ICS 13.110
CCS N 10

中华人民共和国国家标准

GB/T 41254—2022

爆炸保护系统的功能安全评估方法

Functional safety assessment method of explosive protective system

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和控制标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：广州特种机电设备检测研究院、机械工业仪器仪表综合技术经济研究所、东莞汇乐环保股份有限公司、国家防爆设备质量监督检验中心(广东)、普瑞泰格(南京)安全设备有限公司、浙江中控技术股份有限公司、东北大学、广东技术师范大学、华南理工大学、东莞新能源科技有限公司、中国特种设备检测研究院、广东工业大学。

本文件主要起草人：王新华、熊文泽、林卫波、史学玲、梁峻、裘坤、孟邹清、刘瑶、张岩、蒋漳河、钟圣俊、杨勇、汤鹏、朱杰、刘晓亮、靳江红、邵伟、陈朝阳、黄剑锋、谢小鹏、陈祖志、马雷、周有铮、闫炳均、任军民、刘爱华、帅冰、朱明露、张亚彬。

引　言

为了保证爆炸性环境用爆炸保护系统设计和制造的功能安全评估程序和信息的一致性，需要对其进行标准化。

功能安全评估是一种工具，它提供了制造商和用户之间的基本联系。本文件针对爆炸性环境用爆炸保护系统建立了一套实现功能安全、可靠性和有效性的方法。

当爆炸的发生不可避免时，爆炸保护系统可立即终止爆炸和/或限制其影响，并将发生的爆炸风险减小至可接受水平。在设计爆炸保护系统时，通过对系统的预期故障进行适当分析，可有效地提高和保证爆炸保护系统的功能安全。因此，有必要对爆炸保护系统进行功能安全评估。本文件可以为爆炸保护系统提供决策建议，并指导特定类型爆炸保护系统功能安全相关标准的制定。

爆炸保护系统的功能安全评估方法

1 范围

本文件描述了爆炸性环境用爆炸保护系统功能安全评估方法的术语和定义、评估通则、评估程序及文件记录。

本文件适用于爆炸保护系统在设计、制造、使用、维护及检测检验等环节的功能安全评估。

本文件不适用于以下情况：

——潜在点燃源的识别和点燃危险的风险评估；

——爆炸危险环境监测系统的功能安全评估；

——特定类型的爆炸保护系统的符合性验证。

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 2900.35—2008 电工术语 爆炸性环境用设备

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

3 术语和定义

GB/T 20438(所有部分)和GB/T 2900.35—2008界定的以及下列术语和定义适用于本文件。

3.1

失效 failure

在任何系统项目、部分项目、任何管理功能任务或程序中，不执行或不按照预先规定执行的事件，或不可操作的状态。

3.2

爆炸保护系统 explosive protective systems

用于及时终止初期爆炸和/或限制爆炸影响范围的具有独立功能的系统。

3.3

(爆炸保护系统)功能安全 functional safety(of explosive protective systems)

与爆炸保护系统(包含安全相关装置)的预期用途和完整性有关的整体安全的一部分。

注1：功能安全取决于爆炸保护系统及其他安全相关系统的正确施行。

注2：本定义与GB/T 20438.4—2017中的定义相偏离，体现出爆炸安全术语上的差异性。

注3：爆炸保护系统的功能安全也属于爆炸保护系统性能的一部分。

3.4

(爆炸保护系统)功能安全估计 functional safety estimation(of explosive protective systems)

估算或确定爆炸保护系统安全功能失效发生概率的活动。

3.5

(爆炸保护系统)功能安全评价　functional safety evaluation(of explosive protective systems)

