H G

中华人民共和国化工行业标准

HG/T 22820-202X

化工安全仪表系统工程设计规范

Engineering design code for safety instrumented system in chemical industry

XX-XX-XX 发布　　XX-XX-XX 实施

中华人民共和国工业和信息化部 发布

中华人民共和国化工行业标准

化工安全仪表系统工程设计规范

Engineering design code for safety instrumented system in chemical industry

HG/T 22820-202X

主编单位：中石油华东设计院有限公司

批准部门：中华人民共和国工业和信息化部

实施日期：xxxx 年 xx 月 xx 日

XXX 出版社

Xxxx　　北京

前　言

本规范根据工业和信息化部（工信厅科函[2019]195号工业和信息化部办公厅关于印发2019年第二批行业标准制修订项目计划的通知）的要求，中国石油和化工勘察设计协会为技术归口单位，协会自动控制设计专业委员会负责组织，由中石油华东设计院有限公司为主编单位，会同参编单位编制完成。

本规范在制定过程中，编制组进行了广泛的调查研究，认真总结了化工领域安全仪表系统在工程设计、系统集成、运行维护过程中的实践经验，并在广泛征求意见的基础上，最后经审查定稿。

本规范组成内容共有16章。规范正文包含以下内容：总则，术语与缩略语，基本要求，设计原则，系统组成，测量仪表，最终元件，逻辑控制器，网络和通信接口，人机接口，应用程序，供电、接地、防雷与配线，工程设计，集成、组态、调试、验收、联调与确认，维护、维修和变更管理，文档管理。

本规范由工业和信息化部负责管理，由中国石油和化工勘察设计协会技术归口，协会自动控制设计专业委员会负责日常管理，由中石油华东设计院有限公司负责具体技术内容的解释。在执行过程中如有意见和建议，请与自动控制设计专业委员会负联系（联系地址：海徐汇区中山南二路1089号徐汇汇苑大厦12层，邮编：200030，电话：021-64578936）以供今后修订时参考。本规范主编单位、参编单位、主要起草人和主要审查人：

主编单位：中石油华东设计院有限公司

参编单位：浙江中控技术股份有限公司

杭州和利时自动化有限公司

北京康吉森自动化科技有限公司

主要起草人：林洪俊 李胜利 张少鹏 董爱娜 马　涛 俞文光 吴春雪 潘东邱　学 霍光学 王　辉 杨　春 王付霞 张　聪 蔡明锋

主要审查人：曾裕玲 梁　达 李　涛 黄　源 范咏峰 赵　柱 王雪梅魏　毅 张同科 李德刚 梁俊鹏 徐明慧 王秋红 张　志王方良 程　泱 吴天一 朱东利 阎　洁 夏余欢 楼　灵

目　　次

Contents

1 总　则

1.0.1 为了统一安全仪表系统在化工行业的技术要求，推进安全仪表系统工程设计的规范化，达到技术先进、经济合理、安全适用的目的，制定本规范。

1.0.2 本规范适用于化工企业新建、扩建及改建项目安全仪表系统的工程设计。

1.0.3 化工安全仪表系统的工程设计除应符合本规范外，尚应符合国家现行有关标准的规定。

2 术语与缩略语

2.1 术语

2.1.1 安全仪表系统 safety instrumented system；SIS

实现一个或多个安全仪表功能的仪表系统。

注 1：SIS 由任意组合的测量仪表、逻辑控制器及最终元件组成。它也包括通信、供电、供气、伴热、电缆、光缆、取源管件等。

注 2：SIS 也可以包括软件。

注 3：SIS 可以包括人为动作作为 SIF 的一部分，如人工按动紧急停车按钮。

2.1.2 风险 risk

伤害发生可能性与该伤害严重性的组合。

注：发生可能性包括暴露于危险情况的概率，危险事件的发生概率和避免或限制伤害的可能性。

2.1.3 安全仪表系统的安全生命周期 SIS safety life-cycle

从工程方案设计开始到所有安全仪表功能停止使用期间，安全仪表系统实现安全仪表功能涉及的所有必要活动。

2.1.4 危险 hazard

导致人身伤害或疾病、财产损失或环境破坏的潜在根源。

2.1.5 保护层 protection layer

通过控制、预防或减轻以降低风险的任何独立机制。

注：它可能是过程工程机制（如处置危险化学品的容器尺寸），也可能是机械工程机制（如安全阀），或者 SIS，或者是管理规程（如应对紧急危险的应急计划）。可以自动启动或手动启动这些响应机制。

2.1.6 安全功能 safety function

对于特定危险事件，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。

2.1.7 安全仪表功能 safety instrumented function；SIF

只能由 SIS 实现的安全功能。安全仪表功能用来达到一个要求的 SIL。SIL 由其它参与降低相同风险的保护层决定。

2.1.8 故障 fault

由于内部异常状态，导致不能执行所需的功能。

2.1.9 安全完整性 safety integrity

安全仪表系统在需要时执行特定安全仪表功能的能力。

2.1.10 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：目标失效量和 SIL 间的关系见表 1 和表 2。

注 3：SIL4 是安全完整性的最高等级，SIL1 是最低等级。

2.1.11 故障裕度 fault tolerant

在出现故障或错误时，某项功能仍继续执行规定功能的能力。

2.1.12 失效 failure

失去按要求执行的能力。

2.1.13 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；
- 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。

2.1.14 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，但是有更高的成功率（要求模式时），或者有更低的危险事件发生可能性（连续模式时）；
- 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，但是对其它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。

2.1.15 目标失效量 target failure measure

SIF 要求的性能，既可规定为在低要求模式下要求时执行 SIF 的平均失效概率，也可规定为在连续模式时执行 SIF 的危险失效平均频率。表 1 和表 2 给出了 SIL 和目标失效量之间的关系。

2.1.16 测量仪表　sensor

安全仪表系统或基本过程控制系统中检测测量过程变量的设备。

2.1.17 逻辑控制器　logic solver

安全仪表系统或基本过程控制系统中执行一个或多个逻辑功能的设备。

2.1.18 最终元件　final element

安全仪表系统或基本过程控制系统中达到或保持安全状态执行必要物理动作的设备。

注：例如，控制阀、开关设备以及电机，包括他们的辅助元件（如电磁阀和用来驱动控制阀的执行机构）。

2.1.19 关联仪表　signal transmission instrument

安全仪表系统或基本过程控制系统中，在测量仪表与逻辑控制器之间或逻辑控制器与最终元件之间，执行信号变换、信号隔离、能量限制等功能的仪表。如：信号转换器，信号隔离器，继电器，安全栅、电涌保护器等。

2.1.20 基本过程控制系统　basic process control system；BPCS

对来自工艺过程及其关联设备的输入信号、其它可编程电子系统和/或操作员的输入信号进行运算处理，并作出响应输出信号，使工艺过程及其关联设备按所期望的方式运行的系统。但它不执行任何安全仪表功能。

2.1.21 故障安全　fail safe

安全仪表系统发生故障时，使被控制过程转入预定安全状态。

2.1.22 冗余　redundancy

采用两个或多个部件或手段执行一个特定功能或展示信息。

2.1.23 开关量　digital variable

只有两个数值的变量，用来表示事物或事件的状态。也称为数字变量。

2.1.24 开关　switch

具有两种稳定位置的状态器件。有软件开关和硬件开关。

2.1.25 按钮　push button

只有一种稳定位置的状态器件。有软件按钮和硬件按钮。

2.1.26 触点　mechanical contact

由导电的金属元件组成的机械式电气器件。在外界因素作用下可以改变接通或断开导电状态。

2.1.27 可编程电子系统　programmable electronic system；PES

基于可以按功能需要编制或改变运行程序的电子设备，用于控制、保护或监视的系统。

2.1.28 过程安全时间 process safety time

在 SIF 未执行时，从过程失效或基本过程控制系统失效到危险事件发生之间的时间段。

注 1：这只是过程的一个属性。SIF 需在过程延迟的情况下足够快的检测到失效并且完成规定的动作以防止危险事件发生。

注 2：用于确定 SIF 响应时间的过程安全时间为从工艺过程参数超过安全联锁阈值到危险事件发生之间的时间。

2.1.29 旁路 bypass

阻止执行所有或部分安全仪表系统功能的动作或设施。

2.1.30 验证 verification

通过检查和客观证据证实要求已满足。

注 1：是指在相关 SIS 安全生命周期的每个阶段，通过分析和/或测试，证明对于特定的输入、输出在各方面满足为该特定阶段所设置的目标和要求的活动。

注 2：验证活动的例子包括：

- 为确保符合某阶段的目标和要求，对输出进行审查，其中要考虑该阶段的特定输入；
- 设计审查；
- 对设计的产品进行测试，以确保它们按规范工作；
- 在系统各个部分分步组装到一起后进行集成测试，并进行环境性能试验以确保所有部分能按规定方式一起工作。

2.1.31 确认 validation

通过检查和提供客观证据，证实用于某个规定用途的特定要求得到了满足。这是指证明安装后的 SIF 和 SIS 在各方面满足 SRS。

2.1.32 安全要求规格书 safety requirement specification；SRS

包含所有安全仪表功能和与之相关的安全完整性等级要求的规范性文件。

2.1.33 平均恢复时间 mean time to restoration；MTTR

完成功能恢复的平均预计时间。

2.1.34 检验测试 proof test

为了检测安全仪表系统隐性的危险故障的周期性测试。必要时，通过维护将安全仪表系统恢复到新的状态或尽可能接近该状态。

2.1.35 以往使用 prior use

基于以往在类似运行环境的使用经验，由用户开展的文档化评估，以证明某个设备适用

于 SIS，并且能达到所需的功能和安全完整性要求。

注 1：为了基于以往使用证明一个 SIS 设备可用，用户需文档说明设备能在类似的运行环境中实现满意的性能。为高度确定计划的设计、检查、测试、维护和操作具有充分的实践，必须了解在运行环境中设备如何运转。

注 2：经使用证明是基于设备制造商的设计基础（即温度极限、震动极限、腐蚀极限、需要的维护支持）。以往使用在处理设备的安全性能时，设备只能在某个过程领域工厂场地内运行，而这些场地往往不同于制造商的设计基础。

2.1.36 （SIF 的）运行模式 mode of operation（of a SIF）

SIF 的运行方式，可分为低要求模式、高要求模式和连续模式。

1 低要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率不大于一年一次。

2 高要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率大于一年一次。

3 连续模式：在这种运行模式下，SIF 作为正常运行的一部分保持过程处于一种安全状态。

2.1.37 诊断 diagnostics

揭露故障的频繁（相对于过程安全时间）自动测试。

2.1.38 诊断覆盖率 diagnostics coverrage；DC

通过诊断检测出的危险失效率的占比。诊断覆盖率不包括任何被检验测试检测到的故障。

注 1：诊断覆盖率通常应用于 SIS 设备或 SIS 子系统，如通常为传感器、最终元件或逻辑控制器确定诊断覆盖率。

注 2：对安全应用，诊断覆盖率通常应用于 SIS 设备或 SIS 子系统的危险失效。例如，一个设备的危险失效的诊断覆盖率为 DC= $\lambda_{DD}/\lambda_{DT}$，式中 λ_{DD} 是检测到的危险失效率，λ_{DT} 是总的危险失效率。对于一个具有内部冗余的 SIS 子系统，DC 与时间相关：$DC(t)=\lambda_{DD}(t)/\lambda_{DT}(t)$。

注 3：当给出诊断覆盖率（DC）和总的危险失效率（λ_{DT}），则检测到危险失效率（λ_{DD}）和未检测到的危险失效率（λ_{DU}）可以按照如下计算：$\lambda_{DD}=DC\times\lambda_{DT}$，$\lambda_{DU}=(1-DC)\times\lambda_{DT}$。

2.1.39 误停车率 spurious trip rate；STR

特定时间内，在过程未发生异常的情况下安全仪表功能发生安全停车的比例。

2.1.40 共因失效 common cause failure

由单个事件引起不同设备同时失效，此类失效之间没有因果关系。

2.1.41 系统性能力 systematic capability；SC

当设备根据安全手册规定的说明进行应用时，设备的系统性安全完整性达到规定的 SIL 要求的置信度的度量（表示为 SC1 到 SC4），其与特定的安全功能有关。

注 1：系统性能力参照 GB/T 20438.2-2017 和 GB/T 20438.3-2017 中的系统性故障的避免和控制要求确定。

注 2：系统性失效机制取决于设备的特性。对于只由硬件组成的设备，只考虑硬件失效机制。对于由硬件和软件组成的设备，则需要考虑硬件和软件失效机制间的相互影响。

注 3：某设备 SC N 的系统性能力是指当设备按照安全手册规定的 SC N 要求应用时，此设备达到了 SC N 的系统性安全完整性。

2.1.42 结构约束 architectural constraint；AC

对安全回路中的某个组件从硬件结构上进行约束，限制所能达到的 SIL。

2.1.43 可用性 availability

当某一个系统设备发生故障时，系统在保证安全功能的前提下，仍能保证生产过程不中断的能力。

2.1.44 可靠性 reliability

在给定的时间周期内，系统在规定的状态下完成设计功能的能力。

2.2 缩略语

本规范准采用下列缩略语：

BPCS	Basic Process Control System	基本过程控制系统
CPU	Central Process Unit	中央处理单元
DC	Diagnostic Coverage	诊断覆盖率
FAT	Factory Acceptance Testing	工厂验收测试
FVL	Full variability language	完全可变语言
FSA	Functional Safety Assessment	功能安全评估
FST	Full Stroke Test	全行程测试
HAZOP	Hazard and Operability Study	危险和可操作性分析
HFT	Hardware Fault Tolerance	硬件故障裕度
HMI	Human Machine Interface	人机接口
HSE	Health，Safety and Environment	健康、安全和环境
I/O	Input/output module	输入/输出模件

