备案号:J 1808—2014

中华人民共和国化工行业标准

HG/T 20511—2014
代替 HG/T 20511—2000

信号报警及联锁系统设计规范

Design code for signal alarm and interlock system engineering

2014-05-06 发布　　2014-10-01 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

信号报警及联锁系统设计规范

Design code for signal alarm and interlock system engineering

HG/T 20511—2014

主编单位：东华工程科技股份有限公司
批准部门：中华人民共和国工业和信息化部
实施日期：2014年10月1日

前　言

本规范根据工业和信息化部《关于印发2010年第一批行业标准制修订计划的通知》(工信厅科[2010]74号文)和中国石油和化学工业联合会《关于转发工业和信息化部办公厅〈关于印发2010年第一批行业标准制修订计划的通知〉的通知》(中石化联质发[2010]222号文)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东华工程科技股份有限公司等单位修订。

本规范自实施之日起代替《信号报警、安全联锁系统设计规定》HG/T 20511—2000。

本规范在原行业标准《信号报警、安全联锁系统设计规定》HG/T 20511—2000的基础上,由全国化工自动控制设计技术中心站组织我国自动化仪表行业专家,多次召开相关会议研讨、审查,并根据当前我国国民经济建设的政策方针,吸取近年化工系统在信号报警和联锁设计、施工和运行等方面的科研成果和实践经验,以及试行10多年来各单位的反馈意见进行修订。

本规范的主要技术内容:第1部分为信号报警系统,包括一般要求、发讯器、逻辑控制器、人机接口和报警顺序;第2部分为联锁系统,包括一般要求、传感器、逻辑控制器、最终元件、安全联锁系统硬件故障裕度要求、独立性要求、操作员站等。

本规范与HG/T 20511—2000相比,主要变化如下:

1. 增加了“术语和缩略语”章节;

2. 将原规定的信号报警系统中的“灯光显示单元”、“音响单元”、“按钮”、“用DCS/PLC实现的报警”章节归并为“人机接口”;

3. 删除“辅助输出”;

4. 将联锁系统的设计分为安全联锁系统和非安全联锁系统两种类型进行要求;

5. 增加联锁系统的“安全联锁系统的故障裕度要求”等章节内容。

本规范由中国石油和化学工业联合会提出并归口。

本规范的技术内容由东华工程科技股份有限公司负责解释。本规范在执行过程中如有意见和建议,请与东华工程科技股份有限公司联系(联系地址:安徽省合肥市望江东路70号,邮政编码:230024,电子邮箱:xujirong@chinaecec.com),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: 东华工程科技股份有限公司

参 编 单 位: 北京康吉森自动化设备技术有限责任公司
惠生工程(中国)有限公司

主要起草人: 徐继荣　马恒平　高生军　何　蓉　王明玉

主要审查人: 孙建文　于　锋　高　欣　王　颖　赵　柱　周一鸣
张同科　王秋红　董　萍　吴天一　周江萍

目　　次

Contents

1 总　　则

1.0.1 为了统一信号报警及联锁系统工程设计在化工行业的技术要求，推进信号报警及联锁系统工程设计的规范化，达到安全适用、技术先进、经济合理的目的，制订本规范。

1.0.2 本规范适用于化工装置新建、扩建及改建项目信号报警及联锁系统的工程设计。

1.0.3 信号报警及联锁系统的工程设计除应符合本规范要求外，尚应符合现行国家有关标准的规定。

2 术语和缩略语

2.1 术　　语

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

对来自过程的、与该系统相关设备的以及操作员的输入信号进行响应，并产生输出信号使过程及与该系统相关设备按要求方式运行的系统。该系统不应执行安全完整性等级大于或等于1的仪表安全功能。

