



# 中华人民共和国国家标准

GB/T 35320—2017/IEC 61882:2001

---

## 危险与可操作性分析(HAZOP 分析) 应用指南

Hazard and operability studies (HAZOP studies)—Application guide

(IEC 61882:2001, IDT)

2017-12-29 发布

2017-12-29 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 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 HAZOP 原理 .....	2
4.1 一般要求 .....	2
4.2 分析原理 .....	3
4.3 设计描述 .....	5
4.3.1 一般要求 .....	5
4.3.2 设计要求和设计意图 .....	5
5 HAZOP 应用 .....	5
5.1 概述 .....	5
5.2 与其他分析工具之间的关系 .....	6
5.3 HAZOP 的局限性 .....	6
5.4 系统生命周期不同阶段的危险辨识 .....	7
5.4.1 概述 .....	7
5.4.2 概念和定义阶段 .....	7
5.4.3 设计和开发阶段 .....	7
5.4.4 制造和安装阶段 .....	7
5.4.5 操作和维护阶段 .....	7
5.4.6 停用和废弃阶段 .....	7
6 HAZOP 分析程序 .....	7
6.1 分析程序的启动 .....	7
6.2 定义分析的范围和目标 .....	8
6.2.1 一般要求 .....	8
6.2.2 分析范围 .....	8
6.2.3 分析目标 .....	8
6.3 角色和责任 .....	8
6.4 准备工作 .....	9
6.4.1 一般要求 .....	9
6.4.2 设计描述 .....	10
6.4.3 引导词和偏离 .....	10
6.5 分析 .....	11
6.6 文档 .....	14
6.6.1 一般要求 .....	14

6.6.2	记录方式 .....	14
6.6.3	分析的输出 .....	14
6.6.4	报告要求 .....	14
6.6.5	签署文档 .....	15
6.7	跟踪和责任 .....	15
7	审核 .....	15
附录 A (资料性附录)	报告方法 .....	16
A.1	报告选择 .....	16
A.2	HAZOP 工作表 .....	16
A.3	HAZOP 分析报告 .....	17
附录 B (资料性附录)	HAZOP 示例 .....	18
B.1	介绍性实例 .....	18
B.2	操作规程 .....	22
B.3	自动列车保护系统 .....	25
B.3.1	应用 .....	25
B.4	在制定应急预案中的应用 .....	28
B.5	压电阀控制系统 .....	32
B.6	油品气化器 .....	36
参考文献	.....	40
图 1	HAZOP 分析程序 .....	3
图 2	HAZOP 分析程序流程图 .....	12
图 B.1	简化流程图 .....	18
图 B.2	车载 ATP 设备 .....	25
图 B.3	压电阀控制系统 .....	32
图 B.4	油品气化器 .....	36
表 1	基本引导词及其含义 .....	4
表 2	与时间和先后顺序相关的引导词及其含义 .....	4
表 3	偏离及其相应引导词的示例 .....	10
表 B.1	规范性示例节点设计意图表头 .....	19
表 B.2	介绍性示例的 HAZOP 记录表 .....	20
表 B.3	操作规程示例的 HAZOP 工作表 .....	23
表 B.4	自动列车保护系统 HAZOP 工作表示例 .....	26
表 B.5	应急预案 HAZOP 工作表示例 .....	29
表 B.6	压电阀控制系统设计意图示例 .....	33
表 B.7	压电阀控制系统 HAZOP 工作示例表 .....	34
表 B.8	油品气化器 HAZOP 工作表示例 .....	37

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 IEC 61882:2001《危险与可操作性分析(HAZOP 分析) 应用指南》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

- GB/T 7826—2012 系统可靠性分析技术 失效模式和影响分析(FMEA)程序(IEC 60812:2006, IDT)
- GB/T 2900.13—2008 电工术语 可信性与服务质量(IEC 60050(191):1990、Amend.1:1999 And Amend.2:2002, IDT)

本标准做了下列编辑性修改：

- 原国际标准正文中引用有 IEC 60050(191),但在规范性引用文件中未体现,现在国家标准规范性引用文件中添加了 IEC 60050(191)；
- 为符合实际需要,定义 3.1 添加注 2 说明；
- 原国际标准有误,图 1 中“文档和跟踪”将“6.6~7”改为“6.6~6.7”；
- 原国际标准 5.4 之下为悬置段,现添加编号为“5.4.1”,其后内容编号依次顺延；
- 为符合中文标准中流程图的要求,对图 2 的 a)和 b)中的线段、图框进行了部分修改；
- 原国际标准 6.2 之下为悬置段,现添加编号为“6.2.1”,其后内容编号依次顺延；
- 原国际标准表 B.1 无表编号,现添加表编号“B.1”,其后表编号依次顺延；
- 原国际标准表 B.6 无表编号,现添加表编号“B.6”,其后表编号依次顺延；
- 将表 B.2、B.3、B.4、B.7、B.8 中责任人列中的英文姓名用“成员 A、成员 B、成员 C、成员 D、成员 E、成员 F”等替代。
- 为符合标准中附录的提及对应要求,分别在标准正文中对附录 B,表 B.5,表 B.7,表 B.8,图 B.4 添加呼应内容。

本标准由中国机械工业联合会提出。

本标准由全国电工电子可靠性与维修性标准化技术委员会(SAC/TC 24)、全国工业过程测量和控制标准化技术委员会(SAC/TC 124)共同归口。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、中海油安全技术服务有限公司、中国石油天然气管道工程有限公司、中国安全生产科学研究院、北京联合普肯工程技术有限公司、上海撷果商务咨询有限公司、北京华清国诚安全技术有限公司、工业和信息化部电子第五研究所、上海黑马安全自动化系统有限公司。

本标准主要起草人:孟邹清、刘瑶、帅冰、唐彬、张文伟、顾峥、俞文光、周有铮、史学玲、聂中文、赵劲松、崔成志、朱平、刘瑞、李冬、赵建民、肖松青、吴宗之、杨胜松、许亚鹏、孙舒、赵俊丹、王怀义、刘森、刘映蓉、熊文泽、杨柳、游泽彬、史威、李秋娟。

## 引 言

本标准的目的是描述 HAZOP 分析的原理和步骤。HAZOP 是一种用于分析已确定系统的结构化和系统化的技术。它的目标是：

- 识别系统中潜在的危險。这些危險可能包括本质上只与系统现有区域有关的危險和有更大影响范围的危險,例如,某些环境危害。
- 识别系统中潜在的操作性问题,特别是识别操作性干扰的原因和可能导致不合格产品的生产偏离。

HAZOP 分析的重要作用是,通过结构化和系统化的方法辨识潜在危險与可操作性问题,获得的结果有助于确定正确的补救措施。

HAZOP 分析的一个显著特征是一种“检查会议”,会议期间由分析组长引导一个多专业小组,系统地检查一个设计或系统中所有相关部分。它利用一套核心的引导词来识别对系统设计意图的偏离。本技术的目标是用系统化的方式激发参与者的想象力以识别危險与操作性问题。HAZOP 宜被看成是采用基于经验的方法(例如标准规范而不是别的替代方法)来改进设计使之合理。

有许多不同的工具和技术可用于识别潜在的危險和可操作性问题,如检查表,故障模式和影响分析(FMEA),故障树分析(FTA)和 HAZOP 都属此类。某些方法,例如检查表法和“what-if(如果-怎样)”分析,可用于信息较少的系统生命周期早期阶段,或不需要详细分析的后续阶段。HAZOP 分析虽然需要较多的关于被评价系统的详细信息,但是能得到更加全面的在系统设计中有关危險和错误的信息。

术语“HAZOP”也经常被其他危险识别技术关联和引用(如:检查表式 HAZOP、HAZOP 1 或 2、基于知识的 HAZOP)。

在启动 HAZOP 分析之前,宜确认对现行的任务而言,HAZOP 是最合适的技术(单独使用或者与其他技术结合)。做这个判断时,应考虑分析的目的,任意后果可能的严重程度,细节的适当程度,以及相关数据和资源的可用性。

本标准已较成熟并为许多行业 and 不同系统的 HAZOP 分析提供了指导作用。在某些行业,还有更具体的标准和指南,特别是在该技术起源的过程工业,建立了适用于这些工业应用的首选危險分析方法。详细资料请参看本标准的参考文献。

# 危险与可操作性分析(HAZOP 分析) 应用指南

## 1 范围

本标准规定了应用本文件中定义的一套特定的引导词,系统地进行 HAZOP 分析的指南。它还给出 HAZOP 技术的应用和分析步骤的指导,包括定义、准备工作、分析会议和结果报告以及后续措施。

本标准还提供了包括不同工业、行业 HAZOP 应用的分析报告案例。

## 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。

IEC 60050(191) 电工术语 可信性与服务质量 (Electrotechnical terminology—Dependability and quality of service)

IEC 60300-3-9 可信性管理 第 3 部分:应用指南 第 9 节:技术系统的风险分析 (Dependability management—Part 3: Application guide—Section 9: Risk analysis of technological systems)

IEC 60812 系统可靠性分析技术 故障模式及影响分析(FMEA)程序 [Analysis techniques for system reliability—Procedure for failure mode and effects analysis(FMEA)]

IEC 61025 故障树分析 [Fault tree analysis(FTA)]

IEC 61160 设计评审 (Design review)

## 3 术语和定义

IEC 60050(191)界定的以及下列术语和定义适用于本文件。

### 3.1

#### **特性 characteristic**

对要素的定性或定量描述。

注 1: 特性的例子如压力、温度、电压等。

注 2: 在有些领域称之为参数。

### 3.2

#### **设计意图 design intent**

设计者期望的,或设定的要素和特性的行为范围。

### 3.3

#### **偏离 deviation**

设计意图的偏差。

### 3.4

#### **要素 element**

组成节点,用于识别节点的基本特征。

注: 要素的选择可能取决于特定的应用,但是要素可以包含例如有关的物质、执行的活动的、使用的设备等特征。物质应考虑为广义的物质,还应包括数据、软件等。

3.5

**引导词 guide word**

特定的词或短语,用于表达和定义设计意图的某一偏离。

3.6

**伤害 harm**

人身损伤、人的健康损害、财产的损失或环境的损害。

3.7

**危险 hazard**

伤害的潜在根源。

3.8

**节点 part**

被分析的系统的一部分。

注:一个节点可能是物理的(例如,硬件)或者逻辑的(例如,在一个操作步序中的步骤)。

3.9

**风险 risk**

伤害发生的概率与该伤害严重程度的综合。

## 4 HAZOP 原理

### 4.1 一般要求

HAZOP 分析是一个详细地识别危险和可操作性问题的过程,由一个分析团队来完成。HAZOP 包括辨识可能的设计意图偏离,分析这些偏离可能的原因,评估这些偏离的后果。

HAZOP 分析的主要特点包括:

- HAZOP 分析是一个创造性的过程。通过系统地应用一系列引导词来辨识潜在的设计意图的偏离,并利用这些偏离作为“触发器”,激励团队成员思考该偏离发生的原因以及可能产生的后果。
- HAZOP 分析是在一位训练有素、富有经验的分析组组长的引导下进行的。组长应通过逻辑性的、分析性的思维确保对系统进行全面分析。分析组长最好配有一名记录员,该记录员记录识别出的危险和(或)操作异常,以便进一步评估和决策。
- HAZOP 分析需要依赖具备适当的技术水平和经验的多个领域的专家来完成。这些专家要有好的直觉和判断能力。
- HAZOP 分析应在积极思考和坦率的讨论氛围中进行。当识别出一个问题时,做好记录以便后续的评估和决策。
- 对识别出的问题提出解决方案并非 HAZOP 分析的主要目标,但是一旦提出解决方案,做好记录供相关负责人考虑。

