ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 42834—2023

油气管道安全仪表系统的功能安全 运行维护要求

Functional safety of safety instrumented system in oil and gas pipelines—Operation and maintenance requirements

2023-08-06 发布　　2024-03-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：国家石油天然气管网集团有限公司科学技术研究总院分公司、国家管网集团西南管道有限责任公司、机械工业仪器仪表综合技术经济研究所、国家管网集团北方管道有限责任公司、上海燃气工程设计研究有限公司、浙江中控技术股份有限公司、中国石油天然气管道工程有限公司、中国矿业大学(北京)、西南石油大学、美卓伦仪表(常州)有限公司。

本文件主要起草人：李秋娟、刘瑶、徐德腾、帅冰、刁宇、吕峰、崔涛、史学玲、董秀娟、陈朋超、马铁量、陈小华、朱明露、孙向东、郭苗、马云宾、雷柏伟、王健、王磊、孙勇、刘超、陈超声、张杰、靳江红、魏振强、姜念琛、孙永康、周力、杨阳、朱杰、熊文泽、聂中文、刘国豪、李睿、孙舒、卜志军、李东阳、张亚彬、相桂生、刘东、彭国茂、吴志峰、王爱玲、贾彦杰、施隋靖、胡协兰、张韬、赵俊丹、朱桂龙、杜康、朱玉琪。

引　言

安全仪表系统(SIS)是在20世纪八九十年代发展起来的,以其高可靠性、安全性和灵活性在油气管道领域内得到了广泛的应用。执行SIS并对危险工艺状态作出正确响应,可降低危险事件的发生频率或减轻危险事件的后果,因此SIS是保障油气管道生产安全的重要措施。目前国际上已发布相关的功能安全基础标准IEC 61508(所有部分)及针对过程工业的功能安全应用标准IEC 61511(所有部分),我国已将其转化成GB/T 20438(所有部分)《电气/电子/可编程电子安全相关系统的功能安全》和GB/T 21109(所有部分)《过程工业领域安全仪表系统的功能安全》。

油气管道SIS的功能安全系列标准是GB/T 20438(所有部分)和GB/T 21109(所有部分)在油气管道领域的应用。制定该系列标准目的在于规范油气管道领域内SIS各生命周期阶段活动的技术要求、管理要求和应用原则,促进SIS在油气管道领域内的应用和管理的规范化,确保油气管道系统安全可靠运行。目前该系列标准已发布GB/T 32202《油气管道安全仪表系统的功能安全　评估规范》和GB/T 32203《油气管道安全仪表系统的功能安全　验收规范》。

制定本文件的目的在于指导和规范油气管道领域SIS的功能安全运行维护活动,以确保其达到和保持功能安全。

油气管道安全仪表系统的功能安全 运行维护要求

1 范围

本文件规定了油气管道安全仪表系统的运行维护依据、人员要求、运行要求、维护要求、故障处理要求以及管理要求。

本文件适用于油气管道的安全仪表系统运行维护工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 32202—2015 油气管道安全仪表系统的功能安全 评估规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

危险失效 dangerous failure

使给定的安全动作受阻或无法执行的失效。

注1：只有在针对一个给定的SIF时，才可以说某个失效是“危险”的。

注2：实施了故障裕度时，一个危险失效可导致：

- SIF降级，这种情况下可执行安全动作，但是会有更高的PFD或PFH，或
- SIF失效，这种情况下完全无法执行安全动作或已经诱发了危险事件。

注3：没有实施故障裕度时，所有的危险失效都会导致SIF失效。

[来源：GB/T 21109.1—2022，3.2.11]

3.2

安全失效 safe failure

可能触发某个给定的安全动作的失效。

注1：一个失效是“安全的”只是对于某个给定的安全功能来说。

注2：当实施了故障裕度时，安全失效会导致：

- 在安全功能可用的情况下继续运行，但是有更高的要求时成功率或者更低的危险事件发生可能性；
- 触发安全功能误动作。

注3：当未实施故障裕度时，不论过程条件如何，安全失效将触发安全功能。这也称为误动作。

注4：误动作就给定的安全功能来说是安全的，但是对其他安全功能来说可能是危险的。

注5：误动作可能会对过程的生产可用性造成不利影响。

[来源：GB/T 21109.1—2022，3.2.62]

3.3

共因失效　common cause failure

由单一事件引起的不同设备的并发失效，并且这些失效间不互为因果。

注 1：由一个共因引起的所有失效未必恰好在同一时间发生，因此在 SIF 实际失效前有一定时间来检测共因的发生。

注 2：共因失效也可能导致共模失效。

注 3：共因失效的可能性降低了系统冗余或故障裕度的效果（如增加了多通道系统中两个或更多通道的失效概率）。

注 4：共因失效是相关失效，可能由外部事件（如温度、湿度、过电压、火灾、腐蚀）、系统性故障（如设计的、组装的或安装的错误、缺陷）、人为错误（如误用）等引起。

注 5：单个共因失效是属于一组并发失效中的一个失效。

[来源：GB/T 21109.1—2022，3.2.6.1]

