中华人民共和国
石油天然气行业标准
输油气管道工程
安全仪表系统设计规范
SY/T 6966—2023
*
石油工业出版社出版
（北京安定门外安华里二区一号楼）
北京中石油彩色印刷有限责任公司排版印刷
新华书店北京发行所发行
*
850×1168 毫米 32 开本 2.125 印张 63 千字 印 1—500
2023 年 7 月北京第 1 版 2023 年 7 月北京第 1 次印刷
书号：155021·8517 定价：44.00 元

75–010
P 71

SY

中华人民共和国石油天然气行业标准

SY/T 6966—2023
代替 SY/T 6966—2013

输油气管道工程
安全仪表系统设计规范

esign specification for safety instrumented system in oil/gas transportation pipeline engineering

05–26 发布 2023–11–26 实施

国家能源局 发布

中华人民共和国石油天然气行业标准

输油气管道工程
安全仪表系统设计规范

Design specification for safety instrumented system in oil/gas transportation pipeline engineering

SY/T 6966—2023

主编部门：中国石油天然气集团有限公司
批准部门：国家能源局
施行日期：2023 年 11 月 26 日

石 油 工 业 出 版 社

2023 北 京

序号	标准编号	标准名称	代替标准	采标号	出版机构	批准日期	实施日期
308	SY/T 7693—2023	石油天然气钻采设备 防喷器胶芯			石油工业出版社	2023-05-26	2023-11-26
309	SY/T 7694—2023	石油天然气钻采设备井口装置和采油树的修理和再制造			石油工业出版社	2023-05-26	2023-11-26
310	SY/T 7695—2023	石油工业标准化文件的俄文译本通用表述			石油工业出版社	2023-05-26	2023-11-26

前　言

根据国家能源局综合司《关于下达2020年能源领域行业标准制（修）订计划及外文版翻译计划的通知》（国能综通科技〔2020〕106号）的要求，本规范编制组经广泛调查研究，认真总结实践经验，参考国内外有关标准，并在广泛征求意见的基础上，对原规范进行修订。

本规范共分8章和3个附录，主要内容包括：总则、术语及缩略语、基本规定、系统功能及分级、系统设置、设备选型及安装、软件及组态、工程设计与评估。

本规范修订的主要技术内容是：

1　增加了术语“安全”“混合控制器”及其定义；

2　“系统功能及分级”一章优化触发源及联锁动作内容，并对应修改了附录A、附录B；

3　“检测元件”“执行元件”两节补充完善了输油管道站场及附属库区、输气管道站场检测元件及执行元件的设置；

4　“系统设置”“设备选型及安装”两章补充了混合控制器的相关要求；

5　“辅助操作”一节增加了辅助操作盘的设置要求，增加了声光警报器的设置；

6　“系统设置”一章补充了SOE的相关要求；

7　“HMI组态及报警”一节补充了操作画面、维护画面等相关内容；

8　增加“工程设计与评估”一章；

9　附录C增加了SIL验证的相关要求。

本规范由国家能源局负责管理，由石油工业标准化技术委员会石油工程建设专业标准化委员会负责日常管理，由中国石油天然气管道工程有限公司负责具体技术内容的解释。执行过

程中如有意见或建议，请寄送中国石油天然气管道工程有限公司（地址：河北省廊坊市和平路146号，邮编：065000）。

本规范主编单位：中国石油天然气管道工程有限公司
国家管网集团北方管道有限责任公司
机械工业仪器仪表综合技术经济研究所
国家管网集团科学技术研究总院分公司

本规范主要起草人：聂中文　邓东花　王怀义　胡协兰
李　健　陈志强　张　舒　史学玲
刘　瑶　李秋娟　史　威　王永吉
于永志　李　勇　康鹏飞　张书勇
袁　泉　王　勇　郑　前　高铭泽
韩伟伟

本规范主要审查人：田京山　王小林　林　冉　朱瑞苗
张德发　钟小木　臧振胜　王书惠
梁勇强　李昌岑　王多才　陈超声
徐德腾　董秀娟　闫　峰

目　次

Contents

1 总　则

1.0.1 为保障输油、输气管道的安全生产，指导和规范输油气管道工程中安全仪表系统的设计工作，做到技术先进、经济合理、安全适用、节能环保，制定本规范。

1.0.2 本规范适用于陆上原油管道、成品油管道及附属库区工程和天然气管道工程的设计。

1.0.3 安全仪表系统的设计除执行本规范外，尚应符合国家现行有关规范和标准的规定。

2 术语及缩略语

2.1 术　语

2.1.1 监控与数据采集系统　supervisory control and data acquisition system

以多个远程终端监控单元通过有线或无线网络连接起来，具有远程监测控制功能的分布式计算机控制系统。

2.1.2 调度控制中心　control center

监控油气管道输送，负责管道或管网生产运行、调度和管理的中心。

2.1.3 站控制系统　station control system

对工艺站场的生产过程、工艺设备及辅助设施实行自动控制的系统。

2.1.4 基本过程控制系统　basic process control system

不执行任何 SIL ⩾ 1 以上的安全仪表功能，响应过程测量及其他相关设备、其他仪表、控制系统或操作员的输入信号，按过程控制规律、算法、方式，产生输出信号实现过程控制及其相关设备运行的系统。

