ICS 71.120
CCS G 00

中 国 仪 器 仪 表 学 会 标 准

T/CIS 71001—2021

化工安全仪表系统安全要求规格书编制导则

Guidelines for developing safety requirements specification of chemical process safety instrumented systems

中国仪器仪表学会　　发 布

中国仪器仪表学会(China Instrument and Control Society)简称 CIS，是中国仪器仪表与测量控制科学技术工作者自愿组成并依法登记成立的学术性、公益性、非营利性社团法人，是联系仪器仪表与测量控制科技工作者的桥梁和纽带，是发展中国仪器仪表与测量控制科学技术事业的重要社会力量。

地址：北京市海淀区知春路 6 号锦秋国际大厦 A 座 23 层　　邮编：100088
电话：86-10-82800385　　传真：86-10-82800485
网址：www.cis.org.cn　　电子邮箱：scis@cis.org.cn

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。

本文件由中国仪器仪表学会提出并归口。

本文件起草单位：中国石化工程建设有限公司、泰莱思（天津）化工科技有限公司、中国化学品安全协会、中国石化安全工程研究院、中沙天津石化有限公司、中国寰球工程有限公司、中国成达工程有限公司、北京龙湖安全技术研究院、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、汉威科技集团股份有限公司、上海工业自动化仪表研究院有限公司。

本文件主要起草人：黄步余、徐志杰、李文悦、李玉明、范宗海、林融、李少鹏、于宝全、王雪梅、曾裕玲、朱凌云、高生军、张建国、俞文光、范怿涛、牛小民、张艾森。

化工安全仪表系统安全要求规格书
编制导则

1 范围

本文件规定了化工安全仪表系统安全要求规格书的编制原则、编制内容、编制流程、文件结构，并给出了文件结构的相关示例。

本文件适用于化工生产装置及其公用工程和辅助生产设施的安全仪表系统安全要求规格书的编制。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20438（所有部分） 电气／电子／可编程电子安全相关系统的功能安全

IEC 61511-1：2016 过程工业领域安全仪表系统的功能安全 第1部分：框架、定义、系统、硬件和应用程序的安全要求（Functional safety—Safety instrumented systems for the process industry sector—Part 1：Framework，definitions，system，hardware and application programming requirements）

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全仪表功能 safety instrumented function；SIF

由安全仪表系统实现的安全功能。

3.2

安全仪表系统 safety instrumented system；SIS

实现一个或多个SIF的仪表系统。

注：SIS由传感器、逻辑控制器和最终元件任意组合而成，还包括通信和辅助设备、软件及人的行动等。

3.3

安全完整性 safety integrity

SIS在需要时执行所需SIF的能力。

注1：此定义等同于SIS关于所需SIF的可靠性。通常被理解为经济概念而非安全概念的可靠性并没有被用来避免混淆。

注2：能力既包括功能响应（例如，在指定时间内关闭指定阀门），也包括SIS将按要求动作的可能性。

注3：在确定安全完整性时，可以包括导致不安全状态的随机硬件和系统失效的所有原因（例如，硬件失效、软件引起的失效以及由于电气干扰引起的失效）。此类失效中的某些失效，尤其是随机硬件失效，可以使用诸如平均危险失效频率或要求时失效概率之类的措施进行量化。然而，安全完整性还取决于许多系统因素，这些因

素无法准确量化，并且在整个生命周期中通常被定性地考虑。通过硬件容错或其他方法和技术，可以减少系统失效导致SIS危险失效的可能性。

注4：安全完整性包括硬件安全完整性和系统安全完整性，但也可以考虑由硬件和系统交互结合造成的复杂失效。

[来源：IEC 61511-1：2016，3.2.68，有修改]

3.4

安全完整性等级　safety integrity level；SIL

分配给SIF的不同等级（SIL1～SIL4），明确SIS实现的安全完整性要求。

注1：SIL等级越高，低要求模式的平均失效概率，或连续模式/高要求模式的平均危险失效频率越低。

注2：目标失效范围与SIL等级之间的对应关系详见IEC 61511-1：2016中的表4和表5。

注3：SIL4为最高级，SIL1为最低级。

[来源：IEC 61511-1：2016，3.2.69，有修改]

3.5

安全要求规格书　safety requirements specification；SRS

包含所有SIF和与之相关的SIL要求的规范性文件。

[来源：IEC 61511-1：2016，3.2.72，有修改]

