ICS 71.120.01
CCS C4090

团　　体　　标　　准

T/CAMETA 001011-2022

化工安全仪表系统管理规范

Management standard of safety instrumented systems in chemical industry

2022-07-25 发布　　2022-12-01 实施

中　国　机　电　一　体　化　技　术　应　用　协　会　　发　布

目　　次

前　言

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

本文件由中国机电一体化技术应用协会工程技术发展中心组织，中海油惠州石化有限公司、中石油华东设计院有限公司会同浙江中控技术股份有限公司等有关单位组成标准编写组共同编制完成。

本文件在编制过程中，认真贯彻落实国家关于安全仪表系统的有关法律法规、标准规范的要求，广泛调研化工、炼油、煤化工等领域安全仪表系统使用与维护单位的意见；并认真总结实践经验教训，在参考国内外技术标准的基础上多次审查后定稿。

本文件按照安全仪表系统安全生命周期的理念起草编制，共分16章和3个资料性附录，主要包括：危害和风险评估、设计管理、采购管理、逻辑控制器集成、安装调试、安全确认、生产运行管理、变更管理，检修改造、退役、文档信息管理、人力管理。

本文件由中国机电一体化技术应用协会工程技术发展中心负责日常管理，本文件编制组负责具体技术内容的解释。执行过程中若有意见或建议，请联系中国机电一体化技术应用协会工程技术发展中心，以便今后修订时参考。

本文件日常管理单位：中国机电一体化技术应用协会工程技术发展中心

通讯地址：北京市通州区临河里华业东方玫瑰A区B座1110室

邮政编码：101101

电　　话：010-58410001

传　　真：010-53020787

电子邮件：15810867686@126.com

本文件主编单位：中海油惠州石化有限公司

中石油华东设计院有限公司

本文件参编单位：浙江中控技术股份有限公司

施耐德电气（中国）有限公司

聊城市鲁西化工工程设计有限责任公司

鲁西化工集团股份有限公司

北京安稳优自动化技术有限公司

本文件参加单位：江苏新晖测控科技有限公司

本文件主要起草人员：王少勇 林洪俊 左信 徐丽 俞文光 王刚 邱杰

本文件主要审核人员：赵峻松 赵亮 于世恒 钱福群 荣红焕 肖光 李迎涛 李勇贤 杨绍军 赵国荣 张军录 葛涛 李艳芳 殷卫兵 魏兴军 曹志晔 张泽宇 刘伟 曹俊 李涛 孙福生 王成舫 刘彦昌 张斌 张龙 周明军 朱文辉 陆兴旺 武东升 张会国 柴平海 姜志有 苗立民 王鑫 陆新宇 刘利 赵瑛 朱瑞苗 周秀清 李传芳 赵轩　张云东 陈鑫 王宇翔 张习钊

化工安全仪表系统管理规范

1 范围

本文件规定了安全仪表系统的安全生命周期管理的内容、要求、方法。

本文件适用于化工、石化企业新建、改建、扩建、在役安全仪表系统管理。

除执行本文件外，尚应符合国家现行有关法律、规范、标准的要求。

2 规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 21109（所有部分） 过程工业领域安全仪表系统的功能安全

GB/T 50770 石油化工安全仪表系统设计规范

GB/T 20945-2013 信息安全技术 信息系统安全审计产品技术要求和测试评价方法

3 术语和缩略语

下列术语和缩略语适用于本文件。

3.1 术语

3.1.1

伤害 harm

对人体健康的损伤或损害，或对财产或环境的损害。

3.1.2

危害 hazard

伤害的潜在来源。

注：包括可导致人员、财产、环境短期或长期伤害或破坏的事件、场景；其中人员伤害包括短时间内对人员的危险和对人体健康的长期影响。

3.1.3

危害事件 hazardous event

可以导致伤害的事件。

3.1.4

风险 risk

发生伤害的可能性及该伤害严重性的组合。

注：伤害的可能性，包括出现危害事件、危害情景的可能性和避免及限制伤害的可能性。

3.1.5

保护层 protection layer

通过控制、预防或缓解来降低风险的独立的系统、设备或行动。

3.1.6

安全 safety

摆脱不可容忍的风险。

3.1.7

安全功能 safety function

针对特定的危害事件，为达到或维持过程的安全状态，由一个或多个保护层实现的功能。

注 1：分仪表功能和非仪表功能，非仪表功能中的安全功能也是风险消减的方法；

注 2：仪表功能分安全仪表功能和其他通过仪表进行风险消减的方法。

3.1.8

安全仪表功能 safety instrumented function（SIF）

由安全仪表系统（SIS)实现的安全功能。

注 1：SIF 旨在设计实现要求的 SIL，即定义与其他用于消减同一风险的保护层之间的关系；

注 2：SIF 用于保护人员、财产、环境。

3.1.9

安全仪表系统 safety instrumented system（SIS）

用于实现一个或多个安全仪表功能的仪表系统。

注1：安全仪表系统由硬件、软件组成，硬件包括传感器、逻辑控制器、最终元件及通讯网络设备和辅助操作台等附属设备，软件包括应用程序、嵌入式软件和工具软件；

注2：安全仪表系统，可包括作为SIF一部分的人的行为干预；

注3：安全联锁系统、紧急停车系统可参照安全仪表系统管理；

注4：本文件不涉及可燃气体和有毒气体检测报警系统、火灾自动报警系统的管理。

3.1.10

SIS 安全生命周期 SIS safety life cycle

从项目概念定义或可研阶段开始到所有 SIF 停用为止所发生的、包含在 SIF 实现中的必要活动。

3.1.11

功能安全 functional safety

与工艺过程和 BPCS 相关的整体安全的一部分，且依靠 SIS 和其他保护层的正确工作。

3.1.12

功能安全评估 functional safety assessment（FSA）

基于证据的调查，以判定由一个或多个 SIS 和/或其它保护层实现的功能安全。

3.1.13

安全完整性 safety integrity

当作为安全仪表功能和有安全仪表功能要求时，SIS 执行要求的 SIF 的能力。

注 1：能力，包括功能响应和 SIS 按要求动作的可能性；

注 2：安全完整性，是一个安全概念而不是一个经济性概念，所以不用“SIS 满足 SIF 要求的可靠性”表达；

注 3：安全完整性包括硬件、软件、管理三个方面，由硬件安全完整性和系统安全完整性组成，也包括硬件安全完整性和系统安全完整性关联导致的错误。

3.1.14

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（1-4 的 4 个等级中的一个，SIL 1 为最低等级，SIL 4 为最高等级）。

3.1.15

安全要求规格书 safety requirements specification（SRS）

对安全仪表功能（SIFs）及其安全完整性等级做功能要求的规格书。

3.1.16

防卫 security

针对 SIS 硬件、软件进行的故意攻击或非故意人为错误造成的威胁的防护。

3.1.17

确认 validation

通过检查和提供客观证据，确认用于某个规定用途的特定要求得到了满足。

注：在 SIF 分配和 SIS 安装调试完成后，应确认 SIS 符合 SRS 的要求。

3.1.18

验证 verification

通过检查和提供客观证据确认要求已经满足。

注：SIS 安全生命周期各阶段，通过分析和测试证明特定的输入、输出，在各方面应满足该阶段的目标和要求。

3.1.19

检验测试 proof test

为检测 SIS 隐性错误带来的危险而进行的定期测试，以便必要时通过维修把系统复原到“新的”状态或实际上接近这种状态。

3.1.20

变更管理 management of change

与 SIS 相关的永久或暂时性变化、修改，规范进行计划、审批、实施、控制，以保障要求的安全完整性。

3.1.21

风险管理 risk management

基于风险评估来辨识和确定风险控制的优先顺序和安全风险控制措施，以达到安全生产条件、减少和避免生产安全事故的目标。

3.1.22

安全审计 security audit

对事件进行记录和分析，并针对特定事件采取相应比较的动作。

注：事件，试图改变目标状态并造成或可能造成损害的行为的发生。

3.1.23

故障 fault

内部情况或状态的原因，已无能力执行要求的功能。

注 1：失效造成的故障，原因为故障项目自身，或者为生命周期前一阶段的缺陷，如规格书、设计、制造、维修；

注 2：特殊情况下，一个设备故障可以导致一次失效。

3.1.24

失效 failure

执行要求的功能的能力终止或丢失。

注 1：一个设备的失效是一个导致该设备故障状态的事件；

注 2：要求的功能包括确定的行为，和通过应避免的行为来规定的某些功能，应避免的行为的出现就是失效；

注 3：失效是随机的和系统的。

3.1.25

经使用证明 proven in use

针对一个组件的特定配置，基于对其运行经验的分析，证明其危险的系统性故障的可能性低到足够可以保证每个使用该组件的安全功能达到其要求的安全完整性等级。

注 1：经使用证明，应基于制造商的设计基础，例如温度范围、振动极限、腐蚀极限、期望的维修支持等。

3.1.26

以往使用 prior use

基于以往类似操作环境的操作使用经验，用户通过文档评估可以实现要求的功能和满足安全完整性要求的设备适合在SIS中使用。

注1：通过设计、检验、维修、操作经验等可以判断操作环境是否类似或一致；

注2：实际安装使用环境与设计基础不同时，可以通过以往使用评估。

3.1.27

承包商 contractor

在企业的工作场所按照双方协定的要求向企业提供服务的个人或单位。

3.1.28

安全关键设备 safety critical equipment

可提供独立保护层降低场景风险等级或可将场景的风险由“不可接受风险”转变为“可接受风险”的过程控制设备。

3.1.29

嵌入式软件 embedded software

作为系统组成部分由制造商提供且最终用户不能修改的软件，也称固件或系统软件。

注：包括传感器（智能仪表）、逻辑控制器、最终元件（智能执行器）的系统软件。

3.1.30

工具软件 utility software

用来创建、修改、编写应用程序的软件工具。

3.1.31

应用程序 application program

专用于用户应用的程序；通常包含逻辑顺序、许可、限制和表达式，通过控制输入、输出、计算和必要的决策而达到SIS功能要求。

3.1.32

组态 configuration

将监控过程有关数据和所需要的控制规律,按照控制系统或仪表工具软件或嵌入式软件的功能模块和数据规则输入到控制系统或仪表中，使控制系统或仪表具有完成特定监控对象的监控任务的功能；控制系统组态还包括硬件和系统网络的配置。