2.1.5 安全仪表系统　safety instrumented system

实现一个或多个安全仪表功能的仪表系统。

2.1.6 压缩机组监控系统　compressor control system

压缩机、驱动装置及其他辅助设施的监控系统。

2.1.7 危险与可操作性分析　hazard and operability study

在开展工艺危害分析工作中所运用到的，通过使用“引导词”分析工艺过程中偏离正常工况的各种情形，从而发现危害源和操作问题的一种系统性方法。

2.1.8 安全完整性等级　safety integrity level

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）。

2.1.9 故障　fault

由于某个内部状态，无能力按要求执行。

2.1.10 故障安全　fail safe

安全仪表系统发生故障时，被控制过程将转入预定安全状态。

2.1.11 安全功能　safety function

针对特定的危险事件，为达到或保持过程的安全状态，由一个或多个保护层实现的功能。

2.1.12 安全仪表功能　safety instrumented function

由安全仪表系统（SIS）实现的安全功能。

2.1.13 冗余　redundancy

采用两个或多个部件或系统执行同一个功能的方法。

2.1.14 容错　fault tolerance

在出现故障或错误时，功能单元仍继续执行规定功能的能力。

2.1.15 安全　safety

不存在不可接受的风险。

2.1.16 危险　hazard

导致人身伤害或疾病、财产损失、环境破坏、声誉影响等事件的可能。

2.1.17 风险　risk

伤害发生可能性与该伤害严重性的组合。

2.1.18 风险评估　risk assessment

估计风险大小及确定风险容许程度的全过程。

2.1.19 保护层　protection layer

借助控制、预防或减轻以降低风险的任何独立机制。

2.1.20 旁路 bypassing

阻止全部或部分安全仪表系统功能执行的行为或设施。

2.1.21 功能安全 function safety

与 BPCS 和 SIS 有关的整体安全的组成部分，它取决于 SIS 和其他保护层功能的正确执行。

2.1.22 混合控制器 integrated controller

基本过程控制系统和安全仪表系统混合应用的逻辑控制单元。

2.2 缩 略 语

BDV：紧急放空阀（blow down valve）

BPCS：基本过程控制系统（basic process control system）

ESD：紧急停车（emergency shutdown）

ESDV：紧急关断阀（emergency shutdown valve）

FAS：火灾自动报警系统（fire alarm system）

FC：事故关（fail to close）

FO：事故开（fail to open）

HAZOP：危险与可操作性分析（hazard and operability study）

HMI：人机接口（human machine interface）

PFD：失效概率（probability of failure）

SCADA：监控与数据采集（supervisory control and data acquisition）

SCS：站控制系统（station control system）

SIL：安全完整性等级（safety integrity level）

SIS：安全仪表系统（safety instrumented system）

SOA：安全系统目标分析（safety system objectives analysis）

SOE：顺序事件（sequence of events）

SOV：电磁阀（solenoid operated valve）

SRS：安全技术要求（safety requirement specification）

3 基 本 规 定

3.1 设 计 原 则

3.1.1 安全仪表系统应根据已确定的安全技术要求进行设计。

3.1.2 安全仪表系统的工程设计应兼顾可靠性、可用性、可维护性、可追溯性和经济性。

3.1.3 安全仪表系统的设计应遵循安全完整性原则，并应符合下列规定：

1 系统中的各个组成部分应满足安全仪表系统的安全完整性要求。

2 安全完整性可通过冗余、增加测试频率、故障自诊断等手段予以改善。

3.1.4 安全仪表系统的设计应遵循独立设置原则，并应符合下列规定：

1 当安全完整性等级为 SIL2 及以上时，安全仪表系统与基本过程控制系统应分开设置。

2 安全仪表系统与基本过程控制系统合用时，共用部分及执行安全仪表功能部分应与安全完整性等级相适应。

3.1.5 安全仪表系统的设计应遵循故障安全原则，并应符合下列规定：

1 开关量检测元件的接点宜为常闭且带诊断功能的接点。

2 执行元件的安全完整性等级为 SIL2 及以上时，其电磁阀的回路应为励磁型。

3.1.6 安全仪表系统的设计应遵循优先原则，并应符合下列规定：

1 安全仪表系统的动作应优先于基本过程控制系统。

2 执行元件的动作不应受就地 / 远控的约束和限制。

3.1.7 安全仪表系统的设计应遵循简化原则，并应符合下列规定：

1 安全仪表系统应减少中间环节。

2 逻辑控制单元与检测元件、执行元件间应采用硬线方式连接。

3 安全仪表系统不应采用串级停车逻辑。

3.1.8 除超驰和复位外，基本过程控制系统不应介入安全仪表系统的运行或逻辑。

3.1.9 当多个安全仪表功能在同一个安全仪表系统内实现时，系统内的共用部分应符合各功能中最高 SIL 要求。

3.2 系统间的关系

3.2.1 安全完整性等级为 SIL1 时，安全仪表系统和基本过程控制系统可合用。

3.2.2 当可燃气体和有毒气体报警联动安全仪表系统时，宜由可燃气体和有毒气体检测报警控制器发出报警信号至安全仪表系统。

3.2.3 火灾自动报警控制器应将火灾报警信号通过硬线传输至安全仪表系统，并进行安全相关联锁。

4 系统功能及分级

4.0.1 输油管道安全仪表功能应包括站场 ESD 功能和超压保护功能，应符合本规范附录 A 的规定。

4.0.2 输气管道站场安全仪表系统功能应符合本规范附录 B 的规定。

4.0.3 输油气管道站场 ESD 可分为三级：第一级为站场 ESD，第二级为区域 ESD，第三级为单体设备 ESD。

5 系统设置

5.1 系统组成