3.4

最终元件　final element

BPCS 或 SIS 的一部分，为达到或保持安全状态执行必要的物理动作。

注：例如阀门、开关设备以及电机，包括他们辅助的元件（如电磁阀和用来驱动阀门的执行机构）。

3.5

安全仪表系统　safety instrumented system；SIS

用来实现一个或多个 SIF 的仪表系统。

注 1：SIS 由任意组合的传感器、逻辑解算器及最终元件组成。它也包括通信和辅助设备（如电缆、管道、电源、取压管、伴热）。

注 2：SIS 可以包括软件。

注 3：SIS 可以包括人为动作作为 SIF 的一部分。

[来源：GB/T 21109.1—2022，3.2.67]

3.6

安全完整性　safety integrity

在要求时执行所需 SIF 的 SIS 能力。

[来源：GB/T 21109.1—2022，3.2.68]

3.7

安全完整性等级　safety integrity level；SIL

为规定 SIS 应达到的安全完整性要求而分配给 SIF 的离散等级（4 个等级中的一个）。

注 1：SIL 等级越高，期望的 PFD_{avg} 越低，或者导致危险事件的危险失效平均频率越低。

注 2：SIL4 是安全完整性的最高等级，SIL1 是最低等级。

[来源：GB/T 21109.1—2022，3.2.69]

3.8

安全仪表功能　safety instrumented function；SIF

由安全仪表系统（SIS）实现的安全功能。

注：SIF 设计用来达到一个要求的 SIL，SIL 由其他参与降低相同风险的保护层决定。

[来源：GB/T 21109.1—2022，3.2.66]

3.9

故障安全　fail to safe

安全仪表系统发生故障时，使被控过程转入预定安全状态。

3.10

安全要求规格书　safety requirements specification；SRS

包含安全仪表系统应执行的仪表安全功能的所有要求的规格书。

注：该术语与 GB/T 21109.1—2022 不同，以体现行业应用习惯。

3.11

旁路　bypass

阻止全部或部分 SIS 功能执行的行为或设施。

[来源：GB/T 21109.1—2022，3.2.4]

4　缩略语

下列缩略语适用于本文件。

BPCS：基本过程控制系统(Basic Process Control System)

ESD：紧急停车(Emergency Shutdown)

MOC：变更管理(Management of Change)

MPRT：最大允许维修时间(Maximum Permitted Repair Time)

PFD：要求时危险失效概率(Probability of Dangerous Failure on Demand)

PFD_{avg}：要求时危险失效平均概率(Average Probability of Dangerous Failure On Demand)

PFH：每小时的失效概率(危险失效平均频率)[Probability (Average Frequency of Dangerous Failures) of Failure Per Hour]

SIF：安全仪表功能(Safety Instrumented Function)

SIL：安全完整性等级(Safety Integrity Level)

SIS：安全仪表系统(Safety Instrumented System)

SRS：安全要求规格书(Safety Requirement Specification)

5　运行维护依据

运行和维护所依据的文件应包括但不限于以下内容：

——管道工艺操作原理；

——SRS；

——仪表控制流程图(带安全功能回路)；

——逻辑图/因果图(C&E)；

——系统配置和结构图；

——机柜集成图；

——I/O 点表；

——组态文件；

——SIS 操作和维护计划；

——SIS 操作规程；

——SIS 维护手册；

——设备操作手册或说明书；

——SIS 相关管理规定。

6　人员要求

6.1　人员职责

6.1.1　管理人员职责

SIS 管理人员的职责宜包括：

——SIS 旁路操作的审批；
——负责 SIS 的运行考核工作；
——负责监督抽查 SIS 的维护工作；
——负责 SIS 相关的变更审批；
——负责制修订 SIS 的事故事件应急预案，并监督开展演练；
——负责制修订 SIS 管理制度和操作运行手册等；
——负责组织所辖范围内在役管道的 SIS 功能性测试和验收；
——负责定期组织对 SIS 的安全完整性进行评价，并跟踪整改；
——负责组织并参与因 SIS 故障造成安全生产事件的事故调查；
——负责组织和监督检查 SIS 的改造工作；
——负责制定 SIS 的安全计划（包括：SIS 安全确认计划、验证计划、操作计划、维护计划等）；
——负责制修订 SIS 的操作规程和维护规程；
——负责 SIS 安全管理；
——负责更新 SRS。

