ICS 25.040
N 10

中华人民共和国国家标准

GB/T 32202—2015

油气管道安全仪表系统的功能安全评估规范

Functional safety of safety instrumented system in oil and gas pipelines —Assessment code

2015-12-10 发布 2016-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国机械工业联合会提出。

本标准由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本标准主要起草单位:机械工业仪器仪表综合技术经济研究所、中国石油天然气股份有限公司管道分公司、中国石油天然气管道工程有限公司、上海黑马安全自动化系统有限公司、北京市劳动保护科学研究所、深圳市华测检测技术股份有限公司、杭州和利时自动化有限公司、横河电机(中国)有限公司、ABB(中国)有限公司、中国石油北京油气调控中心、中国石油化工集团公司安全环保局、中国石油化工集团公司管道局、中国石油北京天然气管道有限公司。

本标准主要起草人:孟邹清、史学玲、程德发、李秋娟、刘瑶、史威、安垚、王怀义、聂中文、顾峥、冯禄、李官政、朱平、张建国、靳江红、黄劲松、冯晓升、王海青、帅冰、徐皑冬、祁国成、寇建朝、高安东、李国海、相桂生、董秀娟、钱大涛、王毅、姚志强、杨全博、马欣欣、季俊、熊文泽、王春喜、王德吉。

引　言

安全仪表系统在20世纪80～90年代发展起来，以其高可靠性、安全性和灵活性在油气管道领域内得到了广泛应用，是保障油气管道生产安全的重要措施。安全仪表系统用于执行安全仪表功能，以保证运行过程在出现危险情况时进入安全状态，避免或减少对人员、环境、设备造成的危害。因此对安全仪表系统实现的功能安全和安全完整性进行评估十分重要。

目前国际上已发布了相关的功能安全基础标准IEC 61508及针对过程工业的功能安全应用标准IEC 61511，我国已将其转化成GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》和GB/T 21109《过程工业领域安全仪表系统的功能安全》。

《油气管道安全仪表系统的功能安全》系列标准是GB/T 20438和GB/T 21109在油气管道领域的应用规范。其目的在于规范油气管道领域内安全仪表系统评估、验收等活动的技术要求、管理要求和应用原则，促进安全仪表系统在油气管道领域内应用和管理的规范化，确保油气管道系统安全可靠运行。

本标准的目的在于指导和规范油气管道领域安全仪表系统的功能安全评估活动。

油气管道安全仪表系统的功能安全评估规范

1 范围

本标准规定了油气管道安全仪表系统的功能安全评估人员和组织资质要求、评估活动的管理和职责、执行功能安全评估活动的周期和阶段、各阶段评估活动的范围、流程、依据以及文档要求。

本标准适用于新建及改扩建的陆上石油天然气长输管道输送、储存系统中安全仪表系统的功能安全评估。

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 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

3 缩略语、术语和定义

3.1 缩略语

下列缩略语适用于本文件(见表1)。

表1 缩略语

缩略语	全称	解释
BPCS	basic process control system	基本过程控制系统
DC	diagnostic coverage	诊断覆盖率
EUC	equipment under control	受控设备
E/E/PE	electrical/electronic/programmable electronic	电气/电子/可编程电子
FAT	factory acceptance testing	工厂验收测试
HAZOP	hazard and operability studies	危险与可操作性分析
HFT	hardware fault tolerance	硬件故障裕度
MTTR	mean time to restoration	平均恢复时间
MOC	management of change	变更管理
PE	programmable electronic	可编程电子
PFD	probability of dangerous failure on demand	要求时的失效概率
PFH	probability of a dangerous failure per hour	每小时危险失效概率
P&ID	pipe and instrument diagram	管道及仪表流程图
SAT	site acceptance test	现场验收测试
SFF	safe failure faction	安全失效分数

表 1（续）

缩略语	全称	解释
SIF	safety instrumented function	安全仪表功能
SIL	safety integrity level	安全完整性等级
SIS	safety instrumented system	安全仪表系统
SRS	safety requirement specification	安全要求规格书
TI	test interval	检验测试时间间隔

3.2 术语和定义

下列术语和定义适用于本文件。

3.2.1

危险失效 dangerous failure

对执行安全功能有影响的组件和/或子系统和/或系统的失效，其：

a) 在要求时阻止安全功能的执行（要求模式），或导致安全功能失效（连续模式）以致 EUC 进入危险或潜在危险的状态。

b) 降低在要求时安全功能正确执行的概率。

[IEC 61508-4:2010，定义 3.6.7]

3.2.2

安全失效 safe failure

对于执行安全功能有影响的组件和/或子系统和/或系统的失效，其：

a) 导致安全功能的误动作从而使 EUC（或其一部分）进入或保持安全状态；或

b) 增加安全功能的误动作从而使 EUC（或其一部分）进入或保持安全状态的概率。

[IEC 61508-4:2010，定义 3.6.8]

3.2.3

诊断覆盖率 diagnostic coverage；DC

通过自动在线诊断测试检测到的危险失效分数。危险失效分数是由检测到的危险失效率除以总危险失效率计算出的。

注 1：危险失效诊断覆盖率按下式计算：

$$DC = \Sigma\lambda_{DD} / \Sigma\lambda_{Dtotal}$$

式中：

DC ——诊断覆盖率；

λ_{DD} ——检测到的危险失效率；

λ_{Dtotal} ——总的危险失效率。

注 2：该定义仅在单个元件失效率为常数时适用。

[IEC 61508-4:2010，定义 3.8.6]

3.2.4

故障裕度 fault tolerance

在出现故障或误差的情况下，功能单元继续执行要求功能的能力。

[GB/T 21109.1—2007，定义 3.2.23]

3.2.5

硬件故障裕度 hardware fault tolerance

一个部件或子系统在有一个或几个硬件危险故障的情况下，仍能继续承担所要求的安全仪表功能

的能力。

注：如硬件故障裕度为1，意味着有两台设备，且其结构会使得两个部件或子系统的任何一个的危险失效都不能阻止安全动作发生。

3.2.6

功能安全 functional safety

与过程和BPCS有关的整体安全的组成部分，它取决于SIS和其他保护层的正确功能执行。

[GB/T 21109.1—2007，定义3.2.25]

3.2.7

功能安全评估 functional safety assessment

基于证据的调查，以判定由一个或多个保护层所实现的功能安全。

[GB/T 21109.1—2007，定义3.2.26]

3.2.8

硬件安全完整性 hardware safety integrity

安全相关系统安全完整性中，与危险失效模式下的随机硬件失效有关的部分。

注：本术语涉及在危险模式下的失效，即，将削弱其安全完整性的安全相关系统的这类失效。与本术语有关的两个参数是危险失效平均频率和在要求时动作失效的概率。当为保持安全而必须保持连续控制时，使用前一可靠性参数，在安全相关保护系统场合中使用后一可靠性参数。

[IEC 61508-4:2010，定义3.5.7]

3.2.9

检验测试 proof test

周期性测试，用以检测安全相关系统中危险的隐性失效，在必要时通过维修，把系统复原到“新的”状态或实际上接近这种状态。

注1：在本标准中使用“检验测试”，但要注意到同义的术语“周期性测试”。

注2：检验测试的有效性取决于失效覆盖和维修的有效性。在实践中除了低复杂E/E/PE安全相关系统外，100%的隐性失效的检测很难达到。这应该是目标。至少，所有要执行的安全功能应按E/E/PE安全相关系统安全要求规格书进行检查。如果使用分离通道，则对每个通道分别进行检验测试。对于复杂的组件，进行分析，以证明在E/E/PE安全相关系统整体生命周期期间，未被检验测试检测出的隐性危险失效概率可忽略不计。

注3：检验测试需要一定时间完成。在此时间内E/E/PE安全相关系统可能被部分或全部限制。在测试过程中，仅当EUC已停机或E/E/PE安全相关系统仍能保持在要求时的动作能力，检验测试持续时间可忽略不计。

注4：在检验测试期间，E/E/PE安全相关系统可能部分或全部不能响应动作要求。仅在维修时EUC已停机或使用其他等效的风险措施来代替时，MTTR对于SIL的计算可以忽略。

[IEC 61508-4:2010，定义3.8.5]

3.2.10

保护层 protection layer

借助控制、预防或减轻以降低风险的任何独立机制。

注：它可能是装危险化学物品的压力容器的容量这样的一个过程工程机制，也可能是一个安全阀这样的机械工程机制，或者一个安全仪表系统，或者是应对紧急危险的一个应急计划这样的管理规程。可以自动启动或手动启动这些响应机制。

[GB/T 21109.1—2007，定义3.2.59]

3.2.11

以往使用 prior use

部件和子系统之前在类似应用和实际环境中的使用(见GB/T 21109.1—2007的11.5中的“以往使用”)。

3.2.12

经使用验证的　proven-in-use

评估文档记录有适当证据表明：基于部件以往使用的情况，该部件适用于安全仪表系统时（见GB/T 21109.1—2007 的 11.5 中的“以往使用”）。

3.2.13

随机硬件失效　random hardware failure

在硬件中，由一种或几种可能的退化机理而产生的，在随机时间出现的失效。

注 1：在各种元件中，存在以不同速率发生的许多退化机理，在这些元件工作不同的时间之后，这些机理可使制造公差引起元件发生故障，从而使包含许多元件的设备将以可预见的速率，但在不可预见的时间（即随机时间）发生失效。

注 2：随机硬件失效和系统性失效（见 IEC 61508-4：2010 的 3.6.6）的主要区别是由随机硬件失效导致的系统失效率（或其他合适的度量）可以用合理的精度来量化，但系统性失效无法精确预计，因此系统性失效引起的系统失效率则不能精确地用统计法量化。也就是说，由随机硬件失效引起的系统失效率可以用合理的精度来量化，但是由系统性失效引起的系统失效率不能精确地用统计法量化，因为导致系统性失效的这些事件无法简单预测。

[IEC 61508-4：2010，定义 3.6.5]

3.2.14

冗余　redundancy

对于执行一个要求的功能或对于表示信息而言，存在多于一种的方法。

[基于 IEC 62059-11]

