ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41253—2022

过程工业安全监测系统有效性评估规范

Specification of effectiveness evaluation of safety monitoring system in process industry

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

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

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。

本文件由中国机械工业联合会提出。

本文件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。

本文件起草单位：中国石油天然气管道工程有限公司、机械工业仪器仪表综合技术经济研究所、中石化广州工程有限公司、中石化石油工程设计有限公司、北京弗安基科技有限公司、北京中电华劳科技有限公司、和利时科技集团杭州和利时自动化有限公司、浙江中控技术股份有限公司、霍尼韦尔(中国)有限公司、数字流动(苏州)安全科技有限公司。

本文件主要起草人：卜志军、张书勇、李麟、汪涛、马云鹏、潘宇、朱明露、刘瑶、王怀义、史学玲、文科武、田京山、王玥、孙向东、朱桂龙、庞欣然、施隋靖、帅冰、徐德腾、陈小华、王斌斌、周纯杰、靳江红、郭苗、熊文泽、李秋娟、张亚彬。

引　言

在过程工业领域，需要设置安全监测系统，对生产过程中的火灾和可燃/有毒气体泄漏进行监测，及时采取包括声光报警、联锁关断及消防联动等在内的一系列风险降低措施，起到有效减缓事故后果的作用，保护人员、环境及设备的安全。

本文件的目的在于指导和规范过程工业领域安全监测系统有效性评估活动。

通过安全监测系统有效性评估，对过程工业领域的火灾和可燃/有毒气体泄漏，能实现可靠、及时的监测和保护。

过程工业安全监测系统有效性评估规范

1 范围

本文件规定了过程工业安全监测系统的有效性评估人员和组织资质要求、评估活动的管理和职责、执行有效性评估的周期和阶段、各阶段评估活动的范围、流程、依据以及文档要求。

本文件适用于石油天然气、石油化工等过程工业领域的设计、运行、咨询单位对安全监测系统进行有效性评估。过程工业领域的其他行业可参照执行。

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 21109(所有部分) 过程工业领域安全仪表系统的功能安全

GB/T 39173 智能工厂 安全监测有效性评估方法

GB 50084 自动喷水灭火系统设计规范

GB 50116 火灾自动报警系统设计规范

GB 50151 泡沫灭火系统设计标准

GB 50193 二氧化碳灭火系统设计规范

GB 50219 水喷雾灭火系统技术规范

GB 50347 干粉灭火系统设计规范

GB 50370 气体灭火系统设计规范

GB/T 50493 石油化工可燃气体和有毒气体检测报警设计标准

GB 50898 细水雾灭火系统技术规范

GB 50974 消防给水及消火栓系统技术规范

GB 51251 建筑防烟排烟系统技术标准

GB 51309 消防应急照明和疏散指示系统技术标准

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全监测系统 safety monitoring system

用于监测火焰和可燃气体、有毒气体泄漏并具备报警和消防、保护功能的安全控制系统。

3.2

可燃气体 flammable gas

甲类气体或甲、乙A类可燃液体气化后形成的可燃气体或可燃蒸气。

[来源：GB/T 50493—2019，2.0.1]

3.3

有毒气体　toxic gas

劳动者在职业活动过程中，通过皮肤接触或呼吸可导致死亡或永久性健康伤害的毒性气体或毒性蒸气。

[来源：GB/T 50493—2019，2.0.2]

3.4

火焰　flame

在燃烧过程中形成的实体或者羽流，并以固定的波长（由燃料的化学特性决定）辐射能量。

注：通常情况下，所形成辐射能的一部分是人眼可见的。

3.5

安全监测系统有效性　effectiveness of safety monitoring system

安全监测系统在要求条件下执行预期安全动作的能力。

注：安全监测系统由设计、安装、特定场地运行条件以及维护相关的因素决定。安全监测系统的有效性是安全监测有效性、安全监测系统安全可用性和风险减缓设备设施有效性共同作用的结果。安全监测系统有效性评估指南见附录A。

3.6

安全可用性　safety availability

安全监测系统在规定的条件和时间内，成功执行安全监测功能的平均概率。

3.7

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1个）。

注：SIL 4是安全完整性等级的最高等级，SIL1为最低等级。

[来源：GB/T 21109.1—2007，3.2.74，有修改]

3.8

风险减缓设备设施　risk mitigation device and facility

当发生火灾或可燃气体和有毒气体的泄漏时，能减缓或减轻事故后果的设备设施。

注：包括工艺停车系统、消防灭火系统、事故通风系统、应急照明和疏散指示系统等。

3.9

风险减缓有效性　effectiveness of risk mitigation

风险减缓设备设施减缓预期事故后果的程度。

注：防止可燃有毒气体泄漏或小型的火灾事件发展成为足以形成爆炸或人身伤亡的大型气团聚集，或者大型的火灾事故。在及时有效时间内激活启动安全监测系统以减缓这类事件的严重程度。但风险减缓设备设施的执行可能没有效果。例如：

