UDC

中华人民共和国国家标准 GB

**P GB 50770—2013**

**石油化工安全仪表系统设计规范**

**Code for design of safety instrumented systems**

**In petrochemical engineering**

**（20XX年版）**

**局部修订征求意见稿**

2013－02－07 发布 2013－09－01 实施

|  |
| --- |
| 中华人民共和国住房和城乡建设部  联合发布 |
| 国家市场监督管理总局 |

**局部修订说明**

本规范此次修订是根据《住房和城乡建设部关于印发2021年工程建设规范标准编制及相关工作计划的通知》（建标函〔2021〕11号）的要求，由中国石化工程建设有限公司会同有关单位负责对《石油化工安全仪表系统设计规范》GB/T 50770-2013的局部修订。

局部修订的主要内容是：1、增加安全要求规格书、安全完整性等级验证、网络信息安全的内容；2、安全完整性等级评估补充完善为安全完整性等级分级和安全完整性等级验证；3、补充兼顾石油化工装置安全性与可用性的内容；4、完善测量仪表、最终元件和逻辑控制器的独立性和冗余性要求；5、完善维护旁路开关和操作旁路开关的实施要求；6、补充对电动控制阀和电液控制阀用于安全仪表系统的要求；7、增加安全仪表系统投入使用前确认工作的内容。

本规范中下划线表示修改的内容。

本规范由住房和城乡建设部负责管理，由中国石化工程建设有限公司负责具体技术内容的解释。执行过程中如有意见或建议，请寄送至中国石化工程建设有限公司（地址：北京朝阳区安慧北里安园21号，邮编：100101）。

本次局部修订的主编单位、参编单位、主要起草人和主要审查人：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **主编单位：** | 中国石化工程建设有限公司 | | | | |
| **参编单位：** | 中国寰球工程公司  中国石化集团宁波工程有限公司  中国石化安全工程研究院  中石油华东设计院有限公司  中沙（天津）石化有限公司  北京康吉森自动化设备技术有限责任公司  中石化-霍尼韦尔（天津）有限公司  浙江中控技术股份有限公司  杭州和利时自动化有限公司 | | | | |
| **参加单位：** |  | | | | |
|  |  | | | | |
| **主要起草人：** |  | | | | |
|  |  | | | | |
| **主要审查人：** |  |  |  |  |  | |

