备案号：

中华人民共和国石油化工行业标准

HG/T 22820—202×

化工安全仪表系统工程设计规范

Design code for safety instrumented system

in chemical industry

（征求意见稿）

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

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：××××年××月××日

××××出版社

××××年　　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，由中国石油和化工勘察设计协会委托全国化工自动控制设计技术中心站组织编制。

本规范组成内容共有9章。规范正文包含以下内容：总则、规范性引用文件，术语与缩略语，基础规定，设计基本原则，安全仪表系统组成，集成、组态、调试、验收与确认，文档管理。

本规范共有2个附录。附录包含：安全仪表系统逻辑控制器技术规格书模板、安全仪表系统辅助操作台操作面板布置模板。

本规范的技术内容由中石油华东设计院有限公司负责解释（通讯地址：山东省青岛市华严路2号）。

本规范在执行过程中如有意见请寄主编单位或全国化工自动控制设计技术中心站(上海市徐汇区中山南二路1089号徐汇汇苑大厦12层，邮编：200030）

本规范主编单位、主要起草人和主要审查人员：

主编单位：　中石油华东设计院有限公司

参编单位：

主要起草人：林洪俊　×××　×××　×××　×××

主要审查人员：　×××　×××　×××　×××

目　次

1 总　则

1.1.1 本规范规定了安全仪表系统（SIS）的工程设计要求。

1.1.2 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。

1.1.3 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

实现一个或多个安全仪表功能的仪表系统。

2.1.2 风险 risk

伤害发生概率与伤害严重程度的组合。

2.1.3 过程风险 process risk

因异常事件引起过程条件改变而产生的风险。

2.1.4 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。

2.1.5 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。

2.1.6 保护层 protection layer

通过控制、预防、减缓等手段降低风险的任何独立措施。

2.1.7 安全功能 safety function

对于特定危险事件，为了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。

2.1.8 安全仪表功能 safety instrumented function

由安全仪表系统实现的安全功能。

2.1.9 故障 fault

由于内部异常状态导致不能执行所需的功能。

2.1.10 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。

2.1.11 安全完整性等级 safety integrity level

分配给安全仪表功能的不同等级（由低到高为 SIL1~SIL4），明确安全仪表系统实现的安全完整性要求。

2.1.12 失效 failure

丧失按要求执行的能力。

2.1.13 危险失效 dangerous failure

可阻碍或丧失特定安全功能的失效。

2.1.14 安全失效 safe failure

可有助于特定安全功能的失效。

2.1.15 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。

2.1.16 测量单元　measuring unit

安全仪表系统或基本过程控制系统中测量同一过程变量的一组测量仪表的组合。

2.1.17 逻辑控制单元　logic function unit

安全仪表系统或基本过程控制系统中执行同样逻辑功能的一组逻辑控制器的组合。

2.1.18 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。

2.1.19 执行单元　final unit

安全仪表系统或基本过程控制系统中实现或维持同一安全状态的一组执行元件的组合。

2.1.20 执行元件　final element

安全仪表系统或基本过程控制系统中实现或维持安全状态所需物理动作的设备。

2.1.21 辅助仪表　auxiliary 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执行元件之间，执行信号变换、信号隔离、能量限制等功能的设备。如：信号转换器，信号隔离器，继电器，安全栅，浪涌保护器，等。

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

对来自（工艺）过程及其关联设备、其它可编程系统和/或操作员的输入信号作出响应，并产生输出信号，使（工艺）过程及其关联设备按所期望的方式运行。不执行任何安全仪表功能。

2.1.23 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。

2.1.24 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。

2.1.25 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。

2.1.26 开关量　on-off 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。

2.1.27 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。

2.1.28 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。

2.1.29 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。

2.1.30 接点　contact

在外界因素作用下可以改变接通或断开导电状态的电气器件。有机械式和电子式。在可编程序逻辑控制器的运算部件中还有软件接点。

2.1.31 常闭接点　normally closed contact

在没有外界因素影响时，自然情况下闭合的接点。

2.1.32 常开接点　normally open contact

在没有外界因素影响时，自然情况下断开的接点。

2.1.33 可编程电子系统　programmable electronic system

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。

2.1.34 过程安全时间　process safety time

安全仪表功能为动作情况下，从过程参数出现偏差或基本过程控制系统出现故障到危险事件发生之间的时间。

2.1.35 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。

2.1.36 验证　verification

通过检查和提供证据确认要求已经得到满足。

2.1.37 确认　validation

通过检查和提供证据确认特定用途的要求已经得到满足。

2.1.38 安全要求规格书　safety requirement specification

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。

2.1.39 平均恢复时间　mean time to restoration

完成功能恢复的平均预计时间。

2.1.40 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。

2.1.41 先验使用　prior use

基于以往类似运行环境的使用经验，已经被验证过该设备可用于安全仪表系统，可满足特定功能和安全完整性等级的要求。

2.1.42 操作模式　mode of operation

安全仪表功能的操作模式可分为低要求模式、高要求模式和连续模式。

2.1.43 高要求模式　continuous mode

安全相关系统使用的方式，在这种模式下，对一个安全相关系统提出操作要求的频率大于每年一次或大于二倍的检验测试频率。

2.1.44 低要求模式　demand mode

安全相关系统使用的方式，在这种模式下，对一个安全相关系统提出操作要求的频率不大于每年一次或不大于二倍的检验测试频率。

2.1.45 诊断　diagnostics

用于发现故障的频繁（与过程安全时间有关）自动测试。

2.1.46 诊断覆盖率　diagnostics coverrage

通过诊断检测出危险失效发生的概率。诊断覆盖率不包括检验测试检测出的任何故障。

2.1.47 误停车率 spurious trip rate

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。

2.1.48 共因失效 common cause failure

由单个事件引起不同设备同时故障，此类故障之间没有因果关系。

2.1.49 系统性能力 systematic capability

当一个组件按组件符合项安全手册的规定应用时，针对规定的组件安全功能，组件的系统性安全全整性满足规定的 SIL 要求的置信度的度量（表示为 SC1～SC4）。

注 1：系统性能力由用于避免和控制系统性故障的要求来确定。

注 2：相关的系统性失效机理取决于组件的特性。比如一个组件单独由软件构成，则只需考虑软件失效机理。如组件由硬件和软件构成则需要考虑硬件和软件的失效机理。

注 3：当一个组件按组件符合项安全手册的规定应用时，针对规定的组件安全功能，组件具有 SC N 的系统能力意味着 SIL N 的系统性安全完整性已被满足。

2.1.50 结构约束 architectural constraint

对安全回路中的某个组件从硬件结构上进行约束，限制其所能达到的 SIL。

2.1.51 可用性 availability

在高故障裕度条件下，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。

2.1.52 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：

AC	Architectural Constraint	结构约束
AOOS	Allowable maintenance Override Switch	允许维护旁路开关
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
EMC	Electro Magnetic Compatibility	电磁兼容性
FAT	Factory Acceptance Testing	工厂验收测试
FLD	Functional Logic Diagram	功能逻辑图
FBD	Functional Block Diagram	功能块图
FDS	Functional Design Specification	功能设计规定
HAZOP	Hazard and Operability Study	危险和可操作性研究
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、安全和环保
IFAT	Integrated Factory Acceptance Testing	集成工厂验收测试
LOPA	Laver of Protection Analysis	保护层分析
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
PHA	Preliminary Hazard Analysis	预危险分析
PFD_{avg}	Probability of Failure on Demand Average	要求模式的平均失效概率
PFH	Probability of Failure per Hour	每小时失效频率
PLC	Programmable Logic Controller	可编程逻辑控制器
PST	Partial Stroke Test	部分形成测试
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
SFF	Safety Fraction Factor	安全失效分数
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	安全功能需求规格书
STR	Spurious Trip Rate	误停车率
UPS	Uninterruptable Power Supply	不间断电源

3　基础规定

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的安全生命周期内各阶段功能安全管理所需要的管理活动和技术活动。

3.1.2 安全生命周期宜分为工程设计阶段，集成调试、验收测试及确认阶段和运行维护阶段。

3.1.3 安全生命周期工作（图 3.1.1）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与验证，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，安全仪表系统集成、调试、验收测试及确认、安全仪表系统运行维护与变更，安全仪表系统检验测试，安全仪表系统停用等。