3.1.33

现场仪表 field instrument

安装在生产或操作现场，与SIS有信号连接的检测仪表和执行器；本文件简称仪表。

注：包括传感器、最终元件和开关按钮等。

3.1.34

存档 document archiving

把制度、文件、协议合同、纪要、报告、记录、档案、资料等进行档案化分类、整理、保存、管理。

3.2 缩略语

SIS	安全仪表系统	Safety Instrumented System
SIL	安全完整性等级	Safety Integrity Level
SIF	安全仪表功能	Safety Instrumented Function
PFDavg	需求时的平均危险失效概率	Average Probability of Dangerous Failure on Demand
PFD	需求时的危险失效概率	Probability of Dangerous Failure on Demand

PFH	每小时危险失效概率	Probability (average frequency of dangerous failures) of Failure per Hour
PID	管道和仪表流程图	Piping and Instrumentation Diagram
PHA	过程危害分析	Process Hazards Analysis
H&RA	危害和风险评估	Hazard and Risk Assessment
HAZOP	危害与可操作性	Hazard and Operability
LOPA	保护层分析	Layer of Protection Analysis
SRS	安全要求规格书	Safety Requirements Specification
FDS	功能设计规格书	Functional Design Specification
FAT	工厂验收测试	Factory Acceptance Testing
BPCS	基本过程控制系统	Basic Process Control System
SAT	现场验收测试	Site Acceptance Testing
CPU	中央处理器	Central Processing Unit
FAR	现场机柜间	Field Auxiliary Room
CCR	中心控制室	Central Control Room
SOE	事件顺序记录	Sequence of Event
HMI	人机接口	Human Machine Interface
MCC	电机控制中心	Motor Control Centre
TI	检验测试时间间隔	Test Interval
PST	部分行程测试	Partial Stroke Test
ALARP	尽可能低合理可行	As Low As Reasonably Practicable

4 一般规定

4.1 SIS 安全生命周期管理

4.1.1 应按照SIS安全生命周期制定安全仪表系统管理制度，制度体系宜包括管理范围、相关部门及人员、职责分工、管理内容或基本要求、工作流程或程序等；典型的SIS安全生命周期及各阶段管理要求可参考表1；

表1 典型的SIS安全生命周期及各阶段管理基本要求

安全生命周期阶段		基础或条件	目标要求	结果或动作	对应章节	备注
1	危害和风险评估	工艺设计或PID确定，安全目标确定。	确定工艺过程和相关设备的危害及危害事件，确定工艺过程风险，明确风险消减措施及安全功能要求。	列出危害，说明要求的风险消减措施和安全功能。	第5章	基础设计或其他阶段
2	基础设计	可研审批完成，工艺包或总体设计完成。	确定SIS基本的技术要求和系统结构。	基础设计询价文件或数据表，初版SRS。	第6.2条	
3	安全功能分配到保护层	要求的SIF及其安全完整性要求。	给保护层分配安全功能，为每个SIF确定安全完整性等级。	确定所有SIF的SIL（SIL定级）。	第6.2.2条	基础设计阶段

表1 典型的SIS安全生命周期及各阶段管理基本要求（续）

安全生命周期阶段		基础或条件	目标要求	结果或动作	对应章节	备注
4	安全要求规格书	安全要求已分配。	详细规定SIF及其SIL、SIS的要求，以实现要求的功能安全。	SIS的安全要求，应用程序的安全要求。	第6.3条	详细设计阶段
5	详细设计	基础设计完成，SIL定级完成。	设计、规定SIS以实现SIF及其SIL的要求。	详细设计询价文件或数据表。	第6.4条	
6	采购	详细设计询价文件或数据表。	购买符合详细设计要求的SIS。	签订技术协议和商务合同，监造。	第 7 章	第7.4条SIL验证
7	集成	逻辑控制器采购合同签订。	按照采购合同制造集成逻辑控制器及其成套仪表。	硬件及应用程序设计制造、FAT。	第 8 章	采购阶段
8	安装调试	设计制造完成，现场验收或接收。	按照图纸现场安装，SIS及SIS的每个设备可按设计要求操作使用。	校验、安装、测试、试验结果。	第 9 章	
9	安全确认	SIS的安全确认计划。	安装调试后的SIS及其SIFs可实现SRS的要求。	SIS的全部功能符合SIS的安全要求。	第 10 章	也称SAT
10	生产运行	SIS的安全要求及其操作维护计划。	操作维护过程中维持SIS的功能安全。	操作、维护、变更行为，应急、风险、防卫管理。	第11、12章	
11	检修改造	SIS的检修、改造计划。	检修后可维持、改造后可增强SIS的功能安全。	检验、测试、维修结果，改造测试行为。	第 13 章	
12	退役	安全要求和累积的工艺过程信息。	退役之前要求的SIFs可维持操作运行。	不再使用不满足功能安全要求的SIF。	第 14 章	

4.1.2 应按照SIS安全生命周期制定安全计划，明确相应阶段的要求、措施、组织或人员等内容；

4.1.3 应用程序的安全生命周期，宜包括应用程序安全要求、安全验证计划、设计、方法、修改规程、审核测试等，涉及逻辑修改的应按照变更管理审批；

4.1.4 应按照安全计划验证并将验证结果存档；

4.1.5 在役SIS应定期进行功能安全评估和功能安全审计，验证SIS的实际性能是否与预期性能存在差异，并依据评估审计结果更新安全计划。

4.2 其他基本要求

4.2.1 应按照功能安全评估报告、验证报告、设计文件、检验测试周期，制定安全仪表系统维护计划；

4.2.2 工艺过程更改时，安全仪表系统应根据功能安全评估报告进行更改、验证；

4.2.3 对SIS进行系统结构修改时，应进行评估、验证，安全完整性等级应满足原要求；

4.2.4 对SIS设备进行更换时，其安全完整性等级不应低于原设备；同厂家同型号原备件可直接更换，否则应进行功能安全评估或变更审批。

5 危害和风险评估

5.1 项目建设期

5.1.1 应参与项目建设期的危害和风险评估（H&RA）；
5.1.2 应参与识别涉及仪表专业的现有风险；
5.1.3 应参与确认涉及仪表专业的建议风险消减措施；
5.1.4 应跟踪涉及仪表专业的建议风险消减措施的落实关闭；
5.1.5 标准设计、简单工艺可采用故障假设分析（What-if）、检查表（Checklist）等方法进行，复杂工艺宜采用HAZOP分析进行危害和风险评估；
5.1.6 涉及“两重点一重大”和首次工业化设计的建设项目，应在基础设计阶段进行HAZOP分析评估；
5.1.7 按照第15章相关要求存档危害和风险评估报告。

5.2 SIS 安全生命周期其他阶段

5.2.1 应参与SIS安全生命周期其他阶段、按法律法规要求或其他临时要求进行的危害和风险评估，并应参与执行H&RA后更新的安全计划；
5.2.2 涉及“两重点一重大”的在役生产、存储装置，宜每3年进行一次HAZOP分析评估；
5.2.3 应配合PHA小组进行SIS安全生命周期各阶段的危害和风险评估的验证；
5.2.4 按照第15章相关要求存档危害和风险评估报告。

6 设计管理

6.1 一般规定

6.1.1 应对工程设计进行计划管理、技术管理、质量管理；
6.1.2 应对工程设计提出设计基本要求，应对设计统一规定进行审核；
6.1.3 设计基本要求或设计统一规定，应就SIS的应用环境、可靠性原则、可用性原则、配置要求、操作方式、技术规格等提出具体的针对性要求；
6.1.4 应参加危害和风险评估；
6.1.5 应对设计文件进行审查；
6.1.6 设计单位应参加功能设计审查、工厂验收并配合应用程序组态调试；
6.1.7 应组织设计单位进行详细设计交底；
6.1.8 应协调设计单位提交设计变更；
6.1.9 应对工程设计进行考核验收。