3.6

SIS安全生命周期　SIS safety life cycle

从工程概念设计开始到所有SIF停止使用期间，SIS实现SIF涉及的所有必要活动。

3.7

保护层　protection layer

通过控制、预防或减缓来降低风险的任何独立措施。

注：保护层可以是一种工艺工程机制，例如：含有危险化学品的容器的尺寸，一种机械机制，例如：安全阀、SIS或一种管理程序，例如：针对迫在眉睫的危险的应急计划。这些响应可能是自动的，也可能由人的行动触发。

[来源：IEC 61511-1：2016，3.2.57，有修改]

3.8

独立保护层　independent protection layer

能够阻止场景向不期望后果发展，独立于场景初始事件或其他保护层的设备、系统或行动。

3.9

操作模式　mode of operation

SIF的运行方式，可分为低要求模式、高要求模式或连续模式。

[来源：IEC 61511-1：2016，3.2.39，有修改]

3.10

表决　voting

构成SIF子系统的一个或多个组件之间的逻辑关系。

3.11

传感器　sensor

基本过程控制系统或SIS中测量或检测过程变量的部件。

注：例如变送器、转换器、过程开关及位置开关。

3.12

风险　risk

伤害发生概率与伤害严重程度的组合。

[来源：IEC 61511-1：2016，3.2.61，有修改]

3.13

功能安全　functional safety

与过程和基本过程控制系统有关的整体安全的组成部分，它取决于 SIS 和其他保护层的正常功能执行。

3.14

故障　fault

可导致功能单元执行要求功能的能力降低或丧失的异常状况。

3.15

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、其他可编程系统和/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，但并不执行任何 SIF。

注 1：基本过程控制系统包括为确保（工艺）过程按所期望方式运行所必需的所有设备。

注 2：基本过程控制系统通常可以实现各种功能，例如：过程控制功能，监视和报警。

[来源：IEC 61511-1：2016，3.2.3，有修改]

3.16

检验测试　proof test

为了检测 SIS 隐性的危险故障而开展的周期性测试。在必要时，通过维护将 SIS 恢复为“新”的状态或者尽可能接近该状态。

[来源：IEC 61511-1：2016，3.2.56，有修改]

3.17

逻辑控制器　logic solver

基本过程控制系统或 SIS 中执行一个或多个逻辑功能的部分。

3.18

旁路　bypass

阻止执行全部或部分 SIS 功能的动作或设施。

注 1：旁路的示例包括：

——跳车逻辑的输入信号被阻止，但仍可以向操作人员呈现输入参数和报警。

——跳车逻辑至最终元件的输出信号保持在能够防止最终元件动作的正常状态。

——最终元件周围设置有物理旁路管线。

——预先选择的输入状态（例如，开/关输入）或通过工程工具（例如，在应用程序中）强制设置。

注 2：其他术语也用于指代旁路，例如：超驰、禁用、强制、禁止或静音。

[来源：IEC 61511-1：2016，3.2.4，有修改]

3.19

平均恢复时间　mean time to restoration；MTTR

完成功能恢复的预计时间。

注：包括检测到故障的时间、维修开始前花费的时间、有效维修时间以及组件重新投运之前的时间。

3.20

失效　failure

丧失按要求执行的能力。

注 1：设备失效是导致该设备故障状态的事件。

注 2：如果能力的丧失由潜在故障引起，则遇到特定情况时便会发生失效。

注 3：所需功能的性能必然会排除某些运行状况，某些功能可能会根据要避免的运行状况进行指定，而这种运行状况的出现便是一种失效。

注 4：失效可以是随机的，也可以是系统性的。

[来源：IEC 61511-1：2016，3.2.18，有修改]

3.21

过程安全时间　process safety time

SIF 未动作的情况下，从过程参数出现偏离或基本过程控制系统出现故障（有可能引发危险事件）到危险事件发生之间的时间。

3.22

诊断　diagnostics

以发现故障为目的的频繁（相对于过程安全时间）自动测试。

3.23

最终元件　final element

基本过程控制系统或 SIS 中实现或维持安全状态所需物理动作的设备。

4　编制原则

SRS 的内容应基于企业风险标准，依据危险与风险评估（如独立保护层分析）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。