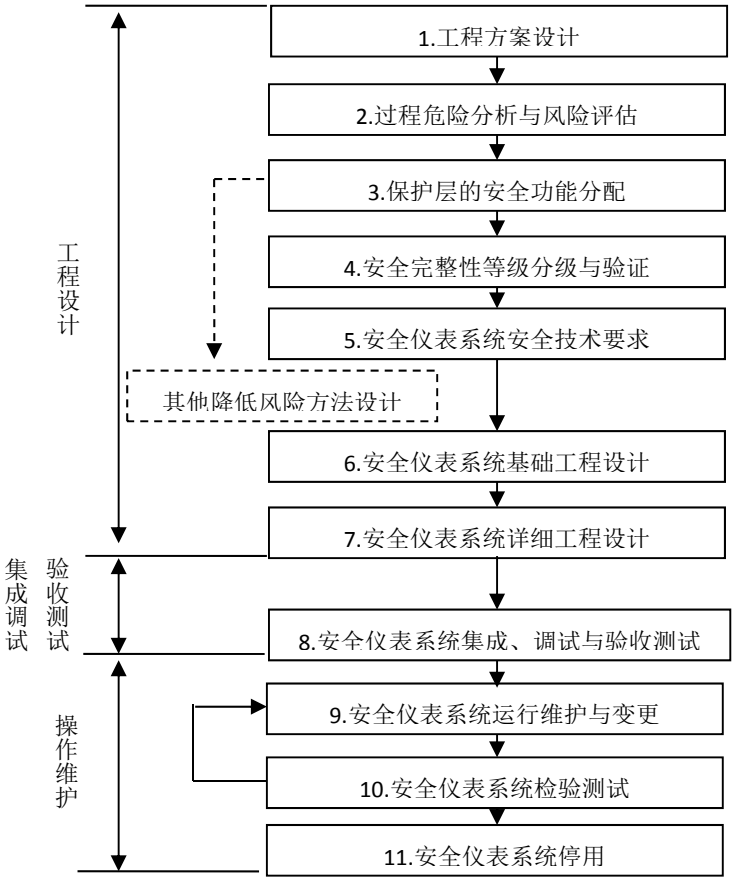

图 3.1.1　安全生命周期工作流程图

3.1.4 工程设计基本内容：

（1） 工程方案设计宜包括初步的过程危险分析、主要安全控制策略和措施及相应的说明。

（2） 过程危险分析和风险评估宜包括识别过程及相关设备的危险事件及原因，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） 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 和《过程工业领域安全仪表系统的功能安全》GB/T 21109 的有关规定。

（4） 安全完整性等级分级可根据过程危险分析和保护层功能分配的结果确定。安全完整性等级验证是贯穿安全生命周期各阶段的管理活动，验证安全仪表功能满足安全技术要求及安全完整性等级的要求。

（5） 安全仪表系统安全技术要求宜通过编制安全要求规格书表述。安全要求规格书应基于企业风险标准，依据危险与风险评估（如保护层分析）辨识得出的风险降低要求，确定工程设计、建设、运行、维护和管理策略。安全要求规格书的内容应包括安全仪表功能及其安全完整性等级的设计原则、过程安全状态、操作模式、检验测试间隔、安全仪表系统的硬件要求、应用程序的安全要求等。

（6） 安全仪表系统的基础工程设计应符合安全技术要求的规定，设计文件宜包括安全仪表系统设计说明、安全仪表系统规格书、安全联锁因果表或功能说明等。

（7） 安全仪表系统的详细工程设计应符合安全技术要求的规定，设计文件宜包括安全仪表系统设计说明、安全仪表系统规格书、功能逻辑图、因果表等。

3.1.5 集成、调试、验收测试及确认基本内容：

（1） 安全仪表系统集成、调试、验收测试及确认，应符合安全仪表系统的安全技术要求、安全仪表系统规格书及功能逻辑图的要求。

（2） 安全仪表系统调试结果应符合安全仪表系统的安全技术要求。

（3） 安全仪表系统验收测试应包括工厂验收和现场验收。安全仪表系统硬件、系统软件和应用程序等，应符合安全仪表系统的安全技术要求。

（4） 安全仪表系统确认宜包括测量仪表、逻辑控制器、执行元件及关联设备的安装与测试符合安全仪表系统工程设计，宜实施安全仪表系统投运前的安全审查并形成记录文档。

3.1.6 运行维护主要内容：

（1） 运行维护应遵循运行维护作业规程，应使运行维护过程符合安全仪表系统安全技术要求、安全仪表系统安全手册的规定，确保安全仪表系统的功能安全。

（2） 安全仪表系统的硬件和应用程序的修改或变更应符合变更管理规程，应对修改或变更涉及的范围进行分析，按审批程序获得授权批准，不应降低设计的安全完整性等级，并应保留变更记录。

（3） 运行维护人员应定期培训，培训内容宜包括安全仪表系统的功能、可预防的过程危险、测量仪表和执行元件、安全仪表系统的逻辑动作、安全仪表系统及过程变量的报警、安全仪表系统动作后的处理等。

（4） 建立检验测试规程并按照安全仪表系统安全技术要求的检验测试间隔要求进行功能测试，做好记录，对发现的失效进行原因分析。

（5） 安全仪表系统的停用应进行审查并得到批准。安全仪表系统更新应制订更新规程。更新后的安全仪表系统应能实现规定的安全仪表功能。

3.2 安全完整性等级

3.2.1 安全完整性应包括硬件安全完整性和系统安全完整性。

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

3.2.3 在低要求操作模式时，安全仪表功能的安全完整性等级应采用要求的危险失效平均概率（PFD_{avg}）衡量，宜根据表 4.2.1 确定。

表 3.2.1 安全完整性等级（低要求操作模式）

安全完整性等级（SIL）	低要求操作模式的平均失效概率（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	$\geq 10^{-3}$ 且 $<10^{-2}$	>100 到≤1000
1	$\geq 10^{-2}$ 且 $<10^{-1}$	>10 到≤100

3.2.4 在连续操作模式或高要求操作模式时，安全仪表功能的安全完整性等级应采用危险失效平均频率（PFH）衡量，宜根据表 4.2.2 确定。

表 3.2.2 安全完整性等级（连续操作模式或高要求操作模式）

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

3.2.5 安全完整性等级分级为 SILa 或 SIL0 指要求时危险失效平均概率（PFDavg）介于 0.1 和 1 之间的风险降低措施。SILa 或 SIL0 联锁保护功能可在安全仪表系统实现，也可在基本过程控制系统实现。

3.2.6 安全完整性等级评估应包括安全完整性等级分级和安全完整性等级验证。

3.2.7 安全完整性等级分级分级方法应根据工艺过程复杂程度、国家标准、企业安全风险矩阵等确定。主要方法可采用保护层分析法、风险矩阵法、校正的风险图法、经验法及其它方法。

3.2.8 安全完整性等级分级宜采用审查会形式。审查资料宜包括管道与仪表流程图（P&ID）、工艺技术说明、危险与可操作性研究（HAZOP）报告、功能逻辑图或因果表、安全联锁说明及其有关文件。参加安全完整性等级分级的主要人员宜包括工艺、过程控制（仪表）、安全、设备、生产操作及管理等专业或岗位。

3.2.9 安全完整性等级验证应包括：

（1） 安全仪表功能的安全完整性等级应进行验证。硬件安全完整性等级验证内容包括安全仪表功能的危险失效平均概率（PFDavg）、结构约束等。系统性能力（SC）可用于系统安全完整性的验证。

（2） 安全仪表功能的要求时危险失效平均概率（PFDavg）验证计算采用的仪表设备可靠性数据宜来自以往使用数据、安全完整性等级认证报告、公开发行的工业数据库或手册等。

（3） 安全完整性等级验证应确定安全仪表系统或安全子系统的检验测试间隔（Ti）。安全仪表系统或安全子系统的检验测试间隔宜与企业计划停车检修时间间隔相同。

（4） 当安全仪表系统的误动作可能造成的损失大于可容忍程度时，可验证安全仪表功能满足可用性的要求，如验证安全仪表功能的误停车率（STR）。

3.3 结构约束、硬件故障裕度

3.3.1 安全仪表功能测量单元、逻辑控制单元、执行单元应满足结构约束或硬件故障裕度的最低要求。最低要求见表 3.3.1 和表 3.3.2。

表 3.3.1 可编程电子逻辑控制器的最小 HFT

SIL	最小 HFT		
	SFF＜60%	60%≤SFF≤90%	SFF＞90%
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	

表 3.3.2 传感器、执行元件和非可编程电子逻辑控制器的最小 HFT

SIL	最小 HFT	SIL	最小 HFT
1	0	3	2
2	1		

3.3.2 可提高安全裕度，增加可靠性或可用性。

4　设计基本原则

4.1.1 安全仪表系统的工程设计应满足石油化工工厂或装置的安全仪表系统安全技术要求。

4.1.2 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，应防止设计不足或过度设计。

4.1.3 石油化工工厂或装置安全仪表功能的安全完整性等级不宜高于 SIL 2 级，不应高于 SIL 3 级。

4.1.4 安全仪表系统可执行一个或多个安全仪表功能。当多个安全完整性等级的安全仪表功能在同一安全仪表系统内实现时，系统内的共用部分应符合各安全仪表功能中最高安全完整性等级要求。