2.1.2 开关量　digital variable

开关量是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”。

2.1.3 诊断覆盖率　diagnostic coverage

诊断测试检测的部件或子系统的失效率与总失效率之比。诊断覆盖率不包括由检验测试检测到的任何故障。

2.1.4 故障裕度　fault tolerance

在出现故障或误差时，功能单元继续执行要求功能的能力。

2.1.5 逻辑控制器　logic solver

本规范逻辑控制器是指执行一个或多个逻辑功能的设备，它既可以是一个基本过程控制系统的一部分，也可以是安全仪表系统的一部分。

2.1.6 最终元件　final element

本规范最终元件是指执行预先设定的动作，使过程达到预定状态的设备，如阀门、电机等，它是联锁系统的组成部分。

2.1.7 人机接口　human machine interface

本规范人机接口是指操作人员与信号报警联锁系统之间进行信息交换的手段，如操作员站、灯屏、音响、按钮、报警器、打印机等。

2.1.8 联锁系统　interlock system

当过程参数越限、设备等状态异常以及操作员输入信号时，执行预先设定要求的系统。联锁系统分为安全联锁系统和非安全联锁系统。联锁系统可由传感器和/或发讯器、逻辑控制器、最终元件及相关软件组成。

2.1.9 发讯器　message-sending device

输出开关量信号的设备

2.1.10 按钮　push button

按钮是只有一种稳定位置的状态器件。有软件按钮和硬件按钮两种。

2.1.11 冗余　redundancy

采用二个或多个部件或系统分别独立执行同一个功能，并且互为备用及切换。

2.1.12 信号报警系统 signal alarm system

以声、光等形式表示过程参数越限、设备等状态异常的系统。

2.1.13 失效 failure

功能单元执行某种功能能力的终止。

2.1.14 安全失效 safe failure

不可能导致安全仪表系统处于潜在危险状态或丧失功能的失效。

2.1.15 安全失效分数 safe failure fraction

导致安全失效或者可检测出的危险失效的装置总硬件随机失效率分数。

2.1.16 安全联锁系统 safety interlock system

安全完整性等级为1、2、3的安全仪表系统。

2.1.17 仪表安全功能 safety instrumented function

本规范仪表安全功能是指用一个或多个传感器、逻辑控制器、最终元件等实现的仪表安全保护功能，防止或减少危险事件发生或保持过程安全状态。

2.1.18 安全完整性等级 safety integrity level

用于规定分配给安全仪表系统的仪表安全功能的的安全完整性要求的离散量等级(SIL 1～SIL 4)。SIL 4是安全完整性最高等级；SIL 1是安全完整性最低等级。

2.1.19 安全仪表系统 safety instrumented system

用于实现一个或几个仪表安全功能的仪表系统。安全仪表系统可由传感器、逻辑控制器、最终元件及相关软件组成。

2.1.20 开关 switch

开关是具有两种稳定位置的状态器件。有软件开关和硬件开关两种。

2.2 缩 略 语

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

SFF —— safe failure fraction(安全失效分数)

SIF —— safety instrumented function(仪表安全功能)

SIL —— safety integrity level(安全完整性等级)