HAZOP 分析包括 4 个基本步骤,见图 1。

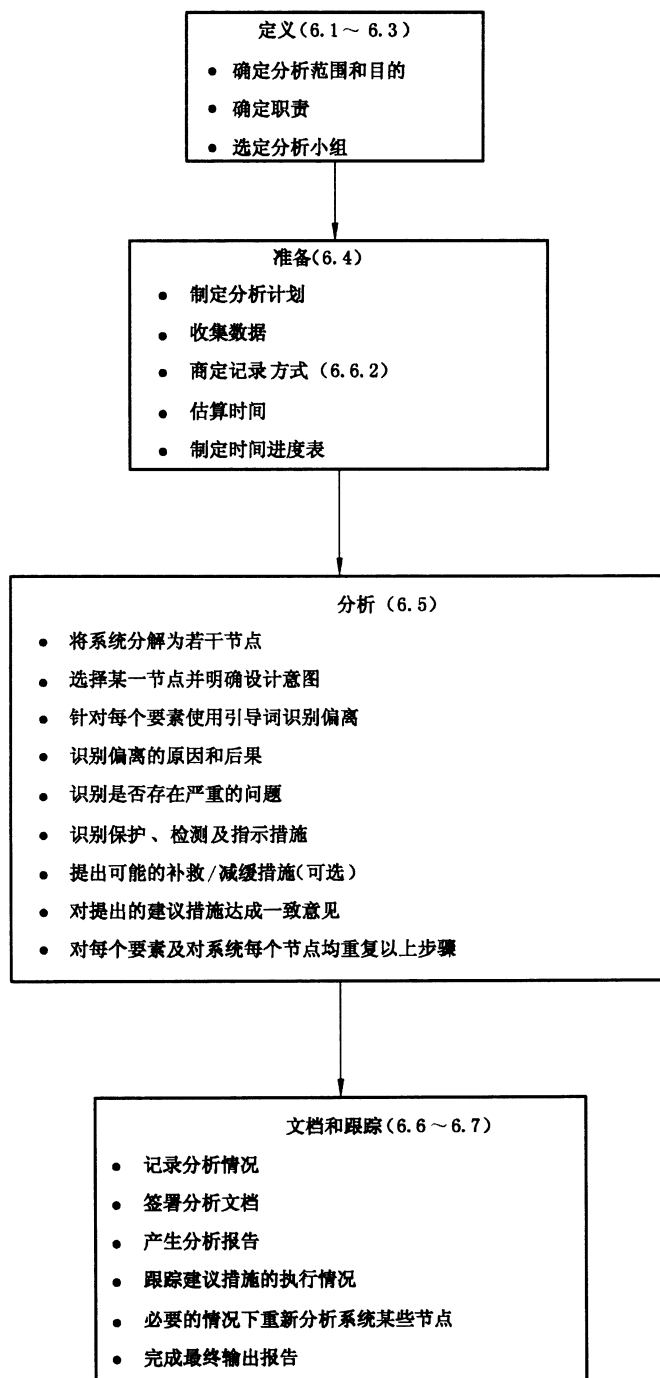


图 1 HAZOP 分析程序

## 4.2 分析原理

HAZOP 的基础是“引导词分析”，即仔细地查找与设计意图的偏离。为便于分析，可将系统分成若干节点，各个节点的设计意图应能充分定义。所选节点的大小取决于系统的复杂性和危险的严重程度。复杂度高或危险性高的系统可划分成若干较小的节点，简单的或低危险性系统可划分成若干较大的节点，以加快分析进程。系统中某个节点的设计意图通过若干要素来表达，这些要素表达了该节点的基本特性和自然的划分。分析要素的选择在某种程度上是一种主观决定，这是由于有多种组合方式都能实现要达到的分析目的。另外，要素的选择也可能取决于特定的应用。要素可能是一个程序中不连续的

步骤或阶段,或是控制系统中的单个的信号和设备元件,或是工艺或电子系统中的设备或零部件等。

有些情况下,可采用如下方式表达系统某一节点功能:

- 来源于某处的输入物料;
- 对该物料进行的某个操作(或活动);
- 送往某一目的地的输出物料。

因此,设计意图将包含以下要素:物料、动作、来源和目的地。

要素通常可通过定量或定性的特性做更明确的定义。例如,在一个化工系统中,“物料”要素可以通过温度、压力和成分等特性进一步定义。对于“输送”这个动作要素,可通过移动速率或承载物体的数量等特性定义。对基于计算机的系统,各节点的主要要素可能是信息,而不是物料。

HAZOP 团队逐个分析每个要素(及其相关的特性),以找出可导致不利后果的偏离。使用预先给定的“引导词”,通过提问的方式来识别设计意图的偏离。引导词的作用是激发分析人员的想象力,使其专注于分析,引发出讨论和各种想法,从而确保分析更完整。基本的引导词及其含义见表 1。

表 1 基本引导词及其含义

引导词	含义
无,没有	完全没有达到设计意图
多,过量	数量上的增加
少,减量	数量上的减少
伴随	性质上的变化(增多)
部分	性质上的变化(减少)
相反	与设计意图逻辑相反
异常	完全替代

另外,与时间和先后顺序相关的引导词及其含义见表 2。

表 2 与时间和先后顺序相关的引导词及其含义

引导词	含义
早	时间上早
晚	时间上晚
先	在顺序上提前
后	在顺序上推后

上述引导词有很多种解释。除上述引导词外,还可使用对偏离的辨识更有利的其他引导词。只要在分析开始前进行了定义,就可以使用这些引导词。在选定系统的某一节点进行分析之后,就要把该节点的设计意图分解为几个单独的要素。然后,将所有相关的引导词应用于每个要素,从而系统地全面地查找每个设计意图的偏离。之后,分析某个偏离可能的原因和后果,并识别出相应失效的检测和指示措施。按确定的格式,记录分析结果(见 6.6.2)。

可把引导词/要素的各种组合视为一个矩阵,其中,行可定义为引导词,列可定义为要素,所形成的矩阵中每个单元都是某个特定的引导词/要素组合。为达到全面地进行危险识别的目的,要素及其相关的特性应涵盖设计意图的所有相关方面,引导词应涵盖所有的设计意图偏离。并非所有的组合都会给

出有意义的偏离,因此,考虑所有引导词/要素的组合时,矩阵可能会出现空格。

矩阵中各单元的分析顺序有两种,一种是逐列,也就是要素优先;一种是逐行,也就是引导词优先。关于分析的详细内容见 6.5,两种顺序的分析见图 2a)和图 2b)。原则上,两种分析的结果应相同。

### 4.3 设计描述

#### 4.3.1 一般要求

对需分析的系统进行准确且全面的设计描述是完成 HAZOP 分析任务的先决条件。设计描述充分描述所分析的系统、节点和要素,并识别其特性。设计描述可以是对物理设计或逻辑设计的描述,描述内容应清晰。

设计描述宜以定性或定量的方式描述各节点和要素的系统功能。还应描述该系统和其他系统、操作者/用户以及可能与环境之间的相互作用。要素或特性与其设计意图的一致性决定了该系统运行的正确性,在有些情况下还决定了系统的安全性。

系统的描述包括两个基本方面:

- 系统的要求;
- 设计的物理描述和/或逻辑描述。

HAZOP 分析结果的质量取决于设计描述包括设计意图的完整性、充分性和准确性。因此,在准备信息资料时宜注意;如果在运行或废弃阶段进行 HAZOP 分析,宜确保系统的任何变更均体现在设计描述中。开始分析前,分析小组应再次审查信息资料。若有必要,宜修改相关信息资料。

#### 4.3.2 设计要求和设计意图

设计 requirements 是系统应满足的定性的和定量的要求,并作为系统设计和设计意图的依据。在设计要求中宜指明系统的用户所有合理使用情形和使用不当时的情形。设计要求和设计意图均应满足用户要求。

设计人员根据系统需求进行系统设计,即实现系统配置,分配子系统和组件的具体功能。要说明组件的规格,并选定组件。设计人员不仅宜考虑设备具有哪些功能,还宜确保设备在非正常条件下不会失效,或在规定的使用期限内不会损坏。宜辨识出异常的行为或特性,以便在设计中予以摒弃,或通过适当的设计降低其影响。上述信息为确定所要分析的各个节点的设计意图奠定了基础。

“设计意图”构成了 HAZOP 分析的基准,宜尽可能准确、完整。设计意图的验证(见 IEC 61160)虽然不在 HAZOP 分析的范围之内,但 HAZOP 组组长应确认设计意图的准确性和完整性,以便使 HAZOP 分析能够顺利进行。通常,多数设计文档中的设计意图局限于系统在正常运行条件下的基本功能和参数,而很少提及可能发生的非正常运行条件和异常的现象(如:可能引起失效的强烈振动、管道内的水击效应、浪涌等),但是这些非正常条件和异常的现象在分析期间都宜予以识别和考虑。此外,在设计意图中,不会明确说明造成材料性能退化的退化机理,如老化、腐蚀和冲蚀等。但是,在分析期间应使用合适的引导词对这些因素进行辨识和考虑。

假如 HAZOP 分析范围涵盖维修、检查、维护相关的活动,并且存在危险,那么在 HAZOP 分析时,预期寿命、可靠性、可维护性和维护支持建议同存在的危险一同被识别和考虑。

## 5 HAZOP 应用

### 5.1 概述

HAZOP 最初是针对流体介质或其他物料处理等过程工业的应用而开发的一种危险辨识技术。但

是近年来,它的应用范围逐步扩大,例如将 HAZOP 技术用于:

- 软件,包括可编程电子系统;
- 与人员运输相关的系统,如公路、铁路的运输系统;
- 分析各类操作程序和规程;
- 评价不同工业的管理规程;
- 评价特定的系统,例如医疗设备。

HAZOP 特别适用于识别系统(在役的或拟建的)的缺陷,包括物料流、人员流或数据流,或工序所包含的事件和活动,或一个程序控制序列。HAZOP 还是新系统设计和开发所需的重要工具,也可以有效地用于分析一个给定系统在不同运行状态下的危险和潜在问题,如:启动、备用、正常操作、正常关停和紧急关停等。HAZOP 不仅能运用到连续工艺流程,也可用于批处理和非稳态工艺流程和相关的位置。HAZOP 可视为是整个工艺流程的价值工程和风险管理活动中不可分割的一部分。

## 5.2 与其他分析工具之间的关系

HAZOP 可以和其他可靠性分析方法联合使用,如:FMEA(故障模式及影响分析,见 IEC 60812)和 FTA(故障树分析,见 IEC 61025)。这种联合使用方式也可用于下列情况:

- 当 HAZOP 分析明确表明设备某特定部件的性能至关重要,需要深入研究时,可采用 FMEA 对设备特定部件进行研究,对 HAZOP 分析进行补充;
- 在通过 HAZOP 分析完单个要素/单个特性的偏离后,可使用 FTA 评价多个偏离的影响,或使用 FTA 量化分析失效的可能性。

HAZOP 本质上是以系统为中心的分析方法,而 FMEA 是以部件为中心的分析方法。FMEA 由一个部件可能发生的故障开始,进而分析整个系统的故障后果,因此 FMEA 是从原因到后果的单向分析。HAZOP 分析的理念则不同,它是识别对设计意图的可能偏离,然后从两个方向进行分析,一个方向查找偏离的可能原因,一个方向推断其后果。

## 5.3 HAZOP 的局限性

尽管已证明 HAZOP 分析可用于不同工业领域,但该技术仍存在局限性,在考虑应用时需要注意:

- HAZOP 作为一种危险识别技术,它单独地分析系统各节点,并且系统地分析偏离对各节点的影响。有时,一个严重的危险会涉及系统内多个节点之间的相互影响。在这种情况下,需要使用事件树和故障树等分析技术对该危险进行更详细地研究。
- 与任何其他危险识别技术一样,HAZOP 分析也无法保证能识别所有的危险或可操作性问题。因此,对复杂系统的研究不宜完全依赖 HAZOP,而宜将 HAZOP 与其他合适的技术联合使用。在有效的、全面的安全管理系统中,将 HAZOP 与其他相关分析技术联合使用是必要的。
- 很多系统是高度关联的,某个系统产生偏离的原因可能源于其他系统。有些减缓措施从局部的角度上看起来是充分的,但不一定能消除真正的原因,甚至仍会导致事故。很多事故的发生是因为小的局部修改并未预见到对别处的影响。这种问题可以通过考虑偏离对其他节点的影响来解决,但实际上很少这样实施。
- HAZOP 分析的成功很大程度上取决于分析组长的能力和经验,以及小组成员的知识、经验和协作。
- HAZOP 仅分析出现在设计描述中的内容,无法分析设计描述中没有出现的行为和操作。