5.1.1 安全仪表系统应包括检测元件、逻辑控制单元、执行元件及辅助操作设施。

5.1.2 安全仪表系统的结构应符合图 5.1.2 的要求。

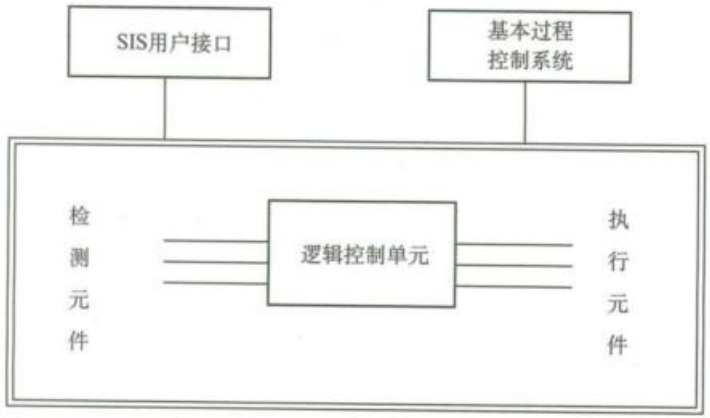


图 5.1.2 安全仪表系统的结构图

注：双划线内的部分为安全仪表系统的组成部分。

5.2 检测元件

5.2.1 独立设置应符合下列规定：

1 SIL1 安全仪表功能回路的检测元件可与基本过程控制回路共用。

2 SIL2、SIL3 安全仪表功能回路的检测元件应与基本过程控制回路分开设置。

5.2.2 冗余设置应符合下列规定：

1 SIL1 安全仪表功能回路可采用单一检测元件。

2 SIL2 安全仪表功能回路宜采用冗余检测元件。

3 SIL3 安全仪表功能回路应采用冗余检测元件。

4 冗余的检测元件宜接入不同的输入模块。

5.2.3 冗余方式应符合下列规定：

1 当系统要求高安全性时，应采用 1oo2 逻辑结构。

2 当系统要求高可用性时，应采用 2oo2 逻辑结构。

3 当系统的安全性和可用性均需保障时，宜采用 2oo3 逻辑结构。

5.2.4 输油管道站场及附属库区检测元件的设置应符合下列规定：

1 站场温度检测元件的设置应符合下列规定：

1）间接加热炉出口应设置温度检测元件；

2）直接加热炉出口应设置温度检测元件。

2 站场压力检测元件的设置应符合下列规定：

1）输油管道首站出站处应设置压力检测元件；

2）输油泵站出站处应设置压力检测元件；

3）减压站出站处应设置压力检测元件；

4）给油泵入口应设置压力检测元件；

5）输油泵进口汇管应设置压力检测元件；

6）输油泵出口汇管应设置压力检测元件。

3 储油罐应设置液位检测元件。

4 设备温度检测元件的设置应符合下列规定：

1）输油泵泵壳宜设置温度检测元件；

2）输油泵驱动端宜设置温度检测元件；

3）输油泵非驱动端宜设置温度检测元件；

4）输油泵电机 U/V/W 三相绕组宜设置温度检测元件；

5）输油泵电机驱动端宜设置温度检测元件；

6）输油泵电机非驱动端宜设置温度检测元件；

7）直接加热炉炉膛应设置温度检测元件。

5 设备振动检测元件的设置宜符合下列规定：

1）输油泵驱动端和非驱动端宜设置振动检测元件；

2）输油泵电机驱动端和非驱动端宜设置振动检测元件。

6 输油泵机械密封宜设置液位/压力检测元件。

5.2.5 输气管道站场检测元件的设置应符合下列规定：

1 站场压力检测元件的设置应符合下列规定：

1）压气站出站应设置压力检测元件；

2）调压后宜设置压力检测元件。

2 设备温度检测元件的设置应符合下列规定：

1）主电机（包含励磁机）轴承应设置温度检测元件；

2）压缩机轴承应设置温度检测元件；

3）燃气轮机轴承应设置温度检测元件；

4）压缩机定子应设置温度检测元件；

5）主电机定子应设置温度检测元件；

6）电加热器出口宜设置温度检测元件。

3 设备压力检测元件的设置应符合下列规定：

1）压缩机出口应设置压力检测元件；

2）压缩机组润滑油总管应设置压力检测元件；

3）压缩机组一级干气密封泄漏气应设置压力检测元件；

4）压缩机组隔离气应设置压力检测元件。

4 电加热器宜设置流量检测元件。

5 设备振动检测元件的设置应符合下列规定：

1）压缩机及主电机轴承应设置振动检测元件；

2）压缩机及燃气轮机轴承应设置振动检测元件。

6 设备位移检测元件的设置应符合下列规定：

1）压缩机及主电机轴承应设置位移检测元件；

2）压缩机及燃气轮机轴承应设置位移检测元件。

7 设备速度检测元件的设置应符合下列规定：

1）压缩机及主电机应设置转速检测元件；

2）压缩机及燃气轮机应设置转速检测元件。

5.3 执 行 元 件

5.3.1 执行元件应具有状态监测功能。

5.3.2 阀门的独立设置应符合下列规定：

1 SIL1 回路的阀门可与基本过程控制系统共用。

2 SIL2 回路的阀门宜与基本过程控制系统分开。当阀门与基本过程控制系统共用时，配套的电磁阀应分别设置。

3 SIL3 回路的阀门应与基本过程控制系统分开。

5.3.3 阀门的冗余设置应符合下列规定：

1 SIL1 回路可采用单台阀门。

2 SIL2 回路宜采用冗余阀门，如采用单台阀门，配套电磁阀应冗余设置。

3 当系统要求高安全性时，冗余电磁阀应采用 1oo2 逻辑结构；当系统要求高可用性时，冗余电磁阀应采用 2oo2 逻辑结构。

4 SIL3 回路应采用冗余阀门。

5 冗余的阀门应接入不同的输出模块。

5.3.4 输油管道站场及附属库区执行元件的设置应符合下列规定：

1 进站应设置紧急关断阀。

2 出站应设置紧急关断阀。

3 输油泵开关柜宜设置 ESD 停泵元件。

4 储油罐罐根部应设置具有 ESD 功能的阀门。

5.3.5 输气管道站场执行元件的设置应符合下列规定：

1 站场执行元件的设置应符合下列规定：

1）进站应设置紧急关断阀；

2）出站应设置紧急关断阀；

3）分输支路应设置紧急关断阀；

4）联络线宜设置紧急关断阀；

5）进出站应设置紧急放空阀。

2 设备本体执行元件的设置应符合下列规定：

1）压缩机进出口应设置紧急关断阀；

2）压缩机进出口汇管应设置紧急放空阀。

5.4 逻辑控制单元

5.4.1 逻辑控制单元应选用与 SIL 要求相适应的可编程序逻辑控制器（PLC）或其他逻辑器件。

5.4.2 独立设置应符合下列规定：

1 SIL1 回路的逻辑控制单元可与基本过程控制单元合用，合用后的混合控制器 SIL 等级应不低于 SIL2。

2 SIL2、SIL3 回路的逻辑控制单元应与基本过程控制单元分开。

3 当采用混合控制器时，基本过程控制系统和安全仪表系统的控制程序、I/O 模块、回路供电应分开，不同系统的输入 / 输出模块与主控制器的通信总线应独立分开。

5.4.3 冗余设置应符合下列规定：

1 SIL1 级安全仪表系统可采用冗余的逻辑控制单元。

2 SIL2 级安全仪表系统宜采用冗余的逻辑控制单元。

3 SIL3 级安全仪表系统应采用冗余的逻辑控制单元。

5.4.4 SOE 功能的分辨率应不大于 100ms。

5.5 接　口

5.5.1 安全仪表系统与其他系统之间的通信不应影响安全仪表系统的功能。其设计应符合下列规定：

1 除基本过程控制系统外，安全仪表系统与其他系统之间不应设置通信接口。安全仪表系统与其他系统之间的连接应采用硬接线方式。当采用混合控制器时，不同系统的输入 / 输出模块与主控制器的通信总线应独立分开。