- 消防灭火系统不能控制火势；
- 疏散报警系统不能够快速启动足以允许人员撤离；
- 人员不能按计划撤离。

4　缩略语

下列缩略语适用于本文件。

DC：诊断覆盖率（Diagnostic Coverage）

ESD：紧急停车（Emergency Shutdown）

FAT：工厂验收测试（Factory Acceptance Test）

FTA:故障树分析(Fault Tree Analysis)
HAZOP:危险与可操作性分析(Hazard and Operability Study)
MooN:从“N”中取“M”(“M”out of “N”)
1ooN:从“N”中取“1”(“1”out of “N”)
2ooN:从“N”中取“2”(“2”out of “N”)
MTTR:平均恢复时间(Mean Time to Restoration)
PFDavg:要求时危险失效平均概率(Average Probability of Dangerous Failure on Demand)
SAT:现场验收测试(Site Acceptance Test)
SFF:安全失效分数(Safety 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)
TI:测试间隔(Test Interval)

5 通用要求

5.1 开展有效性评估的阶段

5.1.1 新建工程初步设计或施工图阶段应实施安全监测系统设计评估;改扩建工程涉及到安全监测对象或监测区域发生变化时,也应对变化部分进行安全监测系统设计评估。

注:设计评估具体实施阶段由项目数据收集及输入条件决定。

5.1.2 在安全监测系统投入运行前应实施安全监测系统投产前评估。

注:投产前评估通常在完成安全监测系统集成、FAT、安装、调试、人员培训、SAT、风险减缓设备设施验收,以及相关操作、维护和检定规程制定后,投产阶段前。

5.1.3 安全监测系统宜结合工艺/安全仪表系统的复审周期,复审周期不应超过5年。符合下列情形,应实施安全监测系统功能复审:

——安全监测系统设计变更或退役前;
——可能出现对安全监测系统产生影响的工艺、设备等的修改实施前;
——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影响安全监测有效性的设计缺陷时;
——国家或行业有新的规定或标准规范发布,并有复查要求时。

5.1.4 对于已开展过有效性评估的同类型站场或装置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 评估内容

5.2.1 安全监测系统有效性评估应包括安全监测有效性、安全监测系统安全可用性和风险减缓有效性的评估。

5.2.2 安全监测有效性评估应按照GB/T 39173执行。

5.2.3 安全监测系统安全可用性评估应包括探测器和控制单元,安全监测系统的可用性指标与探测器和控制单元的平均故障失效率相关,平均故障失效率的评估方法应按照GB/T 21109(所有部分)执行。

注:安全监测系统安全可用性评估案例见附录B。

5.2.4 风险减缓有效性应评估风险减缓设备设施的合规性。

注:风险减缓设备设施合规性评估审查资料清单见附录C。

5.2.5 安全监测系统有效性指标,包括探测器覆盖率、安全可用性和风险减缓设备设施合规性,应根据

风险后果严重性确定，见表1。

表1　安全监测系统有效性指标

风险后果严重性	探测器覆盖率	安全可用性(A)	风险减缓设备设施合规性
Ⅰ	60%	无要求	100%
Ⅱ	80%	≥90%	100%
同一保护区域或装置宜设置多台探测器，采用2ooN联锁逻辑时，探测器覆盖率可降为60%。当单台设备故障或旁路时，联锁逻辑宜按照1ooN执行。			
注1：规定的风险后果等级可参照HAZOP报告设定，以人身伤亡和财产经济损失为例： ● 后果Ⅰ：有人伤害、无人死亡或财产经济损失500万元以内； ● 后果Ⅱ：有人死亡或财产经济损失超过500万元(含)。 注2：表中指标均为最低要求。			