4.1.5 安全仪表系统应独立于基本过程控制系统，并应独立完成安全仪表功能。

4.1.6 当安全仪表系统与基本过程控制系统有共用设备时，安全仪表系统应具有优先权，基本过程控制系统的失效不应影响影响安全仪表系统的功能安全，不应降低安全仪表功能的安全完整性等级。

4.1.7 安全仪表系统宜设计成故障安全型。当安全仪表系统内部产生故障时，安全仪表系统应能按设计预定方式，将过程转入安全状态。故障应包括安全仪表系统故障、电源故障、气源故障、信号线路断路等。

4.1.8 安全仪表系统的逻辑控制器应具有硬件和软件自诊断功能，其它组成部分宜具有自诊断功能。

4.1.9 安全仪表系统的中间环节应尽可能少。

4.1.10 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。

4.1.11 安全仪表系统应根据可用性需求或国家现行防雷标准实施防雷工程。

4.1.12 安全仪表系统的交流供电宜采用 UPS 供电提高可用性，重要装置可采用双路 UPS 供电方式提高可用性。

4.1.13 安全仪表系统的接地应采用等电位连接方式。

4.1.14 安全仪表系统的硬件、操作系统及编程软件应采用正式发布版本。

4.1.15 安全仪表系统软件、编程、升级或修改等文档应备份。

4.1.16 安全仪表系统内的设备应设置同一时钟，并宜与基本过程控制系统的时钟同步。

4.1.17 在大型石油化工项目中设置多套安全仪表系统时，每套系统应能独立工作。

4.1.18 当安全仪表系统输入、输出信号线路中有可能存在来自外部的危险干扰信号时，应采取隔离器、继电器等隔离措施。

4.1.19 安全仪表系统应设计信息安全防护措施。

4.1.20 安全仪表系统的检验测试间隔（Ti）小于工艺装置检修周期时应设计检验测试措施。

5　安全仪表系统组成

5.1 系统组成

5.1.1　安全仪表系统应由测量仪表、执行元件、逻辑控制器、辅助仪表、网络和通信接口、人机接口设备组成。

5.1.2　安全仪表系统宜采用网络结构方式，通过网络交换机把控制器和操作站、工程师站、数据存储站、打印机等设备互联。

5.1.3　安全仪表系统网络应按功能分层设置， 宜按控制范围分区域设置。典型的单装置 SIS 网络拓扑图如图 6.1.3-1 所示。典型的全厂性 SIS 网络拓扑图如图 6.1.3-2 所示。

5.1.4　安全仪表系统网络通讯介质宜采用光纤。

5.1.5　安全仪表系统可与基本过程控制系统通讯。宜通过控制器间进行通讯。通讯数据不应用于安全功能。

5.1.6　安全仪表系统网络不应与工厂管理网络直接链接。

5.1.7　安全仪表系统操作站宜与基本过程控制系统共用。

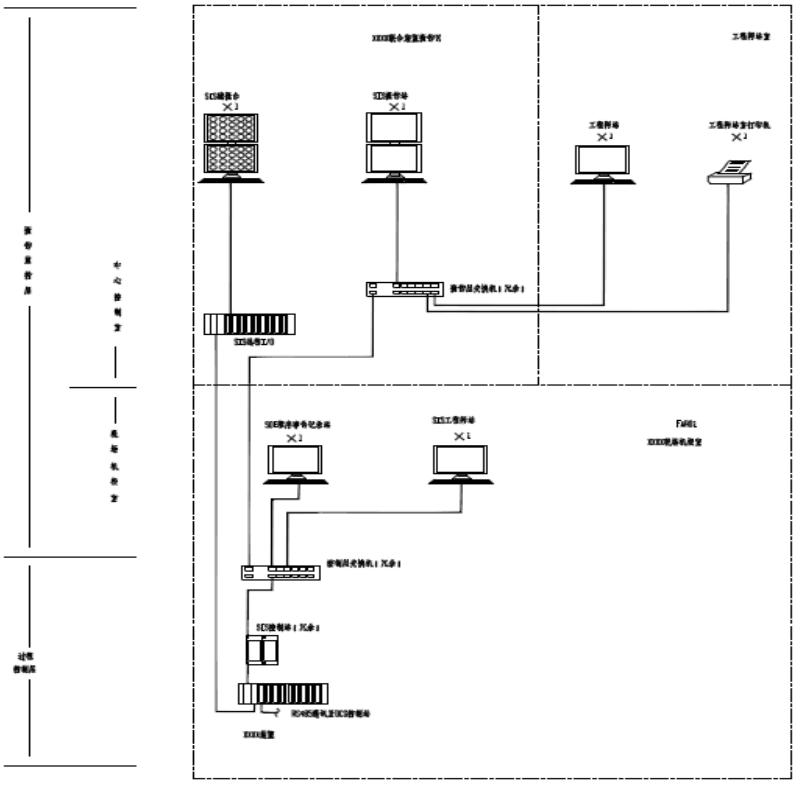

图 6.1.3-1　典型单装置 SIS 网络拓扑图

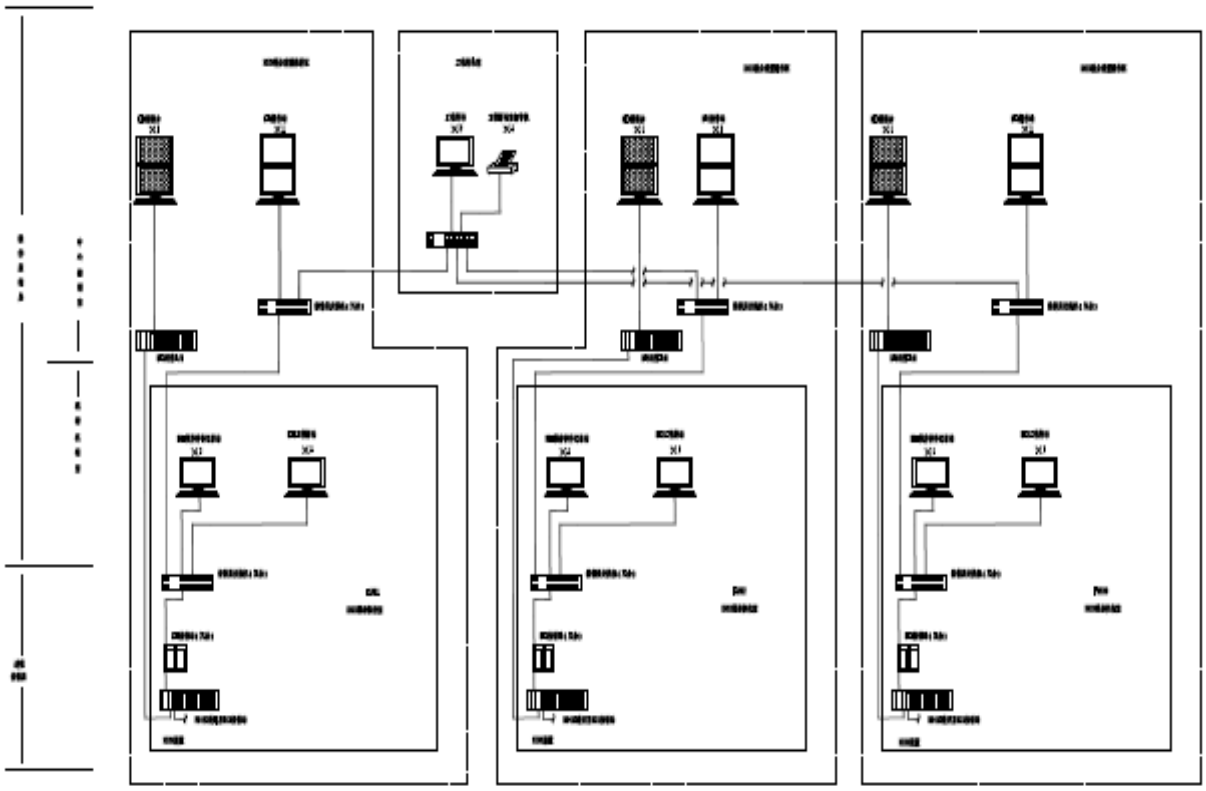

图 6.1.3-2　典型全厂性 SIS 网络拓扑图

5.2 测量仪表

5.2.1 基本规定

5.2.1.1 安全仪表系统宜设置独立的测量仪表，应满足独立完成安全功能的需要。

5.2.1.2 测量仪表或测量仪表单元的性能应满足安全完整性等级和结构约束的要求。

5.2.1.3 测量仪表宜采用模拟量测量仪表，也可采用开关量测量仪表。

5.2.1.4 测量仪表宜采用有故障自诊断功能的智能仪表。宜采用 4mA~20mA 叠加 HART 传输信号的智能变送器。不应采用现场总线或其他通信方式作为安全仪表系统的输入信号。不应采用无线信号作为安全仪表系统的输入信号。