2 安全仪表系统与基本过程控制系统之间可采用硬接线、工业以太网或串行通信的连接方式。

3 安全仪表系统与基本过程控制系统间通信接口和网络宜冗余。

4 通信接口故障应在操作员工作站显示、报警。

5.5.2 操作员接口的失效不应影响操作员采用适当的备用措施将过程带入安全状态，且安全仪表系统的自动功能不应受到影响。操作员接口的设计应符合下列规定：

1 安全仪表系统宜与基本过程控制系统共用操作员 / 工程师工作站及外设。

2 SOE、报警及报告等功能可使用基本过程控制系统的外部设备完成。

3 安全仪表系统的应用软件不应通过操作员接口进行修改。

5.5.3 维护 / 工程师接口的设计应符合下列规定：

1 维护 / 工程师接口宜单独设置。

2 维护 / 工程师接口失效时，不应影响安全仪表系统的功能。

5.6 辅 助 操 作

5.6.1 辅助操作设施宜包括室内辅助操作盘、场区 ESD 按钮、场区声光警报器。

5.6.2 辅助操作盘的设置应符合下列规定：

1 安全仪表系统应设置辅助操作盘，应包括紧急停车按钮、旁路总开关、声光警报器等。

2 应设置站场级、区域级、单体设备级紧急停车按钮。

3 应设置旁路总开关，在总开关处于“允许”状态时，单个回路维护和操作旁路开关才有效。

4 紧急停车按钮、开关、声光报警器等与安全仪表系统应采用硬接线连接。

5.6.3 维护旁路开关的设置应符合下列规定：

1 除 ESD 按钮和执行元件外，其他检测元件应独立设置维护旁路软开关或硬开关。

2 HMI 设置的维护旁路软开关应加键锁或口令保护。

3 维护旁路开关不应屏蔽报警功能，维护旁路状态应报警并记录。

5.6.4 操作旁路开关的设置应符合下列规定：

1 影响工艺过程启动的输入信号应独立设置软开关或硬开关，应根据工艺要求设置操作旁路延时时间，工艺过程正常或延时结束后，应自动解除操作旁路。

2 HMI 设置的操作旁路软开关应加键锁或口令保护。

3 操作旁路开关不应屏蔽报警功能，操作旁路状态应报警并记录。

5.6.5 复位按钮的设置应符合下列规定：

1 安全仪表系统应设置系统程序的复位和现场设备就地复位。

2 辅助操作盘应设置系统程序复位按钮。

3 复位按钮的动作应报警和记录。

5.6.6 场区紧急停车按钮的设置应符合下列规定：

1 站场大门、备用门及工艺设备区逃生通道旁应设置站场级紧急停车按钮。

2 压缩机厂房门口处、装车区应设置区域级紧急停车按钮。

3 输油泵、压缩机、加热炉、装车橇等设备应设置单体设备级紧急停车按钮。

4 紧急停车按钮的动作应报警和记录。

5.6.7 声光警报器的设置应符合下列规定：

1 控制室门口、工艺场区适当位置、压缩机厂房门口、装车区控制室门口设置声光警报器。

2 声光警报器应根据站场的报警分级设置不同的声光报警方式。

6 设备选型及安装

6.1 一 般 规 定

6.1.1 安全仪表系统的设备选型应满足安全完整性等级的要求。

6.1.2 安全仪表系统的设备选型应满足安全功能的要求。

6.1.3 安全仪表系统的设备选型宜满足设备诊断管理的要求。

6.1.4 环境要求应符合国家现行标准《油气田及管道工程计算机控制系统设计规范》SY/T 7628 的相关规定。

6.2 检 测 元 件

6.2.1 检测元件应为模拟量和开关量仪表，模拟量仪表宜选用 4mA ～ 20mA 叠加 HART 传输信号的智能变送器。

6.3 执 行 元 件

6.3.1 SIL2 及以上阀门应具备部分行程测试功能。

6.3.2 紧急关断阀宜采用气液、电液或气动执行机构。

6.3.3 SIL2 及以上回路的紧急放空阀应采用气液、电液或气动执行机构，SIL1 回路的紧急放空阀可采用电动执行机构。

6.3.4 气液、电液和气动执行机构应为故障安全型。

6.3.5 气液、电液执行机构应带蓄能和现场手动操作功能。

6.3.6 气液、电液和气动执行机构应设置就地复位按钮。

6.3.7 开关执行 ESD 动作后，应进行动作信号反馈并记录。

6.4 辅助操作设施

6.4.1 ESD 按钮应具有锁定和复位功能，应具有防误触设计。

6.4.2 旁路开关宜采用旋转钥匙开关。

6.4.3 紧急停车按钮应采用红色，旁路开关应采用黄色，确认按钮应采用黑色，试验按钮应采用白色。

6.4.4 室外安装的声警报器宜选用多声型警报器，声压等级应高于背景噪声 15dB，3m 处声压级应不小于 100dB，且不应大于 120dB。

6.4.5 室外安装的光警报器宜选用多色型警报器。

6.5 逻辑控制单元

6.5.1 逻辑控制单元的最大工作负荷不应超过 50%，不宜大于 500ms。

6.5.2 逻辑控制单元应具有在线自诊断功能。

6.5.3 输入、输出模块信号通道应具有光电或电磁隔离。

6.5.4 混合控制器应选用允许混合应用的 PLC 产品，其中控制程序、I/O 模块、回路供电应独立应用，合用后的混合控制器 SIL 等级应不低于 SIL2。

6.6 供电、接地及电涌保护

6.6.1 安全仪表系统的供电应采用 UPS，供电电压宜为 220V（AC）或 24V（DC）。

6.6.2 供电线路、开关和 24V（DC）电源模块应冗余。

6.6.3 安全仪表系统的电涌保护器应具有诊断功能。

6.6.4 安全仪表系统来自室外 I/O 通道宜设置电涌保护器。

6.6.5 安全仪表系统的接地应符合国家现行标准《油气田及管道工程计算机控制系统设计规范》SY/T 7628—2021 中第 8.3 节的规定。

6.7 仪表安装及配线

6.7.1 现场仪表的取源口宜独立设置，SIL2 及以上回路的应独立设置。

6.7.2 安全仪表系统的接线箱宜独立设置。

6.7.3 安全仪表功能回路不应共用同一公共线。

6.7.4 安全仪表系统与基本过程控制系统的电缆宜分开设置。

6.7.5 不同电压等级的信号不应共用一根电缆，也不应共用一个接线箱。

6.7.6 信号电缆宜采用耐火阻燃型屏蔽电缆。

6.7.7 电缆应连续敷设，中间不应有接头，直埋敷设的电缆应采用铠装铜芯电缆。

7 软件及组态

7.1 软 件 要 求

7.1.1 安全仪表系统编程工具软件应具有符合的安全完整性等级，并符合现行国家标准《电气 / 电子 / 可编程电子安全相关系统的功能安全 第 3 部分：软件要求》GB/T 20438.3 的相关规定。

7.1.2 编程、组态软件应具有以下功能：

1 编程及组态管理。

2 提供标准功能模块。

3 编程及组态检查。

4 仿真及测试。

5 通信管理。

7.1.3 SIS 应用软件编程宜采用负逻辑。

7.1.4 SIS 应用软件编程不应使用结构化文本语言。

7.1.5 SIS 应用软件程序中不应使用跳转指令。

7.2 HMI 组态及报警

7.2.1 操作画面宜包括以下内容：

1 过程执行顺序图。

2 SIS 流程图。

3 SIS 维护旁路画面。

4 SIS 操作旁路画面。

5 SIS 数据总貌画面。

7.2.2 工程师或操作员应能通过维护画面对整个系统进行诊断和维护，能准确显示系统故障位置和原因，画面宜包括：

1 系统诊断画面。

2 系统维护画面。

3 系统资源画面。

4 设备状态画面。

7.2.3 在同一监测点设置多台变送器时，应设多值比较画面，出现偏差时应报警。

7.2.4 安全仪表系统报警管理宜符合国家现行标准《油气输送管道计算机控制系统报警管理技术规范》SY/T 7631 的有关规定。

7.3 逻辑控制单元软件组态

7.3.1 软件组态的安全性应符合下列规定：

1 组态软件应能防止未授权人员修改应用软件。

2 应用软件组态及修改应进行离线测试后，方可下载投入运行。

3 不应对安全仪表系统远程组态。

4 安全仪表系统的应用软件应做备份。

5 系统未使用的输入输出端口应禁止或封闭。

7.3.2 软件组态的可靠性应符合下列规定：

1 断电重启、通信中断等情况下不应产生误动作。

2 输出模块应预设安全输出位置。

3 无理值应钳位。

7.3.3 软件组态的检验应符合下列规定：

1 应用软件组态应与安全技术要求、因果图及逻辑图的要求一致。

2 系统投用前应对应用软件进行 100% 的功能测试。

7.4 软件组态文件

7.4.1 软件组态所需要的输入文件应包括如下内容：

1 P&ID 图。

2 安全技术要求。

3 因果图（表）或逻辑图。

4 安全仪表系统 I/O 点表（带设定值）。

7.4.2 输出文件应包括以下内容：

1 功能开发规格书。

2 带详细注释的程序清单。

3 应用软件使用说明书。

4 系统用户手册。

5 程序和画面原图。

6 逻辑图。

7 地址分配表。

8 FAT 和 SAT 的详细内容和计划。

9 操作维护手册。

10 安全手册。

8 工程设计与评估

8.1 基础工程设计

8.1.1 安全仪表系统基础工程设计文件应根据工艺操作原理、工艺及仪表控制流程图等进行编制，宜包括下列内容：

1 系统配置图。
2 输入、输出点清单。
3 因果图。
4 安全仪表系统逻辑控制单元技术规格书。
5 安全仪表系统检测元件和执行元件技术规格书、数据单。
6 安全技术要求。

8.1.2 安全技术要求宜包括以下内容：

1 确定每个 SIF 的 SIL 等级和过程安全状态，选择励磁或非励磁。
2 数字量输入及其动作。
3 模拟量输入测量范围、报警设置及动作设定点。
4 过程输出及其作用。
5 输入输出的功能关系，包括逻辑、算法及许可条件。
6 手动关断要求。
7 确定 SIF 响应时间要求。
8 失效模式和安全仪表系统要求的响应。
9 复位功能要求。
10 旁路功能要求。
11 测试间隔时间要求和测试措施。
12 部分行程测试功能要求。
13 故障诊断功能要求。