5　编制内容

5.1　基本原则

5.1.1　依据本文件设计的 SIS 系统应符合 GB/T 20438（所有部分）和 IEC 61511-1：2016 的规定。

5.1.2　SRS 的编制应依据危险与风险评估结果，明确 SIS 的通用功能要求和实现功能安全的硬件、软件、工程、管理、运维等要求。

5.1.3　SRS 提出的功能安全要求应清晰、明确，可验证、可维护、可操作，能用于指导 SIS 生命周期各阶段的使用者理解和执行。

5.1.4　SRS 的内容宜包括应用程序的安全要求。

5.2　主要内容

5.2.1　列出所有 SIF 的功能说明，可采用因果表、逻辑说明或逻辑图。

5.2.2　列出各 SIF 相关的输入输出设备清单，通过设备位号予以识别。

5.2.3　识别并考虑共因失效要求。

5.2.4　定义每个已识别的 SIF 的过程安全状态。

5.2.5　定义单个危险事件的过程安全状态，以及多个危险事件同时发生时可能造成的额外风险。如装置跳车时多个设备同时排放至火炬可能产生新的风险。

5.2.6　识别每个 SIF 的危险源，确定危险发生的概率。

5.2.7　确定检验测试间隔的相关要求。

5.2.8　确定检验测试实施的相关要求。

5.2.9　确定每个 SIF 的响应时间要求。通常 SIF 的响应时间是指从信号检测、逻辑处理到最终元件动作完成的响应时间之和。

5.2.10 列出每个 SIF 的 SIL 等级和操作模式(如要求模式、连续模式)。

5.2.11 列出 SIS 过程测量形式、量程范围、精确度等级及联锁设定值等。

5.2.12 列出 SIF 过程输出动作及成功操作的标准,如控制阀的泄漏等级。

5.2.13 说明每个 SIF 输入与输出之间的功能关系,如逻辑关系、数学函数关系及允许触发条件等。

5.2.14 说明每个 SIF 手动停车要求,如控制室或现场手动关闭某台设备。

5.2.15 说明每个 SIF 得/失电联锁停车的相关要求。

5.2.16 说明每个 SIF 停车后的复位要求,如停车后最终元件手动、半自动或自动复位。

5.2.17 说明 SIF 最高允许的误停车率。

5.2.18 说明每个 SIF 的失效模式和 SIS 的预期响应,如报警、自动停车等。

5.2.19 说明 SIS 启动及重启程序的具体要求。

5.2.20 说明 SIS 与其他系统之间的接口要求,如过程接口、通信接口、人机接口等。

5.2.21 说明装置各种运行模式及每种模式下 SIF 操作的相关要求。装置运行模式通常包括开车、正常、牌号切换、其他特殊操作模式(如重启、火灾、低负荷等)。

5.2.22 识别装置内某单元或设备的正常和异常过程操作模式,说明是否需要额外增加 SIF。

5.2.23 说明旁路要求及旁路期间的管理要求,如维护旁路、操作旁路等。

5.2.24 说明 SIS 检测到故障事件时,为达到或保持过程的安全状态需采取的必要措施,及所有相关的人为因素。

5.2.25 确定 SIS 合理的 MTTR,综合考虑备品备件存储、地理位置、路程时间、服务合同、环境限制等。

5.2.26 识别需要避免的 SIS 输出状态的关联危险。

5.2.27 识别在运输、储存、安装及运行过程中 SIS 可能遇到的所有极端环境条件,如:温度、湿度、污染物、接地、电磁干扰(EMI)、射频干扰(RFI)、冲击、振动、静电、防爆、雷电、洪涝、腐蚀及其他相关因素。