5.2.1.5 在爆炸危险场所，测量仪表应选用相应防爆等级的仪表。当选用本质安全防爆方式时，应采用隔离式安全栅。

5.2.1.6 测量仪表安装于地面以上时，防护等级不应低于 IP65；安装于地下检修井内时，防护等级不应低于 IP68。

5.2.1.7 同一被测过程变量的多台测量仪表的取源点和取源部件宜彼此独立，并宜独立于基本过程控制系统测量仪表。节流装置作为测量元件时可以共用，但取压点、引压管路、传感器应彼此独立。

5.2.1.8 仪表选型除应满足本规范外，尚应满足《自动化仪表选型设计规范》HG/T20507 的要求。

5.2.2 测量单元配置

5.2.2.1 每一安全功能可配置 1 台或多台测量仪表，应满足安全仪表功能的危险失效平均概率（PFDavg）和结构约束要求，在此基础上应满足工艺过程可用性要求。

5.2.2.2 同一工艺过程变量的多台测量仪表可通过采用“与”、“或”逻辑的冗余结构提高可靠性或可用性。当系统要求高安全性时，应采用“与”逻辑结构。当系统要求高可用性时，应采用“或”逻辑结构。当系统需要兼顾高安全性和高可用性时，宜采用三取二逻辑结构。

【条文说明：逻辑约定，变量超限为 0】

5.2.2.3 测量仪表冗余配置时，宜设置仪表输出信号之间偏差报警。

5.2.2.4 开关量信号测量仪表，工况正常时，输出信号应为闭合状态；达到设定的安全限值时，或仪表电源、气源等能源中断时，输出信号应为应为断开状态。

5.2.2.5 测量仪表宜在现场测量管路中设置维护、维修用切除设施。

5.3 执行元件

5.3.1 基本规定

5.3.1.1 执行元件可包括控制阀、电磁阀、电机控制器等。

5.3.1.2 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，不宜采用电动控制阀。采用电动执行机构时应采取供电安全保证措施。

5.3.1.3 控制阀应具有能源中断自动达到安全位置的功能，或者自带备用能源。备用能源应满足控

制阀至少一个行程的容量。

5.3.1.4 执行元件应满足安全仪表系统安全技术要求、安全完整性等级要求。

5.3.1.5 SIL 1 级安全仪表功能，控制阀宜与基本过程控制系统分开。当与基本过程控制系统共用控制阀时，应确保安全仪表系统的动作优先并独立完成。

5.3.1.6 SIL 2 级安全仪表功能，控制阀应与基本过程控制系统分开。

5.3.1.7 SIL 3 级安全仪表功能，控制阀应与基本过程控制系统分开。

5.3.1.8 每个执行元件具有独立的控制信号。

5.3.1.9 执行元件应采用触点控制信号，两位式控制方式。联锁前触点闭合，联锁时触点打开，高压电机可除外。

5.3.1.10 在爆炸危险场所，控制阀及附件应满足防爆要求。

5.3.1.11 现场地上安装的控制阀及附件防护等级不应低于 IP65。

5.3.1.12 控制阀应满足《自动化仪表选型设计规范》HG/T20507 的要求。

5.3.2 控制阀附件的配置

5.3.2.1 控制阀电磁阀应安装在靠近执行机构的控制管路上。

5.3.2.2 控制阀电磁阀应采用长期励磁型。

5.3.2.3 控制阀电磁阀性能应满足控制阀的安全完整性等级需要。

5.3.2.4 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，电磁阀组宜采用“与”逻辑模式；当要求高可用性时，电磁阀组宜采用“或”模式。

【条文说明：逻辑约定，启动联锁为 0】

5.3.2.5 电磁阀电源应由安全仪表系统提供。

5.3.2.6 控制阀应配现场阀位显示器，指示阀位。

5.3.2.7 控制阀宜配置阀位行程开关。阀位信号可在安全仪表系统或基本过程控制系统显示阀位。宜设置阀门动作超时报警。

5.3.2.8 当阀位行程开关作为安全功能输入条件时，应满足测量仪表的相关要求。

5.4 逻辑单元

5.4.1 基本规定

5.4.1.1 逻辑控制单元宜采用可编程电子系统。对于输入、输出点数较少、逻辑功能简单的场合，逻辑控制单元可采用继电器组合实现。逻辑控制单元也可采用可编程电子系统和继电器组合实现。

5.4.1.2 用于逻辑控制单元的可编程电子系统应取得国家授权认证机构的功能安全认证。

5.4.1.3 逻辑控制器的响应时间应包括输入、输出扫描处理时间与中央处理单元运算时间，宜为100ms～300ms。

5.4.1.4 逻辑控制器的中央处理单元负荷不应超过50%。

5.4.1.5 逻辑控制器的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%。

5.4.1.6 逻辑控制单元应独立设置，应独立完成安全功能。

【条文说明：基本过程控制系统须经评估符合GB/T21109相关要求后，方可作为安全功能保护层】

5.4.2 逻辑控制器的配置

5.4.2.1 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。

5.4.2.2 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，应采用冗余技术，应允许在线更换单元而不影响逻辑控制器的正常运行。

5.4.2.3 逻辑控制器应有硬件和软件的诊断和测试功能。诊断和测试信息应在工程师站或操作员站显示、记录。

5.4.2.4 逻辑控制器的故障应在安全仪表系统的操作员站报警和基本过程控制系统的操作员站报警。

5.4.2.5 逻辑控制器宜与基本过程控制系统的时钟同步。

5.4.2.6 应配置多台逻辑控制器，应采用冗余结构满足安全完整性等级要求和工艺过程可用性要求。

5.4.3 逻辑控制器的I/O卡件配置

5.4.3.1 I/O卡件信号通道应带光电或电磁隔离。

5.4.3.2 检测同一过程变量的多台变送器信号宜接到不同输入卡件。

5.4.3.3 冗余的执行元件应接到不同的输出卡件，每一输出信号通道应只接一个执行元件。

5.4.3.4 安全功能的I/O卡件应采用模拟信号、开关量信号，不应采用数字通讯信号，不应采用无线信号。

5.4.3.5 输入、输出信号线路中可能存在干扰信号时，模拟信号宜配置信号隔离器，开关量信号宜配置隔离继电器。

5.4.3.6 模拟信号输入卡件应带有线路短路和开路故障检测功能。线路故障时应进行高级别报警和记录。当需要高可靠性时，线路故障信号可预设为有效联锁值信号。

5.4.3.7 变送器输入信号超出4mA~20mA时应进行高级别报警和记录。报警状态可作为提高可靠性或可用性的逻辑输入信号。

5.4.3.8 测量仪表输入信号宜在逻辑控制器中设置仪表维护、维修、周期性检验测试使用的旁路措施。

5.4.3.9 每种 I/O 卡件宜留有不低于 10%的备用通道。

5.4.3.10 I/O 卡件应冗余配置。

5.5 辅助仪表

5.5.1 辅助仪表可包括安全栅、继电器、隔离器、电涌保护器、多路 HART 信号采集器等。

5.5.2 安全仪表功能回路中的辅助仪表性能应满足本回路安全完整性等级的需求。

5.5.3 安全栅应选用隔离式安全栅。

5.5.4 继电器应选用安全型继电器。

5.5.5 电涌保护器应选用线路并联旁路式，其故障不应影响本回路功能安全。

5.5.6 多路 HART 信号采集器应选用线路并联旁路式，其故障不应影响本回路功能安全。

5.6 网络和通信接口

5.6.1 安全仪表系统与基本过程控制系统通信应在控制器之间直接进行。通信接口应冗余配置。宜采用 RS 485 串行通信接口，MODBUS RTU 通信协议。当采用 TCP/IP 通信协议时应采取网络安全措施。

5.6.2 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。

5.6.3 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。安全仪表系统与其它系统之间的连接应采用硬接线方式。

