ICS 13.200
CCS C 68

团　　体　　标　　准

T/CCSAS 054—2025

安全仪表系统(SIS)安全要求规格书(SRS)编写指南

Guidance for drafting safety requirements specification (SRS) of safety instrumented system (SIS)

2025-03-03 发布　　2025-03-03 实施

中国化学品安全协会　发布
中国标准出版社　出版

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国化学品安全协会提出并归口。

本文件起草单位：中科合成油工程有限公司、北京安必达科技有限公司、中国化学品安全协会、中国石化工程建设有限公司、中国安全生产科学研究院、惠生工程（中国）有限公司、山东济炼石化工程有限公司、中国成达工程有限公司、中石油华东设计院有限公司、中国化学赛鼎宁波工程有限公司、中国寰球工程有限公司、中石化宁波工程有限公司、万华化学集团股份有限公司、上海歌略软件科技有限公司、中海壳牌石油化工有限公司、巴斯夫（中国）有限公司、中石化广州工程有限公司、南京聚高工程技术有限公司、中化学赛鼎焦化（山西）工程科技有限公司、珠海安彦企业管理咨询有限公司、浙江石油化工有限公司、新疆天域海安安全技术服务有限公司。

本文件主要起草人：范咏峰、唐彬、王楠、林融、关磊、程泱、王云、张红东、刘友玲、冯建柱、曾裕玲、林洪俊、张志、王雪梅、杨晨、王琳、王成舫、孙金晓、李才华、王娇龙、代轶民、戴益、皮宇、樊清、朱东利、胡兰青、孙彦东、陆兴旺、奚春洪、白艳宏、翟庆伟、付丽君、甘露、荣彦栋、唐孟、陈洪沛、王渤、于森。

安全仪表系统(SIS)安全要求规格书(SRS)编写指南

1 范围

本文件提供了安全仪表系统(SIS)安全要求规格书(SRS)编写的总体要求、节点和流程、输入资料、内容、文件结构等方面的指导,并给出了SRS编写示例。

本文件适用于化工企业安全仪表系统(SIS)安全要求规格书(SRS)的编写。

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

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

3 术语和定义

GB/T 21109.1界定的以及下列术语和定义适用于本文件。

3.1

安全仪表系统 safety instrumented system; SIS

用于实现一个或多个SIF的仪表系统。

注1:SIS由测量仪表、逻辑控制器、最终执行机构,以及软件、通信和附属设备组合而成。

注2:附属设备包括:安全栅、电涌防护器、继电器、隔离器、电缆、引压管、电源、伴热等。

[来源:GB/T 21109.1—2022,3.2.67,有修改]

3.2

安全完整性等级 safety integrity level; SIL

为规定SIF应达到的安全完整性要求而分配给SIF的离散等级(4个等级中的一个)。

注1:SIL有且仅有4个等级,由低到高分别为SIL1、SIL2、SIL3、SIL4。

注2:SIL等级越高,期望的PFD_{avg}越低(低要求模式),或者导致危险事件的PFH越低(连续模式和高要求模式)。

注3:目标失效量和SIL间的关系见GB/T 50770的相关规定。

注4:SIL由SIL定级确定。

[来源:GB/T 21109.1—2022,3.2.69,有修改]

3.3

安全仪表功能 safety instrumented function; SIF

为了防止、减少危险事件发生或保持过程安全状态,由SIS实现具有特定SIL的安全功能。

注1:特定SIL由SIL定级确定,为SIL1、SIL2、SIL3、SIL4等级中的一个。没有SIL等级要求的安全功能不属于SIF。

注2:非安全关键测量仪表和非安全关键最终执行机构不属于SIF。

注 3：SIF 测量仪表和最终执行机构属于安全关键。

注 4：安全关键不一定属于 SIF，安全关键也可能属于 BPCS 联锁。

[来源：GB/T 50770—2013，2.1.9，有修改]

3.4

安全要求规格书　safety requirements specification；SRS

包含 SIS 的总体和通用要求、所有 SIF 要求和与之相关 SIL 要求的工程说明性和规范性文件。

[来源：GB/T 21109.1—2022，3.2.72，有修改]

3.5

SIS 安全生命周期　SIS safety life-cycle

从 SIS 和 SIF 工程方案设计开始到所有 SIF 停止使用期间，SIS 实现 SIF 的所有必要活动。

[来源：GB/T 21109.1—2022，3.2.70，有修改]

3.6

（SIF 的）运行模式　mode of operation（of a SIF）

SIF 的运行方式，包括：低要求模式、高要求模式、连续模式，含义如下：

a）　低要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率不大于一年一次；

b）　高要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率大于一年一次；

c）　连续模式：在这种运行模式下，SIF 作为正常运行的一部分保持过程处于一种安全状态。

[来源：GB/T 21109.1—2022，3.2.39，有修改]

3.7

测量仪表　sensor

BPCS 或 SIS 的一部分，测量过程变量的设备。

[来源：GB/T 50770—2013，2.1.16，有修改]

3.8

逻辑控制器　logic solver

BPCS 或 SIS 的一部分，执行逻辑功能的设备。

[来源：GB/T 50770—2013，2.1.17，有修改]

3.9

最终执行机构　final element

BPCS 或 SIS 的一部分，执行逻辑控制器指令或设定的动作，使过程达到安全状态的设备。

注：也称执行单元。

[来源：GB/T 50770—2013，2.1.18，有修改]

3.10

基本过程控制系统　basic process control system；BPCS

响应过程测量变量以及其他相关设备、仪表、控制系统或操作员的输入信号，按过程控制规律，产生输出信号实现过程控制及其相关设备运行的系统。

[来源：GB/T 50770—2013，2.1.19，有修改]

3.11

过程安全时间　process safety time

如果 SIF 未执行，从过程失效或 BPCS 失效（有可能引发危险事件）到危险事件发生之间的时间段。

注：用于确定 SIF 响应时间要求的过程安全时间指的是，当 SIF 未执行时，在预期的不利条件下，由过程固有特性决定的，从过程达到 SIF 联锁设定值开始到发生特定不可逆的危险状态的时间间隔。

[来源:GB/T 21109.1—2022,3.2.52.1,有修改]

3.12

联锁　interlock

根据对过程参数越限、设备等状态异常以及操作员手动等输入信号的逻辑判断,执行预先设定的动作。

[来源:HG/T 20511—2014,2.1.8,有修改]

3.13

安全关键　safety critical related

包括安全关键测量变量(测量仪表)和安全关键动作(最终执行机构)。

安全关键测量变量(测量仪表)指的是该变量(测量仪表)是发现工艺不安全状态必不可少的变量(测量仪表),只有该变量的检测才能确定发现工艺不安全状态。

安全关键动作(最终执行机构)指的是该动作(最终执行机构)是将工艺过程转入安全状态必不可少的动作(最终执行机构),只有该动作的执行才能将工艺过程转入安全状态。

3.14

非安全关键　non-safety critical related

包括非安全关键测量变量(测量仪表)和非安全关键动作(最终执行机构)。

非安全关键测量变量(测量仪表)指的是该变量(测量仪表)不是发现工艺不安全状态必不可少的变量(测量仪表),该变量没有被检测并不影响安全关键测量变量(测量仪表)可独立确定发现工艺不安全状态。

非安全关键动作(最终执行机构)指的是该动作(最终执行机构)不是将工艺过程转入安全状态必不可少的动作(最终执行机构),该动作没有被执行并不影响安全关键动作(最终执行机构)可独立将工艺过程转入安全状态。

3.15

操作模式　operating mode

过程操作的所有计划状态,包括的模式有:检修或紧急停车后的开车、正常操作、正常停车、临时操作、紧急操作、紧急停车、牌号切换等。

注:也称为过程操作模式(process operating mode)。

[来源:GB/T 21109.1—2022,3.2.45,有修改]

3.16

应用程序　application program

专用于用户应用的程序。通常,它包含为达到 SIS 功能要求而必要的控制输入、输出、计算和决策的逻辑顺序、许可、限制和表达式。

[来源:GB/T 21109.1—2022,3.2.76.1]

3.17

平均恢复时间　mean time to restoration;MTTR

预期的完全恢复的时间。

注:MTTR 包含:

——检测失效的时间(a);

——开始维修前的时间(b);

——实际的维修时间(c);

——组件恢复运行前的时间(d)。

(b)的开始时间是(a)的结束点;(c)的开始时间是(b)的结束点;(d)的开始时间是(c)的结束点。

[来源:GB/T 21109.1—2022,3.2.37.2]

3.18

平均维修时间　mean repair time;MRT

预期的整体维修时间。

注：MRT 包含 MTTR 时间中的时间段(b)、(c)和(d)(见 3.17)。

[来源:GB/T 21109.1—2022,3.2.37.1]

3.19

最大允许维修时间　maximum permitted repair time;MPRT

检测到失效后允许的最长维修时间。

注 1：MRT 可用作 MPRT,但是定义 MPRT 时可以不考虑 MRT。

——可选择小于 MRT 的 MPRT 来降低危险事件的可能性。

——如果可以放宽对危险事件可能性的约束,则可选择大于 MRT 的 MPRT。

注 2：如果定义了 MPRT,在计算随机硬件失效概率时可使用 MPRT 取代 MRT。

[来源:GB/T 21109.1—2022,3.2.37.3]

3.20

安全手册　safety manual

定义如何安全应用 SIS 设备、子系统或系统的信息。

注 1：安全手册可能包括来自制造商和用户的信息。

注 2：对于遵循 GB/T 20438(所有部分)的设备,来自制造商的信息就是安全手册。

注 3：这可能是一份独立文档,也可能是一份文档集。

[来源:GB/T 21109.1—2022,3.2.71,有修改]

3.21

安全失效分数　safe failure fraction;SFF

安全相关组件的属性,定义为平均安全失效率加上检测出的平均危险失效率,与平均安全失效率加上平均危险失效率之比。

注 1：$SFF=(\sum\lambda_{SDavg}+\sum\lambda_{SUavg}+\sum\lambda_{DDavg})/(\sum\lambda_{SDavg}+\sum\lambda_{SUavg}+\sum\lambda_{DDavg}+\sum\lambda_{DUavg})$。

其中,λ_{SD}为检测到的安全失效率;λ_{SU}为未检测到的安全失效率;λ_{DD}为检测到的危险失效率;λ_{DU}为未检测到的危险失效率,avg 代表平均失效率。

注 2：如失效率是常数失效率,$SFF=(\sum\lambda_{SD}+\sum\lambda_{SU}+\sum\lambda_{DD})/(\sum\lambda_{SD}+\sum\lambda_{SU}+\sum\lambda_{DD}+\sum\lambda_{DU})$。

[来源:GB/T 20438.4—2017,3.6.15,有修改]

3.22

确认　validation

通过检查和提供客观证据,证明用于规定用途的特定要求已经得到满足。

注：本文件中是指 SIS 安装完成后,在投入使用前开展的检查和提供客观证据的活动,用来证明 SIS 在各方面均满足 SRS 和 SIS 其他相关安全技术要求。

[来源:GB/T 21109.1—2022,3.2.86,有修改]

4　缩略语

下列缩略语适用于本文件。

ALARP:最低合理可行原则(As Low As Reasonably Practicable)

BPCS:基本过程控制系统(Basic Process Control System)

DC:诊断覆盖率(Diagnostic Coverage)

FIT:菲特(Failure In Time)

注：本文件中,1 FIT=1 failure/10^9 hours。

HAZOP:危险与可操作性分析(Hazard and Operability Studies)
HFT:硬件故障裕度(Hardware Fault Tolerance)
注:也称硬件容错。
IE:初始事件(Initiating Event)
IPL:独立保护层(Independent Protection Layer)
LOPA:保护层分析(Layer Of Protection Analysis)
MPRT:最大允许维修时间(Maximum Permitted Repair Time)
MRT:平均维修时间(Mean Repair Time)
MT:任务时间(Mission Time)
MTTR:平均恢复时间(Mean Time To Restoration)
PFD_{avg}:要求时危险失效平均概率(average Probability of dangerous Failure on Demand)
PFH:每小时危险失效平均频率(average Frequency of a dangerous Failure per Hour)
PHA:过程危险分析(Process Hazard Analysis)
PST:部分行程测试(Partial Stroke Testing)
PTC:检验测试覆盖率(Proof Test Coverage)
P&ID:工艺管道及仪表流程图(Piping & Instrument Diagram)
RRF:风险降低因子(Risk Reduction Factor)
SC:系统性能力(Systematic Capability)
SFF:安全失效分数(Safe Failure Fraction)
SIF:安全仪表功能(Safety Instrumented Function)
SIL:安全完整性等级(Safety Integrity Level)
SIS:安全仪表系统(Safety Instrumented System)
SRS:安全要求规格书(Safety Requirements Specification)
STR:误停车率(Spurious Trip Rate)
TI:检验测试间隔(Proof Test Interval)
UID:公用系统管道及仪表流程图(Utility Piping & Instrument Diagram)

5 总体要求

5.1 编写 SRS 的目的是为了通过规定 SIS 的要求,以保证 SIF 实现所需的功能安全。

5.2 SRS 应包含 SIS 的总体和通用要求、所有 SIF 的安全功能要求和与之相关 SIL 的安全完整性要求,包括 SIS 架构和应用程序。SRS 是 SIS 设计和工程实施的输入条件。

5.3 SRS 应根据 SIL 定级得出的风险降低要求和风险评估中确定的相关要求进行编写。SIL 定级和风险评估应根据企业风险可接受标准确定。企业风险可接受标准不应低于适用的国家标准强制性条款和监管部门的相关要求,不宜低于国家标准推荐性条款的要求。

5.4 SRS 和 SIS 应符合 GB/T 20438(所有部分)、GB/T 21109(所有部分)、GB/T 50770 的相关规定。

5.5 SRS 应是 SIS 的设计依据,是 SIS 的设计应遵循的指导文件,并且应包括目的和应用方法的描述。

5.6 SRS 应清晰、准确、明确、可验证、可测试、可维护、可操作,可用于指导使用者在 SIS 全生命周期遵照执行。

5.7 SRS、设计文件、验证文件、现场工况,SIF 测量仪表、逻辑控制器和最终执行机构的安全手册,相互之间应是协调的。

6 SRS 编写节点和流程

6.1 SRS 编写和更新节点

6.1.1 SRS 编写、更新(完善和维护)包括以下节点:

a) 在“SIS 的 SRS”节点,应编写 SRS 的初版;

b) “SIS 设计和工程(包括 SIL 验证)”节点后,应更新 SRS;

c) “SIS 安装、调试和确认”节点后,SIS 安装、调试、确认和开车过程中如果有涉及 SRS 的修改,应更新 SRS;