5.2.28 确定在发生重大事故时所需任何 SIF 的要求,如控制阀在发生火灾事故时保持正常操作的时间、电缆的防火要求等。

5.3 应用程序的安全要求

5.3.1 列出应用程序支持的 SIF 功能及 SIL 等级。

5.3.2 列出实时性能参数,如 CPU 负荷、通信负荷等。

5.3.3 说明程序时序及时间延迟。

5.3.4 说明设备和操作员接口及其可操作性。

5.3.5 确定各种运行模式应用程序的要求。

5.3.6 确定对异常测量结果,如传感器超量程、变动幅度过大、测量值冻结、检测线路开路/短路等,应采取的措施。

5.3.7 确定应用程序运行所需的外部设备(如传感器和最终元件)的检验测试及诊断要求。

5.3.8 说明应用程序的监控,如应用看门狗、数据有效性确认。

5.3.9 说明 SIS 内其他设备的监控,如传感器、最终元件。

5.3.10 确定在工艺运行时 SIF 实施周期性测试的相关要求。

5.3.11 列出参考输入文件,如 SIF 清单、SIS 配置或结构、SIS 硬件安全完整性要求。

5.3.12 确定对通信接口的要求,如对接收和发送的数据或指令的限制措施、数据有效性检查。

5.3.13 识别并避免应用程序产生的过程危险状态,如同时关闭两个气体隔离阀可能产生压力波动,从而导致危险状态。

5.3.14　确定应用程序的其他安全要求，如联锁设定值的修改保护措施、应用程序的响应时间、功能验收测试、变更管理等。

6　编制流程

6.1　编制节点

SIS 安全生命周期及 SRS 编制活动在其中所处节点，如图 1 所示。

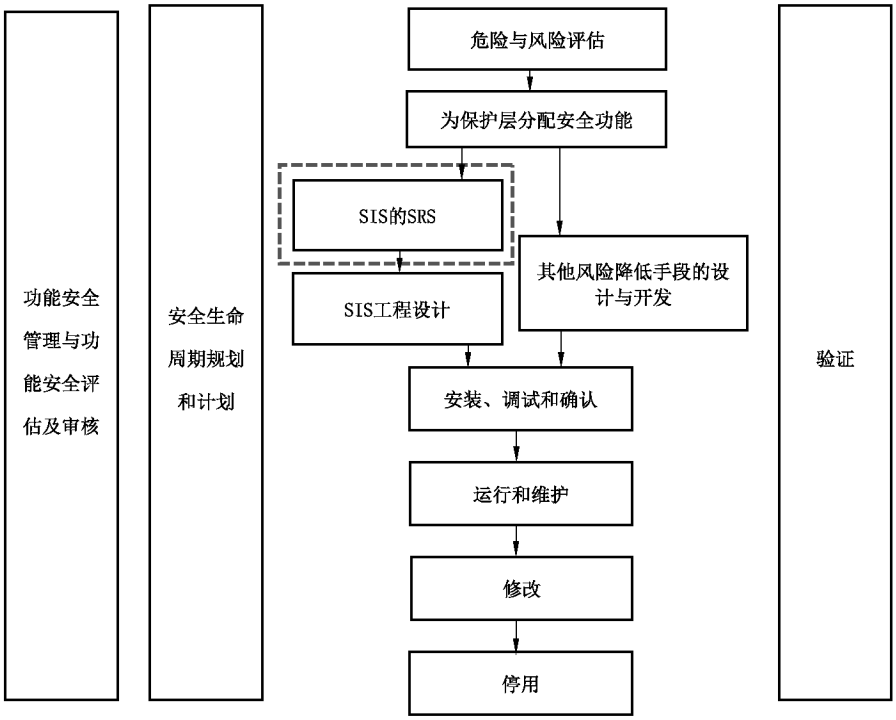
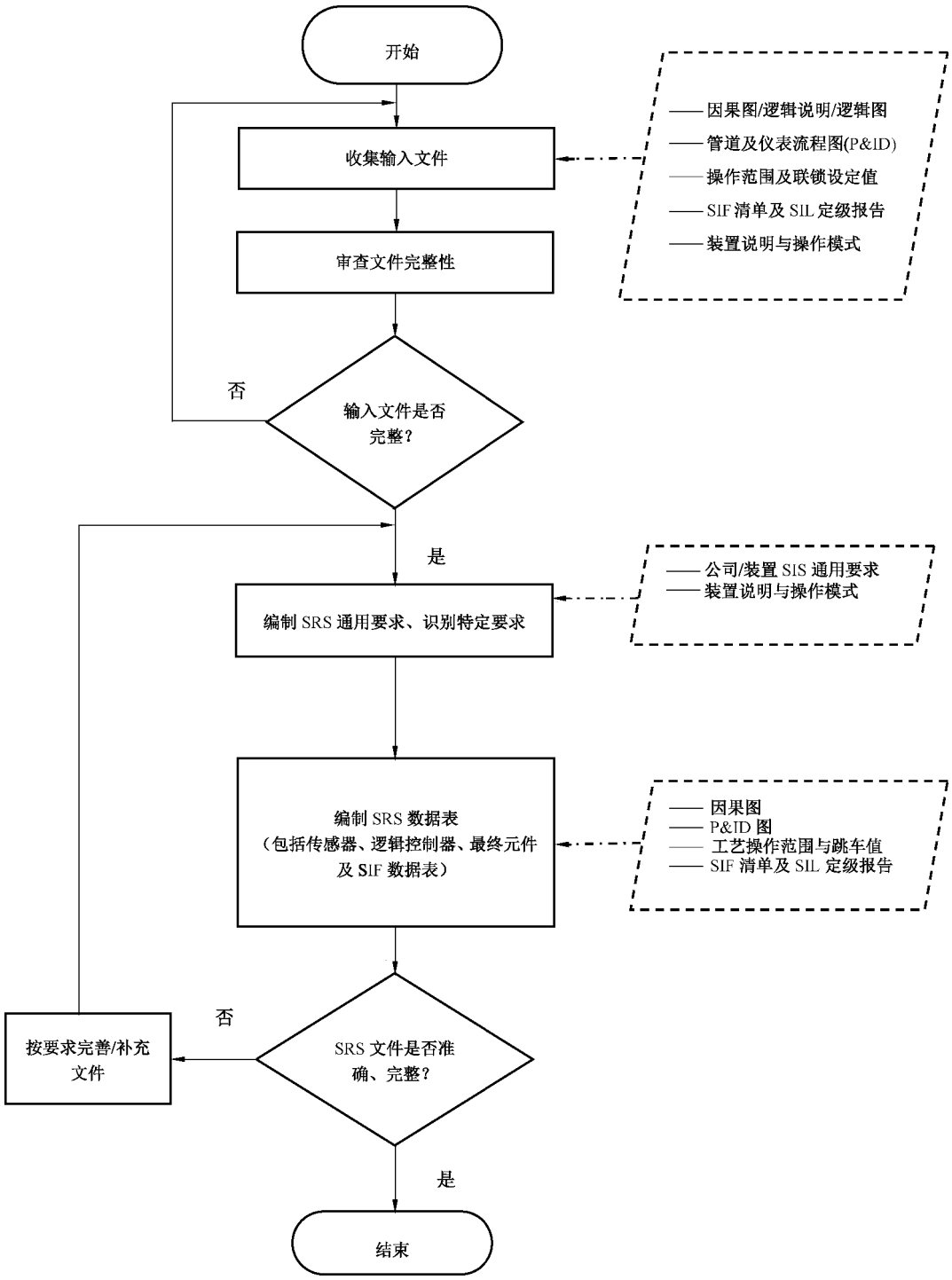