示例：功能元件加倍和增加奇偶校验位都是冗余的例子。

注 1：冗余主要用于提高可靠性（在给定时间范围内功能正确的概率）或可用性（在特定时间点具有功能的概率）。也可通过像 2oo3 这样的架构来使误动作最小化。

注 2：此定义在 IEV191-15-01 中不完整。

注 3：冗余可能是“活动的（hot or active）”（所有冗余项同时运行）、“待机的（cold or stand-by）”（在同一时间只有一个冗余项运行）、“混合的（mixed）”（在同一时间一个或几个项运行和一个或几个项待机）。

[IEC 61508-4：2010，定义 3.4.6]

3.2.15

风险　risk

出现伤害的概率及该伤害严重性的组合。

[GB/T 21109.1—2007，定义 3.2.64]

3.2.16

安全失效分数　safe failure fraction；SFF

导致安全失效或者可检测出的危险失效的装置总硬件随机失效率分数。

$$SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{DD}}{\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU}} \quad \cdots\cdots(1)$$

式中：

λ_S ——安全失效率；

λ_{DD} ——可以被诊断测试检测到的危险失效率；

λ_{DU} ——不能被诊断测试检测到的危险失效率。

3.2.17

安全状态　safe state

达到安全时的过程状态。

[GB/T 21109.1—2007，定义 3.2.66]

3.2.18

安全功能　safety function

针对特定的危险事件，为达到或保持过程的安全状态，由 SIS、其他技术安全相关系统或外部风险降低设施实现的功能。

[GB/T 21109.1—2007，定义 3.2.68]

3.2.19

安全仪表功能　safety instrumented function；SIF

具有某个特定 SIL 的，用以达到功能安全的安全功能，它既可以是一个安全仪表保护功能，也可以是一个安全仪表控制功能。

注：该术语与 GB/T 21109—2007 不同，以体现行业应用习惯。

3.2.20

安全仪表系统　safety instrumented system；SIS

用来实现一个或几个安全仪表功能的仪表系统。SIS 可以由传感器、逻辑控制器和执行器的任何组合组成。

[GB/T 21109.1—2007，定义 3.2.72]

3.2.21

子系统　subsystem

安全相关系统顶层架构设计的实体，子系统的危险失效导致安全功能的危险失效。此处的危险失效见 3.2.1a)。

3.2.22

系统　system

根据设计相互联系的一组元素；系统的一个元素可以是称为子系统的另一系统，该子系统可以是一个主控系统，也可以是一个受控系统，它可能包含硬件、软件和人的交互作用。

注 1：人可以是系统的一部分。

注 2：系统包括传感器、逻辑控制器、最终元件、通信和附属于 SIS 的辅助设备（如：电缆、管道系统和电源）。

[GB/T 21109.1—2007，定义 3.2.84]

3.2.23

低要求模式　low demand mode

仅当要求时才执行将 EUC 导入规定安全状态的安全功能，并且要求的频率不大于每年一次。

注：E/E/PE 安全相关系统只在要求时才对 EUC 或 EUC 控制系统产生影响。如果 E/E/PE 安全相关系统不能执行安全功能，则可能使 EUC 进入安全状态。

3.2.24

高要求模式　high demand mode

将 EUC 导入规定安全状态的安全功能仅当要求时才执行，并且要求的频率大于每年一次。

3.2.25

连续模式　continuous mode

安全功能将 EUC 保持在安全状态是正常运行的一部分。

3.2.26

安全完整性　safety integrity

安全仪表系统在规定时段内、在所有规定条件下满足执行要求的安全仪表功能的平均概率。

[GB/T 21109.1—2007，定义 3.2.73]

3.2.27

安全完整性等级　safety integrity level；SIL

用来规定分配给安全仪表系统的安全仪表功能的安全完整性要求的离散等级（4 个等级中的一

个)。SIL 4 是安全完整性的最高等级,SIL 1 为最低等级。

[GB/T 21109.1—2007,定义 3.2.74]

3.2.28

安全生命周期 safety life cycle

从项目概念阶段开始到所有的安全仪表功能不再适用时为止所发生的、包含在安全仪表功能实现中的必要活动。

[GB/T 21109.1—2007,定义 3.2.76]

3.2.29

安全要求规格书 safety requirements specification

包含安全仪表系统应执行的安全仪表功能的所有要求的规格书。

注:该术语与 GB/T 21109.1—2007 不同,以体现行业应用习惯。

4 与本标准的符合性

为了声明符合本标准各评估节点要求,应满足第 5 章~第 9 章中列出的相应要求,从而达到了各章的目的。

5 一般要求

5.1 目的

确定开展功能安全评估的阶段以及一般要求。

5.2 要求

5.2.1 开展功能安全评估的阶段

5.2.1.1 功能安全评估应贯穿于整个安全生命周期。根据 GB/T 21109,以及油气管道安全仪表系统安全生命周期活动(见图 1),应在以下节点执行功能安全评估活动:

——节点 1:SIS 安全要求评估。应在已执行危险和风险评估、已确定要求的保护层和已制定安全要求规格书之后,即油气管道安全仪表系统安全生命周期活动 1~4 完成之后进行,见第 6 章;

——节点 2:SIS 设计评估。应在安全仪表系统设计完成之后,即油气管道安全仪表系统安全生命周期活动 5 完成之后进行,见第 7 章;

——节点 3:SIS 投产前评估。应在完成安全仪表系统集成、现场施工、人员培训、工厂验收测试(FAT)、安装、调试、现场验收测试(SAT),以及制定好操作和维护规程之后,即油气管道安全仪表系统安全生命周期活动 6~11 完成之后进行,见第 8 章;

——节点 4:功能安全复审。应在取得操作和维护经验之后,或者在对安全仪表系统进行修改之后和退役之前,即油气管道安全仪表系统安全生命周期活动 14~15 完成之后或活动 17 之前进行,见第 9 章。