6.1.2 运行人员职责

SIS 运行人员的职责宜包括：
——ESD 触发条件的确定；
——ESD 的触发操作及必要时 SIF 的手动操作；
——针对 SIS 故障及报警的应急响应；
——监视 SIS 运行状态，记录、报送故障报警信息，并对报警信息进行处理；
——对 SIS 进行旁路或屏蔽等操作；
——按照 SIS 的事故事件应急预案，定期开展演练；
——在确认管道发生重大事故时，主动触发 SIS 功能；
——监督 SIS 系统功能完好；
——参与 SIS 的改造工作；
——识别 SIF 触发条件；
——核对 SIF 执行结果的准确性；
——SIF 动作后的系统恢复；
——SIS 维修维护测试时的应急响应；
——负责 SIS 现场运行等工作（包括日常巡检、手动操作等）；
——负责提出 SIS 的优化建议，并在变更审批后实施。

6.1.3 维护人员职责

SIS 维护人员的职责宜包括：
——编制维护方案；
——SIS 触发后的检查及协助运行人员恢复；
——SIS 故障诊断、处理、恢复；
——SIS 日常性维护、测试；
——SIS 周期性维护、测试；
——完成现场维修作业。

6.2 人员能力

6.2.1 管理人员能力要求

管理人员应进行培训并定期考核，以维持 SIS 系统功能的完整性，确保掌握以下内容：

——功能安全相关法律法规及标准规范；

——所辖范围内在役管道的 SIS 的 SRS；

——SIS 的功能安全管理要求。

6.2.2 运行人员能力要求

运行人员应接受 SIS 功能和操作方面的培训，确保掌握以下内容：

——管道工艺操作原理；

——SRS 的相关要求：

- SIF 动作设定值、条件及动作执行；
- SIF 能预防的危险；
- 旁路操作及使用条件；
- 补偿措施的使用；
- 任何手动停机开关的操作和手动启动活动以及何时应启动这些手动开关（如现场 ESD 按钮、复位按钮等）；
- 系统复位或重启的操作条件和操作内容；
- SIS 诊断或系统报警应采取的措施；
- 对诊断功能的合理验证。

6.2.3 维护人员能力要求

维护人员应进行培训并定期考核，以维持 SIS 系统功能的完整性，确保掌握以下内容：

——安全功能回路安全完整性等级确定原则；

——SIS 触发方式、触发后系统和现场设备的响应；

——SIS 触发后的检查、复位与恢复的方法；

——SIS 硬件特性及软件使用方法；

——SIS 接线原理及接线图；

——SIS 报警含义及需要采取的措施；

——SIS 诊断、维护、检验测试的方法及步骤；

——SIS 旁路的设置及恢复；

——SIS 补偿措施的设置及恢复；

——SRS 的相关要求。

7 运行要求

7.1 一般要求

油气管道 SIS 运行的对象应包括：站场 SIS 的各 SIF、站场 ESD、站场区域 ESD、单体设备 ESD。各系统的运行内容应包括：传感器、逻辑解算器及最终执行元件，以及通信和辅助设备（如电缆、管道、电源、取压管、伴热）。

7.2 环境要求

油气管道 SIS 机柜间运行环境要求：

——温度要求：机柜间温度宜控制在冬季(20±2)℃，夏季(26±2)℃；

——湿度要求：机柜间相对湿度宜不大于 70%，且不应结露；

——电磁干扰控制：机柜间电磁干扰应控制在小于 400 A/m 的持续电磁干扰；

——振动控制：机柜间地面振动控制在振幅小于 0.1 mm，频率小于 25 Hz 的连续振动；

——粉尘控制：空气净化度应控制在尘埃少于 0.2 mg/m^3(粒径小于 10 μm)。

7.3 SIS 操作规程

7.3.1 与 SIS 有关的运行，应按照 SIS 操作规程执行。

注：SIS 操作规程一般在 SIS 运行前的设计阶段由设计和运行人员编制，可作为独立文件或整体运行方案的一部分。

7.3.2 SIS 操作规程应包括但不限于以下内容：

——例行的和异常的操作活动；

——SIS 旁路的应用和控制；

注 1：旁路相关操作需满足以下要求：当由于旁路(维修或测试)导致 SIS 被禁用或降级时，需在相应的操作限制下(持续时间、过程参数等)采取补偿措施以维持安全。需向操作员提供旁路前和旁路中适用的规程，旁路移除前的操作流程，以及处于旁路状态的最大允许持续时间等信息。这些信息需定期复审。