6.2 基础设计

6.2.1 设计要求

6.2.1.1 基础设计之初，应通过设计合同或设计统一规定提出基础设计基本要求；
6.2.1.2 基础设计基本要求，应包括设计范围、标准规范、配置方案、关键技术要求等基本要求和针对具体项目的特殊要求；
6.2.1.3 设计范围，应包括所有SIS硬件和软件相关的设计要求；
6.2.1.4 标准规范，应包括SIS相关的标准规范和项目约定设计遵循的标准规范；

6.2.1.5 配置方案，应明确现场仪表的选型原则和逻辑控制器的功能要求及配置方案或原则；
6.2.1.6 关键技术要求，应包括SIS硬件、软件的关键技术规格或要求和SIS运行维护关键要求，并应体现在安全要求规格书中；
6.2.1.7 SIS关键技术要求，应明确可靠性、可用性及冗余容错配置要求和网络安全等SIS整体和关键部分的关键技术要求；
6.2.1.8 运行维护关键要求，应明确现场仪表检验测试周期、检验测试措施等具体内容。

6.2.2 安全功能分配到保护层

6.2.2.1 宜在危害和风险评估后，根据安全完整性要求将安全功能分配到保护层（也称SIL定级），确定要求的SIF和每个SIF的安全完整性等级；
6.2.2.2 应依据项目复杂性及应用经验，选择一种或多种测定分析方法确定SIF的SIL；
6.2.2.3 应参与确定建议的SIF清单及每个SIF要求的SIL；
6.2.2.4 宜提出失效率的最低要求；
6.2.2.5 对不符合目标SIL的SIF，应参与提出相应建议措施以实现目标SIL的要求；
6.2.2.6 SIL定级完成，应跟踪安全功能分配到保护层的设计；
6.2.2.7 SIL定级完成，可在基础设计阶段进行SIL预验证，避免详细设计阶段、采购阶段调整变化较大。

6.2.3 设计审查

6.2.3.1 应审查与设计要求的一致性；
6.2.3.2 应审查与总体设计或可研的符合性；
6.2.3.3 应审查与危害和风险评估报告的符合性；
6.2.3.4 应审查与初版安全要求规格书的符合性、完整性；
6.2.3.5 应审查联锁逻辑图；
6.2.3.6 应审查仪表规格书或仪表数据表；
6.2.3.7 应审查逻辑控制器规格书；
6.2.3.8 应审查可靠性、可用性及冗余容错配置、系统结构；
6.2.3.9 应审查SIS供电、供气、配线方案；
6.2.3.10 应审查相关控制系统的界面；
6.2.3.11 应审查P&ID；
6.2.3.12 应审查检验测试周期和检验测试措施。

6.3 安全要求规格书

6.3.1 基础设计阶段应编制安全要求规格书（SRS），详细设计阶段应进一步完善安全要求规格书；
6.3.2 SRS应明确所有应用程序和SIS硬件的安全要求；
6.3.3 宜在基础设计阶段初步确定SIF及其SIL、每个功能的过程安全状态、检验测试时间间隔（TI）、SIF的响应时间、SIS信息接口及操作界面、维修测试旁路、失效故障模式等SIS的设计要求；
6.3.4 宜对SIS的诊断功能提出要求；
6.3.5 可提出智能传感器及最终元件的组态及逻辑控制器SOE的要求；
6.3.6 应用程序的安全要求可包含在SRS中，也可以是一个独立的文件；
6.3.7 SRS确定后宜进行SIS安全要求评估，也称SRS的验证或审查；
6.3.8 应依据SRS编制执行SIS安全计划和进行生产运行及检修改造管理，并应根据SIS实际及其功能性和完整性要求编制具体的安全要求技术文件。

6.4 详细设计

6.4.1 设计要求

6.4.1.1 详细设计阶段，应通过设计合同或设计统一规定提出详细设计基本要求；
6.4.1.2 详细设计基本要求，应在基础设计基本要求上进一步细化；
6.4.1.3 应就SIS相关的辅助系统和安装接线提出基本的技术要求。

6.4.2 设计审查

6.4.2.1 应审查与设计要求的一致性；
6.4.2.2 应审查与基础设计的符合性；
6.4.2.3 应审查安全要求规格书；
6.4.2.4 应审查与安全要求规格书的符合性、完整性；
6.4.2.5 应审查联锁逻辑图；
6.4.2.6 应审查仪表规格书或仪表数据表；
6.4.2.7 应审查逻辑控制器规格书；
6.4.2.8 应审查可靠性、可用性及冗余容错配置、系统结构；
6.4.2.9 应审查SIS供电、供气、配线方案；
6.4.2.10 应审查相关控制系统的界面；
6.4.2.11 应审查P&ID；
6.4.2.12 应审查检验测试周期和检验测试措施。

7 采购管理

7.1 采购原则

7.1.1 应按设计文件要求采购，采购变更应与设计单位协同修改；
7.1.2 涉及工艺包指定或要求的采购变更，应征得工艺包供应商的同意或完成相关审批；
7.1.3 应执行国家法律法规和企业管理制度、采购程序、技术规定。

7.2 采购策略

7.2.1 对于多单元多装置的大中型工程逻辑控制器宜框架采购，对于小型工程宜单独采购；
7.2.2 应确定SIS成套的范围，逻辑控制器、传感器、最终元件宜分别采购；
7.2.3 宜在P&ID确定后、仪表选型确定后进行采购，工程设计单位应按计划要求提供用于采购的技术规格书、数据表等技术资料；
7.2.4 应对设计单位提供的技术规格书、数据表等采购资料进行审查；
7.2.5 应根据企业和项目实际，明确逻辑控制器、传感器、最终元件等各类型采购的特殊要求或规定。

7.3 采购合同

7.3.1 招评标

7.3.1.1 应编制招标文件
招评标过程中应编制招标文件，招标文件基本要求如下：

a）招标文件应包括技术要求和商务要求；
b）技术要求应包括技术规格书、数据表等；商务要求应包括资信情况、报价形式、付款条件等；
c）应确定技术规格书中“必须、应、宜、可”类技术要求在招标评标中的权重；
d）应确定偏差处理规定、废标项和报价修改规定；
e）宜规定投标文件的格式或提供投标文件编制模板。

7.3.1.2 应进行资质审查

招评标过程中应根据招标文件要求对产品进行资质审查，主要包括：
a）产品应具有符合IEC 61508或GB/T 20438标准或等同标准的功能安全认证，认证机构应在中国国家认证认可监督管理委员会备案；
b）投标产品安全完整性等级应符合招标文件的要求；
c）投标产品功能应符合招标文件的要求；
d）逻辑控制器产品系统性能力应符合招标文件的要求；
e）投标产品的应用业绩，在产品类型、应用场合、应用时长、应用效果等方面应符合招标文件的要求，经使用证明的应提供相应证明报告；
f）逻辑控制器供应商或集成商，在人员、资质、业绩、工程能力等方面的工程服务能力应符合招标文件的要求。

7.3.1.3 应对投标文件进行技术和商务审查

招评标过程中应针对具体招标文件进行技术和商务审查，主要包括：
a）投标文件的完整性和针对性应符合招标文件的要求；
b）技术审查的内容应包括资质、供货范围、规格型号、招标文件规定的关键技术要求、备品备件、服务范围，服务时机、服务时长、功能测试、安装调试、项目管理等；
c）投标产品或产品系列不应临近制造商建议的产品生命周期寿命期；
d）商务审查应依据招标文件逐一审查，审查内容应包括单价、总价、付款条件等；
e）可编制偏离表并组织投标人答疑。

7.3.2 技术协议

7.3.2.1 技术协议应包括招标要求的、双方约定的、供方承诺的技术事项；
7.3.2.2 技术协议应明确SIF相关的仪表（也称安全仪表）的检验测试或FAT要求；
7.3.2.3 技术协议应明确中间资料、最终资料等图纸资料的提供责任和时间节点；
7.3.2.4 技术协议不应低于招标技术文件的要求；
7.3.2.5 技术协议应作为合同的附件。

7.4 SIL验证

7.4.1 SIS采购完成，应根据采购SIS的资料信息验证SIS的功能和完整性符合SRS的要求；
7.4.2 应验证每个SIF结构均可达到其SIL的要求；
7.4.3 应以企业SIS失效数据库、采购SIS资料信息、以往使用经验数据、SIS相关仪表行业可靠性数据库等为基础验证；
7.4.4 不符合项及建议应在规定时间内整改反馈并按照第15章相关规定记录存档。

7.5 仪表监造

7.5.1 宜对SIL2及以上执行器、安全关键设备等关键仪表进行监造；

7.5.2 宜对SIS相关高压开关阀的性能测试、安全仪表的特殊检验测试等特殊检验测试进行监造；
7.5.3 监造要求应在招标文件和合同中规定，监造方案应与供应商协商一致；
7.5.4 宜编制仪表监造计划和监造方案，并按计划分阶段进行监造。

8 逻辑控制器集成

8.1 一般规定

8.1.1 集成是由制造商或集成商实施的逻辑控制器及其成套仪表的设计、装配、测试工作；
8.1.2 应以工程设计文件、技术协议和SRS为依据，进行功能设计审查、监造、测试等集成全过程管理；
8.1.3 集成工作完成后，可根据项目实际组织GB/T 21109/IEC 61511安全生命周期建议的功能安全评估节点2的功能安全评估，也可在FAT时验证评价实际设计制造的SIS硬件和应用程序是否符合SRS要求达到的功能安全。

