ICS 13.200
C 67
备案号：

AQ

中华人民共和国安全生产行业标准

AQ/T:3049—2013

危险与可操作性分析（HAZOP 分析）应用导则

Hazard and operability studies (HAZOP studies)–Application guide

(IEC 61882:2001, MOD)

2013-06-08 发布　　2013-10-01 实施

国家安全生产监督管理总局　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准使用翻译法修改采用国际电工委员会 IEC 61882:2001《Hazard and operability studies (HAZOP studies) –Application guide》《危险与可操作性分析（HAZOP 分析）应用导则》。本标准做了下列修改：

——删除原标准中的“特别声明”；

——对“IEC 引言”进行了部分修改，增加新的“引言”；

——在“范围”中增加了标准适用范围；

——将原文的“术语和定义”改为“缩略语和定义”，增加“略缩语”；对原文“术语和定义”中引用的 IEC 60050（191）调整到“规范性引用文件”中；

——在规范性引用文件中，用 GB/T 7826 代替 IEC 60812；用 GB/T 7829 代替 IEC 61025；

——增加了表 1“缩略语”，对原文中表的编号进行了重新编排；

——对表 3（原文表 2）的表头改为“与时间和先后顺序（或序列）相关的引导词及其含义”；

——对图 1 中的“6.1~3”改为“6.1~6.3”，“6.6~7”改为“6.6~6.7”；

——对附录 B.1 中第一个表增加了表头“表 B.1 设计目的”，对附录 B.5 中的第一个表增加了表头“表 B.6 状态 1 和状态 2 设计目的”，并对附录 B 中表的编号进行了重新编排。

本标准由国家安全生产监督管理总局提出。

本标准由全国安全生产标准化技术委员会化学品安全分技术委员会（SAC/TC 288/SC 3）归口。

本标准起草单位：中国石油化工股份有限公司青岛安全工程研究院、国家安全生产监督管理总局化学品登记中心、中国石化集团洛阳石油化工工程公司、国家石化项目风险评估技术中心。

本标准主要起草人：张海峰、牟善军、白永忠、党文义、武志峰、文科武、张广文、韩中枢、沈郁、万古军、于安峰、赵文芳。

引言

本标准的目的是描述危险与可操作性分析（Hazard and operability studies，以下简称HAZOP）的原则和程序。HAZOP采用结构化和系统化方式分析给定系统，目的是：

a) 识别系统中潜在的危险。这些危险既包括与系统临近区域密切相关的危险，也包括一些影响范围更广的危险，如某些环境危害；

b) 识别系统中潜在的可操作性问题，尤其是识别可能导致各种事故的生产操作失误与设备故障。

HAZOP分析的重要作用在于，通过结构化和系统化的方式识别潜在的危险与可操作性问题，分析结果有助于确定合适的补救措施。

HAZOP分析的特点是由各专业技术人员组成分析小组，以“分析会议”的形式进行。会议期间，在分析小组组长的引导下，使用一套核心引导词，对系统的设计进行全面、系统地检查，识别对系统设计意图的偏差。该技术旨在利用系统的方法激发参与者的想象力，识别系统中潜在的危险与可操作性问题。HAZOP应视为一种基于经验的方法，用于完善设计，而不是要取代其他的经验方法（如标准规范）。

识别潜在危险与可操作性问题有许多不同的工具和技术，包括检查表法(Checklist)、故障模式和影响分析（FMEA）、故障树分析（FTA）和HAZOP分析等。有些技术，如检查表法(Checklist)和“如果-怎么样(what-if)”分析，既能用于在所获信息较少时的系统生命周期早期，也能用于只需粗略分析的后期。虽然HAZOP分析需要更多的详细信息，却能更加全面地识别出给定系统的危险和设计缺陷。

通常，术语HAZOP常与某些其他危险识别技术相关联（如：检查表式HAZOP、HAZOP 1或2、基于知识的HAZOP）。这些技术术语的使用是不合适的，本标准不予考虑。

对当前任务，开始HAZOP分析前，应确认HAZOP分析是最合适的技术（单独使用或者与其他技术联合使用）。在做出此判断时，应考虑分析目的、后果的严重程度、细化程度以及相关数据和资源的可用性。

本标准从HAZOP的定义、分析步骤、在不同阶段的应用、分析过程中遇到的问题及解决思路等方面，对HAZOP进行了明确的规范和详细的描述，重点规定了HAZOP适用范围、分析原则、HAZOP应用、分析程序、报告要求、后续跟踪和审查等方面的技术要求。