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

3 信号报警系统

3.1 一般要求

3.1.1 信号报警系统可由发讯器、逻辑控制器、人机接口组成。

3.1.2 参与联锁的过程参数应设报警，宜设预报警。

3.1.3 安全联锁系统的硬件和软件故障应设报警；BPCS 的硬件和软件故障宜设报警。

3.1.4 一般信号报警应在操作员站显示，重要信号报警除在操作员站显示外，宜在辅助操作台上设灯光显示单元和音响单元。

3.2 发 讯 器

3.2.1 发讯器输出的开关量信号宜为无源接点。

3.2.2 发讯器属于电气系统时，在信号引入逻辑控制器前宜采用信号隔离器、中间继电器等隔离设备进行信号隔离。

3.3 逻辑控制器

3.3.1 当 BPCS 采用常规仪表时，逻辑控制器宜采用单回路闪光报警器和/或拼装集成式闪光报警器。

3.3.2 当 BPCS 采用可编程电子装置时，逻辑控制器宜与 BPCS 的控制单元共用。

3.4 人 机 接 口

3.4.1 灯光显示单元的设计可分为下列两种情况：

1 当采用非视屏显示器时，灯光显示单元的设计应满足下列要求：

1）当信号报警系统中既有第一报警点又有一般报警点时，其灯光显示单元宜分开排列；

2）应用红色灯光表示越限报警或异常状态，黄色灯光表示预报警或非第一报警；

3）应用闪光、平光或熄灭表示报警顺序的不同状态；

4）应在灯光显示单元上标注报警点名称、报警程度和报警点位号。

2 当采用视屏显示器时，灯光显示单元的设计除满足本规范第 3.4.1 条第 1 款外，还应满足下列要求：

1）报警信息应包括报警参数当前值、报警设定值、文字描述及其他信息；

2）对于重要报警点，宜在辅助操作台上设置灯光显示单元。

注：视频显示器通常指操作员站显示器或大屏幕显示器等；非视频灯光显示单元通常指报警器灯屏、信号灯等。

3.4.2 音响单元的音量应高于背景噪声，在其附近区域应能清晰地听见。

3.4.3 音响单元可采用以下方式区分不同的报警区域、报警功能以及报警程度：

1 采用不同声音或音调的音响报警器；

2 通过改变声音振荡频率或振荡幅度。

3.4.4 按钮的设置应满足报警系统的功能需要，如试验按钮、消音按钮、确认按钮等。

3.4.5 当采用视屏显示器时，功能按钮宜采用显示于屏幕的“软件按钮”，也可采用操作键盘上的专用按键。

3.4.6 确认按钮宜采用黑色，试验按钮宜采用白色，其他功能按钮可根据具体情况采用合适的颜色。

3.4.7 当逻辑控制器采用可编程电子装置时，宜设置报警信息专用打印机。

3.4.8 报警信息的打印可手动触发，也可由报警信号自动触发。

3.5 报警顺序

3.5.1 应根据过程特点、操作要求及报警信号种类等选择报警顺序。

3.5.2 一般闪光报警顺序宜符合表 3.5.2 的规定。

表 3.5.2 一般闪光报警顺序

过程状态	灯光显示	音响	备注
正常	不亮	不响	
报警信号输入	闪光	响	
按动确认按钮	平光	不响	
报警信号消失	不亮	不响	运行正常
按动试验按钮	亮	响	试验、检查

3.5.3 区别第一信号的闪光报警顺序宜符合表 3.5.3 的规定。

表 3.5.3 区别第一信号的闪光报警顺序

过程状态	第一信号灯光显示	其他闪光显示	音响	备注
正常	不亮	不亮	不响	
第一信号输入	闪光	平光	响	有其他信号输入
按动消音按钮	闪光	平光	不响	
按动确认按钮	平光	平光	不响	
报警信号消失	亮	不亮	不响	运行恢复正常
按动复位按钮	不亮	不亮	不响	
按动试验按钮	亮	亮	响	试验、检查

3.5.4 区别瞬时信号的闪光报警顺序宜符合表 3.5.4 的规定。

表 3.5.4 区别瞬时信号的闪光报警顺序

过程状态		灯光显示	音响	备注
正常		不亮	不响	
过程状态		灯光显示	音响	备注
报警信号输入		闪光	响	
按动确认按钮	瞬时信号	不亮	不响	
	持续信号	平光	不响	
报警信号消失		亮	不响	无报警信号输入
按动试验按钮		亮	响	试验、检查

