天然气场站自动化控制系统的功能安全需求分析与逻辑设计

周敬桢　王海鹏
国家管网集团北京管道有限公司河北输油气分公司永清作业区　河北　廊坊　065600

摘　要：我国能源结构优化、“双碳”目标推进，天然气作为清洁高效化石能源，在国家能源体系中的地位愈发重要。天然气场站是连接上下游的枢纽，其安全稳定高效运行意义重大。自动化控制系统是保障场站安全的核心，功能安全是系统设计生命线。本文以国际功能安全标准IEC61508及行业特定标准IEC61511为依据，深入剖析天然气场站运行中的主要危险源与风险场景，开展功能安全需求分析。在此基础上，提出一套基于安全仪表系统（SIS）的完整功能安全逻辑设计方案，涵盖安全仪表功能识别分配、安全完整性等级定级、逻辑控制器架构选择、输入/输出设备冗余配置及软件逻辑实现策略，为天然气场站自动化控制系统设计、实施与运维提供科学、规范且可操作的工程指导。

关键词：天然气场站；功能安全；安全仪表系统（SIS）；安全仪表功能（SIF）

引言

天然气作为易燃易爆危险介质，其输送、储存与分配过程风险高。天然气场站内设备多样，一旦发生泄漏、火灾等事故，会造成财产损失、危及人员生命，影响周边环境与社会稳定。近年来国内外多起天然气场站安全事故，如美国PG&E管道爆炸事故，凸显功能安全失效的灾难性后果。传统依赖操作员经验和基本过程控制系统的安全防护模式，难以满足现代天然气场站对本质安全的要求。自动化控制系统需具备独立可靠执行预定安全功能的能力，即功能安全，其核心是危险发生时能将系统引导至安全状态、降低风险[1]。因此，对天然气场站自动化控制系统进行功能安全需求分析与逻辑设计，是响应法规标准的必然要求，也是提升本质安全、保障能源动脉畅通的关键路径。

1 功能安全基础理论与标准体系

1.1 功能安全核心概念

功能安全是受控设备（EUC）及其控制系统整体安全的一部分，取决于安全相关系统（SRS）正确执行安全功能的能力，核心目标是把风险降至可容忍水平。为实现此目标，有系列关键概念：安全仪表系统（SIS）用于实现一个或多个安全仪表功能（SIF），独立于基本过程控制系统（BPCS），由传感器、逻辑解算器和最终执行元件构成；SIF是SIS执行的具体安全任务，如入口压力超阈值时自动关闭紧急切断阀；为量化SIF可靠性要求，引入安全完整性等级（SIL），从SIL1到SIL4离散分级，等级越高，SIF成功执行概率要求越高，平均失效概率（PFDavg）越低。这些概念是功能安全设计的理论基石。

1.2 IEC61511标准框架

IEC61511是IEC61508在过程工业（包括石油、化工、天然气）的具体化，它定义了SIS从概念设计到退役的全生命周期各阶段的活动。该标准框架的核心流程始于危害与风险分析，通过系统化的方法识别潜在的危险事件。随后，采用保护层分析（LOPA）等半定量工具对风险进行量化，并据此确定是否需要SIF以及所需的SIL等级。在明确了安全需求后，进入SIS的设计与工程阶段，此阶段需严格按照SIL要求，完成硬件架构、软件逻辑和验证方案的详细设计。之后，通过严格的安装、调试与确认程序，确保SIS按设计意图正确部署并能有效执行SIF。系统投运后，还需制定详尽的操作与维护规程，包括定期的功能测试，以维持SIS在整个生命周期内的可靠性。最后，任何对SIS的修改或最终的退役都必须纳入变更管理流程，确保其安全完整性不受损害。本文的研究工作主要聚焦于这一生命周期的前两个关键阶段——需求分析与逻辑设计。

2 天然气场站危险源辨识与风险分析

有效功能安全设计需先全面准确识别天然气场站危险源及事故场景。

2.1 主要危险源

天然气场站危险源多样复杂。物理上，高压环境、极低温条件、高速流体存在直接物理伤害风险；化学上，天然气易燃易爆，爆炸极限范围宽，还有窒息性，泄漏隐患大；设备方面，阀门内漏或外漏、管道裂纹、法兰密封失效、仪表故障、电气火花等常见；人为因素也不容忽视，操作人员误操作、维护保养疏忽、初始设计缺陷都可能引发事故。