**《石油化工安全仪表设计规范》GB50770—2013（20XX年版）**

**修订对照表**

**（方框部分为删除内容，下划线部分为增加内容）**

| 现行《规范》条文 | 修订征求意见稿 |
| --- | --- |
| **2.1 术 语** | **2.1 术 语** |
| **2.1.2**风险 risk  预期可能发生的特定危险事件和后果。 | **2.1.2**风险 risk  危险事件发生概率与危险严重程度的组合。 |
| **2.1.4** 安全生命周期 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的全部时间。 | **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的所有必要活动。 |
| **2.1.7**保护层 protection layer  通过控制、预防、减缓等手段降低风险的措施。 | **2.1.7**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。 |
| **2.1.11**安全完整性 safety integrity  在规定的条件和时间内，安全仪表系统完成安全仪表功能的平均概率。 | **2.1. 11**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。 |
| **2.1.12** 安全完整性等级 safety integrity level  安全功能能的等级。安全完整性等级由低到高为SIL1~SIL4。 | **2.1.12** 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。 |
| **2.1.22** 容错 fault tolerant  在出现故障或错误时，功能单元仍继续执行规定功能的能力。 | **2.1.22** 硬件故障裕度 hardware fault tolerance  在出现故障或错误时，功能单元硬件仍继续执行要求功能的能力。 |
|  | **2.1.31** 结构约束 architectural constraints  在不考虑要求时平均危险失效概率的情况下，对实现安全仪表功能的硬件组成和结构的限制。 |
|  | **2.1.32** 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。 |
|  | **2.1.33**共因失效 common cause failure  由单个事件引起的不同设备的失效，这些失效相互之间独立。 |
|  | **2.1.34 诊断** diagnostics  用于发现故障（与过程安全时间有关）的自动测试。 |
|  | **2.1.35 诊断覆盖率** diagnostics coverage  通过诊断检测出危险失效概率与总失效概率之比。诊断覆盖率不包括检验测试检测出的任何故障。 |
|  | **2.1.36 平均恢复时间** mean time to restoration  完成功能恢复的平均预计时间。 |
|  | **2.1.37** **操作模式** mode of operation  安全仪表功能运行的方式，可分为低要求模式、高要求模式和连续模式。 |
|  | **2.1.38** **以往使用** 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的要求。 |
|  | **2.1.39** **检验测试** proof test  为检测安全仪表系统隐性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为如新的状态或尽可能接近该状态。 |
|  | **2.1.40** **过程安全时间** process safety time  安全仪表功能未动作的情况下，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。 |
|  | **2.1.41** **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。 |
|  | **2.1.42** **误停车率** spurious trip rate  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（特定时间内的停车次数）。 |
|  | **2.1.43** **确认** validation  通过检查和提供证据，证明特定用途的要求已经得到满足。 |
|  | **2.1.44** **验证** verification  通过检查和提供证据，证明目标要求已经得到满足。 |
| **2.2 缩略语** | **2.2 缩略语** |
| FDS (Functional Design Specification)  功能设计规定 | FDS (Functional Design Specification)  功能设计规格书 |
| PFDavg （Probability of Failure on Demand average）  低要求模式的平均失效概率 | PFDavg（Probability of Failure on Demand average）  要求时危险失效平均概率 |
|  | HFT （Hardware Fault Tolerance）  硬件故障裕度 |
|  | IFAT （Integrated Factory Acceptance Testing）  集成工厂验收测试 |
|  | LOPA （Layer of Protection Analysis）  保护层分析 |
|  | MTTR （Mean Time To Restoration）  平均恢复时间 |
|  | PFH （Probability of Failure per Hour）  危险失效平均频率 |
|  | PST （Partial Stroke Test）  部分行程测试 |
|  | RRF （Risk Reduction Factor）  风险降低因子 |
|  | SFF （Safety Fraction Factor）  安全失效分数 |
|  | SRS （Safety Requirement Specification）  安全要求规格书 |
|  | STR （Spurious Trip Rate）  误停车率 |
| **3 安全生命周期** | **3 安全生命周期** |
| **3.1 一般规定** | **3.1 一般规定** |