4 联锁系统

4.1 一般要求

4.1.1 联锁系统的设计应满足化工装置的试车、运行和联锁回路的调试、测试和维护等要求。

注:这些要求通常包括联锁的投入/解除、复位、强制等功能。

4.1.2 安全联锁系统的设计应满足 SIS 的安全要求规定。安全联锁系统的设计应满足 SIF 和 SIL 等级要求,并加以验证。

4.1.3 非安全联锁系统可设计为带电联锁。

4.1.4 安全联锁系统的设计应减少中间环节。

4.1.5 安全联锁系统宜设计成只要把过程置于某个安全状态,则该状态将一直保持到启动复位为止。

4.1.6 在安全联锁系统中实现不同 SIL 等级的 SIF 时,共享或共用的硬件和软件应符合较高 SIL 等级的要求。

4.1.7 安全联锁系统宜设计成失电联锁,如 SIS 的安全要求规定要求设计为带电联锁,则应配置电路完整性检测装置,并在系统内设置电路完整性丧失的报警和记录。

4.1.8 当安全联锁系统为本安系统防爆,并采用隔离型安全栅时,安全栅不宜采用底板供电方式。

注:底板是指带有电子电路的多路供电底板。

4.1.9 安全联锁系统在进行联锁解除、强制、测试、维护时,应采用系统存储器或打印输出设备进行自动记录,并在人机接口应有报警提示。

4.1.10 安全联锁系统的手动紧急停车硬件按钮信号,除引入逻辑控制器外,宜直接启动最终元件。

4.1.11 安全联锁系统中的冗余设备不宜采用同段母线供电。

4.1.12 当安全联锁系统和 BPCS 存在与 SIF 有关的共用设备时,该设备的供电电源应由安全联锁系统提供。

4.1.13 安全联锁系统的电缆宜采用阻燃型对绞屏蔽电缆,并独立设置。

4.1.14 安全联锁系统的电缆接线箱宜独立设置。

4.2 传 感 器

4.2.1 安全联锁系统的传感器宜采用 4mA～20mA 叠加 HART 信号传输的智能变送器,输出信号宜带故障模式输出。

4.2.2 当传感器选择开关量仪表时,开关应选择防抖动型开关。

4.2.3 当安全联锁系统采用冗余的传感器时,传感器可采用不同技术的产品。

4.2.4 当同一过程参数既需要 BPCS 的控制,又参与安全联锁系统的联锁时,则 BPCS 和安全联锁系统用于测量该参数的传感器可采用不同技术的产品。

4.2.5 安全联锁系统与 BPCS 的传感器不宜共用同一过程接口。

4.3 逻辑控制器

4.3.1 非安全联锁系统的逻辑设计可采用正逻辑，对于安全联锁的逻辑设计可采用负逻辑。

注：正逻辑是指联锁输入信号触发时为高电平或布尔量为“1”；负逻辑是指联锁输入信号触发时为低电平或布尔量为“0”。

4.3.2 当用于安全联锁的逻辑控制器采用可编程电子装置时，其设计、制造、认证等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 的有关要求。

4.3.3 用于安全联锁的安全栅、信号隔离器等应使用获得功能安全认证的产品。

4.3.4 安全联锁系统的逻辑控制器应与 BPCS 的时钟保持一致。

4.3.5 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。

4.3.6 冗余传感器的信号宜接入逻辑控制器的不同输入单元。

4.3.7 冗余最终元件的控制信号宜接自逻辑控制器的不同输出单元。

4.3.8 逻辑控制器的中央处理单元负荷不应超过其额定负荷的 50%。

4.3.9 逻辑控制器的内部通信负荷不应超过其额定负荷的 50%。

4.4 最 终 元 件

4.4.1 最终元件宜带有联锁动作的反馈输出。

注：对于控制阀，反馈输出为阀门的联锁位置；对于电机，反馈输出为电机的联锁状态。

4.4.2 当安全联锁系统与 BPCS 控制同一台阀门时，设计应保证安全联锁系统要求阀门的动作优先 BPCS 的要求。

4.4.3 当安全联锁系统的最终元件为阀门时，阀门宜采用气动执行机构。

4.5 安全联锁系统硬件故障裕度要求

4.5.1 当传感器、最终元件和非可编程电子逻辑控制器为故障安全型时，最低硬件故障裕度应满足表 4.5.1 中的要求，否则表 4.5.1 中的最低硬件故障裕度应加 1。