## 5.4 系统生命周期不同阶段的危险辨识

### 5.4.1 概述

HAZOP 分析是一种结构化的危险分析工具,最适用于在详细设计的后期对生产设施进行分析或者在现有设施做出变更时进行分析。以下详细介绍系统生命周期不同阶段 HAZOP 和其他分析方法的应用。

### 5.4.2 概念和定义阶段

系统生命周期中的这一阶段已经明确了设计构思和系统包含的主要部分内容,但引导开展 HAZOP 分析所需的详细设计和文档并未形成。然而,有必要在此阶段识别出主要危险源,以便在设计过程中加以仔细考虑,并有助于后续的 HAZOP 分析工作。为开展上述研究,宜使用其他的分析方法。(关于这些方法的描述,见 IEC 60300-3-9)

### 5.4.3 设计和开发阶段

在系统生命周期的这一阶段,详细设计工作已开展,并已确定操作原理,同时各种相关资料已经准备完成。设计工作趋于完备,并已基本成型。开展 HAZOP 分析的最佳时机恰好在设计完全成型之前。在此阶段,设计达到足够深度,便于通过 HAZOP 方法进行分析以得到好的结论。建立一个管理系统用于评估 HAZOP 分析完成后的任何变更非常重要,该系统应在系统整个生命周期都起作用。

### 5.4.4 制造和安装阶段

当系统调试和操作存在危险,同时操作的步序和指导又很关键时,或者在工程的后期有较大的设计变更时,在启动前建议进行 HAZOP 分析。此时,试运行和操作等数据资料应可用。此外,该分析还宜重新检查前期分析时发现的所有问题,以确保它们得到解决。

### 5.4.5 操作和维护阶段

对于那些影响系统安全、可操作性或影响环境的变更,宜考虑在变更前进行 HAZOP 分析。此外,宜有一个管理程序对系统进行定期检查,消除日常细微变更带来的影响。在本阶段进行 HAZOP 分析时,确保在分析中使用最新的设计文档和操作说明。

### 5.4.6 停用和废弃阶段

在本阶段可能发生正常运行时不会出现的危险,所以本阶段可能需要进行危险分析。如果存有以前的分析记录,则可迅速完成本阶段的分析。在系统整个生命周期中都宜保存好分析记录文件,以确保能迅速解决停用和废弃阶段出现的问题。

## 6 HAZOP 分析程序

### 6.1 分析程序的启动

该项分析应由对项目负有相关责任的人员启动,本标准则称为项目经理。项目经理宜决定何时需要分析并负责指定分析组长,提供分析必需的资源。根据相关法规或公司要求,通常在项目计划阶段确定何时开展 HAZOP 分析,项目经理应在分析组长帮助下确定该项分析的范围和目标。分析开始之前,宜指定具有适当权限的人员负责以确保根据分析确定的行动或建议得到落实。

## 6.2 定义分析的范围和目标

### 6.2.1 一般要求

分析的范围和目标密不可分,应当同时策划。对二者的描述应保证以下几点:

- 系统边界及与其他系统和外界的界面已被明确定义;
- 分析团队任务明确,不会分析与目标无关的范畴。

### 6.2.2 分析范围

取决于以下几个因素,包括:

- 系统的物理边界;
- 可获得的设计说明的详细程度;
- 系统已经完成的 HAZOP 分析或其他相关分析活动的范围;
- 其他适用于本系统的法规要求

### 6.2.3 分析目标

HAZOP 分析力求识别出所有导致各种后果或类型的危险和可操作性问题,但将 HAZOP 分析严格聚焦于危险问题更有利于在较短的时间内以较少的精力完成 HAZOP 分析。

目标定义时宜考虑以下因素:

- 分析结果的使用目的;
- 需要进行分析的生命周期阶段(详见 5.4);
- 可能面临风险的人员或资产,例如:员工,公众,环境和系统等;
- 可操作性问题,包括对产品质量的影响;
- 系统所要求的标准,包括安全和操作性能两个方面。

## 6.3 角色和责任

HAZOP 团队的角色和责任宜在本项目分析启动时就由项目经理明确定义,并与 HAZOP 分析组长达成共识。分析组长宜审核设计,以便确定需要收集的信息和资料,以及团队成员宜具备的技能。并制定里程碑形式的行动计划以确保相关建议得到及时落实。

分析组长确保建立有效的沟通机制传递 HAZOP 分析结果,项目经理确保 HAZOP 分析结论被跟踪,并且应确保设计团队对分析结论实施的决策和贯彻落实的情况形成有效文档。

项目经理和分析组长宜明确 HAZOP 团队的分析活动限定在危险和问题识别范围(然后由项目经理和设计团队解决),或者团队也可给出改进方案。如果是后者,则还需就确保有关改进方案的责任分配以及机制执行的适当授权达成一致。

HAZOP 分析是一种团队合作活动,组成团队的每一名成员都是需经过精心挑选并有明确的作用的成员。团队在确保包括相关的技术、操作技能和经验的人员足够的前提下宜尽可能的精干。一般是 4~7 人,团队越大行动越迟缓。如果是合同承包项目,HAZOP 小组中宜包含承包商和客户两方面的人员。

以下为建议的小组成员各角色职责要求:

- 分析组长:与设计团队和项目没有紧密关系。具备丰富的 HAZOP 分析活动经验并经过严格的训练,有能力和责任实现项目管理层和分析团队之间的沟通,制定分析计划,认同分析团队的构成,确保分析团队得到整体的设计资料,在分析过程中,给出需要使用的引导词,以及引导

词与要素/特性组合后的解释的建议,正确引导分析,确保分析结果有效存档。

- 记录员:记录会议过程,记录所有被识别的危险、问题,建议以及后续行动。协助分析组长制定计划并参与管理,有些时候,可由分析组长兼任。
- 设计者:负责解释设计意图,解释每一个被定义的偏离是如何发生的及相应的系统响应。
- 用户:负责解释分析要素操作的背景条件,可能出现偏离的程度以及偏离出现时对操作的影响。
- 专家:对系统和分析提出专业意见,可在需要时有限参与。
- 维护人员:维护人员代表(根据需要参与)。

开展分析时要充分考虑设计者和用户的观点意见。根据分析所处的生命周期不同,所需的专家类型有所变化。

所有的团队成员都宜有足够的 HAZOP 分析知识,确保他们有效的参与分析,或者经过适当的培训达到此要求。

## 6.4 准备工作

### 6.4.1 一般要求

分析组长应负责如下的准备工作:

- a) 获取信息;
- b) 将信息转化成适当的格式;
- c) 制定会议日程计划;
- d) 安排必要的会议。

此外,分析组长还需安排收集资料,并生成资料库,例如:收集同类或相似技术已经发生的事故。

分析组长保证能够获取最完整的可用设计资料,有遗漏或不完整的资料宜在分析开始前得到纠正。在分析的计划阶段,由熟悉设计的人员根据设计资料对节点、要素及特性进行识别。

分析组长负责准备一个分析计划,计划应包括如下内容:

- 分析目标和范围;
- 成员名单;
- 技术细节:
  - 设计描述分成节点和要素,并明确设计意图,对每一个要素列出部件、物料、活动以及特性清单;
  - 建议使用的引导词清单和引导词与要素/特性组合,参见 6.4.3;
- 一份适当的参考资料列表;
- 会务安排,会议日程,包括其日期、次数和地点;
- 要求的记录格式(参见附录 A);
- 要使用的分析模板。

会议室宜配备相应的会议设施、可视设备及辅助记录工具以保证会议有效进行。

应在首次会议前下发有关分析计划的简要说明和必要的参考资料,以便各个成员熟悉会议内容。要求参加者对下发资料进行审查。

HAZOP 分析的成功与否很大程度上取决于团队成员的洞察力和专注程度,因此确定会议合理的连续分析时间和保证各会议之间必要的时间间隔是十分重要的。这些要求在多大程度上得到满足最终将取决于分析组长。

### 6.4.2 设计描述

典型的设计描述可由以下设计文件组成,其内容应清晰无歧义,并经过审批及有明确的日期标注:

- a) 对于所有系统:
  - 设计要求和描述,流程图,功能块图,控制图,电路图,工程数据表,布置图,公用工程规格,操作和维修要求。
- b) 过程系统:
  - 管道和仪表流程图,材料规格和设备标准、管道和系统平面布置图。
- c) 可编程电子系统:
  - 数据流程图,面向对象设计框图,状态转换框图,时序图及逻辑图。

另外,宜提供如下信息:

- 分析对象的边界和在边界处的界面;
- 系统运行的环境;
- 操作和维修人员的资质,技能和经验;
- 程序和/或操作规程;
- 操作和维修经验和对类似系统的危险认知。

### 6.4.3 引导词和偏离

分析组长宜在 HAZOP 分析的计划准备阶段即给出引导词清单便于后续使用。分析组长宜检查在系统内使用这些引导词是否够用。引导词的选择应深思熟虑。引导词太具体和专业可能限制思路和讨论,但过于笼统则可能无法精确聚焦分析要点。表 3 给出了不同类型的偏离和与之相关的引导词的示例。

表 3 偏离及其相应引导词的示例

偏离类型	引导词	过程工业说明举例	可编程电子系统(PES)说明举例
负	无	完全没有达到设计意图,如无流量	未传递数据或控制信号
数量改变	多 少	数量增加,如过高温度 数量减少,如过低温度	数据传递速率高于期望 数据传递速率低于期望
性质改变	伴随 部分	出现杂质 同时执行另一个操作或步骤 仅部分达到意图,如期望的流体仅部分被传送	存在附加或虚假信号 数据或控制信号不完全
替代	反向 异常	管道内的反向流动或逆向反应 出现不同于原意图的结果,如输送了错误的物料	通常无关联 数据或控制信号不正确
时间	早 晚	早于规定时间发生,如冷却或过滤 晚于规定时间发生,如冷却或过滤	信号过早到达 信号过晚到达
顺序或步序	前 后	早于规定顺序发生,如混合或加热 晚于规定顺序发生,如混合或加热	在一个顺控中,信号过早到达 在一个顺控中,信号过晚到达

在分析不同系统,同一系统的不同生命周期阶段和应用于不同设计中时,同一引导词及其参数/特性组合其意义不尽相同,而对分析过程中的无意义的引导词组合建议被剔除。因此所有引导词及其相关要素/特性组合都要被明确定义并存档,如果某一组合在指定设计中有一种以上解释,则这些解释均建议被一一列出。相反,如果不同的组合具有同一含义,则应给出必要的交叉引用说明。

## 6.5 分析

分析会议在分析组长领导下按照分析计划组织开展。在 HAZOP 分析会议初期,分析组长或者熟悉待分析过程及其问题的小组成员应:

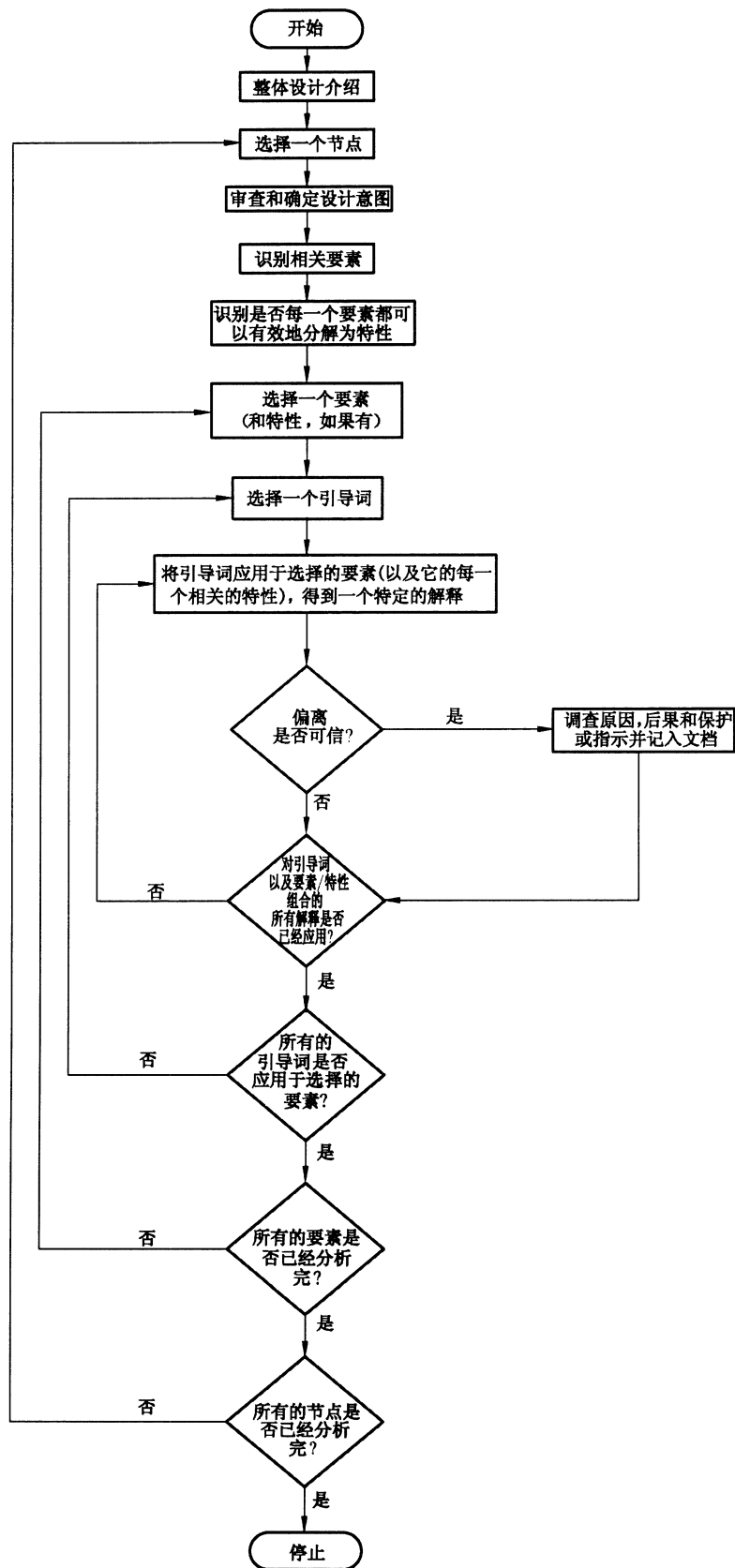
- 介绍分析计划,确保所有成员熟悉系统,分析目标和范围。
- 介绍设计描述和解释建议使用的要素及引导词。
- 审查已知的危险、可操作性问题及需关注的潜在方面。

分析按照被分析主题的流程或序列,按照设计逻辑从输入追踪到输出。HAZOP 危险识别技术要求按照程序化的单步审查过程追溯危险根源。目前有两种审查序列:要素优先和引导词优先,由图 2a)和图 2b)分别说明。其中要素优先序列如下:

- a) 由分析组长选择设计的某一节点作为分析起点并加以标注。然后说明该节点的设计意图,并识别与此节点相关的要素及其特性。
- b) 由分析组长选择出其中的某个要素,并根据团队意见决定引导词是应用于该要素本身还是应用于该要素的某个特性。并确认哪个引导词首先运用到这个要素上。
- c) 对首先选用的引导词和当前要素或特性组合的解释进行分析,以确定是否存在一个可信的对设计意图的偏离。如果识别出一个可信的偏离,则分析其可能的原因和后果。对某些应用来说,根据后果潜在的严重性或基于风险矩阵的风险分级对偏离进行分类是有用的,风险矩阵的使用将在 IEC 60300-3-9 中做进一步论证。
- d) 团队应识别出可能存在于现有节点内或其他节点的针对偏离的各种保护、检测及指示措施。这些可能存在于现有节点内或其他节点。现有的措施不应阻止小组发现或列出潜在危险或可操作性问题,以及不应阻止试图提出减少其发生的可能性或后果严重性的措施。
- e) 分析组长概括总结记录员记录存档的结果。如果需要后续工作,确保负责执行完成后续工作的人员名单被记录在案。
- f) 对该引导词的其他解释重复使用以上过程,然后其他引导词,然后要素的每一种特性(如果对该要素特性的分析已经得到一致认可),然后该节点的每一个要素。在完成对该节点的全面分析后,将该节点标注为完成。这个过程一直重复并持续下去直到顺利完成所有节点的分析工作。

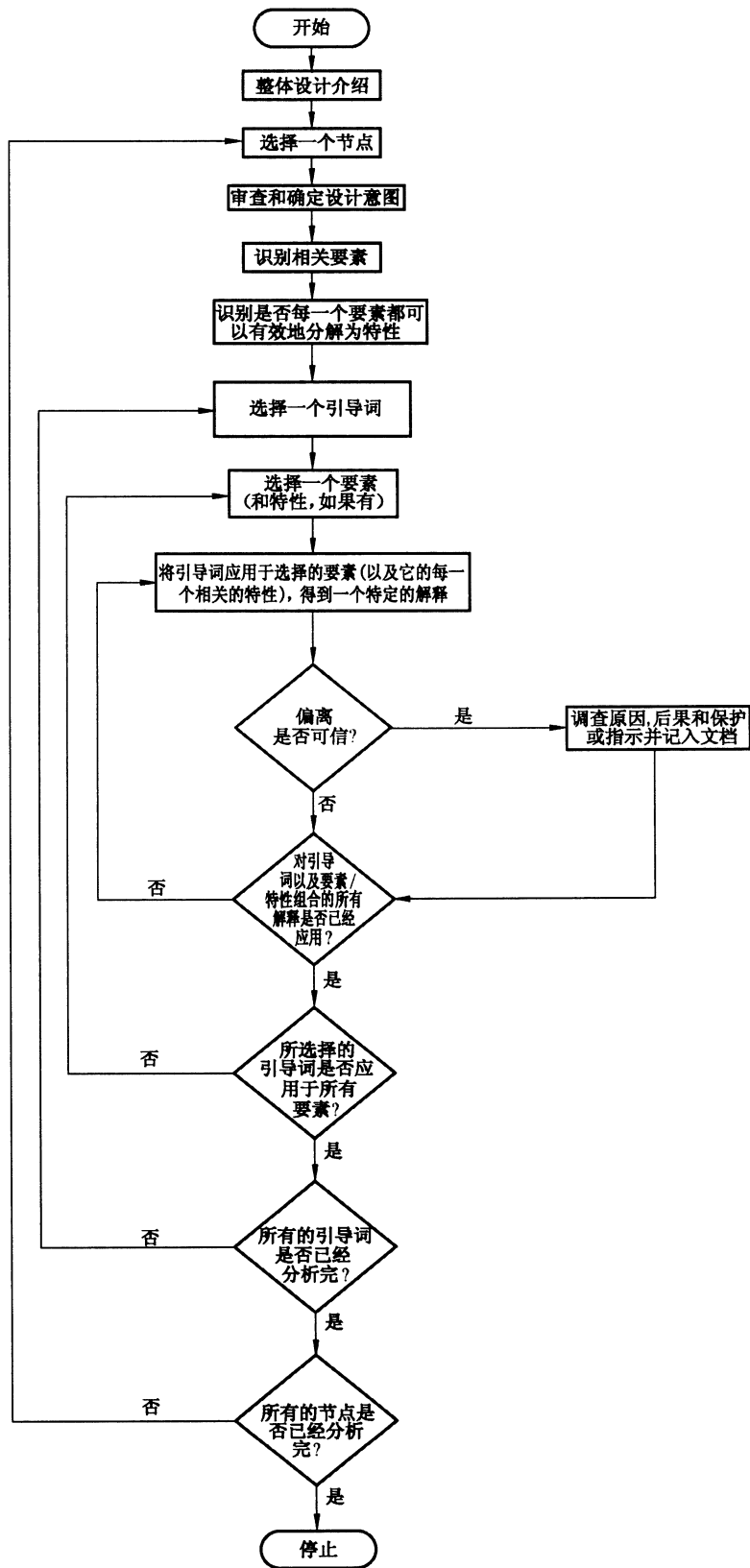
另一种方法是运用引导词针对上面描述内容开展分析,使用第一个引导词引导该节点中每一个要素依次进行,分析完成后再选下一个引导词重复以上分析过程。当前节点内所有要素轮流依照此方法开展分析,而后到下一个节点[见图 2b)]。

针对特定的分析,分析组长和小组应选择采用哪种分析步骤。具体根据实施 HAZOP 分析细节来定。其他影响因素还包括分析目标技术复杂程度,运用 HAZOP 方法的灵活程度,以及参加者的受训程度。具体 HAZOP 示例参见附录 B。



a) HAZOP 分析程序流程图-要素优先

图 2 HAZOP 分析程序流程图



b) HAZOP 分析程序流程图-引导词优先

图 2 (续)

## 6.6 文档

### 6.6.1 一般要求

HAZOP 的首要优势是系统的、规范的和文档化的分析过程。为了从 HAZOP 分析活动中能获得全面的益处,HAZOP 分析应正确的文档化和追踪,HAZOP 分析组长负责确保为每一个会议生成合适的记录,记录员应具备在被分析领域的技术知识和语言能力,以准确领会被关注的要点细节。附录 A 进一步讨论了可用的各种报告方法。

### 6.6.2 记录方式

记录方式应在会议开始前确定并告知记录员,HAZOP 的记录方式有全部记录和部分记录两种基本方式:

- 全部记录包括每一个节点或要素的每一种引导词和要素/特性组合的分析结果。这种方法虽然繁琐,但是分析较完整和彻底,可以通过最严格的审核。
- 而部分记录则仅仅记录被识别出的危险和可操作性问题及其相关的后续行动,部分记录的文档更容易管理。但是由于记录不完整,因此不利于审核,也容易导致今后重复同样分析。因而部分记录是最低要求,宜慎重选择。

选择报告格式考虑以下因素:

- 法规的要求;
- 合同义务;
- 企业规定;
- 可追溯和可审核的需求;
- 系统面临的风险等级;
- 可用的时间和资源。

### 6.6.3 分析的输出

HAZOP 分析输出宜包括:

- 被识别出的危险和可操作性问题的详细描述,以及其监测和/或减缓措施的详细描述;
- 如果必要,提出采用其他技术对相关部分进一步分析的建议;
- 对分析中发现的不确定问题宜采取的行动;
- 根据团队对此系统的了解提出改进问题的建议(如果属于小组职责范围);
- 需要备注在操作和维护规程中需注意的要点
- 列出每次会议的成员名单;
- 列出所有分析的节点清单,以及没有被分析节点的理由;
- 列出小组分析所用的图纸、说明书、数据表、报告等文件及版本号清单。

对于“部分记录”方式,这些输出一般会清楚简明的包含在 HAZOP 工作表里,而对于“全记录”方式,要求的输出需要从整个分析工作表中提炼。

### 6.6.4 报告要求

报告信息宜符合以下要求:

- 每一个危险和可操作性问题都宜作为单项记录;
- 无论系统中是否已有保护或报警,所有的危险和可操作性问题都宜和其发生的原因一起记录;
- 分析团队提出的每一个需要在会后解决的问题及其负责答复人的名字都宜被记录;