本标准主要适用于石油、化工、电子等工业的 HAZOP 分析，也可作为各个行业制定 HAZOP 应用指南的通则。在某些行业，还有更具体的标准和指南，详细资料见本标准的参考文献。本标准的制定，可统一安全工作者对 HAZOP 方法内涵的认识，提高 HAZOP 技术应用水平，为国内各行业开展 HAZOP 分析提供技术指导，同时为 HAZOP 分析的规范化和标准化奠定基础。

危险与可操作性分析（HAZOP 分析）应用导则

1 范围

1.1 本标准规定了应用引导词对系统进行危险与可操作性分析（HAZOP 分析，下同）过程中的技术要求和 HAZOP 分析步骤，包括定义、准备、分析会议、结果记录及跟踪等。另外，本标准提供了 HAZOP 分析文档以及涵盖不同行业的 HAZOP 分析示例。

1.2 本标准适用于石油、化工、电子等工业的HAZOP分析。

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 7826 系统可靠性分析技术 失效模式和效应分析（FMEA）程序（GB/T 7826，IEC 60812，IDT）

GB/T 7829 故障树形图分析（GB/T 7829，IEC 61025，IDT）

IEC 60050（191） 国际电工词汇 第 191 章：可靠性和服务质量（International electrotechnical vocabulary: chapter 191: dependability and quality of service）

IEC 60300-3-9 可靠性管理－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 61160 设计审查（Formal design review）

3 缩略语和定义

3.1 缩略语

该导则使用的缩略语见表1。

表 1 缩略语

缩略语	全称	解释
IEC	International Electronic Commission	国际电工委员会
HAZOP	Hazard and operability studies	危险与可操作性分析
FMEA	Failure mode and effects analysis	故障模式和效应分析
FTA	Fault tree analysis	故障树分析
PID	Piping and instrumentation diagrams	管道和仪表流程图
PES	Programmable electronic system	可编程电子系统
ATP	Atuomatic train protection	列车自动保护
EER	Escape,evacuation and rescue	疏散、撤离和救援
GPA	General purpose alarm	通用报警
PAPA	Prepare to abandon platform alarm	准备弃用平台报警
OIM	Offshore installation manager	海上平台经理
FCV	Flow control valve	流量控制阀
FE	Flow element	流量检测元件
FC	Flow controller	流量控制器
PRV	Pressure-reducing valve	自力式减压阀
TCV	The main burner control valve	主燃烧器控制阀
PV	Pilot valve	导向阀
TC	Temperature controller	温控器
TE	Temperature element	温度检测元件
PSHH	High/high pressure switch	高高限压力开关

3.2 术语和定义

IEC 60050（191）中界定的定义，以及下列术语和定义适用于本文件。

3.2.1

特性 characteristic

要素的定性或定量性质。

注：如压力、温度和电压。

3.2.2

设计目的（意图） design intent

设计人员期望或规定的各要素及特性的作用范围。

3.2.3

偏差 deviation

设计目的（意图）的偏离。

3.2.4

要素 element

系统一个部分的构成因素，用于识别该部分的基本特性。

注：要素的选择取决于具体的应用，包括所涉及的物料、正在开展的活动、所使用的设备等。物料应取其广义，包括数据、软件等。

3.2.5

引导词 guide word

一种特定的用于描述对要素设计目的（意图）偏离的词或短语。

3.2.6

危害 harm

人员身体伤害、健康损害、财产损失或环境破坏。

3.2.7

危险 hazard

潜在的危害。

3.2.8

部分 part

当前分析的对象，该对象是系统的一个部分。

注：一个部分可能是物理的（如硬件）或者逻辑的（如操作步骤）。

3.2.9

风险 risk

危害发生的可能性和严重性的结合。

4 HAZOP分析原则

4.1 概述

HAZOP 分析是对危险与可操作性问题进行详细识别的过程，由一个小组完成。HAZOP 分析包括辨识潜在的偏离设计目的的偏差、分析其可能的原因并评估相应的后果。

HAZOP 分析的主要特征包括：

a) HAZOP 分析是一个创造性过程。通过应用一系列引导词来系统地辨识各种潜在的偏差，对确认的偏差，激励 HAZOP 小组成员思考该偏差发生的原因以及可能产生的后果。

b) HAZOP 分析是在一位训练有素、富有经验的分析组长引导下进行的，组长须通过逻辑分析思维确保对系统进行全面的分析。分析组长宜配有一名记录员，记录识别出来的各种危险和（或）操作扰动，以备进一步评估和决策。
c) HAZOP 分析小组由多专业的专家组成，他们具备合适的技能和经验，有较好的直觉和判断能力。
d) HAZOP 分析应在积极思考和坦率讨论的氛围中进行。当识别出一个问题时，应做好记录以便后续的评估和决策。
e) 对识别出的问题提出解决方案并不是 HAZOP 分析的主要目标，但是一旦提出解决方案，应做好记录供设计人员参考。