2.2 典型风险场景

基于危险源，场站有诸多高风险场景。超压风险突出，源于上游供气异常、调压阀失效或下游用气骤停，可能致管道或容器物理爆炸；欠压风险在特定工况下，气化能力不足或下游用气激增，管网压力过低会吸入空气形成新爆炸环境；泄漏风险贯穿始终，设备问题或外部破坏引发泄漏，遇点火源会触发火灾或爆炸[2]。这些风险场景相互关联升级，如超压未控可能致设备破裂、大规模泄漏和火灾爆炸。LNG场站还有特有风险，如低温灼伤、可燃蒸气云，以及储罐内部翻滚和快速相变等，为功能安全需求分析提供依据。

3 功能安全需求分析

功能安全需求分析的目标是将上述风险场景转化为具体的、可执行的SIF及其对应的SIL要求。

3.1 SIF的识别与定义

SIF的识别是一个严谨的系统工程，通常在HAZOP（危险与可操作性分析）研究的基础上深化展开。其核心思想是，针对每一个被识别出的、且现有保护措施不足以将其风险降至可接受水平的工艺偏差，都需要考虑设置一个独立的保护层，即SIF。这个过程要求工程师将抽象的风险场景具象化为明确的控制逻辑。以“入口超压”这一典型场景为例，其对应的SIF可以被精确定义为：当入口管线的压力信号持续高于预设的高高限值（PSHH）时，系统应自动执行一系列安全动作，包括关闭上游的紧急切断阀（ESDV）以隔离气源，并同步打开站内的放空阀（BDV）以安全泄放超压气体，最终目标是将整个场站的压力引导至一个安全的稳态。每个SIF的定义都必须清晰、无歧义，完整地阐明其触发条件（输入信号）、判断逻辑（何时动作）和预期的安全动作（输出指令），这是确保后续设计准确无误的前提。

3.2 SIL定级方法——保护层分析（LOPA）

在SIF被识别出来之后，必须为其分配一个合适的SIL等级，以明确其可靠性要求。保护层分析（LOPA）作为一种半定量的风险评估方法，为此提供了科学、客观的决策依据。LOPA分析首先需要确定引发特定危险场景的初始事件的发生频率，例如上游调压阀失效导致超压的年发生率。接着，评估该场景一旦发生可能造成的后果严重度，并据此确定社会或企业所能容忍的该事件的最大发生频率。通过计算初始频率与可容忍频率的比值，即可得到所需达到的总风险降低因子（TotalRRF）。随后，分析人员需要逐一审视现有的、独立的保护层（IPL），如基本过程控制系统的调节回路、报警后操作员的人工干预、安全阀的物理泄放等，并为每个有效的IPL赋予一个合理的风险降低因子。将总RRF除以所有现有IPL的RRF乘积，便得到了新增SIF所需提供的风险降低能力[3]。最后，根据这个数值，对照SIL等级与风险降低因子（RRF）或平均失效概率（PFDavg）的对应关系表，即可确定该SIF应达到的SIL等级。通过这一系统化的LOPA流程，能够有效避免功能安全设计中的主观臆断，确保安全投入既充分又不过度，实现了风险控制的精准化管理。

4 功能安全逻辑设计

在明确了SIF和SIL要求后，即可进入SIS的详细逻辑设计阶段。设计的核心原则是独立性、可靠性和可验证性。

4.1 SIS架构设计

SIS的架构设计是其实现高可靠性的物理基础，必须严格匹配所分配的SIL等级对硬件安全完整性的要求。不同的架构在安全性、可用性和成本之间各有权衡。单通道的1oo1架构虽然成本低廉，但其可靠性仅能满足最低的SIL1要求，且一旦故障即丧失保护功能。双通道的1oo2架构通过任一通道动作即触发的方式，极大地提升了安全性，但同时也增加了因单一通道误报而导致系统误停车的风险。相反，2oo2架构要求两个通道同时确认危险才动作，虽然降低了误动作率，但对共因失效极为敏感，即一个共同的干扰源可能同时使两个通道失效，从而导致保护功能完全丧失。综合来看，三通道的2oo3架构因其卓越的平衡性而成为高等级SIL应用的首选，它要求三个通道中有任意两个确认危险才触发安全动作，这不仅显著提高了安全性，还具备良好的抗共因失效能力和较高的系统可用性。因此，对于天然气场站中诸如入口超压保护这类关乎全局安全的关键SIF，采用2oo3架构通常是最佳实践。