——操作所使用的规程、方法和技术；

——当检测到危险失效、旁路、SIF 或部分 SIF 失效时所采取的降低 SIS 风险的补偿措施；

注 2：当某个 SIS 设备被旁路时，只有在危险分析确定已实施补偿措施且其提供了足够的风险降低的情况下，才允许过程继续运行。需制定相应的操作规程。

——执行运行方案活动的日程表；

——负责运行方案活动的人员、部门和组织；

——开展 SIS 操作相关活动的作业人员资质和培训要求；

——明确 SIS 功能的完好率要求和误停车率要求；

——SIF 的触发条件(也包括 ESD 按钮的触发条件)；

——对设计阶段做的假设与 SIS 运行过程中的实际情况进行对比，必要时对 SIS 做修改以确保持续满足 SIL 要求，需要关注的内容包括：SIF 动作频率、SIF 联锁动作、构成 SIS 设备失效及失效模式(在所有可能的运行模式下)、SIF 触发原因、误停车原因及频率、补偿措施涉及的设备失效。

7.4 网络安全

7.4.1 账户管理

为确保 SIS 运行过程中的网络安全，账户管理应遵从但不限于以下方面：

——为管理人员、运行人员、维护人员设置所需的最小权限，实现各用户的权限分离；

——SIS 根据权限不同设置相应的账户及口令。严格执行用户操作权限管理，用户与账户一一对应，用户名和口令备份和定期更新，保密存放，严禁使用默认口令或弱口令；

——SIS 设置专职管理人员；

——对于不再需要访问 SIS 的人员，确保迅速修改、删除或停用其账户；

——定期对账户进行审查和确认，禁止或删除多余用户；

——对于 SIS 中的新应用软件、硬件等，安装后更改所有默认密码；

——对 SIS 的操作和访问等行为进行安全审计，审计覆盖到每个用户，SIS 相关操作日志留存不少于半年。

7.4.2 连接管理

为确保 SIS 运行过程中的网络安全，连接管理应遵从但不限于以下方面：

——禁止 SIS 网络与办公网络、公共网络等非生产控制的网络进行互联；

——定期清理 SIS 网络中无关、无效连接；

——禁止设置 SIS 网络与无线网络连接；

——对 SIS 主机接口进行管理，对于不必要的或无关的接口（如 USB、光驱、无线等）进行封堵或拆除；

——采用专用的移动介质与计算机进行 SIS 维护，避免在 SIS 网络与公共网络之间交叉使用，特殊情况下需要交叉连接时，做好移动介质与计算机的查毒、防毒工作，避免 SIS 感染计算机病毒；

——对 SIS 主机的应用软件安装、运行进行管理；

——SIS 厂家或第三方外来技术服务接入 SIS 系统，需经过有关部门审批；

——在 SIS 网络中部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。

7.4.3 数据管理

为确保 SIS 运行过程中的网络安全，数据管理应遵从但不限于以下几个方面。

——依据《工业数据分类分级指南》，识别 SIS 的研发数据、生产数据、运维数据、管理数据、外部数据等，进行分类分级防护。

——对 SIS 专用软件、工程文件、工程数据等文件至少每半年进行一次详细备份，工程程序更新配置立即备份。数据备份使用专用移动硬盘加密存储，建立专用移动硬盘的使用控制措施。对于不再使用的专用移动硬盘，使用正式的规程可靠并安全地处置。

注：对于存储有数据的移动硬盘，若不再使用可通过如下方式处理：利用焚化或切碎的方法，或者将数据删除供组织机构内其他应用使用。

——备份数据异地存储，存储周期为两年。

7.4.4 应急管理

为确保 SIS 运行过程中的网络安全，应急管理应遵从但不限于以下方面：

——制定 SIS 网络安全事件应急响应预案，当遭受安全威胁导致 SIS 系统出现异常时，立即采取紧急防护措施，防止事态扩大，并逐级报送相关管理部门，同时注意保护现场，以便进行调查取证；