HAZOP 分析包括 4 个基本步骤，见图 1。

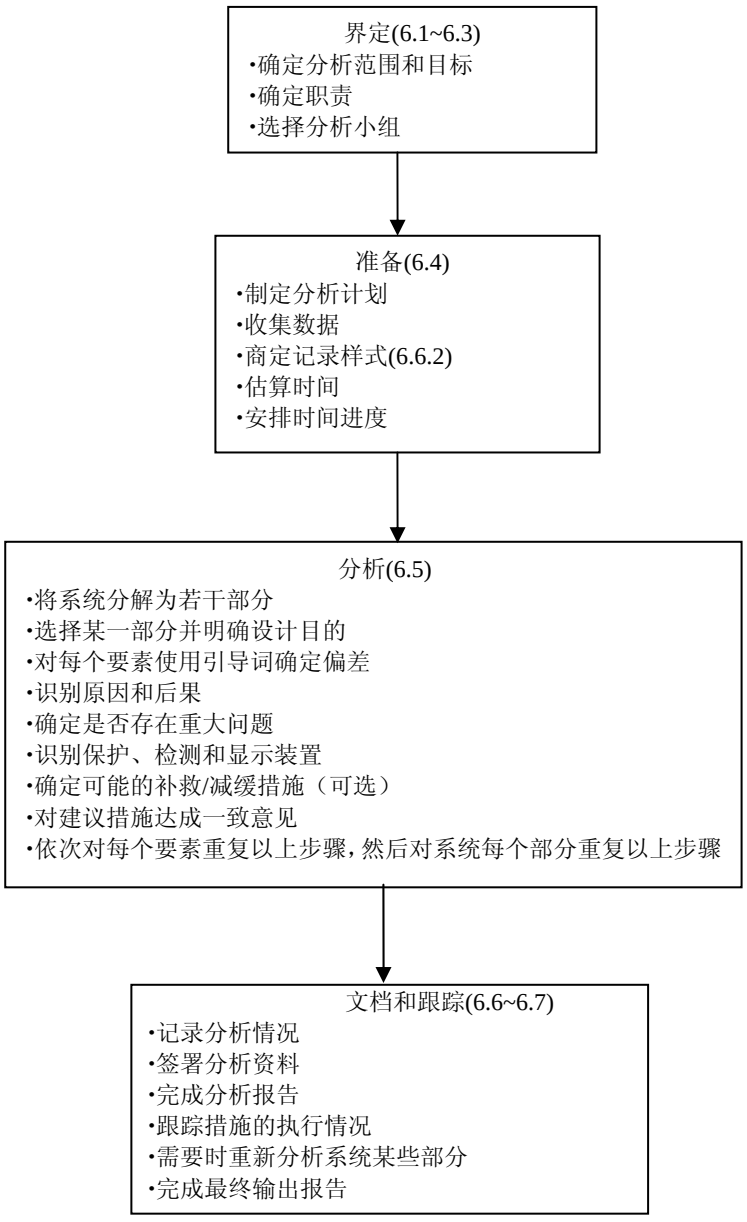


图 1　HAZOP分析程序

4.2　分析原则

HAZOP 分析的基础是“引导词检查”，它是对系统与设计目的偏差的缜密查找过程。为便于分析，可将系统分成多个部分，并充分明确各部分的设计目的。所选部分的大小取决于系统的复杂性和危险的严重程度。为加快分析进程，复杂或高危险系统可分成较小的部分，简单或低危险系统可分成较大的部

分。系统特定部分的设计目的可通过各种要素来表示，要素既代表了该部分的自然划分，也体现了该部分的基本特性。分析要素的选择在某种程度上是一种主观决定，为达到分析目的，可根据不同的应用目的选择不同的要素。要素可能是工艺程序中不连续的步骤或阶段，或是控制系统中的单独信号和设备元件，或是工艺过程或电子系统中的设备或零部件等。

有些情况下，可以用如下方式表示系统某一部分的功能：

a) 物料的输入；

b) 物料的处理；

c) 产物的输出。

因此，设计目的将包含以下要素：物料、生产活动以及可视为该部分要素的输入原料和输出产品。

要素常通过定量或定性的特性做更明确的定义。例如，在化工系统中，“物料”要素可以进一步通过温度、压力和成分等特性定义。对于“运输活动”要素，可通过行驶速率或乘客数量等特性定义。对基于计算机的系统，信息（不是物料）可作为各部分的要素。