表 4.5.1 传感器、最终元件和非可编程电子逻辑控制器的结构约束

SIL	最低硬件故障裕度	SIL	最低硬件故障裕度	SIL	最低硬件故障裕度
1	0	2	1	3	2

4.5.2 可编程电子逻辑控制器的最低硬件故障裕度应满足表 4.5.2 中的要求。

表 4.5.2　可编程电子逻辑控制器的结构约束

SIL	最低硬件故障裕度		
	SFF＜60%	60%≤ SFF≤90%	SFF＞90%
1	1	0	0
2	2	1	0
3	3	2	1

4.5.3　安全联锁系统的子系统的最低硬件故障裕度大于或等于 1 时，当检测到硬件危险故障时，应报警，并记录，同时应执行与故障硬件相关的安全联锁动作或者在故障平均恢复时间内不能完成恢复，则执行与故障硬件相关的安全联锁动作。

4.5.4　安全联锁系统的子系统的最低硬件故障裕度为 0 时，当检测到硬件危险故障时，应报警，并记录，同时应执行与故障硬件相关的安全联锁动作。

4.6　独立性要求

4.6.1　安全联锁系统与 BPCS 之间应保持独立性，当它们之间存在共享设备时，应满足下列要求：

1　BPCS 的失效不应危及安全联锁系统的功能安全；

2　安全联锁系统的失效不宜导致 BPCS 失效；

3　对 BPCS 的任何操作不应对安全联锁系统产生任何危害。

4.6.2　当同一过程变量既需要 BPCS 的控制，又用于安全联锁系统的联锁时，用于检测该变量的传感器宜独立设置。

4.6.3　当 BPCS 的控制和安全联锁系统的保护由同一过程变量控制时，则控制阀不宜共用。

4.7　操 作 员 站

4.7.1　BPCS 与安全联锁系统共用操作员站时，操作员站的失效不应对仪表安全功能产生任何负面影响。

4.7.2　操作员站设置的开关和按钮应满足下列要求：

1　应加键锁或口令保护；

2　开关、按钮的动作应记录，并具有二次确认的操作；

3　开关状态应显示，并记录。

4.7.3　对于重要的联锁单元，操作员站应提供联锁逻辑回路画面，画面包括输入输出状态、逻辑关系、联锁旁路和设备维护状态、诊断结果等的显示、报警。

4.8　设备维护、测试开关的设置

4.8.1　设备维护、测试开关可采用下列方式设置：

1　对于安全联锁系统，可在安全联锁系统的操作员站设置软件开关，或在 BPCS 的操作员站设

置软件开关，开关的状态信号可采用通信方式与安全联锁系统连接；

2 对于非安全联锁系统，可在 BPCS 的操作员站设置软件开关；

3 可在机柜设置硬件开关。

4.8.2 当设置了设备维护开关时，每个联锁单元宜在辅助操作台上设“允许”开关，在“允许”条件下，维护开关才有效，“允许”开关宜采用红色带钥匙开关。

4.8.3 当设置了设备测试开关时，应在现场设置设“允许”开关，在“允许”条件下，测试开关才有效。

4.8.4 设备处于维护状态所用的时间应在操作员站上显示。

4.8.5 当设备维护开关为硬件开关时，应设置维护状态反馈黄色硬件指示灯。

4.8.6 维护、测试状态和“允许”状态应在操作员站显示，并记录。

4.8.7 维护、测试开关动作和“允许”开关动作应在操作员站记录。

4.8.8 维护开关宜采用黄色开关，测试开关宜采用红色开关。

4.9 联锁旁路开关的设置

4.9.1 联锁旁路开关可采用下列方式设置：

1 对于安全联锁系统，可在安全联锁系统的操作员站设置软件开关，或在 BPCS 的操作员站设置软件开关，开关的状态信号可采用通信方式与安全联锁系统连接；

2 对于非安全联锁系统，可在 BPCS 的操作员站设置软件开关；

3 可在辅助操作台设置硬件开关，开关宜采用黄色带钥匙开关。

4.9.2 当工艺过程变量从原始自然值变化到工艺条件正常数值，联锁信号状态发生改变的，宜设置联锁旁路开关。