——定期对 SIS 网络安全事件应急响应预案进行演练，必要时对应急响应预案进行更新。

7.5 操作安全

为确保 SIS 相关操作安全，应遵从但不限于以下方面：

——从事 SIS 运行工作严格执行 SIS 操作规程及现场安全管理规定，确保人身财产安全；

——各站 SIS 功能有专门的说明，包括 SIF 的触发条件、触发后现场设备的动作顺序、站场人员应当采取的措施或行动等；

——现场制定严格的管理规定，确保外来人员不会异常触发 SIF（包括 ESD）；

——现场运行期间需要对 SIS 设置旁路时，严格按照 SIS 操作规程执行，并在监视界面及现场设置明确指示；

——SIS 设置旁路纳入 MOC 管理（联锁变更管理）；

——在现场出现紧急情况且满足 ESD 触发条件时，立即就近触发 ESD 按钮，并按照相关预案处置；

——ESD 按钮旁，设置明显的提醒标识以防误触发。

8 维护要求

8.1 一般要求

8.1.1 应制定 SIS 的维护计划，在开展 SIS 的维护工作前应编制维护方案，并进行审批。

8.1.2 应根据维护计划编制维护规程，维护规程应符合安全要求规格书及设备供应商提供的维护要求。

8.1.3 应根据维护规程对 SIS 进行维护。

8.1.4 按照 GB/T 32202—2015 的要求每 3 年～5 年开展功能安全评估工作，且应确保 SIS 的 SIL 持续满足 SRS 要求。

8.2 维护计划

8.2.1 SIS 的维护工作包括不定期维护和周期性维护。

8.2.2 应由管理人员和维护人员共同编制 SIS 维护计划，维护计划应包括以下内容：

——维护作业范围；

——检验测试活动、预防性维护和故障维修活动；

——维护所使用的规程、方法和技术；

——执行维护活动的计划表；

——负责维护活动的人员、部门和组织；

——开展维护活动的时间；

——遵从操作和维护规程的验证；

——开展维护相关活动的作业人员资质和培训要求；

——SIS 失效或维护导致的 SIS 所有潜在降级模式，以及与降级模式相关的补偿措施、维护动作。

8.3 维护规程

8.3.1 维护规程应有效地确保 SIS 运行与 SRS 相一致，维护规程应涵盖以下内容：

——为维持所要求的 SIS 功能安全所开展的相关工作（例如遵从由 SIL 确定所定义的检验测试间隔）；

——在操作和维护期间为预防不安全状态或降低危险事件后果，所需要的动作和约束条件，如：测试旁路和维修旁路；

——维护人员在旁路前、旁路中、旁路移除前执行的操作，以及处于旁路状态的最大允许持续时间等信息，以及检验测试后是否移除旁路的验证流程；

——SIS 功能包括输出装置的计时要求；

——SIS 报警和停车时的操作响应；

——SIS 系统失效和要求率相关信息维护；

——SIS 审核和测试的结果的相关信息的维护；

——当 SIS 中出现故障或失效时遵从的维护规程，包括：故障检测和维修规程、重新确认规程、维护报告要求、跟踪维护执行情况的规程；

——确保在正常维护活动期间使用的测试设备已被正确校准和维护；

——常规维护过程中所使用的维护设备得到正确维护和校准；

——SIS 检验测试计划；

——不定期维护和周期性维护要求，确保 SIS 有效运行；

——当 SIS 发生故障时，如需要更换 SIS 的元件，更换后按照第 9 章的要求，执行 SIS 变更管理规定；

——与要求率和 SIS 可靠性参数有关的数据收集的规程；

注：收集和分析失效数据有很多好处，包括如果运行中的失效率明显低于设计时的预测，则有可能降低维护成本。新安装的实施成本也可能降低，因为新设计可基于不那么保守的失效率。

——建立 SIS 中每个 SIF 的档案，明确回路中每一个部件规格、型号、技术要求、SIL、检验测试时间等，以及旁路措施、要求等。

8.3.2 维护规程应定期进行复审，如复审过程中存在需要修订的内容，应在修订后进行功能安全的审核，并开展 SIS 系统的测试工作。

8.4 维护内容

8.4.1 维护过程中，如果 SIS 功能被旁路，应取得管理人员同意，以确保维护过程的安全性。检查内容，应当涉及到 SIS 的传感器、逻辑解算器、最终元件等，按照相关要求对各项内容进行仔细检查，对发现的问题及时处理。

8.4.2 不定期维护内容包括日常巡检或智能诊断发现的问题。

8.4.3 周期性维护工作内容参见表 A.1。

8.5 检验测试

8.5.1 开展 SIS 系统的检验测试工作前，应编写每个 SIF 的书面检验测试方案，测试方案应描述需要执行的每个步骤并应包括：

——每个传感器和执行元件的正确操作；

——正确的逻辑动作；

——正确的报警和指示。

8.5.2 SIS 系统的检验测试方法，参见附录 B。

8.5.3 SIS 应定期开展检验测试工作，检验测试频率的选取应确保 PFD_{avg} 计算结果持续满足 SIL 要求。

注 1：在确定的检验测试间隔周期内，需对 SIS 所有 SIF 完成检验测试。

注 2：SIF 不同部分的检验测试间隔可以不同，如逻辑解算器的检验测试间隔可能与传感器或执行元件不同。

8.5.4 应根据历史测试数据、工厂经验和硬件退化情况等各种因素，定期（周期由用户决定）重新评估检验测试频率。

注：用户可以根据这些数据和对检验测试频率原始基础的分析来调整检验测试频率。

8.5.5 SIS 的检验测试最大程度精准的反映实际操作条件，确认整个 SIS 回路的性能。

注 1：需识别可能导致共因失效的失效原因。

注 2：功能测试规程还可强调对于避免引入共因失效的需求。

注 3：使用适当的管理规程审查检验测试的延期，防止重大延迟。

8.5.6 应对 SIS 的各 SIF 逐一进行检验测试，包括传感器、逻辑解算器和最终元件（如关断阀和电机），可以以端到端的形式（即全回路的集成测试）或以分段的形式（即传感器、逻辑解算器和最终元件的设备级测试）进行，每个最终元件应至少在一个 SIF 里以端到端形式测试一次，此最终元件所在的其他 SIF 可以分段的形式进行测试。