5.3　人员要求

5.3.1　有效性评估组成员应独立，独立性水平应符合表2的规定。

表2　独立性水平

风险后果严重性	独立性水平
Ⅰ	独立人员
Ⅱ	独立部门或独立组织

5.3.2　有效性评估组应由具备以下能力的人员组成：

——掌握安全监测系统相关的法律、法规要求；

——具备安全监测系统工程知识和经验；

——具备探测器覆盖率评估的知识和经验(需要时)；

——具备功能安全评估的知识和经验；

——具备对潜在风险或后果的理解，并能够对风险减缓有效性进行评判；

——能够了解新技术，并能判断新技术的新颖性和复杂性；

——以上任意一条要求至少有一名成员掌握。

5.3.3　评估组总人数应不少于3人，高级资质人员人数应不少于三分之一。

5.3.4　评估组人员应进行培训，理解并熟识自身职责范围内的审查内容、流程、依据和准则。职责分工表见附录D。

5.4　评估管理

5.4.1　评估组织方应成立评估组，确认各成员的资质和职责。

5.4.2　执行评估活动的人员应满足5.3的要求。

5.4.3　评估组长应编制评估计划，计划应包括：

——评估范围；

——评估时间和地点；

——参与评估活动的人员、部门、组织或单位；

——需要的资源；

——评估活动的安排；
——评估输出。

5.4.4 在进行有效性评估之前，评估计划应得到评估组织方的批准。

5.4.5 评估组应根据评估计划进行评估管理和开展评估活动。

5.4.6 评估组织方应向评估组提供安全监测系统的所有相关信息，包括先前执行的评估结果、通过该评估提出的建议以及相应的整改报告。

5.4.7 评估活动应文档化。

5.4.8 评估结束后，评估组应提供评估报告，评估组织方宜对报告的完整性进行审查。

5.5 评估报告

评估完成后，应根据评估过程形成对应的评估报告，并正式记录形成档案。报告内容应包括。

——项目背景：项目立项的意义、任务的由来、项目概况等内容。
——评估依据：应列出评估项目应用的法律、法规、技术规范和标准、基础技术资料名称等相关信息。
——评估目的。
——评估范围和内容。
——评估方法。
——评估过程：应明确描述评估过程，包括评估程序、工作进度和人员。
——评估结论与建议：应给出评估对象安全监测系统有效性的评估结果，指出存在的问题，提出合理化建议。
——附件：包含评估工作表、培训记录、评估硬件、软件、工具表（评估过程中所用工具的名称、型号、软件/硬件版本、公司名称、功能描述及在评估项目中的使用情况）及其他资料。

6 安全监测系统设计评估

6.1 评估依据

6.1.1 评估依据应准确、可靠。

6.1.2 应提供但不限于以下文件：

——消防工艺及仪表控制流程图（若需要）；
——工艺及仪表控制流程图；
——因果图或联锁逻辑图；
——设计说明书；
——设备汇总表；
——安全专篇（若有）；
——消防专篇（若有）；
——供货商可提供的设备 SIL 认证资料或长期使用证明材料（若有）；
——安全完整性验证报告（若有）；
——介质参数及工艺参数表；
——物料平衡组分表；
——总图；
——爆炸危险区域划分图；
——防火分区图；
——设备、设施平面布置图；

——安全监测系统设置原则或统一规定；
——风险量化报告、风险量化表、事件树图(若有)；
——三维模型；
——历史安全事件/事故信息采集；
——探测器性能参数；
——探测器安装参数；
——探测器平面布置图；
——大气压力、平均温度、风向和风速的历史数据(适用于可燃、有毒气体探测器采用场景分析法开展有效性评估)；
——区域内可闻声背景噪声及超声背景噪声(适用于超声探测器开展有效性评估)；
——已建设施，宜进行现场勘察，以确保竣工图纸的准确性；
——新建设施，及时收集与评估相关的工程变更资料，以确保数据收集的准确性。

6.2 评估内容

6.2.1 安全监测有效性评估

应按照 GB/T 39173 执行，得出探测器覆盖率量化指标。

6.2.2 安全可用性评估

6.2.2.1 应将安全监测系统所包含的探测器、控制单元的安全可用性进行整体评估。

6.2.2.2 应收集用于评估安全可用性的硬件失效概率以及其他相关资料和数据：
——安全监测系统功能描述；
——硬件失效率数据；
——表决逻辑；
——共因失效因子 β；
——测试间隔 TI；
——平均恢复时间 MTTR；
——诊断测试覆盖率 DC。

6.2.2.3 当安全监测系统与安全仪表系统联动时，宜对安全监测系统的安全完整性进行评估。安全监测系统安全完整性评估包括探测器和控制单元，应评估是否选用了符合相应 SIL 等级要求的部件或子系统，完整性等级宜不低于 SIL1，评估方法应按照 GB/T 21109(所有部分)执行。

注：对于依据以往使用原则选择的部件或子系统，评估其应用适应性以及有效性，包括以下几个方面：
- 制造商在质量、管理等方面的认证报告和文档；
- 标准/规范符合性；
- 在类似操作行规和实际工况中部件或子系统的性能；
- 有效应用案例。

