早期预警。再者，任何对SIS的修改，无论多么微小，都必须纳入严格的变更管理流程，重新评估变更对原有SIL的影响，并在必要时重新进行部分或全部的验证工作，以防止“不经意的改动”侵蚀了系统的安全完整性[4]。最后，完整、准确、及时的文档记录贯穿于SIS生命周期的始终，它不仅是追溯历史、分析问题的依据，也是进行持续改进和满足合规审计要求的基础，是保障SIS长期可靠运行不可或缺的软性支撑。

4 结语

安全仪表系统（SIS）是化工自动化领域守护生命与财产安全的终极屏障。其价值的实现，深深植根于科学严谨的设计与持续可靠的运行之中。本文通过对SIS设计与可靠性两大核心方面的系统探讨，揭示了其背后深刻的工程逻辑。在设计层面，必须以全生命周期管理为纲，以SIL定级为指引，以SRS为依据，通过合理的冗余架构、经过认证的硬件、规范的软件开发流程以及安全导向的辅助设计，构建一个内在坚固的系统。在可靠性层面，必须超越定性的“高可靠”描述，运用FTA、RBD或马尔可夫模型等工具进行精确的定量分析，并结合结构约束进行综合验证。更重要的是，要认识到可靠性是一个动态属性，必须通过制度化的运行维护、在线监视和变更管理，在漫长的服役岁月中不断加以巩固和保障。

参考文献

[1]马小军.安全仪表系统（SIS）在化工过程控制中的应用与评估[J].中国仪器仪表,2026,(04):41-45.

[2]张晓峰.化工安全仪表控制系统集成架构的发展趋势与功能安全优化研究进展[J].中国化工贸易,2026,18(09):25-27.

[3]严阳.化工行业安全仪表系统(SIS)失效模式解析及适配性可靠性提升对策研究[J].中国石油和化工标准与质量,2026,46(01):146-147+150.

[4]刘洪波.化工企业安全仪表系统可靠性与经济性研究[J].中国化工贸易,2025,17(28):70-72.