8.5.7 宜对冗余架构的所有通道进行检验测试，以证实所有的通道都在正确地运行。

8.5.8 如在测试过程中发现传感器、逻辑解算器和最终元件存在任何缺陷，应及时进行修复以确保 SIS 系统的功能安全，在修复完成后应再进行一次检验测试。

8.5.9 如应用程序发生任何变更，应对受影响的 SIF 进行全面的确认和检验测试。

注：如果对变更进行了适当的审查和部分测试，以确保变更是根据更新后的安全要求设计并正确实施的，则允许例外。

8.5.10 检验测试应包括对以下内容的验证：

——操作逻辑顺序，例如因果图中给出的操作逻辑顺序；
——所有输入设备（包括现场传感器和 SIS 输入模块）的操作；
——与每个输入设备相关的逻辑；
——与组合式输入有关的逻辑；
——所有 SIF 的触发条件及触发值；
——报警功能；
——SIS 的响应速度（必要时）；
——SIS 输出模块和所有最终元件的操作；
——传感器和执行器的失电、失气、失信号等失效状态确认测试；
——由 SIS 执行的计算功能；
——执行动作的时序和速度；
——手动操作的功能使过程进入安全状态；
——诊断程序的启动运行；
——SIF 在检验测试后仍可正常运行，例如任何抑制或超驰的复位。

8.5.11 检验测试应输出报告，报告中记录的信息应能够证实检验测试已按要求完成，应至少包括以下内容：

——执行的测试和检查的说明；
——测试和检查的日期；
——执行测试和检查的人员姓名；
——被测系统的序列号或者其他唯一标识符（如回路号、工位号、设备号和 SIF 号）；
——测试和检查的结果，由运行人员和维护人员共同确认（如“发现 as-found”和听任 as-left”状况）。

8.6 维护安全

为确保 SIS 相关维护安全，维护人员应遵照国家安全相关的法律法规、作业安全相关管理规定及维护方案开展维护活动，同时对 SIS 还应遵从以下规定：

——在开展维护作业前，SIS 系统的维护方案通过管理部门的审批；
——维护人员熟悉维护规程、应急预案；
——维护人员资质能力满足第 6 章的要求；
——禁止擅自将 SIS 功能进行屏蔽或旁路，如维护作业需设置旁路，进行风险分析，并根据风险分析结果设置相应的补偿措施且确保其可用，保证屏蔽或旁路时维护作业风险可控；
——旁路实施前和移除后都进行核实；在旁路实施中，设置醒目提示；
——现场设置在线维护作业关键风险点告知牌，明示在线作业风险点；
——在维护过程中如现场出现紧急情况且满足 ESD 触发条件时，立即触发 ESD 按钮，并迅速撤离现场；
——确保在开展维护活动作业前，所使用的测试设备已经过正确的校准和维护；
——维护人员严格按照维护规程开展维护工作，每一项维护作业均设置监督人员，确保过程操作准确，确保 SIS（硬件和软件）的功能和性能可维持其目标安全完整性。

9 故障处理要求

9.1 故障处理应由维护人员完成，处理过程应遵循第8章维护要求。

9.2 故障处理内容应包括但不限于以下几方面内容。

——在SIS出现危险失效时，在SRS中定义的MPRT时间内完成故障处理和恢复，若故障设备设置有冗余，可不采取风险降低补偿措施；若故障设备无冗余则采取补偿措施维持安全运行，如果不能维持安全运行，则采取规定的动作达到或保持过程的安全状态。如果补偿措施依赖于运行人员执行规定动作来响应某个报警，该报警作为SIS的组成部分来进行运行和维护。