d) 工程投运后发生对 SRS 有影响的变更时,应更新 SRS。

6.1.2 各版本可采用版次设计的方式编写。

6.1.3 对 SRS 有影响的变更包括:联锁逻辑、SIL 定级、运行模式、联锁设定值、仪表选型、表决结构、失效数据、SIL 验证等方面的变化。

6.1.4 SIS 安全生命周期、SRS 编写和更新节点示意见图 1。

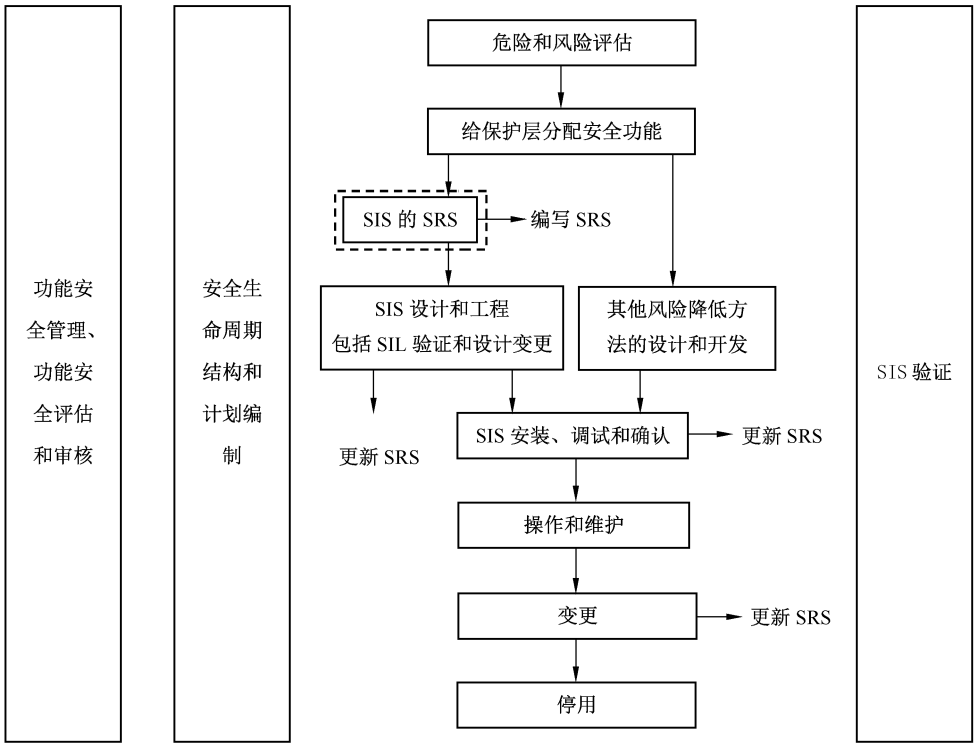

图 1 SIS 安全生命周期、SRS 编写和更新节点示意

6.2 编写流程

SRS 编写流程示意见图 2。SIS 设计有变更时,应更新 SRS。

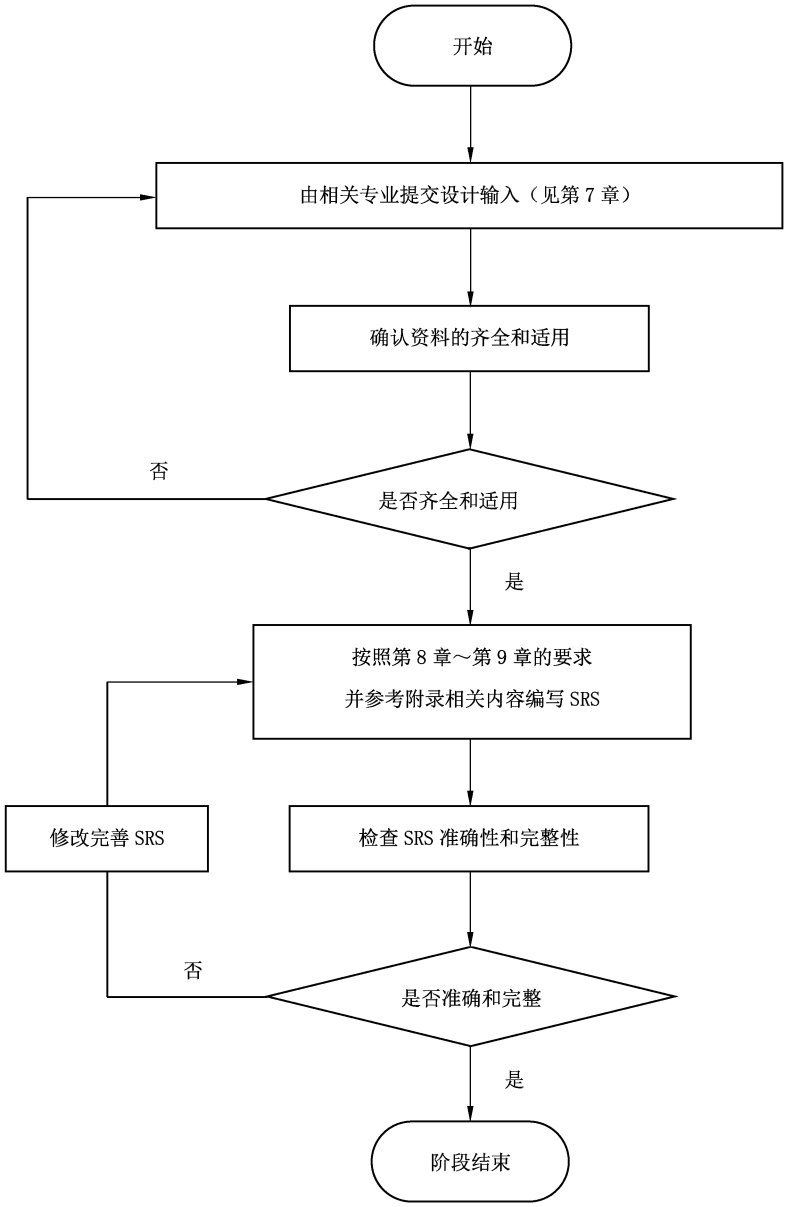

图 2　SRS 编写流程示意

7　SRS 编写输入资料

SRS 编写输入资料宜包括但不限于以下资料：

a）　P&ID、UID；

b）　装置说明与操作模式；

c）　联锁逻辑要求，以逻辑说明、逻辑图、因果表等形式表达；

d）　复位要求；

e）　过程安全时间；

f）　工程设计仪表规格书（包括最终执行机构安全状态要求）；

g）　操作范围及联锁设定值；

h) 逻辑控制器规格书；
i) HAZOP 报告；
j) SIL 定级报告(明确 SIF 和非 SIF),包括 SIF 回路组成一览表及 SIL 等级；
k) 操作和维修要求；
l) 装置运行检维修周期,设计寿命,可用性的要求。

8 SRS 内容

8.1 通则

8.1.1 SRS 应明确 SIS、SIF 和 SIL 的通用要求与具体要求,应包括实现功能安全的硬件、软件、工程、管理、运维等方面的要求。通用要求是对 SIS、SIF 和 SIL 的目的、原则、总框架、准则、共性的要求,具体要求是对于 SIF 的具体要求。SIF 清单和 SRS 数据表属于具体要求。

8.1.2 SRS 宜通过文字说明、表格、逻辑图、因果表等形式相结合的方式进行表述。表格包括:SIF 清单、SRS 数据表等。每个 SIF 应单独在 SIF 清单中列出并单独定义 SRS 数据表。

8.2 主要内容

8.2.1 SRS 应包括 SIF 要求和 SIL 要求。

8.2.2 SRS 宜包括应用程序安全要求。应用程序安全要求见 8.3。

8.2.3 SRS 宜包括下列内容。

a) 列出所有 SIF 的功能说明和联锁逻辑要求,联锁逻辑要求可采用逻辑说明、逻辑图、因果表等形式表达。
b) 列出每个 SIF 的测量仪表和最终执行机构的位号。
c) 识别和考虑共因失效,需要时,给出消除或减缓措施。
d) 定义每个 SIF 的过程安全状态,例如,防止储罐溢罐的 SIF,过程安全状态为关闭储罐入口切断阀,此状态可避免或充分减轻特定的危险事件(此处指的是储罐溢罐)。
e) 当多个 SIF 同时动作可能导致额外风险情况时,应进行风险分析并确定安全保护措施和方案。
f) 列出每个 SIF 的假定要求来源和要求发生的频率。
g) 确定每个 SIF 的测量仪表、逻辑控制器和最终执行机构的 TI。
h) 确定每个 SIF 对测量仪表、逻辑控制器和最终执行机构实施检验测试的要求;设置阀门 PST 时,应确定相关要求。
i) 确定每个 SIF 的响应时间的要求,SIF 的响应时间＝测量仪表响应时间＋逻辑控制器响应时间(包括输入、逻辑运算和输出等环节)＋最终执行机构响应时间＋各个环节的滞后时间。
j) 列出每个 SIF 的 SIL 等级和运行模式(低要求模式、高要求模式、连续模式)。
k) 列出每个 SIF 的测量仪表的过程测量变量、测量范围、精确度等级和联锁设定值等。
l) 列出每个 SIF 的最终执行机构的动作和相关要求,例如要求关闭控制阀、动作时间要求小于 10 s。
m) 说明每个 SIF 的输入和输出之间的功能关系,包括逻辑关系、数学函数关系及允许触发条件等,例如防止储罐溢罐 SIF,输入为高高液位联锁,逻辑表决关系为三取二,输出为关闭储罐进口切断阀,逻辑表决关系为一取一。
n) 说明每个 SIF 的手动停车要求,例如可在控制室辅助操作台和现场具备手动关闭切断阀的

功能。

o) 说明每个 SIF 的联锁方式，得电联锁或者失电联锁的要求，例如 SIF-101 中的 XV-101 电磁阀为失电（非励磁）联锁。

p) 说明每个 SIF 在联锁动作后的复位要求，例如防止储罐溢罐 SIF，高高液位联锁关闭储罐入口切断阀后，切断阀应保持关闭状态，直到储罐液位恢复正常并且启动复位为止。

q) 有可用性要求的 SIF，说明其最高允许的 STR。

r) 说明每个 SIF 的失效模式和要求的 SIS 响应（例如报警、自动停车）。

s) 说明开停工过程启动和重新启动 SIS 的具体要求。

t) 说明 SIS 和其他系统（包括 BPCS 和操作员）之间的所有接口要求，包括过程接口、通信接口、人机接口等。

u) 说明装置各种操作模式及每种模式下 SIF 的相关要求。

v) 说明 8.3 中列出的应用程序安全要求。

w) 说明每个 SIF 的旁路要求和旁路期间的管理要求，旁路包括维护旁路和操作旁路。

x) 说明每个 SIF 在检测到故障事件时，为达到和保持某个安全状态应采取的必要措施，宜考虑所有相关人员因素。例如检测到 SIF 测量仪表故障时执行联锁，或者一定期限内暂时不执行联锁而是采取必要的安全补偿措施，到期无法解除故障时执行联锁。

y) 确定每个 SIF 合理的 MTTR，综合考虑备品备件数量、存储、地理位置、路程时间、备件安装、服务合同、环境限制等。

z) 识别需要避免的 SIS 输出状态的关联危险。

aa) 识别在运输、存储、安装及运行中可能遇到的极端环境条件。

bb) 识别正常和异常过程操作模式，说明是否需要额外增加 SIF。

cc) 需要时，确定 SIF 应满足的特殊要求。例如，如果 SIF 控制阀需要在火灾场景下的一定时间内有效动作，应确定此 SIF 控制阀的防火要求，包括控制阀内件、控制阀执行机构、电缆等的防火要求。

dd) SIS 的总体和通用要求。

8.3 应用程序安全要求

8.3.1 通则

8.3.1.1 应用程序安全要求可作为 SRS 中的一部分，也作为一个独立文档，例如应用程序要求规格书。

8.3.1.2 应用程序安全要求应从 SRS 和 SIS 的架构（布局和内部结构）中推导。每个 SIS 子系统的应用程序安全要求输入信息应包括：

a) 每个 SIF 的安全要求，包括测量仪表表决等；

b) SIS 架构和安全手册提出的要求，例如硬件和嵌入式软件的限制和约束；

c) 来自 GB/T 21109.1 相关的安全计划的要求。

8.3.1.3 应为每个可编程控制器规定应用程序安全要求。

8.3.1.4 应用程序的设计、编程、组态、测试、集成、确认、运行维护及变更等应符合 SRS 和工程设计文件的要求。

8.3.1.5 应规定应用程序进行离线和在线测试的方式。应用程序应在确认其功能满足特定的目标和要求后，再投入运行。

8.3.1.6 应用程序应同时进行本地备份和异地备份。数据应采用专用光盘或磁介质进行复制和备

份，专用光盘或磁介质不应在安全仪表系统以外的电脑和电子产品上使用，电子版文件的复制应防止病毒。

8.3.1.7 逻辑设计应具有可读性，复杂功能逻辑图应有相应的逻辑功能说明。

8.3.1.8 应用程序组态编程应与 SRS、逻辑说明、逻辑图、因果表一致。程序执行顺序及时间应符合过程安全的要求。

8.3.1.9 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。

8.3.2 主要内容

应用程序安全要求应符合相关的功能安全（包括 SIF 和 SIL）的要求。应用程序安全要求应足够详细，以使设计和实施达到要求的功能安全，并应能开展功能安全评估。宜确定以下方面对应的功能安全相关的应用程序安全要求：

a） 需要实现的 SIF 及其 SIL；
b） 实时性能参数，例如 CPU 负荷、通信负荷、有故障时可接受的实时性能以及特定时间内接收到的所有联锁信号；
c） 程序次序和延时；
d） 设备和操作员接口及其可操作性；
e） SRS 中规定的所有相关的过程操作模式；
f） 针对异常测量结果，例如测量仪表值超量程、欠量程、变化幅度过大、测量值冻结、检测线路开路/短路，采取的措施；
g） 由应用程序执行的对测量仪表和最终执行机构进行检验测试和自动诊断测试的功能；
h） 应用程序的自监测，例如应用程序驱动的程序监视器和数据有效性确认；
i） 对测量仪表和最终执行机构的监测；
j） 过程运行时，SIF 的定期测试；
k） 相关资料，例如 SIF 清单、SIF 数据表、SIS 配置和架构、SIS 硬件安全完整性要求；
l） 通信接口，包括限制其使用的措施，以及接收和发送的数据或指令的有效性检查；
m） 识别和避免由应用程序产生的过程危险状态，例如同时关闭两个气体隔离阀可能导致压力波动，从而导致危险状态；
n） 每个 SIF 的过程变量验证标准的定义；
o） 网络安全、防火墙等；
p） 其他方面，例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。

8.3.3 编写要求

应用程序安全要求的编写应符合以下要求：

a） 应包括描述支持应用程序安全要求的意图和方法；
b） 在 SIS 全生命周期内，对使用该文档的人员来说应是清晰的、不会有歧义的并且易于理解的，人员包括设计人员、验证人员、工厂操作人员、维护人员和应用编程人员等；
c） 应可验证、可测试和可修改；
d） 通过相关文件应可追溯，包括详细设计文档、SRS 以及识别所需的 SIF 和 SIL 的 PHA。

9 SRS 文件结构

9.1 SRS 文件结构宜包括：总则、概述、工厂及项目装置概况、相关资料、总体要求、SRS 编写节点和 SRS 主要内容、应用程序安全要求、SIS 总体和通用要求、SIF 通用要求、SIF 清单、SRS 数据表、逻辑要求、具体要求、版次说明等部分。

9.2 SRS 文件宜为一个文件或几个文件的集合。

9.3 SIF 清单和 SRS 数据表示例见附录 A。

9.4 因果表示例见附录 B。

9.5 SRS 输入资料示例见附录 C。

9.6 SRS 编写示例见附录 D。

9.7 本文件附录中的示例是具体项目可能的选择，不属于本文件正文要求。在满足标准规范和监管文件要求的前提下，不同工程公司和企业可具有不同的选择。

附 录 A
（资料性）
SIF 清单和 SRS 数据表示例

A.1 概述

模板表格为示例，企业可根据具体情况确定适合的项目模板。确定项目模板后，具体填写可包含以下情况。

a） 不适合项目的，填写“不适合”。

b） 有些项可统一说明，填写“见统一说明”。例如仪表的使用期限、检测到故障时的响应。

c） 有些项内容可能较多，表格中可能填写不下，可另页填写或者采用其他方式表达，例如表 A.3 中的“与其他测量仪表组成群组”项，有时可能较为复杂，可通过专门文件说明、逻辑图、等方式进行表达。

d） 有些内容可分阶段逐步填写的。

e） 其他可能的情况。

A.2 SIF 清单示例

SIF 清单格式和填写示例见表 A.1。

表 A.1 SIF 清单格式和填写示例

序号	SIF 编号	SIF 功能说明	SIL 等级/ 验证达到的 SIL 等级	目标失效量/ 验证达到的目标失效量 （PFD_{avg}/RRF/PFH）	备注
1	SIF-101	液位（LT-10101、LT-10102 和 LT-10103，三取二）高高联锁关闭储罐（T-101）进口切断阀（XV-10101）	SIL2/SIL2	RRF＝200/RRF＝236 （低要求运行模式填写 PFD_{avg} 或 RRF，高要求或者连续运行模式填写 PFH）	略
略	略	略	略	略	略