4.9.3 联锁旁路开关状态应在操作员站显示，并记录。

4.9.4 联锁旁路开关动作应在操作员站记录。

4.10 联锁复位按钮的设置

4.10.1 联锁复位按钮可采用下列方式设置：

1 对于安全联锁系统，可在安全联锁系统的操作员站设置软件按钮，或在 BPCS 的操作员站设置软件按钮，开关的状态信号可采用通信方式与安全联锁系统连接；

2 对于非安全联锁系统，可在 BPCS 的操作员站设置软件按钮；

3 可在辅助操作台设置硬件按钮。

4.10.2 联锁复位状态应在操作员站显示，并记录。

4.10.3 联锁复位按钮动作应在操作员站记录。

4.10.4 联锁复位按钮宜采用灰色按钮。

4.11 紧急停车按钮的设置

4.11.1 非安全联锁系统的紧急停车按钮可在 BPCS 操作员站上设置软件按钮实现，安全联锁系统的紧急停车按钮应在辅助操作台上设置硬件按钮实现。

4.11.2 在辅助操作台设置的硬件按钮应引入联锁系统的逻辑控制器，并在系统内设置状态报警并

记录。

4.11.3 紧急停车按钮不应设维护开关。

4.11.4 紧急停车按钮应采用红色蘑菇头按钮，并带防护罩。

4.12 工程师站及事件顺序记录站

4.12.1 安全联锁系统应设工程师站。

4.12.2 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联锁系统动作和诊断状态。

4.12.3 安全联锁系统应设事件顺序记录站。当安全联锁系统设置了独立的操作员站时，事件顺序记录站宜与操作员站共用。当安全联锁系统没有设置独立的操作员站时，事件顺序记录站可与安全联锁系统的工程师站共用，也可单独设置。

4.12.4 事件顺序记录站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。

4.12.5 工程师站和事件顺序记录站宜设置防病毒等保护措施。

4.12.6 工程师站和事件顺序记录站宜采用台式计算机。

本规范用词说明

1 为便于在执行本标准条文时区别对待，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 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

《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—2007

中华人民共和国化工行业标准

信号报警及联锁系统设计规范

HG/T 20511—2014

条 文 说 明

目　　次

修 订 说 明

《信号报警及联锁系统设计规范》HG/T 20511—2014，经工业和信息化部2014年5月6日以第32号公告批准发布。

本规范是在《信号报警、安全联锁系统设计规定》HG/T 20511—2000的基础上修订而成，上一版的主编单位是中国东华工程公司，主要起草人员：王浩、章敦辉、任广东。

本规范修订过程中，编制组参照国家标准《过程工业领域安全仪表系统的功能安全》GB/T 21109—2007和《电气/电子/可编程电子安全相关系统的功能安全》GB/T 20438—2006的要求，进行了广泛的调查研究，总结了国内近几年来化工装置信号报警及联锁系统设计中的实践经验，同时参考了国外先进技术法规、技术标准。

为便于广大设计、施工、科研、学校等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，《信号报警及联锁系统设计规范》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规范规定的参考。