6.2.3 风险减缓设备设施有效性评估

6.2.3.1 风险减缓设备设施有效性应根据 GB 50084、GB 50116、GB 50151、GB 50193、GB 50219、GB 50347、GB 50370、GB/T 50493、GB 50898、GB 50974、GB 51251、GB 51309 进行合规性评估。

6.2.3.2 检查风险减缓设备设施的设计成果、建设成果审查过程的完整性。

6.2.3.3 应检查行业监管机构规定的批复文件或验收文件的完整性。

6.2.3.4 当行业监管机构无强制要求时，应检查企业自验收文件和报备文件的完整性。

7 安全监测系统运行前评估

7.1 评估依据

7.1.1 评估依据应准确、可靠。

7.1.2 应提供但不限于以下文件：

——设计文件；

——前一阶段安全监测系统评估报告；

——厂家设备相关技术文件；

——变更文件(若有，至少应包括变更工作单、变更说明及变更影响分析报告)；

——相应的程序控制文件；

——操作维护文件。

7.2 评估内容

7.2.1 评估组应核实：

——设备性能参数是否符合设计要求；

——设备安装和布置是否符合设计要求；

——执行过一次安全监测系统设计评估；

——正确执行项目设计变更规程；

——已解决由先前的安全监测系统设计评估提出的建议；

——实现安全监测系统评估的计划或策略已经就位；

——系统调试成果记录文件(应细化，以检查记录文件为准则)。

7.2.2 针对探测器覆盖率的确认，评估组应审查：

——确认评估报告建议的落实情况(若有)；

——对探测器布点进行复核；

——对变更的复核(若有)。

7.2.3 针对探测器和控制单元，评估组应审查：

——应有满足安全完整性等级的证明文件(如需要)；

——应有国家强制规定的型式许可认证证书；

——应有防爆及防护相关证明文件。

7.2.4 针对安装，评估组应审查：

——应有关于材料、工作质量、检验和测试的说明和规程；

——应有检验记录和验收报告；

——检查运行条件是否满足设计要求；

——对变更的复核(若有)。

7.2.5 针对风险减缓设备设施，评估组应审查：

——应有满足国家强制性认证的证书文件或测试报告；

——应有设备相关技术文件；

——应有验收报告；

——对变更的复核(若有)。

8 安全监测系统功能复审

8.1 复审依据

应提供但不限于以下材料：

——设计文件；

——前一阶段的安全监测系统评估报告、复审报告等；

——设计变更文件或变更资料(若有)；

——事故调查报告(若有)。

8.2 复审内容

8.2.1 应对下面的工作项进行审查评判：

——设计、运行和维护状况是否符合国家和行业的标准和规范要求；

——修改变更是否遵循相关的变更管理规范，是否针对影响的范围和深度进行了评估，以及是否采取了必要的应对措施；

——设备运行情况是否良好；

——检维修及检定记录是否齐全；

——前一阶段的安全监测系统有效性评估报告是否有效；

——是否有安全监测系统的操作规程、维护规程、备品备件管理，以及文档管理等相关规定。

8.2.2 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。

附 录 A
（资料性）
安全监测系统有效性评估指南

A.1 概述

安全监测系统的有效性主要指火灾、可燃性气体和有毒气体检测与报警系统有效性，它由设计、安装、特定场地运行条件以及维护相关的多个因素决定，是安全监测有效性、安全监测系统安全可用性和风险减缓设备设施有效性共同作用的结果。

安全监测系统的设计分为两类，规范型设计和性能评估型设计。规范型设计采用 GB/T 50493、GB 50116 等这类基于大量工程经验的规范型技术标准，设计工作高效简单，这种设计方式无需考虑系统的失效风险，也不用计算探测器的覆盖率。

而在过程工业，特别是石油化工天然气领域复杂多变的环境中，规范型设计在很多场景下存在不完全适用的情况。因此，在过程工业领域中，有必要采用基于性能评估型设计。本文件提供了一种基于性能评估的设计方法，应用范围仅限于过程工业领域。

A.2 性能三要素

采用基于性能评估的设计时，系统的性能取决于三个方面：探测覆盖率、安全可用性以及风险减缓设备设施有效性。

探测覆盖率，需要考虑选择的探测技术是否适合工艺过程，探测器的性能参数是否满足减缓事故后果的要求（比如探测器的灵敏度是否足够高，以及反应速度是否足够迅速等），以及探测器的布放位置在多大程度上能够保证当危险发生时能够被及时地探测到（一般以百分比表示）。