A.3 SRS 数据表示例

A.3.1 概述

SRS 数据表包括 SIF 数据表、测量仪表数据表、逻辑控制器数据表和最终执行机构数据表。

A.3.2 SIF 数据表示例

SIF 数据表格式和填写示例见表 A.2。SIL 定级假设采用 LOPA 分析。

表 A.2　SIF 数据表格式和填写示例

<table>
<tr><td>SIF 编号</td><td colspan="3">SIF-101</td></tr>
<tr><td>SIF 描述</td><td colspan="3">储罐(T-101)液位高高联锁</td></tr>
<tr><td>HAZOP 报告</td><td colspan="3">略(填写 HAZOP 报告文件名、编号、日期、版次)</td></tr>
<tr><td>LOPA 报告</td><td colspan="3">略(填写 LOPA 报告文件名、编号、日期、版次)</td></tr>
<tr><td>危险事件说明</td><td colspan="3">溢罐,着火爆炸,造成人员伤亡、财产损失和环境影响</td></tr>
<tr><td>安全状态</td><td colspan="3">储罐(T-101)进口切断阀(XV-10101)关闭</td></tr>
<tr><td>SIF 功能说明</td><td colspan="3">液位(LT-10101、LT-10102 和 LT-10103,三取二)高高联锁关闭储罐(T-101)进口切断阀(XV-10101)</td></tr>
<tr><td>逻辑图号</td><td colspan="3">IS-10101</td></tr>
<tr><td>因果表号</td><td colspan="3">YGB-101</td></tr>
<tr><td>运行模式</td><td colspan="3">低要求运行模式</td></tr>
<tr><td>SIL 等级/验证达到的 SIL 等级</td><td colspan="3">SIL2/SIL2</td></tr>
<tr><td>目标失效量/验证达到的目标失效量
(PFD_{avg}/RRF/PFH)</td><td colspan="3">RRF=200/RRF=236
(低要求运行模式填写 PFD_{avg}或 RRF,高要求或者连续运行模式填写 PFH)</td></tr>
<tr><td>过程安全时间</td><td colspan="3">180 s</td></tr>
<tr><td>SIF 响应时间要求</td><td colspan="3">≤90 s(以要求“≤1/2 过程安全时间”举例)</td></tr>
<tr><td>最高允许的 STR/验证达到的 STR</td><td colspan="3">略(需要考虑可用性时,根据要求填写)</td></tr>
<tr><td rowspan="3">输入位号</td><td>LT-10101</td><td rowspan="3">输出位号</td><td>XV-10101</td></tr>
<tr><td>LT-10102</td><td></td></tr>
<tr><td>LT-10103</td><td></td></tr>
<tr><td>逻辑要求</td><td colspan="3">液位(LT-10101、LT-10102 和 LT-10103,三取二)高高联锁关闭储罐(T-101)进口切断阀(XV-10101)</td></tr>
<tr><td>手动停车</td><td colspan="3">设置手动停车,防火堤外现场按钮(HS-10101A)和辅操台按钮(HS-10101B),任一触发时停车</td></tr>
<tr><td>复位</td><td colspan="3">设置复位,RS-101</td></tr>
<tr><td>使用期限</td><td colspan="3">≥20 年</td></tr>
<tr><td>操作模式</td><td colspan="3">略
(说明装置各种操作模式及每种模式下 SIF 的相关要求。没有需要说明的,则不填写。
装置操作模式通常包括检修或紧急停车后的开车、正常操作、正常停车、临时操作、紧急操作、紧急停车、牌号切换等)</td></tr>
<tr><td>环境条件</td><td colspan="3">略</td></tr>
<tr><td>多 SIF 同时动作产生新风险(如果存在分析并说明)</td><td colspan="3">未发现(根据设计文件填写)</td></tr>
<tr><td>其他要求 1</td><td colspan="3">略(填写 SIS 输出状态危险组合、正常和异常操作模式、SIF 在意外事故中的要求等内容)</td></tr>
<tr><td>其他要求 2</td><td colspan="3">略</td></tr>
</table>

A.3.3 测量仪表数据表示例

测量仪表数据表格式和填写示例见表 A.3。

表 A.3 测量仪表数据表格式和填写示例

位号	LT-10101
P&ID 号	PID-101
安装位置和用途描述	储罐(T-101)液位测量
设备类型	雷达液位计
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-10101
因果表号	YGB-101
与其他测量仪表组成群组	与 LT-10102 和 LT-10103 组成三取二逻辑表决
信号类型	4 mA～20 mA
测量范围	0～100%
联锁设定值	80%
响应时间要求	≤2 s(根据过程安全时间、产品情况等,综合确定)
TI/a	2
MRT/h	24
MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	0FIT
未检测到的安全失效率(λ_{SU})	260FIT
检测到的危险失效率(λ_{DD})	736FIT
未检测到的危险失效率(λ_{DU})	79FIT
SFF	92.7%
具备的 SC 等级	SC3
检测到故障时的响应	故障导向联锁状态
维护旁路	设置

表 A.3　测量仪表数据表格式和填写示例（续）

操作旁路	不设置
安全手册	填写安全手册文件名和编号，或者填写随仪表设备提供
共因失效因子(β)	5%
与 BPCS 的独立性	与 BPCS 独立
其他要求 1	例如冗余配置仪表有多样性要求时，填写相关要求（还可填写 SIS 输出状态危险组合、正常和异常操作模式、SIF 在意外事故中的要求等内容）
其他要求 2	例如冗余配置有进不同 I/O 的要求时，填写相关要求

A.3.4　逻辑控制器数据表示例

逻辑控制器数据表格式和填写示例见表 A.4。

表 A.4　逻辑控制器数据表格式和填写示例

位号	SIS-10101
设备类型	逻辑控制器
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-10101
因果表号	YGB-101
响应时间要求	≤500 ms（根据过程安全时间、产品情况等，综合确定）
TI/a	2
MRT/h	24
MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	略
未检测到的安全失效率(λ_{SU})	略
检测到的危险失效率(λ_{DD})	略
未检测到的危险失效率(λ_{DU})	略
SFF	略
具备的 SC 等级	SC3

表 A.4　逻辑控制器数据表格式和填写示例（续）

检测到故障时的响应	故障导向联锁状态
接口要求	和 BPCS 间设置通信接口
安全手册	填写安全手册文件名和编号，或者填写随仪表设备提供
其他要求 1	略
其他要求 2	略

A.3.5　最终执行机构数据表示例

最终执行机构数据表格式和填写示例见表 A.5。

表 A.5　最终执行机构数据表格式和填写示例

位号	XV-10101
P&ID 号	PID-101
安装位置和用途描述	储罐(T-101)进口切断阀
设备类型	气动切断阀
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-10101
因果表号	YGB-101
与其他最终执行机构组成群组	无
响应时间要求	≤60 s(根据过程安全时间、产品情况等，综合确定)
TI/a	2
MRT/h	24
MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	略(注)
未检测到的安全失效率(λ_{SU})	略(注)
检测到的危险失效率(λ_{DD})	略(注)
未检测到的危险失效率(λ_{DU})	略(注)
SFF	略
具备的 SC 等级	SC3
得电/失电联锁	电磁阀失电(非励磁)联锁

表 A.5　最终执行机构数据表格式和填写示例（续）

联锁安全状态	失电联锁关闭 XV-10101
信号/动力中断时的动作	失电联锁关闭 XV-10101、气源故障关闭 XV-10101(FC)
现场手动复位	无现场手动复位
手动要求	设置手动关闭 XV-10101 的现场手动操作柱
阀门 PST	带
安全手册	填写安全手册文件名和编号，或者填写随仪表设备提供
共因失效因子(β)	3%
与 BPCS 的独立性	与 BPCS 独立
其他要求 1	根据需要填写，例如阀门泄漏等级等(还可填写 SIS 输出状态危险组合、正常和异常操作模式、SIF 在意外事故中的要求等内容)
其他要求 2	根据需要填写，例如气动执行机构供风独立性要求等
注：最终执行机构由若干部分组成时，例如控制阀主要由电磁阀、执行机构和阀体组成，可给出整体的失效率数据，或者分别给出各个组成部分的失效率数据。	

附 录 B
（资料性）
因果表示例

因果表格式和填写示例见表 B.1。

表 B.1 因果表格式和填写示例

<table>
<tr><td colspan="5" rowspan="4">逻辑联锁号：IS-10101
所属 SIF 的 SIF 编号：SIF-101

功能说明：
液位（LT-10101、LT-10102 和 LT-10103，三取二）≥80％联锁关闭储罐（T-101）进口切断阀（XV-10101）

注：本因果表中的测量仪表测量的均为安全关键变量，最终执行机构执行的均为安全关键动作。</td><td>序号</td><td>1</td><td>2</td><td rowspan="5">备注</td></tr>
<tr><td>位号</td><td>XV-10101</td><td>略</td></tr>
<tr><td>描述</td><td>储罐进口阀</td><td>略</td></tr>
<tr><td>P&ID 号</td><td>101</td><td>略</td></tr>
<tr><td>动作</td><td>关闭</td><td>略</td></tr>
<tr><td rowspan="2">序号</td><td rowspan="2">位号</td><td rowspan="2">描述</td><td rowspan="2">P&ID 号</td><td rowspan="2">修改</td><td></td><td></td><td></td><td rowspan="6"></td></tr>
<tr><td>备注</td><td></td><td></td></tr>
<tr><td>1</td><td>LT-10101</td><td>液位高高</td><td>101</td><td></td><td>1</td><td>×</td><td></td></tr>
<tr><td>2</td><td>LT-10102</td><td>液位高高</td><td>101</td><td></td><td>1</td><td>×</td><td></td></tr>
<tr><td>3</td><td>LT-10103</td><td>液位高高</td><td>101</td><td></td><td>1</td><td>×</td><td></td></tr>
<tr><td>4</td><td>略</td><td>略</td><td>略</td><td></td><td>略</td><td>略</td><td></td></tr>
</table>

附 录 C
（资料性）
SRS 编写输入资料示例

C.1 概述

SRS 编写输入资料要求见第 7 章。

为了使得附录 D 中的 SRS 编写示例更具有针对性，本附录给出了 LOPA 分析表示例，内容来源于 AQ/T 3054—2015 中 G.1 给出的案例。

C.2 LOPA 分析表示例

LOPA 分析表示例见表 C.1，内容同 AQ/T 3054—2015 中的表 G.2，格式有修改。示例中数据的是否合理不在本文件范围。

表 C.1 LOPA 记录表

主题	描述	概率	频率/(次/a)
分析节点	正己烷缓冲罐		
场景	正己烷缓冲罐溢流，溢流物未被防火堤包容		
后果描述/等级	由于储罐溢流和防火堤失效，导致释放的正己烷流出防火堤，发生火灾和人员伤亡 后果等级 5		
初始事件	BPCS LIC-90 控制回路失效		1×10^{-1}
使能必要事件/条件	无		
条件修正	点火概率	1	
	人员暴露概率	0.5	
	致死概率	0.5	
IPL	防火堤(释放后保护设施)	1×10^{-2}	
其他保护措施	人员响应行动	1	
后果发生频率			2.5×10^{-4}
现有风险等级	高风险		
需求的 SIL 等级或建议的 IPL	增加一个独立的 SIF，用于检测和阻止溢流	1×10^{-2} (SIL1)注 3	

表 C.1　LOPA 记录表（续）

主题	描述	概率	频率/(次/a)
减缓后的后果发生频率			2.5×10^{-6}
减缓后的风险等级	中风险		
备注	1. 人员行动不作为 IPL，原因如下： ——操作人员不总是在现场； ——BPCS 液位控制回路失效(IE)导致系统不能产生报警，从而不能提醒操作人员采取行动以阻止缓冲罐进料。 2. 企业可采用成本效益分析，决定是否需采用额外的措施进一步降低风险。 3. 此数据来源于 AQ/T 3054—2015 中的表 G.2，实际工程中有多种方式获得，例如可根据 GB/T 21109.3—2007 中的 F.11 获得，即如果需要一个新的 SIF，则可由该事件的严重性等级的公司准则除以中间事件可能性来计算所需的完整性等级。低于此数的 SIF 的一个 PFD_{avg} 被选作 SIS 的最大值。举例，以表 C.1 中的数据为例，假设所示例场景的风险可接受标准为后果发生频率 $F\leqslant1\times10^{-5}$，而示例的中不考虑 SIF 的后果发生频率为 2.5×10^{-4}，前者除以后者可得到存在的风险缺口为 $PFD_{avg}=0.04$，相当于 RRF=25，也就是宜设置 $PFD_{avg}=0.04$(RRF=25)的 SIF		

C.3　SRS 编写输入资料的准备

C.3.1　SIF 相关信息的梳理

为编写 SRS，需要对 LOPA 报告进行梳理，包括对 LOPA 分析表的梳理。梳理示意见表 C.2 和表 C.3。

表 C.2　SIF 清单梳理示例

序号	SIF 编号	SIF 功能说明	SIL 等级/验证达到的 SIL 等级	目标失效量/验证达到的目标失效量(PFD_{avg}/RRF/PFH)	备注
1	SIF-101 (假设的编号)	检测和阻止正己烷缓冲罐溢流	SIL1/	$PFD_{avg}=1\times10^{-2}$/ RRF=100	略

表 C.3　SIF 数据表梳理示例

SIF 编号	SIF-101(假设的编号)
SIF 描述	检测和阻止正己烷缓冲罐溢流(依据表 C.1)
HAZOP 报告	略(根据项目文件填写)
LOPA 报告	略(根据项目文件填写)
危险事件说明	由于储罐溢流和防火堤失效，导致释放的正己烷流出防火堤，发生火灾和人员伤亡。后果等级 5(依据表 C.1)

表 C.3　SIF 数据表梳理示例（续）

安全状态	远程控制阀 RBV 关闭（依据 AQ/T 3054—2015 中的 G.1.6）		
SIF 功能说明	LT-95 高液位联锁关闭远程控制阀 RBV （依据 AQ/T 3054—2015 中的 G.1.6）		
逻辑图号	IS-101（假设的编号，根据设计文件填写）		
因果表号	YGB-101（假设的编号，根据设计文件填写）		
运行模式	低要求运行模式（依据初始事件发生频率为 1×10^{-1}/a）		
SIL 等级/验证达到的 SIL 等级	SIL1（依据表 C.1）		
目标失效量/验证达到的目标失效量（PFD_{avg}/RRF/PFH）	$PFD_{avg}=1\times10^{-2}$（依据表 C.1）		
过程安全时间	略（根据设计文件填写）		
SIF 响应时间要求	略（根据设计文件填写）		
最高允许的 STR/验证达到的 STR	略（通常由设计和企业协商确定）		
输入位号	LT-95	输出位号	RBV
逻辑要求	LT95 高液位联锁关闭远程控制阀 RBV		
手动停车	略（根据设计文件填写）		
复位	设置复位，RS-101（假设的编号，根据设计文件填写）		
使用期限	略（根据设计文件填写）		
操作模式	略（根据设计文件填写）		
环境条件	略（根据设计文件填写）		
多 SIF 同时动作产生新风险（如果存在分析并说明）	未发现（根据设计文件填写）		
注：根据 AQ/T 3054—2015 中的 G.1.6，新增的独立的 SIF（即表 C.3 中的 SIF-101），用于检测和阻止溢流，采用独立的液位传感器、逻辑控制器和独立的截断阀。当检测到高液位时，该 SIF 联锁关流量控制阀 LV-90 和远程截断阀 RBV。假设工程设计按照高液位联锁关闭 LV-90 为非安全关键动作考虑，LV-90 不属于 SIF-101，LT-95 高液位关闭 LV-90 是为了之后的重新开车前 LV-90 处于关闭状态；RBV 为安全关键。			

C.3.2　可靠性数据和基本信息的收集

C.3.2.1　概述

C.3.2 给出了 SIF-101 的测量仪表、逻辑控制器、最终执行机构的可靠性数据、基本信息与要求，数据和要求均为假设。SIF 的 SIL 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、SIL 认证

报告、公开发行的工业数据库或手册等。基本信息和要求可来自 HAZOP 报告、LOPA 报告、设计文件、企业管理要求、项目统一规定等。

SRS 需要建立全生命周期的管理，根据不同阶段和版次的 SRS，选择适用的仪表设备可靠性数据来源，例如初版的 SRS 在 SIS 设计之前，此时的数据可以来源于公开发行的工业数据库或手册。