LOPA	Layer of Protection Analysis	保护层分析
LVL	Limited variability language	有限可变语言
MooN	“M” out of “N”	“N”取“M”
MOS	Maintenance Override Switch	维护旁路开关
MTTR	Mean Time To Restoration	平均恢复时间
OOS	Operational Override Switch	操作旁路开关
PES	Programmable Electronic System	可编程电子系统
PFD	Probability of Dangerous Failure on Demand	要求时危险失效概率
PFDavg	Average Probability of Dangerous Failure on Demand	要求时危险失效平均概率

PFH Probability (average frequency of dangerous failures)of Failure per Hour 每小时失效概率（危险失效平均频率）

PLC	Programmable Logic Controller	可编程逻辑控制器
PST	Partial Stroke Test	部分行程测试
RRF	Risk Reduction Factor	风险降低因子
SAT	Site Acceptance Testing	现场验收测试
SC	Systematic Capability	系统性能力
SER	Sequence of Events Recorder	事件顺序记录
SIF	Safety Instrumented Function	安全仪表功能
SIL	Safety Integrity Level	安全完整性等级
SIS	Safety Instrumented System	安全仪表系统
SRS	Safety requirement specification	安全要求规格书
STR	Spurious Trip Rate	误停车率
UPS	Uninterruptable Power Supply	不间断电源

3 基本要求

3.1 安全生命周期

3.1.1 化工厂或装置工程设计中，应确定安全仪表系统安全生命周期内所需要的技术活动和管理活动。安全仪表系统设计应按照安全生命周期进行，完成相关工作。

3.1.2 安全仪表系统的安全生命周期宜分为工程设计阶段、集成调试阶段和运行维护阶段。如图 3.1.2 所示。

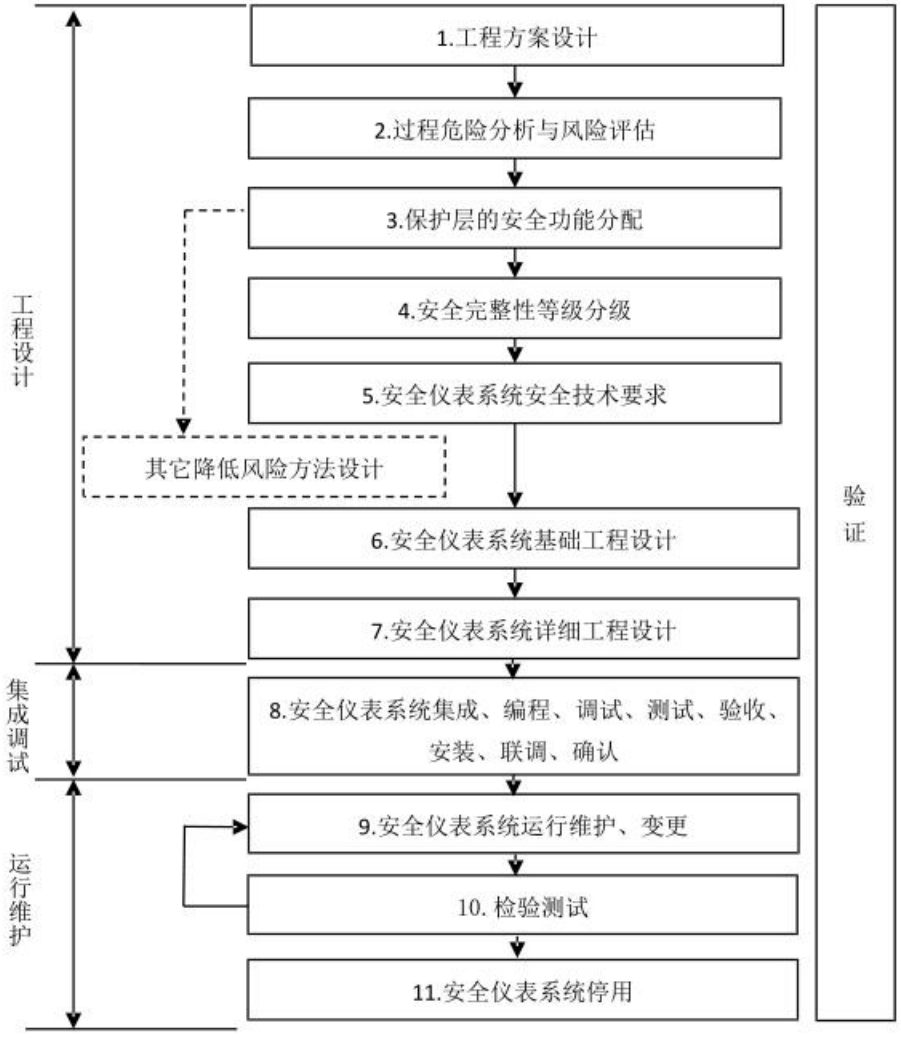

图 3.1.2 安全仪表系统安全生命周期工作流程

3.1.3 对安全仪表系统实际安全完整性与目标安全完整性应进行符合性验证。需要时可对安全仪表系统的可用性进行验证，如误停车率（STR）。

3.1.4 工程设计阶段宜包括工程方案设计，过程危险分析与风险评估，保护层的安全功能分

配，安全完整性等级分级，确定安全仪表系统安全技术要求，安全仪表系统基础工程设计，安全仪表系统详细工程设计。

3.1.5 集成调试阶段宜包括安全仪表系统硬件集成、应用软件编制、调试、测试、验收、安装、联调及确认。

3.1.6 运行维护阶段宜包括安全仪表系统维护、变更、检验测试、停用等。

3.1.7 工程方案设计宜包括初步的危险分析，自动检测、报警、控制、联锁方案，仪表选型方案，其它安全措施等。

3.1.8 过程危险分析和风险评估宜包括识别工艺过程、相关设备及生产环境的危险事件、原因、危险事件发生的顺序、可能性及后果，确定降低风险的要求和措施，确定安全仪表功能等。

3.1.9 保护层安全功能的分配可包括分配预防、控制或减缓过程危险的保护层安全功能，分配安全仪表功能的风险降低目标。保护层的安全功能分配应符合现行国家标准《电气/电子/可编程电子安全相关系统的功能安全》GB/T 20438、《过程工业领域安全仪表系统的功能安全》GB/T 21109 和《保护层分析（LOPA）应用指南》GB/T32857 的有关规定。

3.1.10 安全仪表功能的安全完整性等级分级应根据过程危险分析和保护层功能分配的结果确定，不得低于分配的风险降低目标。

3.1.11 安全仪表系统安全技术要求应基于国家和企业风险标准，依据过程危险分析与风险评估得出的风险降低要求，确定工程设计、运行、维护和管理策略。安全技术要求可通过编制安全要求规格书表述。安全要求规格书的内容应包括过程与环境安全要求、安全仪表功能及与之相关的安全完整性等级要求、安全仪表系统的硬件性能与规格要求、应用程序的安全要求等。

3.1.12 安全仪表系统的基础工程设计应根据安全技术要求，编制满足安全完整性等级要求和满足可用性、可维护性、经济性的安全仪表系统技术方案。设计文件宜包括安全联锁因果表或联锁逻辑图、逻辑控制器技术规格书、测量仪表及最终元件选型及数据表等。

3.1.13 安全仪表系统的详细工程设计应根据安全技术要求和基础设计编制安全仪表系统技术文件。设计文件宜包括安全仪表系统逻辑控制器技术规格书、联锁逻辑图、输入/输出点清单、报警联锁设定值表、测量仪表及最终元件仪表规格书等。

3.1.14 集成、编程、调试、测试、验收、安装、联调、确认应包括下列内容：

1 安全仪表系统集成、编程、调试应在集成工厂根据安全仪表系统的安全技术要求、设备技术规格书及联锁逻辑图的要求进行。

2 安全仪表系统测试、验收应包括工厂测试、验收和现场测试、验收。测试、验收内容应包括安全仪表系统硬件、系统软件和应用程序等。

3 安全仪表系统应根据安装设计要求安装，应根据联锁逻辑图等设计文件联调。

4 安全仪表系统投用前应开展确认工作，确认系统具备投入使用条件。确认内容宜包括测量仪表、逻辑控制器、最终元件及关联设备的测试、安装、联调等程序和最终结果符合要求。

3.1.15 安全仪表系统运行维护阶段应建立保持安全仪表系统功能安全有效性的运行维护作业规程。运行维护应按照安全技术要求、安全手册和维护规程进行。

3.1.16 安全仪表系统的硬件、软件的变更应进行风险评估和可靠性、可用性需求验证，满足需求目标。变更过程应按照变更管理程序进行，获得授权批准，并应保留变更记录。

3.1.17 安全仪表系统应按照检验测试间隔要求进行功能测试。对发现的失效进行原因分析并消除。检验测试应按照检验测试管理程序进行，并应保留测试记录。

3.1.18 安全仪表系统的停用应进行审查并得到批准。安全仪表系统的更新应进行安全评估、验证，更新后的安全仪表系统应实现规定的安全仪表功能和安全完整性等级。更新过程应按照更新管理程序进行，获得授权批准，并应保留更新记录。

3.1.19 运行维护人员应定期培训。培训内容宜包括安全仪表系统功能、测量仪表、最终元件、逻辑控制器、系统故障报警、仪表维护旁路、操作旁路、联锁逻辑图、安全技术要求等。

3.2 安全完整性

3.2.1 安全仪表系统安全完整性应包括硬件设备安全完整性和系统安全完整性。硬件设备安全完整性应包括硬件设备危险失效率和结构约束。

3.2.2 硬件设备安全完整性等级可分为 SIL 1、SIL 2、SIL 3、SIL 4。

3.2.3 在低要求模式时，硬件设备安全完整性等级应采用要求时危险失效平均概率（PFDavg）或风险降低因子（RRF）衡量。应根据表 3.2.3 确定。

表 3.2.3 安全完整性等级（低要求模式）

安全完整性等级（SIL）	要求时危险失效平均概率（PFD_{avg}）	风险降低因子（RRF）
4	$\geq 10^{-5}$ 且 $<10^{-4}$	>10000 到≤100000
3	$\geq 10^{-4}$ 且 $<10^{-3}$	>1000 到≤10000

2	≥10^{-3} 且<10^{-2}	>100 到≤1000
1	≥10^{-2} 且<10^{-1}	>10 到≤100

3.2.4 在连续模式或高要求模式时，硬件设备安全完整性等级应采用每小时危险失效平均频率（PFH）衡量，应根据表 3.2.4 确定。

表 3.2.4 安全完整性等级（连续模式或高要求模式）

安全完整性等级（SIL）	每小时危险失效平均频率（PFH）
4	≥10^{-9} 且<10^{-8}
3	≥10^{-8} 且<10^{-7}
2	≥10^{-7} 且<10^{-6}
1	≥10^{-6} 且<10^{-5}

3.2.5 安全仪表功能的硬件设备危险失效平均概率或每小时危险失效平均频率应包括安全仪表功能回路中所有设备的危险失效平均概率或每小时危险失效平均频率。

3.2.6 安全仪表功能的硬件设备配置结构应满足结构约束的要求。结构约束可通过硬件故障裕度（HFT）要求表达。

3.2.7 安全仪表系统可分解为独立子系统（如测量仪表、逻辑控制器、最终元件），硬件故障裕度可在子系统层级指定。

3.2.8 安全仪表系统或子系统的硬件故障裕度应符合下列要求之一：

（1）表 3.2.8 的要求；

（2）GB/T 20438.2-2017 的 7.4.4.2（路线 1H）的要求；

（3）GB/T 20438.2-2017 的 7.4.4.3（路线 2H）的要求。

表 3.2.8 不同 SIL 对应的最小 HFT 要求

SIL	运行模式	要求的最小 HFT
1	任何模式	0
2	低要求模式	0
2	高要求/连续模式	1

3	任何模式	1
4	任何模式	2

注 1：表中 FVL 和 LVL 可编程设备的诊断覆盖率不应小于 60%。

2：表中设备失效率计算中使用的可靠性数据应由不小于 70%的统计置信区间上限确定。

3.2.9 安全仪表系统的系统性能力可分为 SC1、SC2、SC3、SC4 共 4 级。

3.2.10 安全仪表系统的安全完整性等级应为硬件安全完整性等级与系统性能力等级中的较小值。

3.2.11 仪表设备可靠性数据宜来自以往使用数据、安全完整性认证报告、公开发行的数据库或手册等。

4 设计原则

4.0.1 安全仪表系统的工程设计应满足化工厂或装置的安全仪表系统安全技术要求。

4.0.2 安全仪表系统的工程设计应兼顾安全完整性、可用性、可维护性、可追溯性和经济性，应防止设计不足或过度设计。

4.0.3 化工厂或装置安全仪表功能的安全完整性等级不应高于 SIL 3 级。

4.0.4 安全仪表功能的响应时间应小于过程安全时间。

4.0.5 安全仪表系统可执行一个或多个安全仪表功能。当多个安全仪表功能在同一安全仪表系统内实现时，系统的共用部分应满足所有相关安全仪表功能的安全技术要求，包括安全仪表功能要求和安全完整性等级要求。