3 信号报警系统

3.3 逻辑控制器

3.3.1 单回路闪光报警器、拼装集成式闪光报警器为定型产品，这类产品已将信号报警逻辑和声、光报警进行了集成。

3.4 人机接口

3.4.4 不同的报警顺序需要不同数量的按钮。各按钮的功能应满足下列要求：

1 确认按钮：表明操作人员确认了一个新的报警，并消除音响声音；

2 消音按钮：消除音响声音，但不影响灯光显示方式；

3 复位按钮：如报警信号消失，按动该按钮使该点恢复到正常状态；

4 试验按钮：用于检查音响和全部回路是否完好。

3.4.7 非针式打印机，如激光、喷墨打印机通常是页打印，只有一条报警信息，也会走一整页打印纸。

4 联锁系统

4.1 一般要求

关于过程工业的安全仪表系统的国家标准《过程工业领域安全仪表系统的功能安全》GB/T 21109—2007 涉及从初始概念、设计、实现、运行、维护直到停用的所有安全生命周期阶段的工作，本规范是工程设计规范，工作重点是 SIS 的设计工作，即是 SIS 的安全生命周期的一个阶段的工作，为了避免与其他有关标准相冲突，本规范将 SIS 的安全完整性（包括硬件系统完整性和系统安全完整性）设计定义为安全联锁系统的设计。

SIL 4 在化工行业的应用是极少的，其应用有很多附加要求。考虑到本规范的通用性，没有将 SIL 4 的 SIS 设计要求纳入本规范。

国家标准《过程工业领域安全仪表系统的功能安全》GB/T 21109—2007 定义仪表安全功能的操作模式有要求模式和连续模式两种。化工行业中的大多数应用在要求不是很频繁的情况下都使用要求操作模式，这类情况下，SIF 的 SIL 应根据 GB/T 21109.1—2007 表 3“安全完整性等级：要求时的失效概率”的数据确定。当应用要求很频繁（例如要求率每年大于 1），这类应用可当作连续操作模式，SIF 的 SIL 应根据 GB/T 21109.1—2007 表 4“安全完整性等级：SIF 的危险失效频率”的数据确定。

4.1.1 这些要求通常包括联锁的投入/解除、复位、强制等功能。

4.1.2 SIS 的安全要求规定是通过对过程及相关设备的危险和风险评估和给保护层分配的仪表安全功能及相关的安全完整性等级中得到的，它是为了达到所要求的安全功能，而对每个 SIS 回路的 SIF 和相关安全完整性进行要求的描述。

SIS 的安全要求规定是自控专业进行安全联锁设计的输入条件，包括下列方面的内容：

1 达到要求的功能安全所必需的所有 SIF 的描述；

2 对每个 SIF 的过程安全状态的定义；

3 每个 SIF 的 SIL 等级和操作模式的要求；

4 失效模式和要求的 SIS 响应（如报警、自动停机）的要求；

5 SIS 使过程进入安全状态的响应时间的要求；

6 SIS 过程测量和它们的停车点的要求；

7 SIS 过程输出动作及其成功操作判据的描述；

8 SIS 过程输入和输出之间的功能关系，包括逻辑功能、数学功能等；

9 与启动和重新启动 SIS 程序有关的任何特殊要求；

10 与带电或断电停车的有关要求；

11 人工停车要求；

12 联锁的投入/解除、复位、强制的要求；

13 SIS 与其他系统(包括 BPCS 和操作员)之间的接口要求;

14 识别和考虑共同原因失效的要求;

15 检验测试间隔时间要求;

16 SIS 故障平均修复时间要求;

17 对任何能经受一次重大意外事故的 SIF 的要求的定义(如定义在一次火灾事故中阀门保持可操作性的时间的要求)。

4.1.3 非安全联锁一般用于安全性要求不高的场合,联锁设计成带电联锁,主要是从延长设备寿命、降低能耗的角度考虑的。

4.1.5 复位一般采用操作员手动动作实现,不采用自动复位,因为自动复位启动过程时可能产生潜在的危险。当安全联锁系统执行多个动作,联锁复位执行时各最终元件也应保持在安全状态,再根据工艺操作手册分步启动最终元件。

4.1.7 带电联锁指过程达到或超过联锁设定点时,联锁系统带电动作。如电磁阀,当过程正常时,电磁阀不带电,当联锁动作时,电磁阀带电。

4.1.10 对于要求按顺序停车的场合,一般有多个最终元件,最终元件的启动是按一定的逻辑顺序先后启动的,所以对于这类场合,手动停车信号一般不用于直接启动最终元件。