C.3.2.2 测量仪表

测量仪表可靠性数据、基本信息与要求收集示例见表 C.4。

表 C.4 测量仪表可靠性数据、基本信息与要求收集示例

位号	LT-95
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	正己烷缓冲罐液位测量
设备类型	雷达液位计(根据设计文件填写)
制造商和型号	略(根据设计文件填写)
所属 SIF 的 SIF 编号	SIF-101(根据设计文件填写)
逻辑图号	IS-101(根据设计文件填写)
因果表号	YGB-101(根据设计文件填写)
与其他测量仪表组成群组	无(根据设计文件填写)
信号类型	4 mA～20 mA(根据设计文件填写)
测量范围	0～100%(根据设计文件填写)
联锁设定值	80%(根据设计文件填写)
响应时间要求	≤2 s(根据设计文件填写)
TI/a	2(由设计单位和企业协商确定)
MRT/h	24(根据企业管理要求填写)
MTTR/h	24(根据企业管理要求填写)
MPRT/h	24(根据企业管理要求填写)
PTC	95%(根据安全手册或其他文件填写)
MT/a	10(根据安全手册或其他文件填写)
失效率数据来源	SIL 证书(假设)
检测到的安全失效率(λ_{SD})	0FIT(根据失效率数据来源填写)
未检测到的安全失效率(λ_{SU})	260FIT(根据失效率数据来源填写)
检测到的危险失效率(λ_{DD})	736FIT(根据失效率数据来源填写)
未检测到的危险失效率(λ_{DU})	79FIT(根据失效率数据来源填写)
SFF	92.7%
具备的 SC 等级	SC3(根据失效率数据来源填写)
检测到故障时的响应	故障导向联锁状态(根据设计文件填写)
维护旁路	设置(根据设计文件填写)

表 C.4　测量仪表可靠性数据、基本信息与要求收集示例（续）

操作旁路	不设置(根据设计文件填写)
安全手册	略(通常由 SIL 认证机构提供或者制造商提供)
共因失效因子(β)	5%(假设)
与 BPCS 的独立性	与 BPCS 独立(依据 AQ/T 3054—2015 中图 G.2)
其他要求 1	略(根据设计文件填写)
其他要求 2	略(根据设计文件填写)

C.3.2.3　逻辑控制器

逻辑控制器可靠性数据、基本信息与要求收集示例见表 C.5。

表 C.5　逻辑控制器可靠性数据、基本信息与要求收集示例

位号	SIS-101(根据设计文件填写)
设备类型	逻辑控制器
制造商和型号	略(根据设计文件填写)
所属 SIF 的 SIF 编号	SIF-101(根据设计文件填写)
逻辑图号	IS-101(根据设计文件填写)
因果表号	YGB-101(根据设计文件填写)
响应时间要求	≤500 ms(根据设计文件填写)
TI/a	2(由设计单位和企业协商确定)
MRT/h	24(根据企业管理要求填写)
MTTR/h	24(根据企业管理要求填写)
MPRT/h	24(根据企业管理要求填写)
PTC	95%(根据安全手册或其他文件填写)
MT/a	10(根据安全手册或其他文件填写)
失效率数据来源	SIL 证书(假设)
检测到的安全失效率(λ_{SD})	略(根据失效率数据来源填写)
未检测到的安全失效率(λ_{SU})	略(根据失效率数据来源填写)
检测到的危险失效率(λ_{DD})	略(根据失效率数据来源填写)
未检测到的危险失效率(λ_{DU})	略(根据失效率数据来源填写)
SFF	略
具备的 SC 等级	SC3(根据失效率数据来源填写)

表 C.5　逻辑控制器可靠性数据、基本信息与要求收集示例（续）

检测到故障时的响应	故障导向联锁状态(根据设计文件填写)
接口要求	和 BPCS 间设置通信接口(根据设计文件填写)
安全手册	填写安全手册文件名和编号,或者填写随仪表设备提供。
其他要求 1	略(根据设计文件填写)
其他要求 2	略(根据设计文件填写)

C.3.2.4　最终执行机构

SIF-101 的最终执行机构 RBV 由电磁阀、气动执行机构、阀体三部分组成,可靠性数据、基本信息与要求收集示例分别见表 C.6、表 C.7、表 C.8。

如果可获取最终执行机构整体的可靠性数据,宜给出整体数据,如果无法获取整体可靠性数据,则需要分别给出各个组成部分的可靠性数据。

表 C.6　RBV 电磁阀可靠性数据、基本信息与要求收集示例

位号	RBV 电磁阀(根据设计文件填写)
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	D101 出口切断阀配套的电磁阀(根据设计文件填写)
设备类型	两位三通电磁阀(根据设计文件填写)
制造商和型号	略(根据设计文件填写)
所属 SIF 的 SIF 编号	SIF-101(根据设计文件填写)
逻辑图号	IS-101(根据设计文件填写)
因果表号	YGB-101(根据设计文件填写)
与其他最终执行机构组成群组	无(根据设计文件填写)
响应时间要求	略(填写 RBV 整体响应时间要求)
TI/a	2(由设计单位和企业协商确定)
MRT/h	24(根据企业管理要求填写)
MTTR/h	24(根据企业管理要求填写)
MPRT/h	24(根据企业管理要求填写)
PTC	95%(根据安全手册或其他文件填写)
MT/a	10(根据安全手册或其他文件填写)
失效率数据来源	SIL 证书(假设)
检测到的安全失效率(λ_{SD})	略(根据失效率数据来源填写)
未检测到的安全失效率(λ_{SU})	略(根据失效率数据来源填写)

表 C.6　RBV 电磁阀可靠性数据、基本信息与要求收集示例（续）

检测到的危险失效率(λ_{DD})	略(根据失效率数据来源填写)
未检测到的危险失效率(λ_{DU})	略(根据失效率数据来源填写)
SFF	略
具备的 SC 等级	SC3(根据失效率数据来源填写)
得电/失电联锁	失电联锁(根据设计文件填写)
联锁安全状态	失电联锁关闭 RBV(根据设计文件填写)
信号/动力中断时的动作	失电联锁关闭 RBV、气源故障关闭 RBV(FC)
现场手动复位	无现场手动复位(根据设计文件填写)
手动要求	无(根据设计文件填写)
阀门 PST	带(根据设计文件填写)
安全手册	填写安全手册文件名和编号,或者填写随仪表设备提供
共因失效因子(β)	略(根据实际情况填写)
与 BPCS 的独立性	与 BPCS 独立(依据 AQ/T 3054—2015 中图 G.2)
其他要求 1	略(根据设计文件填写)
其他要求 2	略(根据设计文件填写)

表 C.7　RBV 气动执行机构可靠性数据、基本信息与要求收集示例

位号	RBV 执行机构(根据设计文件填写)
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	D101 出口切断阀
设备类型	气动执行机构(根据设计文件填写)
制造商和型号	略(根据设计文件填写)
所属 SIF 的 SIF 编号	SIF-101(根据设计文件填写)
逻辑图号	IS-101(根据设计文件填写)
因果表号	YGB-101(根据设计文件填写)
与其他最终执行机构组成群组	无(根据设计文件填写)
响应时间要求	略(填写 RBV 整体响应时间要求)
TI/a	2(由设计单位和企业协商确定)
MRT/h	24(根据企业管理要求填写)
MTTR/h	24(根据企业管理要求填写)
MPRT/h	24(根据企业管理要求填写)

表 C.7　RBV 气动执行机构可靠性数据、基本信息与要求收集示例（续）

PTC	95%（根据安全手册或其他文件填写）
MT/a	10（根据安全手册或其他文件填写）
失效率数据来源	SIL 证书（假设）
检测到的安全失效率（λ_{SD}）	略（根据失效率数据来源填写）
未检测到的安全失效率（λ_{SU}）	略（根据失效率数据来源填写）
检测到的危险失效率（λ_{DD}）	略（根据失效率数据来源填写）
未检测到的危险失效率（λ_{DU}）	略（根据失效率数据来源填写）
SFF	略
具备的 SC 等级	SC3（根据失效率数据来源填写）
得电/失电联锁	失电联锁（根据设计文件填写）
联锁安全状态	失电联锁关闭 RBV（根据设计文件填写）
信号/动力中断时的动作	失电联锁关闭 RBV、气源故障关闭 RBV（FC）
现场手动复位	无现场手动复位（根据设计文件填写）
手动要求	无（根据设计文件填写）
阀门 PST	带（根据设计文件填写）
安全手册	填写安全手册文件名和编号，或者填写随仪表设备提供
共因失效因子（β）	略（根据实际情况填写）
与 BPCS 的独立性	与 BPCS 独立（依据 AQ/T 3054—2015 中图 G.2）
其他要求 1	气动执行机构要求供风独立（根据设计文件填写）
其他要求 2	略（根据设计文件填写）

表 C.8　RBV 阀体可靠性数据、基本信息与要求收集示例

位号	RBV 阀体（根据设计文件填写）
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	RBV 阀体（根据设计文件填写）
设备类型	切断阀（根据设计文件填写）
制造商和型号	略（根据设计文件填写）
所属 SIF 的 SIF 编号	SIF-101（根据设计文件填写）
逻辑图号	IS-101（根据设计文件填写）
因果表号	YGB-101（根据设计文件填写）
与其他最终执行机构组成群组	无（根据设计文件填写）

表 C.8　RBV 阀体可靠性数据、基本信息与要求收集示例（续）

响应时间要求	略(填写 RBV 整体响应时间要求)
TI/a	2(由设计单位和企业协商确定)
MRT/h	24(根据企业管理要求填写)
MTTR/h	24(根据企业管理要求填写)
MPRT/h	24(根据企业管理要求填写)
PTC	95%(根据安全手册或其他文件填写)
MT/a	10(根据安全手册或其他文件填写)
失效率数据来源	SIL 证书(假设)
检测到的安全失效率(λ_{SD})	略(根据失效率数据来源填写)
未检测到的安全失效率(λ_{SU})	略(根据失效率数据来源填写)
检测到的危险失效率(λ_{DD})	略(根据失效率数据来源填写)
未检测到的危险失效率(λ_{DU})	略(根据失效率数据来源填写)
SFF	略
具备的 SC 等级	SC3(根据失效率数据来源填写)
得电/失电联锁	失电联锁(根据设计文件填写)
联锁安全状态	失电联锁关闭 RBV(根据设计文件填写)
信号/动力中断时的动作	失电联锁关闭 RBV、气源故障关闭 RBV(FC)
现场手动复位	无现场手动复位(根据设计文件填写)
手动要求	无(根据设计文件填写)
阀门 PST	带(根据设计文件填写)
安全手册	填写安全手册文件名和编号,或者填写随仪表设备提供
共因失效因子(β)	略(根据实际情况填写)
与 BPCS 的独立性	与 BPCS 独立(依据 AQ/T 3054—2015 中图 G.2)
其他要求 1	泄漏等级符合 API 598 的规定(根据设计文件填写)
其他要求 2	气动执行机构要求供风独立(根据设计文件填写)

附 录 D
（资料性）
SRS 编写示例

SRS 编写示例如下，供参考。

注 1：《SRS 编写示例》不同于 T/CCSAS 054《安全仪表系统（SIS）安全要求规格书（SRS）编写指南》正文，SRS 编写示例具备项目属性，可包括 SRS 以外的一些要求，例如 SIL 定级要求和 SIL 验证要求等，而这些要求是必要的，是有利于项目执行的。《SRS 编写示例》对于 SRS 本身的内容也是在标准要求的基础上对于针对项目的具体体现。

注 2：《SRS 编写示例》的内容仅为示例，不作为标准要求。在满足标准规范和监管文件要求的前提下，不同工程公司和企业可能具有不同的选择。

××××××公司

××××××项目

××××××装置

安全仪表系统（SIS）安全要求规格书（SRS）

D.1 总则

D.1.1 适用范围

本安全要求规格书（以下简称“本 SRS”）是为××××××公司××××××项目××××××装置（以下简称“本项目装置”）编写的，本 SRS 从 SIS 总体和通用要求、SIF 通用要求、具体的 SIF 及其对应的 SIL 的要求等方面，规定了 SIS 的要求，包括工程设计、验证、选型、制造、安装、硬件系统集成、软件组态编程、系统测试验收、运行、维护、安全管理策略等方面的相关要求。

本 SRS 适用于本项目装置，包括建设、投运期间相关的变更。

本 SRS 应在 SIS 安全生命周期的各个阶段执行，安全仪表系统（SIS）和安全仪表功能（SIF）的设计、验证、安装、运维和管理应符合本 SRS 的规定。

D.1.2 缩略语

下列缩略语适用于本 SRS。

ALARP：最低合理可行原则（As Low As Reasonably Practicable）

BPCS：基本过程控制系统（Basic Process Control System）

DC：诊断覆盖率（Diagnostic Coverage）

FIT：菲特（Failure In Time）

注：本 SRS 中，1 FIT＝1 failure/10^9 hours。

HAZOP：危险与可操作性分析（Hazard and Operability Studies）

HFT：硬件故障裕度（Hardware Fault Tolerance）

注：也称硬件容错。

IE：初始事件（Initiating Event）

IPL：独立保护层（Independent Protection Layer）

LOPA：保护层分析（Layer Of Protection Analysis）

MPRT：最大允许维修时间（Maximum Permitted Repair Time）

MRT:平均维修时间(Mean Repair Time)

MT:任务时间(Mission Time)

MTTR:平均恢复时间(Mean Time To Restoration)

PFD_{avg}:要求时危险失效平均概率(average Probability of dangerous Failure on Demand)

PFH:每小时危险失效平均频率(average Frequency of a dangerous Failure per Hour)

PHA:过程危险分析(Process Hazard Analysis)

PST:部分行程测试(Partial Stroke Testing)

PTC:检验测试覆盖率(Proof Test Coverage)

P&ID:工艺管道及仪表流程图(Piping & Instrument Diagram)

RRF:风险降低因子(Risk Reduction Factor)

SC:系统性能力(Systematic Capability)

SFF:安全失效分数(Safe Failure Fraction)

SIF:安全仪表功能(Safety Instrumented Function)

SIL:安全完整性等级(Safety Integrity Level)

SIS:安全仪表系统(Safety Instrumented System)

SRS:安全要求规格书(Safety Requirements Specification)

STR:误停车率(Spurious Trip Rate)

TI:检验测试间隔(Proof Test Interval)

UID:公用系统管道及仪表流程图(Utility Piping & Instrument Diagram)

D.1.3 本 SRS 程度用词说明

D.1.3.1 为便于在执行本 SRS 条文时区别对待,对要求严格程度不同的用词说明如下:

a) 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”;

b) 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”;

c) 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”;

d) 表示有选择,在一定条件下可以这样做的,采用“可”。

D.1.3.2 本 SRS 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”。

D.2 概述

D.2.1 目的

本 SRS 的目的是为了保证实现所需的功能安全,规定 SIS、SIF 及其对应的 SIL 的要求。

D.2.2 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

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 32857　保护层分析(LOPA)应用指南
GB/T 50770　石油化工安全仪表系统设计规范
SH/T 3082　石油化工仪表供电设计规范
T/CCSAS 045—2023　安全仪表功能(SIF)安全完整性等级(SIL)验证导则
T/CCSAS 054—2024　安全仪表系统(SIS)安全要求规格书(SRS)编写指南
ISA TR 84.00.03 Automation Asset Integrity of Safety Instrumented Systems (SIS)
ISA TR 96.05.01 Partial Stroke Testing of Automated Valves

D.3　工厂及项目装置概况

本项目装置为××××××公司××××××项目××××××装置,建设单位为××××公司,建设地点位于××××。

本项目装置设置了一套 BPCS 和一套 SIS。BPCS 采用×××公司的×××系统,SIS ×××公司的×××系统。(如果 BPCS 和 SIS 尚未确定厂家,则不注明厂家。)