4.0.6 安全仪表系统应独立于基本过程控制系统，应独立完成安全仪表功能。

4.0.7 安全仪表系统与基本过程控制系统之间的共用设备应优先执行安全仪表功能。

4.0.8 非安全仪表功能在安全仪表系统中实施不应影响安全仪表功能的执行。

4.0.9 安全仪表系统宜设计为故障安全型，包括安全仪表系统电源故障、气源故障、信号线路断路、设备故障等。

4.0.10 安全仪表系统宜具有故障自诊断功能，可编程逻辑控制器应具有故障自诊断功能。

4.0.11 安全仪表系统中间环节宜尽可能少。

4.0.12 可编程逻辑控制器的中央处理单元、输入输出单元、通信单元及电源单元等，应采用冗余技术。

4.0.13 安全仪表系统的交流供电应采用 UPS 供电。

4.0.14 安全仪表系统设备之间应时钟同步。安全仪表系统应与基本过程控制系统的时钟同步。

4.0.15 大型工艺装置之间、重要工艺装置之间安全仪表系统逻辑控制器应独立设置。在满足可靠性、可用性、可维护性等要求时，工艺装置之间可共用安全仪表系统逻辑控制器。

4.0.16 安全仪表系统应设置信息安全防护措施。

4.0.17 仪表设备检验测试间隔宜与工艺装置停车检修间隔相同。当仪表设备检验测试间隔小于工艺装置停车检修间隔时应设计检验测试措施。

4.0.18 安全仪表系统过程测量数据、输出信息、报警信息、操作信息、动作信息等记录存储时间不宜少于 180 天。

5　系统组成

5.0.1 安全仪表系统应包括测量仪表、逻辑控制器、最终元件、关联仪表、测量管路、信号线路、网络和通信接口、人机接口设备等。

5.0.2 可编程电子系统逻辑控制器应包括中央处理单元、输入单元、输出单元、电源单元、通信单元等。

5.0.3 关联仪表应包括逻辑控制器输入、输出回路中的信号分配器、隔离器、信号转换器、安全栅、电涌防护器、继电器等。

5.0.4 人机接口设备应包括操作站、报警灯、仪表维护旁路用开关、操作旁路开关、复位按钮、紧急停车按钮、工程师站、事件顺序记录站等。

5.0.5 安全仪表系统逻辑控制器内和逻辑控制器与工程师站、操作站、事件顺序记录站之间应采用网络通信互联。

5.0.6 安全仪表系统网络应按功能分层设计，宜分为安全逻辑控制层和操作监控层。

5.0.7 安全仪表系统网络宜分域设计，可按工艺装置或装置群分域。

5.0.8 安全仪表系统网络应冗余配置。

5.0.9 安全仪表系统网络通信介质可采用通信光纤或通信电缆。

6 测量仪表

6.1 基本规定

6.1.1 测量仪表的性能和配置应满足安全仪表功能及其安全完整性等级、结构约束的需求。

6.1.2 测量仪表的配置应满足可用性的要求。

6.1.3 测量仪表宜采用模拟量输出信号测量仪表，也可采用开关量输出信号测量仪表。测量仪表不应采用现场总线信号或其它通信协议信号作为安全仪表功能的输入信号，不应采用无线信号作为安全仪表功能的输入信号。测量仪表宜采用具有故障自诊断功能的智能仪表。

6.1.4 测量仪表与逻辑控制器之间信号回路中的信号分配器、隔离器、信号转换器、安全栅、电涌防护器、继电器等关联仪表，其性能和配置应满足安全仪表功能及其安全完整性等级的需求。安全栅宜选用隔离型。

6.1.5 测量仪表宜在测量管路中设计仪表维护、维修、检验测试用措施。

6.1.6 测量仪表选型除应满足本规范外，尚应满足现行行业标准《自动化仪表选型设计规范》HG/T20507 的要求。

6.2 独立性设计

6.2.1 安全仪表系统测量仪表独立性设计应满足安全技术要求。

6.2.2 SIL 1 级安全仪表功能的测量仪表宜与基本过程控制系统分开。

6.2.3 SIL 2 级安全仪表功能的测量仪表应与基本过程控制系统分开。

6.2.4 SIL 3 级安全仪表功能的测量仪表应与基本过程控制系统分开。

6.2.5 安全仪表系统与基本过程控制系统的测量仪表取源点宜分开设置。

6.2.6 安全仪表系统冗余的测量仪表之间取源点宜分开设置。

6.2.7 安全仪表系统与基本过程控制系统的测量仪表测量管路应分开设置。

6.2.8 安全仪表系统冗余的测量仪表之间测量管路应分开设置。

6.2.9 在测量仪表测量管路中应设计仪表维护、维修、检验测试用措施。

6.3 冗余设计

6.3.1 安全仪表系统的测量仪表冗余设计应满足下列要求：

1 应满足安全仪表功能对测量仪表安全完整性等级的故障裕度要求；

2 应满足安全仪表功能安全完整性对测量仪表结构约束的要求；

3 应满足工艺装置对测量仪表可用性的要求。

6.3.2 当要求高安全性时，测量仪表应采用安全性冗余结构，单一测量仪表的动作应能实现安全联锁功能。

6.3.3 当要求高可用性时，测量仪表应采用可用性冗余结构，单一测量仪表的动作不能实现安全联锁功能。

6.3.4 当要求兼顾安全性和可用性时，测量仪表应采用兼顾安全性和可用性的冗余结构，如三取二表决机制结构。

6.3.5 测量仪表冗余配置时，宜设置仪表信号之间偏差报警。

7 最终元件

7.1 基本规定

7.1.1 最终元件的性能和配置应满足安全仪表功能及其安全完整性等级、结构约束的要求。

7.1.2 最终元件的配置应满足可用性需求。

7.1.3 最终元件可为控制阀、电机控制器等。动作方式宜为两位式，控制信号宜为开关量信号。

7.1.4 控制阀宜采用气动执行机构，也可采用电液执行机构或电动执行机构。控制阀应为故障安全型。

7.1.5 最终元件与逻辑控制器之间信号回路中的继电器、隔离器、电涌防护器、安全栅等关联仪表，其性能和设置应满足安全仪表功能及其安全完整性等级的需求。安全栅宜选用隔离型。

7.1.6 控制阀宜设计检验测试、维护、维修用措施。

7.1.7 控制阀选型除应满足本规范外，尚应满足现行行业标准《自动化仪表选型设计规范》HG/T20507 的要求。

7.2 独立性设计

7.2.1 安全仪表系统最终元件的独立性设计应满足安全技术要求。

7.2.2 SIL 1 级安全仪表功能的控制阀宜与基本过程控制系统分开。当控制阀与基本过程控制系统共用时，安全仪表功能的需求应被优先执行，并由安全仪表系统独立完成。

7.2.3 SIL 2 级安全仪表功能的控制阀应与基本过程控制系统分开。

7.2.4 SIL 3 级安全仪表功能的控制阀应与基本过程控制系统分开。

7.3 冗余设计

7.3.1 安全仪表系统的最终元件冗余设计应满足下列要求：

1 应满足安全仪表功能对最终元件安全完整性等级的要求；

2 应满足安全仪表功能安全完整性对最终元件结构约束的要求；

3 应满足工艺装置对最终元件可用性的要求；

7.3.2 当要求高安全性时，控制阀应采用安全性冗余结构，单一控制阀的动作应能实现安全

功能。

7.3.3 当要求高可用性时，控制阀应采用可用性冗余结构，单一控制阀的动作不能实现安全功能。

7.4 控制阀附件的配置

7.4.1 气动执行机构的控制电磁阀应安装在靠近气缸、膜头的气动控制管路上。

7.4.2 气动执行机构的控制电磁阀应选用长期带电型，正常时励磁，联锁时非励磁。

7.4.3 气动执行机构控制电磁阀的安全完整性应满足控制阀的安全完整性要求。

7.4.4 气动执行机构的控制电磁阀可通过冗余配置提高可靠性或可用性。当要求高安全性时，电磁阀应采用安全性冗余结构，单一电磁阀的动作应能实现控制阀的安全功能。当要求高可用性时，电磁阀应采用可用性冗余结构，单一电磁阀的动作不能实现控制阀的安全功能。

7.4.5 控制阀应配置现场阀位指示器。

7.4.6 控制阀应配置阀位行程开关。

7.4.7 当控制阀实际检验测试间隔小于计划停车检修间隔，且不具备在线检验测试手段时，可设计部分行程测试措施。

8 逻辑控制器

8.1 基本规定

8.1.1 逻辑控制器可采用可编程电子系统、继电器系统或可编程电子系统与继电器的组合系统。

8.1.2 用于逻辑控制器的可编程电子系统应取得功能安全认证。

8.1.3 逻辑控制器的安全完整性应满足安全仪表功能及其安全完整性等级、结构约束的需求。

8.1.4 逻辑控制器的配置应满足可用性的要求。

8.1.5 逻辑控制器应独立设置，应独立完成安全仪表功能的逻辑控制功能。

8.1.6 可编程电子系统逻辑控制器应冗余配置。

8.1.7 逻辑控制器所有部件应满足安装环境的防电磁干扰、防腐蚀、防潮湿、防锈蚀等要求。

8.1.8 可编程电子系统逻辑控制器的中央处理单元、输入单元、输出单元、电源单元、通信单元等应为独立的单元，应允许在线更换而不影响逻辑控制器的正常工作。

8.1.9 可编程电子系统逻辑控制器的响应时间不宜大于 300ms。响应时间应包括输入处理时间、输入扫描时间、中央处理单元扫描时间、应用软件执行时间、输出扫描时间、输出处理时间、通信时间等。

8.1.10 可编程电子系统逻辑控制器的中央处理单元负荷不应超过额定负荷的 50%。

8.1.11 可编程电子系统逻辑控制器内部通信负荷不应超过 50%，采用以太网的通信负荷不应超过 20%。

8.1.12 可编程电子系统逻辑控制器应具有故障诊断、测试功能。诊断和测试信息应在工程师站显示、记录。

8.1.13 可编程电子系统逻辑控制器的故障应可在安全仪表系统或基本过程控制系统的操作员站报警。

8.2 逻辑控制器输入、输出卡件配置

8.2.1 输入、输出卡件应采用冗余技术。

8.2.2 输入、输出卡件信号通道间应采用光电或电磁技术隔离。

8.2.3 输入、输出卡件宜具有线路断路和短路检测功能，并在安全仪表系统或基本过程控制系统操作员站报警。

8.2.4 安全仪表功能输入、输出卡件的过程输入、输出信号不应采用总线信号，不应采用无线信号。

8.2.5 冗余配置的测量仪表信号宜接到不同的输入卡件。

8.2.6 冗余配置的最终元件宜接到不同的输出卡件。每一输出信号通道应只接一个最终元件。

8.2.7 各类输入、输出卡件宜预留不低于10%的备用通道。

8.2.8 当测量仪表、最终元件端可能引入电气干扰或危害电压时，应在输入、输出卡件之前信号回路中设置隔离措施。模拟量信号宜设置信号隔离器，开关量信号宜设置隔离继电器。

9　网络和通信接口

9.1 基本规定

9.1.1 安全仪表系统通信网络应采用工业交换机，并应冗余配置。安全仪表系统的交换机不应采用级联或堆叠方式扩展交换机端口数量。

9.1.2 网络和通信接口负荷不应超过 50%，采用以太网通信时负荷不应超过 20%。

9.1.3 安全仪表系统网络可包括安全功能网络和非安全功能网络。逻辑控制器内单元间通信网络应为安全功能网络。逻辑控制器之间通信执行完全功能时其通信网络应为安全功能网络。逻辑控制器、操作站、工程师站间通信网络可为非安全功能网络。