确定爆炸保护系统的功能安全是否满足预期可接受标准的程序和活动。

3.6

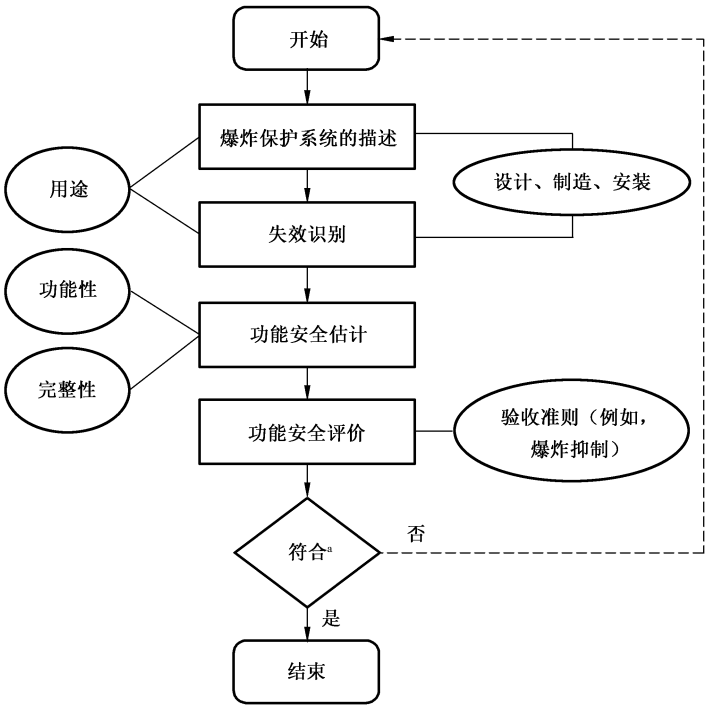
(爆炸保护系统)功能安全评估　functional safety assessment(of explosive protective systems)

对爆炸保护系统的功能安全进行估计和评价的全部活动。

4　功能安全评估通则

4.1　功能安全评估步骤

爆炸保护系统的功能安全评估应按图1所示步骤逐步开展,确保功能安全评估人员用一种系统化的方法检查并核实爆炸保护系统的全部或部分功能,使之依据设计时的经济技术要求达到足够的功能性和完整性级别。



注:虚线内容不属于功能安全评估的一部分。

[a] 符合性确认不是功能安全评估的组成部分。

图1　爆炸保护系统功能安全评估流程

爆炸保护系统功能安全评估分为以下4个步骤:

a)　第一步:爆炸保护系统的描述(见5.2);

b)　第二步:失效/故障的识别(见5.3);

c)　第三步:功能安全估计(见5.4);

　　1)　功能性;

　　2)　完整性;

d)　第四步:功能安全评价(见5.5)。

上述4个步骤是决定爆炸保护系统是否达到预期用途中所需预期功能安全级别的基础。功能安全评估结果应在技术文件中详细说明(见第6章)。

如果没有达到预期所要求的功能性和完整性级别,则有必要改进爆炸保护系统或重新定义更合适的预期用途。

注:选择适当的措施改进爆炸保护系统不属于本文件的内容。

如果功能安全评估由制造商完成,则在技术文件中应对功能安全评估结果进行详细说明(见第6章)。

功能安全评估的实施和执行应以定性方法为支撑,并在适当情况下以定量方法加以补充。

4.2 功能安全评估范围

爆炸保护系统应基于4.3规定的所需信息开展评估。

爆炸保护系统的功能安全评估应限于其预期用途和可合理预期的误用。

注:可合理预期的误用指操作者因疏忽或错误理解而对爆炸保护系统的不正确使用和/或操作。误用不是正常操作的一部分。可预期的误用不包括故意行为。

4.3 功能安全评估所需信息

爆炸保护系统功能安全评估所需信息应至少包括:

a) 预期用途;

b) 用于爆炸保护系统设计的安全特性;

c) 维护要求;

d) 实际和可预期的周边区域环境;

e) 相关设计图纸;

f) 设计计算及开展检查的结果。

如果可获取,还应包括:

a) 测试报告;

b) 事故案例;