……

建设地点环境条件见表 D.1。

表 D.1　建设地点环境条件

大气压		
温度	平均	
	极限高温	
	极限低温	
雷暴日		
湿度		
降水		
沿海		

净化风质量和供气压力见表 D.2。

表 D.2　净化风质量和供气压力

最低供气压力	
最高供气压力	
露点	
含尘颗粒直径	
含尘量	
油分含量	

……

D.4 相关资料

本 SRS 编写输入资料包括以下资料：

a） P&ID、UID；
b） 装置说明与操作模式；
c） 逻辑要求，以逻辑说明、逻辑图、因果表等形式表达；
d） 复位要求；
e） 过程安全时间；
f） 工程设计仪表规格书（包括最终执行机构安全状态要求）；
g） 操作范围及联锁设定值；
h） 逻辑控制器规格书；
i） HAZOP 报告；
j） SIL 定级报告（明确 SIF 和非 SIF），包括 SIF 回路组成一览表及 SIL 等级；
k） 操作和维修要求；
l） 装置运行检维修周期，设计寿命，可用性的要求；
m） ××××××会议纪要；
n） 当前阶段已有的仪表设备可靠性数据。

D.5 总体原则和要求

D.5.1 本 SRS 应与本文件在 D.2.2 列出的规范性引用文件结合使用。

D.5.2 SRS 编写的总体要求、节点和流程、输入资料、内容、文件结构应符合 T/CCSAS 054—2024 的相关规定。

D.5.3 本 SRS 和 SIS 应符合 GB/T 20438（所有部分）、GB/T 21109（所有部分）、GB/T 50770 的相关规定。

D.5.4 SRS 应包含 SIS 的总体和通用要求、所有 SIF 的安全功能要求和与之相关 SIL 的安全完整性要求。SRS 是 SIS 设计和工程实施的输入条件。

D.5.5 本 SRS 是根据 HAZOP 分析和 SIL 定级得出的风险降低要求编写的。

注 1：HAZOP 分析和 SIL 定级应根据企业风险可接受标准确定。

注 2：企业风险可接受标准不应低于适用的国家标准强制性条款和监管部门的相关要求，不宜低于国家标准推荐性条款的要求。

注 3：SIL 定级宜采用 LOPA 分析。

D.5.6 SRS 应是 SIS 的设计依据，是 SIS 的设计应遵循的指导文件，并且应包括目的和应用方法的描述。

D.5.7 SRS 应清晰、准确、明确、可验证、可测试、可维护、可操作，能用于规范 SIS 安全生命周期各阶段使用者的遵照和执行。

D.5.8 SRS、设计文件、验证文件、现场工况，SIF 测量仪表、逻辑控制器和最终执行机构的安全手册，相互之间应是协调的。

D.5.9 SRS 应明确 SIS、SIF 和 SIL 的通用要求与具体要求，应包括实现功能安全的硬件、软件、工程、管理、运维等方面的要求。通用要求是对 SIS、SIF 和 SIL 的目的、原则、总框架、准则、共性的要求，具体要求是对于具体 SIF 的要求。SIF 清单和 SRS 数据表属于具体要求。

D.5.10 SRS 宜通过文字说明、表格、逻辑图、因果表等形式相结合的方式进行表述。表格包括：SIF 清单、SRS 数据表等。每个 SIF 应单独在 SIF 清单中列出并单独定义 SRS 数据表。

D.5.11 SIS 集成、调试、验收测试与确认，应符合 SRS 和 SIS 其他相关安全技术要求以及详细工程设

计文件的要求。SIS 投入使用前应开展确认工作。确认内容宜包括测量仪表、逻辑控制器、最终元件及关联设备的安装、测试与联合调试等。

D.6 SRS 编写节点和 SRS 主要内容

D.6.1 SRS 编写节点和更新过程

SRS 编写、更新(完善和维护)包括以下节点:

a) 在“SIS 的 SRS”节点,应编写 SRS 的初版;

b) “SIS 设计和工程(包括 SIL 验证)”节点后,应更新 SRS;

c) “SIS 安装、调试和确认”节点后,SIS 安装、调试、确认和开车过程中如果有涉及 SRS 的修改,应更新 SRS;

d) 工程投运后发生对 SRS 有影响的变更时,应更新 SRS。

各版本可采用版次设计的方式编写。

对 SRS 有影响的变更包括:联锁逻辑、SIL 定级、运行模式、联锁设定值、仪表选型、表决结构、失效数据、SIL 验证等方面的变化。

SIS 安全生命周期、SRS 编写和更新节点示意见 T/CCSAS 054—2024 中的图 1。

D.6.2 SRS 主要内容

SRS 的主要内容应符合 T/CCSAS 054—2024 的规定。

D.7 应用程序安全要求

D.7.1 应用程序安全要求可作为 SRS 中的一部分,也作为一个独立文档,例如应用程序要求规格书。

D.7.2 应用程序安全要求应从 SRS 和 SIS 的架构(布局和内部结构)中推导。每个 SIS 子系统的应用程序安全要求输入信息应包括:

a) 每个 SIF 的安全要求,包括测量仪表表决等;

b) SIS 架构和安全手册提出的要求,例如硬件和嵌入式软件的限制和约束;

c) 来自 GB/T 21109.1 相关的安全计划的要求。

D.7.3 应为每个可编程控制器规定应用程序安全要求。

D.7.4 应用程序的设计、编程、组态、测试、集成、确认、运行维护及变更等应符合 SRS 和工程设计文件的要求。

D.7.5 应规定应用程序进行离线和在线测试的方式。应用程序应在确认其功能满足特定的目标和要求后,再投入运行。

D.7.6 应用程序应同时进行本地备份和异地备份。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。

D.7.7 逻辑设计应具有可读性,复杂功能逻辑图应有相应的逻辑功能说明。

D.7.8 应用程序组态编程应与 SRS、逻辑说明、逻辑图、因果表一致。程序执行顺序及时间应符合过程安全的要求。

D.7.9 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。

D.7.10 应用程序安全要求的内容应符合 T/CCSAS 054—2024 中 8.3.2 的规定。

D.7.11 应用程序安全要求的编写应符合以下要求:

a) 应包括描述支持应用程序安全要求的意图和方法;

b) 对 SIS 安全生命周期任何阶段将使用该文档的人员来说应是清晰的、不会有歧义并且易于理解的,人员包括设计人员、验证人员、工厂操作人员、维护人员和应用编程人员等;

c) 应可验证、可测试和可修改；

d) 通过相关文件应可追溯，包括详细设计文档、SRS 以及识别所需的 SIF 和 SIL 的 PHA。

D.8 SIS 总体和通用要求

D.8.1 通则

SIS 的工程设计、验证、选型、制造、安装、硬件系统集成、软件组态编程、系统测试验收、运行、维护、安全管理策略等应符合本 SRS、设计文件、安全手册等的要求。

D.8.2 接口

D.8.2.1 SIS 逻辑控制器的接口

D.8.2.1.1 输入、输出卡件信号通道应带光电或电磁隔离。

D.8.2.1.2 检测同一过程变量的冗余测量仪表信号宜接到不同输入卡件。

D.8.2.1.3 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。

D.8.2.1.4 输入、输出卡件不应采用现场总线数字信号。

D.8.2.1.5 本安回路应采用隔离型安全栅。

D.8.2.1.6 输入、输出回路宜具有线路断路和短路检测功能，并在安全仪表系统中报警和记录。

D.8.2.1.7 SIS 逻辑控制器与 SIS 辅助操作台之间的信号往来采用硬接线，包括以下信号：

a) SIS 辅助操作台上的紧急停车按钮至 SIS 逻辑控制器的紧急停车信号；

b) SIS 逻辑控制器的输出至 SIS 辅助操作台上的报警灯屏的信号；

c) SIS 辅助操作台上的允许旁路开关至 SIS 逻辑控制器的允许旁路信号；

d) 其他信号(根据设计文件设置)。

D.8.2.2 SIS 逻辑控制器的网络和通信接口

D.8.2.2.1 SIS 逻辑控制器的输入、输出信号，均应通信至 BPCS。

D.8.2.2.2 SIS 与 BPCS 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，应采取工业防火墙等网络安全措施。

D.8.2.2.3 SIS 与 BPCS 通信接口应冗余配置。通信接口应有诊断功能。

D.8.2.2.4 SIS 与 BPCS 通信不应通过工厂管理网络传输。

D.8.2.2.5 除旁路信号和复位信号外，BPCS 不应采用通信方式向 SIS 发送指令。

D.8.2.2.6 除 BPCS 外，SIS 与其他系统之间不应设置通信接口。SIS 与其他系统之间的连接应采用硬接线方式。

D.8.2.2.7 通信接口的故障不应影响 SIS 的安全功能。通信接口故障应在操作员站或工程师站显示、报警。

D.8.2.2.8 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%。

D.8.2.2.9 SIS 应通过冗余配置的工业交换机组网。SIS 的交换机不宜采用级联或堆叠方式扩展交换机端口数量。

D.8.2.3 SIS 的人机接口

D.8.2.3.1 SIS 宜设置操作员站，操作员站可采用 SIS 的操作员站，也可采用 BPCS 的操作员站。在操作员站失效时，SIS 的逻辑处理功能不应受影响。本项目装置 SIS 设置操作员站，并采用 SIS 的操作员站。

D.8.2.3.2 本项目装置 SIF 测量仪表的输入信号均应设置联锁值越限报警，旁路开关不应屏蔽报警

功能。

D.8.2.3.3 本项目装置 SIF 联锁的输入和输出信号均应做报警画面。

D.8.2.3.4 SIS 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。

D.8.2.3.5 SIS 操作员站不应具有修改安全仪表系统应用程序的功能或权限。

D.8.2.3.6 SIS 操作员站设置的软件旁路开关应加键锁或口令保护，并应设置旁路状态报警和记录。

D.8.2.3.7 SIS 操作员站应提供程序运行状态、联锁动作、输入/输出状态、诊断结果等显示、报警及记录等功能。

D.8.2.3.8 基本过程控制系统的操作员站可设置安全仪表系统安全联锁动作前的预报警。

D.8.3 SIS 事件顺序记录站

D.8.3.1 采用可编程电子系统的 SIS 应设事件顺序记录站。事件顺序记录站可单独设置，也可与 SIS 的工程师站共用。工程师站和事件顺序记录站应采用专用计算机。

D.8.3.2 本项目装置单独设置 SIS 事件顺序记录站。SIS 事件顺序记录站记录的历史数据保存时间不小于 180 d，应能通过其他存储介质备份更长时间。

D.8.3.3 SIS 事件顺序记录站应记录每个事件的时间、日期、标识、状态等。SIS 事件顺序记录站应设密码保护。

D.8.4 SIS 时钟同步

D.8.4.1 SIS 应采用同一时钟源。SIS 的逻辑控制器、工程师站、操作员站等设备，可采用逻辑控制器的时钟作为时钟源，使 SIS 内设备的时钟一致。

D.8.4.2 SIS 应与 BPCS 的时钟同步。

D.8.5 供电

D.8.5.1 SIS 的测量仪表、逻辑控制器、最终执行机构均应采用不间断电源(UPS)供电。

D.8.5.2 供电应符合 SH/T 3082 的规定。

D.8.6 动力中断

电源、气源等动力中断时，仪表的状态应符合设计文件的要求和本 SRS 的要求。

D.8.7 选型

SIS 测量仪表、逻辑控制器、最终执行机构的选型应符合本 SRS、设计文件、安装环境等要求。

D.8.8 SIS 逻辑控制器的应用程序

D.8.8.1 应用程序的组态应使用制造商的标准组态工具软件。

D.8.8.2 应用程序组态工具软件应具有下列功能：

a) 应用程序版本管理；
b) 应用程序正确性检查；
c) 标准功能块及其符号说明；
d) 应用程序的编辑、编译、下装及运行管理；
e) 应用程序的离线仿真测试功能；
f) 组态管理功能。

D.8.8.3 应用程序的设计、编程、组态、测试、集成、确认、运行维护及变更等应符合本 SRS 和工程设计文件的要求。

D.8.8.4 应用程序应进行离线和在线测试，确认其功能满足特定的目标和要求后再投入运行。

D.8.8.5 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。

D.8.8.6 应用程序应同时进行本地备份和异地备份。

D.8.9 网络信息安全

D.8.9.1 应进行网络安全风险评估或分析，采取相应的网络安全策略和安防措施。

D.8.9.2 SIS 宜按生产装置或联合装置进行物理网络分区，不同网络分区应相互隔离。

D.8.9.3 SIS 不应接入无线仪表和无线网络。

D.8.9.4 SIS 的服务器、操作员站、工程师站、事件顺序记录站及其他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。

D.8.9.5 SIS 应与工厂信息网络直接相连。与 SIS 无关的设备或网络不应接入 SIS 网络或利用网络传输数据。

D.8.10 确认

D.8.10.1 SIS 投入使用前应开展确认工作。确认工作是指检查最终交付的 SIS 的硬件、软件、应用程序等符合 SRS 和 SIS 其他相关安全技术要求，并与工程设计文件一致。

D.8.10.2 SIS 的确认工作宜包括下列内容：

a) SIS 逻辑控制器验收测试发现的问题已整改；
b) SIF 测量仪表、逻辑控制器、最终执行机构等的设置与安装符合 SRS 和 SIS 其他相关安全技术要求、安全手册和工程设计文件；
c) SIS 的联合调试符合 SRS 和 SIS 其他相关安全技术要求以及工程设计文件要求；
d) 供电、接地、供气、保温伴热等符合工程设计文件；
e) SIS 与 BPCS 的数据通信正常；
f) 维护旁路和操作旁路、紧急停车、复位等功能正常；
g) SIS 相关技术文件完整、准确；
h) 确认工作应记录归档。

D.9 SIF 通用要求

D.9.1 安全关键和非安全关键

D.9.1.1 在对联锁逻辑确定具体 SIF 时，应区分联锁逻辑中的安全关键和非安全关键。SIF 属于安全关键，只有安全关键才有可能属于 SIF，非安全关键不属于 SIF，不应参与 SIL 验证。

注 1： 联锁逻辑不等同于 SIF。SIF 应有特定的 SIL 等级，是对某一场景的安全保护功能。联锁逻辑是采用因果关系对保护功能的表达。联锁逻辑可以有 SIL 等级要求，也可以没有 SIL 等级要求。只有具有 SIL 等级要求的联锁逻辑才属于 SIF。一个具有 SIL 等级要求的联锁逻辑可能是一个 SIF，也可能包含多个 SIF，反之亦然。

注 2： 区分安全关键和非安全关键、确定 SIF 是 SIL 定级的工作。如果 SIL 验证中发现 SIF 中包括了非安全关键，可提出复核要求并由相关人员确定安全关键和非安全关键，以及 SIF。

D.9.1.2 LOPA 分析报告宜说明选择安全关键的理由，区别安全关键的风险和非安全关键的风险辨识。

D.9.2 运行模式

除非特殊说明，SIF 均为低要求模式。

D.9.3 SIL 等级

D.9.3.1 在低要求运行模式时，SIF 的 SIL 等级应采用 PFD_{avg} 或 RRF 衡量，根据表 D.3 确定。

表 D.3　SIL 等级(低要求运行模式)

SIL	PFD_{avg} 范围	RRF 范围[a]
1	$10^{-2} \leqslant PFD_{avg} < 10^{-1}$	$10 < RRF \leqslant 100$
2	$10^{-3} \leqslant PFD_{avg} < 10^{-2}$	$100 < RRF \leqslant 1\ 000$
3	$10^{-4} \leqslant PFD_{avg} < 10^{-3}$	$1\ 000 < RRF \leqslant 10\ 000$
4	$10^{-5} \leqslant PFD_{avg} < 10^{-4}$	$10\ 000 < RRF \leqslant 100\ 000$
[a] $RRF = 1/PFD_{avg}$。		

D.9.3.2　在连续运行模式或高要求运行模式时,SIF 的 SIL 等级应采用 PFH 衡量,根据表 D.4 确定。

表 D.4　SIL 等级(连续运行模式或高要求运行模式)

SIL	PFH 范围
1	$10^{-6} \leqslant PFH < 10^{-5}$
2	$10^{-7} \leqslant PFH < 10^{-6}$
3	$10^{-8} \leqslant PFH < 10^{-7}$
4	$10^{-9} \leqslant PFH < 10^{-8}$