9.1.4 安全仪表系统与基本过程控制系统通信不应执行非安全功能。通信接口的故障不应影响安全仪表系统的功能安全。

9.1.5 除旁路信号和复位信号外，基本过程控制系统不应采用通信方式向安全仪表系统发送指令。

9.1.6 安全仪表系统与基本过程控制系统应直接通信，不应通过工厂管理网络传输。通信宜采用 RS485 串行通信接口，MODBUS RTU 通信协议。

9.1.7 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，应采用硬接线方式连接。

9.2 信息安全

9.2.1 安全仪表系统的逻辑控制器采用可编程电子系统时应进行信息安全风险分析与评估，根据评估结果采取相应的信息安全防护措施。

9.2.2 安全仪表系统宜按生产装置或生产区域进行网络分域，分域间宜进行隔离。

9.2.3 安全仪表系统不应接入无线仪表和无线网络。

9.2.4 安全仪表系统的服务器、操作员站、工程师站、事件顺序记录站及其它终端设备应采取防病毒和相应信息安全防护措施。

9.2.5 安全仪表系统不应直接与工厂信息网络相连。安全仪表系统无关的设备或网络不应接入安全仪表系统或利用安全仪表系统网络传输数据。

9.2.6 安全仪表系统的服务器、工程师站、事件顺序记录站 、操作员站等人机接口网络设备应严格管理操作权限。

10 人机接口

10.1 操作员站

10.1.1 安全仪表系统可设操作员站，用于过程信号报警、系统故障报警、联锁动作报警、运行与维护状态显示，联锁逻辑显示，联锁复位、联锁旁路操作与状态显示。

10.1.2 安全仪表系统操作员站失效应不影响安全仪表系统的功能安全。

10.1.3 安全仪表系统操作员站可共用基本过程控制系统的操作员站，也可独立设置操作员站。

10.1.4 操作员站不应具有修改安全仪表系统应用程序的权限。

10.1.5 操作员站设置的软件旁路开关应加键锁或口令保护。

10.1.6 基本过程控制系统的操作员站可设置联锁保护参数预报警。

10.2 辅助操作台

10.2.1 辅助操作台应设置在控制室操作间，安装按钮、开关、报警灯、音响器等。

10.2.2 辅助操作台宜按工艺装置分别设置。

10.2.3 辅助操作台的形式、颜色宜与操作站的操作台协调一致。

10.2.4 辅助操作台上按钮、开关、报警灯的布置、标识应便于操作人员辨识和操作。

10.2.5 辅助操作台上的按钮、开关、报警灯、音响器应采用硬接线方式接入安全仪表系统输入、输出卡件。

10.2.6 紧急停车按钮应为红色，复位按钮宜为绿色，试验按钮宜为白色，确认按钮宜为黑色。

10.2.7 报警灯光宜采用下列颜色：

1 越限报警或紧急状态为红色；

2 预报警或旁路状态为黄色；

3 设备运转或过程变量正常为绿色。

10.2.8 关键报警除了在操作站显示外，宜同时在辅助操作台上设置硬件报警灯显示。

10.3 仪表维护旁路开关

10.3.1 在测量仪表输入信号通道上宜设置仪表维护旁路开关。手动紧急停车输入信号不应设置仪表维护旁路开关。输出信号不应设置仪表维护旁路开关。

10.3.2 仪表维护旁路开关可在下列设备上以下列方式设置：

1 在安全仪表系统的工程师站设置软件开关；.

2 在机柜内设置硬件开关；

3 在辅助操作台设置硬件开关。

10.3.3 仪表维护旁路开关采用软件开关或在机柜内设硬件开关方式时，每个安全联锁单元或工艺区域宜在操作室辅助操作台上设置硬件“允许旁路”开关作为软件开关或机柜内硬件开关生效的“允许”条件。

10.3.4 对仪表维护旁路、允许旁路的操作应进行报警和记录。宜设计旁路限时，超过设定的旁路时间报警。

10.4 操作旁路开关

10.4.1 当工艺过程变量或设备状态从初始值到正常值一直处于联锁设定值范围内，不旁路不能建立正常工艺条件时，应设置操作旁路开关。

10.4.2 在操作旁路状态，联锁输入信号应正常显示、报警。

10.4.3 输出信号不应设置操作旁路。

10.4.4 紧急停车命令和功能不应设置操作旁路。

10.4.5 操作旁路开关可在下列设备上以下列方式设置：

1 在安全仪表系统操作员站设置软件开关；

2 在基本过程控制系统操作员站设置软件开关；

3 在辅助操作台设置硬件开关。

10.4.6 对操作旁路操作应进行报警和记录。

10.5 联锁复位按钮

10.5.1 安全仪表功能联锁逻辑应设置复位按钮。

10.5.2 复位按钮可按下列方式设置：

1 在安全仪表系统操作员站设置软件按钮；

2 在基本过程控制系统操作员站设置软件按钮；

3 在辅助操作台设置硬件按钮；

4 需要时在控制室和现场分别设置按钮，两处均复位操作后复位指令生效。

10.5.3 对复位操作应进行记录。

10.6 紧急停车按钮

10.6.1 安全仪表功能应根据工艺和安全需求设置紧急停车按钮。

10.6.2 紧急停车按钮宜按下列方式设置：

1 在辅助操作台设置硬件按钮；

2 需要时在辅助操作台和现场均设置硬件按钮，在一处停车操作后即停车指令生效。

10.6.3 硬件紧急停车按钮应配防护罩。

10.6.4 紧急停车按钮信号和功能不应被旁路。

10.6.5 对紧急停车操作应作报警和记录。

10.7 工程师站及事件顺序记录站

10.7.1 采用可编程电子系统的安全仪表系统应设工程师站，用于安全仪表系统组态、系统诊断、系统变更、系统更新、系统维护等。

10.7.2 工程师站应能显示操作站的内容。

10.7.3 工程师站应设不同级别的访问权限及保护密码。

10.7.4 安全仪表系统应设事件顺序记录站。事件顺序记录站可单独设置，也可与工程师站共用。

10.7.5 事件顺序记录站应记录每个事件的时间、日期、标识、状态等。事件顺序记录站应设密码保护。

10.7.6 工程师站和事件顺序记录站宜采用位置固定的台式计算机。

10.7.7 工程师站及事件顺序记录站失效应不影响安全仪表功能。

10.7.8 工程师站及事件顺序记录站可配置打印机。

11 应用程序

11.1 基本要求

11.1.1 应用程序的逻辑功能应采用布尔逻辑及布尔代数运算规则。

11.1.2 应用程序的组态宜采用功能逻辑图或布尔逻辑表达式。

11.1.3 应用程序的组态应使用安全仪表系统制造厂的标准组态工具软件。

11.1.4 应用程序组态工具软件应具有下列功能：

1 应用程序版本管理；

2 应用程序正确性检查；

3 标准功能块及其符号说明；

4 应用程序的编辑、编译、下装及运行管理；

5 应用程序的离线仿真测试；

6 组态管理。

11.2 应用程序的安全性

11.2.1 应用程序的设计、编程、组态、测试、集成、确认、运行维护及变更等应符合安全仪表系统安全技术要求、工程设计文件要求，工作程序、规则、人力、管理等应符合安全手册的要求。

11.2.2 应用程序应进行离线和在线测试，确认其功能满足既定要求后再投入运行。

11.2.3 应用程序宜采用光盘或磁介质进行复制和备份，电子版文件的复制应防止病毒侵入。

11.2.4 应用程序应同时进行本地备份和异地备份。

11.3 应用程序设计和组态

11.3.1 应用程序设计文件应包括下列内容：

1 应用程序说明；

2 输入点、输出点、通信点清单；

3 功能逻辑图；

4 其它要求。

11.3.2 逻辑设计应具有可读性，复杂功能逻辑图应有相应的逻辑功能说明。

11.3.3 应用程序组态应与安全仪表系统安全技术要求、功能逻辑图、因果表等要求一致。程序执行顺序及时间应符合过程安全的要求。

11.3.4 应用程序组态宜使用标准功能块。标准功能块应为经功能测试正确的逻辑功能块。

11.3.5 应用程序组态文件应包括功能逻辑图、用户手册、使用说明等。

11.3.6 采用逻辑语言的软件组态文件还应包括源程序、程序说明等。

12 供电、接地、防雷与配线

12.0.1 安全仪表系统供电设计应符合现行行业标准《仪表供电设计规范》HG/T 20509。安全仪表系统的交流供电宜采用两路独立的 UPS 电源供电。

12.0.2 安全仪表系统接地设计应符合现行行业标准《仪表系统接地设计规范》HG/T 20513。安全仪表系统应与基本过程控制系统共用接地网。

12.0.3 安全仪表系统应根据安全技术要求和雷电风险控制要求进行防雷工程设计。防雷设计宜符合现行行业标准《石油化工仪表防雷工程设计规范》SH/T 3164。

12.0.4 安全仪表系统配管配线设计应符合现行行业标准《仪表配管配线设计规范》HG/T 20512。安全仪表系统可与基本过程控制系统共用汇线槽、电缆沟，不宜共用接线箱，不宜共用穿线管。

13 工程设计

13.1 基础工程设计

13.1.1 安全仪表系统基础工程设计应根据工艺要求、工况条件、环境条件和安全仪表系统安全技术要求编制。设计文件宜包括下列内容：

1 安全联锁因果表，复杂联锁说明；

2 逻辑控制器技术规格书；

3 测量仪表、最终元件、关联仪表选型原则及仪表数据表；

4 安全仪表系统配置图。

13.1.2 逻辑控制器技术规格书宜包括下列内容：

1 基本要求；

2 选型原则；

3 控制器；

4 操作员站；

5 辅助操作台；

6 工程师站和事件顺序记录站；

7 应用程序组态；

8 通信；

9 负荷；

10 维护；

11 供电及接地；

12 验收测试；

13 运行环境；

14 储运条件；

15 技术服务；

16 质量保证；

17 文档资料。

13.1.3 测量仪表、最终元件、关联仪表的数据表宜包括下列内容：

1 工艺条件；

2　环境条件；

3　仪表规格；

4　安全完整性；

5　检验测试间隔。

13.2 详细工程设计

13.2.1　安全仪表系统详细工程设计文件应根据安全仪表系统安全技术要求、基础工程设计文件及工艺要求编制。设计文件宜包括下列内容：

1　逻辑控制器技术规格书；

2　安全仪表系统配置图；

3　联锁逻辑图或因果表，复杂联锁说明；

4　输入、输出点清单；

5　联锁及报警设定值表；

6　应用程序需要的技术资料；

7　测量仪表、最终元件、关联仪表的仪表规格书；

8　操作员站、辅助操作台及机柜布置图；

9　输入、输出卡件及端子布置图、接线图；

10　供电及接地系统图；

11　远程控制器或远程输入、输出卡件及端子布置、接线图；

12　回路接线图或接线表；

13　系统网络通信电缆、光缆连接表。

13.2.2　逻辑控制器技术规格书宜包括下列内容：

1　系统技术规格；

2　硬件配置基本要求；

3　软件配置基本要求；

4　备品备件及辅助工具；

5　应用程序组态、生成、调试；

6　工厂验收；

7　现场验收；

8　运行、维护培训；

9　现场服务；

10　保证期；

11　其他技术要求。

12　输入、输出汇总表；

13　硬件设备汇总表。

13.2.3　安全仪表系统测量仪表、最终元件、关联仪表的技术规格书宜包括下列内容：

1　工艺条件；

2　环境条件；

3　仪表规格；

4　安全完整性；

5　检验测试间隔；

6　其他技术要求。

14 集成、组态、调试、验收、联调与确认

14.1 集成、组态、调试

14.1.1 逻辑控制器、工程师站、操作员站、事件顺序记录站、辅助操作台、控制机柜、端子柜、安全栅柜、电涌保护器柜、继电器柜、电源柜、网络机柜等集成应符合安全仪表系统安全技术要求和详细工程设计文件的要求。