| **3.1.1**石油化工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所需要的管理活动。 | **3.1.1**石油化工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，集成调试及验收测试阶段和操作维护阶段 | **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3.1.3）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、安全完整性等级评估及审查、安全仪表系统技术要求、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、调试及验收测试、安全仪表系统操作维护与变更、安全仪表系统功能测试、安全仪表系统停用等。  **图3.1.3 安全生命周期工作流程** | **3.1.3**安全生命周期工作（图3.1.3）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、安全完整性等级评估及审查、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3.1.3 安全生命周期工作流程** |
| **3.2.3**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/T20438、《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**。** | **3.2.3**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宜符合现行国家标准《电气/电子/可编程电子安全相关系统的功能安全》GB/T20438、《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/T 32857的有关规定。 |
| **3.2.4** 安全完整性等级可根据过程危险分析和保护层功能分配的结果评估并确定**。** | **3.2.4**安全完整性等级评估包括安全完整性等级分级和验证。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可通过计算安全仪表功能的要求时危险失效平均概率及其它相关参数，证明安全仪表功能满足安全技术要求及目标安全完整性等级的要求。 |
| **3.2.5**安全仪表系统技术要求可包括安全仪表功能及其安全完整性等级、过程安全状态、操作模式、检验测试间隔等。 | **3.2.5**安全仪表系统安全技术要求可通过编制安全要求规格书表述。安全要求规格书可基于企业风险标准，依据危险分析与风险评估（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可包括安全仪表功能及其安全完整性等级、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。 |
| **3.2.6**安全仪表系统基础工程设计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。 | **3.2.6**安全仪表系统的详细工程设计应符合安全技术要求，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、功能逻辑图或因果表等。 |
| **3.2.7**安全仪表系统的详细工程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、组态编程等。 | **3.2.7**安全仪表系统的详细工程设计应符合安全技术要求，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、功能逻辑图或因果表等。 |
| **3.3 集成、调试及验收测试** | **3.3 集成、调试、验收测试及确认** |
| **3.3.1**安全仪表系统集成、调试、验收测试，应符合安全仪表系统规格书及功能逻辑图的要求。 | **3.3.1**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。 |
| **3.3.2**安全仪表系统调试结果应符合安全仪表系统技术要求。 | **3.3.2**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。 |
| **3.3.3**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、系统软件和应用软件等，应符合安全仪表系统技术要求。 | **3.3.3**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。 |
|  | **3.3.4**安全仪表系统确认宜包括确认测量仪表、逻辑控制器、最终元件及关联设备的安装、测试与联合调试符合安全仪表系统安全技术要求和工程设计。 |
| **3.4 操作维护** | **3.4 运行维护** |
| **3.4.1**操作维护应遵循操作维护作业程序，应使操作维护过程符合安全仪表系统技术要求的功能安全。 | **3.4.1**运行维护应遵循运行维护作业程序，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。 |
| **3.4.2**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修改程序，并应按审批程序获得授权批准，不应改变设计的安全完整性等级，并应保留变更记录。 | **3.4.2**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修改程序，应对涉及的风险进行分析，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。 |
| **3.4.3**操作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、测量仪表和最终元件、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。 | **3.4.3**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、测量仪表和最终元件、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。 |
| **3.4.4**功能测试应按安全仪表系统的技术要求确定，并应按测试程序进行功能测试。 | **3.4.4**运行维护应建立检验测试程序，并按照安全仪表系统安全技术要求的检验测试间隔进行功能测试，做好记录。 |
| **4 安全完整性等级** | **4 安全完整性等级** |
| **4.1 一般规定** | **4.1 一般规定** |
| **4.1.3**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平均失效概率衡量，宜根据表4.1.3确定。  表4.1.3 安全仪表功能的安全完整性等级（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  （PFDavg） | | 4 | ≥10-5 到<10-4 | | 3 | ≥10-4 到<10-3 | | 2 | ≥10-3 到<10-2 | | 1 | ≥10-2 到<10-1 | | **4.1.3**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时危险失效平均概率（PFDavg）衡量，宜根据表4.1.3确定。  表4.1.3 安全完整性等级（低要求操作模式）   |  |  |  | | --- | --- | --- | | 安全完整性等级  （SIL） | 要求时危险失效平均概率  （PFDavg） | 风险降低因子  （RRF） | | 4 | ≥10-5 到<10-4 | >10000到≤100000 | | 3 | ≥10-4 到<10-3 | >1000到≤10000 | | 2 | ≥10-3 到<10-2 | >100到≤1000 | | 1 | ≥10-2 到<10-1 | >10到≤100 | |