D.9.3.3　SIF 的 SIL 等级应根据 SIL 定级确定。

D.9.3.4　石油化工和化工装置 SIF 的 SIL 等级不应高于 SIL3 级。如果在确定 SIL 等级时,有可能达到 SIL4,应重新分配保护层的安全功能,或采用多个独立的 SIF,使 SIL 等级不高于 SIL3。

D.9.4　SIF 目标失效量

应确定用于 SIL 验证的 SIF 目标失效量。SIL 定级给出明确的目标失效量时,SIF 目标失效量应采用此目标失效量。SIL 定级没有给出明确的目标失效量,只给出 SIL 等级时,SIF 目标失效量应参考表 D.3 或表 D.4,可采用要求达到的 SIL 等级对应的最小的 PFD_{avg} 或最大的 RRF 或最小的 PFH,例如当 SIF 为低要求运行模式时,SIL1 对应的 PFD_{avg} 范围为 $0.01 \leqslant PFD_{avg} < 0.1$,最小的 PFD_{avg} 为 0.01。

D.9.5　SIF 响应时间

D.9.5.1　SIF 的响应时间应小于过程安全时间,并有满足标准要求的足够的安全余量。本项目装置采用 SIF 的响应时间应小于过程安全时间的 1/2。

注:SIF 的响应时间=测量仪表响应时间+逻辑控制器响应时间(包括输入、逻辑运算和输出等环节)+最终执行机构响应时间+各个环节的滞后时间。

D.9.5.2　SIS 测量仪表、逻辑控制器、最终执行机构的响应时间应符合本 SRS 和设计文件的要求。

D.9.6　最高允许的 STR

当 SIF 的误动作可能造成的损失大于可容忍程度时,可规定可用性要求,并验证 SIF 满足可用性要求,例如验证 SIF 的 STR 满足企业可用性要求。

本项目装置没有可用性要求,不需要进行可用性验算。

D.9.7　手动停车

D.9.7.1　手动停车包括现场操作柱、控制室辅助操作台紧急停车按钮、SIS 操作站软按钮等。

D.9.7.2 手动停车应根据本 SRS 和设计文件进行设置。

D.9.7.3 紧急停车按钮应符合如下规定：

a) 紧急停车按钮宜设置在辅助操作台或现场，应带防护罩；

b) 紧急停车按钮动作应设状态报警和记录；

c) 紧急停车按钮不应设维护旁路开关或操作旁路开关。

D.9.8 复位

D.9.8.1 SIS 应被设计成一旦其将过程置于某个安全状态，除非另有规定，过程应保持在该安全状态直至工艺过程恢复正常并且 SIS 被复位。

D.9.8.2 本项目装置复位按钮采用 SIS 操作站软按钮。

D.9.8.3 复位按钮的动作应设置事件记录。

D.9.9 操作模式

D.9.9.1 装置操作模式通常包括检修或紧急停车后的开车、正常操作、正常停车、临时操作、紧急操作、紧急停车、牌号切换等。

D.9.9.2 SIF 数据表中应说明装置各种操作模式及每种模式下 SIF 的相关要求。没有需要说明的，则不填写。

D.9.10 检验测试间隔(TI)

D.9.10.1 SIS 或安全子系统的 TI 的确定宜综合考虑 SIL 验证的符合性、制造商要求和企业检维修与停车的整体规划。SIS 或安全子系统的 TI 宜与企业计划停车检修时间间隔相同。

D.9.10.2 为满足 SIL 验证的符合性，SIS 或安全子系统的 TI 与企业计划停车检修时间间隔相同具有困难时，可采用不同的时间间隔。同一 SIF 的测量仪表、最终执行机构和逻辑控制器可采用不同的 TI。

D.9.10.3 应根据历史检验测试数据、工厂经验、硬件退化情况、企业计划停车检修时间间隔等各种因素，定期和需要时重新评估检验测试间隔。

D.9.10.4 企业计划停车检修时间间隔大于 TI 时，应具备满足要求的在线检验测试设施，并应制定详细的在线检验测试程序，应有安全补偿措施，分析并保证在线检验测试的安全性。在线检验测试设施应为 SIS 设计的必要组成部分。

D.9.10.5 SIL 验证应按照实际的 TI 进行验证。

D.9.11 检验测试的实施

D.9.11.1 检验测试应包括 SIF 测量仪表、逻辑控制器、最终执行机构的检验测试，并应进行 SIF 回路的检验测试，包括从 SIF 测量仪表到逻辑控制器、逻辑控制器到最终执行机构的信号通路的检验测试等。

D.9.11.2 应确定每个 SIF 的检验测试文件，包括检验测试程序、评估细则、需要的工具清单等。

D.9.11.3 检验测试的内容应包括制造商特定要求的检验测试内容，还应包括设计文件、安全手册等要求的检验测试内容。

D.9.11.4 检验测试的实施应符合本 SRS、设计文件、安全手册、制造商要求、厂家资料等的规定。

D.9.11.5 检验测试的实施可参考 ISA TR 84.00.03 的相关规定。

D.9.12 功能安全认证

D.9.12.1 用于逻辑控制器的可编程电子系统应取得功能安全认证。

D.9.12.2 SIF 测量仪表和 SIF 最终执行机构可取得功能安全认证，也可没有功能安全认证。

D.9.12.3 SIF 测量仪表、SIF 最终执行机构、SIF 逻辑控制器的性能和设置应满足本 SRS 要求。

D.9.13 失效率数据(可靠性数据)

SIF 的 SIL 验证计算采用的仪表设备失效率数据(可靠性数据)宜来自以往使用数据、SIL 认证报告、公开发行的工业数据库或手册等。

D.9.14 检测到故障时的响应

D.9.14.1 在 SIS 中检测(通过诊断测试、检验测试或其他方式)到一个危险故障时,应执行联锁或采取补偿措施来维持安全运行。如果不能维持安全运行,则应采取规定的动作来达到或保持过程的安全状态。如果补偿措施依赖于操作员执行规定动作来响应某个报警(如打开或关闭阀门),该报警则应作为 SIS 的组成部分。

注 1:检测到故障未立即执行联锁,而是采取补偿措施来维持安全运行时,应有时间限制,除非另有规定,时间不应超过 MPRT。在 MPRT 时间内,应有满足要求的补偿措施来维持安全运行,达到 MPRT 时间,如果仍然不能解除故障并恢复正常,应立即执行联锁。在 MPRT 时间内,如果不能维持安全运行,应立即执行联锁。

注 2:可以在 SRS 中规定达到或保持过程的安全状态所需的特定动作(故障响应)。它可以是过程的安全停车,也可以是依赖于该故障 SIS 降低风险过程的一部分。

注 3:维持安全运行所需的补偿措施取决于安全完整性要求、危险事件对应的可容忍风险、SIS 硬件故障裕度、预期的平均维修时间以及其他保护层的可用性。在某些情况下,只要采取动作确保在 PFD_{avg} 计算时假设的 MPRT 时间内完成危险失效的维修即可;但在其他情况下,可能需要提供其他措施来补偿缺失的风险降低直至 SIS 完全恢复。

D.9.14.2 当 SIS 的某个危险故障是通过某个报警来获得操作员注意时,应对该报警进行适当的检验测试和变更管理。

D.9.14.3 应确定检测到故障时的系统行为对 SIL 验证的影响。

D.9.15 故障模式

D.9.15.1 两种常见的故障模式如下:

a) 将测量仪表配置成故障导向执行联锁的状态;

b) 将测量仪表配置成故障导向远离执行联锁的状态(即不执行联锁)。

注:如果将测量仪表设计成故障导向远离执行联锁的状态(即不执行联锁),确保操作员能得到测量仪表故障的报警以及培训操作员采取的纠正动作。关于对检测出故障的要求,见 D.9.13。

D.9.15.2 除非特殊说明,本项目装置 SIF 测量仪表检测到故障时,应配置成故障导向联锁状态。

注:考虑到满足要求的补偿措施的确定具有一定的复杂性以及在 MPRT 时间内可以解除故障并恢复正常具有一定的难度和不确定性,本项目装置采用了 D.9.15.1 两种常见故障模式中的 a)。当有可用性需求时,本项目装置采用的是通过可用性冗余配置实现,而不是通过 D.9.15.1 中的 b)的方式实现。

D.9.16 失电联锁和得电联锁

D.9.16.1 除非特殊说明,SIF 测量仪表作为联锁输入触发条件时,对于开关量类型的 SIF 测量仪表(例如压力开关、液位开关、阀位回讯等),其输出接点应设计成“故障安全型”,在工况异常(达到联锁条件)时,输出接点断开,直接触发或者与其他逻辑输入信号逻辑组合后触发执行联锁。

D.9.16.2 除非特殊说明,SIF 测量仪表作为允许启动输入触发条件时,对于开关量类型的 SIF 测量仪表(例如压力开关、液位开关、阀位回讯等),其输出接点应设计成“故障安全型”,在工况达到允许启动条件时,输出接点闭合,直接触发或者与其他逻辑输入信号逻辑组合后触发允许启动逻辑。

D.9.16.3 除非特殊说明,SIF 最终执行机构为气动控制阀时,应设计为联锁触发条件满足时 SIF 逻辑控制器输出断开接点信号,气动控制阀的电磁阀失电,执行联锁。

D.9.16.4 除非特殊说明，去 MCC 的联锁停机信号，对于中、高压电机(≥6 kV)，接点闭合停机，接点断开无动作；对于低压电机(≤1 kV)，接点断开停机，接点闭合无动作。

D.9.16.5 除非特殊说明，去 MCC 的启动电机信号，接点闭合启动，接点断开无动作；去 MCC 的允许启动信号，接点闭合允许启动，接点断开无动作。

D.9.16.6 除非特殊说明，SIS 辅助操作台上的紧急停车按钮至 SIS 逻辑控制器的紧急停车信号，接点断开联锁停车，接点闭合无动作。

D.9.16.7 除非特殊说明，SIS 逻辑控制器的输出至 SIS 辅助操作台上的报警灯屏的信号，接点闭合为报警。

D.9.16.8 除非特殊说明，SIS 辅助操作台上的允许旁路开关至 SIS 逻辑控制器的允许旁路信号，接点闭合为允许旁路，接点断开为不允许旁路。

D.9.17 维护旁路开关

D.9.17.1 维护旁路开关用于现场仪表和线路维护时旁路信号输入，使安全仪表系统逻辑控制器的输入信号处于正常状态。

D.9.17.2 维护旁路开关采用软件开关的方式时，每个安全联锁单元或工艺区域宜设硬件“允许旁路”开关作为软件维护旁路开关的“允许”条件。当维护旁路开关切换到旁路位置，且“允许旁路”开关切换到允许位置时方可实现旁路功能。可对一次允许旁路操作的仪表数量进行限制。“允许旁路”开关宜布置在辅助操作台上，由操作员管理。“允许旁路”开关和软维护旁路开关设置示例见图 D.1。本项目装置在辅助操作台上设置一个硬件“允许旁路”开关，同时，一次允许旁路操作的仪表数量限制为不应超过 2 个。

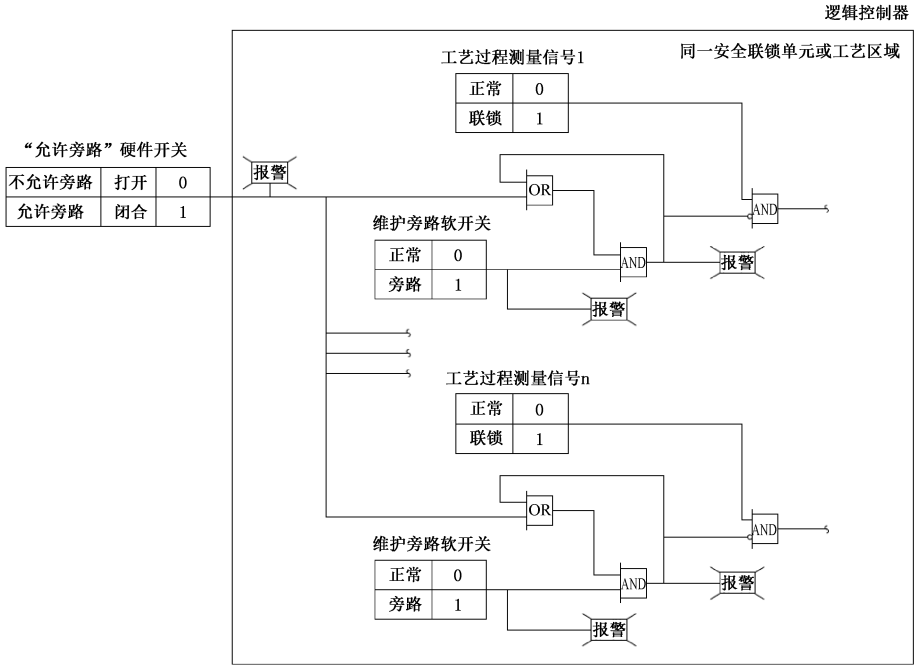

图 D.1 允许旁路开关与软维护旁路开关设置示例

D.9.17.3 除非特殊说明，本项目装置 SIF 测量仪表均设置维护旁路开关。

D.9.17.4 本项目装置维护旁路开关采用 SIS 操作站软开关。

D.9.17.5 维护旁路开关应设置在测量仪表输入信号通道上，手动紧急停车输入信号不应设维护旁路开关，SIS 输出信号不应设维护旁路开关。

D.9.17.6　维护旁路开关的操作应有报警和记录。维护旁路开关不应用于其他用途。

D.9.17.7　处于维护旁路状态时，应能监测工艺过程状态，应定期提示操作员 SIF 处于维护旁路状态，直至旁路解除。设置旁路计时报警，当旁路时间超过 8 h 仍未解除时再次报警。

D.9.17.8　维护旁路开关正常时应置于非旁路状态。

D.9.17.9　维护旁路开关的操作应严格管理。在由于旁路（维修或测试）导致 SIS 被禁用或降级时，应在相应的操作限制下（持续时间、过程参数等）采取补偿措施以维持安全。应向操作员提供旁路前和旁路中适用的规程，旁路移除前应做什么，以及处于旁路状态的最大允许持续时间等信息。这些信息应定期复审。

注：操作和维护规程可包括检验测试后是否移除旁路的验证。

D.9.17.10　当某个 SIS 设备被旁路时，只有在危险分析确定已实施补偿措施且其提供了足够的风险降低的情况下，才允许过程继续运行。应制定相应的操作规程。

D.9.18　操作旁路开关

D.9.18.1　操作旁路开关用于工艺开工和特殊过渡过程，在开工过程中输入信号还没正常之前使用，将输入信号暂时旁路，使安全仪表系统逻辑控制器的输入不受输入信号的影响。工艺过程正常后，操作旁路开关应置于非旁路状态，保持安全仪表系统的完整和正常运行。应当严格限制操作旁路开关的使用。操作旁路开关在工艺非开工时间应置于非旁路状态。操作旁路开关不应用于其他用途。

D.9.18.2　当工艺过程变量从初始值变化到工艺条件正常值，信号状态不改变时，不应设置操作旁路开关；当工艺过程变量从初始值变化到工艺条件正常值，信号状态发生改变且无旁路不能建立正常工艺条件时，应设置操作旁路开关。

D.9.18.3　操作旁路开关应设置在输入信号通道上，输出信号不应设置操作旁路开关；操作旁路开关的动作应设置报警和记录。

D.9.18.4　本项目装置操作旁路开关采用 SIS 操作站软开关。

D.9.19　阀门部分行程测试（PST）

D.9.19.1　阀门 PST 设施通常用于紧急停车状态为关闭位置的气动切断阀。装置正常运行时，在不影响过程正常运行和安全前提下，对处于全开位置的气动切断阀关闭部分行程，应控制阀门 PST 可以关闭的行程，以保证不干扰过程控制。SIF 的动作应优先于阀门 PST。气动切断阀 PST 设施可分为机械制动、智能阀门定位器、智能阀位变送器、电磁阀组等方式。

D.9.19.2　企业根据生产管理需求，对气动切断阀需要采用较长的检验测试间隔，且不具备在线测试手段，在不能满足 SIL 验证或者工程公司、专利商有要求时，可设置阀门 PST 设施。