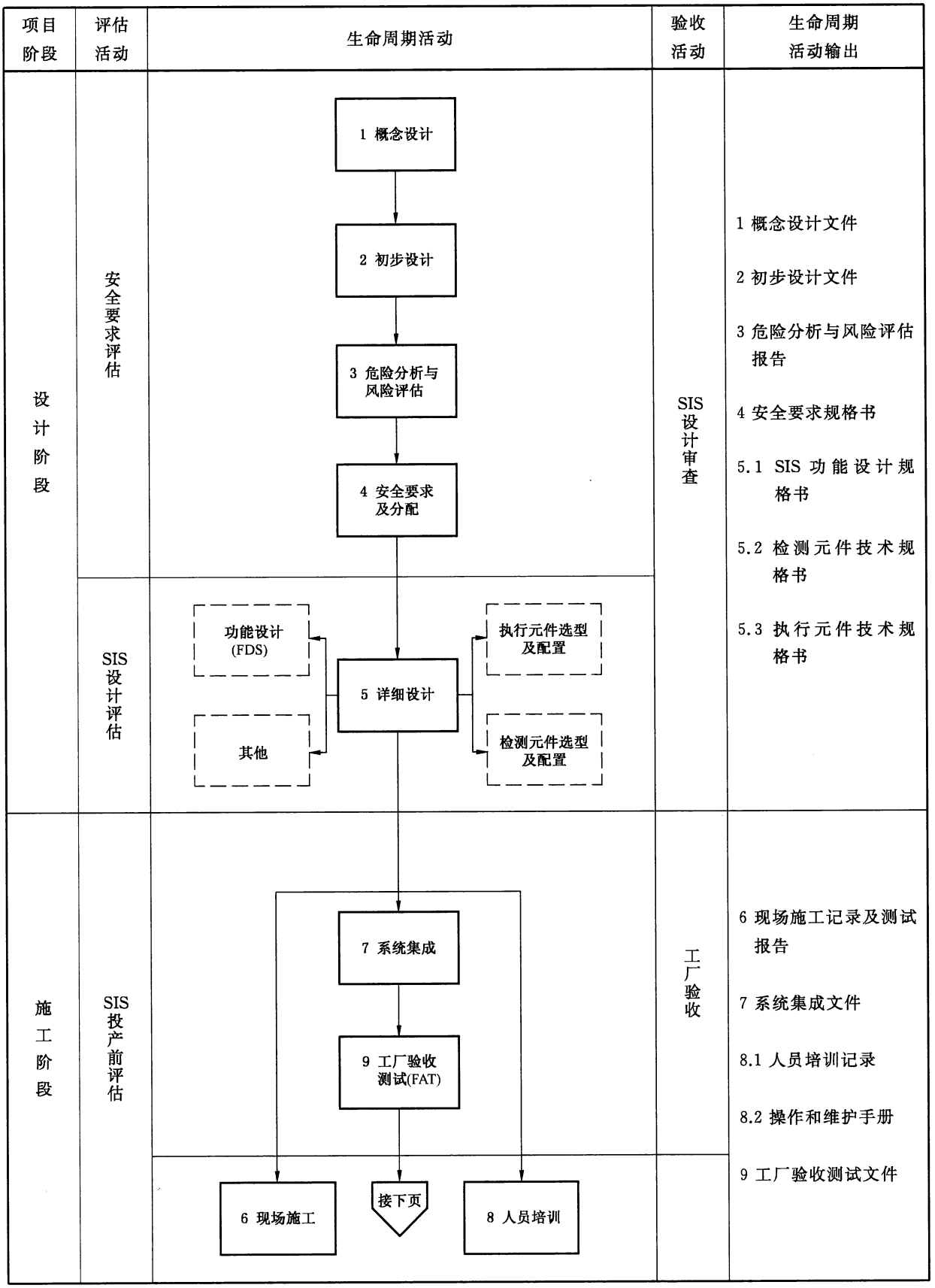

图 1　油气管道安全仪表系统功能安全评估节点图

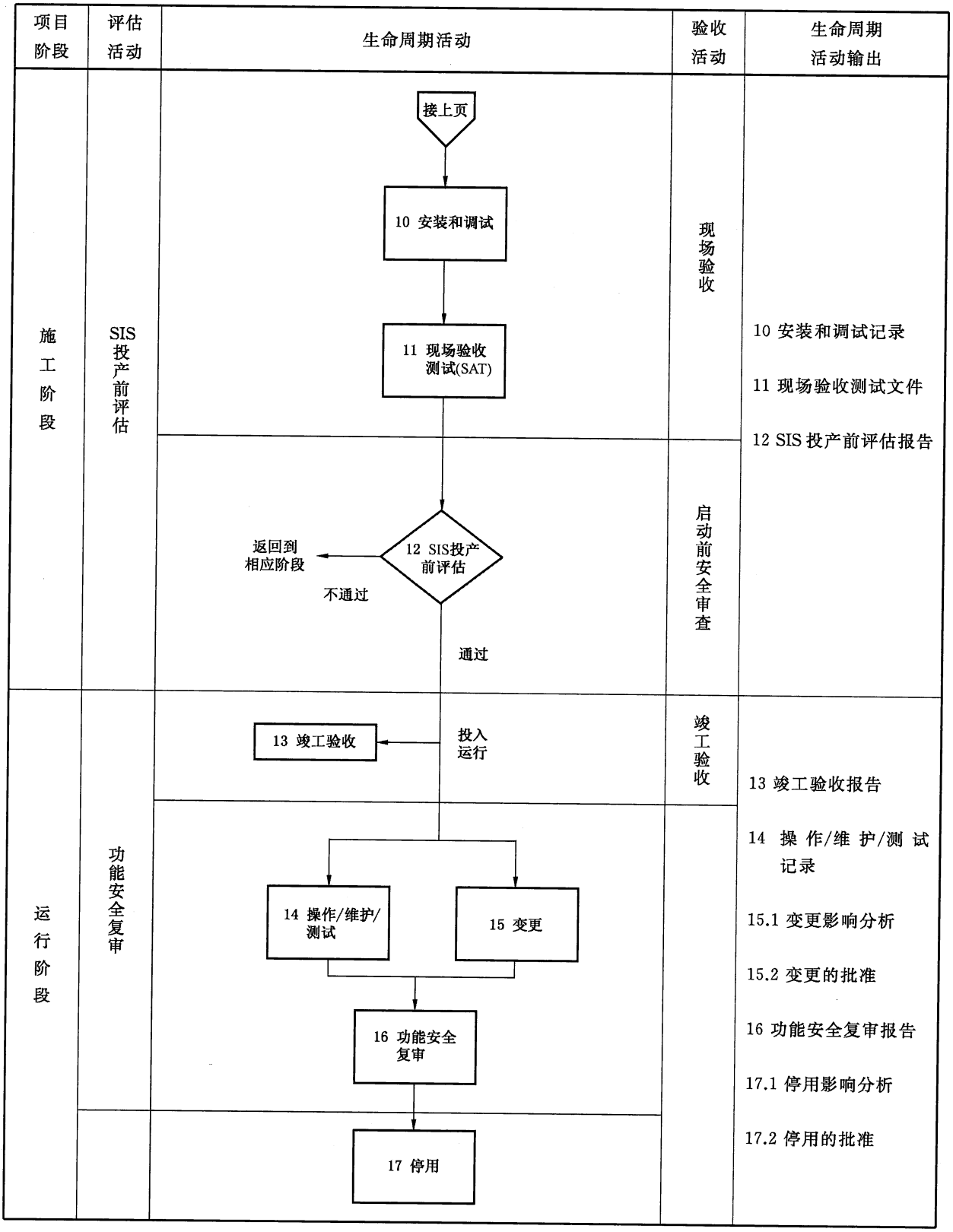
项目阶段
评估活动
生命周期活动
验收活动
生命周期活动输出
施工阶段
SIS投产前评估
接上页
10 安装和调试
11 现场验收测试(SAT)
现场验收
10 安装和调试记录
11 现场验收测试文件
12 SIS投产前评估报告
12 SIS投产前评估
返回到相应阶段
不通过
通过
启动前安全审查
运行阶段
功能安全复审
13 竣工验收
投入运行
竣工验收
13 竣工验收报告
14 操作/维护/测试
15 变更
16 功能安全复审
17 停用
14 操作/维护/测试记录
15.1 变更影响分析
15.2 变更的批准
16 功能安全复审报告
17.1 停用影响分析
17.2 停用的批准

图 1（续）

5.2.1.2 在设计阶段应完成SIS安全要求评估和SIS设计评估。

5.2.1.3 在安全仪表系统投入运行前应完成SIS投产前评估。

5.2.1.4 对于已开展过功能安全评估的同类型站场可参考采用评估结论，但应做差异分析，并对差异部分进行评估。

5.2.1.5 对于改、扩建项目应按照安全生命周期各节点执行功能安全评估活动，对于简单变更参照第9章功能安全复审要求执行。

5.2.2 人员要求

5.2.2.1 功能安全评估组成员应是独立的，独立性水平应满足GB/T 20438的要求，项目设计的人员或项目组其他相关人员应该配合评估组参与评估活动。

5.2.2.2 评估组成员应了解功能安全基础标准GB/T 20438和过程工业领域的应用标准GB/T 21109，并经过培训和考核，取得相应证书。

5.2.2.3 评估组成员应具备石油天然气管道工程相关经验及相关法律法规知识，以确保评估结果的合理可信。

5.2.2.4 评估组内高级资质人员人数不应少于总数的三分之一。

注：评估组只需要满足5.2.2.1要求，并包括了分别满足5.2.2.2、5.2.2.3、5.2.2.4要求的人员，即可声明符合5.2.2，而不需要评估组每一成员都同时满足5.2.2.2、5.2.2.3、5.2.2.4要求。

5.2.2.5 对压气站、储气库、输油首站、储油库、输油泵站、输油热站等工艺系统相对复杂的站场，其安全仪表系统开展功能安全评估的高级资质人员人数应不少于总数的三分之二。

5.2.3 机构要求

应由具有资质的机构在其资质证书认可的业务范围内从事功能安全评估活动。

5.2.4 功能安全评估管理

5.2.4.1 评估组织方应成立评估组，并明确各成员的职责和独立性要求。

5.2.4.2 执行功能安全评估活动的人员或机构应满足5.2.2、5.2.3的要求。

5.2.4.3 评估组应编制功能安全评估计划，计划应包括：

——需要执行功能安全评估活动的生命周期阶段，即功能安全评估的范围；

——在各阶段要求执行的活动；

——参与评估活动的人员、部门、组织或其他单位；

——为完成功能安全评估活动需要的所有资源；

——完成功能安全评估活动应得到的输出。

5.2.4.4 在整个安全生命周期当中，功能安全评估计划应不断地更新和维护。任何的设备或系统变更都可能需要附加的功能安全评估活动，以确定是否会产生新的危险。

5.2.4.5 在进行功能安全评估之前，功能安全评估计划应得到评估组织方的同意。

5.2.4.6 评估组应根据功能安全评估计划进行功能安全评估管理和开展功能安全评估活动。

5.2.4.7 评估组织方应向评估组提供安全仪表系统的所有相关信息，包括先前执行的功能安全评估的结果、通过该评估提出的建议以及相应的整改报告。

5.2.4.8 所有的功能安全评估活动都应实现文档化。

5.2.4.9 评估结束后，评估组应提供评估报告，评估组织方应对此报告进行审查。

5.2.4.10 评估组织方应对评估建议的实现进程进行跟踪。在建议的问题解决后，应进行确认。

5.2.4.11 评估结果仅对评估期间的SIS现状有效，一旦SIS作出任何变更，则先前的评估结果不再有效，但可作为下次功能安全评估活动的参考。

5.2.4.12 用于SIS开发、安装、调试、测试、维护的设备工具、材料的性能和质量，应符合相应的SIS功能安全要求。

6 SIS安全要求评估

6.1 目的

审查并判断安全仪表系统的安全要求规格书的制定、安全功能的提出以及安全完整性等级的确定过程是否达到功能安全。

6.2 评估依据

6.2.1 应采用与实际最符合的评估依据。

6.2.2 评估的基础依据包括：危险分析与风险评估报告、安全要求分配报告、安全要求规格书。必要情况下，还应包括以上各活动的相关程序文档，以及分析报告中记录的分析和引用资料。