8.2 功能设计

8.2.1 集成商应进行功能设计（FDS)、编制设计文件，功能设计应包括硬件功能设计和软件功能设计；
8.2.2 硬件FDS是逻辑控制器及其成套仪表的结构、布置、安装、接线、标识等硬件集成相关的技术规定；
8.2.3 硬件FDS，应明确系统网络结构、硬件配置、冗余容错配置、安装布置、电源规范、电缆规范、接地规范、编号及命名规则、备用原则等技术要求和规范；
8.2.4 软件FDS是逻辑控制器、HMI、通讯等应用程序组态及测试的技术规定；
8.2.5 软件FDS，应明确I/O点、变量、程序块、应用程序等命名规则、逻辑控制器应用程序组态规范、SOE、HMI操作画面规定、工具软件权限管理等具体技术要求和规定；
8.2.6 应按照GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》等相关标准规范，进行工控网络安全设计；
8.2.7 企业、设计单位应对FDS进行审查，共同批准后执行。

8.3 硬件集成

8.3.1 集成前应检查确认硬件正确、完好；
8.3.2 应按硬件FDS及相关规范安装、接线；
8.3.3 宜按SH/T 3521《石油化工仪表工程施工技术规程》相关规定检查、上电、测试，签字版硬件集成测试报告存档。

8.4 软件组态

8.4.1 依据工程设计文件和软件FDS进行的软件组态，也称应用程序开发；
8.4.2 逻辑控制器应用程序开发，应确定程序扫描时间、系统内存分配、应用层诊断、组态检查、故障检测、在线测试、离线测试等内容与功能；
8.4.3 非SIF相关的应用程序，也应按照FDS统一要求组态并应不影响SIF；
8.4.4 宜分别备份逻辑控制器组态、成套仪表组态，企业作为SIS节点性文档存档。

8.5 条件会

8.5.1 企业宜组织设计单位、制造商或集成商召开条件会，以保障SIS的设计、制造可按技术要求和计划进度完成；
8.5.2 条件会包括开工会、中间条件会，中间条件会可召开若干次；
8.5.3 开工会应确定系统的硬件配置、软件清单，以及交换的资料内容、交换时间、资料形式等；

8.5.4 中间条件会可根据系统集成难点、进度制约点择机召开，并确定交换的资料内容、交换时间、资料形式等；
8.5.5 会议应形成共同签署的纪要，相关单位按照合同方式履约执行。

8.6 监造

8.6.1 监造内容应包括硬件、软件的符合性，集成过程符合性、质量符合性、进度符合性；
8.6.2 可采用驻厂监造、按进度节点到厂监造、远程监造等多种形式。

8.7 工厂验收测试

8.7.1 工厂验收测试（FAT）应包括硬件测试、系统功能测试、软件测试，FAT应由制造商或集成商、设计单位、企业共同完成；
8.7.2 FAT程序应由制造商或集成商编制、并宜符合GB/T 25928《过程工业自动化系统出厂验收测试(FAT)、现场验收测试》相关规定要求，企业应对FAT程序进行审查、审批后执行；
8.7.3 测试环境宜符合FAR设计要求的条件，测试工具检定合格、精度等级适合；
8.7.4 应按照合同检查硬件配置、型号、数量及软件授权、版本、参数；
8.7.5 应按照FDS检查硬件集成，并应按照合同的系统网络结构进行FAT；
8.7.6 应从时效性、可用性、完整性等方面测试验证是否可达到SRS要求的安全目标，系统功能测试宜包括冗余、掉电、负荷、时钟同步、系统诊断、网络通讯、工控网络安全等验证或测试，无法验证测试的功能可通过第三方测试证明；
8.7.7 应按规范检验测试逻辑控制器成套的仪表；
8.7.8 逻辑控制器应用程序测试，应包括应用程序内部数据流、控制功能、联锁逻辑、趋势记录、报警、SOE功能、辅助操作、接口通讯、项目文件备份恢复、组态文件下载上传等验证测试；
8.7.9 逻辑控制器应用程序测试记录，应明确应用程序及工具软件版本、测试结果、测试人员、测试日期等基本信息；
8.7.10 I/O测试，宜按信号类型及仪表位号顺序测试记录；
8.7.11 不符合项或未完成项应明确整改计划，SIF相关的修改或变更应进行功能安全评估；
8.7.12 FAT报告应包括签字版测试记录、验收结论及其他相关评估，企业作为SIS节点性文档存档。

9 安装调试

9.1 仪表校验

9.1.1 施工单位应对仪表取源点位置、仪表安装位置进行实测，据此调整仪表零点、量程和组态；
9.1.2 企业应检查确认实测资料及变更资料；
9.1.3 应按规范进行安装前的校验或仪表投用前的校验；
9.1.4 企业应检查审核仪表校验记录。

9.2 仪表安装

9.2.1 安装位置应符合设计要求，变送器与取源点相对位置正确、维护方便、固定可靠；
9.2.2 仪表测量引线配管应符合设计要求，管径、材质、压力等级正确，管阀件型式正确，位置正确、坡度正确、连接可靠、无U型弯；
9.2.3 仪表绝热、伴热应符合设计要求；热源正确，取源点、回水点相对独立，不受其他仪表用热开关影响，管径、材质正确；仪表、测量引线、回水管线保温完整；

9.2.4 仪表隔离吹洗应符合设计要求，管径、材质、压力等级正确，管阀件型式正确，位置正确、连接可靠；
9.2.5 仪表电缆引入、接线应符合设计要求，密封严密、接线牢固；
9.2.6 仪表接地应符合设计要求，接地线径、颜色正确、接地可靠；
9.2.7 执行机构供气应符合设计要求，不受其他执行机构用气开关影响，管径、材质、压力等级正确；
9.2.8 仪表布线敷设应符合设计规定，安全仪表宜采用独立接线箱。

9.3 逻辑控制器安装

9.3.1 现场验收
9.3.1.1 逻辑控制器到安装前应按合同、FAT报告现场验收；
9.3.1.2 应确认外观完好、数量符合、证书图纸资料齐全。
9.3.2 安装条件确认
9.3.2.1 FAR、CCR按照设计建设验收完成，符合SH/T 3006《石油化工控制室设计规范》要求；
9.3.2.2 无强电磁干扰性作业；
9.3.2.3 接地系统验收测试合格；
9.3.2.4 220V AC供电回路、负荷、技术参数符合设计要求，MCC等关联系统断开或隔离；
9.3.2.5 现场安装方案、监理或质量监督方案审批完成。
9.3.3 安装接线
9.3.3.1 应按照控制室设备布置图进行机柜等设备就位,按照施工规范设备说明书安装要求进行固定；
9.3.3.2 应按照机柜内部布置图进行模块安装；
9.3.3.3 应按照接线图、回路图进行机柜或设备间电缆连接、仪表信号接线、与其他控制系统间的信号和通信连接。

9.4 逻辑控制器上电

9.4.1 宜由安装承包商、企业、制造商或集成承包商共同检查确认规格型号、标识、接线正确；
9.4.2 宜按FDS、SH/T 3081《石油化工仪表系统接地设计规范》相关规定进行接地检查、测试；
9.4.3 宜按FDS、SH/T 3082《石油化工仪表供电设计规范》相关规定进行供电检查、测试；
9.4.4 宜按SH/T 3551《石油化工仪表工程施工质量验收规范》相关规定上电、记录。

9.5 逻辑控制器测试

9.5.1 应检查测试确认逻辑控制器CPU、输入输出模块、系统网络运行正常；
9.5.2 宜按8.7.6条进行SIS系统功能现场测试并记录；
9.5.3 应测试确认与其他控制系统间的通信、硬接线信号正常、正确。

9.6 回路试验

9.6.1 应以回路为基本单位编制回路试验档案，参考示例见附录A；
9.6.2 标准校验仪器、试验工具、回路试验档案合格齐全；
9.6.3 宜按GB 50093《自动化仪表工程施工及质量验收规范》相关要求进行信号模拟和试验；
9.6.4 应模拟测试信号开路报警、输入信号报警及溢出、开关量状态报警等报警或报警值，控制阀故障安全等功能；
9.6.5 应测试辅操台和现场操作按钮、报警开关以及SOE功能；
9.6.6 试验时应记录试验数据和问题，签字版回路试验记录作为SIS节点性文档存档。

9.7 联锁试验

9.7.1 联锁试验档案宜包括逻辑输入条件、逻辑关系、联锁动作、联锁值、试验结果、试验人等基本信息（参考示例见附录B），试验档案宜由企业工艺专业负责，试验过程宜工艺专业负责仪表专业配合；
9.7.2 应按联锁试验档案试验联锁动作、旁路、部分行程测试（PST）等所有功能；
9.7.3 所有信号（含3取2等多信号表决的传感器），均应从现场一次表进行信号模拟；
9.7.4 对联锁响应时间有要求的SIF应做联锁响应时间测试；
9.7.5 签字版联锁试验记录作为SIS节点性文档存档。