D.9.19.3　在阀门上采用 PST 措施时，认定的危险失效 DC 应低于 70%。

D.9.19.4　阀门 PST 的配置和要求宜符合 ISA TR96.05.01 的相关规定。

D.9.19.5　阀门 PST 不应降低 SIF 的可靠性。

D.9.19.6　应分析阀门 PST 对 STR 的影响，SIF 的 STR 应低于企业最高允许的 STR。

D.9.19.7　应制定完善的阀门 PST 管理制度。

D.9.20　SIF 的独立性

D.9.20.1　同一个测量仪表、逻辑控制器、最终执行机构和关联设备可用于不同的 SIF，共用部分应满足所有相关 SIF 的 SRS，包括 SIF 要求和 SIL 要求，并应进行验证。

D.9.20.2　SIS 逻辑控制器应独立于 BPCS 控制器，并应独立完成 SIF。SIS 逻辑控制器可执行非 SIF。SIF 应具有优先权，非 SIF 的失效或指令不应影响 SIF 的有效性，包括不应降低 SIF 的 SIL。

D.9.20.3　BPCS 不应执行 SIF。

D.9.21 SIF 的冗余配置

D.9.21.1 SIF 的冗余配置包括安全性冗余配置和可用性冗余配置。

D.9.21.2 SIF 安全性冗余配置应同时满足 SIF 危险失效率（PFD_{avg}或 PFH）、HFT 和 SC 的要求。SIF 安全性冗余配置还应符合 GB/T 50770 的相关规定。

注 1：根据 SIF 要求的 SIL 等级，结合标准规范和监管文件的要求、工程经验，给出初步设计方案，包括冗余配置方案，在确定仪表选型后，再验证冗余配置方案合规性，如果有不满足，则调整设计方案，直至满足合规性。

注 2：SIF 要达到 SIL'n'，合规性判定包括同时满足以下要求：

a） PFD_{avg}/RRF/PFH 在 SIL'n'范围内，可参考 D.9.21.2 的注 3；

b） HFT 满足 SIL'n'的要求，可参考 D.9.21.2 的注 4；

c） SC 达到 SC'n'或以上，可参考 D.9.21.2 的注 5；

d） 其他标准规范和监管文件要求，例如 GB/T 50770 的相关要求，可参考 D.9.21.2 的注 6、注 7。

注 3：危险失效率（PFD_{avg}或 PFH）对 SIF 安全性冗余配置的要求和验证可参考 T/CCSAS 045—2023 中的 7.4、附录 C、附录 D。

注 4：HFT 对 SIF 安全性冗余配置的要求和验证可参考 T/CCSAS 045—2023 中的 7.5。

注 5：SC 对 SIF 安全性冗余配置的要求和验证可参考 T/CCSAS 045—2023 中的 7.6。

注 6：GB/T 50770 对于 SIF 测量仪表和控制阀的安全性冗余配置的要求为：

a） SIL1 的 SIF，可采用单一测量仪表、可采用单一控制阀；

b） SIL2 的 SIF，宜采用冗余测量仪表、宜采用冗余控制阀；

c） SIL3 的 SIF，应采用冗余测量仪表、应采用冗余控制阀。

注 7：本项目装置规定 SIF 逻辑控制器采用兼顾安全性和可用性的配置。

D.9.21.3 SIF 可用性冗余配置应满足法律、法规、规章、标准规范要求和企业可容忍风险标准的要求。在 SIF 的误停车不涉及法律、法规、规章、标准规范要求时，企业可决定最高允许的 STR，并据此确定 SIF 的可用性配置。

D.9.21.4 当测量仪表需要调整安全性或者可用性冗余结构时，可参考表 D.5 和表 D.6 进行合理调整。冗余配置的同一变量测量仪表宜设置偏差报警。

表 D.5 冗余结构示例

单一仪表	1oo1
安全性冗余结构	1oo2、1oo3
可用性冗余结构	2oo2、3oo3
兼顾安全性和可用性的冗余结构	2oo3、2oo4

表 D.6 冗余结构的调整对安全性和可用性的影响

冗余结构的调整	安全性	可用性	备注
1oo1 改为 1oo2	提高	降低	提高了安全性，降低了可用性
1oo1 改为 2oo2	降低	提高	降低了安全性，提高了可用性
1oo1 改为 2oo3	提高	提高	兼顾了安全性和可用性
1oo2 改为 2oo3	小幅降低	提高	兼顾了安全性和可用性
2oo2 改为 2oo3	提高	小幅降低	兼顾了安全性和可用性

D.9.22 共因失效

D.9.22.1 可行的范围内，应减少共因失效。在确定共因失效系数时，应识别和考虑共因失效根源。共因失效根源举例如下：

a) 物理和化学：设备在共同的内部或外部条件下，导致冻结、堵塞、自聚等；
b) 机械：设备在共同的机械影响下，例如震动；
c) 技术：设备使用了相同或者相似的技术；
d) 电气：设备共用电源、仪表路径、接线柜；
e) 环境：设备暴露于相同的环境，例如电磁干扰；
f) 人为因素：设备由相同或相似的人员设计、安装、维护和测试。

D.9.22.2 减少共因失效可从共因失效根源着手，采用多种举措实现，包括：冗余设备和相关敷设设备的独立性、物理上的分类、多样性、良好的工程实践等。

D.9.22.3 除非特殊说明，本项目装置共因失效因子(β)可参考 GB/T 20438.6 的相关说明进行评估确定，也可按照表 D.7 确定。表 D.7 中的 β 值应根据现场实际情况进行修正。

表 D.7 典型仪表共因失效因子(β)参考值

名称		共因失效因子(β)
测量仪表	开关	0.05
	变送器	0.04
	可燃气、毒性气探测器	0.06
最终执行机构	切断阀	0.03
	电磁阀(同一阀门)	0.10
	电磁阀(不同阀门)	0.03
	控制阀	0.03
	泄压阀	0.05
	继电器	0.03

D.9.23 隔离措施

D.9.23.1 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。

D.9.23.2 本项目装置来自 MCC 的 SIS 数字量输入信号和至 MCC 的 SIS 数字量输出信号均在 SIS 侧配置继电器，进行隔离。

D.9.24 取源

D.9.24.1 SIS 测量仪表的取源点宜独立于 BPCS 测量仪表的取源点。

D.9.24.2 SIS 不同测量仪表的取源点宜独立设置。

D.9.25 SIL 验证范围

D.9.25.1 SIL 验证应以 SIF 回路进行，应包括 SIF 测量仪表、逻辑控制器、控制阀、部分附属设备。应包含在 SIL 验算中的附属设备包括：安全栅、隔离栅、电涌防护器、SIS 侧继电器、SIS 侧隔离器、一入二

出信号分配器等。可不包含在 SIL 验算中的附属设备包括:引压管、电缆、接线箱、端子排、电源、伴热、电机、电气侧继电器等。

D.9.25.2 SIF 控制阀的执行机构、电磁阀、阀体均应参与 SIL 验算。

D.9.25.3 非 SIF 可不进行 SIL 验算。

D.9.25.4 除非 SIS 紧急停车按钮和相关环节(包括操作人员和获取信息的措施)满足功能安全标准的要求并获得置信,SIS 紧急停车按钮不应参与 SIL 验算,不应降低 SIF 可以达到的危险失效率。

D.9.25.5 非安全关键测量仪表和非安全关键最终执行机构不应参与 SIL 验算,不应降低 SIF 可以达到的危险失效率。

D.9.26 测量仪表和最终执行机构的共用

D.9.26.1 SIL1 的 SIF,SIF 测量仪表和最终执行机构宜与 BPCS 测量仪表和最终执行机构分开设置。SIL2 和 SIL3 的 SIF,SIF 测量仪表和最终执行机构应与 BPCS 测量仪表和最终执行机构分开设置。

D.9.26.2 当 SIS 与 BPCS 共用测量仪表和最终执行机构时,共用设备应符合 GB/T 20438(所有部分)、GB/T 21109(所有部分)、GB/T 50770 的相关规定。SIS 应具有优先权,BPCS 的失效或指令不应影响 SIS 的功能安全,包括不应降低 SIF 的 SIL 等级。

D.9.26.3 当 SIS 与 BPCS 共用测量仪表和最终执行机构时,共用设备应同时满足相关 SIF 和 BPCS 控制的要求,包括本 SRS 和设计文件的要求。

D.9.26.4 SIS 与 BPCS 共用气动调节阀时,应配置 SIS 驱动的电磁阀,确保安全仪表系统的动作优先并独立完成。电磁阀应安装在阀门定位器与执行机构之间,电磁阀宜采用 24VDC 长期励磁型,电磁阀电源应由 SIS 提供。

D.9.26.5 当 SIS 与 BPCS 共用测量仪表和最终执行机构时,应进行 SIL 验证。应分析 SIS 与 BPCS 共用设备对 SIF 的 SIL 定级的影响。SIL 验证时,应注意 SIS 与 BPCS 共用设备对运行模式的影响,例如从低要求运行模式改变为连续运行模式。共用设备应满足 SIF 安全生命周期的相关要求,包括维护规程和策略。

D.9.27 SIL 验证不合格调整

SIL 验证不满足要求时,可采取下列措施:

a) 选择高可靠性设备;
b) 提高冗余配置;
c) 缩短 TI(如适用);
d) 提高检验测试覆盖率;
e) 减少共因失效;
f) 增加 PST 功能;
g) 重新进行安全评估,考虑是否可以通过增加保护层来降低 SIL 等级要求。

D.9.28 变更

SIF 有变动时(包括仪表设备的型号、软件的版本号、制造商、联锁逻辑、独立和共用、场景等方面的变动),应重新开展 SIL 评估,包括 SIL 定级和 SIL 验证。

D.9.29 安全手册

D.9.29.1 安全手册的目的是用文件记录如何才能安全应用某设备、SIS 子系统或系统的所有相关必要信息。

D.9.29.2 安全手册内容应涵盖在设备的预期配置和预期运行环境下,SIS 相关的运行、维护、故障检测

和约束。

D.9.29.3 安全仪表系统安全手册包括逻辑控制器制造商及关联设备制造商的安全手册、现场测量仪表及最终元件制造商的安全手册。

D.9.29.4 SIF 相关仪表的工程设计、验证、选型、制造、安装、运行、操作、维护、检验测试、安全管理策略等应符合本 SRS、设计文件、安全手册等的要求。

D.9.30 降级

D.9.30.1 检测到故障时的响应应符合 D.9.14 的规定。

D.9.30.2 失效模式应符合 D.9.15 的规定。

D.9.30.3 除非特殊说明，本项目装置中 SIS 测量仪表诊断出故障后的降级策略见表 D.8。

表 D.8 SIS 测量仪表诊断出故障后的降级策略

初始表决	一个仪表检测到故障后的表决降级	二个仪表检测到故障后的表决降级	三个仪表检测到故障后的表决降级
四取三	三取二	二取一	执行联锁
四取二	三取一	执行联锁	执行联锁
三取二	二取一	执行联锁	执行联锁
三取一	执行联锁	执行联锁	执行联锁
二取二	一取一	执行联锁	不适用
二取一	执行联锁	执行联锁	不适用
一取一	执行联锁	不适用	不适用

D.9.30.4 除非特殊说明，本项目装置 SIF 测量仪表检测到故障时，应配置成故障导向联锁状态。

注： 考虑到满足要求的补偿措施的确定具有一定的复杂性以及在 MPRT 时间内可以解除故障并恢复正常具有一定的难度和不确定性，本项目装置采用了 D.9.15.1 两种常见故障模式中的 a)。当有可用性需求时，本项目装置采用的是通过可用性冗余配置实现，而不是通过 D.9.15.1 中的 b)的方式实现。

D.9.31 应用程序

应用程序安全要求、应用程序的开发和测试应符合 GB/T 21109.1、本 SRS、设计文件的相关规定。

D.9.32 非 SIF 联锁

在 PFD_{avg} 介于 10^{-1} 和 1 之间时，联锁保护功能可由 BPCS 实现，也可由 SIS 实现。

注 1： PFD_{avg} 介于 10^{-1} 和 1 之间的联锁保护功能在实际工程中通常是指 SIL 评估未达到 SIL1 级，但具有风险降低要求的联锁保护功能。PFD_{avg} 介于 10^{-1} 和 1 之间的联锁保护功能不需要进行 SIL 验证。

注 2： 有些资料、文献和标准将 PFD_{avg} 介于 10^{-1} 和 1 之间的联锁保护功能称为 SILa 或者 SIL0 的联锁保护功能。SILa 或者 SIL0 的联锁保护不属于 SIF，SILa 和 SIL0 不是 SIL 等级，SIL 等级有且仅有 SIL1、SIL2、SIL3、SIL4 四个级别。

注 3： 在 PFD_{avg} 介于 10^{-1} 和 1 之间时，联锁保护功能由 BPCS 实现时，满足 D.9.33 的规定，当不能满足 D.9.33 的规定时，联锁保护应由 SIS 实现。例如，SIL 定级某联锁保护 PFD_{avg} 为 0.2，对应 RRF 为 5，假设同一个事故场景中，BPCS 已经作为 IPL 达到两次，第一次为 BPCS 控制，第二次为 BPCS 报警和人员响应，并且 RRF 分别取值为 10，合计 RRF 达到了 100，这时，上述 PFD_{avg} 为 0.2 的联锁保护不应由 BPCS 实现，而由 SIS 实现。

注 4： 除非 ALARP 分析可以忽略 PFD_{avg} 介于 10^{-1} 和 1 之间的风险，不忽略 PFD_{avg} 介于 10^{-1} 和 1 之间的风险。

注 5： 对于同一个事故场景，当 BPCS 已经作为 IPL 两次，每次 RRF 取值为 10，合计达到 100，假设其中一个 IPL 为

BPCS 联锁，并且 SIL 定级为仍然存在 PFD_{avg} 为 0.2 的风险缺口，对应 RRF 为 5，这时此 RRF 为 5 的风险缺口联锁保护不应由 BPCS 实现，此时有两个可行工程设计方案，一是此 RRF 为 5 的风险缺口联锁保护由 SIS 实现；二是将 RRF 为 10 的 BPCS 联锁和 RRF 为 5 的风险缺口联锁合并为 SIS 联锁，RRF 按照 50，定级为 SIL1，由 SIS 实现。

注 6：对于同一个事故场景，当 BPCS 已经作为 IE，同时 BPCS 联锁作为 IPL 一次，RRF 取值为 10，假设 SIL 定级为仍然存在 PFD_{avg} 为 0.2 的风险缺口，对应 RRF 为 5，这时此 RRF 为 5 的风险缺口联锁保护不应由 BPCS 实现，此时有两个可行工程设计方案，一是此 RRF 为 5 的风险缺口联锁保护由 SIS 实现；二是将 RRF 为 10 的 BPCS 联锁和 RRF 为 5 的风险缺口联锁合并为 SIS 联锁，RRF 按照 50，定级为 SIL1，由 SIS 实现。

D.9.33 BPCS 多个回路作为 IPL

D.9.33.1 BPCS 作为 IE 时，在同一个场景中 BPCS 作为 IPL 应不超过一次，且其 RRF 应小于或等于 10。

D.9.33.2 BPCS 不作为 IE 时，在同一个场景中 BPCS 作为 IPL 不应超过两次，其中单个 IPL 的 RRF 应小于或等于 10，BPCS 作为 IPL 合计的 RRF 应小于或等于 100。

D.9.33.3 以下两种情况应按照 GB/T 32857 相关要求进行评估：

a) BPCS 作为 IE 并且在同一个场景中 BPCS 作为 IPL 一次，同时 BPCS 作为 IE 和作为 IPL 共用了控制器；

b) BPCS 不作为 IE 时，在同一个场景中 BPCS 作为 IPL 两次，同时 BPCS 作为两次 IPL 共用了控制器。

D.9.34 测量仪表的信号延迟

D.9.34.1 当希望减少因测量仪表虚假信号引起的误停车，可在 SIS 逻辑控制器实现逻辑功能组态时加测量仪表的信号延迟，只有当测量仪表信号达到联锁设定值并保持达到联锁设定值超过一个特定的延迟时间，才算达到了联锁设定值并执行联锁。延迟时间应根据仪表类型和工艺过程的特点确定，应符合本 SRS 和设计文件的规定。延迟时间应计入 SIF 响应时间，并应符合 D.9.5 的规定。