5.6.4 网络通信接口的故障不应影响安全仪表系统的安全功能。通信接口故障应在操作站或工程师站显示、报警。

5.6.5 网络通信接口负荷不应超过 50%。

5.6.6 网络通信介质宜采用光纤，网络交换机宜采用一体化光纤通信接口。

5.6.7 网络通讯交换机应采用冗余的双电源接入口。

5.7 人机接口单元

5.7.1 操作员站

5.7.1.1 安全仪表系统可设操作站。在操作员站失效时，安全仪表系统的逻辑处理功能不应受影响。宜共用基本过程控制系统的操作站，也可设独立的操作员站。

5.7.1.2 操作员站可用于过程信号报警和联锁动作报警的显示和记录。

5.7.1.3 操作员站可显示联锁逻辑，输入、输出状态，系统报警，参数报警。

5.7.1.4 在操作员站可设置联锁复位功能软件按钮。

5.7.1.5 在操作员站可设置仪表维护旁路、工艺操作旁路软件开关，并应加键锁或口令保护，应设置旁路状态报警和记录。

5.7.1.6 操作员站应提供程序运行、预报警、连锁动作、输入状态、输出状态、故障诊断等显示及事件记录等功能。

5.7.1.7 操作员站应具有冗余的网络接口。

5.7.2 辅助操作台

5.7.2.1 紧急停车按钮/开关、允许旁路开关、试灯按钮、消音按钮应安装在辅助操作台指示与操作面上。

5.7.2.2 信号报警器宜采用下列颜色的灯光；

1 红色灯光表示越限报警或紧急状态；

2 黄色灯光表示预报警；

3 绿色灯光表示运转设备或过程变量正常。

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

5.7.2.4 关键信号报警除在操作员站显示外，应同时在辅助操作台显示

5.7.2.5 操作台上的按钮、开关、报警灯等与逻辑控制器连接，两者相距较近时应采用硬接线方式；两者相距较远时，应采用系统远程输入、输出卡件或控制器方式进行信号连接。

5.7.2.6 操作台形式宜于操作站协调一致。

5.7.2.7 在操作室内，宜按工艺装置独立设置辅助操作台，也在操作台面上分区布置不同装置的按钮、开关、报警灯等。

5.7.3 仪表维护旁路开关

5.7.3.1 每个测量仪表输入宜设置维护旁路开关。可按下列方式设置：

1 在安全仪表系统的操作员站设置软件开关；.

2 通过基本过程控制系统的操作员站设置软件开关，通过通讯方式送达安全仪表系统控制器；

3 在辅助操作台或机柜设置硬件开关。

5.7.3.2 采用软件维护旁路开关的方式时，应按联锁单元，或工艺工段，或工艺装置设“允许旁路”开关，作为软件维护旁路的逻辑生效条件。

5.7.3.3 测量仪表信号被旁路时应设置旁路状态报警和记录。

5.7.3.4 应制定仪表维护旁路操作规定，旁路状态时应通过其它措施监控工艺过程状态，并通过报警等措施提示工艺操作员安全仪表功能已处于维护旁路状态，直至旁路解除。每个“允许旁路”开关同一时间内宜仅允许两组测量仪表旁路。

5.7.4 操作旁路开关

5.7.4.1 当工艺装置初始工艺条件超过联锁设定值致使装置无法开车时，该安全仪表功能回路应设

置操作旁路开关。工艺条件具备投用条件后应解除旁路。

5.7.4.2 操作旁路开关应设置在输出信号通道上，但不应旁路紧急停车命令。

5.7.4.3 启动操作旁路后应在操作站进行报警和记录。

5.7.4.4 操作旁路开关可按下列方式设置：

1 在安全仪表系统的操作员站设置软件开关；

2 在基本过程控制系统的操作员站设置软件开关，通过通讯方式送达安全仪表系统逻辑控制器；

3 在辅助操作台设置硬件开关。

5.7.4.5 应制定操作旁路操作规定，旁路状态时应通过其它措施监控工艺过程状态，并通过报警等措施提示工艺操作员安全仪表功能已处于维护旁路状态，直至旁路解除。

5.7.5 复位按钮

5.7.5.1 每组联锁应设置独立的复位按钮。

5.7.5.2 复位按钮可按下列方式设置：

1 在安全仪表系统的操作员站设置软件按钮；

2 在基本过程控制系统的操作员站设置软件复位按钮，通过通讯方式送达安全仪表系统逻辑控制器；

3 在辅助操作台设置硬件复位按钮；

4 需要时可同时在现场设置硬件复位按钮，现场和控制室两处都复位后，联锁逻辑复位生效；

5.7.5.3 复位按钮的动作应设置事件记录。

5.7.6 紧急停车按钮

5.7.6.1 每组联锁宜设紧急停车按钮。

5.7.6.2 紧急停车按钮可按下列方式设置：

1 在辅助操作台设置硬件按钮；

2 需要时可同时在现场设置硬件按钮，只要在一处按动，停车命令即生效。

5.7.6.3 紧急停车按钮应配防护罩。安装于现场的按钮应符合防爆要求，防护等级不应低于 IP65。

5.7.6.4 紧急停车按钮按动后应在操作站报警和记录。

5.7.6.5 紧急停车按钮信号和逻辑不应被旁路。

5.7.7 工程师站及事件顺序记录站

5.7.7.1 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编程、系统诊断、系统维护。

5.7.7.2 工程师站应设不同级别的权限密码保护。工程师站应显示安全仪表系统动作和诊断状态。

5.7.7.3 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，也可与安全仪表系统的工程师站共用。

5.7.7.4 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。

5.7.7.5 工程师站和事件顺序记录站宜采用台式计算机，不宜采用移动笔记本电脑。

5.7.7.6 工程师站及事件顺序记录站失效时，安全仪表系统的安全功能不应受影响。

5.7.8 打印机

5.7.8.1 宜配置网络打印机。

5.7.9 信息安全

5.7.9.1 安全仪表系统的逻辑控制器采用可编程电子系统时，应进行网络安全风险评估，采取相应的网络安全策略和安防措施。

5.7.9.2 安全仪表系统不应与工厂管理网络直接链接。与安全仪表系统无关的设备或网络不应接入安全仪表系统网络或利用安全仪表系统网络传输数据。

5.7.9.3 安全仪表系统不应接入无线仪表和无线网络。

5.7.9.4 安全仪表系统的服务器、操作员站、工程师站极其它终端设备应采取防病毒、防黑客等保护措施。防病毒、防黑客软件宜基于信任机制的白名单技术。

6　工程设计

6.1　基础工程设计程序与内容

6.1.1　安全仪表系统基础工程设计工作宜按下列程序进行：

1　应根据工艺安全联锁保护需求绘制工艺管道及仪表流程图（P&ID），因果表或联锁逻辑框图；

2　编制仪表选型方案；

3　绘制安全仪表系统配置图；

4　参加工艺装置风险分析、保护层分配、安全仪表系统需求规格书（SRS）编制等活动。

5　根据安全评估报告（如 HAZOP、LOPA 报告）和安全仪表系统需求规格书（SRS），完善 P&ID、因果关系表或联锁逻辑框图，编制安全仪表系统工程设计文件。

6.1.2 安全仪表系统基础工程设计文件应根据工艺安全联锁说明、P&ID、安全仪表系统安全技术要求等进行编制。宜包括下列内容：

1　仪表回路索引表；

2　联锁逻辑框图，因果表，复杂逻辑功能说明；

3　安全仪表系统逻辑控制器技术规格书；

4　安全仪表系统测量仪表、执行元件、辅助仪表技术规格书；

5　安全仪表系统配置图。

6.1.3 安全仪表系统逻辑控制器技术规格书应包括下列主要内容：

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　系统通信；

9　系统负荷；

10　维护和安全、可靠性；

11　系统供电及接地；

12　验收测试要求；

13　环境要求；

14　机械要求；

15 技术服务；

16 质量保证；

17 文档资料。

6.1.4 安全仪表系统测量仪表、执行元件的技术规格书应包括项目应用环境和条件、设计条件、失效率范围、检验测试周期、技术说明和规定、技术数据表等。

6.1.5 在进行安全仪表功能回路设计时，应合理分配失效率的权重。

【条文说明　失效率分配按照满足安全要求、投资低的原则，可按下述比例做预分配：检测单元∑PFDavg 约占 30%，∑PFDavg 执行单元约占 50%，逻辑控制单元∑PFDavg 约占 10%，辅助仪表∑PFDavg 约占 10%】