14.1.2 集成商宜进行功能设计。功能设计宜包括下列内容：

1 安全仪表系统网络结构设计，包括网络分层、分域设计；

2 安全仪表系统设备编号设计，包括人机接口设备编号，机柜编号，卡件编号，通道编号，线缆编号等；

3 安全仪表系统设备布置设计，包括机柜分柜原则，机柜内布置，卡件布置，通道分配等；

4 安全仪表系统配线设计，包括机柜间配线，机柜内配线等；

5 安全仪表系统供电设计，包括机柜外供电系统，机柜内仪表设备供电等；

6 安全仪表系统接地设计，包括接地原则，机柜内仪表设备接地，机柜外接地界面。

7 安全仪表系统组态设计，包括组态原则，逻辑符号，逻辑约定，流程画面，报警画面，仪表画面，颜色规定，文字格式等。

8 安全仪表系统报表设计，包括报警报表，SER 报表。

功能设计应经业主和工程设计单位审核、批准后执行。

14.1.3 应用程序编译、调试及下装应经过完整、详细地检查和测试。

14.1.4 硬件、软件集成后应按照详细工程设计文件、供货合同、功能设计对所有功能和要求进行检查、调试、测试。

14.1.5 安全仪表系统集成文件宜包括下列主要内容：

1 硬件规格书；

2 软件规格书；

3 硬件配置图；

4 机柜布置及接线图；

5 供电图；

6 接地图；

7 负荷计算表；

8 功耗计算表；

9 输入、输出卡件通道分配表；

10 组态文件（源程序、功能逻辑图等）；

11 运行维护手册。

14.2 验收

14.2.1 集成验收应包括工厂验收、现场验收、逻辑控制器与基本过程控制系统之间的联动验收。验收应对所有硬件和软件进行测试，测试结果应满足相关相求。

14.2.2 工厂验收测试应在集成工厂进行。宜包括下列内容：

1 测试内容、测试程序确定；

2 测试用标准仪器检查；

3 集成文件检查；

4 硬件测试及检查；

5 冗余和容错功能检验；

6 在线可维护性测试，包括在线更换卡件、在线修改及下装软件；

7 应用程序的逻辑功能测试；

8 测试完成，测试报告签字。

14.2.3 现场验收测试应在应用控制室进行。宜包括下列内容：

1 测试内容、测试程序确定；

2 集成文件及有关资料检查；

3 安装、接线检查；

4 冗余功能、在线更换卡件功能测试；

5 操作员站画面测试；

6 工程师站及事件顺序记录站功能测试；

7 辅助操作台按钮、开关、报警灯功能测试；

8 网络功能测试；

9 诊断功能测试；

10 测试完成，测试报告签字。

14.2.4 逻辑控制器与基本过程控制系统之间的联动验收测试，可在逻辑控制器集成工厂、基本过程控制系统集成工厂、现场应用控制室进行。验收测试宜包括下列内容：

1 双向通信测试；

2 联动画面测试；

3 联动功能测试；

4 测试完成，测试报告签字。

14.3 联调

14.3.1 测量仪表、逻辑控制器、最终元件、管道、线路、供电、供气、接地等施工完毕后，应按照详细工程设计文件对测量仪表、逻辑控制器、最终元件和关联仪表进行联合调试。

14.3.2 联调宜包括下列内容：

1 测量仪表输出值与操作站、工程师站指示值一致；

2 逻辑控制器输出值与最终元件动作一致；

3 联锁输入、联锁动作、动作循序与工程设计联锁逻辑要求一致。

14.3.3 联调内容、结果应进行记录、归档。

14.4 确认

14.4.1 安全仪表系统投入使用前应进行确认。

14.4.2 安全仪表系统的确认宜包括下列内容：

1 测量仪表、逻辑控制器、最终元件等的设置、安装等符合安全仪表系统安全技术要求、工程设计文件和安全手册；

2 供电、接地、供气、保温伴热、隔离吹洗、配管配线等符合工程设计文件；

3 逻辑控制器验收测试发现的问题已经整改完毕；

4 安全仪表系统联调发现的问题已经整改完毕；

5 安全仪表系统与基本过程控制系统通信和功能测试结果符合工程设计要求；

6 安全仪表功能安全完整性验证结果符合安全技术要求；

7 安全仪表系统相关技术文件完整；

8 确认内容应记录归档。

15 维护、维修和变更管理

15.0.1 维护、维修应根据安全技术要求、工程设计文件、安全手册，制定安全仪表系统运行维护内容、维护程序、维修程序、检验测试计划、作业章程。应编制维护、维修、检验测试记录或报告。

15.0.2 变更管理应制定变更管理程序，包括提出变更原因，提出变更方案，审核变更方案，评估需要变更的安全仪表功能及其安全完整性等级，变更方案的工程设计与实施，变更的联锁逻辑功能测试与确认，变更文件的归档，运行维护内容的更新等。

16 文档管理

16.0.1 安全仪表系统安全生命周期各阶段文档的电子版和/或纸质版应异地存档保存。文档应包括工程设计文件，集成、组态文件，验收测试文件，单校、联调文件，确认文件，维护、维修文件，变更文件等。

16.0.2 文档管理应包括文件命名规则、文件格式、文件传递方式、文件控制程序、文件审核流程及文件版本管理等。

本规范用词说明

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：

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：

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：

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，采用“可”。

2　条文中指明应按其它有关标准执行的写法为：“应符合……的规定”或“应按……执行”。

引用标准目录

《电气/电子/可编程电子安全相关系统的功能安全 第 1 部分：一般要求》GB/T 20438.1/IEC 61508-1

《电气/电子/可编程电子安全相关系统的功能安全 第 2 部分：电气/电子/可编程电子安全相关系统的要求》GB/T 20438.2/IEC 61508-2

《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/IEC 61508-3

《电气/电子/可编程电子安全相关系统的功能安全 第 4 部分：定义和缩略语》GB/T 20438.4/IEC 61508-4

《电气/电子/可编程电子安全相关系统的功能安全 第 5 部分：确定安全完整性等级的方法示例》GB/T 20438.5/IEC 61508-5

《电气/电子/可编程电子安全相关系统的功能安全 第 6 部分：GB/T 20438.2 和 GB/T 20438.3 的应用指南》GB/T 20438.6/IEC 61508-6

《电气/电子/可编程电子安全相关系统的功能安全 第 7 部分：技术和措施概述》GB/T 20438.7/IEC 61508-7

《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、硬件和应用程序要求》GB/T 21109.1/IEC 61511-1

《过程工业领域安全仪表系统的功能安全 第 2 部分：GB/T 21109.1 的应用指南》GB/T 21109.2/IEC 61511-2

《过程工业领域安全仪表系统的功能安全 第 3 部分：确定要求的安全完整性等级的指南》GB/T 21109.3/IEC 61511-3

《电气电子可编程电子安全相关系统的功能安全 功能安全概念及 GB / T 20438 系列概况》GB/Z 29638/ IEC/TR 61508-0

《自动化仪表选型设计规范》HG/T20507

《仪表供电设计规范》HG/T 20509

《仪表配管配线设计规范》HG/T 20512

《仪表系统接地设计规范》HG/T 20513

《石油化工仪表防雷工程设计规范》SH/T 3164

中华人民共和国化工行业标准

化工安全仪表系统工程设计规范

Engineering design code for safety instrumented system in chemical industry

HG/T 22820-202x

条文说明

Explanation of Provisions

制订说明

《化工安全仪表系统工程设计规范》HG/T22820—202x，经工业和信息化部xx年x月x日以第xx号公告批准发布。

本规范制订过程中，编制组进行了广泛调查研究，总结了我国化工厂或装置采用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，广泛征求了化工安全仪表系统工程设计、制造、操作维护等方面技术人员的意见，在此基础上编制了本规范。

为了便于化工安全仪表系统设计、建设和操作维护等有关人员在使用本规范时能正确理解和执行条文规定，《化工安全仪表系统工程设计规范》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、依据以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标准规定的参考。

HG/T 22820-202X 首次发布。

目　次

2 术语与缩略语

2.1 术语

2.1.5 保护层 protection layer

化工厂或装置典型多保护层结构如图 1 所示：

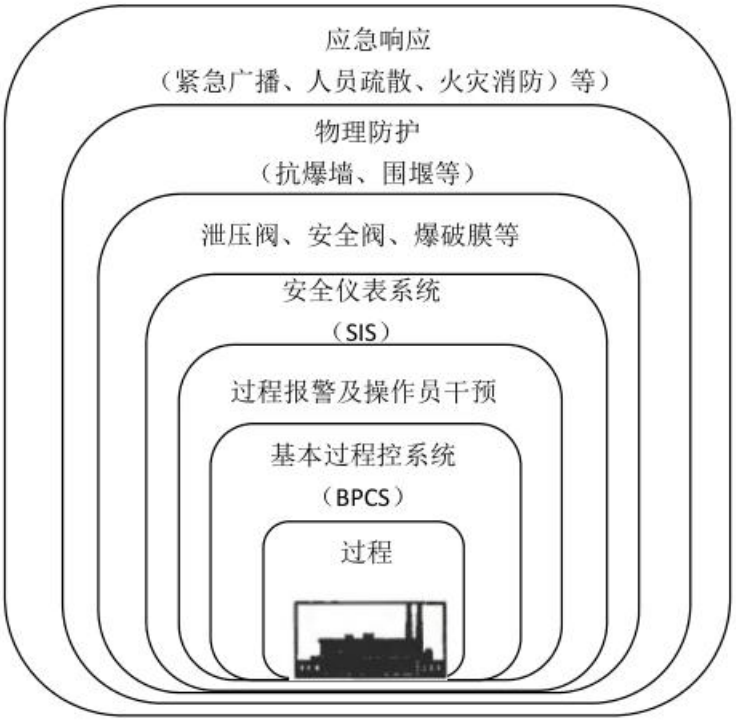

图 1 化工厂或装置的典型多保护层结构

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

基本过程控制系统用于生产过程的连续测量、常规控制（如连续、顺序、间歇控制等）、操作管理，保证生产装置的平稳运行。在化工厂或装置中，基本过程控制系统通常采用分散控制系统（DCS）。基本过程控制系统不应执行 SIL 1、SIL 2、SIL 3 的安全仪表功能。

3 基本要求

3.1 安全生命周期

3.1.1 安全仪表系统的安全生命周期是安全仪表系统安全功能存在的全过程。引用安全生命周期的目的是为了确定实现功能安全目标所必要的活动，并进行策划与组织安排，以便在设计、集成调试以及运行维护各阶段内有效实施，确保安全仪表系统满足功能安全的要求。

3.1.2 安全仪表系统的安全生命周期包括从工程方案设计到运行维护，直至停用的全过程，涉及工程设计和安全仪表系统集成、建设、确认、运行等多方面的工作。本规范重点说明安全仪表系统工程设计，简要说明相关的系统集成、运行维护等方面的要求。

3.1.3 安全完整性验证贯穿于安全仪表系统安全生命周期各阶段，涵盖安全仪表系统各组成部分。可采用分段验证方式，如设计验证和最终验证，也可采用最终验证一段验证方式。设计验证是指在设计初期根据经验数据对安全仪表功能进行验证，指导安全仪表回路的构建和设计。最终验证是指采用安全仪表系统的实际可靠性数据对安全仪表回路进行验证。

对于经验证不符合目标安全完整性要求的安全仪表功能，应提出整改措施，达到目标安全完整性要求。可通过选择硬件危险失效率低的设备、改变冗余结构形式、提高设备的诊断覆盖率、调整设备检验测试间隔等措施提高安全完整性等级。

化工厂和装置的安全仪表系统通常工作于低要求模式，失效率验证采用危险失效平均概率验证。在连续模式或高要求模式时，失效率验证采用每小时危险失效平均频率验证。安全完整性等级验证内容宜包括系统性能力。

若企业对连续稳定生产、尽可能减少误停车有要求，且安全仪表功能的误动作造成的损失（如经济损失、声誉损失等）大于可容忍程度时，可通过计算误停车率（STR）验证是否满足可用性要求。

对于经验证不符合可用性要求的安全仪表功能，应提出整改措施，可选择硬件安全失效率低的设备、采用可用性冗余配置或兼顾安全性与可用性的冗余配置等。提高安全仪表功能的可用性时，应满足目标安全完整性等级要求。

3.1.7 工程方案设计是指在工程前期开展的设计工作，可包括可行性研究、工艺包设计、基础设计前期等。工程方案设计应根据工艺技术的特点、生产操作方式、运行维护方式、以往经验等，对工艺过程中可能发生的危险和风险进行初步分析，提出需采取的安全措施和保护系统。

3.1.8 过程危险分析和风险评估的详细内容及方法不属于本规范的内容。过程危险是因异常事件引起过程条件变化产生的危险，包括由于过程、基本过程控制系统和相关人员因素等引发的特定危险事件。风险评估是分析特定危险事件可能发生的频率和后果的严重程度，确定工程的可承受风险。化工厂或装置的过程危险分析和风险评估通常采用危险和可操作性研究（HAZOP）方法，也可采用安全检查表、故障模式和影响分析、因果分析等方法。

3.1.9 安全功能是针对特定的危险事件，为达到或保持过程的安全状态，由安全仪表系统、其他安全相关系统或外部风险降低设施实现的功能。一个安全功能应能防止一个特定的危险事件。安全功能可采用安全仪表系统和其他的保护层来实现。在化工厂或装置中通常采用多个保护层，当某一个保护层失效时不会产生或导致严重后果。

分配安全功能是给各相关的保护层进行安全功能分配，不仅仅是给安全仪表系统。

3.1.11 安全仪表系统的安全技术要求是安全仪表系统工程设计的基础性依据，因此应为安全仪表系统安全生命周期的重要环节。安全要求规格书（SRS）是描述安全仪表系统安全技术要求的一种表现形式。安全要求规格书的编制应依据前面分析、评估、分配、定级结果，明确为实现功能安全对安全仪表系统的硬件、软件、工程、管理、运行维护等相关要素的要求。安全要求规格书提出的功能安全要求应清晰明确、可验证、可维护、可操作，以便安全仪表系统安全生命周期各阶段的使用者理解和执行。

安全要求规格书的主要内容包括安全仪表功能的说明、安全仪表功能的安全完整性等级和运行模式、输入输出设备清单、共因失效要求、过程安全状态、过程安全时间、响应时间、单个或多个危险事件发生时可能造成的风险、联锁设定值、检验测试间隔、检验测试实施、测量仪表类型及精度、控制阀泄漏等级、输入与输出功能关系、手动停车要求、得/失电联锁、复位、旁路、误停车率（若需要）、不同工艺操作模式的要求、关联动作、通信接口、极端环境或重大事故时的要求、应用程序的安全要求等。