| **4.1.4**在高要求操作模式时，安全仪表功能的安全完整性等级应采用每小时危险失效频率衡量，宜根据表4.1.4确定。  表4.1.4安全仪表功能的安全完整性等级（高要求操作模式）   |  |  | | --- | --- | | 安全完整性等级  （SIL） | 高要求操作模式的危险失效频率（每小时） | | 4 | ≥10-9 到< 10-8 | | 3 | ≥10-8 到< 10-7 | | 2 | ≥10-7 到< 10-6 | | 1 | ≥10-6 到< 10-5 | | **4.1.4**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4.1.4确定。  表4.1.4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 | ≥10-9 到< 10-8 | | 3 | ≥10-8 到< 10-7 | | 2 | ≥10-7 到< 10-6 | | 1 | ≥10-6 到< 10-5 | |
|  | **4.1.5**安全完整性等级分级为SIL a或SIL 0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。SIL a或SIL 0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。 |
| **4.2 安全完整性等级评估** | **4.2 安全完整性等级评估** |
|  | **4.2.1** 安全完整性等级评估包括安全完整性等级分级和安全完整性等级验证**。** |
|  | **4.2.2** 安全完整性等级分级 |
| **4.2.1**安全完整性等级评估宜包括下列内容：  1 确定每个安全仪表功能的安全完整性等级；  2 确定诊断、维护和测试要求 | **4.2.2.1** 安全完整性等级分级宜包括以下内容：  1 确定每个安全仪表功能的安全完整性等级；  2 明确每个安全仪表功能的操作模式及功能要求；  3 明确每个安全仪表功能的可用性要求（若需要）； |
| **4.2.2** 安全完整性等级评估方法应根据工艺过程复杂程度、国家现行标准、风险特性和降低风险的方法、人员经验等确定。主要方法应包括保护层分析法、风险矩阵法、校正的风险图法、经验法及其他方法。 | **4.2.2.2** 安全完整性等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。主要方法应包括保护层分析法、风险矩阵法、校正的风险图法、经验法及其它方法。 |
| **4.2.3**安全完整性等级评估宜采用审查会形式。审查的主要文件宜包括管道与仪表流程图（P&ID）、工艺说明书、装置及设备布置图、危险区域划分图、安全联锁因果表及其他有关文件。参加评估的主要人员宜包括工艺、过程控制（仪表）、安全、设备、生产操作及管理等方面。 | **4.2.2.3** 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、危险和可操作性研究（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。 |
|  | **4.2.3**安全完整性等级验证 |
|  | **4.2.3.1** 安全仪表功能的安全完整性等级应进行验证。硬件安全完整性验证内容宜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。 |
|  | **4.2.3.2** 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。 |
|  | **4.2.3.3** 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。 |
|  | **4.2.3.4** 当安全仪表功能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）。 |
| **5 设计基本原则** | **5 设计基本原则** |
| **5.0.1**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功能、安全完整性等级等要求。 | **5.0.1**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。 |
| **5.0.3** 安全仪表系统应由测量仪表、逻辑控制器和最终元件等组成。 | **5.0.3** 安全仪表系统应由测量仪表、逻辑控制器、最终元件和关联设备组成。 |
| **5.0.4**安全仪表系统的功能应根据过程危险及可操作性行分析，人员、过程、设备及环境的安全保护，以及安全完整性等级等要求确定。 | **5.0.4** 此条删除。 |
| **5.0.5**石油化工工厂或装置的安全完整性等级不应高于SIL3级。 | **5.0.5**石油化工工厂或装置安全仪表功能的安全完整性等级不应高于SIL3级。 |
| **5.0.6**安全仪表系统应符合安全完整性等级要求。安全完整性等级可采用计算安全仪表系统的失效概率的方法确定。 | **5.0.6** 此条删除。 |
| **5.0.7**安全仪表系统可实现一个或多个安全仪表功能，多个安全仪表功能可使用同一个安全仪表系统。当多个安全仪表功能在同一个安全仪表系统内实现时，系统内的共用部分应符合各功能中最高安全完整性等级要求。 | **5.0.7**安全仪表系统可实现一个或多个安全仪表功能，多个安全仪表功能可使用同一个安全仪表系统。当不同安全完整性等级的安全仪表功能在同一个安全仪表系统内实现时，系统内的共用部分应符合各安全仪表功能中最高安全完整性等级要求。 |
| **5.0.9**安全仪表系统不应介入或取代基本过程控制系统的工作。 | **5.0.9**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或指令不应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。 |
| **5.0.10**基本过程控制系统不应介入安全仪表系统的运行或逻辑运算。 | **5.0.10** 此条删除。 |
| **5.0.11**安全仪表系统应设计成故障安全型。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。 | **5.0.11**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。 |