D.9.34.2 除非另有规定，当过程安全时间小于等于 10s 时，不应设置 SIF 测量仪表的信号延迟。

D.9.35 要求来源和要求发生的频率

SIF 的运行方式，包括低要求模式、高要求模式、连续模式，含义如下：

a) 低要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率不大于一年一次；

b) 高要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率大于一年一次；

c) 连续模式：在这种运行模式下，SIF 作为正常运行的一部分保持过程处于一种安全状态。

“要求来源和要求发生的频率”中的“要求”等同于“低要求模式、高要求模式”中的“要求”。SIF 应定义 SIF 的运行模式，可不具体描述“要求来源和要求发生的频率”，需要描述时，可以写在表 D.10SIF 数据表的“其他要求”中。

要求来源和要求发生的频率通常由 IE、SIF 触发前起作保护作用的独立保护层、使能必要事件/条件等方面的因素综合确定。

示例：

要求发生频率＝IE 频率×SIF 触发前起作保护作用的独立保护层的 PFD(例如 BPCS 的 PFD)×使能必要事件/条件发生的概率(如果适用)

注：上述公式中不乘以 SIF 触发后起作保护作用的独立保护层的 PFD(例如安全阀的 PFD)，不乘以条件修正因子。

D.10 SIF 清单

本项目装置共有 SIF××个，其中 SIL1 的××个、SIL2 的××个、SIL3 的××个。

以下为本项目装置的 SIF 清单。

……

（SIF 清单格式和填写示例见附录 A）

表 D.9 是依据附录 C 而给出的 SRS 清单的示例。

表 D.9 SIF 清单

序号	SIF 编号	SIF 功能说明	SIL 等级/验证达到的 SIL 等级	目标失效量/验证达到的目标失效量（PFD_{avg}/RRF/PFH）	备注
1	SIF-101	检测和阻止正己烷缓冲罐溢流	SIL1/	$PFD_{avg}=1\times10^{-2}$/RRF=100	

D.11 SRS 数据表

SRS 数据表包括 SIF 数据表、测量仪表数据表、逻辑控制器数据表和最终执行机构数据表。

以下为本项目装置的 SRS 数据表，以所属 SIF 的 SIF 编号，按照 SIF 数据表、测量仪表数据表、逻辑控制器数据表和最终执行机构数据表双级排序。

……

（SRS 数据表格式和填写示例见附录 A）

表 D.10～表 D.15 是依据附录 C 而给出的 SRS 数据表的示例。

表 D.10 SIF 数据表

SIF 编号	SIF-101
SIF 描述	检测和阻止正己烷缓冲罐溢流
HAZOP 报告	略
LOPA 报告	略
危险事件说明	由于储罐溢流和防火堤失效，导致释放的正己烷流出防火堤，发生火灾和人员伤亡。后果等级 5
安全状态	远程控制阀 RBV 关闭
SIF 功能说明	LT-95 高液位联锁关闭远程控制阀 RBV
逻辑图号	IS-101
因果表号	YGB-101
运行模式	低要求运行模式
SIL 等级/验证达到的 SIL 等级	SIL1/

表 D.10　SIF 数据表（续）

目标失效量/验证达到的目标失效量（PFD_{avg}/RRF/PFH）	$PFD_{avg}=1\times10^{-2}$/RRF=100		
过程安全时间	略		
SIF 响应时间要求	略		
最高允许的 STR/验证达到的 STR	略		
输入位号	LT-95	输出位号	RBV
逻辑要求	LT95 高液位联锁关闭远程控制阀 RBV		
手动停车	略		
复位	设置复位，RS-101		
使用期限	略		
操作模式	略		
环境条件	略		
多 SIF 同时动作产生新风险（如果存在分析并说明）	未发现（根据设计文件填写）		

表 D.11　测量仪表数据表

位号	LT-95
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	正己烷缓冲罐液位测量
设备类型	雷达液位计
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-101
因果表号	YGB-101
与其他测量仪表组成群组	无
信号类型	4 mA～20 mA
测量范围	0～100%
联锁设定值	80%
响应时间要求	≤2 s

表 D.11　测量仪表数据表（续）

TI/a	2
MRT/h	24
MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	0FIT
未检测到的安全失效率(λ_{SU})	260FIT
检测到的危险失效率(λ_{DD})	736FIT
未检测到的危险失效率(λ_{DU})	79FIT
SFF	92.7%
具备的 SC 等级	SC3
检测到故障时的响应	故障导向联锁状态
维护旁路	设置
操作旁路	不设置
安全手册	略
共因失效因子(β)	5%
与 BPCS 的独立性	与 BPCS 独立
其他要求 1	略
其他要求 2	略

表 D.12　逻辑控制器数据表

位号	SIS-101
设备类型	逻辑控制器
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-101
因果表号	YGB-101
响应时间要求	≤500 ms
TI/a	2

表 D.12　逻辑控制器数据表（续）

MRT/h	24
MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	略
未检测到的安全失效率(λ_{SU})	略
检测到的危险失效率(λ_{DD})	略
未检测到的危险失效率(λ_{DU})	略
SFF	略
具备的 SC 等级	SC3
检测到故障时的响应	故障导向联锁状态
接口要求	和 BPCS 间设置通信接口
安全手册	填写安全手册文件名和编号,或者填写随仪表设备提供
其他要求 1	略
其他要求 2	略

表 D.13　最终执行机构数据表-RBV 电磁阀

位号	RBV 电磁阀
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	RBV 电磁阀
设备类型	气动切断阀
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-101
因果表号	YGB-101
与其他最终执行机构组成群组	无
响应时间要求	略
TI/a	2
MRT/h	24

表 D.13　最终执行机构数据表-RBV 电磁阀（续）

MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	略
未检测到的安全失效率(λ_{SU})	略
检测到的危险失效率(λ_{DD})	略
未检测到的危险失效率(λ_{DU})	略
SFF	略
具备的 SC 等级	SC3
得电/失电联锁	失电联锁
联锁安全状态	失电联锁关闭 RBV
信号/动力中断时的动作	失电联锁关闭 RBV、气源故障关闭 RBV(FC)
现场手动复位	无现场手动复位
手动要求	无
阀门 PST	带
安全手册	填写安全手册文件名和编号，或者填写随仪表设备提供
共因失效因子(β)	略
与 BPCS 的独立性	与 BPCS 独立
其他要求 1	略
其他要求 2	略

表 D.14　最终执行机构数据表-RBV 气动执行机构

位号	RBV 执行机构
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	D101 出口切断阀
设备类型	气动执行机构
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-101

表 D.14　最终执行机构数据表-RBV 气动执行机构（续）

因果表号	YGB-101
与其他最终执行机构组成群组	无
响应时间要求	略
TI/a	2
MRT/h	24
MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	略
未检测到的安全失效率(λ_{SU})	略
检测到的危险失效率(λ_{DD})	略
未检测到的危险失效率(λ_{DU})	略
SFF	略
具备的 SC 等级	SC3
得电/失电联锁	失电联锁
联锁安全状态	失电联锁关闭 RBV
信号/动力中断时的动作	失电联锁关闭 RBV、气源故障关闭 RBV(FC)
现场手动复位	无现场手动复位
手动要求	无(假设设计文件如此)
阀门 PST	带(假设设计文件如此)
安全手册	填写安全手册文件名和编号,或者填写随仪表设备提供
共因失效因子(β)	略
与 BPCS 的独立性	与 BPCS 独立
其他要求 1	气动执行机构要求供风独立
其他要求 2	略

表 D.15　最终执行机构数据表-RBV 阀体

位号	RBV 阀体
P&ID 号	AQ/T 3054—2015 中图 G.2
安装位置和用途描述	RBV 阀体
设备类型	切断阀
制造商和型号	略
所属 SIF 的 SIF 编号	SIF-101
逻辑图号	IS-101
因果表号	YGB-101
与其他最终执行机构组成群组	无
响应时间要求	略
TI/a	2
MRT/h	24
MTTR/h	24
MPRT/h	24
PTC	95%
MT/a	10
失效率数据来源	SIL 证书
检测到的安全失效率(λ_{SD})	略
未检测到的安全失效率(λ_{SU})	略
检测到的危险失效率(λ_{DD})	略
未检测到的危险失效率(λ_{DU})	略
SFF	略
具备的 SC 等级	SC3
得电/失电联锁	失电联锁
联锁安全状态	失电联锁关闭 RBV
信号/动力中断时的动作	失电联锁关闭 RBV、气源故障关闭 RBV(FC)
现场手动复位	无现场手动复位
手动要求	无
阀门 PST	带
安全手册	填写安全手册文件名和编号,或者填写随仪表设备提供
共因失效因子(β)	略
与 BPCS 的独立性	与 BPCS 独立
其他要求 1	泄漏等级符合 API 598 的规定
其他要求 2	气动执行机构要求供风独立

D.12 逻辑要求

应对每一个 SIF 给出对应的逻辑要求，逻辑要求可采用逻辑说明、逻辑图、因果表等形式表达。

以下为本项目装置的 SIF 的逻辑要求，以所属 SIF 的 SIF 编号排序。

……

注：逻辑说明、逻辑图、因果表应注明安全关键和非安全关键。

（因果表格式和填写示例见附录 B）

表 D.16 是依据附录 C 而给出的因果表的示例。假设工程设计按照，高液位联锁关闭 RBV 为安全关键动作，高液位联锁关闭 LV-90 为非安全关键动作考虑。

表 D.16 因果表 YGB-101

<table>
<tr><td colspan="4" rowspan="4">逻辑联锁号：IS-101
所属 SIF 的 SIF 编号：SIF-101

功能说明：
LT-95 高液位联锁关闭远程控制阀 RBV

注：本因果表中的测量仪表测量的均为安全关键变量，最终执行机构执行的均为安全关键动作。</td><td>序号</td><td>1</td><td>2</td><td rowspan="5">备注</td></tr>
<tr><td>位号</td><td>RBV</td><td></td></tr>
<tr><td>描述</td><td>正己烷缓冲罐进口阀</td><td>略</td></tr>
<tr><td>P&ID 号</td><td>101</td><td>略</td></tr>
<tr><td colspan="2">动作</td><td>关闭</td><td>略</td></tr>
<tr><td rowspan="2">序号</td><td rowspan="2">位号</td><td rowspan="2">描述</td><td rowspan="2">P&ID 号</td><td rowspan="2">修改</td><td></td><td></td><td></td></tr>
<tr><td>备注</td><td></td><td></td></tr>
<tr><td>1</td><td>LT-95</td><td>正己烷缓冲罐液位高高</td><td>101</td><td></td><td></td><td>×</td><td></td></tr>
<tr><td>2</td><td>略</td><td>略</td><td>略</td><td>略</td><td>略</td><td>略</td><td></td></tr>
</table>

D.13 具体要求

略。

D.14 对照表

GB/T 21109.1—2022 和 T/CCSAS 054—2024 的对照表见表 D.17。

表 D.17　GB/T 21109.1—2022 和 T/CCSAS 054—2024 的对照表

GB/T 21109.1—2022		T/CCSAS 054—2024						
10.3.2	内容	8.2.3	附录 D	附录 A				
				表 A.1	表 A.2	表 A.3	表 A.4	表 A.5
a)	SIF 描述	a)		√	√			
b)	SIF 输入和输出清单	b)	D.9.1、D.9.32		√			
c)	识别和考虑共因失效	c)	D.9.20、D.9.21、D.9.22、D.9.23、D.9.26、D.9.33			√		√
d)	SIF 过程安全状态定义	d)			√			
e)	多个 SIF 同时发生的危险	e)			√			
f)	SIF 触发源和要求频率	f)	D.9.35					
g)	TI	g)	D.9.10			√	√	√
h)	执行检验测试的要求	h)	D.9.11、D.9.19、D.9.29			√ 注 1	√ 注 1	√ 注 1
i)	SIF 响应时间要求	i)	D.9.5、D.9.34		√	√	√	√
j)	SIF 的 SIL 和运行模式	j)	D.9.2、D.9.3、D.9.4	√	√			
k)	SIF 测量、范围、精度和联锁值	k)				√		
l)	SIF 动作成功的描述	l)						√
m)	SIF 输入和输出的功能关系	m)		√ 注 2	√ 注 2	√ 注 2	√ 注 2	√ 注 2
n)	SIF 手动停车要求	n)	D.9.7		√			
o)	得电或失电跳闸	o)	D.9.16					
p)	SIF 复位要求	p)	D.9.8		√			
q)	SIF 最大允许 STR	q)	D.9.6		√			
r)	SIF 失效模式和响应	r)	D.8.6、D.9.14、D.9.15、D.9.30			√	√	√
s)	启动和重新启动要求	s)	注 3					
t)	SIS 和其他系统接口	t)	D.8.2					
u)	工厂操作模式	u)	D.9.9					
v)	应用程序安全要求	v)	D.9.31					
w)	旁路要求	w)	D.9.17、D.9.18			√		

表 D.17　GB/T 21109.1—2022 和 T/CCSAS 054—2024 的对照表（续）

GB/T 21109.1—2022		T/CCSAS 054—2024						
10.3.2	内容	8.2.3	附录 D	附录 A				
				表 A.1	表 A.2	表 A.3	表 A.4	表 A.5
x)	检测到故障时的响应	x)	D.8.6、D.9.14、D.9.15、D.9.30			√	√	√
y)	MRT	y)				√	√	√
z)	SIS 输出状态危险组合	z)			√ 注 4			
aa)	极端环境条件	aa)	D.3		√			
bb)	正常和异常操作模式	bb)	D.9.9		√ 注 4	√ 注 4		√ 注 4
cc)	SIF 在意外事故中的要求	cc)			√ 注 4	√ 注 4		√ 注 4

注 1：安全手册可能会包含相关内容，如果安全手册没有包含相关内容，可以在其他要求中体现，或者专门文件进行相关说明。

注 2：SIF 输入和输出的功能关系包括：输入和输出之间的功能关系、输入之间的功能关系、输出之间的功能关系。

注 3：如果相关要求，可以专门说明。

注 4：如果相关要求，可以在其他要求中体现，或者专门文件进行相关说明。

注 5：如果有要关注的内容在附录 A 表格中没有体现，可以在相关表格的其他要求中体现，或者专门文件进行相关说明。

D.15　版次说明

本 SRS 是第三版，历次版本发布情况如下：

——2021 年 5 月首次发布；

——2022 年 9 月第一次修订；

——本次为第二次修订。

本次修订主要变化内容如下：

a) 增加了 SIF-×××、SIF-×××、SIF-×××，更新了 SRS 的相关内容；

b) 经验证，SIF-×××不能满足目标失效量要求，修改了仪表选型，更新了相关失效率数据，更新了 SRS 的相关内容；

c) SIF-×××存在 BPCS 和 SIS 共用测量仪表，重新进行了 SIL 定级和 SIL 验证，更新了 SRS 的相关内容；

d) SIF-×××的最终执行机构 XV-×××，根据本项目装置实际情况无法做到 TI 为 2 年，修改了仪表选型，更新了相关失效率数据，并已重新验证并满足要求，更新了 SRS 的相关内容；

e) SIF-×××的测量仪表修改了仪表选型，更新了相关失效率数据，已重新验证并满足要求，更新了 SRS 的相关内容；

f) ……

参 考 文 献

[1] GB/T 21109.1—2022 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、硬件和应用编程要求

[2] GB/T 21109.3—2007 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

[3] AQ/T 3054—2015 保护层分析(LOPA)方法应用导则

[4] HG/T 20511—2014 信号报警及联锁系统设计规范

中国化学品安全协会
团 体 标 准
安全仪表系统(SIS)安全要求规格书(SRS)编写指南
T/CCSAS 054—2025
*
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)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 4 字数 110 千字
2025 年 3 月第 1 版 2025 年 3 月第 1 次印刷
*
书号:155066·5-10259 定价 97.00 元

T/CCSAS 054-2025