c) 安全相关的出版物。

如果爆炸保护系统没有相关的事故案例,则应使用可获取的类似爆炸保护系统的信息。当爆炸保护系统缺少事故案例、仅出现少量事故或轻微事故时不应直接将其评定为低风险。

功能安全评估所需信息也包括其他可能的预防措施。

上述所需信息需要根据爆炸保护系统相关技术的发展而不断更新。

对于定量评估,应在确定数据适用性的前提下使用由数据库、手册、实验室和制造商的规格书中提供的数据。任何与数据相关的不确定性都应记录在第6章规定的文件中。

注:数据用于定义可预期的操作要求,与可靠性、适用性、耐用性、通用性、良性的故障及失效保护特性和标签、警告、标识、可追溯性要求和指示相关。相对于测试数据,基于间接来自经验的专家意见的一致性数据,宜用于定性评估。

5 功能安全评估程序

5.1 原则

爆炸保护系统功能安全的评估,应根据对爆炸保护系统的功能和所防护的爆炸类型的理解,按照

图 1 所示的功能安全评估流程和步骤开展进行。

功能安全评估应包括爆炸保护系统的维护。制造商提供的说明书中应包含所必需的维护要求，以及与预期用途相关的系统维护不到位的情况。

爆炸保护系统功能安全评估的示例见附录 A。

5.2 爆炸保护系统的描述

爆炸保护系统按以下方式分为两类：

a) 被动系统，如阻火器、通风系统等；

b) 主动系统，如抑制系统等。

爆炸保护系统的预期用途应至少从以下方面进行描述：

a) 爆炸保护系统的生命周期；

b) 在使用、时间、空间方面的限制；

c) 功能的精确定义；

d) 制造材料的选择；

e) 性能、寿命和配置；

f) 爆炸类型的描述；

g) 工艺条件的限制；

h) 维护要求。

5.3 失效的识别

5.3.1 通则

应根据爆炸保护系统的潜在失效源对爆炸保护系统进行功能安全评估，为此，应从以下方面分析爆炸保护系统预期使用时的功能和状态：

a) 可能出现的运行故障；

b) 爆炸保护系统的可靠性；

c) 可合理预期的误用。

应通过功能和系统分析对潜在失效进行评估，并在整个生命周期中分别给予考虑。

注：失效识别方法的示例见附录 B。

5.3.2 失效识别的开展

5.3.2.1 设计与制造

应从以下方面识别爆炸保护系统在设计与制造过程中存在的潜在失效：

a) 按照预期用途，判断以下方面是否存在潜在失效：

1) 阻火器是否具有足够的热传导率；

2) 泄放装置是否具有有效压力释放能力；

3) 抑制系统是否具有足够的抑制效能；

b) 爆炸保护系统机械结构的尺寸，判断是否存在以下的潜在失效：

1) 抗压性不足；

2) 耐温性不足；

3) 抗振动与抗冲击能力不足；

4） 防老化或防腐蚀能力不足；

c） 根据爆炸的性质，判断安装场所、安装位置或安装方法是否合适；

d） 与工艺相关的模式、环境温度、环境压力以及运行阈值或灵敏度是否正确；

e） 软件和控制设备（硬件）是否兼容，软件是否具备合理的安全诊断报警能力；

f） 硬件是否具有抗电磁干扰的能力；

g） 是否具备额外的故障安全措施，如合理的安全冗余；

h） 在电源失效的情况下，是否应具有措施保障系统的预期用途。

5.3.2.2 安装

应从以下方面识别爆炸保护系统安装过程中存在的潜在失效：

a） 破空阀、泄压装置前面的危险区域、反冲力、人员受伤风险等对预期功能的影响；

b） 密封不充分；

c） 电气条件不满足（如短路、开路、过载和接地故障等）；

d） 控制和指示设备的能量供应和/或后备电源不足。