| **5.0.13**安全仪表系统的中间环节应少。 | **5.0.13**安全仪表系统的中间环节应尽可能少。 |
| **5.0.16**安全仪表系统的交流供电宜采用双路不间断电源的供电方式。 | **5.0.16**安全仪表系统的交流供电应采用UPS供电，宜采用双路不间断电源的供电方式。 |
| **5.0.20**安全仪表系统内的设备宜设置同一时钟。 | **5.0.20**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。 |
| **6 测量仪表** | **6 测量仪表** |
| **6.1 一般规定** | **6.1 一般规定** |
| **6.1.6** 测量仪表及取源点宜独立设置。 | **6.1.6**安全仪表系统的测量仪表宜独立于基本过程控制系统设置。对于与基本过程控制系统共用仪表本体的测量仪表，安全仪表系统测量仪表的取源点、引压管线、传感器等应独立设置，不应与基本过程控制系统共用。 |
| **6.2 测量仪表的独立设置** | **6.2 测量仪表的独立设置** |
| **6.2.1** SIL 1级安全仪表功能，测量仪表可与基本过程控制系统共用。 | **6.2.1** SIL 1级安全仪表功能，测量仪表宜与基本过程控制系统分开。 |
| **6.2.2** SIL 2级安全仪表功能，测量仪表宜与基本过程控制系统分开。 | **6.2.2** SIL 2级安全仪表功能，测量仪表应与基本过程控制系统分开。 |
| **6.3 测量仪表的冗余设置** | **6.3 测量仪表的冗余设置** |
|  | **6.3.1**测量仪表的冗余设置分为安全性冗余和可用性冗余。 |
|  | **6.3.2** 测量仪表的安全性冗余设置： |
| **6.3.1** SIL 1级安全仪表功能，可采用单一测量仪表。 | **1** SIL 1级安全仪表功能，可采用单一测量仪表。 |
| **6.3.2** SIL 2级安全仪表功能，宜采用冗余测量仪表。 | **2** SIL 2级安全仪表功能，宜采用冗余测量仪表。 |
| **6.3.3** SIL 3级安全仪表功能，应采用冗余测量仪表。 | **3** SIL 3级安全仪表功能，应采用冗余测量仪表。 |
|  | **6.3.3**当安全仪表功能的误动作造成的损失大于可容忍程度时，可按高可用性要求实施测量仪表的可用性冗余设置。测量仪表的可用性冗余设置不应降低安全仪表功能的安全完整性等级。 |
| **6.4 测量仪表的冗余方式** | **6.4 测量仪表的冗余方式** |
| **6.4.1** 当系统要求高安全性时，应采用 “或”逻辑结构。 | **6.4.1** 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会引起安全联锁动作。 |
| **6.4.2** 当系统要求高可用性时，应采用 “与”逻辑结构。 | **6.4.2** 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会引起安全联锁动作。 |
| **6.4.3** 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。 | **6.4.3** 当要求兼顾高安全性和高可用性时，测量仪表宜采用三取二逻辑结构。 |
|  | **6.4.4** 冗余设置的测量仪表宜设置输入信号偏差报警。 |
| **6.5 开关量测量仪表** | **6.5 开关量测量仪表** |
| **6.5.3**重要的输入回路宜设置线路开路和短路故障检测。输入回路的开路和短路故障，宜在安全仪表系统中报警和记录。 | **6.5.3** 此条删除。 |
| **7 最终元件** | **7 最终元件** |
| **7.1 一般规定** | **7.1 一般规定** |
| **7.1.1**最终元件应包括控制阀（调节阀、切断阀）、电磁阀、电机等。 | **7.1.1**最终元件应包括控制阀（调节阀、切断阀）、电磁阀、电机控制器等。 |
| **7.1.2**最终元件宜采用气动控制阀。不宜采用电动控制阀。 | **7.1.2**最终元件宜采用气动控制阀。当无仪表气源供应时，也可采用电动控制阀或电液控制阀。当采用电动控制阀时，应采取安全措施。 |
| **7.1.3**最终元件的设置应满足安全完整性等级的要求。 | **7.1.3**最终元件的设置应满足安全仪表系统安全技术要求、安全完整性等级的要求。 |
| **7.2 控制阀的独立设置** | **7.2 控制阀的独立设置** |
| **7.2.1** SIL 1级安全仪表功能，控制阀可与基本过程控制系统共用，应确保安全仪表系统的动作优先。 | **7.2.1** 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。 |
| **7.2.2** SIL 2级安全仪表功能，控制阀宜与基本过程控制系统分开。 | **7.2.2** SIL 2级安全仪表功能，控制阀应与基本过程控制系统分开。 |
| **7.3 控制阀的冗余设置** | * 1. **控制阀的冗余设置** |
|  | **7.3.1** 控制阀的冗余设置分为安全性冗余和可用性冗余**。** |
|  | **7.3.2** 控制阀的安全性冗余设置： |
| **7.3.1** SIL 1级安全仪表功能，可采用单一控制阀。 | **1** SIL 1级安全仪表功能，可采用单一控制阀。 |
| **7.3.2** SIL 2级安全仪表功能，宜采用单一控制阀。 | **2** SIL 2级安全仪表功能，宜采用单一控制阀。 |
| **7.3.3** SIL 3级安全仪表功能，应采用冗余控制阀。 | **3** SIL 3级安全仪表功能，应采用冗余控制阀。 |
| **7.3.4** 控制阀冗余方式可采用一个调节阀和一个切断阀，也可采用二个切断阀。 | **7.3.3**当安全仪表功能的误动作造成的损失大于可容忍程度时，可按高可用性要求实施控制阀的可用性冗余设置。控制阀的可用性冗余设置不应降低安全仪表功能的安全完整性等级。 |
| **7.4 控制阀附件的配置** | **7.4 控制阀附件的配置** |
| **7.4.5**当系统要求高安全性时，冗余电磁阀宜采用“或”逻辑结构；当系统要求高可用性时，冗余电磁阀宜采用“与”逻辑结构。 | **7.4.5** 此条删除。 |
|  | **7.4.6** 当安全完整性等级验证不满足目标安全完整性等级时，控制阀可设置部分行程测试设施。 |
|  | **7.5 控制阀的冗余方式** |
|  | **7.5.1**当要求高安全性时，控制阀应采用安全性冗余结构，单一控制阀的动作会引起安全联锁动作。控制阀安全性冗余结构可采用二个切断阀，也可采用一个切断阀和一个调节阀。 |
|  | **7.5.2**当要求高可用性时，控制阀或电磁阀应采用可用性冗余结构，单一控制阀或电磁阀的动作不会引起安全联锁动作。 |
| **8 逻辑控制器** | **8 逻辑控制器** |
| **8.1 一般规定** | **8.1 一般规定** |
| **8.1.2**用于逻辑控制器的可编程电子系统应取得国家权威机构的功能安全认证。 | **8.1.2**用于逻辑控制器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。 |