4.2 输入/输出设备选型与配置

SIS的可靠性不仅取决于其核心逻辑解算器，同样高度依赖于其感知危险的“感官”（传感器）和执行命令的“四肢”（最终执行元件）。在传感器选型上，必须选用专为安全应用设计、并通过相应SIL认证的高可靠性设备。对于SIL2及以上等级的SIF，普遍采用冗余配置策略，例如使用三台压力变送器并通过2oo3表决来获取一个可靠的测量值，以此消除单点故障的影响。传感器的安装细节，如引压管的走向、伴热防冻措施等，也需精心设计，以防止堵塞、冻结等外部因素导致信号失真。在最终执行元件方面，紧急切断阀（ESDV）扮演着至关重要的角色[4]。其选型需综合考量阀门类型、执行机构的驱动力和响应速度、故障安全位置（通常为故障关FC）、全行程关闭时间以及密封性能（如内漏等级）等多个维度。与传感器类似，对于极高安全要求的场合，也可考虑阀

门本身的冗余设计。逻辑解算器作为SIS的“大脑”，通常采用经过权威机构认证的专用安全PLC。这类控制器内部往往集成了三重化（TMR）或双通道自诊断等高级架构，能够实时监测自身健康状态，并在检测到故障时导向安全，从而满足SIL3甚至更高的安全完整性要求。

4.3 安全逻辑软件设计

为确保软件的正确性和鲁棒性，开发过程必须遵循严格的规范。在编程语言的选择上，应优先采用结构化文本（ST）或功能块图（FBD）等高级语言，因为它们逻辑清晰、易于追溯和验证，而应避免使用难以理解和维护的底层指令。在设计原则上，首要的是贯彻“故障安全”（Fail-Safe）理念，即无论系统内部发生何种类型的故障（如通信中断、电源波动、CPU错误），其最终行为都必须是导向预设的安全状态。其次，必须对所有开关量输入信号施加防抖（De-bouncing）处理，以滤除因接点抖动或电磁干扰产生的瞬时毛刺，防止误触发。此外，合理设置时间延迟也至关重要，例如在超压判断前加入短暂的确认延时，可以有效区分真实的危险工况与瞬时干扰；而在SIF复位前设置必要的等待时间，则能确保危险已彻底解除。逻辑中还需清晰地定义各种联锁和许可条件，例如，只有在特定的工艺条件下才允许对某个SIF进行旁路操作。关于旁路管理，必须设计一套安全的逻辑，包括操作授权、行为记录和超时自动恢复等功能，并对旁路的持续时间进行严格限制，以最大限度地降低因人为干预带来的安全风险。

4.4 人机界面（HMI）与操作员交互

尽管SIS强调其独立性，但操作员作为最后一道防线，其与SIS的有效交互同样重要。为此，SIS的人机界面（HMI）应在物理或逻辑上与BPCS的HMI进行隔离，以维持其独立性并防止相互干扰。在SIS的HMI上，所有安全仪表功能（SIF）的状态——包括正常、报警、已触发、处于旁路等——都必须清晰、直观地呈现给操作员。同时，SIS自身的健康诊断信息，如模块故障、通信异常等，也应实时显示，以便于维护人员及时发现潜在问题。HMI上还需提供必要的操作接口，如手动触发紧急停车、执行SIF复位等，但所有这些关键操作都必须辅以严格的权限管理和详尽的操作日志记录，确保任何操作都有据可查，责任可追溯，从而在保障安全的同时，也规范了操作行为。

5 结语

天然气场站自动化控制系统功能安全是国家能源基础设施安全运行的基石。本文系统阐述从危险源辨识到SIS逻辑设计的完整方法论。研究表明，风险驱动是前提，需基于科学风险评估确定功能安全需求，保障安全投入精准有效；独立性是核心，SIS要在物理和逻辑上独立于BPCS，避免共因失效；全生命周期管理是关键，功能安全贯穿SIS全过程，需建立完善体系。未来，数字化、智能化发展下，功能安全将与网络安全深度融合形成综合防护体系，先进方法也将引入功能安全设计以提升效率和质量。本文的设计框架和案例能为相关工程实践提供参考，助力我国天然气行业高质量、安全发展。

参考文献

[1]赵舒青.天然气场站自动化控制系统开发研究[J].中国设备工程,2020,(10):227-228.

[2]刘浩,郭伟,韩玉龙.天然气场站自动化与智能化建设研究[J].自动化应用,2024,65(11):255-257.

[3]滕玉龙.浅谈天然气场站电气自动化设备安全运行的对策分析[J].中国设备工程,2021,(08):65-66.

[4]李智.如何加强天然气场站电气自动化设备的可靠性[C]//中国智慧工程研究会智能学习与创新研究工作委员会.2020万知科学发展论坛论文集（智慧工程三）.重庆巴南天然气有限责任公司;,2020:696-704.