6.1.6 基础设计阶段应对硬件故障裕度和冗余措施进行可靠性、可用性检查，可对安全仪表功能进行可靠性、可用性预验算。

6.2　详细工程设计程序与内容

6.2.1 安全仪表系统详细工程设计工作宜按下列程序进行：

1 编制逻辑控制器、测量仪表、执行元件、辅助仪表规格书；

2 配合安全仪表系统询价、采购及确认；

3 配合安全仪表系统 SIL 验证，并根据 SIL 验证报告修改工程设计文件。

4 配合应用程序组态、工厂验收（FAT）。

6.2.2 安全仪表系统详细工程设计宜包括下列内容：

1 仪表回路索引表；

2 联锁逻辑图，联锁因果表，复杂逻辑功能说明；

3 逻辑控制器数据表，技术规格书；

4 测量仪表、执行元件、辅助仪表数据表，技术规格书；

5 安全仪表系统配置图；

6 联锁及报警值一览表；

7 操作台面板布置图；

8 机柜内布置图；

9 I/O 卡件通道分配图；

10 仪表回路图。

6.3　可靠性、可用性辅助措施设计

6.3.1 供电、接地、防雷

6.3.1.1　安全仪表系统宜采用一级负荷中特别重要负荷供电，宜采用 UPS 供电。可与 BPCS 共用 UPS。

【条文说明　采用 UPS 供电的目的是为了提高可用性。宜采用双路供电，进一步提高可用

性】

6.3.1.2 系统供电应符合《仪表供电设计规范》HG/T 20509。

6.3.1.3 安全仪表系统应采用等电位接地原则，应接地至厂内公共电气接地网。

6.3.1.4 系统接地应按照《仪表系统接地设计规范》HG/T 20513。

6.3.1.5 安全仪表系统应根据可用性需求和仪表设备保护需求设置防雷措施，系统防雷可参考《石油化工仪表防雷工程设计规范》SH/T 3164。

6.3.2 供气

6.3.2.1 安全仪表系统气动执行元件宜采用独立的供气支管。

【条文说明　　采用独立的供气支管是为了提高可用性】

6.3.2.2 安全仪表系统气动执行元件供气应符合《仪表供气设计规范》HG/T 20510。

6.3.3 测量引线配管

6.3.3.1 测量引线配管应避免产生附加测量误差。

6.3.3.2 测量引线配管设计应符合《仪表配管配线设计规范》HG/T 20512。

6.3.4 保温、绝热、伴热

6.3.4.1 测量仪表测量管路温度应保证测量仪表稳定、准确测量，应采取必要且可靠的保温、绝热、伴热措施。

6.3.4.2 保温、绝热、伴热应符合《仪表及管线伴热和绝热保温设计规范》HG/T 20514。

6.3.5 隔离、吹洗

6.3.5.1 仪表测量测量管路不宜采用间断隔离吹洗方式。

6.3.5.2 测量仪表测量管路连续隔离冲洗宜采用独立的吹洗支管。

6.3.6 配线

6.3.6.1 安全仪表系统可与基本过程控制系统共同布线，共用汇线槽、保护管。

6.3.6.2 测量仪表、执行元件用电缆宜采用独立的接线箱。

6.3.6.3 仪表配线设计应符合《仪表配管配线设计规范》HG/T 20512。

7　集成、组态、调试、验收与确认

7.1　逻辑控制器集成

7.1.1 集成范围、内容

7.1.1.1 集成范围可包括逻辑控制器、人机接口、辅助仪表、网络接口等。

7.1.1.2 集成内容应包括硬件集成和软件集成。

7.1.1.3 集成工程包括安全仪表系统供电、接地、配线、安装、测试等。

7.1.2 系统功能设计

7.1.2.1　系统集成商宜进行功能设计（FDS）。功能设计可包括如下内容：

1　系统设计，包括系统网络分层、分域结构设计；

2　编号设计，包括设备编号，机柜编号，卡件编号，通道编号，线缆编号等；

3　布置设计，包括机柜分柜设计，机柜内布置，卡件布置，通道分配等；

4　配线设计，包括柜间布线，柜内布线等；

5　供电设计，包括机柜供电系统，柜内仪表设备供电；

6　接地设计，包括接地系统，柜内接地，柜外接地界面。

7　画面设计，包括逻辑画面、报警画面等，规定画面形式，画面颜色，线条颜色，文字格式；

8　报表设计，包括报警报表，操作报表。

7.1.2.2 功能设计应经业主和工程设计单位审核、批准。

7.1.2.3 系统供应商应根据批准后的功能设计进行系统集成。

7.1.3 系统设备

7.1.3.1 机柜

1　安全仪表系统应设置独立的机柜，不与基本过程控制系统混用。

2　大中型装置宜按工艺装置设置独立的安全仪表系统机柜，小型装置可与其他装置合用安全仪表系统机柜。

3　机柜应采用钢制，规格宜为 2100mm×800mm×800mm（高×宽×深）。

4　机柜内宜设置温度检测，自动控制风扇启停，超温自动报警。

5　机柜内宜预留 20%的有效安装空间。

6　机柜宜安装于控制室内，防护等级不应低于 IP30。

7.1.3.2 直流电源

1　机柜内系统逻辑控制器用直流电源应独立设置，不应与其它仪表共用。

2　直流电源宜分散布置于用电机柜，分散输出。

3　直流电源应按 1:1 模式冗余配置。

7.1.3.3 操作台

1　操作台宜采用钢制。

2 操作台型式、尺寸、颜色宜与基本过程控制系统一致

7.2 应用程序及组态

7.2.1 安全仪表功能宜采用过程用二进制逻辑图表达。应用程序应根据逻辑图编制。

7.2.2 应用程序的组态应使用制造厂的标准组态工具软件。

7.2.3 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 提供标准功能模块及其符号说明；

4 应用程序的编辑、翻译、下装及运行管理；

5 应用程序的离线仿真仿真测试功能。

7.2.4 应用程序的设计、编程、组态、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。

7.2.5 应用程序组态分工应通过合同约定。可采用如下方式：

1 用户与供货商一起组态；

2 用户组态，供货商指导；

3 供货商组态，用户检查。

7.2.6 应用程序文件应至少包括下列内容

1 应用程序说明；

2 输入点、输出点、通信点清单；

3 联锁功能逻辑图；

4 复杂逻辑说明；

7.2.7 应用程序组态前宜进行功能设计（FDS），的要求。

7.2.8 应用程序设计和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。

7.2.9 应用编程应进行离线测试后再下载投入运行。

7.2.10 应用程序应进行备份，宜本地和异地同时备份。

7.2.11 应用程序组态和备份应有防病毒措施

7.3 验收

7.3.1 验收测试应包括系统工厂验收测试和现场验收测试。

7.3.2 工厂验收

7.3.2.1 工厂测试应在系统集成商工厂，在系统集成安装、接线、组态完毕后进行。

7.3.2.2 集成商应提供测试程序、测试内容及步骤，用户应进行审批。

7.3.2.3 工厂测试应至少测试如下内容：

1 所有 I/O 通道性能；

2 所有应用程序逻辑功能；

3 每种冗余和容错功能；

4 每种在线插拔更换卡件功能；

5 在线修改及下装软件功能；

6 自诊断功能测试；

7 辅助操作台按钮、开关、指示灯；

7.3.2.4 如下内容应进行检查：

1 对操作站画面；

2 报表种类、形式、内容；

3 数据库格式、内容；

4 检查测试用的标准仪器；

5 依据的工程设计文件版本的有效性，设计变更；

6 系统工程文件；

7.3.2.5 验收完成，各方在测试报告签字。

7.3.3 现场验收

7.3.3.1 现场测试应在用户现场，在系统安装完毕后进行。

7.3.3.2 集成商应提供现场验收测试程序、测试内容及步骤，用户应进行审批。

7.3.3.3 现场测试应至少测试如下内容：

1 50% I/O 通道；

2 50% 逻辑功能；

3 每种冗余和容错功能；

4 每种在线插拔更换卡件；

5 辅助操作台按钮、开关、指示灯；

6 系统控制器负荷；

7.3.3.4 如下内容应进行检查：

1 依据的工程设计文件版本的有效性，设计变更。

2 系统安装；

3 系统布线；

4 系统工程文件

5 随机设备资料

7.3.3.5 现场验收测试完成，各方在测试报告签字。

7.4 联调

7.4.1 系统联调应在接线全部完成后进行。

7.4.2 施工单位应提供系统联调步骤，由用户审批。

7.4.3 应至少测试如下内容：

1 应对所有仪表设备进行 100%的连通测试；

2 应对所有联锁逻辑进行 100%联调测试。

7.4.4 现场联调完成，各方在测试报告签字。

7.5 确认

7.5.1 安全仪表系统投运使用前宜开展确认工作。

7.5.2 安全仪表系统的确认工作可包括下列内容：

1 安全仪表系统逻辑控制器验收测试发现的问题已经整改；

2 安全仪表系统的测量仪表、逻辑控制器、执行元件及其关联设备的安装与设置符合安全技术要求和工程设计文件；

3 安全仪表系统的联合调试符合安全技术要求和工程设计文件、设计变更；

4 安全仪表系统的供电、接地等符合工程设计文件;