注1：有些时候，这些报告的名字并不固定如上，且文件形式也并不单一。如：采用HAZOP分析方法开展危险分析与风险评估，则该报告可为HAZOP分析报告。

注2：应考虑油气管道自身特点，如：距离远，线路长、环境复杂，要注意外部环境及自然灾害可能造成的影响。

6.2.3 为了实施SIS安全要求评估，评估组织方应提供以下资料：

——危险分析和风险评估报告；

——安全要求分配报告；

——SIS安全要求规格书。

必要时，还应提供如下资料：

——工艺流程图；

——P&ID图；

——因果图；

——总平面布置图；

——设计说明书；

——操作原理；

——危险事件分类及统计；

——风险分级；

——其他可作为危险和风险分析依据的资料；

——SIL分级；

——保护层分类及降险统计；

——人员能力分级；

——所需的安全功能清单和每个安全功能的安全完整性等级(SIL)；

——每个需要SIF的潜在危险事件及其事件链(如原因、发展和终端事件)；

——过程公共原因需要考虑的事项(如腐蚀、堵塞、涂层破损等)；

——影响SIS的管理要求。

6.3 评估内容

6.3.1 对SIS安全要求规格书进行评估

6.3.1.1 安全要求规格书应包括安全功能要求和安全完整性要求两方面的内容。安全要求规格书可以是一套文件或资料。

6.3.1.2 安全要求规格书中对于SIS要求的表述应清楚、精确、可验证、可维护和可行，且易于被在生命周期任何阶段有可能使用这些信息的人理解。

6.3.1.3 应对安全功能要求的以下内容进行评估：

——达到要求的功能安全所必需的所有安全仪表功能的描述；

——对每个已确定的事件，定义其过程安全状态；

——SIS的过程输入及其动作设定点；

——工艺变量的正常操作范围及操作界限；

——SIS的过程输出及其作用；

——过程输入输出的功能关系，包括逻辑、数学功能及所需的许可；

——励磁触发或非励磁触发的选择；

——手动关断的考虑；

——SIS失去驱动源采取的动作；

——对任何可诊断的危险故障的响应动作；

——人机界面要求；

——复位功能。

6.3.1.4 应对安全完整性要求的以下内容进行评估：

——每个安全仪表功能所需的SIL；

——达到所需的SIL的诊断要求；

——达到所需的SIL的维修和检验测试要求；

——如果误动作是不可接受的，对误动作率的要求。

6.3.2 对安全功能要求的提出过程进行评估

6.3.2.1 应开展过一次危险分析与风险评估。

6.3.2.2 开展危险分析与风险评估的过程应符合国家、行业或企业相关标准、规范要求，包括：分析评估资质、组织管理、实施流程、文档化和发布签署等。

6.3.2.3 应已评估工艺、设备、设施、人员等方面所有合理可预见的情况，包括故障状况、误用、人员误操作、异常的EUC运行模式等。

6.3.2.4 应已明确所有辨识出的合理可预见情况下，受控设备的危险和危险事件。

6.3.2.5 应已明确导致已确定的危险和危险事件发生的事件顺序。

6.3.2.6 应已评估已确定的危险事件的发生频率(或频率等级)，频率或频率等级的定义和选择应符合国家、行业或企业相关标准、规范要求，并具有可信的来源。

6.3.2.7 应已评估已确定的危险事件后果的严重性程度，后果及其严重性等级的定义和选择应符合国家、行业或企业相关标准、规范要求，并具有可信的来源。

6.3.2.8 应已评估与已确定的危险和危险事件相关的事故风险，风险分级准则应符合国家、行业或企业相关标准、规范要求。

6.3.2.9 应依据明确的风险可接受准则开展分析评估，该准则应符合国家、行业或企业相关标准、规范要求。

6.3.2.10 对提出的降低或消除危险和风险的措施，应有明确的实施和追踪的负责人。

6.3.2.11 应已详细记录6.3.2.1～6.3.2.10各项活动所分析及引用的资料的名称及版本号。

6.3.2.12 应已详细记录6.3.2.1～6.3.2.10各项活动内容，形成文档，并由相关责任人签署。

6.3.3 对安全完整性要求的提出过程进行评估

6.3.3.1 安全要求分配应在开展过一次危险与风险分析后展开。

6.3.3.2 安全要求分配应包括了安全功能要求分配和安全完整性要求分配。

6.3.3.3 开展安全要求分配的过程应符合国家、行业或企业相关标准、规范要求，包括：分析评估资质、组织管理、实施流程、文档化和发布签署等。

6.3.3.4 应明确定义用于预防、控制或减轻来自过程及其相关装置危险的保护层及其安全功能，包括由安全仪表系统执行的安全仪表功能(SIF)。

6.3.3.5 应已评估并识别各保护层之间的相关性和独立性，如 SIS 与 BPCS 之间、SIS 与其他保护层之间存在的潜在的共因失效。

6.3.3.6 应已评估并识别各保护层与触发事件或原因之间的相关性和独立性，如 SIS 与触发事件或原因之间存在的潜在的共因失效。

6.3.3.7 应已评估并记录已确定的独立保护层的风险降低能力，各保护层风险降低能力的定义和选择应符合国家、行业或企业相关标准、规范要求，并具有可信的来源。

6.3.3.8 应已分析并规范记录被定义 SIF 的安全功能要求和安全完整性要求的信息。

6.3.3.9 应已分析并规定各 SIF 最大可接受误动作率要求(如果需要)。

6.3.3.10 应已分析并识别单个或多个 SIF 动作可能带来的附加危害。

6.3.3.11 应已分析并识别各 SIF 是励磁触发还是非励磁触发，如果为励磁触发，应审查失电对安全运行的影响。

6.3.3.12 应已分析并识别各 SIF 运行可能需要的其他辅助设备或设施，如气动阀供气系统，并审查其失效对安全运行的影响。

6.3.3.13 应已详细记录 6.3.3.1～6.3.3.12 各项活动中所分析及引用的资料的名称及版本号。

6.3.3.14 应已详细记录 6.3.3.1～6.3.3.12 各项活动内容，形成文档，并由相关责任人签署。

6.4 报告要求

6.4.1 SIS 安全要求评估报告应为功能安全评估报告的一部分。

6.4.2 SIS 安全要求评估报告应结构清晰、表述准确、无歧义，并可追溯。

6.5 报告内容

6.5.1 项目背景

应包括立项意义、任务由来、项目概况等相关内容。

6.5.2 评估依据

应列出评估项目所引用的法律法规、技术规范和标准、基础技术资料名称等相关信息。

6.5.3 评估目的

应明确描述评估目的。

6.5.4 评估范围和内容

应明确描述评估的范围和内容。

6.5.5 评估方法

根据项目的特点，应明确表达采用的评估方法。

6.5.6 评估过程

应明确描述评估工作过程，包括评估程序、工作进度、参加人员等，可用图、表、文字描述等方式

表述。

6.5.7 评估结论与建议

应根据 6.3 中所述内容的评判结果，给出对站场工艺、设备等的危险与风险分析结论、安全仪表功能的完整性结论、SIS 安全要求的完整性结论等，并指出存在的问题，提出有针对性的建议。

6.5.8 附件

6.5.8.1 评估工作表

应给出评估工作过程中生成的调研表、分析记录表等。样表参见附录 A。

6.5.8.2 评估软件工具的采用

应明确评估过程中所用软件、测试等辅助工具的名称、型号、软件版本号、出品公司、功能说明以及在本项目中的使用情况。

6.5.8.3 其他资料

应给出评估工作所依据的必要资料，如分析图纸、评估准则来源、分析评估假设及来源等。

7 SIS 设计评估

7.1 目的

审查并判断安全仪表系统的设计是否符合安全要求规格书以达到功能安全。

7.2 评估依据

7.2.1 评估依据应准确、可靠。

7.2.2 应提供但不限于以下所列资料：

——安全要求规格书；

——SIS 安全要求评估报告及整改报告；

——设计说明书；

——操作原理；

——设备汇总表；

——供应商可提供的设备 SIL 认证资料或长期使用说明材料；

——设计过程中做的 SIL 评估报告。

7.3 评估内容

7.3.1 一般要求

应根据 SIS 安全要求规格书，开展本评估节点的评估。

7.3.2 SIS 执行功能评估

若同时执行安全仪表功能和非安全仪表功能时，无论正常或故障状态，任何对于安全仪表功能有不利影响的部分都应该被当作评估的一部分考虑进来，并应符合 SIF 要求的最高 SIL 要求。

7.3.3 独立性评估

应评估 SIS 相对于 BPCS 的独立性，除非特殊情况，应尽量保持充分的独立性。在非完全独立情况下，应从工艺过程特性、设备性能、操作和维护规程等方面进行深入评估。

7.3.4 可操作性评估

应评估 SIS 可操作性是否符合功能安全要求规格书要求。

7.3.5 可维修性评估

应评估 SIS 可维修性是否符合功能安全要求规格书要求。

7.3.6 可测试性评估

应评估 SIS 可测试性是否符合功能安全要求规格书要求。对于 7.3.4～7.3.6，需要在线测试和可能产生报警的系统，应考虑到旁路设施。

7.3.7 方便易用性评估

为了保证 SIL 在实施中的实现，应考虑人的能力和限制；应审查 SIS 的设计是否适合于分派给操作员和维护人员的任务。所有的人-机接口设计应遵循良好的人员操作惯例，并适合操作员可接受的培训或认知水平。

7.3.8 硬件故障裕度(HFT)评估

7.3.8.1 应对构成安全仪表功能回路的每一部分评估硬件故障裕度；通常一个安全仪表功能回路由传感器、逻辑控制器和执行器三部分组成；每一部分都应符合最低硬件故障裕度的要求。PE 逻辑控制器的最低硬件故障裕度要求见表 2，除 PE 逻辑控制器外的所有子系统(如传感器、执行器和非 PE 逻辑控制器)的最低硬件故障裕度要求见表 3。

表 2 PE 逻辑控制器的最低硬件故障裕度

SIL	最低硬件故障裕度		
	SFF＜60%	60%≤SEF≤90%	SFF＞90%
1	1	0	0
2	2	1	0
3	3	2	1
注：本规范不考虑 SIL4 的情况。			

表 3 传感器、执行器和非 PE 逻辑控制器的最低硬件故障裕度

SIL	最低硬件故障裕度
1	0
2	1
3	2

7.3.8.2 对于主导失效模式不是安全失效，且危险失效不能被诊断测试检测的传感器、执行器和非 PE 逻辑控制器，其最低硬件故障裕度应增加 1。

7.3.8.3 当使用的设备符合所有下列各项时，表 3 中规定的除 PE 逻辑控制器外所有子系统（如传感器、执行器和非 PE 逻辑控制器）的最低硬件故障裕度可减少 1：

a) 所选择的设备硬件符合以往使用的原则；应有优良使用记录；

b) 设备只允许调整过程参数；如测量范围、上限或下限失效指示；

c) 设备过程参数的调整受保护，如跳线、密码。

7.3.9 检测到故障时的系统行为的评估

7.3.9.1 硬件故障裕度大于 0 的子系统

对于硬件故障裕度大于 0 的任何子系统，应评估其检测到危险故障时（利用诊断测试、检验测试或任何其他办法）是否可导致：

a) 用以达到或保持某种安全状态的一个规定动作；

b) 在修复故障的同时继续过程的安全运行。如果故障的修复不能在计算硬件随机失效概率中假设的平均恢复时间（MTTR）内完成，则应产生一个规定的动作以达到或保持某个安全状态。

7.3.9.2 低要求运行模式下，硬件故障裕度为 0 的子系统

对于无冗余、被安全仪表功能完全依赖且仅按要求模式实现安全仪表功能的子系统，应评估其检测到危险故障时（利用诊断测试、检验测试或任何其他办法）是否可导致：

a) 用以达到或保持某个安全状态的一个规定动作；

b) 在计算硬件随机失效概率中假定的平均恢复时间（MTTR）时段内修复故障子系统。在这段时期应由附加的措施和约束保证过程持续安全。这些措施和约束提供的风险降低，应等于无任何故障时的仪表安全系统所提供的风险降低。在 SIS 操作和维护程序中应规定这些附加措施和约束。如果不能保证在规定的平均恢复时间（MTTR）内完成修复，则应执行一个规定动作以达到或保持某个安全状态。

7.3.9.3 高要求或连续运行模式下，硬件故障裕度为 0 的子系统

对于无冗余、被安全仪表功能完全依赖且按连续模式实现安全仪表功能的子系统，应评估其检测到危险故障时（利用诊断测试、检验测试或任何其他办法）是否可导致一个规定动作，以达到或保持某种安全状态。