- 编号系统宜保证每一个危险、可操作性问题、提问建议等都有可识别的唯一编号；
- 分析文档宜归档以保证其在需要时可检索且在危险日志(如果有)中被引用。

准确地说,得到最终文档的人员名单宜按公司内部规定或相关法规要求决定,但一般宜包括项目经理,分析组长和保证后续行动或建议落实的相关责任人(见 6.1)。

#### 6.6.5 签署文档

分析报告在分析结束后宜产生并得到团队的一致通过。如果无法取得一致意见,宜注明理由。

#### 6.7 跟踪和责任

HAZOP 分析的目的不是重新设计一个系统。通常组长没有权利确保分析小组的建议得以实施。

在任何由 HAZOP 分析结果导致的重大更改被执行前,只要变更文档已形成,项目经理宜重新召集 HAZOP 团队开展工作以保证没有新的危险或可操作性或维修问题存在。

在如 6.3 所述相关情况下,项目经理可授权 HAZOP 分析团队执行建议和设计变更,此时 HAZOP 团队可完成以下附加工作:

- 小组对关键问题及修改设计或完善相关操作和维护规程达成共识;
- 确认各项修改和变更,进一步和项目管理层交换意见以获得批准;
- 组织进一步的包括系统界面在内的 HAZOP 分析。

注:最终输出报告至少包括如下文档信息:HAZOP 分析报告、建议措施执行跟踪情况报告、后续的必要的 HAZOP 分析报告及相关支持文件。

### 7 审核

HAZOP 分析的程序及结果可服从于公司内部的或监管机构的审核。审核的准则和问题可在公司运作程序中进行规定。这些可能包括人员、程序、准备、文档及跟踪。也宜包括技术方面彻底的检查。

**附 录 A**  
**(资料性附录)**  
**报告方法**

**A.1 报告选择**

可用的记录形式有多种,如:

- 只要满足清晰易读的基本要求,可在准备好的表格上进行手工记录,这种形式尤其适合小型项目的 HAZOP 分析。
- 可以在 HAZOP 分析会后,对手稿式的 HAZOP 记录进行文字的再处理,并生成质量良好的副本,供正式使用。
- 可在 HAZOP 分析会议期间,使用装有标准字处理或电子表格处理软件的便携式电脑,生成工作表。
- 可使用各种不同复杂程度的特定计算机软件,协助记录 HAZOP 分析结果。借助投影仪,使用特定的软件显示分析记录,有助于节省分析成本。

**A.2 HAZOP 工作表**

制定记录分析结果和跟踪结果的工作表单。不论采取何种报告形式,工作表单包括下文所述的基本特征以满足特定要求,表格样例在下文中给出。工作表的版面设计各有不同,取决于它是手工记录表还是电子化记录表。手工记录表通常包括表头和表列。

表头中可包括下列信息:项目名称、分析对象、设计意图、节点、小组成员、分析的图纸或文件、日期和页码等。

表列的标题可为以下各项:

a) 分析期间完成的内容:

- 1) 要素;
- 2) 引导词;
- 3) 偏离;
- 4) 原因;
- 5) 后果;
- 6) 需要采取的措施。

也可记录其他信息,如保护措施、严重程度、备注、风险等级等。

b) 在后续跟踪过程中完成的内容:

- 1) 建议措施;
- 2) 优先等级/风险级别;
- 3) 行动的负责人;
- 4) 完成状况;
- 5) 备注。

注:1)、2)和3)点提到的各栏内容也可以在会议期间完成。

电子化的报告便于更灵活地进行版面设计,更好地进行信息说明,更容易地准备所需的报告,如:

- 详细的工作表;

- 原因和(或)后果的报告;
- 后续跟踪报告(包含责任人和完成状态)。

使用现有的文字处理系统,可较容易地生成各个公司自己风格的报告。此外,多种商业化的软件包能简化数据记录和报告生成。这些软件包在协助记录员完成任务过程中,能够发挥作用。不过,有些软件通过使用预设的引导词-要素(或特性)组合而成的偏离列表,而不是采用把引导词和要素(或特性)直接组合产生偏离的方法。此作法试图取代 HAZOP 组长角色。尽管这些软件可以识别很多危险,能形成和人工 HAZOP 分析结果类似的输出结果,此做法与本标准所描述的 HAZOP 工作模式进行 HAZOP 分析相比,在危险的识别方面缺乏全面性及准确性。这些软件应用于连续化流程以外领域时,会受到限制。尤其需要指出的是,本标准不提倡使用软件完全代替分析组长。因此使用软件完全取代 HAZOP 分析组长的方法不能视为本标准定义的 HAZOP 分析。

### A.3 HAZOP 分析报告

编制 HAZOP 分析的最终报告,宜包括以下内容:

- 概要;
- 结论;
- 范围和目标;
- 逐条列出的分析结果(见 6.6.3);
- HAZOP 工作表;
- 分析中使用的图纸和文件清单;
- 在分析过程中用到的以往的 HAZOP 分析报告、基础数据等。

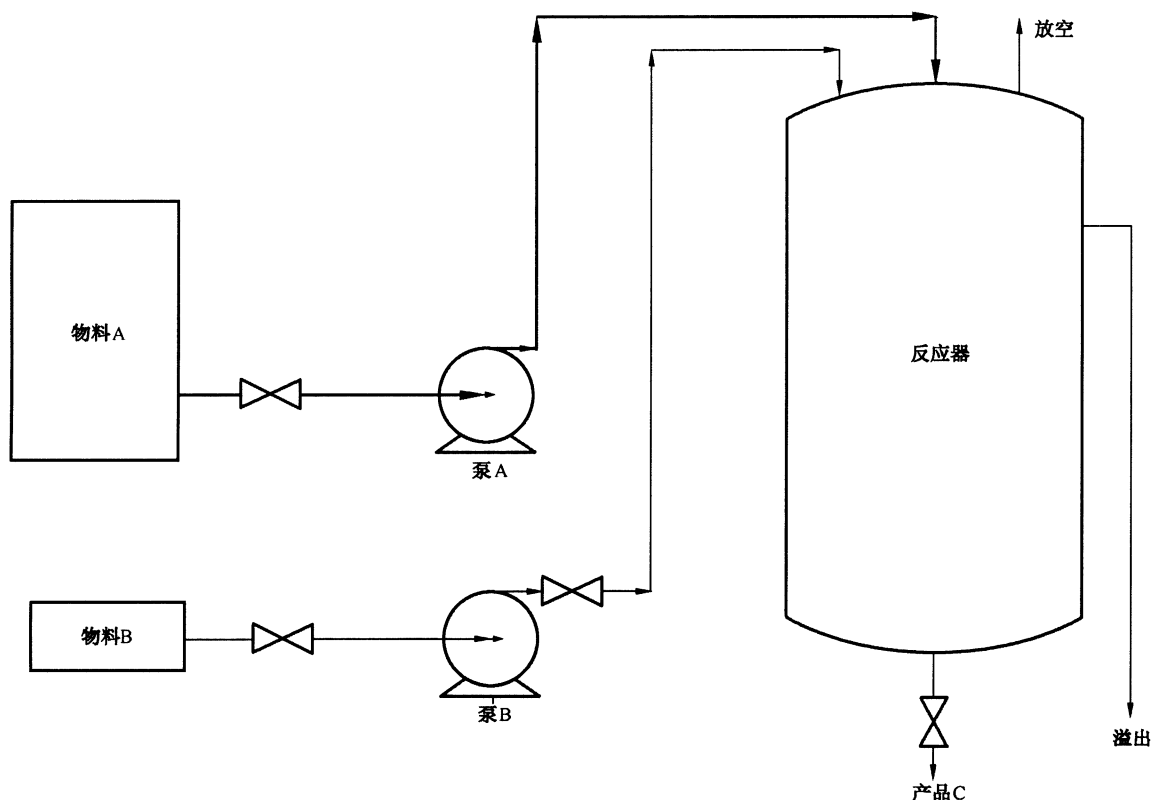
**附录 B**  
(资料性附录)  
**HAZOP 示例**

附录 B 包含的示例旨在举例说明本标准中描述的 HAZOP 分析原则(特别是 4.2、6.4 和 6.5)如何应用于不同行业和活动。注意,为达到举例说明的目的,各个示例已被大幅度简化。在任何情况下,这些示例都不具备实际案例分析的复杂性。还宜注意,此处仅提供示例的结果。

### B.1 介绍性实例

本示例的目的是介绍 HAZOP 分析方法的基本情况。本例选自一本关于 HAZOP 的出版物<sup>[1]</sup>。

假设一简单的工艺装置,如图 B.1 所示。物料 A 和物料 B 通过泵连续地从各自的供料罐输送至反应器,在反应器中合成并生成产品 C。假定为了避免爆炸危险,在反应器中 A 总是多于 B。完整的设计描述将包括很多其他细节,如:压力影响、反应和反应物的温度、搅拌、反应时间、泵 A 和泵 B 的匹配性等,但为简化示例,这些因素将被忽略。装置中待分析的部分用粗线条表示。



反应:  $A+B=C$

反应器中组分 A 必须总是多于组分 B,以避免爆炸。

**图 B.1 简化流程图**

节点是从物料 A 供料罐到反应器之间的管道,包括泵 A。这个节点的设计意图是连续地把物料 A 从罐中输送到反应器,且物料 A 的流速应大于物料 B。根据 4.2 建议的要素,设计意图表头可通过如表 B.1 所示给出:

表 B.1 规范性示例节点设计意图表头

物料	活动	来源	目的地
A	输送 (>B 速率)	物料 A 罐	反应器

将表 3 中列出的各个引导词(加上分析准备期间确定的其他引导词,见 6.4)依次用于这些要素,结果记录在 HAZOP 工作表中。“物料”和“活动”要素可能的 HAZOP 输出例子见表 B.2,其中,使用了“部分记录”方式,仅记录了有意义的偏离。在分析完与该节点相关的每个要素的每个引导词后,可以再选取另一节点(如:物料 B 的输送管路),重复该过程。最终,该系统的所有节点都会通过这种方式分析完毕,并对结果进行记录。

表 B.2 介绍性示例的 HAZOP 记录表

分析项目:过程示例									
表页:1/2									
图纸编号: 版本号: 日期:1998年12月17日									
小组成员: 成员 A、成员 B、成员 C、成员 D、成员 E、成员 F 会议日期:1998年12月15日									
节点: 从供料罐 A 到反应器的输送管道									
设计意图: 物料:A 活动:以大于物料 B 的输送速率连续输送 起始点:装有原料 A 的供料罐 终止点:反应器									
序号	引导词	要素	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
1	无	物料 A	无物料 A	A 供料罐是空的	没有 A 流入反应器;爆炸	无显示	此情况不可接受	考虑在 A 供料罐安装一个低液位报警,且液位低低联锁停泵 B	成员 E
2	无	输送物料 A (以大于输送 B 的速率)	没有输送物料 A	泵 A 停止;管路堵塞	爆炸	无显示	此情况不可接受	增加物料 A 流量的测量和流量报警,以及当 A 低流量时联锁停泵 B	成员 F
3	多	物料 A	物料 A 过量使罐溢出	当有足够的容量时,从槽车向罐中加料	物料从罐中溢出到围堰内	无显示	这应该在前面的罐的节点分析中被识别	如果先前罐节点分析中,这一风险没有被识别出来,考虑增加高液位报警	成员 C
4	多	输送 A	输送量过多;物料 A 流速增大	叶轮尺寸选错;泵选型不对	产量可能减少;产品中将含有过量的 A	无		在试车时测试泵的流量和特性; 修改试车程序;	成员 F
5	少	物料 A	物料 A 供料不足	A 供料罐液位低	不足的净吸压头; 可能引起汽蚀并导致爆炸; 流量不足;	无	同 1,此情况不可接受	同 1,在 A 供料罐安装一个低液位报警器	成员 E
6	少	输送物料 A (以大于输送 B 的速率)	A 的流速降低	管线部分堵塞;泄漏; 泵工作不正常	爆炸	无显示	此情况不可接受	同 2	成员 F

表 B.2 (续)