安全可用性，主要沿用 GB/T 20438（所有部分）、GB/T 21109（所有部分）功能安全相关标准的条款进行分析和计算。

风险减缓设备设施有效性，这一部分的评估较为复杂，可能涉及到其他的风险控制层（系统），如消防联动控制系统（较为典型的如自动灭火系统），以及 ESD 紧急停车系统。这些系统的软硬件设计和系统结构，都会影响到火灾和气体系统的整体有效性。另外，对于额外需要进行紧急疏散的场合，除了紧急疏散照明和指示系统，疏散人员的主观因素更加难以量化分析。

A.3 设置原则

安全监测系统设置原则，即企业如何定义可以接受的风险和灾害。对于任何企业而言，要做到在任何情况下百分之百检测到工厂内的意外泄漏是不可能的，石油、天然气、石化工厂内的各类工艺装置中，除了主要设备以外，还有不计其数的各类容器，以及各种管路，从兼顾安全性以及经济性的角度来说，设计安全监测系统按照风险和灾害的重要程度有所取舍。因此，安全监测系统对预期风险能够降低到什么程度，需要企业结合工厂实际的平面布局和布置、工艺装置部署情况、人员情况、国家和地方相关的法律法规等进行综合考量后确定。关于安全监测系统的设置原则，针对火灾、可燃性气体、毒性气体等不同类型的风险给出设置原则。

对于火灾类风险，根据火灾探测的目的，设置原则分为两种。第一种采用基于及早发现和及早处理的原则，比如说当汽油泵燃烧时，快速处理，并将火灾扑灭在萌芽阶段。基于此原则，可设置火焰探测器，因为汽油燃烧时最先具备探测能力的是火焰探测器，此时设置火焰探测器能够实现快速检测，继而

以快速连锁关停汽油泵，并联动启动水灭火系统进行灭火。第二种则采用基于当重大事故即将发生时处理的原则。基于此原则，对于浮顶油罐可以设置固定温度启动的泡沫灭火系统。当浮顶罐内部的温度超过150℃时，如果不进行及时灭火，火灾事故将无法控制，此时易熔合金快速熔断，泡沫灭火系统开始喷放，尝试将浮顶罐内发生的火灾及时控制或直接扑灭。

对于可燃气体类风险，也分为两种。第一种采用空间覆盖原则，也即围绕潜在泄漏设备布设探测器的原则。基于此原则，在设计可燃气探测系统之前，需要先定义出哪些设备是潜在的泄漏源。假设有一组LPG泵，虽然泄漏场景（泄漏方向、泄漏强度、何时泄漏等）难以预测，但既然泄漏的源头是LPG泵组，那么紧靠泵组设置探测器是正确的。然而，紧靠泵组设置探测器并不能够保证一定可以及时探测到气体泄漏。如果该LPG泵组体积小，占地面积少，泄漏气体就在泵组附近形成具有爆炸力的气团，那么通过几何分析法，可以计算并判断出探测器的覆盖率。如果LPG泵组体积巨大，或者这种泵组和周围的阀门，管路，接口数量巨大，并连成一片，将很难确保泄漏气体能够被及时探测到。理论上，按照几何分析法，只要设置足够多的探测器，就一定能确保爆炸性气云在具备相应爆炸力的尺寸之前被探测器捕获。可是实际项目中，要达到这种效果，探测器的数目也将随着潜在泄漏区域的体积变大成而以几何级数攀升，以至于设置如此多的探测器在经济性方面变得不可行。针对这类应用场景，推荐采用场景分析法，虽然要确保泄漏气体在其泄漏区域内百分之百被检测到很困难，但是当气体扩散以后被其他区域的探测器捕获的可能性则会提升，当把邻近区域甚至较远区域的探测器进行统筹考虑时，爆炸性气云被探测的可能性就能够大幅提升。

第二种原则是围绕气体容易聚集、沉降而产生危险的区域布设探测器，或者会直接产生危险的区域。比如一个单体设备，管路较为密集，中间部分设备有一定的下沉，该场所很容易产生可燃性气体聚集，即便是很小的泄漏，随着时间的推移，也有可能形成巨大的可燃性气体云团，当气体云团在装置较为密集的半开放式空间被点燃时，爆炸所产生的巨大冲击力会严重破坏工艺装置和相关建筑，并危及周边的作业人员，所以，虽然此类区域不是直接的潜在泄漏区域，依然需要布置气体探测器。

对于毒性气体类风险，采用与可燃性气体探测器类似的设置原则。

A.4 设计步骤

第一阶段为风险分析阶段。该部分需要定义出涉及的危险区域，风险场景，风险发生导致的后果，风险发生的频率，以及如果不对所涉及的风险进行减缓，将发生的后果。

第二阶段确定安全监测系统的性能要求。根据第一阶段的分析结论，基于性能要求可以进一步制定出概念性设计，但概念性设计仅为初步设计，是否能够满足所需要的性能要求，需要通过计算来验证。