5.3.2.3 操作和维护

应识别爆炸保护系统在使用和维护过程中的潜在系统失效场景及防止失效措施，在使用和维护过程中的潜在失效如下：

a） 泄漏污染；

b） 人为干预不正确或不充分（错误操作、错误安装、错误维护、意外干预）；

c） 故障显示信息以及缺少紧急停机程序。

应在使用说明中对这些缺失或不足的情况以及潜在失效加以详细说明。

5.3.2.4 修改

对爆炸保护系统进行任何与安全有关的修改后，应将其视为新的系统重新进行功能安全评估。

5.4 功能安全估计

5.4.1 通则

对于爆炸保护系统，应通过失效识别结合风险可接受标准要求，确定爆炸保护系统的功能安全要求。

失效识别后，应通过确定失效概率估计爆炸保护系统的功能安全。

应根据爆炸保护系统在降低失效概率和/或系统与安全相关的设备的复杂性方面的设计安全要求，开展定性地、半定量地或定量地功能安全估计。

爆炸保护系统的功能安全估计应从以下两方面进行：

a） 功能性，即完成系统预期用途所需功能的能力（例如，阻止初期爆炸、减少爆炸压力）；

b） 完整性，即按要求或按时执行这些功能的可靠性。

完成所需功能的能力可通过可靠性数据和/或对系统结构的容错性表述来部分量化。

对于可能导致系统保护功能失效的每一个参数，如针对功能和完整性要求相关的，应对其进行可靠性估计和评价。

5.4.2 功能性

依据失效发生概率，功能安全估计的功能性应包括技术故障和运行故障，如在不同运行模式和维护

活动过程中以及事件本身期间，根据故障，可合理预期的使用和误用中预测其行为。

对于已确定的爆炸特征，通常应基于最坏的情况开展功能安全估计，即爆炸保护系统的安全功能缺失。当不适用时，应在只影响爆炸保护系统部分性能的情况下开展功能安全估计，如可部分减少爆炸带来的危害，即在一定程度上降低爆炸超压。

对于识别出的每种类型的失效（见 5.3），应评估它们能降低性能和相关概率的程度。在这种情况下，考虑并评价影响系统行为的各种参数的临界性，例如：

a） 条件和操作模式（如安装和运行要求，维护要求，测试、复位、联动装置、旁路）；
b） 所需的响应和反应时间（传感器到执行器的响应时间和预防措施的反应时间）；
c） 故障功能、状态、响应时间；
d） 故障安全功能，安全状态；
e） 危险失效和相关行动的监测和探测能力；
f） 考虑到安全特性的爆炸保护系统灵敏度；
g） 设计与控制参数；
h） 系统结构、冗余、容错；
i） 接口、系统元件的影响、安全相关控制元件以及安全装置；
j） 检测/测试方法；
k） 其他系统对正常功能的依赖性/独立性；
l） 系统性的/与测试无关的失效。

5.4.3 完整性

对于安全相关设备，应根据功能安全完整性要求进行定义和评估，属于爆炸保护系统性能的一部分。

对于简单的预防系统，可经过经验验证或评估后符合要求的功能，在此基础上进行评估（即在使用中证明）。

对于每一个安全功能，导致安全功能无法实现的事件概率（即失效概率或要求时的失效概率），应根据下述因素并进行估算：

a） 运行模式（高要求模式/连续模式、低要求模式）；
b） 假定要求率；
c） 体系结构/体系结构的约束；
d） 系统性失效；
e） 共因失效；
f） 平均维修时间；
g） 检测/测试间隔；
h） 诊断覆盖率和安全失效分数。

完整性评估的结果应采用可靠性数据的形式，根据情况采用要求时平均失效概率或每小时危险失效的概率（即失效率），既可单独用于不同的功能，也可作为整体用于爆炸保护系统功能。