5 安全仪表系统与基本过程控制系统的网络通信正常；

6 安全仪表系统的旁路、手动停车、复位功能正常；

7 安全仪表系统的相关技术文件完整、准确。

7.6 投运

7.6.1 系统投运应在系统确认后进行。

7.6.2 系统投运期间，SIS 供货商应派员保运，并检查、考核系统运行状态。

7.6.3 系统实际运行指标应符合设计要求和供货合同要求。

7.7 运行维护与变更管理

7.7.1 运行维护管理应包括制定运行维护程序、人员职责、定期检验测试计划及报告、停车期间的系统检查、允许旁路开关、维护旁路开关及操作旁路开关使用等。

7.7.2 变更管理应包括变更原因及方案、系统的版本升级、增减或修改逻辑、审核评估变更方案、确认变更的安全仪表功能、变更方案的设计与实施、变更逻辑功能的测试与验证、变更报告及运行维护程序更新等。

7.7.3 工艺装置变更后，应进行相应的安全评估，据此变更安全仪表功能。

7.7.4 应定期进行功能安全分析评估

7.7.5 运行维护和变更应记录归档。

8　文档管理

8.1.1 安全生命周期工程设计各阶段的文档应包括安全仪表系统的安全要求规格书、工程设计、应用程序组态、设计审查等文件，电子版文件和纸质文件应同时异地存档保存。

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

引用标准名录

下列文件对于本规范的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本规范。凡是不注日期的引用文件，其最新版本（包括勘误表）适用于本规范。

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 1 部分：一般要求

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 2 部分：电气/电子/可编程电子安全相关系统的要求

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 3 部分：软件要求

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 4 部分：定义和缩略语

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 5 部分：确定安全完整性等级的方法示例

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 6 部分：GB/T 20438.2 和 GB/T 20438.3 的应用指南

GB/T 20438.7/IEC 61508-7　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/Z 29638/ IEC/TR 61508-0　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/T 21109.1/IEC 61511-1　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、硬件和软件要求

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 2 部分：GB/T 21109.1 的应用指南

GB/T 21109.3/IEC 61511-3　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

附录 A　　安全仪表系统逻辑控制器技术规格书模板　（资料性附录）

附录 B　　安全仪表系统辅助操作台操作面板布置模板（资料性附录）

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

Design code for safety instrumented system in chemical industry

HG/T 22820—202×

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—202×，经工业和信息化部××××年×月×日以第××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、技术规范，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，仅供使用者参考。

2　术语与缩略语

2.1 术语

2.1.6 保护层　protection layer

化工厂或装置典型多保护层结构如图 1 所示：

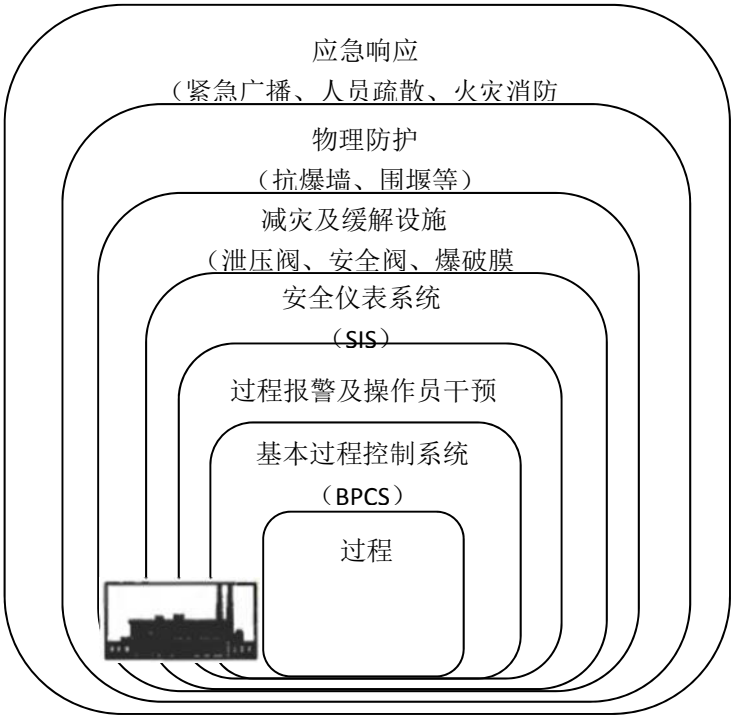

图 1 化工厂或装置的典型多保护层结构图

2.1.22 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　基础规定

3.1　安全生命周期

3.1.1 安全仪表系统的安全生命周期，是安全工程和安全功能存在的全过程。引用安全生命周期时间和阶段的目的，是为了确定实现功能安全目标所必要的管理活动，并进行策划与组织安排，以便在各阶段内有效实施，确保安全仪表系统的设计、安装、调试以及运行等满足总体功能安全的要求。

3.1.2，3.1.3 安全仪表系统的安全生命周期，包括从工程方案设计阶段安全仪表系统的设计策略，到操作维护阶段，直到安全仪表系统停用的全过程，涉及工程设计和安全仪表系统制造集成、建设、生产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、系统集成和操作维护的要求。

4　设计基本原则

4.1.3 化工装置的安全完整性等级最高为 SIL 3 级，不宜高于 SIL 2 级。如果在确定安全完整性等级时，有可能达到 SIL 3 或 SIL 4，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，使安全完整性等级一般不高于 SIL 2，不超过 SIL 3。

4.1.6 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。大型石油化工工厂的安全仪表系统应与基本控制系统的时钟同步。可采用时钟同步系统作为时钟源。

5　安全仪表系统组成

5.2　测量仪表

5.2.1　基本规定

5.2.1.2 测量仪表是安全仪表系统的组成部分，可采用计算低要求操作模式的平均失效概率的方法设计和验证测量仪表的安全完整性等级；也可根据经验使用原则，有实际证据证明这种测量仪表在以前的使用中有足够的安全完整性，就可确定选用该测量仪表符合相应的安全完整性等级。

5.2.1.3 安全仪表系统的测量仪表不宜采用现场开关量仪表，因为现场开关量仪表长期不动作，会出现触点黏合或接触不良，导致不动作或误动作，影响安全仪表的功能实现。

5.2.1.4 安全仪表系统的输入信号不应采用通信信号，包括采用 HART、FF、PROFIBUS-PA、MODBUS RTU、TCP/IP 等通信协议的通信信号。

5.3　执行元件

5.3.1 基本规定

5.3.1.3 安全仪表系统的最终元件为气动控制阀，执行安全仪表功能时，安全仪表系统优先动作。气动控制阀宜采用弹簧复位式单作用气动执行机构。采用双气缸执行机构时，宜配备空气储罐或专用供气管路。

5.3.1.4 最终元件是安全仪表系统的组成部分。可采用计算低要求操作模式的平均失效概率的方法设计和验证最终元件的安全完整性等级；也可根据经验使用原则，有实际证据证明这种最终元件在以前的使用中有足够的安全完整性，就可确定选用该最终元件符合相应的安全完整性等级。

5.3.2 控制阀附件的配置

5.3.2.1 调节阀带电磁阀配置示例见图 2。切断阀带电磁阀配置示例见图 3。

图中 SOV 为电磁阀。电磁阀励磁，A→B 通，阀开；电磁阀非励磁，B→C 通，阀关。

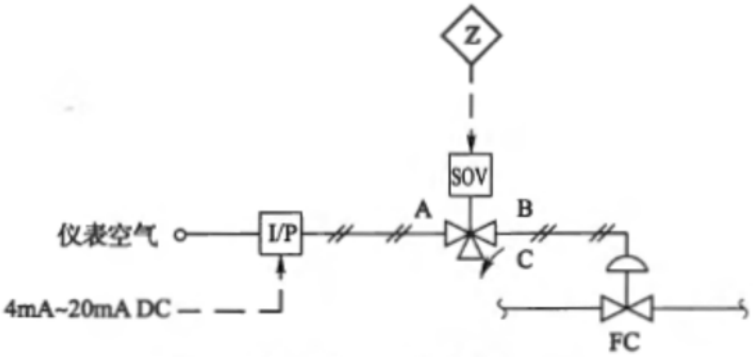

图 2 调节阀带电磁阀配置示例

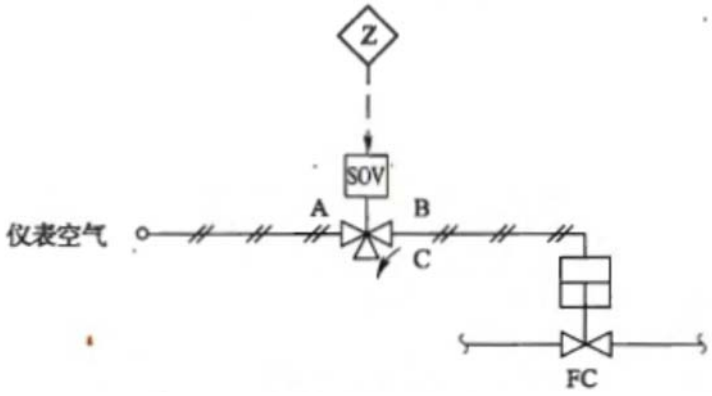

图 3 切断阀带电磁阀配置示例

5.3.2.1 安全仪表系统的电磁阀应优先选用耐高温(H 级)绝缘线圈，长期带电型，隔爆型。石油化工过程的最终元件的电磁阀以断电为故障安全方式。在工艺过程正常运行时，电磁阀应励磁工作。