| **8.2 逻辑控制器的独立设置** | **8.2 逻辑控制器的独立设置** |
| **8.2.1** SIL 1级安全仪表功能，逻辑控制器宜与基本过程控制系统分开。 | **8.2.1** SIL 1级安全仪表功能，逻辑控制器应与基本过程控制系统分开。 |
| **8.3 逻辑控制器的冗余设置** | **8.3 逻辑控制器的冗余设置** |
| **8.3.1** SIL 1级安全仪表功能，可采用冗余逻辑控制器。 | **8.3.1** SIL 1级安全仪表功能，应采用冗余逻辑控制器。 |
| **8.3.2** SIL 2级安全仪表功能，宜采用冗余逻辑控制器。 | **8.3.2** SIL 2级安全仪表功能，应采用冗余逻辑控制器。 |
| **8.4 逻辑控制器的配置** | **8.4 逻辑控制器的配置** |
| **8.4.1** 逻辑控制器应符合安全完整性等级要求，应独立完成安全仪表功能。 | **8.4.1** 逻辑控制器应符合安全仪表系统安全技术要求和安全完整性等级要求，应独立完成安全仪表功能。 |
| **8.4.2** 逻辑控制器硬件和软件版本应是正式发布版本。 | **8.4.2** 此条删除。 |
| **8.4.3** 逻辑控制器宜与基本过程控制系统的时钟保持一致。 | **8.4.3** 逻辑控制器宜与基本过程控制系统的时钟同步。 |
| **8.4.5** 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，应允许在线更换单元而不影响逻辑控制器的正常运行。 | **8.4.5** 逻辑控制器的中央处理单元、输入/输出单元、电源单元、通信单元等应为独立的单元，应允许在线更换单元而不影响逻辑控制器的正常运行。 |
| **8.4.6**逻辑控制器应有硬件和软件诊断和测试功能。诊断和测试信息应在工程师站或操作站显示、记录。 | **8.4.6**逻辑控制器应有硬件和软件诊断和测试功能。诊断和测试信息应在工程师站或操作员站显示、记录。 |
| **8.4.7**逻辑控制器的系统故障宜在安全仪表系统的操作站报警，也可在基本过程控制系统的操作站报警。 | **8.4.7**逻辑控制器的故障应在安全仪表系统的操作员站或基本过程控制系统的操作员站报警。 |
| **8.5 逻辑控制器的接口配置** | **8.5 逻辑控制器的接口配置** |
| **8.5.3** 冗余的最终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最终元件。 | **8.5.3** 冗余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。 |
| **8.5.5**本安回路应采用隔离式安全栅。 | **8.5.5** 此条删除。 |
| **8.5.6**需要线路检测的回路，应采用带有线路短路和开路检测功能的输入、输出卡。 | **8.5.6**重要的输入/输出回路宜具有线路开路和短路检测功能，在安全仪表系统中报警和记录。 |
|  | **8.5.7**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、开关信号宜配置隔离继电器。 |
| **9 通信接口** | **9 网络和通信接口** |
| **9.1 一般规定** | **9.1 一般规定** |
| **9.1.1**安全仪表系统与基本过程控制系统通信宜采用RS485串行通信接口，MODBUS RTU或TCP/IP通信协议。 | **9.1.1**安全仪表系统与基本过程控制系统通信宜采用RS485串行通信接口，MODBUS RTU通信协议。当采用MODBUS TCP/IP通信协议接入基本过程控制系统的交换机时，应采取网络安全措施。 |
| **9.1.2**安全仪表系统与基本过程控制系统通信接口宜冗余配置。冗余通信接口应有诊断功能。 | **9.1.2**安全仪表系统与基本过程控制系统通信接口应冗余配置。冗余通信接口应有诊断功能。 |
| **9.2 通信接口的配置** | **9.2 网络和通信接口的配置** |
| **9.2.1**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。 | **9.2.1**通信接口的故障不应影响安全仪表系统的安全功能。通信接口故障应在安全仪表系统的操作员站或工程师站显示、报警。 |
| **9.2.2**网络通信接口负荷不应超过50%。 | **9.2.2**网络和通信接口负荷不应超过50%，采用以太网的通信负荷不应超过20%。 |
|  | **9.2.3**安全仪表系统应通过冗余配置的交换机组网。安全仪表系统不同网络分区应相互隔离。 |
|  | **9.2.4**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。 |
|  | **9.3 网络信息安全** |
|  | **9.3.1** 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。 |
|  | **9.3.2** 安全仪表系统不应与工厂管理网络直接相连。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。 |
|  | **9.3.3** 安全仪表系统不应接入无线仪表和无线网络。 |
|  | **9.3.4** 安全仪表系统的服务器、操作员站、工程师站及其它终端设备应采取防病毒等保护措施。防病毒软件宜采用基于信任机制的白名单技术。 |
| **10 人机接口** | **10 人机接口** |
| **10.1 操作员站** | **10.1 操作员站** |
| **10.1.2**安全仪表系统应采用操作员站作为过程信号报警和联锁动作报警的显示和记录。 | **10.1.2**安全仪表系统的操作员站应作为过程信号报警和联锁动作报警的显示和记录。 |
| **10.1.3**操作员站不应修改安全仪表系统的应用软件。 | **10.1.3**操作员站不应修改安全仪表系统的应用程序。 |
| **10.1.5**操作员站应提供程序运行，联锁动作，输入、输出状态，诊断结果等显示，并应具有报警及记录等功能。 | **10.1.5**操作员站应提供程序运行、联锁动作、输入、输出状态、诊断结果等显示、报警及事件记录等功能。 |
|  | **10.1.6**在操作员站可设置安全仪表系统安全联锁动作前的预报警。 |
| **10.2 辅助操作台** | **10.2 辅助操作台** |
| **10.2.4**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。 | **10.2.4**关键信号报警除在操作员站显示外，宜同时在辅助操作台显示。 |
| **10.2.5** 紧急停车按钮、开关、信号报警器等与安全仪表系统连接，应采用硬接线方式，不应采用通信方式。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。 | **10.2.5** 辅助操作台的紧急停车按钮、开关、信号报警器等与安全仪表系统连接，应采用硬接线方式，不应采用通信方式。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。 |