14 应用程序的安全要求。
15 人机界面要求。
16 与相关系统接口要求。

8.2 详细工程设计

8.2.1 安全仪表系统详细工程设计文件应根据安全仪表系统基础工程设计文件及详细工程设计阶段的要求进行编制，宜包括下列内容：

1 系统配置图。
2 输入、输出点清单。
3 端子接线图。
4 逻辑框图。
5 辅助操作设施安装示意图。

8.3 安全完整性等级评估

8.3.1 初步设计及改造项目的可研阶段宜进行 HAZOP 分析。

8.3.2 初步设计阶段宜进行 SIL 评估。

8.3.3 设备型号确定后可进行 SIL 验证。

8.3.4 站场安装、调试运行后，应进行功能安全确认工作。

8.3.5 安全仪表功能回路的评估过程宜符合本规范附录 C 的要求。

8.3.6 工艺过程或安全仪表功能发生变化时，应重新进行 SIL 评估和验证。

8.3.7 SIL 评估过程中应合理配置保护层安全功能。

附录 A　输油管道站场及附属库区安全仪表系统功能表

表 A　输油管道站场及附属库区安全仪表系统功能表

系统功能	ESD 分级	触发源	联锁动作
ESD	站场 ESD	调控中心紧急停站命令	1. 触发所有运行的加热炉、给油泵、输油泵停车。 2. 关闭进出站紧急关断阀。 3. 切断电源（应急电源除外）。 4. 开启站场声光警报器。 5. 触发全线水击超前保护程序
		ESD 手动按钮动作（辅助操作盘、现场）	
		同一区域 2 个或 2 个以上火焰探测器报警信号	
	区域 ESD（装车区）	装车区的 ESD 手动按钮动作	1. 触发装车泵停车。 2. 关闭装车紧急关断阀。 3. 开启站场声光警报器
		装车区的 2 个或 2 个以上火焰探测器报警信号	
	输油泵单体设备 ESD	站控室辅助操作盘单机组 ESD 按钮、泵控制柜上 ESD 按钮（如有）、泵本体 ESD 按钮	触发单台泵机组紧急停车
		输油泵温度高高报警	
		输油泵振动高高报警	
		输油泵泵壳温度高高报警	
		输油泵机械密封泄漏检测高高报警	
		输油泵电机温度高高报警	
		输油泵电机振动高高报警	
		输油泵电机 U/V/W 三相绕组温度高高报警	

续表 A

系统功能	ESD 分级	触发源	联锁动作
ESD	加热炉单体设备 ESD	加热炉出口油温高高报警	触发单台加热炉紧急停车
		直接加热炉炉膛温度高高报警	
		站控室辅助操作盘单台加热炉 ESD 按钮、加热炉控制柜上 ESD 按钮	
	罐单体设备 ESD	罐液位高高报警	关闭进罐紧急关断阀
超压保护		给油泵入口压力低低报警	触发顺序停泵程序
		输油泵机组入口汇管压力低低报警	
		输油泵机组出口汇管压力高高报警	
		出站压力高高报警	
		减压站出站压力高高报警	关闭减压站进站紧急关断阀

附录 B　输气管道站场安全仪表系统功能表

表 B　输气管道站场安全仪表系统功能表

系统功能	ESD 分级	触发源	联锁动作
ESD	站场 ESD	调控中心紧急停站命令	1. 触发运行压缩机组 ESD 停车。 2. 关闭压缩机组进出口紧急关断阀，打开压缩机紧急放空阀。 3. 关闭外输加热系统。 4. 关闭进出站紧急关断阀，联锁打开越站阀（过程控制系统执行）。 5. 打开站内紧急放空阀。 6. 切断电源（应急电源除外）。 7. 开启站场声光警报器
		ESD 手动按钮（辅助操作盘、现场）	
		压缩机厂房 2 个或 2 个以上的火焰探测器高高报警	
	区域 ESD（泄压）	控制室辅助操作盘 ESD 手动按钮（合建站）	1. 触发区域运行压缩机组 ESD 停车。 2. 关闭区域压缩机组进出口紧急关断阀，打开压缩机紧急放空阀。 3. 关闭区域外输加热系统。 4. 关闭区域进出站紧急关断阀，联锁打开越站阀（过程控制系统执行）。 5. 打开区域紧急放空阀。 6. 开启站场声光警报器
		压缩机厂房 ESD 手动按钮； 控制室辅助操作盘 ESD 手动按钮	1. 触发运行压缩机组 ESD 停车。 2. 关闭压缩机组进出口紧急关断阀，打开压缩机紧急放空阀。 3. 开启站场声光警报器

续表 B

系统功能	ESD 分级	触发源	联锁动作
ESD	区域 ESD（保压）	压缩机厂房 2 个或 2 个以上的可燃气体浓度探测器检测到可燃气体浓度超过最低爆炸下限的 40% LEL	1. 触发运行压缩机组 ESD 停车。 2. 关闭压缩机组进出口紧急关断阀。 3. 开启站场声光警报器
		压气站出站压力高高报警	触发运行机组 ESD 停车（保压）
	压缩机单体设备 ESD（泄压）	压缩机组火灾报警（燃驱机组）	1. 触发单机组 ESD 停车。 2. 关闭单机组进出口紧急关断阀，打开对应的紧急放空阀
		压缩机组一级干气密封泄漏气压力高高报警	
		辅助操作盘单机组 ESD 按钮、UCP 机柜面板上 ESD 按钮、现场压缩机组 ESD 按钮	
	压缩机单体设备 ESD（保压）	压缩机或主电机、燃气轮机轴承振动高高报警	1. 触发单机组 ESD 停车。 2. 关闭单机组进出口紧急关断阀
		压缩机或主电机、燃气轮机轴承位移高高报警	
		压缩机或主电机（包含励磁机）、燃气轮机轴承温度高高报警	
		压缩机或主电机定子温度高高报警	
		压缩机或主电机、燃气轮机转速超速	
		压缩机组润滑油总管压力低低报警	
		压缩机组隔离气压力低低报警	
		压缩机组箱罩内可燃气体浓度超过 40%LEL	
		压缩机出口压力高高报警	
	电加热器单体设备 ESD	电加热器出口温度高高报警	停电加热器
		电加热器流量低低报警	
	分输支路 ESD	分输支路压力高高报警	关闭出站紧急关断阀

附录 C　安全仪表系统 SIL 评估过程

C.0.1　安全仪表系统 SIL 评估过程应包括以下内容：

1　搜集文件，包括工艺及仪表控制流程图、工艺说明书、站场总平面布置图、工艺设备布置图、危险区域划分图、因果图、设备技术资料、企业运行风险标准及其他有关文件。

2　危险分析，确定安全仪表系统的安全仪表功能。

3　风险分析，确定安全仪表系统的安全功能回路的目标 SIL 等级。

4　确定安全仪表系统操作模式。

5　确定安全仪表系统结构约束。

6　确定安全仪表系统可靠性数据。

7　计算 SIF 回路的 SIL 等级。

8　安全仪表系统 SIL 设计验证。

C.0.2　SIL 验证宜在 SIL 定级和基础设计完成后进行。

C.0.3　SIL 验证所需资料宜包括以下内容：

1　检修周期或建议的检验测试周期。

2　SIS 各子系统、部件资料。

3　企业提供的失效数据资料或第三方失效数据。

4　其他相关资料。

C.0.4　验证计算应包括以下内容：

1　要求时失效概率 PFD 应满足既定 SIL 要求。

2　结构约束应满足既定 SIL 要求。

3　检验测试周期（T_i）应满足既定 SIL 要求。

C.0.5　PFD 验证宜采用以下方法：

1　公式计算法。

2　故障树方法（FTA）。

3　方框图（RBD）。

C.0.6　验证应统筹考虑以下因素：

1　设备选择。

2　结构约束。

3　部件或子系统的检验测试周期（T_i）。

4　设备的诊断覆盖率。

5　共因失效。

C.0.7　输油气管道工程应采用低要求操作模式，低要求操作模式下的平均失效概率要求应根据表 C.0.7 确定。

表 C.0.7　安全完整性等级：低要求操作模式的失效概率

安全完整性等级（SIL）	平均失效概率（PFD）	风险降低
4	$10^{-5} \sim < 10^{-4}$	$>$ 10000 ~ 100000
3	$10^{-4} \sim < 10^{-3}$	$>$ 1000 ~ 10000
2	$10^{-3} \sim < 10^{-2}$	$>$ 100 ~ 1000
1	$10^{-2} \sim < 10^{-1}$	$>$ 10 ~ 100