图 1　SIS 安全生命周期框图

6.2　编制流程图

典型的 SRS 编制流程如图 2 所示。



注：虚线框内容为该步骤对应的典型输入文件类型。

图 2　典型的 SRS 编制流程图

7 文件结构

7.1 SRS 文件的结构应包括通用要求、特定要求、SIF 清单、SRS 数据表、逻辑要求等。

典型的 SRS 文件结构示例见附录 A。

SRS 的通用要求主要来自危险与风险评估对 SIS 的要求，见 5.2 和 5.3 的内容要求。

SRS 的特定要求应单独列出。

7.2 SIF 清单包括 SIS 中的 SIF 说明、SIF 类型、SIL 等级、SIF 所有输入和输出设备、输入位号及表决逻辑、输出位号及表决逻辑、逻辑控制器以及 SIF 注释等。

典型 SIF 清单示例见附录 B。

7.3 SRS 数据表包括 SIF 数据表、传感器数据表、逻辑控制器数据表、最终元件数据表。

典型 SRS 数据表示例见附录 C。

7.4 逻辑要求宜采用因果表、逻辑说明或逻辑图的形式给出。

因果表示例见附录 D。

附 录 A
（资料性）
典型的 SRS 文件结构示例

下面给出了典型的 SRS 文件结构示例。

示例：

1 概述
- 1.1 项目背景
- 1.2 编写目的与适用范围
- 1.3 适用标准及规范
- 1.4 输入文件

2 术语及缩略语
- 2.1 术语
- 2.2 缩略语

3 SIS 的通用要求
- 3.1 定义
- 3.2 设计的要求
- 3.3 审查的要求
- 3.4 逻辑控制器
- 3.5 接口（如过程接口、通信接口、人机接口等）
- 3.6 顺序事件记录
- 3.7 环境条件
- 3.8 电源
- 3.9 动力中断（如电源、气源等）
- 3.10 软件的要求