7.3.10 SIS 组件或子系统的选择和集成的评估

7.3.10.1 对于 SIL 1～SIL 3 的应用而言，应评估是否选用了符合相应 SIL 等级要求的部件或子系统。

注：其中对于依据以往使用原则选择的部件和子系统，评估是否证明了其对于该安全仪表系统的适应性，包括以下几个方面：

——制造商对质量、管理和配置管理的考虑；

——标准/规范符合性；

——在类似操作行规和实际环境中部件或子系统的性能；

——大量的操作经验。

7.3.10.2 应评估是否选用了符合 SIS 安全要求规格书的部件或子系统。

7.3.10.3 SIL4 的应用不在本部分考虑范围之内。

7.3.11 对维护和测试的评估

7.3.11.1 应允许以点-点或分几部分对 SIS 进行测试；

7.3.11.2 对在线测试的要求如下：

——在预定的过程停机时间间隔(即通常所说的大修时间间隔)大于检验测试间隔的情况下，需要在线测试；

——若需要在线测试，应有可供在线测试的设施；

——当要求在线检验测试时，测试设施应是用来测试未检测到的失效的 SIS 设计的整个部分；

——SIS 的在线测试/旁路设施：

- 应符合安全要求规格书所定义的维护和测试要求；
- SIS 任何部分的旁路都应通过报警和/或操作规程对操作员发出警告。

7.3.12 SIF 的 PFD/PFH 的评估

7.3.12.1 在低要求运行模式下运行的安全仪表功能，应使用在要求时执行其设计功能的平均失效概率(PFD)来表示目标失效量，如表 4 所示(参见 GB/T 21109.1—2007，表 2)。应对每个 SIF 分别评估其 PFD，每个 SIF 的 PFD 应小于或等于安全要求规格书中所规定的目标失效量。

表 4 在低要求模式下，安全仪表功能的目标失效量

安全完整性等级	低要求运行模式(在要求时就执行其设计功能要求的平均失效概率)
4	$\geqslant 10^{-5}$ 至 $<10^{-4}$
3	$\geqslant 10^{-4}$ 至 $<10^{-3}$
2	$\geqslant 10^{-3}$ 至 $<10^{-2}$
1	$\geqslant 10^{-2}$ 至 $<10^{-1}$

7.3.12.2 在高要求或连续运行模式下运行的安全仪表功能，应使用每小时的危险失效频率(PFH)来表示目标失效量，如表 5 所示(参见 GB/T 21109.1—2007，表 3)。应对每个 SIF 分别评估其 PFH，每个 SIF 的 PFH 应小于或等于安全要求规格书中所规定的目标失效量。

表 5 在高要求或连续模式下，安全仪表功能的目标失效量

安全完整性等级	连续运行模式(每小时危险失效频率)
4	$\geqslant 10^{-9}$ 至 $<10^{-8}$
3	$\geqslant 10^{-8}$ 至 $<10^{-7}$
2	$\geqslant 10^{-7}$ 至 $<10^{-6}$
1	$\geqslant 10^{-6}$ 至 $<10^{-5}$

7.3.12.3 应对用于计算 SIF 硬件失效概率的资料和数据进行评估：

——SIS 的结构；

——各部分的表决结构；

——各部件或子系统的失效率数据；

——检验测试时间间隔 TI；

——平均恢复时间 MTTR；

——共因失效因子 β。

7.3.13 其他相关内容的评估

7.3.13.1 应审查SIS是否能把过程置于某个安全状态，并可以保持在安全状态直到启动一次复位为止；若安全要求规格书有特殊规定的情况，则依照安全要求规格书进行评估。

7.3.13.2 应评估是否有与逻辑控制器无关的手动机制（如应急停机按钮），用于直接启动SIS最终元件。

7.3.13.3 对于失去驱动源（如电源、空气、液压或气压源）而不进入安全状态的SIS设备，驱动源和SIS线路完整性的丧失应能检测和报警（如线路终端监视、驱动源供给压力测量、液压或气压压力监测）并按照GB/T 21109.1—2007中11.3采取动作。

注1：可通过使用辅助供给来提高驱动源完整性（如备用电池、不间断电源、储气罐、液压蓄能器、第二气源）。

注2：驱动源的丧失可能会影响多个SIF甚至多个SIS。因此应考虑多个SIF间的共因失效。

7.4 报告要求

7.4.1 SIS设计评估报告应为功能安全评估报告的一部分。

7.4.2 SIS设计评估报告应结构清晰、表述准确、无歧义，并可追溯。

7.5 报告内容

7.5.1 项目背景

应包括立项意义、任务由来、项目概况等相关内容。

7.5.2 评估依据

应列出评估项目所引用的法律法规、技术规范和标准、基础技术资料名称等相关信息。

7.5.3 评估目的

应明确描述评估目的。

7.5.4 评估范围和内容

应明确描述评估的范围和内容。

7.5.5 评估方法

根据项目的特点，应明确表达采用的评估方法。

7.5.6 评估过程

应明确描述评估工作过程，包括评估程序、工作进度、参加人员等，可用图、表、文字描述等方式表述。

7.5.7 评估结论与建议

应根据7.3中所述内容的评判结果，给出对SIS安全设计和实现的完整性结论，包括系统性完整性、软件完整性和硬件完整性；指出存在的问题，并以简洁、概括的语言给出有针对性的建议。

7.5.8 附件

7.5.8.1 评估工作表

应给出评估工作过程中生成的调研表、分析记录表等。样表参见附录B。

7.5.8.2 评估软件工具的采用

应明确评估过程中所用软件、测试等辅助工具的名称、型号、软件版本号、出品公司、功能说明以及在本项目中的使用情况。

7.5.8.3 其他资料

应给出评估工作所依据的必要资料，如分析图纸、评估准则来源、分析评估假设及来源等。

8 SIS运行前评估

8.1 目的

在投运前对SIS的最后审查，以判断SIS在设备设施、操作程序、培训等方面的所有相关内容是否完整并充分，是否具备安全投运条件。

8.2 一般要求

8.2.1 在投运前应开展一次SIS运行前评估。

8.2.2 开展SIS运行前评估的过程应符合国家、行业或企业相关标准、规范要求，包括：分析评估资质、组织管理、实施流程、文档化和发布签署等。

8.2.3 应对实施SIS运行前评估的人员进行培训，以确保其理解并熟识自身职责范围内的审查内容、流程、依据、准则等知识。

8.2.4 SIS运行前评估可采用简单审查和详细审查两种方式。对于新建、扩建及大范围改建项目，宜采用详细审查；对于小范围改建项目，宜采用简单审查。

注：简单审查是指仅针对变更部分进行8.4中所列内容的审查；详细审查是指针对整个SIS进行8.4中所列所有内容的审查。

8.2.5 应组织一个小组开展SIS运行前评估活动。当评估项目较小或采用简单审查时，宜组织一个1人～2人的工作小组；当评估项目较复杂或采用详细审查时，宜组织一个大的工作组分工审查。

8.2.6 如果需要，可召开会议解决评估过程中的问题。

8.2.7 应在SIS运行前评估通过以后，组织投运。

8.2.8 应记录所有的SIS运行前评估活动，形成文档，并由相关责任人签署。

8.3 评估依据

8.3.1 不同的企业不同的项目应依据各自情况，制定符合国家、行业相关标准基本要求同时满足企业自身情况需求的运行前评估计划，并应据此开展评估准备和执行评估。

8.3.2 对于简单审查，如简单的变更，应依据如下资料：

——变更工作单；

——变更说明；

——变更影响分析报告；

——相应的程序控制文件。

8.3.3 对于详细审查，则应提供满足8.4所列所有项审查的相关资料。主要有：

——设计文件；

——厂家设备相关技术文件；

——变更文件(若有)；

——设计审查阶段的生成文件；

——操作维护文件。

8.4 评估内容

8.4.1 在已确定的危险出现之前(即投产运行前),评估组应核实:

——执行过一次 SIS 安全要求评估;

——执行过一次 SIS 设计评估;

——正确执行项目设计变更规程;

——已解决由先前的功能安全评估提出的建议;

——根据设计构造和安装安全仪表系统,已确认和解决任何差异;

——与安全仪表系统有关的安全、操作、维护和紧急规程都已到位;

——安全仪表系统确认计划编制是合适的并已完成确认活动;

——人员培训已完成,有关安全仪表系统的相应信息已提供给维护和操作人员;

——实现 SIS 运行前评估的计划或策略已经就位。

8.4.2 针对硬件,评估组应审查:

——硬件是否有满足 SRS 要求的安全完整性等级的证明文件;

——硬件运行条件是否满足 SIS 物理运行环境的要求:

- 温度范围;
- 湿度范围;
- 振动和冲击;
- 污染气体;
- 粉尘;

——是否采取了保护 SIS 环境抗电磁干扰的预防措施,考虑以下方面:

- SIS 的内在设计;
- 实际安装(例如,把电源和信号电缆分离);
- 保护所有的输入和输出,避免输入电缆感应所产生的电压峰值的损害;
- EMC 测试规程;

——是否定义了关于设备之间的通讯协议;

——SIS 界面在数据显示、报警等方面是否进行了定义;

——SIS 界面是否独立于 BPCS 界面。如果不独立,当 BPCS 有变更时,是否有措施可以避免不期望的 SIS 逻辑变更。

8.4.3 针对安装,评估组应审查:

——是否有关于材料、工作质量、检验和测试的说明和规程;

——是否有监督以确保安装期间能够按照说明和规程正确执行;

——是否有预期的安装条件,当安装环境不满足预期条件时,是否有足够的防护措施;

——安装活动是否与其他工程活动有交叉,如果有是否有足够的防护措施来保证安装的质量;

——安装人员与监督人员是否有充分的独立性;

——是否保存了必要的检验记录;

——安装和检验规程在细节上是否足够清楚,以便使安装人员不用自己作出重要决策和解释;

——是否遵守了设计的保护、隔离和其他特殊要求;

——对于设计的变更是否有相关规程和说明。

8.4.4 针对安全功能确认,评估组应审查:

——是否有关于每个 SIF 确认的相关说明或规程;

——在安全功能确认的测试期间,是否有监督以确保说明和规程的实施;