注：安全完整性等级为 SIL1 ~ SIL4 共四级，输油气管道的安全完整性等级最高为 SIL3。

标准用词说明

1　为便于在执行本规范条文时区别对待，对要求严格程度不同的用词说明如下：

1）表示很严格，非这样做不可的用词：
正面词采用“必须”，反面词采用“严禁”。

2）表示严格，在正常情况下均应这样做的用词：
正面词采用“应”，反面词采用“不应”或“不得”。

3）表示允许稍有选择，在条件许可时首先应这样做的用词：
正面词采用“宜”，反面词采用“不宜”。

4）表示有选择，在一定条件下可以这样做的用词，采用“可”。

2　本规范中指明应按其他有关标准、规范执行的写法为：“应符合……的规定”或“应按……执行”。

引用标准名录

《电气 / 电子 / 可编程电子安全相关系统的功能安全　第 3 部分：软件要求》GB/T 20438.3

《油气田及管道工程计算机控制系统设计规范》SY/T 7628

《油气输送管道计算机控制系统报警管理技术规范》SY/T 7631

中华人民共和国石油天然气行业标准

输油气管道工程
安全仪表系统设计规范

SY/T 6966—2023

条 文 说 明

修 订 说 明

《输油气管道工程安全仪表系统设计规范》（SY/T 6966—2023），经国家能源局于2023年5月26日以第4号公告批准发布，自2023年11月26日起实施。

本规范在《输油气管道工程安全仪表系统设计规范》（SY/T 6966—2013）的基础上修订而成，上一版的主编单位是中国石油天然气管道工程有限公司，主要起草人是聂中文、邓东花、王怀义、张文伟、卢文达、安垚、程德发、史威、李秋娟、史学玲、朱坤锋、孙立刚、单富强、高原、王勇、杨立萍、胡协兰、郑前、莫巨华、袁泉、李勇、姜宇澄、韩伟伟。

本规范修订过程中，本规范编制组对我国输油气管道安全仪表系统设计现状和特点做了广泛调查研究，收集、听取了各方面的意见，总结了我国陆上原油管道、成品油管道及附属库区、天然气管道等工程安全仪表系统的实践经验，参考了国外先进的技术法规、技术标准，广泛征求了油气管道行业安全仪表系统工程设计、制造、操作维护等技术人员的意见，在此基础上编制了本规范。

为便于广大设计、施工和生产单位有关人员在使用本规范时能正确理解和执行条文规定，本规范编制组按章、节、条顺序编制了本规范的条文说明，对条文规定的目的、依据及执行中需注意的有关事项进行了说明。但是，本条文说明不具备与规范正文同等的法律效力，仅供使用者作为理解和把握规范规定的参考。

目　次

2　术语及缩略语

2.1　术　　语

2.1.3　站控制系统也可称为站场控制系统或站控系统。

2.1.8　“安全完整性等级”术语引用《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》GB/T 21109.1—2022 的相关定义。

2.1.9　“故障”术语引用《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》GB/T 21109.1—2022 的相关定义。

2.1.11　“安全功能”术语引用《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》GB/T 21109.1—2022 的相关定义。

2.1.12　“安全仪表功能”术语引用《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》GB/T 21109.1—2022 的相关定义。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。

2.1.17　“风险”术语引用《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》GB/T 21109.1—2022 的相关定义。

2.1.20　旁路是指阻断输入信号，使逻辑发送给执行元件的输出信号保持在正常状态；或用预设值代替输入信号，使逻辑正常执行的一种功能。旁路不影响输入参数的报警功能。旁路的形式较多，包括超驰、阻止、禁用、强制、抑制或屏蔽。输油气管道安全仪表系统旁路的形式通常包括：

1. 在检测元件周围设置的物理旁路。

2. 预选输入状态（如开/关输入）或通过一种工程工具（如在应用程序里）强制设置。

3 基本规定

3.1 设计原则

3.1.3 系统安全完整性是指在规定的条件和时间内，安全仪表系统完成安全仪表功能的平均概率。系统中的各个组成部分需满足安全仪表系统的安全完整性要求。安全仪表系统的安全完整性可通过冗余、增加测试频率、故障自诊断等手段予以改善。

3.1.4 安全仪表系统与基本过程控制系统从功能上和结构上分开设置，避免因基本过程控制系统软、硬件的修改影响安全仪表系统安全功能的故障概率。安全仪表系统与基本过程控制系统合用时，共用设备有 SIL 认证并满足使用现场的 SIL 要求。

3.1.5 所谓“故障安全”是指发生故障时，能够进入预定安全状态的能力。故障安全型设计在安全仪表系统中的任何元件、设备、环节或能源失效时，系统能使生产过程处于预定的安全状态。故障安全型设计的最大优点是可确保安全仪表系统中的各个环节随时处于被监控状态，保证系统的可靠性，可最大限度地满足安全完整性要求。在非励磁停车设计中，应特别注意对继电器或开关量仪表触点粘连所引起系统失效处理。在系统执行重要的安全功能处，应考虑采用表决系统来满足安全完整性要求。

3.2 系统间的关系

3.2.1 基本过程控制系统是执行常规正常生产功能的控制系统。基本过程控制系统执行基本生产控制功能，以达到生产过程的正常操作要求。

安全仪表系统则监视生产过程的状态，判断危险条件，防

止风险的发生或者减轻风险造成的后果。因此，一个生产过程应具备过程控制系统和安全仪表系统这两类不同功能的系统，基本过程控制系统用来执行系统的基本控制功能，而安全仪表系统则监视生产过程的状态，以保证整个系统的安全运行。

基本过程控制系统与安全仪表系统的功能不同，基本过程控制系统执行基本过程控制功能以达到生产过程的操作要求；安全仪表系统则监视生产过程的状态，判断是否出现危险条件，防止风险的发生或者减轻风险发生后造成的后果。基本过程控制系统是主动的、动态的，安全仪表控制系统则是被动的、休眠的。