第三阶段为验证阶段。分为三部分来执行，对应于安全监测系统性能三要素。第一部分是探测覆盖率，第二部分是系统安全可用性，第三部分是风险减缓设备设施有效性。

综合三部分的评估结果，最终可以判断所设计的安全监测系统是否能够满足第二阶段定义的性能要求，详见如下。

——第一部分需要评估探测覆盖率，探测覆盖率的计算需要采用布点分析技术。采用两种办法来实现，第一种是几何法，第二种是场景模拟法。几何法采用的是空间几何计算，通过比对探测器的有效探测范围和危险源周围风险区域的重合程度，来判断探测器覆盖率。场景模拟法主要用于气体探测，采用软件模拟技术预测特定场景下气体泄漏时产生的气云团，并与气体探测器的布置方案进行对比，从而得出探测器的覆盖率。两种办法分别适用于不同的场景，有时候亦可互为补充。

——第二部分需要评估系统安全可用性，主要是沿用功能安全系统标准GB/T 20438（所有部分）、

GB/T 21109(所有部分)中的相关要求和条款,对所涉及的部件或子系统的平均危险失效率进行叠加计算。通常安全监测系统安全可用性评估只包括探测器和控制单元,安全可用性指标与探测器和控制单元的平均故障失效率相关,平均故障失效率的评估方法参照GB/T 20438(所有部分)。安全监测系统的部件或子系统有时会涉及到其他功能安全回路,如工艺连锁系统或者紧急停车系统,此时安全监测系统的部件或子系统尚需要遵循所在功能安全回路的要求。

——第三部分比较难以衡量,特别是涉及消防联动灭火系统的应用,通常风险减缓设备设施有效性从风险减缓设备设施的合规性进行评估。

附 录 B
（资料性）
安全监测系统安全可用性评估案例

B.1 概述

本附录通过实例，对安全监测系统的安全可用性进行评估，给出分步骤的示例和说明。

本案例中所涉及的对于平均故障失效率的计算，见 GB/T 20438.6。

B.2 安全监测系统的表决逻辑

进行安全监测系统安全可用性评估之前，有必要对安全可用性评估的表决逻辑进行说明，避免概念上的混淆。

除了所需完成功能的不同，安全监测系统与 SIS，例如 ESD 系统，在传感元件（组）部分，测量和检测介质的方式有本质区别，这决定了两种系统在表决逻辑上的差异。

ESD 系统通常采用直接接触方式对信号进行检测，例如压力、温度、液物位等，在每个取源（测量）位置上，多个传感元件具备完全相同的工况条件，并能够获取完全相同的测量信息，如果传感元件（组）采用 MooN 表决逻辑决定逻辑解算器的有效输入，则 N 集合中的每一项具有同等表决权重。

安全监测系统检测的主要介质为火焰、可燃性气体、有毒气体等，这类危险（源）是否能够被有效检测到，与传感元件的工况条件如具体安装位置、所在空间的特点密切相关。例如受到气体自由扩散、稳态或非稳态对流的影响，可燃性、有毒气体无法被附近的气体探测器均匀检测到；火焰探测器由于检测视角的不同，其能够有效检测到火焰的能力也不完全相同。对于安全监测系统来说，传感元件之间的表决权重需要根据具体应用的特点分析和确定，不能简单地套用 MooN 表决逻辑。

为了降低系统因单个传感元件故障误动的可能性，安全监测系统的传感元件（组）可采用合适的表决逻辑。为了实现这一目的，可采用近似策略，如可将两只贴邻安装且设置相同的传感器（探测器）视为同一位置，即视为具有相同的表决权重，并可采用 MooN 表决逻辑（此时 N＝2），通常 N 不宜大于 3。此时，注意以下事项：