这些结果将用于功能安全评估，并供用户验证爆炸保护系统如何在爆炸风险综合评估中起作用和降低爆炸总风险的前提条件。

这些结果应成为文件记录的一部分。

注：这些失效都是测试或监控设备不能发现的，包括：设计失效、软件错误、信号识别、安装偏差等。

5.5 功能安全评价

应对功能安全估计的可接受性开展功能安全评价。因此，应根据预期用途预先确定验收标准。验

收标准可以是定性的、半定量的或定量的。

对于概率估计，可接受标准可以是定性的、半定量的或定量的。

将确定的爆炸保护系统要求时的失效概率和定义的可接受标准进行比较，可说明是否有必要采取风险降低措施。

为了确定降低风险的措施，首先应分析爆炸保护系统的构成或属性，这些是总体风险的决定因素。应对每一项确定的降低风险措施进行分析，审查与各项相关的安全效益和实用性。

可接受的爆炸保护系统应包含以下要求：

a) 系统能在初期阶段阻止爆炸，或者将爆炸影响减少到可接受的程度；

b) 在a)的系统发生故障、失效和/或干扰时，通过使用例如故障安全技术或冗余等方法可保证该功能仍然有效。

6 文件记录

6.1 制造商文档

功能安全评估文件应说明已遵循的程序和已取得的结果，应包括但不限于：

a) 已开展功能安全评估的爆炸保护系统(如规格、限制、预期用途、操作描述)(见4.2和5.2)；

b) 已做出的任何相关假设(如载荷、强度、安全系数)；

c) 基于4.3a)～d)的使用说明；

d) 开展功能安全评估所需的更多信息(见4.3)；

e) 所使用的数据和参考资料(例如，数据库、事故案例、广泛应用于类似爆炸保护系统功能安全方面的经验；应评估与所用数据相关联的不确定度及其对功能安全评估的影响)；

f) 失效识别(见5.3)；

g) 功能安全评价的最终结果(见5.5)；

h) 为消除失效或增加功能安全而实施的安全措施(如标准或其他规范)。

6.2 用户文档

制造商应向用户提供6.1a)、d)、h)的信息。

附 录 A
（资料性）
功能安全评估示例

A.1 概述

以下为使用失效模式、影响和危害程度分析（FMECA）进行功能安全评估时一种可能形式的结果示例。

图 A.1 给出安装在除尘器上的爆炸抑制和隔离系统最重要的组件。系统按如下流程操作。

a） 如果除尘器内发生爆炸，压力开始增大。由压力传感器记录压力-时间曲线，并由分析装置进行连续分析。当压力达到报警值水平时（压力上升速率达到一定值），分析单元将向控制单元发送信号。

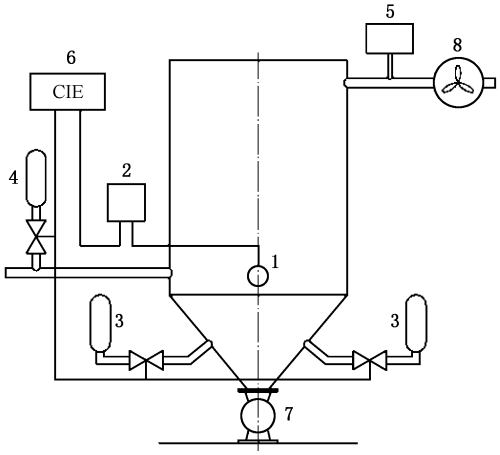
b） 控制单元启动（触发/激活）安装在除尘器上的两个 HRD 灭火器，对爆炸进行抑制。

c） 同时，启动将除尘器与上游生产装置隔离的 HRD 灭火器，以防止爆炸回火到相连的设备中。

当除尘器发生爆炸时，也可解除除尘器出口处的锁气卸灰装置，但是在本示例中未考虑这一措施。

因此，当检测到压力上升速率过高时，在除尘器内部启动该功能，表明发生爆炸，并在 HRD 灭火器的触发过程中停止。

当电源出现故障时，将由防爆系统的电池进行供电。电池可供电 4 h，4 h 之后的安全功能丧失不予考虑。在短路、开路等情况下，系统将强制程序进入安全状态。在本例分析中，没有考虑关闭系统过程中的爆炸残留风险。