分析项目:过程示例									
表页:2/2									
图纸编号: 版本号:									
日期:1998年12月17日									
小组成员: 成员 A、成员 B、成员 C、成员 D、成员 E、成员 F									
会议日期:1998年12月15日									
节点: 从供料罐 A 到反应器的输送管道									
设计意图: 物料:A 活动:以大于物料 B 的输送速率连续输送									
起始点:装有原料 A 的供料罐 终止点:反应器									
序号	引导词	要素	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
7	伴随	物料 A	在供料罐中除了物料 A 还有其他物料	可能含有其他物质	未知	所有罐车装的物料在卸入罐前应接受检查和分析	此情况是可接受的	检查操作程序	成员 A
8	伴随	输送 A	输送 A 的过程中,可能发生冲刷、腐蚀、结晶或分解						成员 D
9	伴随	目的地反应器	外部泄漏	管线、阀门或密封泄漏	环境污染;可能爆炸		验收合格	将能联锁停车的流量传感器尽可能靠近反应器安装	成员 B
10	相反	输送 A	反向流动;原料从反应器流向供料罐	反应器压力高于泵出口压力	装有反应物料罐被返回的物料污染	无显示	情况不令人满意	考虑管线上安装一个止逆阀	成员 E
11	异常	物料 A	原料 A 错误;供料罐内物料不是 A 物料	供料罐内原料错误	未知,将取决于原料	所有罐车装的物料在卸入罐前应接受检查和分析	此情况可以接受		
12	异常	目的地反应器	外部泄漏;反应器无物料进入	管线破裂	环境污染;可能爆炸	管道完整性	检查管道设计	规定流量联锁停车应有足够快的响应以阻止发生爆炸	成员 E

## B.2 操作规程

下面是一个安全关键塑料元件的小批量生产过程。元件需要严格满足材料特性和颜色的质量要求。加工顺序如下：

- a) 取 12 kg 粉末“A”；
- b) 放入搅拌器；
- c) 取 3 kg 着色剂粉末“B”；
- d) 放入搅拌器；
- e) 启动搅拌器；
- f) 混合 15 min；停止搅拌器；
- g) 取出搅拌后的混合物，分成 3 包（每包 5 kg）；
- h) 清洗搅拌器；
- i) 向混合容器中加入 50 L 树脂；
- j) 向混合容器中加入 0.5 kg 硬化剂；
- k) 加入 5 kg 混合粉末（“A”和“B”）；
- l) 搅拌 1 min；
- m) 5 min 内把混合物倒入模具。

HAZOP 分析的目的是检查哪些步骤有可能造成产品不符合产品质量要求。因为 HAZOP 分析对象是一个操作步序，所以 HAZOP 节点即为相关的操作步骤。从步序的 HAZOP 分析报告选取的部分内容见表 B.3。本示例采用了“部分记录”。

表 B.3 操作规程示例的 HAZOP 工作表

分析题目：操作规程		版本号：		表页：1/2					
程序题目：X 元件的小规模生产		日期：							
小组成员：成员 A、成员 B、成员 C、成员 D		会议日期：							
节点：									
步骤 1：取 12 kg 粉末 A									
序号	要素	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
1	取粉末 A	无	没有取 A	操作失误	最终产品不合格	操作人员应注意到搅拌机中颗粒大小，颜色可能太亮	完全无物料 A 被认为是不可信的	无	
2	取粉末 A	伴随	和 A 一起添加了其他原料	原料 A 被杂质污染	颜色不合格，最终混合物不合格	使用前对所有供货商送达的原料 A 进行取样检验		检查供货商的质量保证程序	成员 A
3	取粉末 A	异常	取用了其他物料	操作人员取用了错误的物料	混合物不可用；导致财产损失；	仅把装有 A 和 B 的袋子放在操作区		每周检查物料保存是否规范；考虑对每种原料与混合产品使用不同颜色的包装袋；	成员 A
4	取 12 kg 粉末 A	多	取了过量的 A	称重错误/操作人员失误	产品颜色不合格	每周检查一次称重；每 6 月保养一次称重设备		成员 B 负责对操作人员强调精确称重的重要性	成员 B
5	取 12 kg 粉末 A	少	取了过少的 A	称重错误/操作人员失误	同上	同上		同上	成员 B
6	搅拌机	异常	原料 A 没有放在正确的容器内，而是放在了其他地方	操作人员失误		操作现场只有一台搅拌机		如果需要安装其他混合器，那么要对安装位置进行审查	成员 A

表 B.3 (续)

分析题目：操作规程										表页：2/2
程序题目：X 元件的小规模生产					版本号：					日期：
小组成员：成员 A、成员 B、成员 C、成员 D										会议日期：
节点：										
步骤 1：取 12 kg 粉末 A										
序号	要素	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人	
7	加硬化剂	无	未加入硬化剂	操作人员失误	最终混合物不合格；财产损失	操作人员应签署加料单以确保硬化剂已经加入；最后还要对浇铸强度进行检测		审查操作人员失误概率，看是否还需要其他安全措施	成员 A	
8	加硬化剂	伴随	其他物料同硬化剂一起加入	硬化剂被杂质污染	最终混合物不可用	供货商提供的质量保证书；对所有硬化剂进行取样检测		无		
9	加硬化剂	异常	加入的不是硬化剂而是其他物料		最终混合物不可用	不同硬化剂的物理隔离；操作人员检查	如果可行，订购提前做好并袋装的硬化剂，错误的几率会大大降低	等待新硬化剂订购结果；采购询问和审查	成员 B	
10	取 0.5 kg 硬化剂	多	加入了过多的硬化剂	称重错误/操作人员失误	产品组件过脆；可能导致完全失效。	每周检查一次称重；每 6 月保养一次称重设备	安全措施不够	调查获得 0.5 kg 预先称好的袋装硬化剂的可能性；对每一批交付产品进行取样检查	成员 B	
11	取 0.5 kg 硬化剂	少	加入了过少的硬化剂	同上	最终混合物不合格	同上	同上	同上	成员 B	

### B.3 自动列车保护系统

本节的目的是通过给出一个对系统框图级别进行 HAZOP 分析的典型的小例子来说明本标准中的若干要点。这个例子分为两部分：

- 对系统的一个简要描述和一个框图；
- 研究若干潜在的偏离的 HAZOP 工作表样例,采用“部分记录”的报告形式(见表 B.4)。

需注意的是,本例子中使用的系统的设计细节有限。设计与 HAZOP 工作表样例仅作为示意,而不是来自于实际系统。把它们包含在内只用于展示过程,而不保证完整。

#### B.3.1 应用

##### B.3.1.1 系统目的

本例涉及应用于自动列车保护(ATP)的车载设备。这是一种应用于很多地铁列车和一些干线列车上的功能。ATP 监测列车速度,并将该速度与列车预设的安全速度进行比较,如果识别出超速情况,将自动启动紧急制动。所有 ATP 系统都包含车载设备和将信息从轨旁传送到列车的轨旁设备。目前有很多种不同的 ATP 系统,只是在实现基本需求的方式细节上有区别。

##### B.3.1.2 系统描述

在列车上有一个或多个天线,用于接收轨旁设备发送的安全速度或停车点信息的信号。这些信息先经过一些处理,再传送到可编程电子系统(PES)。PES 的其他主要输入来自于转速计或其他测量实际列车速度的设施。PES 的主要输出是送到安全继电器的信号,例如用于控制紧急制动的信号。图 B.2 给出了系统的一个简单框图。

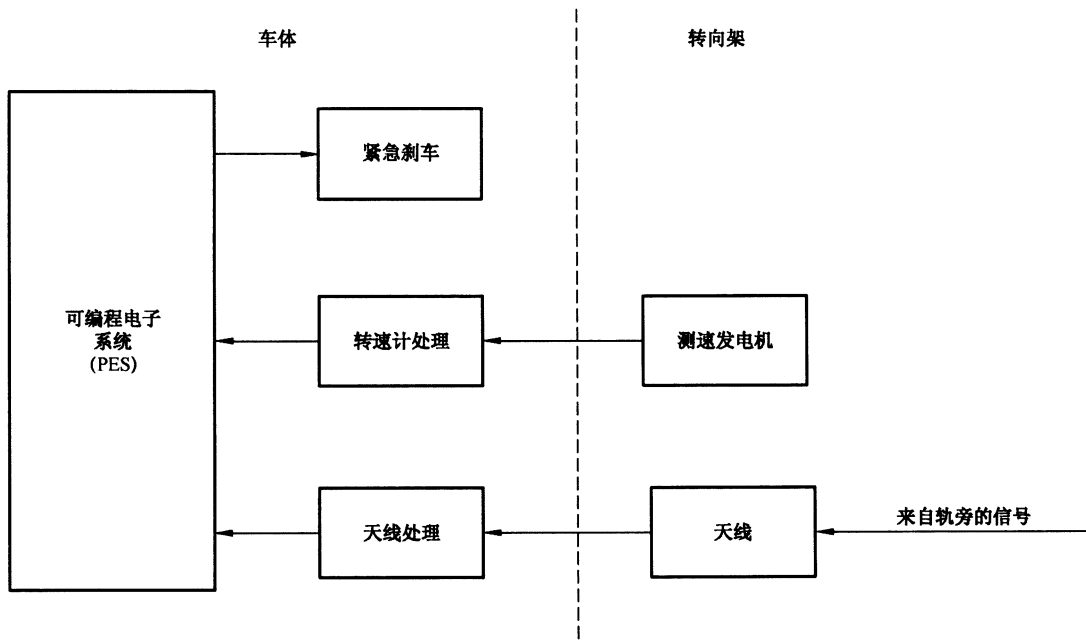


图 B.2 车载 ATP 设备

表 B.4 自动列车保护系统 HAZOP 工作表示例

分析题目:自动列车保护系统									表: 1/2	
参考图纸编号:ATP 框图					版本号:1			日期:		
小组成员:成员 A,成员 B,成员 C									会议日期:	
节点:				来自轨旁设备的输入						
设计意图:				通过天线向可编程电子系统(PES)提供安全速度和停车点信息的信号						
序号	要素	特性	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
1	输入信号	幅值	无	未检测到信号	发射机故障	在单独的轨旁设备分析中已考虑			审查轨旁设备分析的输出	成员 A
2	输入信号	幅值	多	大于设计幅值	发射机安装位置离轨道过近	可能损坏设备	安装过程中需执行的检查		安装过程中增加检查	成员 A
3	输入信号	幅值	少	小于设计幅值	发射机安装位置离轨道过远	可能丢失信号	同上		安装过程中增加检查	成员 A
4	输入信号	频率	异常	检测到不同的频率	接收到邻近轨道的信号	向处理器传送错误的值	目前无		检查是否需要对此采取保护措施	成员 A
5	天线	位置	异常	天线在错误的位置	安装支架故障	可能触碰轨道并被损坏	电缆需要应提供二次支撑		确保电缆能使天线不接触轨道	成员 B
6	天线	电压	多	电压大于预期值	天线与导电轨短路	天线和其他设备带电			检查是否有防止此情况发生的保护措施	成员 A

表 B.4 (续)

分析题目:自动列车保护系统									表: 2/2	
参考图纸编号:ATP 框图					版本号:1				日期:	
小组成员:成员 A,成员 B,成员 C									会议日期:	
节点:				来自轨旁设备的输入						
设计意图:				通过天线向可编程电子系统(PES)提供安全速度和停车点信息的信号						
序号	要素	特性	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
7	天线	输出信号	异常	发射不同的信号	接收到邻近电缆的杂散信号	错误的信号可能会被使用			确保对电缆干扰有充分的防护措施	成员 B
8	转速计	速度	无	未测到速度	车轮突然锁死	可能显示速度为零			检查对此情况的保护措施	成员 A
9	转速计	速度	异常	检测到错误的速度	锁死的车轮突然释放后发出混乱的信号	可能显示错误的速度			检查对此情况的保护措施	成员 C
10	转速计	速度	伴随	指示多个速度	车轮旋转导致的输出突变	可能根据错误的速度引发动作			检查此现象是否为实际问题	成员 C
11	转速计	输出电压	无	无输出	车轴锁死	可能显示速度为零			检查此现象的含义	成员 A
12	转速计	输出信号	伴随	输出信号混乱	混入其他信号	可能显示错误的速度			检查此现象是否是一个可信的故障	成员 C