——故障处理前向管理人员汇报，获得管理人员授权后，开始故障处理工作。故障处理前做技术交底和风险分析，紧急故障可先处理再补充记录。

注1：对于突发的自动化仪表故障不能及时处理且影响到正常运行监控，需将故障设备隔离，尽量采用就地方式运行，并在恢复正常前按照制定的管控措施管理。

注2：自动化仪表系统异常事件发生后，要及时开展应急抢修，如果对工艺运行造成影响，按照《调度管理程序》要求进行汇报。

——故障排除时按照相关安全要求、程序、作业指导书和维护依据，分析故障原因，逐级处理、排除。

——对于短时间内无法恢复的站场/阀室与调控中心SCADA数据中断的故障，需及时补报维修作业计划，同时给调控中心自动化运维电话报备。

——故障处理结束后，恢复现场设备及工艺流程，对故障产生的原因进行深入分析，并编制分析报告。

——现场异常状态信息的搜集，非紧急情况下，充分利用多媒体手段，如照片、录像等，第一时间记录故障设备报警灯、故障代码等信息并纳入事故/事件分析报告。

——对SIS系统及其传感、执行部件故障进行详细记录，建立企业级SIS故障失效数据库，记录内容包括：故障现象、故障影响、故障分析等。

10 管理要求

10.1 变更管理

10.1.1 对SIS系统进行修改前，应确保无论进行任何变更都能够保持所要求的安全完整性。

10.1.2 SIS系统的管理人员应编制书面的变更管理规程，用于明确SIS变更的各个过程，包括启动、记录、检查、审核和批准。

10.1.3 下列情况应按照变更管理程序执行：

——系统扩建；

——更改操作步骤；

——由于新的或修订后的安全立法要求所需的更改；

——更改工艺流程；

——更改硬件、软件；

——修改更正系统故障；

——由于故障率高于期望值导致的更改；

——由于SIS功能增加或减少的更改(包括对SIS联锁设置旁路)。

10.1.4 变更管理程序应保证在进行变更前考虑下列问题：

——所要变更的技术基础；

——变更对生产风险的影响；

——操作步骤的修改；
——变更所需的时间；
——管理部门对变更的要求；
——系统的可扩展性；
——对响应时间的影响；
——变更的操作方式(在线/离线)；
——若变更影响安全，则对变更方案进行重新调整，直至计划的变更能够维持 SIS 系统的 SIL 要求。

10.1.5 变更的检查应保证：
——维持所要求的 SIL 等级；
——变更过程中有专人监护；
——由 SIS 的相关管理人员参加检查过程。

10.1.6 变更过程应包括：变更计划及方案、变更影响分析(风险分析)、变更审批、变更设计、变更执行、变更确认，所有变更应遵循设计文件。

10.1.7 未经授权批准不得擅自开展 SIS 系统的修改活动。

10.1.8 应由经过适当培训的合格人员执行变更，应事先告知所影响的相应人员并就变更对其进行适当培训。

10.1.9 变更完成后，应进行相应的功能性测试，确保功能安全。

10.1.10 对 SIS 的所有变更应保留相应的信息，包括：
——变更的描述；
——变更的理由；
——可能会受影响的已确定的危险；
——变更活动对 SIS 的影响分析；
——变更要求的所有批准文件；
——验证所有更改已正确实现，以及 SIS 按要求执行所使用的测试；
——相应的配置历史；
——验证所有更改不会对未修改的 SIS 组成部分产生不利影响所使用的测试。

10.2 备品备件管理

SIS 备品备件应遵循但不限于以下原则进行管理。
——根据各 SIF 要求的 MPRT 及备品备件供应周期，制定 SIS 备品备件储备标准，并实行定额储备管理。
——备品备件的规格、数量及技术指标满足 SRS 要求。
——备品备件放置在专用库房，实行专人管理。专用库房内的温度、湿度符合要求，无腐蚀性气体，物品归类定点存放。
——建立备品备件出入库台账，及时补充相应备品备件。

10.3 文档管理

10.3.1 文档管理的内容应包括但不限于：
——SRS；
——SIF 档案；
——维护检修记录；
——各种图纸(包括 SIS 逻辑因果图、接线图、设备布置图等)；

——SIS 设备的 SIL 认证相关资料(包括:认证证书、安全手册、认证报告等);
——SIS 设备说明书;
——SIS 管理制度;
——故障分析报告;
——SIS 操作规程;
——SIS 维护规程。