9.8 相关系统联调

9.8.1 与SIS相关的MCC、BPCS等所有系统，应与SIS进行系统联调；
9.8.2 系统联调包括系统间的信号往来、通信及功能测试；
9.8.3 系统联调无法通过回路试验、联锁试验完成的，应单独进行试验测试。

10 安全确认

10.1 一般规定

10.1.1 安全确认是SIS安装调试后企业生产部门对安全仪表系统的确认与接受程序，也称现场验收（SAT）,可与GB/T 21109/IEC 61511安全生命周期建议的节点3的功能安全评估一并进行；
10.1.2 应按照SRS、FAT报告、安装调试记录参与编制安全确认程序或计划；
10.1.3 宜由仪表专业组织SIS制造商或集成商及安装施工承包商交付、企业生产部门确认接收；
10.1.4 宜采用联合验收的方式现场确认，确认SIS符合设计的功能安全要求、满足生产操作的需求。

10.2 系统恢复

10.2.1 应确认所有旁路、强制、测试信号等非正常运行状态已经取消并恢复正常或评估审批通过；
10.2.2 应确认所有测试仪器工具、现场试验设施或措施、设备均已移除；
10.2.3 应确认逻辑控制器状态正常，所有SIS硬件为可用状态。

10.3 确认要求

10.3.1 应确认SIS硬件、应用程序、其他工具软件的版本和功能；
10.3.2 应确认传感器测量精度、逻辑控制器信号处理精度、标准校验仪器精度符合要求；
10.3.3 应确认正常启动、急停后启动、正常操作、急停、临时操作、紧急操作、停机和特殊操作模式等所有操作模式符合SRS要求，SIS故障可满足故障安全的功能要求；
10.3.4 应测试SIS诊断报警功能，确认仪表风等公用工程故障及恢复时SIS均可保持设计的状态；
10.3.5 应确认BPCS、MCC等与SIS相关的其他控制系统状态、工作正常、不影响SIS操作；
10.3.6 应确认报警联锁值正确；
10.3.7 应确认回路试验完成合格；
10.3.8 应确认联锁试验完成合格；
10.3.9 应确认系统恢复正常和SIS符合SRS的要求。

11 生产运行管理

11.1 SIS 投用

11.1.1 安全确认完成，未完成项或不合格项补救方案审批完成；
11.1.2 确认操作规程、维护规程符合SRS要求，操作规程应包含正常操作、异常操作的各种操作模式；
11.1.3 操作人员SIS操作、应急操作相关培训合格；

11.1.4 SIS维护人员SIS软硬件及维护培训合格；
11.1.5 无系统报警，无过程报警或符合试生产条件或评估审批许可；
11.1.6 试生产相关联合验收合格。

11.2 试生产管理

11.2.1 试生产的工艺条件、操作要求与正常生产运行不同，其管理制度或方案可与正常生产不同；
11.2.2 依据试生产变更或试生产维护管理制度，可临时解除联锁进行维修作业；
11.2.3 试生产方案批准的临时旁路、参数调整等可不再审批，但应按规定记录；
11.2.4 现场仪表的检查、故障维修作业，应在功能安全评估确定的最大允许旁路状态时间内完成；
11.2.5 逻辑控制器系统报警、硬件故障及应用程序修改，可按应急恢复方案或相应处置方案处理。

11.3 操作管理

11.3.1 操作规程应明确每种操作模式（操作、开车、停车、维护等）下操作人员与SIS的交互动作；
11.3.2 SIS操作、维护、巡检、应急管理制度审批执行，SIS操作及维护规程审批执行；
11.3.3 操作人员、维护人员SIS培训合格，并依据国家法规和企业性质取得应持有的从业许可证；
11.3.4 SIS正常操作应按照操作规程操作；异常或SIS故障时的异常操作，应有补偿措施并确认SIS功能状态符合功能安全要求；
11.3.5 宜有操作日志或记录、联锁台账、报警台账、旁路台账、变更台账等操作记录或台账。

11.4 维护管理

11.4.1 一般规定

11.4.1.1 应依据SRS及安全计划编制维护计划和维护规程，明确检查、检验测试、预防性维修、预测性维修和故障维修的维护内容与要求；
11.4.1.2 应按照SRS要求和企业实际，编制检验测试计划和检验测试作业指导书；
11.4.1.3 维护作业应在维护作业工单批准后执行，维修作业不应由1人单独完成，作业完成应关闭工单并提交维护报告或记录；
11.4.1.4 联锁摘除和恢复应办理工作票或作业票，并应经相关部门会签和领导审批；
11.4.1.5 用于维护作业的SIS工程师站，不宜同时用做操作员站；
11.4.1.6 应有SIS应急恢复或应急故障处理预案。

11.4.2 检查

11.4.2.1 应通过周期性检查和专项检查发现SIS相关的故障或失效；
11.4.2.2 应依据SRS要求及安全计划，确定巡检、定期保养等周期性检查的内容和周期；
11.4.2.3 装置停车或SIF回路旁路状态时，可根据需要进行介入检查；
11.4.2.4 宜根据企业实际、气候条件及政策要求，确定专项检查的内容和要求；
11.4.2.5 检查记录按照第15章相关规定存档。

11.4.3 检验测试

11.4.3.1 一般规定

检验测试的一般要求如下：

a）应通过检验测试查找未发现故障、识别可能导致故障的原因，并通过功能测试避免引入常见原因故障；

b）逻辑控制器、现场仪表均应按计划、规程及不同的TI进行检验测试，并宜通过制度或管理程序监控计划实施、防止检验测试的延误；

c）应按历史测试数据、应用经验和硬件状况评估确定实际TI，与SRS中依据PFDavg或计算PFH确定的理论检验测试频率存在偏差以及生产运行期实际无法检验测试的，应通过企业级审批并应有增加巡检频次等补偿措施或手段；

d）应以安全的方式维修处理检验测试发现的故障或失效，维修、更换硬件的应重新做检验测试；

e）应用程序变更，应按照变更管理审批，变更部分应测试合格且应对未变更部分无影响。

11.4.3.2 校验检定

检验测试的校验检定要求如下：

a）SRS要求的检验测试周期内，应按SH/T 3521《石油化工仪表工程施工技术规程》进行现场仪表校验，属于强制检定的按相关规定检定；

b）停工检修期间，应按相应规范规程进行仪表的校验和检定；

c）生产运行期间的现场仪表校验，应按变更管理办理临时停用或旁路许可并在允许时间内完成。

11.4.3.3 在线测试

检验测试的在线测试要求如下：

a）宜按SRS、历史测试数据、经使用证明数据以及企业SIS运行实际，编制实施在线测试计划；

b）最终元件的在线测试，评估审批后应在允许时间内完成并记录存档。

11.4.3.4 离线测试

检验测试的离线测试要求如下：

a）智能传感器嵌入式软件升级完成，应离线测试合格后投用；

b）功能安全评估后允许旁路或切除的现场仪表，应在允许时间内离线测试；

c）应用程序变更，应先进行离线组态和测试。

11.4.3.5 点检

检验测试的点检要求如下：

a）每个检修周期，宜进行逻辑控制器点检和系统功能测试并记录存档；

b）逻辑控制器软硬件升级或更新后，宜根据实际情况更新点检或检验测试要求。

11.4.4 维修

11.4.4.1 维修包括预防性维修、预测性维修和故障维修，预防性维修和预测性维修应有计划；

11.4.4.2 维修规程宜包括SIS的故障诊断、维修更换、维修后确认、维修报告、维修后跟踪等内容；

11.4.4.3 按照第15章相关规定整理维修报告或记录并存档；

11.4.4.4 宜在检修期间进行软硬件升级或更新；

11.4.4.5 应根据维修内容和维修后跟踪情况更新SIS失效数据库。

11.4.5 备件管理

11.4.5.1　宜综合运行维护经验、SIS失效数据库、制造商生命周期建议，建立SIS备件台账并提出建议更新计划；
11.4.5.2　备件类型和数量应满足允许旁路持续时间内更换的需求；
11.4.5.3　维修更换的备件应检验测试合格，逻辑控制器备件的更换宜在方案审批后实施；
11.4.5.4　规格型号、固件版本、制造商建议的生命周期阶段有1项不符的备件更换，应按变更管理审批；
11.4.5.5　宜在检修期间检验测试所有备件，淘汰或不合格的原因、结果作为SIS失效数据库的参考。

11.5　应急管理

11.5.1　应急预案

11.5.1.1　宜根据企业规模及危险化学品类型编制实施SIS应急管理制度和应急预案，并组织相关培训；
11.5.1.2　应急预案应符合国家、所在行政区域政策及管理要求，评估与企业内部、关联企业、政府管理部门之间的影响并确定是否联动；
11.5.1.3　SIS应急恢复方案，应明确SIS硬件更换、应用程序恢复等应急恢复作业步骤；
11.5.1.4　手动操作的按钮或最终元件，可编制专项管理规定或应急处置方案防止误动作；
11.5.1.5　宜按备件更新应急计划、升版安全计划和应急恢复方案。