标引序号说明：

1——与分析单元连接的压力传感器；

2——压力传感器分析装置；

3——抑制除尘器爆炸的高释放率（HRD）灭火器；

4——将除尘器与上游生产装置隔离的 HRD 灭火器；

5——粉尘浓度监测设备；

6——控制和指示设备（CIE）；

7——锁气卸灰装置；

8——风机。

注：本例是假设性示例，并不完整，仅作为示例来理解，本例的标引序号也是表 A.3 中的组件序号。

图 A.1 除尘器的爆炸抑制和隔离系统

A.2 安全功能的分解

对系统安全功能进行分解，得到的系统功能框图如图 A.2 所示。

图 A.2 系统功能框图

A.3 系统要求

当传感器/分析仪给出信号时，该功能为打开每个灭火器的活瓣。

爆炸抑制和隔离系统的关键部件是传感器、控制单元和 HRD 灭火器，因此在本示例中仅对这些部件进行分析。假定其中一个 HRD 灭火器没有打开，此时系统的安全功能失效（系统的抑制能力仍可用于较弱的爆炸；如果除尘器中的点火位置远离管道与除尘器的连接处，则很可能不需要进行隔离）。

假定系统的要求频率为每年一次，粉尘爆炸是由静电放电或进入除尘器的高温颗粒物引起。

A.4 HRD 灭火器

A.4.1 概述

爆炸抑制和隔离系统一个非常重要的部件是 HRD 灭火器。本示例中的灭火器使用机电式触发的活瓣，电容放电驱动力矩电机松开活瓣的锁止机构。储存抑制剂的容器与阀门连接，容器内用氮气预压至 6 MPa，锁止机构松开时氮气推动活瓣开启，通过喷嘴将抑制剂释放到要保护的结构中。考虑到系统冗余，在抑制器中安装两套力矩电机和电子释放装置，且两套力矩电机和释放电子装置均可正常运转。

A.4.2 HRD 灭火器部件失效率

表 A.1 为针对 HRD 灭火器进行的 FMECA 分析示例，表中提供了 HRD 灭火器 17 个部件的部件失效率，为每运行百万小时的失效数。作为示例，这些数据均为虚构数据。

表 A.1 HRD 灭火器部件失效率的示例

序号	部件描述	部件数量	部件失效率 $(\times 10^{-6})$/h	总失效率 $(\times 10^{-6})$/h
1	管道过滤器	1	0.300	0.300
2	外壳	1	0.040	0.040
3	活瓣	1	0.040	0.040
4	枢轴	1	0.100	0.100
5	锁销	1	0.150	0.150
6	平垫片	1	0.140	0.140
7	圆柱头螺钉	8	0.008	0.064
8	密封垫圈	2	0.140	0.280
9	测压开关	1	1.100	1.100