#### B.4 在制定应急预案中的应用

组织需要制定应急预案以应对各种预期的紧急情况,这些紧急情况包括对炸弹威胁的反应、紧急电力供应或发生火灾时人员的逃离。这些应急预案的有效性和完整性能通过各种方式进行试验——通常是某种形式的演习。这种演习很有意义,但花费较大,且由于其自身性质,会中断正常的工作。在真实紧急情况下对应急系统进行测试的机会是很少的,甚至演习也不一定涵盖所有可能的情况。

HAZOP 分析能提供一种成本相对较低的方式,识别应急预案中可能存在的多种不足,以此来弥补缺乏演习或者紧急事件很少发生所导致的经验不足。HAZOP 分析方法在应急预案中的应用示例见表 B.5。

在海上油气平台上,为应对可能对生命构成威胁的事件,有必要提前做好疏散、撤离和救援(EER)的有效安排。这些安排旨在确保所有人员能够对危险形势迅速作出反应,并能快速撤离到安全的应急集合点,然后通过直升机或救生艇有控制地按先后顺序撤离平台,最后获得救援,并送往安全地方。有效的救援(EER)安排是整个海上设施系统必不可少的部分。在典型的救援(EER)计划中,通常有很多不同的阶段(要素)如:

- a) 通过仪表自动或操作人员手动发出报警(GPA);
- b) 将情况通报给当地守护船以及岸上应急服务机构;
- c) 人员沿着指定路线撤离到集合地点;
- d) 集合,包括现场人员登记;
- e) 穿戴救生设备等;
- f) 等待海上平台经理(OIM)或其代表发出“准备弃用平台警报”(PAPA);
- g) 人员从集合点前往所选撤离方法对应的出口;
- h) 通常通过直升机或特殊形式的救生艇撤离;
- i) 如果没有更好的撤退办法,就直接逃入海里逃生;
- j) 援救救生艇里的人员或那些直接进入海里逃生的人员,并前往安全之地。

表 B.5 应急预案 HAZOP 工作表示例

节点:报警系统									
设计意图:发出报警(GPA)信号									
要素: 输入:触发信号 电能									
人员: 起始点:所有报警发生器 终止点:平台上所有人员									
序号	要素	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
1	GPA 触发信号和电能	无	无报警信号	1) 仪表或操作人员未启动 GPA 2) 操作人员手动启动 GPA,报警器未运行 3) 没有电能	未能警告人员 同上 同上	无 双重连接; 故障安全模式,即“电流接通,弹簧关闭” 保持电源供应	不太可能,但是有可能性 不太可能 同上	无	
2		多	报警信号过多	1) 虚假性质的报警 2) 恶作剧性质的报警	人员收到不必要的警告 同上	无 纪律和守则	可能 不太可能	启动报警是否需要两个按钮? 无	
3	输入	多	过量电能	电能过载	损坏报警系统	专用电源保护	不太可能	无	
4		少	信号触发过少	触发信号仅到达部分报警器	某些人员未听到报警	报警器的例行检查		无	
5			电能不足	部分供电丢失	警报器可能不响	专用电源	不太可能	无	
6		伴随	伴随触发	触发其他动作		不可能存在于专门的硬接线电路中		无	

表 B.5 (续)

节点:报警系统									
设计意图:发出报警(GPA)信号									
要素: 输入:触发信号 电能									
人员: 起始点:所有报警发生器 终止点:平台上所有人员									
序号	要素	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
7			电能泄漏	错误的能量形式,如火花	可能造成损坏	有屏蔽的电源电路		无	
8		部分	部分报警器不响	有信号无电能或有电能无信号	某些人员未听到报警		上面均已考虑到		
9		相反	相反的输入相反的电能	报警条件反转没有任何建设性意义			系统不包括“解除警报”	开发“解除警报”系统	
10	输入	异常	有其他输入	多重输入	取决于输入的信号	不可能有专门的保护电路	可能需要现场试验系统	考虑耐高温电缆	
11	报警触发并传送人员	无	报警器未响	声音设备故障 电缆损坏	人员未听到警告	双扩声系统 双电缆 双电源 多声道扬声器	不太可能	无	
12		多	报警声音过大	音响设备功率过大	人员耳朵遭受损害	音响设备音量不能超过安全水平		无	
13		少	报警声音过小	声音太过微弱	部分人员未听到报警	无		确保系统提供超过背景噪音至少15 dB 以上的音量	

表 B.5 (续)

节点:报警系统									
设计意图:发出报警(GPA)信号									
要素: 输入:触发信号 电能									
人员: 起始点:所有报警发生器 终止点:平台上所有人员									
序号	要素	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
14		伴随	有其他报警声音	报警失真、泛音或回音	缺乏明确的信号	无		建议开展声学工程分析	
15		部分	部分报警器不响	警报传输有误	某些人员未听到报警		如上述报警声过小		
16		相反	反向报警传输				见“解除警报”的注释		
17		异常	报警声音异常(GPA报警未触发)	系统错误地发出“PAPA”信号	人员产生混乱,一些人可能错误地放弃平台	无		重新检查信号逻辑,使“PAPA”仅能在GPA报警后发出	
18		早	报警过早	过早启动GPA报警	产生不必要的报警,导致工作混乱	无		对平台上人员制定明确的指导方针	
19		晚	报警过晚	过晚启动GPA报警	有些人员可能被困或被迫使用其他的和不太理想的路线	无		同上	

**B.5 压电阀控制系统**

压电阀控制系统(见简化的图 B.3)介绍了如何将 HAZOP 应用于一个详细的电子系统(具体分析过程见表 B.7)。

压电阀是一种由压电陶瓷驱动的阀门。陶瓷元件受电力驱动,在充电状态下延伸。充电后的压电陶瓷会关闭阀门,而放电后的压电陶瓷会打开阀门。如果压电陶瓷没有失去或得到电荷,阀门的状态保持不变。

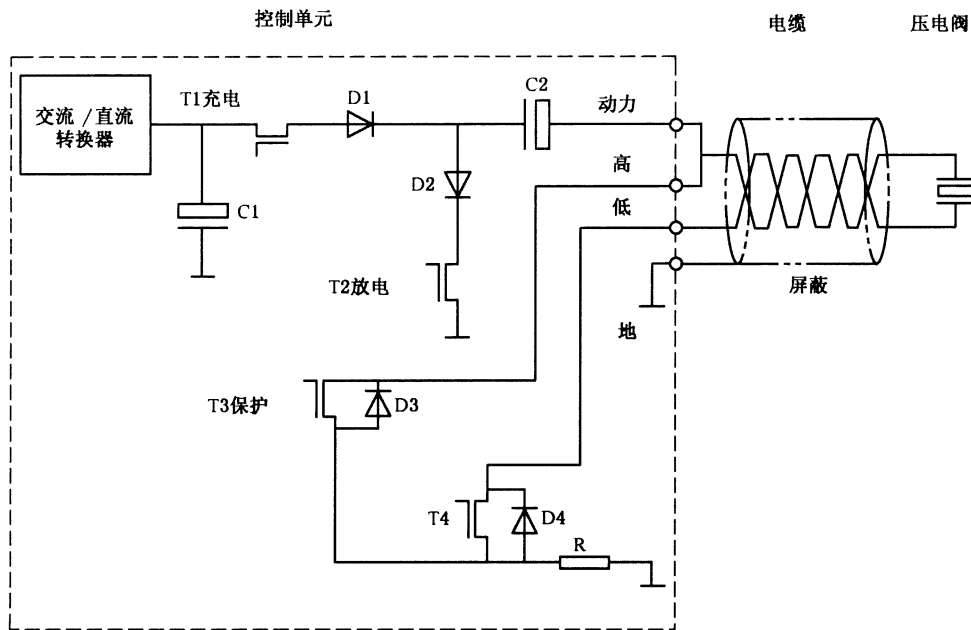
系统向一个反应容器(图中未显示)内喷入一种易燃易爆的液体。包括反应容器、管道和泵等在内的整个系统属于一个单独的 HAZOP 分析。这里只给出了对一个电子单元的 HAZOP 分析的使用。

该单元的操作设计为包含两种状态,需要关闭阀门时为“状态 1”,需要打开阀门时为“状态 2”。

电容器 C1 上的电荷通过晶体管 T1 传导到耦合电容器 C2,并通过动力线传导到压电阀以关闭阀门。此时晶体管 T2 和保护用晶体管 T3 都是断开的(高阻)。

通过晶体管 T2 对电容器 C2 放电打开阀门。为避免对阀门进行非对称的充电,例如受机械或热应力影响,晶体管 T4 将低侧接地。

电缆双绞线采用电气屏蔽以防止阀门受电磁干扰的影响。



**图 B.3 压电阀控制系统**

状态 1 描述:关闭阀门

考虑的部分:从交流/直流变换器和从电容器 C1 通过晶体管 T1、二极管 D1 和电容器 C2 到阀门动力侧的电缆,及从阀门接地侧通过晶体管 T4 和电阻器 R 到地的电缆。

状态 2 描述:打开阀门

考虑的部分:从阀门动力侧通过晶体管 T3、二极管 D3 和电阻器 R 到地的电缆。

设计意图如表 B.6 所示。

表 B.6 压电阀控制系统设计意图示例

输入	活动	来源	目的地
状态 1:关闭阀门 1.C1 充电	1.通过 T1、D1 和 C2 传送电荷	C1 和变换器	1.向阀门动力侧供电
特性: 电压 电容	2.通过 T4 和 R 传送电荷到地	阀门的低侧	2.低侧向地放电
2.到 T1、T3 和 T4 的控制信号	3.控制导通 T1 及控制 T4 对地导通 4.通过 T2 隔离 5.通过 T3 防止过充电	来自控制器的信号	T1、T3 和 T4 对地泄放过充的电荷
	6.通过 D2 防止电荷回流	阀门动力侧	
状态 2:打开阀门 1.阀门动力侧放电 特性: 电压 电容	1.通过 T1 隔离 C1 和变换器 2.通过 D2 和 T2 传送供电电荷 3.通过 D3、D4 和 R 传送阀门的任何电荷	阀门的动力侧和 C2	地
2.到 T1、T2 和 T4 的控制信号	4.通过 T4 隔离阀门的低充电侧	来自控制器的信号	T1、T2 和 T4

表 B.7 压电阀控制系统 HAZOP 工作示例表

分析项目:压电阀控制系统		表页:1/2						
图纸编号:		版本号:						
小组成员:开发工程师、系统工程师、质量经理		日期:						
节点:		会议日期:04.11.97						
状态 1:系统关闭阀门								
设计意图: 传输规定数量的电荷到压电执行器以在规定时间内关闭阀门								
要素	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
输入: C1 的电荷	无	无电荷;包括不传输电荷	供电中断 变换器故障 C1 故障 T1 永久断开 T2 永久导通 T1 故障 二极管 (D1、D3) 故障 - 二极管 D1 开路;无电流流过 - 二极管 D3 短路;经 D4 与阀门低侧短接或经 R 与地短接 C2 故障 断线 T4 故障 R 故障 T3 故障	没有电荷经过 C2 流入压电阀 阀门无法关闭; 永久打开 反应物质进入容器	无	该情况不可接受 需修改设计	上层报警 测试程序	责任人 B

表 B.7 (续)