11.5.2　应急演练

11.5.2.1　SIS操作人员和维护人员，应熟知其SIS应急操作权限设置及操作；
11.5.2.2　应急演练方案应充分评估与SIS相关的BPCS、MCC等其他控制系统的状态及可能影响，应急演练宜重点演练手动联锁复位等操作转换性节点；
11.5.2.3　宜根据企业实际分级组织应急演练，部门级可每年1次维护人员SIS应急恢复演练；
11.5.2.4　应急演练结束，应有演练评价或结论并提出建议或意见；
11.5.2.5　按照第15章相关规定记录存档演练内容、人员、地点、时间、评价等基本信息。

11.5.3　事件事故管理

11.5.3.1　事故管理制度中应明确涉及SIS的事件、事故管理流程和处理程序，并宜档案化管理；
11.5.3.2　事件、事故处理过程中，新发现异常或变化应按照变更管理要求进行功能安全评估和审批；
11.5.3.3　非计划性停车等未遂事件，宜按照事故进行调查、防范和管理；
11.5.3.4　宜按事故经过、原因分析、整改措施等方面编制存档事故报告，并将故障、隐患记录在SIS失效数据库中；
11.5.3.5　事件、事故过后，宜组织经验交流或培训，必要时升版操作规程、检修规程、应急预案甚至管理制度。

11.5.4　应急信息化管理

11.5.4.1　应急管理制度、预案、演练及事件、事故，宜在企业公众信息系统或平台发布；
11.5.4.2　可通过信息系统管理SIS失效数据库；
11.5.4.3　可根据企业及所在行政区域的信息化管理现状和政策，确定与制造商、关联企业、政府管理部门之间信息共享的形式及内容；
11.5.4.4　宜建设、完善、升级应急信息化系统，不断提高应急信息化管理水平和效率。

11.6　防卫管理

11.6.1　工控信息安全

11.6.1.1 应按照国家信息安全法律法规、标准规范，评估安全仪表系统的作用、制定安全仪表系统信息安全防护方案，以满足GB/T 22239-2019等标准规范要求的网络安全等级保护基本要求；
11.6.1.2 信息安全防护方案应与工程项目同步设计、同步建设，并依据安全需求不断升级、完善；
11.6.1.3 应采取纵深分层防御、分域隔离防护的策略；
11.6.1.4 不应将安全仪表系统直接接入管理网络；
11.6.1.5 应建立工控信息安全管理制度，明确工控信息安全的建设、维护、升级等管理措施；
11.6.1.6 应宣贯或培训工控网络安全知识、制度；
11.6.1.7 应执行授权管理，限制企业内部人员和外来服务人员的操作、修改，并应限制第三方设备和承包商自有设备接入SIS；
11.6.1.8 可编制并根据实际演练SIS网络安全防护应急预案；
11.6.1.9 宜按国家法律、规范、标准，适时进行网络安全防护系统升级或工控网络安全审计。

11.6.2 防护安全

11.6.2.1 SIS调试、维护、检修改造、技术服务等企业外部人员，宜通过安全培训并审批后入场；
11.6.2.2 应评估企业内外无关生产人员或集体的危害或威胁，外部人员或承包商的设备或个人电脑接入SIS前应安全审计合格；
11.6.2.3 宜有FAR、CCR内防火及防台风、防地震等防灾害应急预案；
11.6.2.4 宜有防强电磁干扰措施和反无人机方案或措施；
11.6.2.5 宜有时钟同步定期检测等网络安全定期检查测试计划和措施；
11.6.2.6 应防范社会事件、公共安全事件波及企业。

11.7 风险管理

11.7.1 风险管理制度

11.7.1.1 应建立健全安全风险分级管控和隐患排查治理双重预防工作机制；
11.7.1.2 宜按危害和风险评估报告、SRS，制定SIS风险管理制度和具体风险控制措施；
11.7.1.3 宜定期进行SIS风险评估，并根据评估结果修订SIS风险管控清单和措施；
11.7.1.4 应按企业或当地ALARP进行风险控制和闭环管理；
11.7.1.5 宜按SIS安全生命周期各阶段的功能安全评估结果更新风险控制措施甚至管理制度。

11.7.2 人员风险管理

11.7.2.1 宜根据事故档案、人员实际以及行业事故案例确定合理的人为错误影响因子；
11.7.2.2 宜评估人员的有意识和无意识行为影响，并通过培训、演练及标准化管理提高SIS操作、维护人员技术水平及风险防控能力；
11.7.2.3 可评估SIS操作、维护作业环境对人员的危害。

11.7.3 环境风险管理

11.7.3.1 宜评估维护、应急处置等对现场环境和自然环境的影响，如有影响应提出相应风险消减措施；
11.7.3.2 宜评估供电、仪表风等公用工程系统风险以及与SIS相关的其他控制系统的风险；
11.7.3.3 宜根据危害和风险评估或安全评价结果，更新环境风险管控计划或措施。

11.7.4 财产风险管理

11.7.4.1 宜按逻辑控制器、现场仪表、应用软件分别建立和更新设备台账；
11.7.4.2 宜根据操作、维护、检修记录及事故档案，建立、更新SIS故障隐患档案；

11.7.4.3　宜根据SIS故障隐患档案及制造商生命周期建议，制定SIS维护、检修改造计划。

12　变更管理

12.1　一般规定

12.1.1　应以保障SIS安全完整性为目标建立变更管理制度，明确变更计划、审核、批准及程序的原则要求与可执行性规定；
12.1.2　变更宜在功能安全评估完成且确认风险消减措施合理可行后批准实施，评估内容宜包括变更的原因、修改作业对SIS的影响、可能的危险及对SIF的影响、可接受的修改、变更的验证测试、详细的修改计划或方案等；
12.1.3　变更级别可分部门级和企业级，或可分为一般变更和重大变更，变更性质可分临时性变更和永久性变更，临时性变更包括紧急变更；
12.1.4　变更作业至少应由2名具备相应经验和资质的人员同时完成，修改完成后应验证测试变更部分可实现SIS性能要求且应对SIS未变更部分无影响；
12.1.5　变更申请单或审批流程应有变更验收的闭环管理要求，参考性示例见附录C；
12.1.6　变更后宜更新变更台账及相关的设备台账、联锁台账、操作规程；
12.1.7　变更后应对相关规程、图纸资料等安全生产信息进行更新，并对相关人员进行培训；
12.1.8　旁路应分级授权管理，并宜通过功能安全评估确定纳入变更管理的旁路；
12.1.9　功能安全评估报告、变更申请单、修改后验证测试记录、变更档案应作为SIS失效数据库的参考，并按照第15章相关规定存档。

12.2　工艺变更

12.2.1　工艺变更包括工艺条件变化、工艺要求变化、工艺流程变化等方面的变化；
12.2.2　涉及SIF的工艺变更，宜由工艺专业提出和组织审批；
12.2.2　涉及工艺方案调整、PID改变等重大工艺过程变更的，宜按技术改造立项管理。

12.3　设备变更

12.3.1　设备变更包括机械设备变化、设备要求变化等方面的变化；
12.3.2　涉及SIF的设备变更，宜由设备专业提出和组织审批；
12.3.3　变更前应从危险、危害、防卫等方面进行功能安全评估。

12.4　SIS 变更

12.4.1　SIS变更包括逻辑控制器硬件、现场仪表、应用程序、工具软件等SIS的变化、修改；BPCS等与SIS相关的其他控制系统的变化、修改，涉及SIF的也应按SIS变更评估审批；
12.4.2　SIS变更应由仪表专业提出和组织审批并执行；
12.4.3　嵌入式软件、工具软件升级等软件更新和硬件固件版本升级，不宜在生产运行期间实施；
12.4.4　变更后宜对比验证测试或在合理时限内定期观察监控运行状况，并宜根据观察监控运行情况进行功能安全评估，评估合格后关闭SIS变更审批或流程；
12.4.5　变更后宜更新SIS设备台账或备份应用程序。

12.5　管理变更

12.5.1　管理变更包括与SIS相关的管理机构、人员、管理职责、管理制度的变化、修改；
12.5.2　管理变更应为企业级变更或重大变更，变更后应修改或升版相关管理制度和执行性文档。

12.6 停用

12.6.1 生产运行期间现场仪表故障损坏，允许时间内无法维修恢复且功能安全评估后可临时或长期停用的，可按变更管理审批后停用；
12.6.2 涉及逻辑控制器硬件的停用，应为长期停用并应按变更管理制度评估和审批；
12.6.3 长期停用应为企业级变更或重大变更，可依据变更管理制度及具体评估结果确定允许的停用时间，但不应超过1个检修周期。

12.7 功能安全复审

12.7.1 第1次停工检修，可结合取得的操作和维护经验组织GB/T 21109/IEC 61511安全生命周期建议的功能安全评估节点4的首次功能安全复审；
12.7.2 涉及“两重点一重大”的在役生产、存储装置用SIS，可每3年或每个检修周期进行一次功能安全评估或功能安全复审；
12.7.3 装置扩建、改建后和进行技术改造的SIS，SIS投用前应进行功能安全评估或复审；
12.7.4 应以最新的法律、文件、标准、规范和存档的操作、维护、事故、变更文档为依据复审或评估；
12.7.5 宜评价变更、硬件实际失效概率、软硬件版本、应用程序缺陷，确认SIS安全功能的完整性和可靠性；
12.7.6 宜由企业SIS操作、维护技术人员与制造商或专业评估机构人员通过会议形式评估；
12.7.7 按照第15章相关规定存档。