ESD 是安全仪表系统实现站场安全保护功能的主体部分。

3.2.3 当发生火灾时，由火灾自动报警系统发出综合报警信号至安全仪表系统，并自动进行安全相关联锁，联锁形式可分为延时后无人工干预后联锁或增加人工确认后联锁。

5 系统设置

5.1 系统组成

5.1.2 SIS 用户接口是操作员接口和维护 / 工程师接口。SIS 和 HMI 之间交流的信息或数据既可能同 SIS 有关，也可能是资料性的。

5.2 检测元件

5.2.1 检测元件分开独立设置，指采用多台仪表将控制功能与安全联锁功能隔离，即基本过程控制系统与安全仪表系统的实体分离。

当多个检测元件仅用于检测、显示功能时，可与基本过程控制系统共用。当检测元件用于控制功能时，基本过程控制系统应与安全仪表系统分别设置。

5.2.2 检测元件冗余设置，指采用多台仪表完成相同的功能，通过冗余提高系统的安全性和可用性。

5.2.3 对于冗余方式的选择，综合考虑可靠性、可用性和经济性，防止设计不足或过度设计。NooM 表示 M 个检测元件中有 N 个元件达到触发条件时，该安全仪表功能回路才可联锁动作。

5.3 执行元件

5.3.5 第 2 款第 1）项中压缩机进出口紧急关断阀一般为气动阀、气液联动阀，部分管道公司也习惯采用电动阀。

5.4 逻辑控制单元

5.4.3 SIL1 级安全仪表系统逻辑控制单元中的中央处理单元、

电源模块、通信网络与接口可以冗余配置；SIL2 级安全仪表系统逻辑控制单元中的中央处理单元、电源模块、通信网络与接口通常冗余配置，输入 / 输出模块通常冗余配置；SIL3 级安全仪表系统逻辑控制单元中的中央处理单元、电源模块、输入 / 输出模块及通信网络与接口需要冗余配置。

5.5 接　口

5.5.1 当安全仪表系统与基本过程控制系统共用以太网时，如基本过程控制系统受网络安全影响，可采取相应的技术手段来保证安全仪表系统的正常工作。安全仪表系统与基本过程控制系统之间串行通信，基本过程控制系统为主站，安全仪表系统为从站。

5.5.3 维护 / 工程师接口用于安全仪表系统编程组态、调试、系统诊断、状态监测、修改及系统维护。

5.6 辅 助 操 作

5.6.2 根据辅助操作盘设置要求，盘面布置示意图如图 1 所示。

5.6.3 维护旁路开关用于现场仪表和线缆维护时暂时旁路信号输入，使逻辑控制单元的输入不受现场仪表信号的影响。需严格限制维护旁路开关的使用，维护旁路开关在非维护时间需要置于正常状态，保持安全仪表系统的完整和正常运行。

5.6.4 操作旁路的应用多用于流程启动、停止状态，例如在流程启动前，泵入口汇管压力低低报警，此时如果不旁路该信号，则泵无法启动，泵入口汇管压力也无法达到正常值。因此在启动前需要先将该信号置于操作旁路，以满足启动条件。

5.6.5 现场设备复位需要就地完成，阀门需要采用设备本体复位方式，泵、压缩机等设备可以在控制柜复位。

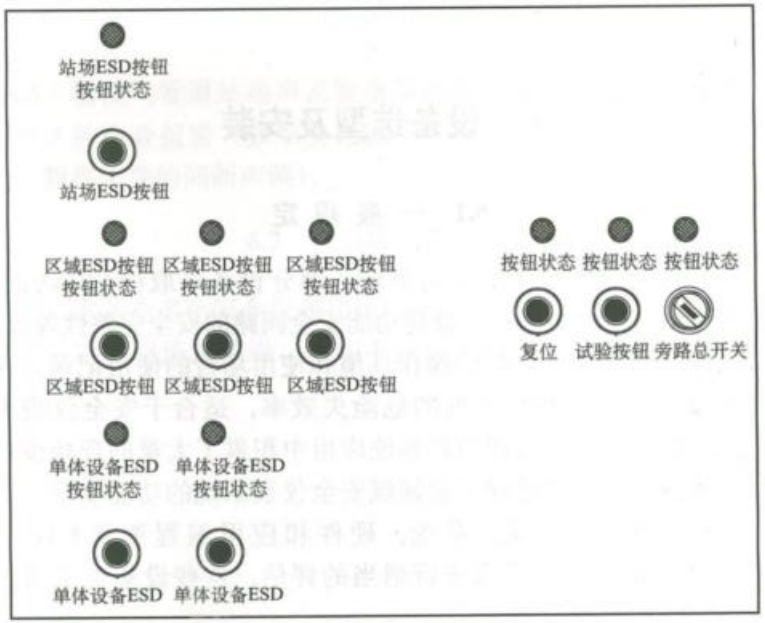


图 1　辅助操作盘盘面布置示意图

6 设备选型及安装

6.1 一 般 规 定

6.1.1 目前的过程工业应用领域，部分设备未取得 SIL 认证，可通过结构约束的手段，提高功能安全回路的安全完整性等级，可依据产品在以往类似的操作环境和使用场合的使用记录，评估该设备是否具有足够低的危险失效率，适合于安全仪表系统。例如，在基本过程控制系统应用中积累了大量的现场设备使用经验，按照《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》GB/T 21109.1—2022 中的要求进行适当的评估，这些设备也可用于 SIS 系统。

6.2 检 测 元 件

6.2.1 逻辑控制单元通常具有接收 HART 协议并具有设备诊断的功能。

6.3 执 行 元 件

6.3.5 气液、电液执行机构一般采用管道用气，当管道气中断时无动力源，无法进行操作，此时需要手动开关阀门。通常情况下，手动操作功能采用物理锁锁止。

6.3.7 通常开关类没有 SIL 等级的认证，为了事件记录应进行动作信号的反馈。执行元件，如阀门动作后，行程位置需反馈。阀门反馈一般采用行程开关，这类反馈设备不需要 SIL 等级认证，常接入 BPCS 系统，仅为动作信号的事件记录或报警。

6.4 辅助操作设施

6.4.5 输油气管道站场声光警报器通常采用红、黄双色闪光报警及3种声音报警（频率变化的持续声调、频率不变的持续声调、频率不变的间断声调）。

6.7 仪表安装及配线

6.7.3 本条指多个安全仪表功能回路之间不应共用同一公共线。

6.7.7 电缆应连续敷设，中间不应有接头，但可采用接线箱进行连接。

7 软件及组态

7.2 HMI 组态及报警

7.2.1 过程执行顺序图显示停车因果关系及顺序。SIS 流程图显示 SIS 参数的动态流程图画面。SIS 维护旁路画面通常以列表及图标方式显示每个停车的因果关系，每一停车原因可单独设置维护旁路 / 正常状态。SIS 操作旁路画面通常以列表及图标方式显示每个需旁路回路的输入、输出关系，对每个回路通常单独设置操作旁路开关、延时时间、剩余时间和剩余时间报警。SIS 数据总貌画面通常以列表显示所有 SIS 相关参数值。

7.2.2 系统诊断画面通常显示系统设备、供电、通信及网络的运行状态及故障设备的位置。系统维护画面通常根据自诊断结果，显示维护提示指导进行维修维护。系统资源画面通常显示整个系统资源的使用情况及各设备负荷。设备状态画面通常显示故障设备位置及相关故障信息。