| **10.3 维护旁路开关的设置** | **10.3 维护旁路开关的设置** |
| **10.3.2** 采用软件开关的方式时，每个安全联锁单元宜设硬件旁路开关作为软件开关的“允许”条件。 | **10.3.2** 采用软件开关的方式时，每个安全联锁单元或工艺区域应设“允许旁路”开关作为软件维护旁路开关的“允许”条件。 |
|  | **10.3.4** 应制定维护旁路操作程序，维护旁路操作和旁路状态时应能监测工艺过程状态，并定期提示操作员安全仪表功能处于维护旁路状态，直至旁路解除。 |
| **10.4 操作旁路开关的设置** | **10.4 操作旁路开关的设置** |
|  | **10.4.4** 应制定操作旁路操作程序，操作旁路操作和旁路状态时应能监测工艺过程状态，并定期提示操作员安全仪表功能处于操作旁路状态，直至旁路解除。 |
| **10.5 复位按钮的设置** | **10.5 复位按钮的设置** |
| **10.5.1** 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按钮；  3 在辅助操作台设置硬件按钮； | **10.5.1** 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按钮；  3 在辅助操作台设置硬件按钮；  4 在最终元件现场设置硬件开关（若需要）。 |
| **10.5.2** 复位按钮的动作应设置报警和记录。 | **10.5.2** 复位按钮的动作应设置事件记录。 |
| **10.6 紧急停车按钮的设置** | **10.6 紧急停车按钮的设置** |
| **10.6.1** 紧急停车按钮应设置在辅助操作台上。 | **10.6.1** 紧急停车按钮宜设置在辅助操作台或现场，应带防护罩。 |
| **10.7 工程师站及事件顺序记录站** | **10.7 工程师站及事件顺序记录站** |
| **10.7.1** 安全仪表系统应设工程师站。工程师站应用于安全仪表系统组态编程、系统诊断、状态监测、编辑、修改及系统维护。 | **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。工程师站应用于安全仪表系统组态编程、系统诊断、状态监测、编辑、修改及系统维护。 |
| **10.7.5** 工程师站和事件顺序记录站，宜采取防病毒等保护措施。 | **10.7.5** 此条删除。 |
| **11 应用软件** | **11 应用程序** |
| **11.1 组态及编程** | **11.1 组态及编程** |
| **11.1.1** 应用软件的逻辑功能应采用布尔逻辑及布尔代数运算规则。应用软件的逻辑设计宜采用正逻辑。 | **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** 应用软件的组态宜采用功能逻辑图或布尔逻辑表达式。 | **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** 应用软件的组态应使用制造厂的标准组态工具软件。 | **11.1.3** 应用程序的组态应使用制造厂的标准组态工具软件。 |
| **11.1.4** 应用软件组态工具软件应具有下列功能：  1 区分应用软件版本；  2 组态检查；  3 提供标准功能模块；  4 组态管理、仿真及测试； | **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功能。 |
|  | **11.1.5** 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。 |
| **11.2 应用软件的安全性** | **11.2 应用程序的安全性** |
| **11.2.1** 应用软件的安全控制应包括应用软件设计、软件组态及编程、软件集成、软件运行和维护管理、系统确认等。 | **11.2.1** 应用程序的安全控制应包括应用程序设计、组态及编程、验收测试、确认、运行维护、变更、检验测试等。 |
|  | **11.2.1A** 应用程序应通过审查、分析、仿真及测试技术和活动确认功能满足安全技术要求和工程设计文件的要求，并形成记录。 |
| **11.2.2** 应用软件组态编程应进行离线测试后再下载投入运行。 | **11.2.2** 应用程序组态编程应进行离线测试后再下载投入运行。 |
| **11.2.3** 数据宜采用光盘进行复制，磁介质文件的复制应防止病毒。 | **11.2.3** 数据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。 |
| **11.2.4** 应用软件应同时进行本地备份和异地备份。 | **11.2.4** 应用程序应同时进行本地备份和异地备份。 |
| **11.3 应用软件的设计和组态** | **11.3 应用程序的设计和组态** |
| **11.3.1** 应用软件文件应包括下列内容：  1 应用软件说明；  2 输入点、输出点、通信点清单；  3 功能逻辑图；  4 文档要求。 | **11.3.1** 应用程序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 文档要求。 |
| **11.3.3** 应用软件组态编程应与功能逻辑图、因果表或逻辑功能说明一致。程序执行顺序及时间应符合过程安全的要求。 | **11.3.3** 应用程序组态编程应与安全仪表系统安全技术要求、功能逻辑图、因果表或逻辑功能说明一致。程序执行顺序及时间应符合过程安全的要求。 |
| **11.3.4** 应用软件组态文件应包括功能逻辑图、用户手册、使用说明等。 | **11.3.4** 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。 |
| **11.3.4** 采用逻辑语音的软件组态文件还应包括源程序、程序说明等。 | **11.3.4** 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。 |
| **12 工程设计** | **12 工程设计** |
| **12.1 基础工程设计** | **12.1 基础工程设计** |
| **12.1.1** 安全仪表系统测量仪表、安全仪表控制系统、安全仪表系统最终元件的技术规格书，应根据完全完整性等级进行编制。 | **12.1.1** 安全仪表系统测量仪表、安全仪表系统逻辑控制器、安全仪表系统最终元件的技术规格书，应根据相关工艺要求和安全仪表系统安全技术要求进行编制。 |
| **12.1.2** 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、工艺管道及仪表流程图等进行编制，应包括下列内容：   1. 功能逻辑图、因果表及复杂逻辑功能说明； 2. 安全仪表控制系统技术规格书； 3. 安全仪表系统测量仪表、安全仪表系统最终元件的选型原则及技术规格书。 | **12.1.2** 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、工艺管道及仪表流程图等进行编制，应包括下列内容：   1. 功能逻辑图、因果表及复杂逻辑功能说明； 2. 安全仪表系统逻辑控制器技术规格书；   3 安全仪表系统测量仪表、安全仪表系统最终元件的选型原则及技术规格书。 |