13 检修改造

13.1 检修

13.1.1 检修为SIS的计划性停工检修；
13.1.2 检修计划、检修方案应审批后执行，涉及变更的应按变更管理审批；
13.1.3 逻辑控制器、现场仪表应分别做检修方案，特殊仪表、SIF相关的开关阀宜有特殊要求或专项检修及测试方案；
13.1.4 检修作业人员资质及管理要求应不低于SIS维护要求；
13.1.5 宜按第11章相关内容组织检修后的SIS投用及开工；
13.1.6 宜按第15章相关规定进行检修准备和实施过程文档管理，并更新相关台账、规程、SIS失效数据库。

13.2 改造

13.2.1 涉及SIF软件变化、SIS硬件增减等系统结构变化的宜按技术改造立项管理，涉及逻辑控制器CPU数量变化的宜按改建或扩建项目管理；
13.2.2 改造项目应有改造原因、内容、实施计划以及相应的功能安全评估和审批；
13.2.3 改造过程，宜按第9章安装调试相关要求实施；
13.2.4 SIS投用前，可按第10章相关要求进行验收确认；
13.2.5 宜按第15章相关规定进行改造过程文档管理，并更新相关台账、规程、SIS失效数据库。

14 退役

14.1 退役原因

14.1.1 退役为SIS到达报废年限或无法保障相应功能安全之前已不再适合继续运行的状态或阶段；
14.1.2 SIS或SIF可全部或部分退役。

14.2 退役条件

14.2.1 国家或行业规定要求强制退役的；
14.2.2 SIS硬件已经停产或出现严重质量问题的；
14.2.3 制造商建议的生命周期将至、无法升级更新且经使用证明故障率较高的；
14.2.4 SIS失效数据库和经使用证明无法保证或达到SRS的功能安全要求的；
14.2.5 装置或单元报废、迁移或根本性改造、改建的。

14.3 退役评估

14.3.1 退役前应组织GB/T 21109/IEC 61511安全生命周期建议的功能安全评估节点5的退役评估；
14.3.2 应以最新法律、文件、标准、规范、制造商建议和操作、维护、变更、改造文档为依据评估；
14.3.3 可由SIS操作、维护技术人员与制造商或专业评估机构人员共同评估；
14.3.4 评估报告按照第15章相关规定存档。

14.4 退役程序

14.4.1 应按退役评估报告编制审批SIS退役方案；
14.4.2 退役过程应保障SIS的功能安全正常和不影响关联装置、系统及操作；
14.4.3 退役过程应不影响与SIS相关的其他控制系统的运行和安全；
14.4.4 退役评估报告、退役方案、退役过程记录，按照第15章相关规定存档；
14.4.5 可按SIS安全生命周期各阶段文档信息编制退役SIS的总体评价报告。

15 文档信息管理

15.1 一般规定

15.1.1 文档信息，是与SIS相关的图纸、资料、文件、档案等文档和应用程序、数据库、白名单库等信息的总称；
15.1.2 SIS安全生命周期各阶段宜信息化、动态化、档案化管理；
15.1.3 文档信息的名称、格式、版次应规范统一，内容可追溯并动态更新；
15.1.4 电子版和纸版宜同时存档，保留时限应不早于SIS退役；
15.1.5 电子版文档应有备份，并宜在每次检修后重新备份；
15.1.6 纸版文档宜有日期、签名或公章、文档名称等基本信息；
15.1.7 对设备工具、人员、参考标准等有要求的测试、评估、验证文档，应按本文件相关规定记录；
15.1.8 可按图纸资料、协议合同、方案规程、台账档案、计划纪要等分类、建立、更新文档信息索引。

15.2 管理制度

15.2.1 宜有SIS文档信息管理制度或在企业文档管理制度中涵盖；
15.2.2 应明确文档信息管理的基本要求、责任人或部门；
15.2.3 宜根据文档信息的重要性分级管理和要求；
15.2.4 宜明确保密原则、要求以及可查阅人员的权限范围；
15.2.5 可明确企业与制造商、行业、学术界等信息交流机制或要求。

15.3 文档管理

15.3.1 宜按设计阶段存档设计过程及存档版设计图纸资料；
15.3.2 H&RA、功能安全评估等评估报告及过程资料，应注明SIS安全生命周期阶段和版次；

15.3.3 系统集成、安装、调试过程图纸、记录及报告原件可做资料留存，最终版或签字版应扫描存档；
15.3.4 可按照硬件或服务类别存档技术协议、评估合同、维护服务合同，并宜留存可编辑版；
15.3.5 操作规程、操作记录、变更台账、应急处置方案、演练记录、事故台账等生产操作相关各类方案规程和记录台账，宜由工艺专业存档管理；
15.3.6 维护规程、应急恢复方案、SIS设备台账、回路试验档案、检验测试记录、组态备份等SIS维护档案资料，应由仪表专业按SIS名称动态管理；
15.3.7 检修改造宜按照实施年份命名和项目全过程统一存档管理，并作为节点事件在SIS安全生命周期信息库中记录；
15.3.8 样本、维护手册、认证资料等产品资料和其他参考资料可按产品类型存档。

15.4 信息管理

15.4.1 SIS失效数据库

15.4.1.1 宜以SIF为单位建立SIS失效数据库，按逻辑控制器、传感器、最终元件、应用程序分项记录；
15.4.1.2 宜包括失效项目、失效内容、失效原因、失效时间、补偿措施、评估结论等信息；
15.4.1.3 生产运行、维护、检修改造的过程文档信息，应作为SIS失效数据库的基本来源；
15.4.1.4 制造商生命周期建议、行业SIS故障事故信息，可作为SIS失效数据库的参考信息；
15.4.1.5 SIS退役1个月内宜分类汇总失效信息并存档。

15.4.2 SIS安全生命周期信息库

15.4.2.1 FAT后宜建立SIS安全生命周期信息库或档案；
15.4.2.2 可按本文件定义的SIS安全生命周期阶段，记录各阶段和功能安全评估各节点的时间、结论及重要节点事件信息。

15.5 计划管理

15.5.1 宜在基础设计开始后分阶段编制SIS安全生命周期安全计划，并根据实施情况动态更新；
15.5.2 宜有SIS安全生命周期各阶段的验证计划；
15.5.3 生产运行期间，宜有检验测试计划、变更计划、检修计划、退役计划等具体计划或方案。

16 人力管理

16.1 人力配置

16.1.1 可行性研究、工程立项、工程设计、安全计划中应包括人力配置及能力要求；
16.1.2 人力配置方案应分析人员的流动性，并宜有备用方案。

16.2 人力资质

16.2.1 应符合国家和行业强制要求的从业资格或资质要求；
16.2.2 从业资格或资质应在有效期内；
16.2.3 可根据企业及SIS实际调整人员的工作经验、资质等具体要求，不同岗位应有资质差别。

16.3 人力培训

16.3.1 应有SIS培训计划，可有专项计划和年度计划；
16.3.2 SIS安全生命周期各阶段要求的培训应有记录或考核；
16.3.3 培训不合格者，不应上岗。

16.4 承包商管理

16.4.1 承包商包括SIS集成商、施工承包商、维护承包商、检修承包商、改造承包商、评估机构等参与SIS安全生命周期各阶段工作的非企业人员或集体；

16.4.2 应审查承包商资质和人员资质，并执行人员数量要求；

16.4.3 承包商在企业发生的事故宜纳入企业事故管理；

16.4.4 宜定期再评价长期合作承包商的资质与业绩。

附录 A

（资料性）

回路试验档案见表 A.1

表A.1 ***（公司/部门）***（装置/单元）SIS回路试验档案

****年**月**日

回路序号	仪表位号	检测位置	仪表名称	仪表型号	量程	故障状态	AHH	AH	AL	ALL	开路报警	溢出报警	联锁值	0	50%	100%	备注	试验人	监督人