——是否有相关规程可用于对 SRS 中所定义的 SIF 进行功能测试；
——测试规程在细节上是否足够清楚，以便参与功能测试的相关人员不用自己作出重要方面的决策或解释；
——测试记录是否保存；
——测试是否涵盖了 SRS 中所定义的 SIF；
——如果开展在线功能测试，规程是否能确保该测试的安全实施；
——测试实施和相关参与人员是否进行了适合于他们的培训。

8.4.5 针对应用程序确认，评估组应审查：
——是否有关于应用程序测试的相关标准和规程；
——是否有监督以确保标准和规程的实施；
——关于说明、设计方面存在的缺陷或在应用程序期间发现的缺陷，是否有制定或修正规程；
——对 SRS 的偏差，是否有备案文件证明；
——关于 SRS 的更改是否经过变更管理审核；
——应用程序的测试是否由负责说明、设计和开发的相关人员参与和审核；
——是否对最终测试文档进行审核，以确保所有的 SRS 要求都已经过测试且符合设计。

8.4.6 针对操作运行，评估组应审查：
——是否针对防止越权访问系统制定了合适的规程；
——操作说明和规程是否有文档记录；
——是否有合格的用户/操作手册；
——用户/操作手册中是否描述了可能的失效相关的风险以及针对失效的必要措施；
——执行操作任务的人员和所涉及的相关人员是否接受了相关的培训；
——是否有管理规程，以确保操作规程充分贯穿整个 SIS 使用过程；
——对于设计中给出的假设条件，在操作和维护规程中是否有说明。

8.5 报告要求

8.5.1 SIS 运行前评估报告应为功能安全评估报告的一部分。

8.5.2 SIS 运行前评估报告应结构清晰、表述准确、无歧义，并可追溯。

8.6 报告内容

8.6.1 项目背景

应包括立项意义、任务由来、项目概况等相关内容。

8.6.2 评估依据

应列出评估项目所引用的法律法规、技术规范和标准、基础技术资料名称等相关信息。

8.6.3 评估目的

应明确描述评估目的。

8.6.4 评估范围和内容

应明确描述评估的范围和内容。

8.6.5 评估方法

根据项目的特点，应明确表达采用的评估方法。

8.6.6 评估过程

应明确描述评估工作过程，包括评估程序、工作进度、参加人员等，可用图、表、文字描述等方式表述。

8.6.7 评估结论与建议

应根据 8.4 中所述内容的评判结果，给出对 SIS 生命周期中硬件实现、应用程序编程实现、安装/调试/功能测试活动、操作维护活动等的完整性结论等；指出存在的问题，并以简洁、概括的语言给出有针对性的建议。

8.6.8 附件

8.6.8.1 评估工作表

应给出评估工作过程中生成的调研表、分析记录表等。样表参见附录 C。

8.6.8.2 评估软件工具的采用

应明确评估过程中所用软件、测试等辅助工具的名称、型号、软件版本号、出品公司、功能说明以及在本项目中的使用情况。

8.6.8.3 其他资料

应给出评估工作所依据的必要资料，如分析图纸、评估准则来源、分析评估假设及来源等。

9 功能安全复审

9.1 目的

针对下列活动发生时，评估 SIS 是否仍然持续地满足功能安全的设计要求：

——安全仪表系统修改或退役；

——可能对安全仪表系统产生影响的工艺、设备等的修改；

——同类生产设施或本生产设施出现重大意外事故，需要对 SIS 的设计和运行维护状态进行审查，确定是否存在隐患；

——国家或行业有新的规定或标准规范发布，要求对在役 SIS 进行安全审查；

——为了避免因设备老化、人员变动等因素对 SIS 安全运行造成不利影响，需要对 SIS 运行和相关联的项目进行周期性复审。

9.2 评估节点

应制定复审管理规则，定期对 SIS 的运行和维护状况进行全面和系统性的评审，确保 SIS 的功能安全水平持续符合设计要求：

a) 安全仪表系统修改或退役实施前，应开展复审；

b) 可能对安全仪表系统产生影响的工艺、设备等的修改实施前，应开展复审；

c) 如果出现与功能安全管理体系有关的严重安全事故或发现明显的 SIS 设计缺陷，可即时安排复审活动；

d) 国家或行业有新的规定或标准规范发布，并有审查要求时，应开展复审；

e) 工艺/安全仪表系统每运行 3 年～5 年之后应进行周期性复审。

9.3 复审依据

应提供但不限于以下所列材料：

——SIS 变更文件或变更资料；

——工艺、设备变更文件或变更资料；

——事故调查报告；

——以往的功能安全评估报告、复审报告等。

9.4 复审内容

9.4.1 复审应对下面的项目进行审查评判：

a) SIS 的设计，以及运行和维护状况是否符合国家和行业的最新标准和规范要求；

b) SIS 的操作规程、维护规程、备品备件管理，以及文档管理等规定是否遵循和执行；

c) SIS 的安全功能回路设计、仪表选型等是否满足必要的风险降低要求；

d) 基于实际的 SIS 运行和维护状况，对 SIF 的 SIL 评估计算所依据的要求率、失效率，以及检验测试时间间隔等评估基础进行必要的更新和修订；

e) SIS 的操作和维护人员，是否具备相应的专业能力；

f) SIS 的修改变更是否遵循了相关的变更管理规定，是否针对影响的范围和深度进行了评估，以及采取了必要的应对措施；

g) 对以往功能安全评估内容进行复核。

9.4.2 复审可采取现场调研、走访、审查以及讨论等形式，必要时应进行实际的功能测试。

9.5 报告要求

9.5.1 功能安全复审报告应为功能安全评估报告的一部分。

9.5.2 功能安全复审报告应结构清晰、表述准确、无歧义，并可追溯。

9.6 报告内容

9.6.1 项目背景

应包括立项意义、任务由来、项目概况等相关内容。

9.6.2 评估依据

应列出评估项目所引用的法律法规、技术规范和标准、基础技术资料名称等相关信息。

9.6.3 评估目的

应明确描述评估目的。

9.6.4 评估范围和内容

应明确描述评估的范围和内容。

9.6.5 评估方法

根据项目的特点，应明确表达采用的评估方法。

9.6.6 评估过程

应明确描述评估工作过程，包括评估程序、工作进度、参加人员等，可用图、表、文字描述等方式

表述。

9.6.7 评估结论与建议

应根据 9.4 中所述内容的评判结果，给出对 SIS 的设计、运行、维护、修改与变更等的完整性结论等；指出存在的问题，并以简洁、概括的语言给出有针对性的建议。

9.6.8 附件

9.6.8.1 评估工作表

应给出评估工作过程中生成的调研表、分析记录表等。样表参见附录 D。

9.6.8.2 评估软件工具的采用

应明确评估过程中所用软件、测试等辅助工具的名称、型号、软件版本号、出品公司、功能说明以及在本项目中的使用情况。

9.6.8.3 其他资料

应给出评估工作所依据的必要资料，如分析图纸、评估准则来源、分析评估假设及来源等。

9.7 执行和追踪

因复审而形成的改进意见或建议措施应有专人负责实施和状态追踪。

附 录 A
（资料性附录）
SIS 安全要求评估工作表样表

SIS 安全要求评估的工作表样表见表 A.1。

表 A.1 SIS 安全要求评估工作表样表

所评估的系统/区域的说明	日期	时间
参与人员名单	传阅	
意见		

序号	评估基础依据	有/无	情况描述
1	危险分析与风险评估报告		
2	安全要求分配报告		
3	安全要求规格书		
4	其他必要资料		

SIS 安全要求规格书	□	整项不适用		
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
1 建立了 SIS 安全要求规格书	□	□	□	□	
2 SIS 安全要求规格书包含了达到要求的功能安全所必需的所有安全仪表功能	□	□	□	□	
3 每个安全仪表功能都有功能描述	□	□	□	□	
4 每个安全仪表功能都定义了过程安全状态	□	□	□	□	
5 明确了 SIS 的所有过程输入	□	□	□	□	
6 明确了每个安全仪表功能的动作设定点	□	□	□	□	
7 明确了所有工艺变量的正常操作范围和操作界限	□	□	□	□	
8 明确了 SIS 的所有过程输出及其作用	□	□	□	□	
9 明确了过程输入输出的功能关系：包括逻辑、数学功能及所需的许可	□	□	□	□	

表 A.1（续）

SIS 安全要求规格书	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
10 每个安全仪表功能都明确了其为励磁触发或非励磁触发	□	□	□	□	
11 是否包含了手动关断的考虑	□	□	□	□	
12 每个安全仪表功能都明确了失电将采取的动作	□	□	□	□	
13 每个安全仪表功能中，对于可诊断的危险故障都明确了响应动作	□	□	□	□	
14 包含了人机界面要求	□	□	□	□	
15 设置了复位功能	□	□	□	□	
16 每个安全仪表功能明确了所要达到的 SIL	□	□	□	□	
17 每个安全仪表功能明确了达到所需的 SIL 的诊断要求	□	□	□	□	
18 每个安全仪表功能明确了达到所需的 SIL 要求的维修和检验测试要求	□	□	□	□	
19 误动作风险是否可接受	□	□	□	□	
20 如果误动作风险不可接受，明确了对误动作率的要求	□	□	□	□	
危险分析与风险评估	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
21 是否开展过危险分析与风险评估	□	□	□	□	
22 在开展危险分析与风险评估前是否制定了计划	□	□	□	□	
23 是否按照计划实施了危险分析与风险评估	□	□	□	□	
24 是否由具有评估资质的人员执行危险分析与风险评估	□	□	□	□	
25 危险分析与风险评估中各项活动是否形成文档，并由相关责任人签署	□	□	□	□	
26 危险分析与风险评估过程中是否对工艺、设备、设施、人员等方面所有可预见情况进行了评估？包括故障状况、误用、人员误操作、异常的 EUC 运行模式等	□	□	□	□	
27 是否明确了 25 中所有可预见情况下受控设备的危险和危险事件	□	□	□	□	