10.3.2 文档的存储应采用纸质或电子形式,并妥善保管,电子文档要留有备份。

10.3.3 文档资料应齐全完整、内容准确,并依据实际情况及时更新。

10.3.4 文档的保存期限应综合考虑维护周期、功能安全评估及其他管理要求进行确定。

附 录 A
（资料性）
周期性维护内容及周期

SIS 系统周期性维护内容及周期见表 A.1。

表 A.1 SIS 系统周期性维护内容及周期

序号	类别	维护内容	维护周期
1	机柜及附属设施	检查机柜风扇温控开关设定是否合理、工作是否正常	1 个月
		检查机柜照明	1 个月
		检查机柜温控开关功能的正确性	1 个月
		检查机柜门的开关性能	1 个月
		检查 24 V 电源是否正常	1 个月
		检查标签是否齐全	1 个月
		检测机柜工作接地和保护接地电阻值	6 个月
		检查机柜内线号、电缆挂牌、器件标志牌、螺丝、线槽盖、地沟盖板和配线图是否齐全，若有缺失则补齐	6 个月
		轻轻拽动机柜内非弹簧端子的接线，确保紧固	6 个月
		检查机柜内布线是否整齐和无临时接线	6 个月
		检查柜内与户外电缆沟的密封性，确保其完全隔离	6 个月
		检查机柜内带有状态指示灯的保险端子和继电器，状态显示是否正常	6 个月
		检查电源防浪涌抑制器是否正常	12 个月
		检查信号防雷击端子是否正常	12 个月
		检查保险端子内部保险端子是否正常	12 个月
2	系统	查看 SIS 控制器带系统时间的模块(CPU、I/O、通信和冗余模块)是否与基准时间一致	1 个月
		检查和测试 SIS 控制器包括：检查控制网络各连接节点的牢固性；测试冗余配置 CPU 的冗余功能；检查 SIS 控制器的配置信息；检查 SIS 控制器程序的扫描周期，最长扫描周期不大于 100 ms；查看 CPU 运行信息是否有严重错误；检查 SIS 控制器内存的利用率	6 个月
		程序备份	6 个月
		调控中心计算机与 SIS 系统、ESD 系统的数据通信的状态测试	6 个月
		冗余功能测试	12 个月
		实际动作测试	12 个月
		按钮及信号回路接地测试； 数字量输入/出回路测试； 模拟量输入/出回路测试	12 个月

表 A.1 SIS 系统周期性维护内容及周期（续）

序号	类别	维护内容	维护周期
2	系统	系统不间断电源充放电测试	12 个月
		单体设备控制测试	12 个月
		SIS 保护程序测试、ESD 保护程序测试。 注：保护逻辑程序测试时，需在站场停输后进行，当涉及全线的保护逻辑程序时，在全线停输后进行测试	12 个月

附 录 B
（资料性）
功能测试方法

B.1 实际动作测试

实际动作测试按以下步骤进行：

a） 向相关部门通报即将进行的测试及所需时间；
b） 对工艺及设备情况进行现场确认；
c） 关闭自动放空/泄压阀门前（或后）的手动放空/泄压阀，防止测试期间造成油气损失；
d） 将压缩机组、输油泵等大型设备进行卸载；
e） 选择任一 ESD 按钮触发紧急关断程序，观察现场设备是否按照程序设定要求进行动作，报警功能是否完整，ESD 逻辑功能执行是否准确无误；
f） 不进行现场设备及工艺恢复，逐次测试其他 ESD 按钮及远控触发 ESD 等触发条件是否能触发紧急关断程序；
g） 测试完毕并确认无误后，恢复现场设备及工艺；
h） 向相关部门通报测试完毕。

B.2 模拟测试

在特殊情况下，在执行机构不能动作的情况下，可以通过模拟测试诊断 ESD 系统的功能完整性，按以下步骤进行：

注：模拟测试的触发条件需从信号源头或者距离源头最近的可操作的接线端子处给定信号，不能直接从程序中强制给定信号。

a） 向相关部门通报即将进行的测试及所需时间；
b） 休眠（旁路）ESD 系统；
c） 断开 ESD 系统 DO 输出（针对常开点）；
d） 通过触发条件，逐点触发 ESD，观察 HMI 是否有相应报警，软件及硬件设备是否指示相应执行机构的命令已输出；
e） 测试完毕后，接回 DO 输出端子；
f） 取消休眠或旁路；
g） 向相关部门通报测试完毕。

B.3 系统冗余功能测试

系统冗余功能测试按以下步骤进行：

a） 根据系统硬件配置，通过主备切换或停用单台设备的方式对其进行电源冗余测试，网络冗余测试及控制器冗余测试；
b） 测试前向调控中心汇报，说明有可能出现的通信中断或其他报警；
c） 现场安排站场人员，对执行机构进行监视，一旦执行机构出现误动作，立即采取相应措施，排查故障原因后再恢复状态；
d） 测试前先将 ESD 系统休眠、DO 输出端子断开，ESD 放空阀（泄放阀）前后的手动阀关闭，避免误触发造成站场生产中断。

参 考 文 献

[1] GB/T 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

[2] GB/T 21109.1—2022 过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和应用编程要求

[3] GB/T 32203—2015 油气管道安全仪表系统的功能安全 验收规范

[4] SY/T 6966 输油气管道工程安全仪表系统设计规范

[5] SY/T 7628—2021 油气田及管道工程计算机控制系统设计规范

[6] IEC 61508(所有部分) Functional safety of electrical/electronic/programmable electronic safety-related systems

[7] IEC 61511(所有部分) Functional safety-Safety instrumented systems for the process industry sector