A.4.3 故障的后果和危险性

对于每个故障都估计了其潜在后果，通常将故障的危险程度分成以下 4 个等级。

——1：轻微故障。不影响系统功能。

——2：不太严重的故障。对系统功能只有轻微的影响。

——3：严重故障。系统未直接失效。

——4：极其严重的故障。整个系统失效。

在 FMECA 分析的文档中根据上述分级的后果和危险程度进行说明（见表 A.2）。

表 A.2 HRD 灭火器部件失效的后果和危险程度

序号	部件	功能辨识	失效形式	失效率 ($\times 10^{-6}$)/h	失效影响	危险程度等级	备注
1	管道过滤器	填充过程中过滤氮气	堵塞	0.300	无法填充	1	受监控
2	外壳	容纳所有功能部件	裂纹，断裂	0.040	压力损失	3	受监控
3	活瓣	关闭压力容器	裂纹，断裂	0.040	压力损失	3	受监控
4	枢轴	活瓣的旋转轴	断裂	0.090	压力损失	3	受监控
			卡死	0.010	无法按照要求开启阀门	4	待机失效，通过选择材料组合和表面处理以防止
5	锁销	手动锁定开启机构	卡死	—	活瓣不能锁定或解锁	2	锁定或解锁时会注意到
			断裂	0.090	活瓣不能锁定或解锁	2	锁定或解锁时会注意到
			忘记解锁	0.010	无法按照要求开启阀门	3	受电气监控
6	平垫片	阀门外壳和驱动机构之间的垫圈	泄漏	0.140	无	1	—
7	圆柱头螺钉	固定电子元件外壳	松动，断裂	0.064	无	1	—
8	密封垫圈	螺栓密封	泄漏	0.280	无	1	—
9	测压开关	监测系统压力	无法开启	0.500	无法监测压力损失	3	待机失效，在首次检查中优先得到监控
			无法关闭	0.500	报警	2	受监控
			泄漏	0.100	压力损失	3	受监控
注：只有部分组件和功能作为 FMECA 分析的部件在本表中列出。							

对 HRD 灭火器的 FMECA 分析中，仅考虑危险程度 1 的轻微故障时可估计 HRD 灭火器总的要求时的失效概率。已经对控制单元和传感器进行了类似的分析，在此不再详述。

A.4.4 计算结果

基于为 HRD 灭火器、控制单元和与分析单元相连接的压力传感器准备的 FMECA 和/或失效模式和影响分析(FMEA)分析结果,估计爆炸抑制和隔离系统的爆炸抑制功能失效概率见表 A.3。

表 A.3 爆炸抑制功能要求时的平均失效概率(PFDavg)

组件	组件序号	平均失效概率(PFDavg)
与分析单元连接的压力传感器	1	8.8×10^{-4}
控制单元	6	1.7×10^{-3}
HRD 阀	3	6.6×10^{-3}
总功能	—	9.1×10^{-3}

从表 A.3 可以看出,根据 GB/T 20438(所有部分),该功能符合 SIL 2 的要求。

附 录 B
（资料性）
失效识别方法

B.1 概述

有许多方法可以识别失效、估计概率并评估这些失效的影响，由于每种方法都是针对特定应用场景而开发的，因此在功能安全评估的不同应用中，有必要对一些细节进行修改。

本文件参考了GB/T 27921—2011中的两种风险评估方法，并对这两种风险评估方法进行了简要的介绍和描述，可为风险评估方法在爆炸保护系统功能安全评估中的应用提供指导。

B.2 失效模式和影响分析（FMEA）及失效模式、影响和危害程度分析（FMECA）

FMEA和FMECA用于识别和描述系统失效、冗余和共因失效、功能、失效模式、原因、影响、检测方法、平均维修时间和对安全相关系统中安全功能关键组件的测试间隔。

在分析系统前需要将系统分解成组件，找到适合此系统故障的级别，该级别取决于FMEA或FMECA的分析目标和有效的技术文档。在很多情况下，FMEA或FMECA分析都是作为故障树分析的前期准备或作为功能安全评估的基础。

FMEA或FMECA由相关工程领域的团队以及具有丰富系统产品经验的人员执行。有标准的表格（附录A给出了FMEA或FMECA表格的示例）记录系统中每个组件的信息，可包括以下内容：

a) 组件的名称和类型；
b) 功能；
c) 失效模式；
d) 失效原因；
e) 局部故障影响；
f) 全局故障影响；
g) 故障检测；
h) 补偿/保护冗余；
i) 意见、建议和后续行动跟踪。

在FMEA或FMECA分析表格中，也可用一列记录失效的概率及其后果。失效的概率和后果经排序可分类，如低、中、高或风险矩阵等。每个类别的含义和重要性在文本中进行定义，并根据人员、经济和环境对失效后果进行分类。在功能安全评估中，通常需要用到定量或半定量的概率估算，该数据由制造商给出，或者从通用数据中获得。