分析项目:压电阀控制系统							表页:2/2	
图纸编号:				版本号:		日期:		
小组成员:开发工程师、系统工程师、质量经理							会议日期:04.11.97	
节点:		状态 1:系统关闭阀门						
设计意图:		传输规定数量的电荷到压电执行器以在规定时间内关闭阀门						
要素	引导词	偏离	可能的原因	后果	安全措施	注释	建议措施	责任人
输入: C1 的电荷	多	电荷多于规定数量	C2 充电过高 转换器故障 晶体管 T1 未及时断开 C2 故障 交流/直流变换器输出电压过高 晶体管 T1 未及时断开 保护用晶体管 T3 故障	压电阀早于规定时间关闭 压电阀损坏	流量计显示数值过高; 晶体管 T3 对压电阀放电; 未显示	该情况不可接受	考虑上层报警	责任人 A
C1 的电荷	少	电荷少于规定数量	电量不足 电缆绝缘故障;电荷消失 T1 断开过早 T2 部分导通	C2 电荷不足 阀门晚于规定时间关闭	无	该情况不可接受	报警	责任人 B
输入: C1 的电荷	伴随	T1 与 T2 均导通	C2 充电不足 阀门无法关闭 反应物质进入容器	失控的化学反应	未显示	小差异可能可接受	报警 测试程序 复位 定义可接受的差异	责任人 B

B.6 油品气化器

油品气化器由包含加热盘管和燃烧器的加热炉构成,加热炉的燃料为天然气(见简化的图 B.4)。

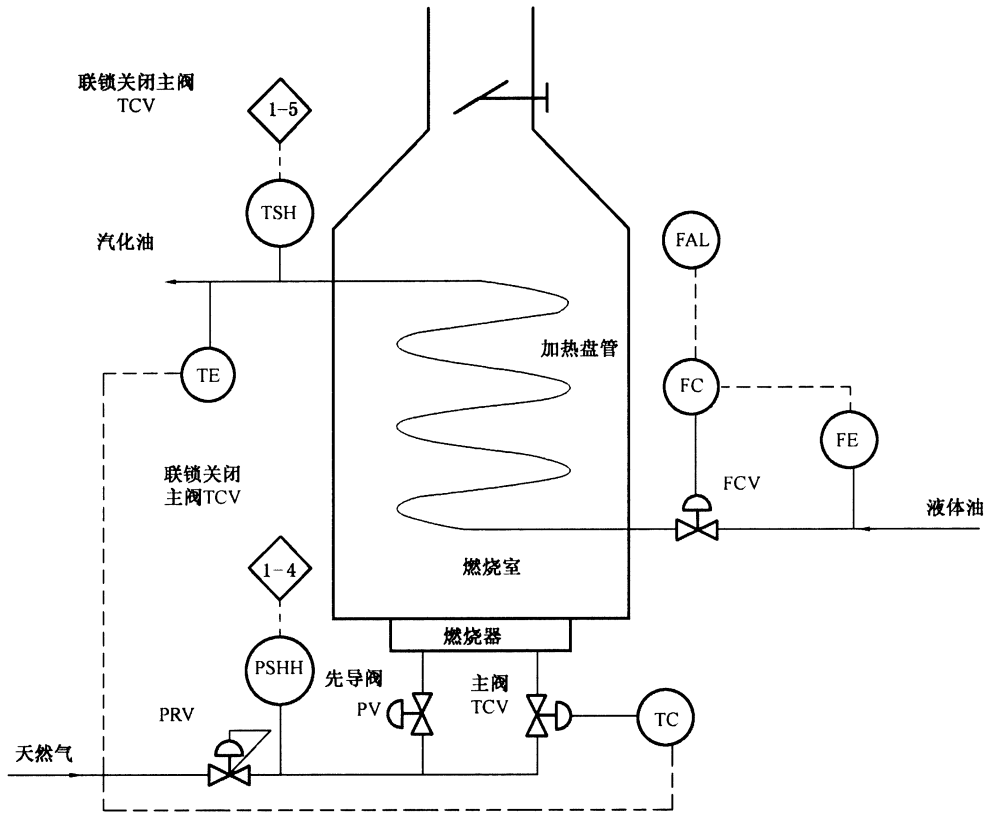


图 B.4 油品气化器

油以液态进入加热盘管,加热气化,离开加热盘管时成为过热油气。

天然气和外部的空气一起进入燃烧器,燃烧产生高温火焰。燃烧产生的烟气通过烟筒排出。

油的流量控制系统包括:流量控制阀 FCV、油流量检测元件 FE、流量控制器 FC 和低流量报警器 FAL(油量减少到一定程度会报警)。

天然气流经一个自力式减压阀 PRV,到达主燃烧器控制阀 TCV、长明灯减压阀 PV。主燃烧器控制阀是由温控器 TC 来控制,TC 接收温度检测元件 TE 的信号,TE 测量的是气化油出口温度。

在天然气管线上的高/高限压力开关 PSHH 参与联锁,如果天然气压力过高,将通过联锁功能块 I-4 关闭主燃烧器控制阀 TCV。如果超过最高允许温度,油出口高温开关 TSH 将通过联锁功能块 I-5 关闭主燃烧器控制阀 TCV。此外,还有一个火焰探测装置(图 B.4 中没有画出),在火焰熄灭时控制回路将自动关闭两个天然气阀门。

HAZOP 具体分析过程见表 B.8。

表 B.8 油品气化器 HAZOP 工作表示例

分析项目： 油品气化器									
图纸编号：					版本号：			日期：	
小组成员：成员 A、成员 B、成员 C、成员 D、成员 E								会议日期	
节点：从油入口（在流量测量前）到气化盘管，再到油气出口 （在温度控制后）					设计意图：输入：油由进料线流入，由加热炉加热 活动：气化，使其过热并将油气输送到后续流程				
序号	引导词	要素	偏离	可能的原因	后果	安全措施	备注	建议安全措施	责任人
1	无	油流量	无油流量	—— 供料系统故障； —— 流量控制阀 FCV 关闭	加热盘管过热并被损坏	低流量报警 FAL； 高温联锁停车 TSH	安全措施取决于操作人员的快速反应	考虑低流量 FE 联锁关闭主燃烧器控制阀 TCV	成员 A
				—— 盘管堵塞； —— 油品气化器出口被堵塞	油在气化器中沸腾； 可能过热并导致加热盘管结焦	低流量报警 FAL； 高温联锁停车 TSH			
2	无	加热	未加热	加热炉内火焰熄灭	未气化的液态油进入后续加工系统	无		—— 研究液态油对后续加工系统的影响； —— 考虑加热炉火焰熄灭联锁关闭 FCV； —— 考虑增加气化油出口温度低的报警	成员 B
3	大	油流量	油流量过大	—— 油压力过大； —— 流量控制器 FC 故障； —— FC 的设定值错误	气化器负荷过大，导致对油不能充分加热（见第 6 点）	无		—— 检查在高油压状态下，FCV 控制油流量的性能； —— 考虑增加气化油出口温度低的报警	成员 E
4	多	加热	加热过多	炉温过高	—— 加热盘管过热； 可能导致油管结焦、堵塞	高温联锁开关 TSH 关闭主燃烧器控制阀 TCV		审查燃料气流量控制的安全措施	成员 C

GB/T 35320—2017/IEC 61882:2001

表 B.8 (续)

分析项目：油品气化器									
图纸编号：					版本号：			日期：	
小组成员：成员 A、成员 B、成员 C、成员 D、成员 E								会议日期	
节点：从油入口（在流量测量前）到气化盘管，再到油气出口 （在温度控制后）					设计意图：输入：油由进料线流入，由加热炉加热 活动：气化，使其过热并将油气输送到后续流程				
序号	引导词	要素	偏离	可能的原因	后果	安全措施	备注	建议安全措施	责任人
4	多	加热	加热过多	炉温过高	——温度过高的油气输送到下游系统	高温联锁开关 TSH 关闭主燃烧器控制阀 TCV		检查油气温度过高对后续流程的影响	成员 B
5	小	油流量	油流量过小	油压力过小	与第 4 点相同	与第 1 点相同	安全措施足够	不必采取行动	
6	少	加热	加热不足	气化炉供热不足	可能导致油不能气化，或过热不足，去后续流程的气化油温度过低	无	考虑是否构成安全问题	检查油未气化或低温油对后续流程的影响	成员 B
								考虑增加气化油出口温度低报警	成员 C
7	伴随	油	油中含杂质	油混入杂质，例如： ——带水 ——固体、不挥发物、腐蚀物或不稳定组分	水快速沸腾可能会把液态油带入后续加工系统	无		检查油中可能存在的水分	成员 B
					可能导致盘管部分堵塞或全部堵塞（见第 1 点），积炭或腐蚀和泄漏（见第 11 点）	无		检查可能存在的杂质	成员 B

表 B.8 (续)

分析项目：油品气化器									
图纸编号：					版本号：			日期：	
小组成员：成员 A、成员 B、成员 C、成员 D、成员 E								会议日期	
节点：从油入口（在流量测量前）到气化盘管，再到油气出口（在温度控制后）					设计意图：输入：油由进料线流入，由加热炉加热 活动：气化，使其过热并将油气输送到后续流程				
序号	引导词	要素	偏离	可能的原因	后果	安全措施	备注	建议安全措施	责任人
8	相反	油流量	反向流动	进料中断，可能导致油蒸气从后续流程逆流至盘管和进油系统	可能导致进油系统过热并损坏进油系统	无		检查单元之间内部联系并考虑安装止逆装置	成员 B
9	异常	油	其他物质	错误地将其他物质输入蒸发器	不同的物质有不同的影响	前一工序的输入控制		检查控制措施是否合适	成员 C
10	异常	气化器	闪爆	天然气与空气的混合气被意外点燃	损坏气化器； 导致供油系统起火	气化器联锁装置等	安全措施可能不够	——考虑在供油系统安装火焰切断阀门； ——审查加热炉上防止爆炸的安全措施	成员 D
11	异常	油流量	油气 气化油流向 其他流程	——泄漏； ——盘管故障	持续的进料和油品倒流向炉膛提供燃料，导致炉膛持续着火； 释放浓烟； 可能损坏燃烧室	无		——考虑在供油系统安装火焰切断阀门； ——向炉内提供紧急灭火蒸汽； ——考虑在烟道中安装高温报警或联锁跳车装置以切断燃料气供应； ——确保对盘管进行常规检查	成员 D

参 考 文 献

- [1] A Guide to Hazard and Operability Studies.Chemical Industries Association, London, UK, (1977), 1992.
- [2] Das PAAG-Verfahren.International Social Security Association, (ISSA), c/o B.G.Chemie, heidelberg, Germany, 2000, ISBN 92-843-7037-X.
- [3] Storingsanalyse Waarom? Wanner? Hoe? Dutch Labour Inspectorate, 1979.Body of text in Dutch, appendices in English.
- [4] Kletz, Trevor A.HAZOP and HAZAN-Identifying and Assessing Chemical Industry Hazards, Institution of Chemical Engineers, Rugby, UK, 1999, ISBN 0-85295-421-2.
- [5] Knowlton, Ellis.An Introduction to Hazard and Operability Studies, The Guide Word Approach, Chemetics International, Vancouver, Canada, 1992, ISBN 0-9684016-0-0.(Also available in French, Spanish, Finnish, Arabic, Chinese, Hindi and Korean).
- [6] Knowlton, Ellis.A manual of Hazard & Operability Studies, The creative identification of deviations and disturbances.Chemetics International, Vancouver, Canada, 1992,ISBN 0-9684016-3-5.
- [7] Redmill, Felix; Chudleigh, Morris and Catmur, James.System Safety: HAZOP and Software HAZOP.Wiley, 1999, ISBN 0-471-98280-6.
- [8] Crawley, Frank; Preston, Malcolm and Tyler, Brian, HAZOP: Guide to best practice. Guidelines to best practice for the process and chemical industries.European Process Safety Centre, Chemical Industries Association & Institution of Chemical Engineers.Rugby, England, IChem, 2000, ISBN 0-85295-427-1.
- [9] Guidelines for Hazard Evaluation Procedures.Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA, 1999,ISBN 0-8169-0491-X.
- [10] Defence Standard 00-58, HAZOP Studies on Systems Containing Programmable Electronics, Ministry of Defence, Uk, 2000.
-