附录 B

（资料性）

联锁试验档案见表 B.1

表B.1 ***（公司/部门）***（装置/单元）联锁试验档案

序号	联锁编号	联锁名称	联锁旁路	联锁条件	联锁值	逻辑关系	联锁动作	试验结果	试验日期	试验人		备注
										工艺	仪表	

附录 C

（资料性）

变更申请单见表 C.1

表 C.1 工艺变更申请单

顺序号：项目号-单元号-4 位年号-3 位流水号

<table>
<tr><td colspan="2">申请部门</td><td></td><td>申请人</td><td></td><td>申请日期</td><td></td></tr>
<tr><td>变更类型</td><td>工艺</td><td colspan="5">☐工艺联锁　☐生产装置改、扩建　☐技改技措　☐报警　☐其他</td></tr>
<tr><td colspan="3">公司级变更　☐　运行部级变更　☐</td><td colspan="4">永久性变更　☐　临时性变更　☐</td></tr>
<tr><td colspan="7">变更起止时间：　年　月　日　时　分 至　年　月　日　时　分</td></tr>
<tr><td colspan="7">变更建议（内容）：
变更理由：</td></tr>
<tr><td colspan="7">功能安全评估（必要时应附相关报告）：
风险评估（必要时应附相关报告）：
安全保障措施：</td></tr>
<tr><td colspan="7">审 批 意 见</td></tr>
<tr><td colspan="2">部门</td><td colspan="2">专业工程师/主管审核意见及签字</td><td colspan="3">部门副经理、经理审核意见及签字</td></tr>
<tr><td colspan="2">申请部门</td><td colspan="2">年　月　日</td><td colspan="3">年　月　日</td></tr>
<tr><td rowspan="3">审批部门</td><td>☐指挥中心</td><td colspan="2">年　月　日</td><td colspan="3">年　月　日</td></tr>
<tr><td>☐设备中心</td><td colspan="2">年　月　日</td><td colspan="3">年　月 日</td></tr>
<tr><td>☐其他：</td><td colspan="2">年　月　日</td><td colspan="3">年　月　日</td></tr>
<tr><td colspan="2">部门（中心）经理/公司分管领导审批</td><td colspan="5">年　月　日</td></tr>
<tr><td colspan="7">变 更 关 闭 确 认</td></tr>
<tr><td colspan="7">※ 本人确认与本变更相关的所有工作已完成，相关的文件和图纸已更新，而且无未完成问题。</td></tr>
<tr><td colspan="2">确认人</td><td colspan="2">签字</td><td colspan="3">日期</td></tr>
<tr><td colspan="2">变更作业人</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">变更负责人</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">变更部门验收负责人</td><td colspan="2"></td><td colspan="3"></td></tr>
</table>

主管部门验收负责人		
文档验收人		

保存部门：　　保存期：

本文件用词说明

为便于对标准条文理解和执行时区别对待，相关用词说明如下：

1）应 shall，表示严格，在正常情况下应这样做的；

正面用词采用“应”，反面用词采用“不应”；

2）宜 can，表示允许有选择，在条件许可时首先应这样做的；

正面用词采用“宜”，反面用词采用“不宜”；

3）可 may，表示有选择，在一定条件下可以这样做的，采用“可”。

ICS 71.120.01
CCS G98

团　　体　　标　　准

T/CAMETA 001011-2022

化工安全仪表系统管理规范

条文说明

目　　次

1 范围

化工企业为GB/T 4754-2017《国民经济行业分类》定义的化学原料和化学制品制造业（简称化工）；石化企业为GB/T 4754-2017定义的石油、煤炭及其他燃料加工企业，包括精炼石油产品制造（简称炼油）和煤炭加工（简称煤化工）；本文件适用于化工、石化企业，化学纤维制造业、医药制造业、石油和天然气开采业、管道运输业可参考执行。

5 危害和风险评估

5.1 项目建设期

5.1.1 项目的规模及管理不同，基础设计之前可能有可行性研究、工艺包设计、总体设计等阶段。危害和风险评估（H&RA），无论是只有在基础设计阶段进行，还是在可行性研究、工艺包设计、总体设计、详细设计阶段进行，仪表专业均应参与；可采用书面或会议的形式评估危害、风险、防护，并宜对工控网络安全进行评价。

6 设计管理

6.1 一般规定

6.1.1 设计统一规定，也称设计规定、设计一般规定、项目统一规定、项目技术规定，并宜分基础设计工程和详细设计工程两个阶段编制；关于安全仪表系统，设计统一规定宜包括采用的设计规范、设计范围、设计分工、设计基础数据、系统结构、可靠性与可用性原则、现场仪表及逻辑控制器选型原则、检测周期及检测措施、仪表安装、仪表布线、绝热伴热、供电、供风等。

6.2 基础设计

6.2.1 设计要求

6.2.1.5 现场仪表的选型原则，包括仪表原理、仪表类型、仪表材质、可靠性、智能化、自诊断、信号制、防爆等级、防护等级、防护方式、过程接口、接线口、产地要求等；

6.2.1.8 仪表检验测试周期及检验测试措施条文解释

可按照如下要求明确仪表检验测试周期及检验测试措施：

a）根据装置生产运行实际及SIS运行维护维修经验，结合具体的传感器、最终元件提出具体的可执行的或可接受的检验测试周期作为设计基本要求，供SIS设计、采购过程中使用；

b）不同类型的传感器、最终元件应有不同的检验测试措施，可根据现场仪表类型、运行维护维修经验和企业生产实际，提出可执行的检验测试措施作为设计基本要求，供SIS设计、采购过程中参考。

6.2.2 安全功能分配到保护层

6.2.2.1 可按照如下要求进行安全功能分配到保护层（SIL定级）：

6.2.2.1.1 宜由企业组织并成立PHA小组共同完成；

6.2.2.1.2 PHA小组宜由企业、设计单位、第三方机构组成，企业应至少安排1名具有生产操作经验的人员（工程师或操作员）和1名仪表工程师参加，设计单位应至少安排1名工艺工程师和1名仪表工程师参加；

6.2.2.1.3 确定第三方机构条文解释

可按照如下要求选择确定第三方机构：

a）宜根据机构或从业资质、业绩、人员资质等可量化标准选择；

b）应有1名主席、1名工艺工程师、1名仪表工程师参加；

c）主席宜取得TüV Rheinland、Exida 、Bureau Veritas等国际认证机构或上海仪器仪表自控系统检验测试所有限公司等国内认证机构版发的功能安全专家或5年以上功能安全工程师证书，工程师应取得功能安全工程师证书，证书均在项目执行期间有效；

d）宜有符合GB/T 21109/IEC 61511、GB/T 20438/IEC 61508标准的分析软件；

e）应无因评估失误、错误导致事故或者造成SIS设计被迫变更的不良业绩。

6.2.2.1.4 进行SIL定级评估条文解释

可按如下要求进行SIL定级评估：

a）危害和风险评估结果应作为输入条件；

b）宜根据制造商失效数据库、国内工业失效数据库、企业SIS失效数据库核算评价；

c）可根据GB/T 21109/IEC 61511-1:2016表4或表5确定需求操作模式下要求的SIL、可根据表5确定连续操作模式下要求的SIL；

d）宜评价保护层的独立性、差异性和通常原因造成的失效；

e）一个BPCS保护层设置的降低因子应小于等于10；

f）采用LOPA时应对每个场景的初始事件、独立保护层进行分析，初始事件应包括外部事件、设备故障、人员失误；

g）可依据分析结果提出建议的安全关键设备或安全关键活动；

h）可将SIF和SIL要求等SIL定级评估结果形成标准文档或建议的安全要求规格书。

6.2.2.1.5 进行SIL定级结果评价条文解释

宜按如下要求进行SIL定级结果评价：

a）全程参与的人员及资质；

b）是否符合GB/T 21109/IEC 61511-3:2016相关要求；

c）SIL定级或评估合同执行情况；

d）可分不合格、合格、良好三个等级综合评定SIL定级结果。

6.3 安全要求规格书

6.3.1 编制安全要求规格书条文解释

可依据如下内容编制安全要求规格书：

a）危害和风险评估报告及安全功能分配到保护层结果；

b）SIS相关法律文件及GB/T 21109/IEC 61511-3:2016的规定；

c）确定的SIF及其SIL；

d）以SIF为单位编制安全要求规格书，可包括或体现GB/T 21109/IEC 61511-1:2016第10.3.2条要求的29项内容。

6.3.4 为达到所需要的SIL对SIS硬件及自诊断等安全完整性的要求，SIS的系统性能力、结构应符合GB/T 20438/IEC 61508和所有SIF的要求；

6.3.6 应用程序的安全要求可包括GB/T 21109/IEC 61511-1:2016第10.3.5条要求的14项内容，包括传感器表决在内的SIF安全要求和SIS结构及安全手册，可作为应用程序的安全要求的输入条件；

6.3.7 可参考T/CIS 71001-2021《化工安全仪表系统安全要求规格书编制导则》部分要求编制、审查；

6.3.8 具体的安全要求技术文件，包括安全要求规格书、安全计划以及与SIS安全生命周期管理相关的其他执行性文件。

6.4 详细设计

6.4.1.3 SIS 相关的辅助系统，主要指系统供电、检测仪表绝热和伴热以及隔离吹洗；安装接线，包括逻辑控制器和现场仪表的安装接线，例如控制柜内安装接线和控制阀的供风配管、布线、配线、接线等。

7 采购管理

7.3 技术协议

7.3.2.2 逻辑控制器技术协议条文解释

逻辑控制器技术协议，宜明确如下内容：

a）补充的技术条款；

b）补充的技术服务条款；

c）逻辑控制器软件、硬件升级方案；

d）组态、安装、调试、投用、修改、培训的责任；

e）与其它控制系统通信的责任；

f）对成套的第三方产品的要求、责任；

g）图纸资料提供要求，包括种类、文字、介质、数量等。

7.4 SIL 验证

7.4.1 进行 SIL 验证条文解释

可按照如下要求进行 SIL 验证：

a）SIL验证宜与SIL定级统一计划安排；

b）SIL验证的人员组成、第三方机构选择、基本要求和验证结果评价，宜参考条文说明第6.2.2条相关要求执行。