4 SIF 的通用要求
- 4.1 SIF 说明
- 4.2 输入输出设备清单
- 4.3 共因失效要求
- 4.4 过程安全状态
- 4.5 检验测试间隔
- 4.6 检验测试实施
- 4.7 响应时间
- 4.8 装置运行模式（如开车、正常、牌号切换、火灾、低负荷等）
- 4.9 传感器
- 4.10 输出动作
- 4.11 功能关系
- 4.12 手动停车
- 4.13 得/失电联锁
- 4.14 停车复位
- 4.15 误停车率
- 4.16 失效模式
- 4.17 启动及重启
- 4.18 接口（如过程接口、通信接口、人机接口等）
- 4.19 SIS 操作模式（如要求模式、连续模式等）
- 4.20 旁路

附 录 B
（资料性）
SIF 清单示例

表 B.1 给出了 SIF 清单示例。

表 B.1 SIF 清单示例

序号	SIF 说明	SIF 类型	SIL 定级	输入		输入群组逻辑	输出		输出群组逻辑	逻辑控制器	SIF 注释
				位号	表决逻辑		位号	表决逻辑			

附 录 C
（资料性）
SRS 数据表示例

表 C.1～表 C.4 给出了 SRS 数据表中的 SIF 数据表、传感器数据表、逻辑控制器数据表和最终元件数据表的示例。

表 C.1 SIF 数据表示例

位号	类别
SIF 说明	
选定的 SIL 等级	SIF 群组
允许最高误停车率	
操作模式	设备位号
保护层分析(LOPA)参考	
LOPA 描述	
逻辑与运行	
装置运行模式的 SIF 正常/异常模式	
SIF 的特殊模式(开车、顺控等)	
过程安全状态	
过程安全时间	
过程安全时间	
SIF 响应时间	
测试	
检验测试间隔(月)	
测试程序(参考)	
复位	
复位	
注释	
极端环境条件	
意外事故时 SIF 要求	

表 C.2　传感器数据表示例

位号	设备类型
工况说明	
表决逻辑	SIF 群组
设备选择依据	参考数据
检验测试间隔(月)	MTTR(h)
测试类型	是否为安全关键
是否考虑共因失效	制造商/型号
认证的 SIL 等级	
输入详情	
信号类型	工程单位
量程上限	量程下限
联锁值	联锁值裕度
对故障的响应	诊断要求
旁路	
维护旁路	

表 C.3　逻辑控制器数据表示例

位号	设备类型
工况说明	
检验测试间隔(月)	MTTR(h)
系统响应时间	安全手册
认证的 SIL 等级	诊断要求
设备选择依据	制造商/型号

表 C.4　最终元件数据表示例

位号	设备类型
工况说明	
表决逻辑	SIF 群组
设备选择依据	参考数据
检验测试间隔(月)	MTTR(h)
测试类型	是否为安全关键
是否考虑共因失效	制造商/型号
最终元件动作方式	动作时间
成功动作标准	诊断要求
认证的 SIL 等级	
输出详情	
得/失电联锁	信号/动力中断时的动作
复位	
手动复位	
手动停车	
手动停车	
旁路	
维护旁路	
注释	
为避免重大事故损失对最终元件的要求	

附　录　D
（资料性）
因果表示例

表 D.1 给出了因果表的示例。

表 D.1　因果表示例

							输出或结果	电磁阀/控制阀位号	说明	P&ID号	表决	SIL等级	备注	图例：
输入或原因														
联锁号	仪表位号	说明	P&ID号	表决	SIL 等级	联锁值	备注							

T/CIS 71001—2021

中国仪器仪表学会标准

化工安全仪表系统安全要求规格书

编制导则

T/CIS 71001—2021

*

中国标准出版社出版发行

北京市朝阳区和平里西街甲2号(100029)

北京市西城区三里河北街16号(100045)

网址:www.spc.org.cn

服务热线:400-168-0010

2021年3月第一版

*

书号:155066·5-2876

T/CIS 71001-2021