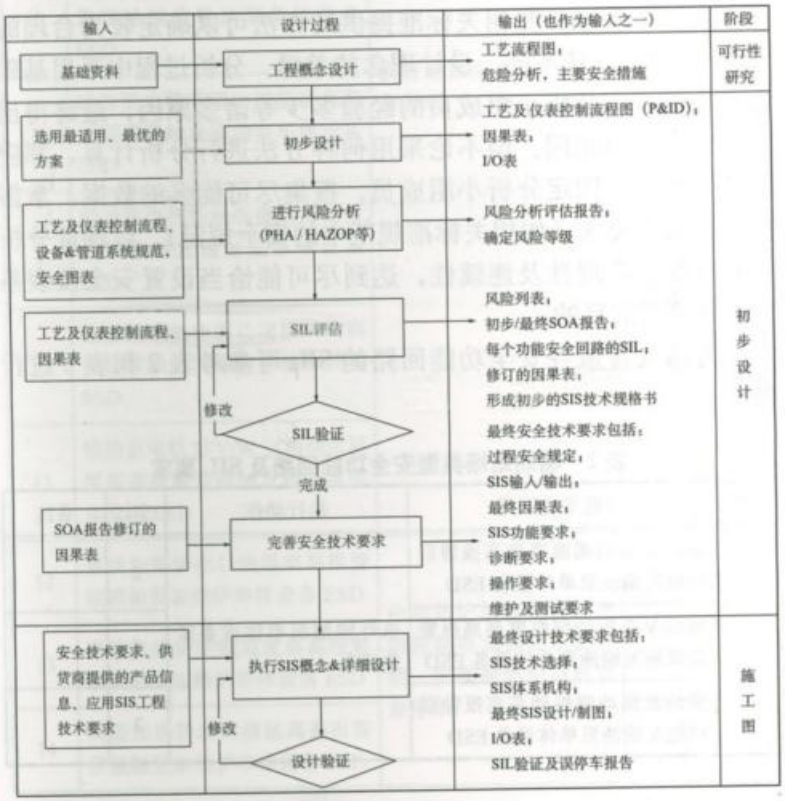
7.3 逻辑控制单元软件组态

7.3.1 软件组态的安全性通常包括软件设计、软件组态及编程、软件集成、软件运行和维护管理、系统确认，以及软件组态的全过程安全性。

8 工程设计与评估

安全仪表系统设计一般分为可行性研究、初步设计、施工图三个阶段。本规范不包括评估、验证、验收等内容，具体评估、验证、验收等方面的要求参见其他相关规范。安全仪表系统的设计过程可参考表 1。

表 1 安全仪表系统设计过程



8.1 基础工程设计

8.1.1 因果图也可称为因果关系图或因果表。

8.3 安全完整性等级评估

确定所需的 SIL 是整个系统设计过程中最重要的环节之一。对每项安全功能确定适当的安全完整性等级，进而采取相应的安全仪表系统，使安全仪表系统能够发挥恰当的作用，避免盲目追求过高安全等级导致过多的停车和泄压带来的运行及操作风险，或过低的安全等级造成潜在的安全隐患。

到目前为止，世界上还没有一个统一的、绝对权威的 SIL 评定方法。虽然参照相关标准提供的方法可以确定较为合理的 SIL，但由于方法不同、设计理念的差异、分析过程中采用基础数据的区别、分析小组成员的经验多少等诸多原因，最终得出的结论会不尽相同。但不论采用何种方法进行分析计算，都应制订好程序，固定分析小组成员，搜集尽可能多的数据，掌握最低的安全要求（如相关标准规范中的安全规定），以保证分析的有效性、合理性及连续性，达到尽可能恰当设置安全仪表系统及其等级的目的。

输油气管道各安全功能回路的 SIL 可参考表 2 和表 3 进行确定。

表 2 输油站场典型安全功能回路及 SIL 要求

序号	功能安全回路	执行动作	SIL	备注
1	输油泵驱动端温度高高报警联锁触发输油泵单体设备 ESD	执行输油泵单体设备紧急停车	2	
2	输油泵非驱动端温度高高报警联锁触发输油泵单体设备 ESD		2	
3	输油泵驱动端振动高高报警联锁触发输油泵单体设备 ESD		2	

续表 2

序号	功能安全回路	执行动作	SIL	备注
4	输油泵非驱动端振动高高报警联锁触发输油泵单体设备 ESD	执行输油泵单体设备紧急停车	2	
5	输油泵泵壳温度高高报警联锁触发输油泵单体设备 ESD		2	
6	输油泵机械密封泄漏（压力开关）检测高高/（液位开关）检测低低报警联锁触发输油泵单体设备 ESD		2	
7	输油泵电机驱动端温度高高报警联锁触发输油泵单体设备 ESD		2	
8	输油泵电机非驱动端温度高高报警联锁触发输油泵单体设备 ESD		2	
9	输油泵电机驱动端振动高高报警联锁触发输油泵单体设备 ESD		2	
10	输油泵电机非驱动端振动高高报警联锁触发输油泵单体设备 ESD		2	
11	输油泵电机 U/V/W 三相绕组温度高高报警联锁触发输油泵单体设备 ESD		2	
12	直接加热炉出口油温高高报警联锁触发加热炉单体设备 ESD	由加热炉单体设备的逻辑控制单元完成逻辑控制，实现加热炉单机紧急停车	1	
13	直接加热炉炉膛温度高高报警联锁触发加热炉单体设备 ESD		1	
14	间接加热炉出口油温高高报警联锁触发加热炉单体设备 ESD		1	

续表 2

序号	功能安全回路	执行动作	SIL	备注
15	给油泵入口压力低低报警联锁触发超压保护	触发顺序停泵程序	1	
16	输油泵进口汇管压力低低报警联锁触发超压保护		1	
17	输油泵出口汇管压力高高报警联锁触发超压保护		1	
18	在首站、输油泵站出站压力高高报警联锁触发超压保护		2	
19	减压站出站处压力高高报警联锁触发超压保护	关闭减压站进站电动阀	1	
20	罐液位高高报警触发罐单体设备 ESD	关闭罐前进罐阀门	2	

表 3　输气站场安全功能回路及 SIL 要求

序号	功能安全回路	执行动作	SIL	备注
1	压缩机组一级干气密封泄漏气压力高高报警联锁触发单体设备 ESD（泄压）	触发单机组 ESD 停车，关闭单机组进出口紧急关断阀，打开对应的紧急放空阀	1	
2	压缩机组火灾报警（燃驱机组）		2	
3	压缩机或主电机、燃气轮机轴承振动高高报警联锁触发单体设备 ESD（保压）	触发单机组 ESD 停车，关闭单机组进出口紧急关断阀	2	
4	压缩机或主电机、燃气轮机轴承位移高高报警联锁触发单体设备 ESD（保压）		2	

续表 3

序号	功能安全回路	执行动作	SIL	备注
5	压缩机或主电机（包含励磁机）、燃气轮机轴承温度高高报警联锁触发单体设备 ESD（保压）	触发单机组 ESD 停车，关闭单机组进出口紧急关断阀	2	
6	压缩机或主电机定子温度高高报警联锁触发单体设备 ESD（保压）		2	
7	压缩机组转速超速联锁触发单体设备 ESD（保压）		1	
8	压缩机组润滑油总管压力低低报警联锁触发单体设备 ESD（保压）		1	
9	压缩机组隔离气压力低低报警联锁触发单体设备 ESD（保压）		1	
10	压气站出站压力高高报警联锁触发超压保护	触发运行机组 ESD 停车（保压）	2	
11	分输支路压力高高报警	关闭出站紧急关断阀	2	
12	电加热器出口温度高高报警触发安全联锁保护	停电加热器	2	
13	电加热器流量低低报警触发安全联锁保护		2	