4.1.11 此条中的"母线"是指安全联锁系统内部的供电系统,而非电气专业的配电系统。当安全联锁系统设有冗余的配电系统时,冗余设备的电源应引自不同的配电系统。例如从 UPS 引出的两路电源分别构成两套独立的配电系统时,则控制器的冗余电源卡的输入电源应引自不同的配电系统。

4.2 传 感 器

4.2.1 对于非机械式开关型仪表,一般具有故障模式,如继电器输出,仪表故障时,继电器去磁;如晶体管输出,仪表故障时,晶体管截止。对于模拟信号输出的智能仪表,一般也具有故障模式,当仪表故障时,输出信号低于或高于仪表的正常输出范围 4mA～20mA,如 3.2mA 或 21.6mA。

4.2.3、4.2.4 条文中要求采用不同技术的产品是为了避免共因失效,"不同技术的产品"通常指不同类型的仪表或同一类型不同生产厂家的产品或同一类型同一生产厂家不同系列的产品等。

4.3 逻辑控制器

4.3.1 安全联锁系统的逻辑设计采用负逻辑,主要是从以下方面考虑的:

1 当传感器采用开关量仪表时,开关一般都选择常闭型,即正常时闭合,达到联锁设定点时断开,即联锁输入信号触发时布尔量为"0";

2 逻辑控制器的初始状态或故障状态时,软件中的布尔量为"0"。

4.5 安全联锁系统硬件故障裕度要求

规范中定义的硬件最低故障裕度要求是为了减轻 SIF 设计中的潜在缺陷,这些潜在缺陷可能是由于 SIF 设计中所作的假设的数量,以及在各种过程应用中使用的部件或子系统故障率的不确定所导致的。

4.5.1 对于传感器,故障安全型通常指断电、CPU 故障、断线时,传感器传输的信号可以执行联锁

动作，使设备/单元/装置等达到安全状态；对于最终元件，故障安全型通常指断电、断气、断信号时，最终元件的状态或位置应该为设备/单元/装置处于安全状态；非可编程逻辑控制器，通常为用继电器构成的逻辑电路，故障安全型是指断电联锁。

4.5.4 现行国家标准《过程工业领域安全仪表系统的功能安全》GB/T21109.1—2007 第 11.3.2 条规定在要求模式时，硬件故障时可以执行联锁动作，也可以在平均恢复时间内联锁不动作，但需要有附加的措施或约束；现行国家标准《过程工业领域安全仪表系统的功能安全》GB/T21109.1—2007 第 11.3.3 条中规定在连续模式时，硬件故障时就应执行联锁动作。考虑到前者要求的附加措施或约束，在实际应用中很难实现或很难判断其有效性，本规范从安全性角度出发，规定在故障裕度为 0 时，硬件故障时即执行联锁动作。

4.6 独立性要求

4.6.2 在安全联锁设计时应尽量避免采用同一过程变量既需要 BPCS 的控制，又用于安全联锁系统的联锁，因为 BPCS 的失效，很可能是因为工艺原因使传感器失效，如堵塞，即使传感器独立设置，安全联锁系统的传感器也会因共因失效原因而失效。

4.8 设备维护、测试开关

4.8.1 设备维护开关是用于传感器的维护，当维护开关处于有效状态时，传感器的信号不会引起联锁动作；设备测试开关是用于最终元件的测试，当测试开关处于有效状态时，最终元件会执行联锁动作，但该动作不会影响装置、转动设备的正常运行。

4.9 联锁旁路开关的设置

4.9.1 联锁旁路开关处于有效状态时，联锁信号的触发不会引起联锁动作。

4.12 工程师站及事件顺序记录站

4.12.1 工程师站用于安全联锁系统组态编程、系统诊断、状态监测、编辑、修改及系统维护。