3.1.15 安全仪表系统安全手册包括逻辑控制器的安全手册、关联设备的安全手册、测量仪表和最终元件的安全手册。

3.1.16 用户应制定变更管理程序，保证安全仪表系统发生改变时符合安全完整性相关要求。变更记录应包括变更内容描述、变更原因、变更活动对安全仪表系统的影响分析、变更的批准、变更验证结果、变更时间、相关文件等。

3.2 安全完整性

3.2.2 SIL 等级越高，失效的概率或频率越低。

3.2.3 通常化工厂和装置的安全仪表系统工作于低要求模式。

风险降低因子（RRF）与要求时危险失效平均概率（PFDavg）互为倒数，代表目标风险降低倍数。

在要求时危险失效平均概率介于 10^{-1} 和 1 之间时，联锁保护功能可由基本过程控制系统实现，也可由安全仪表系统实现。

3.2.5 安全仪表功能的硬件失效率计算举例：

某安全仪表功能为低要求模式，该安全仪表功能的硬件危险失效平均概率计算如下：

$$\Sigma PFD_{功能}=\Sigma PFD_{测量}+\Sigma PFD_{逻辑}+\Sigma PFD_{最终}$$

其中：

$\Sigma PFD_{功能}$：安全功能危险失效平均概率。

$\Sigma PFD_{测量}$：测量仪表危险失效平均概率。计算范围包括测量仪表和测量仪表信号回路上的关联仪表。

$\Sigma PFD_{逻辑}$：逻辑控制器危险失效平均概率。

$\Sigma PFD_{最终}$：最终元件危险失效平均概率。计算范围包括最终元件和最终元件控制信号回路上的关联仪表。

3.2.9 SC 等级越高，系统性能力越高。

3.2.10 SIF 的安全完整性等级 SIL N 应为硬件安全完整性 SIL X（X=1~4）和系统性能力 SC Y（Y=1~4）的较小值，即 N=min（X，Y）。

4 设计原则

4.0.3 化工厂或装置的安全仪表功能安全完整性等级最高为 SIL3 级。如果在确定安全仪表功能安全完整性等级时高于 SIL3 级，应重新分配保护层的安全功能，或采用多个独立的安全仪表功能，使安全完整性等级不高于 SIL3。为分散风险，许多企业规定安全完整性等级最高为 SIL3 级，不宜高于 SIL2 级。

4.0.4 考虑到检测和控制的滞后、工艺过程的滞后，安全仪表功能的响应时间应留有安全富裕量。有企业和组织建议安全仪表功能的响应时间不应超过过程安全时间的 50%。

4.0.6 安全仪表系统应能够不依赖于基本过程控制系统独立完成安全仪表功能，基本过程控制系统的失效不应影响安全仪表系统执行安全功能，不应降低安全仪表功能的安全完整性等级。

4.0.7 安全仪表系统对共用设备具有优先权是指共用设备优先执行安全仪表功能。

4.0.9 故障安全型可实现当安全仪表系统或子系统发生故障时，安全仪表系统能按设计预定方式，将过程转入安全状态。工程设计应严格遵守故障安全型的基本设计原则。

一个安全仪表功能由多个环节组成，而这些环节的功能安全方式之间可能存在矛盾，此时，安全性应从整体安全考虑，故障安全型应是整体更安全，应以整体安全利益最大化为原则进行处理。

案例 1：高压电机的联锁停机，宜采用触点闭合停机这种非故障安全型联锁方式，更有利于电气控制设备断电停机，而不宜采用触点断开停机的故障安全型联锁方式。

案例 2：变送器故障报警信号处理，宜根据测量仪表子系统结构、变送器故障影响后果评估确定处理方案，在满足安全需求的前提下，减少不必要的联锁停车带来的损失，而不宜直接采用故障报警信号触发联锁保护的故障安全型方案，例如，对于同一参数二取二、三取二类可用性冗余配置的测量仪表子系统结构，变送器故障信号可直接作为联锁保护触发信号；对于一取一、二取一类可靠性冗余配置的测量仪表子系统结构，应根据变送器故障影响后果评估，对变送器故障信号选择采用高级别报警方案，或采用作为联锁保护触发信号。

4.0.13 对于故障安全型安全仪表系统，UPS 用于保证可用性。

4.0.14 安全仪表系统的逻辑控制器、工程师站、操作站等设备，可采用逻辑控制器的时钟作为时钟源，使安全仪表系统内设备的时钟一致。

安全仪表系统与基本过程控制系统的时钟同步便于事故后原因分析。时钟同步措施可采用同

一时钟源，或采用基本过程控制系统的时钟信号。时钟同步措施需与控制系统信息安全防护要求相结合。

4.0.15 工艺装置间安全仪表系统逻辑控制器的独立性应根据生产风险控制需求、信息安全防护需求、装置开停工计划需求、系统检维修管理需求、控制点数量等因素决定。

4.0.17 逻辑控制器检验测试间隔一般容易实现与工艺装置停工检修间隔相同，测量仪表和控制阀检验测试间隔常常会小于工艺装置停车检修间隔。

当仪表设备检验测试间隔小于工艺装置停工检修间隔时，可选择如下检验测试措施：

1 检验测试在工艺设施允许的时段内进行。例如，当油品储罐处于备用时段时，对高高液位安全联锁保护功能暂时没有需求，此时段允许对作为终端元件的罐根切断阀进行检验测试；

2 选择检验测试间隔更长的仪表设备；

3 提高仪表设备故障诊断水平；

4 仪表设备采取可用性冗余配置；

5 设计仪表设备硬件旁路和/或软件旁路；

6 控制阀配置部分行程或全行程测试功能（PST 或 FST）。

仪表设备检验测试应在执行相应管理措施和相应应急措施的情况下进行。

5　系统组成

5.0.9 安全仪表系统网络典型结构如图 2 和图 3 所示。

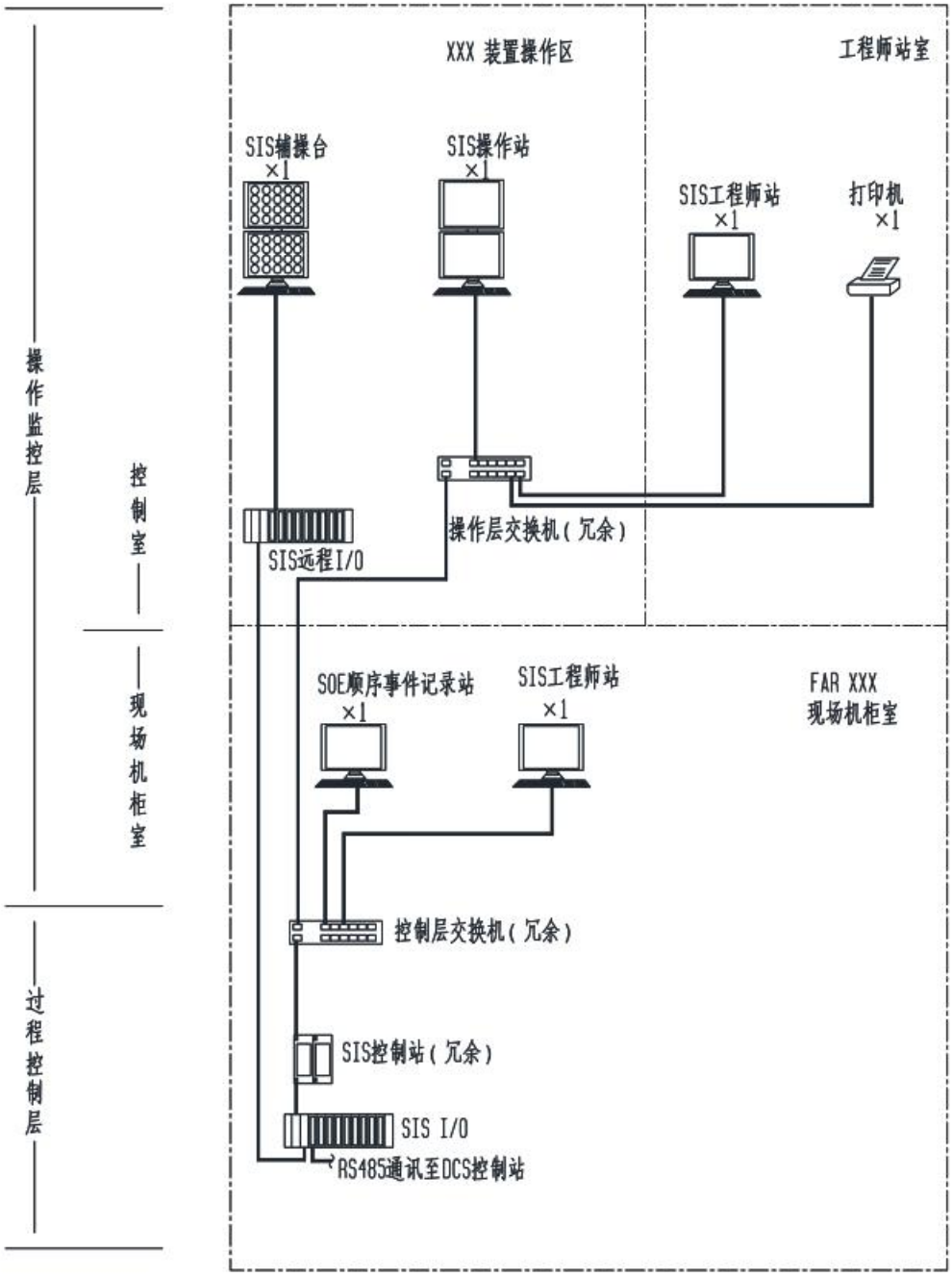

图 2　工艺装置安全仪表系统网络典型结构图

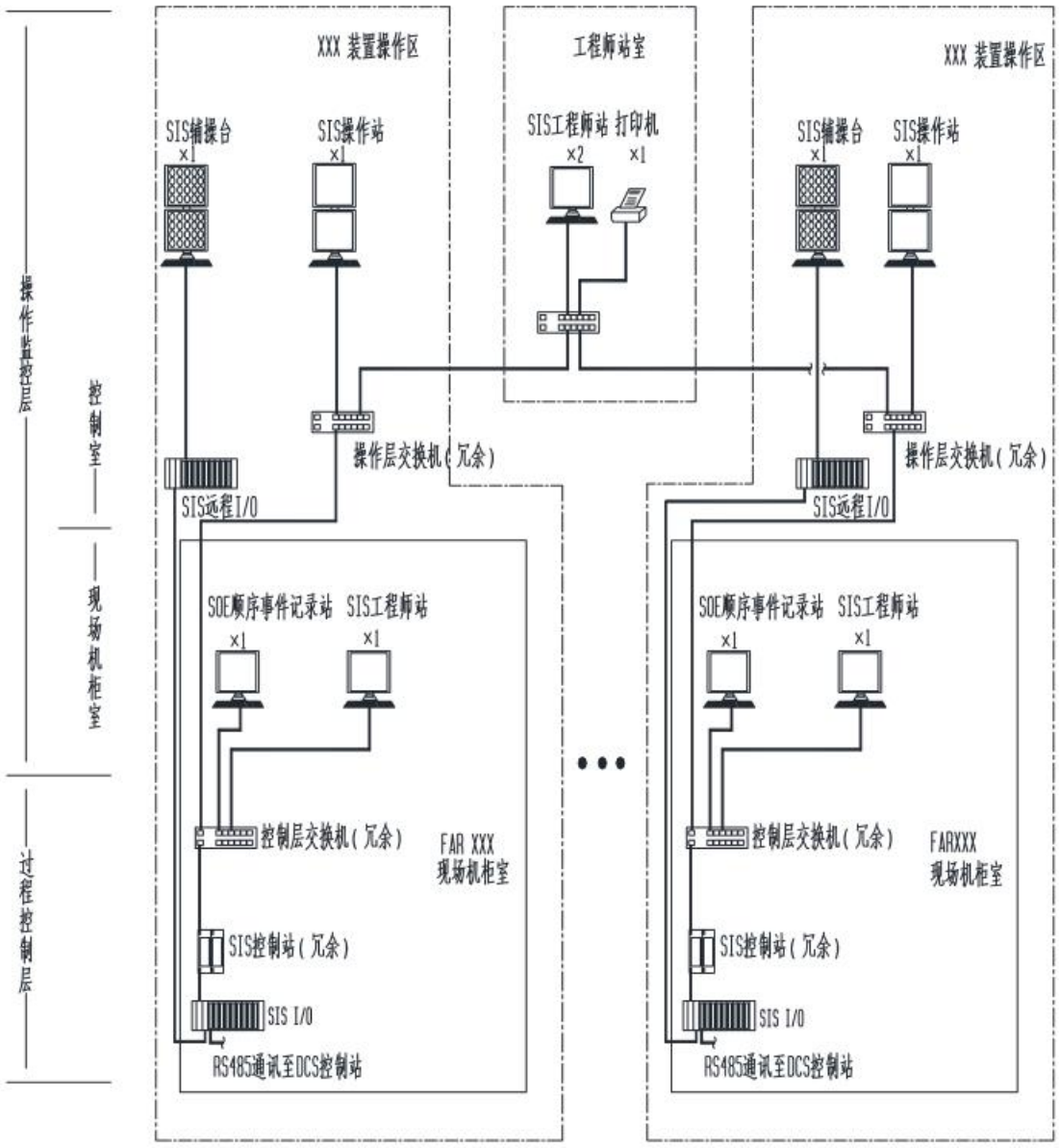

图 3　化工厂安全仪表系统网络典型结构图

6 测量仪表

6.1 基本规定

6.1.2 在满足安全可靠性的前提下满足可用性。

6.1.3 开关量测量仪表因为长期不动作容易造成触点粘合或接触不良，可能导致不动作或误动作，影响安全仪表功能实现。因此，安全仪表系统不宜采用开关量测量仪表。

目前，通信信号、无线信号还易受内外因素影响导致通信中断或信号错误，若作为联锁保护输入信号尚不能满足可靠性、可用性的需求。因此，目前安全仪表系统测量仪表信号不应采用通信信号、无线信号，如：FF、PROFIBUS-PA、MODBUS RTU、TCP/IP 等通信协议的通信信号。