——对传感器（探测器）的功能、性能充分了解，确保其符合该策略；

——对应用场合和应用特点充分了解，确保此种策略是适合的；

——对传感器（探测器）的使用、维护特点充分了解，确保不会因使用、维护不当，使传感器（探测器）的性能不满足要求。

需要特别注意的是，此处的表决逻辑与探测器的覆盖有效性评估中的表决逻辑（1ooN 或 2ooN）所表达的意义是不同的，注意加以区分。

B.3 安全监测系统功能描述

假设有某天然气压缩机厂房，根据项目设计文件，厂房内共布置了 1 台压缩机，8 只火焰探测器，以及一台用于火灾报警的控制器，如图 B.1 所示。

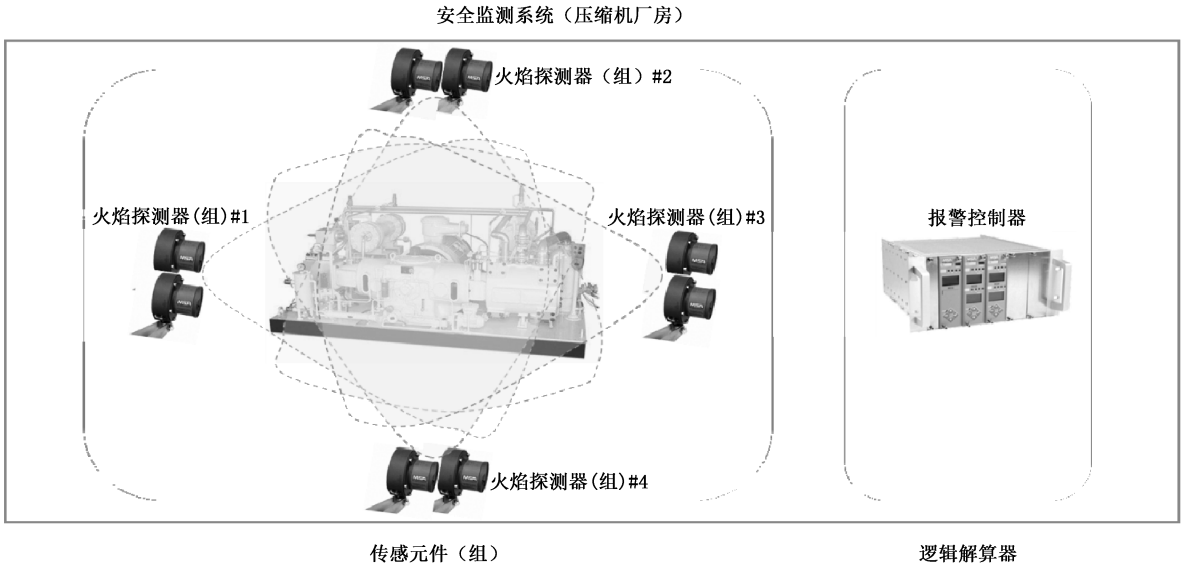

图 B.1　天然气压缩机厂房火焰探测器布置

该安全监测系统包括：8 只火焰探测器，1 台火灾报警控制器，用于监测压缩机厂房的 1 台压缩机可能产生的火焰风险，保护的对象即为压缩机厂房内的 1 台压缩机。其中，8 只火焰探测器分为 4 组，在 4 个不同方向上分别贴邻部署 2 只，并具备基本相同的检测视角；该安全监测系统的报警触发条件为，当有 2 只或以上的火焰探测器报警，火灾报警控制器将输出预设的报警信号。

根据前述章节，每个不同方向上贴邻安装的 2 只火焰探测器可采用近似策略，视为具有同等表决权重的传感器（探测器）。为了简化模型，假设火焰探测器（组）的表决逻辑为 2oo2。但该安全监测系统传感元件实际采取的表决逻辑为 2oo8。

B.4　安全监测系统功能安全相关技术参数

表 B.1 为所涉及子系统或部件的失效率数据（示例）。

表 B.1　硬件失效率（按照故障类别）

子系统/部件	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
火焰探测器	1.05E-04	3.55E-05	8.82E-05	9.80E-06	95.9%
报警控制器	1.15E-07	1.50E-08	2.48E-07	2.50E-09	99.3%

其他需要使用的用于评估安全可用性的参数见表 B.2（示例）。

表 B.2　安全可用性评估参数（其他）

可用性参数	火焰探测器	报警控制器
平均恢复时间 MTTR（小时）	72	8
测试间隔 TI（年）	1	3
表决逻辑	2oo2	1oo1
共因失效因子 β	1.0E-01	2.0E-02
诊断检测覆盖率（DC）	90%	99%

B.5 安全监测系统安全可用性评估

安全监测系统安全可用性与该系统的 PFDavg 密切相关，其关系见式(B.1)：

$$A = 1 - P \quad \cdots\cdots (B.1)$$

式中：

A ——安全监测系统的安全可用性；

P ——安全监测系统的平均故障失效率。

B.2 中的案例安全监测系统安全可用性计算过程如下：

a) 安全监测系统的平均故障失效率，见式(B.2)：

$$P = P_{FD} + P_{LS} \quad \cdots\cdots (B.2)$$

式中：

P ——安全监测系统的平均故障失效率；

P_{FD} ——火焰探测器的平均故障失效率；

P_{LS} ——控制单元的平均故障失效率。

b) 传感元件(组)的平均故障失效率，见式(B.3)：

$$P_{FD} = 1 \times 10^{-1} \quad \cdots\cdots (B.3)$$

c) 逻辑解算器的平均故障失效率，见式(B.4)：

$$P_{LS} = 3.48E\text{-}05 \quad \cdots\cdots (B.4)$$

d) 安全监测系统安全可用性见式(B.5)：

$$A = 90.00\% \quad \cdots\cdots (B.5)$$

当 2 只火焰探测器的安装位置不变，但其表决逻辑改为：1 只火焰探测器报警时，报警控制器将输出预设的报警信号，则该安全监测系统的传感元件(组)部分用于评估安全可用性的表决逻辑为 1oo2，安全监测系统安全可用性 A 安全监测系统＝99.21%。