表 A.1（续）

危险分析与风险评估	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
28 是否明确了导致危险和危险事件发生的事件顺序	□	□	□	□	
29 是否评估了已确定的危险事件的发生频率（或频率等级）	□	□	□	□	
30 频率或频率等级的定义和选择是否符合国家、行业或企业相关标准、规范要求	□	□	□	□	
31 定义的频率或频率等级是否具有可信的来源	□	□	□	□	
32 是否评估了已确定的危险事件后果的严重性程度	□	□	□	□	
33 后果及其严重性等级的定义和选择是否符合国家、行业或企业相关标准、规范要求	□	□	□	□	
34 后果及其严重性等级的定义是否具有可信的来源	□	□	□	□	
35 是否评估了与已确定的危险和危险事件相关的事故风险	□	□	□	□	
36 风险分级准则是否符合国家、行业或企业相关标准、规范要求	□	□	□	□	
37 是否是依据明确的风险可接受准则开展分析评估	□	□	□	□	
38 风险可接受准则是否符合国家、行业或企业相关标准、规范要求	□	□	□	□	
39 对提出的降低或消除危险和风险的措施，是否有明确的实施和追踪的负责人	□	□	□	□	
40 提出的降低或消除危险和风险措施是否都已实现？如果未实现是否给出了说明	□	□	□	□	
41 危险分析和风险评估过程中的各项活动所分析和引用的资料的名称及版本号是否有详细记录	□	□	□	□	
安全要求分配	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
42 是否开展过安全要求分配	□	□	□	□	
43 安全要求分配是否是在危险与风险分析后展开	□	□	□	□	
44 安全要求分配是否包括了安全功能要求分配和安全完整性要求分配	□	□	□	□	

表 A.1（续）

安全要求分配	□	整项不适用		
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
45 开展安全要求分配是否制定了计划	□	□	□	□	
46 是否按照计划实施了安全要求分配	□	□	□	□	
47 是否由具有资质的人员执行安全要求分配	□	□	□	□	
48 安全要求分配中各项活动是否均形成文档，并由相关责任人签署	□	□	□	□	
49 是否明确定义了用于预防、控制或减轻来自过程及其相关装置危险的保护层及其安全功能，包括由安全仪表系统执行的安全仪表功能(SIF)	□	□	□	□	
50 是否评估并识别了各保护层之间的相关性和独立性，如 SIS 与 BPCS 之间、SIS 与其他保护层之间存在的潜在的共因失效	□	□	□	□	
51 是否评估并识别了各保护层与触发事件或原因之间的相关性和独立性，如 SIS 与触发事件或原因之间存在的潜在的共因失效	□	□	□	□	
52 是否评估并记录了已确定的独立保护层的风险降低能力	□	□	□	□	
53 各保护层风险降低能力的定义和选择是否符合国家、行业或企业相关标准、规范要求	□	□	□	□	
54 各保护层风险降低能力的定义和选择是否具有可信来源	□	□	□	□	
55 是否分析并规范记录了被定义 SIF 的安全功能要求和安全完整性要求的信息	□	□	□	□	
56 误动作可接受吗？如果否，是否分析并规定了各 SIF 最大可接受误动作率要求	□	□	□	□	
57 是否分析并识别了各 SIF 的行为可能带来的危害(如：集中释放至火炬系统)	□	□	□	□	
58 是否分析并识别了各 SIF 是励磁触发还是非励磁触发	□	□	□	□	
59 如果为励磁触发，是否评估了失电对安全运行的影响	□	□	□	□	
60 是否分析并识别了各 SIF 运行可能需要的其他辅助设备或设施，如气动阀供气系统。是否审查其失效对安全运行的影响	□	□	□	□	
61 是否详细记录了安全要求分配过程中所分析及引用的资料的名称及版本号	□	□	□	□	

附 录 B
（资料性附录）
SIS 设计评估工作表样表

SIS 设计评估的工作表样表见表 B.1。

表 B.1 SIS 设计评估工作表样表

所评估的系统/区域的说明		日期	时间
参与人员名单		传阅：	
意见			
序号	评估基础依据	有/无	情况描述
1	安全要求规格书		
2	SIS 安全要求评估报告及整改报告		
3	设计说明书		
4	操作原理		
5	设备汇总表		
6	供应商可提供的设备 SIL 认证资料或长期使用说明材料		
7	设计过程中做的 SIL 评估报告		
8	其他必要资料		

SIS 设计评估		□	整项不适用		
		选择		需要修改项目		整改原因和要求
		是	否	必改项	待改项	
1 SIS 执行安全仪表功能外，同时还执行非安全仪表功能吗？若同时执行非安全仪表功能，设计中是否充分考虑了正常或故障状态下对安全仪表功能的影响并应符合 SIF 要求的最高 SIL 要求		□	□	□	□	

表 B.1（续）

SIS 设计评估	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
2 SIS 与 BPCS 间是否存在共用？是否保持了充分的独立性？若未能保持充分独立性，SIS 的设计是否对共用设备设置了超驰，操作和维护规程中对共用设备是否根据安全仪表功能的 SIL 要求进行规定	□	□	□	□	
3 SIS 的可操作性是否符合功能安全要求规格书	□	□	□	□	
4 SIS 的可维修性是否符合功能安全要求规格书要求	□	□	□	□	
5 SIS 的可测试性是否符合功能安全要求规格书要求	□	□	□	□	
6 系统是否需要在线测试？是否可能产生报警？若是，SIS 的设计是否考虑到了旁路设施	□	□	□	□	
7 SIS 的设计是否考虑了人的能力和限制	□	□	□	□	
8 SIS 的设计是否适合于分派给操作员和维护人员的任务	□	□	□	□	
9 人-机接口设计是否遵循了良好的人员操作惯例？是否适合操作员可接受的培训或认知水平	□	□	□	□	
10 SIS 设计中各个安全仪表功能回路的传感器是否符合本标准表 3 中的最低故障裕度要求（7.3.8.1～7.3.8.3）	□	□	□	□	
11 SIS 设计中各个安全仪表功能回路的 PE 逻辑控制器是否符合最低故障裕度要求（7.3.8.1～7.3.8.2）	□	□	□	□	
12 SIS 设计中各个安全仪表功能回路的执行器是否符合本标准表 3 中的最低故障裕度要求（7.3.8.1～7.3.8.3）	□	□	□	□	
13 对于硬件故障裕度大于 0 的子系统：					
13.1 当检测到危险故障时（利用诊断测试、检验测试或任何其他办法），是否可导致用以达到或保持某种安全状态的一个规定动作	□	□	□	□	
13.2 当检测到危险故障时，是否可在修复故障的同时继续过程的安全运行？如果故障的修复不能在计算硬件随机失效概率中假设的 MTTR 内完成，是否会产生一个规定的动作达到或保持某安全状态	□	□	□	□	
14 对于低要求运行模式下硬件故障裕度为 0 的子系统：					

表 B.1（续）

SIS 设计评估	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
14.1 当检测到危险故障时(利用诊断测试、检验测试或任何其他办法)，是否可导致用以达到或保持某个安全状态的一个规定动作	□	□	□	□	
14.2 当检测到危险故障时(利用诊断测试、检验测试或任何其他办法)，是否可在计算硬件随机失效概率中假定的 MTTR 内修复子系统	□	□	□	□	
14.3 在修复过程中，是否设置了附加的措施和约束保证过程持续安全	□	□	□	□	
14.4 如果设置了，这些措施和约束提供的风险降低，是否等于无任何故障时的仪表安全系统所提供的风险降低	□	□	□	□	
14.5 在 SIS 操作和维护程序中是否规定了这些附加措施和约束	□	□	□	□	
14.6 是否考虑到如果不能保证在规定的 MTTR 内完成修复，则应执行一个规定动作以达到或保持某个安全状态	□	□	□	□	
15 对于高要求或连续运行模式下，硬件故障裕度为 0 的子系统：					
当检测到危险故障时(利用诊断测试、检验测试或任何其他办法)是否可导致一个规定动作，以达到或保持某种安全状态	□	□	□	□	
16 是否选用了符合相应 SIL 等级要求的部件或子系统？(仅对于 SIL 1～3 而言)	□	□	□	□	
17 根据以往使用原则选择的部件和子系统，是否有以下几方面的证明： a) 制造商对质量、管理和配置管理的考虑； b) 标准/规范符合性； c) 在类似操作行规和实际环境中部件或子系统的性能； d) 大量的操作经验。	□	□	□	□	
18 SIS 设计选用的部件或子系统是否符合 SIS 安全要求规格书	□	□	□	□	
19 SIS 设计是否允许以点-点或分几部分对 SIS 进行测试	□	□	□	□	
20 是否需要在线测试(见 7.3.11)	□	□	□	□	
20.1 若需要，是否在 SIS 设计中考虑了可供在线测试的设施	□	□	□	□	

表 B.1（续）

SIS 设计评估	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
20.2 在线测试设施是否可用来测试未检测到的失效的 SIS 设计的整个部分	□	□	□	□	
20.3 SIS 的在线测试及旁路设施是否符合安全要求规格书所定义的维护和测试要求	□	□	□	□	
20.4 SIS 任何部分的旁路是否都考虑了通过报警和/或操作规程对操作员发出警告	□	□	□	□	
21 对于在低要求运行模式下运行的安全仪表功能，各个 SIF 的 PFD 是否小于或等于安全要求规格书中所规定的目标失效量	□	□	□	□	
22 对于高要求或连续运行模式下运行的安全仪表功能，各个 SIF 的 PFH 是否小于或等于安全要求规格书中所规定的目标失效量	□	□	□	□	
23 SIS 设计当前涉及的下列资料和数据计算后的 SIF 硬件失效概率是否符合 SRS 中的要求： a) SIS 的结构； b) 各部分的表决结构； c) 各部件或子系统的失效率数据分析； d) 检验测试时间间隔 TI； e) 平均恢复时间 MTTR； f) 共因失效因子 β。	□	□	□	□	
24 SIS 当前的设计是否能把过程置于某个安全状态，并可以保持在安全状态直到启动一次复位为止？是否符合安全要求规格书的有关规定	□	□	□	□	
25 SIS 设计是否有与逻辑控制器无关的手动机制（如应急停机按钮），用于直接启动 SIS 最终元件	□	□	□	□	
26 对于失去驱动源（如电源、空气、液压或气压源）而不进入安全状态的 SIS 设备，驱动源和 SIS 线路完整性的丧失是否能检测和报警（如线路终端监视、驱动源供给压力测量、液压或气压压力监测）并按照 GB/T 21109.1—2007 中 11.3 采取动作	□	□	□	□	