6.1.4 安全仪表系统测量信号回路上的关联仪表，其性能应满足安全仪表系统对测量仪表的相关要求，输出信号宜采用模拟信号，也可采用开关量信号；不应采用现场总线信号或其它通信协议信号；不应采用无线信号。关联仪表宜采用具有故障自诊断功能的智能仪表。

6.2 独立性设计

6.2.2~6.2.4 应慎重选择安全仪表系统与基本过程控制系统共用单一测量仪表的方案，因为单一测量仪表的失效可能产生危险情况。只有测量仪表危险失效率降到足够低，且安全仪表系统能够在要求的时间内把过程置于预定的安全状态时，安全仪表系统与基本过程控制系统才能共用单一测量仪表。对 SIL2、SIL3 的 SIF 来说，安全仪表系统通常需要独立设置且冗余配置的测量仪表来满足硬件故障裕度要求和要求的安全完整性。

节流装置作为流量测量元件时可以共用。

独立设置的安全仪表系统测量仪表，可通过隔离器或保证基本过程控制系统失效不会导致安全仪表系统产生危险失效的手段，将信号传送到基本过程控制系统，在基本过程控制系统中进行测量信号比较，以提高诊断水平；或进行适当算法（如“三取中”），通过降低安全仪表系统的要求率来提高安全性。

安全仪表系统与基本过程控制系统共用测量仪表时测量仪表宜由安全仪表系统供电。

6.2.5 为防止共因失效，安全仪表系统与基本过程控制系统测量仪表取源点宜分开设置。除非经评估，被测工况、仪表结构难以使取源点或取源部件失效，风险在容许范围内，可以共用取源点。

6.2.6 为防止共因失效，安全仪表系统冗余的测量仪表之间的取源点宜分开。除非经评估，

被测工况难以使取源点失效或取源部件失效，失效风险在容许范围内，可以共用取源点。

6.2.7 为防止共因失效，安全仪表系统与基本过程控制系统测量仪表的测量管路应分开设置。两者共用取源点时，一次取压阀及至变送器间的测量管路应分开设置。

当安全仪表系统与基本过程控制系统的测量仪表安装在同一仪表连通管上时，连通管与工艺设备间不宜设置切断阀，或对切断阀采取加铅封等管控措施，防止误关；工况条件或通过增加措施应保证连通管畅通，测量液位时连通管内与设备内介质应均质，以保证不产生不可接受的附加测量误差。

6.2.8 为防止共因失效，安全仪表系统冗余的测量仪表之间测量管路应分开设置。共用取源点时，一次取压阀及至变送器间的测量管路应分开设置。

当冗余的测量仪表安装在同一仪表连通管上时，连通管与工艺设备间不宜设置切断阀，或对切断阀采取加铅封等管控措施，防止误关；工况条件或通过增加措施应保证连通管畅通，测量液位时连通管内与设备内介质应均质，以保证不产生不可接受的附加测量误差。

6.3 冗余设计

6.3.2 测量仪表的安全性冗余设计可参考如下策略：

1 SIL 1 级安全仪表功能可采用单一测量仪表。

2 SIL 2 级安全仪表功能宜采用冗余测量仪表。

3 SIL 3 级安全仪表功能应采用冗余测量仪表。

安全性冗余结构案例见表 1：

表 1 安全性冗余结构案例

安全完整性等级	安全性冗余结构	备 注
SIL 1	一取一	
SIL 2	二取一	
SIL 3	二取一	
	三取一	

6.3.3 可用性冗余结构案例见表 2：

表 2　可用性冗余结构案例

安全完整性等级	可用性冗余结构	备注
SIL 1	二取二	
SIL 2	二取二	
SIL 3	二取二	
	三取三	

可用性冗余结构会降低安全性。采用可用性冗余结构时应计算、验证其安全性，冗余结构应满足安全完整性等级要求。

7 最终元件

7.1 基本规定

7.1.3 控制阀通常为两位式开关阀，也可以是配置了电磁阀等控制附件的调节阀，电磁阀等控制附件由安全仪表系统直接驱动，安全仪表系统对控制阀具有优先控制权。

7.1.4 气动控制阀宜采用弹簧复位式单作用气动执行机构。气动控制阀采用双气缸双作用执行机构时，宜配置空气储罐。应慎重选用电动控制阀，应对其电源的危险失效风险进行分析，根据分析结果采取安全措施，如提高电源规格，设置电源故障报警，采用耐火保护措施等。电动控制阀不宜用于 SIL2、SIL3 需求的安全仪表功能。

故障安全型控制阀，当能源中断、控制信号中断时，控制阀使用蓄能机构自动达到预定的安全位置。常用蓄能机构：复位弹簧，空气储罐，蓄能器。

7.2 独立性设计

7.2.2~7.2.4 应慎重选择安全仪表系统与基本过程控制系统共用单一最终元件的方案，因为单一最终元件的失效可能产生危险情况。只有最终元件危险失效率降到足够低，且安全仪表系统能够在要求的时间内把过程置于预定的安全状态时，安全仪表系统与基本过程控制系统才能共用单一最终元件。

实际上，安全仪表系统与基本过程控制系统共用单一最终元件实现 SIL1 的安全功能也是很困难的，失效率需要足够低，需要保证安全仪表系统动作优先于基本过程控制系统，还宜设计因共用的最终元件检出故障、维护或检验测试而需要停止使用的时段内需采取的替代措施。因此，对于 SIL2、SIL3 的安全仪表功能需要独立设置最终元件。

当共用的最终元件为控制阀时，还需考虑如下要求：

•控制阀设计应保证基本过程控制系统失效不会导致控制阀无法执行安全仪表系统控制信号；

• 控制阀设计应兼容安全仪表系统和基本过程控制系统的需求；

• 应有控制阀在类似过程应用中可靠运行的经验；

• 应有保证控制阀安全完整性的操作、维护规程。

7.3 冗余设计

7.3.2 控制阀的安全性冗余设置可参考如下策略：

1 SIL 1 级安全仪表功能可采用单一控制阀。

2 SIL 2 级安全仪表功能宜采用冗余配置的控制阀。

冗余方式：

a 可采用两台独立设置的安全仪表系统控制阀；

b 可采用一台独立设置的安全仪表系统控制阀和共用一台基本过程控制系统的控制阀，但共用的控制阀设计应保证安全仪表功能的需求应被优先执行，并由安全仪表系统独立完成，且满足安全完整性等级要求。

3 SIL 3 级安全仪表功能应采用冗余配置的控制阀。

冗余方式：宜采用两台独立设置的安全仪表系统控制阀。

7.3.3 控制阀可用性冗余结构会降低其安全性。采用可用性冗余结构时应计算、验证其安全性，冗余结构应满足安全完整性等级要求。

7.4 控制阀附件的配置

7.4.1 气动执行机构的控制电磁阀安装位置示例见图 4 和图 5。电磁阀的安装位置和气路连接保证控制阀优先执行安全仪表功能，且由安全仪表系统独立完成。

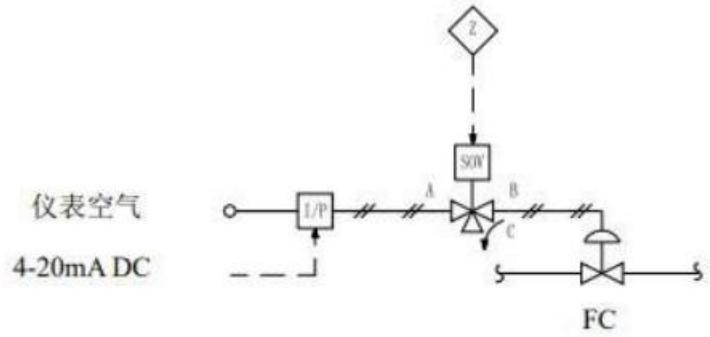

图 4 气动调节阀控制电磁阀安装位置示例

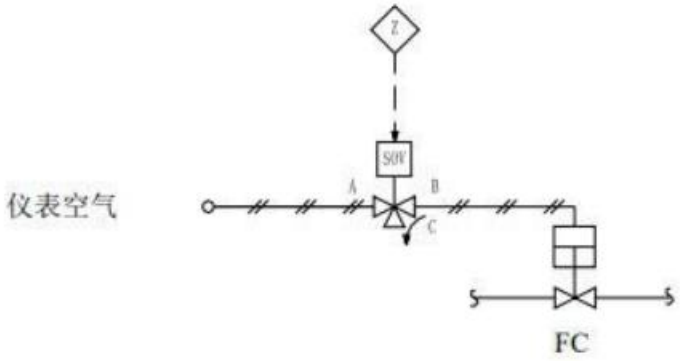

图 5　气动切断阀控制电磁阀安装位置示例

图 4 和图 5 中 SOV 为电磁阀。电磁阀通电励磁，A—B 通，控制阀打开；电磁阀断电非励磁，B—C 通，控制阀关闭。

7.4.2 气动执行机构的控制电磁阀应选用耐高温(H 级)绝缘线圈，适合长期带电。在工艺过程正常运行时电磁阀应带电励磁，要求联锁动作时断电非励磁。

7.4.4 气动执行机构的控制电磁阀安全性冗余结构配置示例如图 6、图 7 所示。

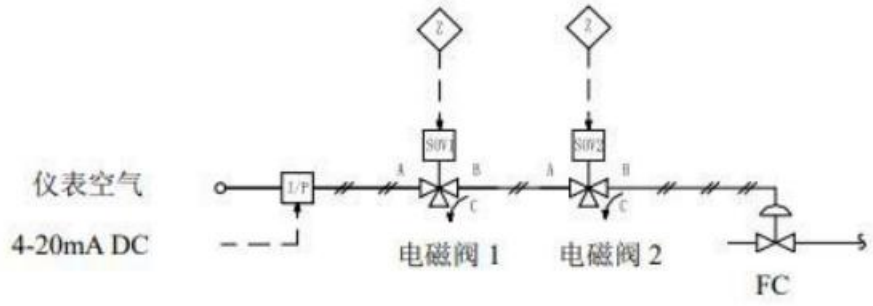

图 6　气动调节阀控制电磁阀安全性冗余结构配置示例

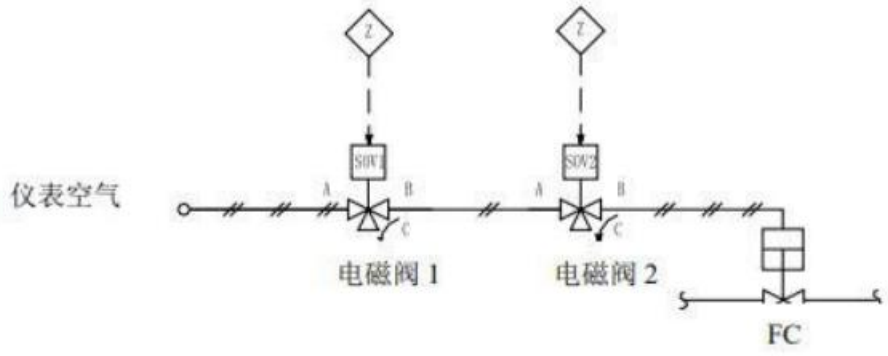

图 7　气动切断阀控制电磁阀安全性冗余结构配置示例

图 6 和图 7 中，当电磁阀 1 带电励磁其 A—B 则通，电磁阀 2 带电励磁其 A—B 则通，控制阀将打开。当电磁阀 1 带电励磁，其 A—B 则通，电磁阀 2 断电非励磁其 B—C 则通，控制阀将关闭。当电磁阀 1 断电非励磁，其 B—C 则通，电磁阀 2 带电励磁其 A—B 则通，控制阀将关闭。当电磁阀 1 断电非励磁其 B—C 则通，电磁阀 2 断电非励磁其 B—C 则通，控制阀将关闭。