当采用 1 只或 3 只火焰探测器时(安装位置不变，仅改变触发报警的表决逻辑)，也可按照此方法计算出相关表决逻辑下的安全可用性，见表 B.3。

表 B.3 安全监测系统安全可用性对比(根据表决逻辑)

火焰探测器(组)表决逻辑	1oo1	1oo2	1oo3	2oo2	2oo3
安全可用性	95.00%	99.21%	99.50%	90.00%	98.57%

附 录 C
（资料性）
风险减缓设备设施合规性评估审查资料清单

风险减缓设备设施合规性评估审查资料清单见表 C.1。

表 C.1 风险减缓设备设施合规性评估审查资料清单

序号	工程阶段	名称	审查资料
1	初步设计		消防设计专篇、安全设施设计专篇审查意见和结论
2	施工阶段	消防设计审核	资料审查的材料包括： a） 建设工程消防设计审查申请表； b） 消防设计文件。 具有下列情形之一的，同时提供特殊消防设计文件，或者设计采用的国际标准、境外消防技术标准的中文文本，以及其他有关消防设计的应用实例、产品说明等技术资料，专家评审论证材料： 1） 国家工程建设消防技术标准没有规定的； 2） 消防设计文件拟采用的新技术、新工艺、新材料可能影响建设工程消防安全，不符合国家标准规定的； 3） 拟采用国际标准或者境外消防技术标准的。 消防设计文件包括但不限于： a） 建筑构造和耐火等级； b） 总平面布局和平面布置； c） 安全疏散设施； d） 消防给水和消防设施； e） 消防电源及配电。 结论性文件：消防设计审核合格文件
3	竣工阶段	消防验收	审查资料包括： a） 建设工程消防验收申请表； b） 有关消防设施的工程竣工图纸； c） 符合要求的检测机构出具的消防设施及系统检测合格文件。 结论性文件：消防验收合格意见
4	运行阶段	消防备案	审查资料包括： a） 工程消防验收备案表； b） 有关消防设施的工程竣工图纸； c） 符合要求的检测机构出具的消防设施及系统检测合格文件。 结论性文件：备案凭证
5	改扩建		修改了消防功能的改扩建工程，按照上述 3 和步骤 4 提供审查资料

附 录 D
（资料性）
评估组职责分工表

评估组职责分工表样例见表 D.1。

表 D.1 评估组职责分工表样例

角色	阶段		
	初步设计、施工图阶段	投入运行前阶段	复审阶段
组长	a) 组织、执行评估活动； b) 与其他组织之间的沟通与协调； c) 确保评估目标、主体与评估过程一致； d) 编制评估计划及完成整体评估报告	a) 组织、执行评估活动； b) 与其他组织之间的沟通与协调； c) 确保评估目标、主体与评估过程一致； d) 编制评估计划及完成整体评估报告	a) 组织、执行评估活动； b) 确保评估目标、主体与评估过程一致； c) 编制评估计划及完成整体评估报告编制
组员	a) 安全监测系统探测器、控制器及系统参数确认； b) 安全监测有效性评估(探测器覆盖率)； c) 安全可用性评估； d) 风险减缓有效性评估	a) 安全可用性评估； b) 风险减缓有效性评估	a) 安全可用性评估； b) 风险减缓有效性评估

参 考 文 献

[1] 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

[2] GB/T 20438.6 电气/电子/可编程电子安全相关系统的功能安全 第6部分:GB/T 20438.2和GB/T 20438.3的应用指南

[3] GB/T 50493—2019 石油化工可燃气体和有毒气体检测报警设计标准

[4] BP GP 24-85 6 July 2017-Design basis for fire and gas detector placement

[5] BP GP 30-85 6 July 2017-Fire and Gas Detection

[6] ISA-TR84.00.07—2018 Guidance on the Evaluation of Fire, Combustible Gas, and Toxic Gas System Effectiveness

[7] SHELL DEP 32.30.20.11-Gen.Februray 2014-FIRE,GAS AND SMOKE DETECTION SYSTEMS