附 录 C
（资料性附录）
SIS 运行前评估工作表样表

SIS 运行前评估的工作表样表见表 C.1。

表 C.1 SIS 运行前评估工作表样表

<table>
<tr><td colspan="3">所评估的系统/区域的说明</td><td>日期</td><td>时间</td></tr>
<tr><td colspan="3"></td><td></td><td></td></tr>
<tr><td colspan="3">参与人员名单</td><td colspan="2">传阅：</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="5">意见</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td>序号</td><td colspan="2">评估基础依据</td><td>有/无</td><td>情况描述</td></tr>
<tr><td colspan="5">详细审查</td></tr>
<tr><td>1</td><td colspan="2">设计文件</td><td></td><td></td></tr>
<tr><td>2</td><td colspan="2">厂家设备相关技术文件</td><td></td><td></td></tr>
<tr><td>3</td><td colspan="2">变更文件(若有)</td><td></td><td></td></tr>
<tr><td>4</td><td colspan="2">设计审查阶段的生成文件</td><td></td><td></td></tr>
<tr><td>5</td><td colspan="2">操作维护文件</td><td></td><td></td></tr>
<tr><td>6</td><td colspan="2">其他必要的文件</td><td></td><td></td></tr>
<tr><td colspan="5">简单审查</td></tr>
<tr><td>1</td><td colspan="2">变更工作单</td><td></td><td></td></tr>
<tr><td>2</td><td colspan="2">变更说明</td><td></td><td></td></tr>
<tr><td>3</td><td colspan="2">变更影响分析报告</td><td></td><td></td></tr>
<tr><td>4</td><td colspan="2">相应的程序控制文件</td><td></td><td></td></tr>
<tr><td>5</td><td colspan="2">其他必要资料</td><td></td><td></td></tr>
<tr><td colspan="2">SIS 运行前评估</td><td>□</td><td colspan="2">整项不适用</td></tr>
<tr><td colspan="2"></td><td colspan="2">选择</td><td>需要修改项目</td><td>整改原因和要求</td></tr>
<tr><td colspan="2"></td><td>是</td><td>否</td><td>必改项 待改项</td><td></td></tr>
<tr><td colspan="2">1 是否执行过一次 SIS 安全要求评估</td><td>□</td><td>□</td><td>□ □</td><td></td></tr>
<tr><td colspan="2">2 是否执行过一次 SIS 设计评估</td><td>□</td><td>□</td><td>□ □</td><td></td></tr>
<tr><td colspan="2">3 是否正确地执行了项目设计变更规程</td><td>□</td><td>□</td><td>□ □</td><td></td></tr>
</table>

表 C.1（续）

SIS 运行前评估	□	整项不适用			
	选择		需要修改项目		整改原因和要求
	是	否	必改项	待改项	
4 是否已解决由先前的功能安全评估提出的建议	□	□	□	□	
5 是否根据设计构造和安装安全仪表系统，并已确认和解决任何差异	□	□	□	□	
6 与安全仪表系统有关的安全、操作、维护和紧急规程是否都已到位	□	□	□	□	
7 安全仪表系统确认计划编制是否合适？确认活动是否已完成	□	□	□	□	
8 人员培训是否已完成？有关安全仪表系统的相应信息是否已提供给维护和操作人员	□	□	□	□	
9 实现 SIS 运行前评估的计划或策略是否已经就位	□	□	□	□	
10 硬件是否有满足 SRS 要求的安全完整性等级的证明文件	□	□	□	□	
11 硬件运行条件是否满足 SIS 物理运行环境的要求（包括：温度范围、湿度范围、振动和冲击、污染气体、粉尘）	□	□	□	□	
12 是否采取了保护 SIS 环境抗电磁干扰的预防措施？（SIS 的内在设计、实际安装、保护所有的输入和输出避免输入电缆感应所产生的电压峰值的损害、EMC 测试规程）是否将电源和信号电缆分离	□	□	□	□	
13 是否定义了关于设备之间的通讯协议	□	□	□	□	
14 SIS 界面在数据显示、报警等方面是否进行了定义	□	□	□	□	
15 SIS 界面是否独立于 BPCS 界面？如果不独立，当 BPCS 有变更时，是否有措施可以避免不期望的 SIS 逻辑变更	□	□	□	□	
16 是否有关于材料、工作质量、检验和测试的说明和规程	□	□	□	□	
17 是否有监督以确保安装期间能够按照说明和规程正确执行	□	□	□	□	
18 是否有预期的安装条件？当安装环境不满足预期条件时，是否有足够的防护措施	□	□	□	□	
19 安装活动是否与其他工程活动有交叉，如果有是否有足够的防护措施来保证安装的质量	□	□	□	□	
20 安装人员与监督人员是否有充分的独立性	□	□	□	□	

表 C.1（续）

SIS 运行前评估	□	整项不适用		
	选择		需要修改项目	整改原因和要求
	是	否	必改项	待改项	
21 是否保存了必要的检验记录	□	□	□	□	
22 安装和检验规程在细节上是否足够清楚，以便使安装人员不用自己作出重要决策和解释	□	□	□	□	
23 是否遵守了设计的保护、隔离和其他特殊要求	□	□	□	□	
24 对于设计的变更是否有相关规程和说明	□	□	□	□	
25 是否有关于每个 SIF 确认的相关说明或规程	□	□	□	□	
26 在安全功能确认的测试期间，是否有监督以确保说明和规程的实施	□	□	□	□	
27 关于说明、设计方面存在的缺陷或在应用程序期间发现的缺陷，是否有制定或修正规程	□	□	□	□	
28 对 SRS 的偏差，是否有备案文件证明	□	□	□	□	
29 关于 SRS 的更改是否经过变更管理审核	□	□	□	□	
30 应用程序的测试是否由负责说明、设计和开发的相关人员参与和审核	□	□	□	□	
31 是否对最终测试文档进行审核，以确保所有的 SRS 要求都已经过测试且符合设计	□	□	□	□	
32 是否针对防止越权访问系统制定了合适的规程	□	□	□	□	
33 操作说明和规程是否有文档记录	□	□	□	□	
34 是否有合格的用户/操作手册	□	□	□	□	
35 用户/操作手册中是否描述了可能失效相关的风险以及针对失效的必要措施	□	□	□	□	
36 执行操作任务的人员和所涉及的相关人员是否接受了相关的培训	□	□	□	□	
37 是否有管理规程，以确保操作规程充分贯穿整个 SIS 使用过程	□	□	□	□	
38 对于设计中给出的假设条件，在操作和维护规程中是否有说明	□	□	□	□	

附 录 D
（资料性附录）
功能安全复审工作表样表

功能安全复审的工作表样表见表 D.1。

表 D.1 功能安全复审工作表样表

<table>
<tr><td colspan="3">所评估的系统/区域的说明</td><td colspan="2">日期</td><td>时间</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">参与人员名单</td><td colspan="3">传阅：</td></tr>
<tr><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="6">意见</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td>序号</td><td colspan="2">评估基础依据</td><td colspan="2">有/无</td><td>情况描述</td></tr>
<tr><td>1</td><td colspan="2">SIS 变更文件或变更资料</td><td colspan="2"></td><td></td></tr>
<tr><td>2</td><td colspan="2">工艺、设备变更文件或变更资料</td><td colspan="2"></td><td></td></tr>
<tr><td>3</td><td colspan="2">事故调查报告</td><td colspan="2"></td><td></td></tr>
<tr><td>4</td><td colspan="2">以往的功能安全评估报告、复审报告等</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">功能安全复审</td><td>□</td><td colspan="3">整项不适用</td></tr>
<tr><td colspan="2"></td><td colspan="2">选择</td><td colspan="2">需要修改项目</td><td>整改原因和要求</td></tr>
<tr><td colspan="2"></td><td>是</td><td>否</td><td>必改项</td><td>待改项</td><td></td></tr>
<tr><td colspan="2">1 SIS 的设计是否符合国家和行业的最新标准和规范要求</td><td>□</td><td>□</td><td>□</td><td>□</td><td></td></tr>
<tr><td colspan="2">2 SIS 的运行和维护状况是否符合国家和行业的最新标准和规范要求</td><td>□</td><td>□</td><td>□</td><td>□</td><td></td></tr>
<tr><td colspan="2">3 SIS 的操作规程、维护规程是否很好地遵循和执行</td><td>□</td><td>□</td><td>□</td><td>□</td><td></td></tr>
<tr><td colspan="2">4 SIS 的备品备件管理规定是否很好地遵循和执行</td><td>□</td><td>□</td><td>□</td><td>□</td><td></td></tr>
<tr><td colspan="2">5 SIS 的文档管理规定是否很好地遵循和执行</td><td>□</td><td>□</td><td>□</td><td>□</td><td></td></tr>
<tr><td colspan="2">6 SIS 的安全功能回路设计是否满足必要的风险降低要求</td><td>□</td><td>□</td><td>□</td><td>□</td><td></td></tr>
</table>

表 D.1（续）

功能安全复审	□	整项不适用		
	选择		需要修改项目	整改原因和要求
	是	否	必改项	待改项	
7 SIS 的仪表选型是否满足必要的风险降低要求	□	□	□	□	
8 针对实际的 SIS 运行和维护状况，为保证 SIF 的 PFD 仍然满足 SIL 要求，SIF 的 SIL 评估计算所依据的要求率、失效率，以及检验测试时间间隔等是否需要更新和修订	□	□	□	□	
9 SIS 的操作和维护人员，是否具备相应的专业能力	□	□	□	□	
10 SIS 的修改变更是否遵循了相关的变更管理规定	□	□	□	□	
11 是否针对 SIS 修改的影响的范围和深度进行了评估，以及采取了必要的应对措施	□	□	□	□	
12 对以往功能安全评估内容是否进行了复核	□	□	□	□	
可增加必要的复核内容……	□	□	□	□	

参 考 文 献

[1] ANSI/ISA-S84.01:1996 Application of Safety Instrumented Systems for the Process Industries.

[2] OLF 070—2004 Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry.

中 华 人 民 共 和 国
国 家 标 准
**油气管道安全仪表系统的功能安全
评估规范**
GB/T 32202—2015
*
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.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 2.75 字数 74 千字
2016年1月第一版 2016年1月第一次印刷
*
书号:155066·1-53010 定价 39.00 元

打印日期:2016年1月28日 F009B