气动执行机构的控制电磁阀可用性冗余结构配置示例如图 8、图 9 所示。

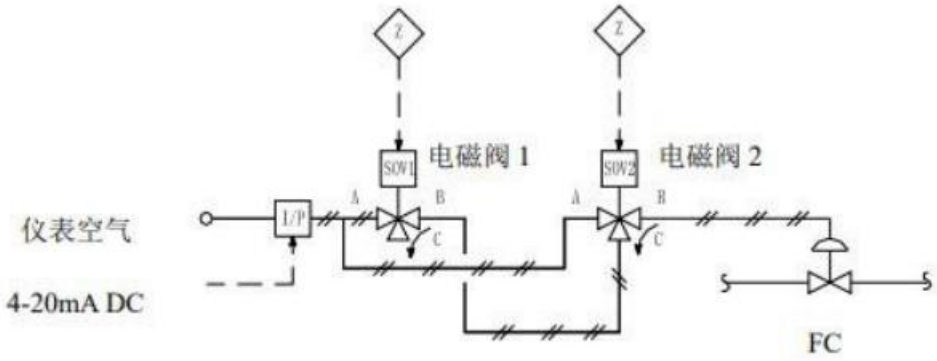

图 8　气动调节阀控制电磁阀可用性冗余结构配置示例

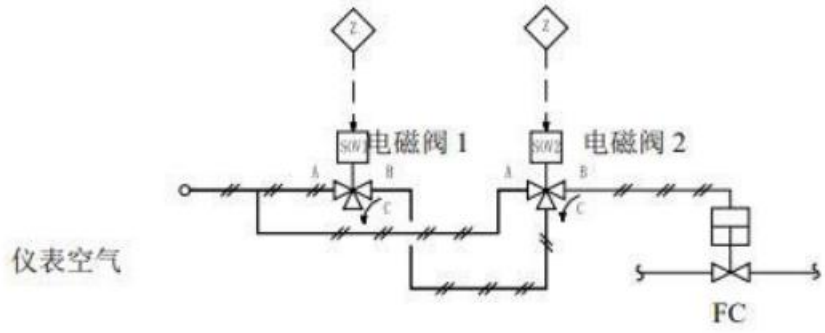

图 9　气动切断阀控制电磁阀可用性冗余结构配置示例

图 8 和图 9 中，当电磁阀 1 带电励磁其 A—B 则通，电磁阀 2 带电励磁其 A—B 则通，控制阀将打开。当电磁阀 1 带电励磁其 A—B 则通，电磁阀 2 断电非励磁其 B—C 则通，控制阀将打开。当电磁阀 1 断电非励磁其 B—C 则通，电磁阀 2 带电励磁其 A—B 则通，控制阀将打开。当电磁阀 1 断电非励磁其 B—C 则通，电磁阀 2 断电非励磁其 B—C 则通，控制阀将关闭。

电磁阀的可用性冗余结构会降低其安全性，应保证可用性冗余结构满足控制阀安全完整性等级要求。

7.4.6 阀位行程开关一般用于阀位在控制室的远程指示。该用途不属于安全仪表功能，阀位指示可在基本过程控制系统执行。阀门动作宜设置超时报警。

当阀位行程开关作为其它安全仪表功能的测量仪表时，阀位行程开关应满足安全仪表功能对测量仪表的相关要求。

7.4.7 控制阀部分行程测试的行程测试范围、测试方式、实施时机应得到工艺操作和管理人员的许可。

8 逻辑控制器

8.1 基本规定

8.1.1 继电器系统适用于输入输出点数较少、逻辑功能简单的场合。

8.1.6 安全仪表系统逻辑控制器冗余配置，以实现安全性、可用性和可维护性。采用可编程电子系统作为安全仪表系统逻辑控制器时，冗余方式可为中央处理单元、通信单元及电源单元等冗余配置，输入、输出单元采用冗余技术，应具备在线更换模件而不影响逻辑控制器正常运行的措施。

8.2 逻辑控制器输入、输出卡件配置

8.2.8 现场仪表与控制室内仪表不共电源、不共接地是常见的电气干扰引入案例。在控制室内仪表前端设置信号隔离器是消除干扰的有效措施。

安全仪表系统与电机控制系统间的联锁信号线路是常见的危害电压引入通道，容易因误操作等原因将 220V 电压引入 24V 的仪表回路，导致仪表或卡件损坏。在安全仪表系统与电机控制系统之间信号线路上设置隔离继电器是防止危害的有效措施。

9 网络和通信接口

9.1 基本规定

9.1.6 串行通信接口的数据量不应超过通信卡件的通信能力，通信速率应符合通信卡件的技术规格。安全仪表系统与基本过程控制系统的串行通信，基本过程控制系统应为主站，安全仪表系统应为从站。当安全仪表系统采用 MODBUS TCP/IP 通信方式接入基本过程控制系统网络交换机时，通信链路应设置工业防火墙等网络安全防护措施。

9.2 信息安全

9.2.5 安全仪表系统信息可通过基本过程控制系统传输至工厂信息网络。

10 人机接口

10.1 操作员站

10.1.1 操作员站应可设置多种报警显示、不同报警级别、不同报警音响，记录、存储报警状态和相关数据，调用、显示、分析报警数据。

10.1.3 多台操作员站间宜实现功能冗余。

10.2 辅助操作台

10.2.2 按工艺装置分别设置辅助操作台，便于快速、准确监控、操作。当合用一个操作台时，应在操作台面分区布置。

10.2.4 辅助操作台台面布置应易于辨识，便于操作。

10.2.5 辅助操作台上的按钮、开关、报警灯接入安全仪表系统输入、输出卡件的常见方式：

1 在现场控制室（LCR）内，操作间辅助操作台上的按钮、开关、报警灯采用硬接线接至机柜间安全仪表系统输入、输出卡件。

2 在中心控制室（CCR）内，操作间辅助操作台上的按钮、开关、报警灯采用硬接线接至机柜间安全仪表系统远程输入、输出卡件，远程输入、输出卡件宜经通信光纤接至现场机柜室（FAR）的安全仪表系统控制器。

10.2.8 相比操作站报警，硬件报警灯具有更清晰的警示作用。可通过风险评估选择需要在辅助操作台上显示的关键报警，例如：重要过程参数达到联锁值，联锁启动，安全仪表系统故障等。

10.3 仪表维护旁路开关

10.3.1 仪表维护旁路开关用于现场仪表和线路维护时旁路输入信号，使安全仪表系统逻辑控制器的输入信号处于正常状态。

对三取二（2OO3）冗余结构的测量仪表，可不设仪表维护旁路开关。

10.3.2 仪表维护旁路开关无安全功能要求，数量多，不适合设硬件开关。

10.3.3 仪表维护旁路会使安全功能失效，因此，仪表维护旁路操作必须在工艺操作人员已知晓、有准备、允许下才能进行、生效。当采用软件开关或机柜内硬件开关作为旁路开关时，工艺操作人员不易看清旁路状态，不利于安全生产。在辅助操作台设硬件允许旁路开关，由工艺操作员管理。只有当仪表维护旁路开关切换到旁路位置，且允许旁路开关切换到允许位

置时，方可实现旁路功能，以此保证安全生产。

根据风险情况和管控能力，宜对同时允许旁路的仪表数量进行限制。

典型的软件仪表维护旁路开关和硬件允许旁路开关设置示例如图 10 所示。

机柜内硬件仪表维护旁路开关和操作台硬件允许旁路开关设置方案与图 10 类似，不再重复。

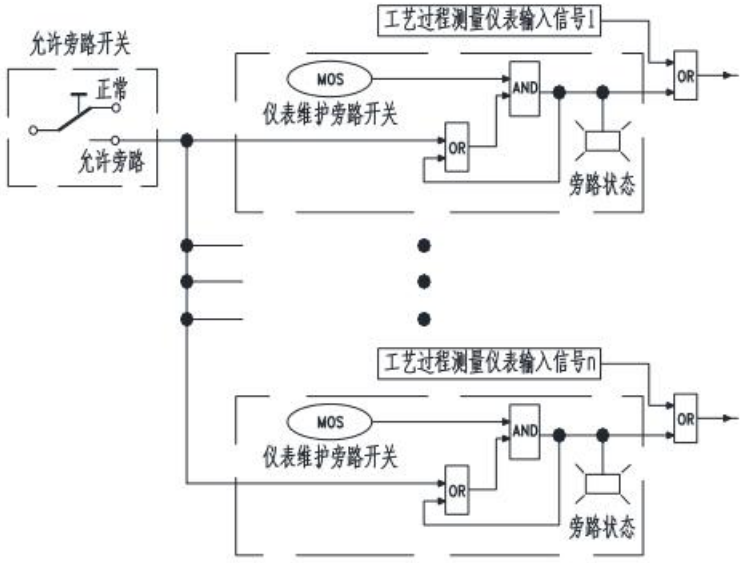

图 10　软件仪表维护旁路开关和硬件允许旁路开关典型设置示例

图 10 中，逻辑状态设定：允许旁路开关，“1”对应允许旁路，“0”对应正常；仪表维护旁路开关，“1” 对应旁路，“0”对应正常；工艺过程测量仪表输入信号，“1”对应正常，“0”对应联锁。

10.3.4 应严格管控仪表维护旁路操作。正常运行时仪表维护旁路开关应置于非旁路状态。

10.4 操作旁路开关

10.4.1 操作旁路开关通常用于工艺装置开工过程和生产工艺转换过程，在此过程中输入信号还没有达到正常状态。将输入信号暂时旁路，解除自动联锁功能，使工艺装置得以开工或工艺转换。工艺条件正常后，操作旁路开关应置于非旁路状态，使安全仪表功能恢复正常联锁保护功能。应严格管控操作旁路开关的使用。

10.5 联锁复位按钮

10.5.1 联锁复位按钮和复位逻辑应具有以下功能：

1 联锁输入工艺条件达到联锁设定值，应自动联锁；

2 联锁输入工艺条件恢复到正常状态，不进行复位操作，联锁状态应保持不变；

3 联锁输入工艺条件恢复到正常状态，进行复位操作，联锁应自动解除；

4 联锁输入工艺条件处于正常状态时，进行复位操作，联锁状态应保持不变。

10.6 紧急停车按钮

10.6.3 防护罩用于防止紧急停车按钮被误碰误撞造成误停车。防护罩上不应设置妨碍其紧急开启的附件，如权限锁等。

10.7 工程师站及事件顺序记录站

10.7.5 事件顺序记录站记录的历史数据保存时间不宜小于 180 天。可能通过其他存储介质备份更长时间。

11 应用程序

11.1 基本要求

11.1.4 组态工具软件的应用程序开发语言常用三类：

1 固定程序语言（Fixed Program Language -FPL）：仅能对有限参数进行调整或组态，如智能变送器、智能阀门定位器等的组态语言；

2 有限可变语言（Limited Variability Language -LVL）：通常为可编程电子系统的应用程序组态工具，对安全仪表系统而言，指按照 GB/T 15969-3 / IEC 61131-3 标准的组态编程语言，采用功能逻辑块图等形式；

3 完全可变语言（Full Variability Language -FVL）：指高级语言，如 C++、Pascal 等编程语言。

化工安全仪表系统应用程序的设计与组态宜采用有限可变语言。

11.3 应用程序设计和组态

11.3.2 为了正确设计，正确组态，正确修改，正确更新，逻辑设计应有可读性，复杂功能逻辑图应有逻辑功能说明。

12 供电、接地、防雷与配线

12.0.1 两路独立的 UPS 电源供电，供电可靠性高，以保证安全仪表系统的可用性、安全性。

两路独立的 UPS 电源宜采用两套独立的 UPS 装置。两路供电从 UPS 到安全仪表系统直流电源装置保持相互独立。

安全仪表系统的机柜风扇、照明等辅助设施的供电宜采用非 UPS 电源，以减少其故障、维修可能造成对 UPS 供电系统的不利影响。

安全仪表系统可与基本过程控制系统共用 UPS 装置，除非经评估不满足工艺装置对安全性或可用性的要求。

13 工程设计

13.1 基础工程设计

13.1.3 在安全仪表功能安全完整性设计时，可通过在测量仪表、逻辑控制器、最终元件之间合理分配失效率权重，以优化设计。

失效率权重分配案例：测量仪表为 35%，最终元件为 55%，逻辑控制单元为 10%。

13.2 详细工程设计

13.2.1 详细工程设计文件可由工程设计单位和逻辑控制器集成单位合作完成，以利于设计文件与实物的一致性。

14 集成、组态、调试、验收、联调与确认

14.1 集成、组态、调试

14.1.5 集成文件是集成工厂在设计、制造、集成、验收测试等过程中产生并应提交用户的文件。

14.3 联调

14.3.1 联调是在测量仪表、逻辑控制器、最终元件和关联仪表间进行的回路联合调试，检查接线正确性、信号传输的正确性、逻辑关系的正确性。