| **12.1.3** 安全仪表控制系统技术规格书应包括下列主要内容： | **12.1.3** 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： |
| **12.2 详细工程设计** | **12.2 详细工程设计** |
| **12.2.1** 安全仪表系统详细工程设计文件应根据安全仪表系统基础工程设计文件及详细工程设计阶段的要求进行编制，应包括下列内容：  1 安全仪表控制系统技术规格书；  2 硬件配置图；  3 功能逻辑图、因果表及复杂逻辑功能说明；  4 输入、输出点清单；  5 联锁及报警设定值；  6 应用软件需要的技术资料。 | **12.2.1** 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详细工程设计阶段的要求进行编制，应包括下列内容：  1 安全仪表系统逻辑控制器技术规格书；  2 硬件配置图；  3 功能逻辑图、因果表及复杂逻辑功能说明；  4 输入、输出点清单；  5 联锁及报警设定值；  6 应用程序需要的技术资料。 |
| **12.2.2** 安全仪表控制系统合同技术附件，应包括系统硬件清单，软件清单，应用软件组态、生成、调试，操作和维护培训，工厂验收，现场验收及现场服务等。 | **12.2.2** 安全仪表系统逻辑控制器合同技术附件，应包括系统硬件清单，软件清单，应用程序组态、生成和调试，运行和维护培训，工厂验收，现场验收及现场服务等。 |
| **12.2.3** 详细工程设计文件应包括下列内容：   1. 系统总说明及配置图； 2. 操作站及机柜布置图； 3. 输入、输出卡件及端子布置图、接线图； 4. 供电及接地系统图； 5. 远程控制器或远程输入、输出卡件及端子布置、接线图； 6. 回路接线图； 7. 电缆（光缆）连接表； 8. 其它。 | **12.2.3** 详细工程设计文件应包括下列内容：   1. 系统总说明及配置图； 2. 操作员站、辅助操作台及机柜布置图； 3. 输入、输出卡件及端子布置图、接线图； 4. 供电及接地系统图； 5. 远程控制器或远程输入、输出卡件及端子布置、接线图； 6. 回路接线图（表）； 7. 电缆（光缆）连接表； 8. 其它。 |
| **13 组态、集成与调试、验收测试** | **13 组态、集成与调试、验收测试与确认** |
| **13.1 组态、集成与调试** | **13.1 组态、集成与调试** |
| **13.1.1** 安全仪表控制系统工程文件应包括下列主要内容： | **13.1.1** 安全仪表系统逻辑控制器工程文件应包括下列主要内容： |
| **13.1.3** 应用软件组态应满足功能逻辑图和因果表的要求。系统软件、应用软件编译、调试及下装，应经过完整、详细地检查和测试。 | **13.1.3** 应用程序组态应满足功能逻辑图和因果表的要求。系统软件、应用程序编译、调试及下装，应经过完整、详细地检查和测试。 |
| **13.2 验收测试** | **13.2 验收测试** |
| **13.2.1** 验收测试应包括工厂验收测试、工厂联合测试和现场验收测试。 | **13.2.1** 安全仪表系统逻辑控制器的验收测试应包括工厂验收测试、工厂集成验收测试和现场验收测试。 |
| **13.2.3** 工厂联合测试应包括下列主要内容：  1 与基本过程控制系统的工厂联合测试宜在基本过程控制系统制造厂进行；  2 在基本过程控制系统工厂完成安全仪表系统通信测试、软件画面测试等；  3 与其它控制系统的工厂联合测试宜在安全仪表系统制造厂进行；  4 在安全仪表系统制造厂完成与其它控制系统的通信测试、软件画面测试等；  5 工厂联合测试完成，测试报告签字。 | **13.2.3** 工厂集成验收测试应包括下列主要内容：  1 与基本过程控制系统的工厂集成验收测试宜在基本过程控制系统制造厂进行；  2 在基本过程控制系统工厂完成安全仪表系统通信测试、软件画面测试等；  3 与其它控制系统的工厂集成验收测试宜在安全仪表系统制造厂进行；  4 在安全仪表系统制造厂完成与其它控制系统的通信测试、软件画面测试等；  5 工厂集成验收测试完成，测试报告签字。 |
|  | **13.3 确认** |
|  | **13.3.1** 安全仪表系统投入使用前宜开展确认工作。 |
|  | **13.3.2** 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整改；  2 安全仪表系统的测量仪表、逻辑控制器、最终元件及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；  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； |
| **14 操作维护与变更管理** | **14 运行维护与变更管理** |
| **14.0.1** 操作维护管理应包括操作维护规程、维护人员职责、定期诊断测试计划及报告、停车期间的系统检查、维护旁路开关及操作旁路开关的使用等。 | **14.0.1** 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、维护旁路开关及操作旁路开关的使用等。 |
| **14.0.2** 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、变更软件功能的离线测试与检查、变更报告及操作维护规程更新等。 | **14.0.2** 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。 |
|  | **14.0.3** 所有的运行维护和变更应记录归档，并定期进行功能安全分析评估。 |
| **15 文档管理** | **15 文档管理** |
| **15.0.1** 安全生命周期各阶段的文档应包括安全仪表系统的工程设计、应用软件组态编程、设计审查等文件，磁介质和纸介质文件应同时存档保存。 | **15.0.1** 安全生命周期工程设计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，电子版文件和纸质版文件应同时异地存档保存。 |
| **15.0.2** 文档管理应包括文件命名规则、文件格式、文件传递方式、文件控制规程、文件审核流程及文件版本管理等。 | **15.0.2** 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。 |

中华人民共和国国家标准

**石油化工安全仪表系统设计规范**

**Code for design of safety instrumented systems**

**In petrochemical engineering**

**GB 50770—2013**

**（20XX年版）**

**条文说明**