5.3.2.4

（1） 当系统要求高安全性时，调节阀、切断配电阀带冗余电磁阀配置可选用图 4、图 5 所示配置方式。

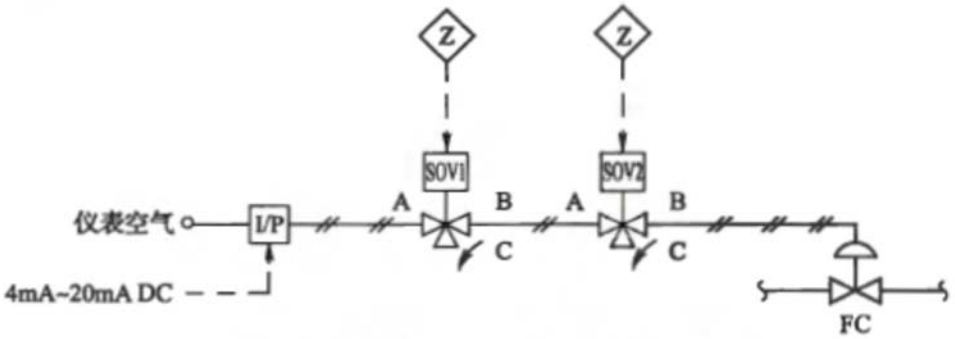

图 4 调节阀带冗余电磁阀配置示例

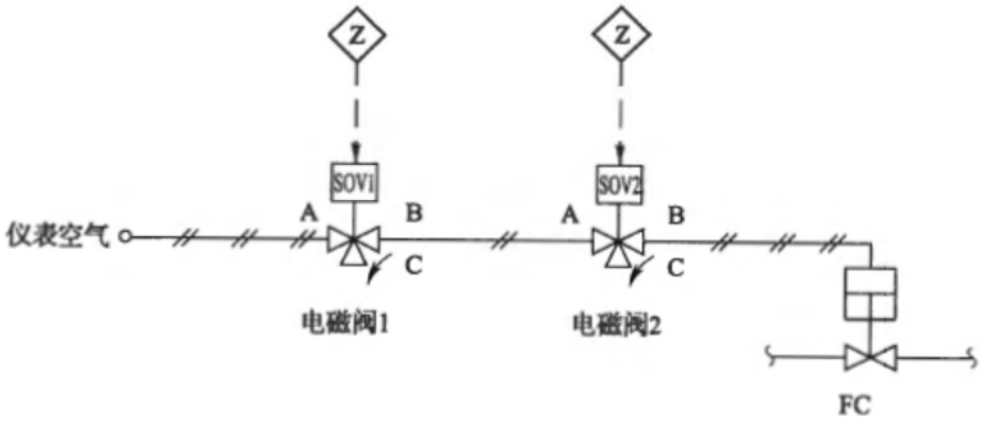

图 5 切断阀带冗余电磁阀配置示例

图中，当电磁阀 1 励磁，A→B 通；电磁阀 2 励磁，A→B 通，则控制阀开。当电磁阀 1 励磁，A→B 通；电磁阀 2 非励磁，B→C 通，则控制阀关。当电磁阀 1 非励磁，B→C 通；电磁阀 2 励磁，A→B 通，则控制阀关。当电磁阀 1 非励磁，B→C 通；电磁阀 2 非励磁，B→C 通，则控制阀关。

（2） 当系统要求高可用性时，调节阀、切断阀带冗余电磁阀配置可选用图 6、图 7 所示配置方式。

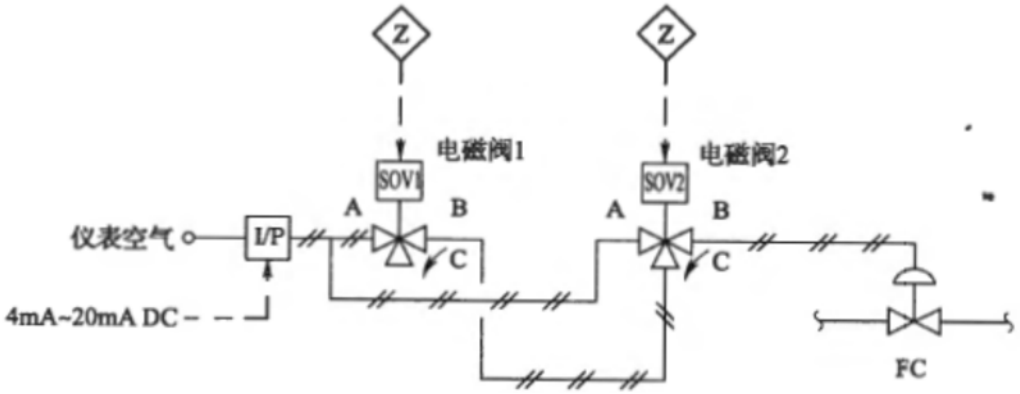

图 6 调节阀带冗余电磁阀配置示例

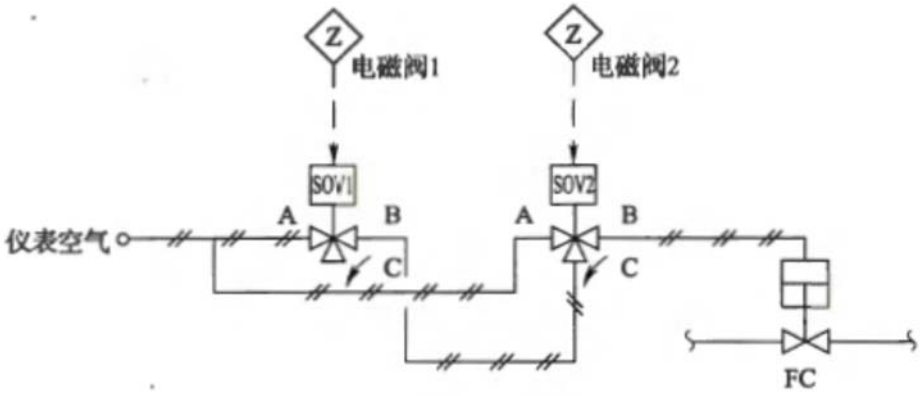

图 7 切断阀带冗余电磁阀配置示例

图中，当电磁阀 1 励磁，A→B 通；电磁阀 2 励磁，A→B 通，则控制阀开。当电磁阀 1 励磁，A→B 通；电磁阀 2 非励磁，B→C 通，则控制阀开。当电磁阀 1 非励磁，B→C 通；电磁阀 2 励磁，A→B 通，则控制阀开。当电磁阀 1 非励磁，B→C 通；电磁阀 2 非励磁，B→C 通，则控制阀关。

5.4 逻辑单元

5.4.3 逻辑控制器的响应时间包括输入处理时间、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。

5.4.13 逻辑控制器与基本控制系统时钟同步的目的是，当发生事故后，通过对两个系统各自记录的事件的对比和追溯，协助查找事故原因。

5.6 网络和通信接口

5.6.1 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。

5.7 人机接口单元

5.7.1 操作员站

5.7.1.1 安全仪表系统采用操作员站作信号报警的方式时，可在多台操作站报警，实现报警冗余。操作员站还可设置不同报警级别、多种报警显示、不同的报警音响，记录、存贮报警状态和相关数据，调用、显示、分析报警数据。

5.7.2 辅助操作台

5.7.2.5 当采用导线连接的常规信号超过一定距离时，为避免因线路衰减、电磁干扰等因素产生传输差错，可采用远程接口的方式利用系统内部的通信网络进行信号连接，实现准确、可靠的信号传输。

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、逻辑控制器、网络设备等应严格管理外部访问，防止计算机病毒侵入系统。

5.7.9 信息安全

5.7.9.4 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、逻辑控制器、网络设备等应严格管理外部访问，防止计算机病毒侵入系统。