B.3 故障树分析（FTA）

故障树是一种风险分析方法，通过故障树分析可根据子系统（组件）的失效模式和操作人员的行为来找出不希望出现的系统失效模式，故障树能列出所有可能发生失效事故的逻辑关系，这些由故障树逻辑图来记录，如图B.1所示。

故障树图包含两个基本元素："逻辑门"和"事件"，逻辑门是故障逻辑在故障树中的通路，并显示故障事件和由该事件导致的更高层级事件之间的关系。两种主要类型的门是"与"门和"或"门，"与"门表示当输入的所有事件同时发生输出事件才发生，"或"门表示当输入事件至少有一个发生则输出事件发生。还有许多其他类型的门，使用它们表示逻辑关系的频率较低。一旦逻辑被记录在故障树中，只要给定关于故障树中底事件的发生频率/概率就可以计算顶事件的发生频率，这些频率/概率通常可以是电

子、电气或机械部件、软件的故障率，并且这些数据可以从数据库或典型行业数据中获得。故障树分析还可以评估人员操作的失效率，根据故障树的布尔逻辑算法，最终确定顶事件的发生频率。在“或”门中，事件的发生频率都可以相加，在“与”门中，一个事件的发生频率可以和其他任意数量的事件概率相乘（作为一阶近似解）。在评估故障树时，重要的是要清楚哪些数据是频率（以每单位时间内发生的事件为单位）以及哪些是概率（无量纲）。还有用于评估大型和复杂故障树的专业技术，例如，最小割集技术。

FTA 特别适用于离散项目、成套机械设备以及爆炸保护系统的可靠性评估。

FTA 应用于复杂机械时会过于复杂且耗时，除非在没有量化的情况下使用，以高度概括不同组件和功能之间的相互作用。

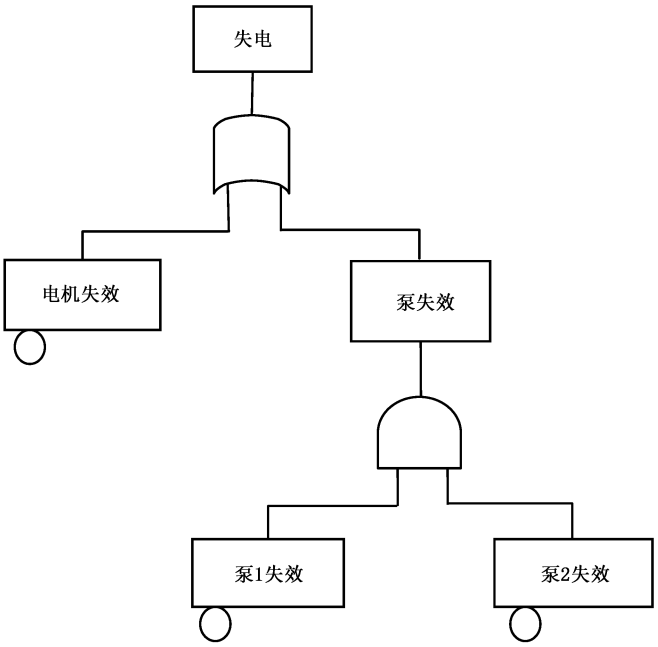


图 B.1　电源的故障树分析

参 考 文 献

[1] GB/T 16855.1—2018 机械安全 控制系统安全相关部件 第1部分:设计通则

[2] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语

[3] GB/T 27921—2011 风险管理 风险评估技术

[4] GB 28526—2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

[5] EN 13237: 2012 Potentially explosive atmospheres—Terms and definitions for equipment and protective systems intended for use in potentially explosive atmospheres

[6] EN 15233: 2007 Methodology for functional safety assessment of protective systems for potentially explosive atmospheres

[7] EN 50495: 2010 Safety devices required for the safe functioning of equipment with respect to explosion risks