HAZOP 小组使用预先确定的“引导词”，对每种要素（和相关的特性）进行分析，通过问询过程，识别并确认会导致不利后果的偏差。引导词的作用是激发分析人员的想象性思维，使其专注于分析，提出观点并进行讨论，从而尽可能使分析完整全面。基本引导词及其含义见表 2。

表 2 基本引导词及其含义

引导词	含义
无，空白（NO 或者 NOT）	设计目的的完全否定
多，过量（MORE）	量的增加
少，减量（LESS）	量的减少
伴随（AS WELL AS）	性质的变化/增加
部分（PART OF）	性质的变化/减少
相反（REVERSE）	设计目的的逻辑取反
异常（OTHER THAN）	完全替代

与时间和先后顺序（或序列）相关的引导词及其含义见表3。

表 3 与时间和先后顺序（或序列）相关的引导词及其含义

引导词	含义
早（EARLY）	相对于给定时间早
晚（LATE）	相对于给定时间晚
先（BEFORE）	相对于顺序或序列提前
后（AFTER）	相对于顺序或序列延后

上述引导词有多种解释。除上述引导词外，还可能有对辨识偏差更有利的其他引导词，这类引导词如果在分析开始前已经进行了定义，就可以使用。选定系统的一部分进行分析，将该部分的设计目的分为几个单独的要素。然后，将所有相关的引导词应用于每个要素，从而系统地完成对偏差的全面分析。运用一个引导词，分析某种偏差的可能原因和后果，也可以检查故障检测或显示装置。按确定的格式，记录分析结果（见 6.6.2）。

引导词/要素的组合可视为一个矩阵，其中，引导词定义为行，要素定义为列，所形成的矩阵中每个单元都是特定引导词/要素的组合。为全面进行危险识别，要素及关联特性应涵盖设计目的的所有相关方面，引导词应能引导出所有偏差。并非所有组合都会给出有意义的偏差，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。分析详情见 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 概述

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。设计描述应充分描述所分析的系统及其组成部分和要素，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，其描述内容应清晰。

设计描述应以定性或定量的方式表述各部分和要素的系统功能。此外，设计描述还应描述分析系统和其他系统、系统和操作者/用户、以及系统和环境的相互作用。系统各要素或特性与其原设计目的的一致性决定了系统操作的正确性，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：

a) 系统要求；

b) 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（包括设计目的）的完整性、充分性和准确性。因此，在准备信息资料时应注意：如果 HAZOP 分析在系统运行、停用和拆除阶段进行，应注意确保对体系所做过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，应进行修改。

4.3.2 设计要求和设计目的

设计要求是系统必须满足的定性和定量要求，是系统的设计目的和系统设计的依据。用户可能遇到的所有合理使用情形和误用情形都应予以识别。设计要求和最终设计目的应满足用户要求。

设计人员根据设计要求进行系统设计，即实现系统配置，分配子系统和组件的具体功能。组件可以是指定的或挑选的。设计人员不仅应考虑设备具有哪些功能，还应确保设备在非正常条件下不会失效，并在规定的使用期限内运行正常。应辨识出不安全行为或特性，以便在设计中予以排除，或通过适当的设计降低其影响。上述信息为确定待分析部分的设计目的提供了基础。

“设计目的”构成分析的基准，应尽可能准确完整。设计目的的验证（参见 IEC 61160）虽然不在 HAZOP 分析的范围之内，但分析组长应确认设计目的准确完整，使分析顺利进行。通常，设计文件中的设计目的叙述多局限于正常运行条件下系统的基本功能和参数，而很少涉及可能发生的非正常运行条件和不利的活动（如：强烈的振动、管道的水击、可能引发失效的电涌）。但是，在 HAZOP 分析期间，对这些非正常条件和不利活动应予以识别和考虑。此外，设计目的的描述中也未明确说明功能失效机理，如老化、腐蚀和侵蚀，以及造成材料特性失效的其他机理。但是，在 HAZOP 分析期间必须使用合适的引导词对这些因素进行识别和考虑。

系统预期使用年限、可靠性、可维护性、维修保障以及进行维护期间可能遇到的危险，只要它们在 HAZOP 分析的范围之内，也应予以识别和考虑。

5 HAZOP的应用

5.1 概述

HAZOP 技术最初是化学行业用来分析流体介质处理和物料输送中的安全问题所开发的技术。但是近几年，它的应用范围逐步扩大，例如：

a) 软件应用，包括可编程电子系统；

b) 人员输送系统，如公路、铁路；

c) 检查不同的操作顺序和操作程序；

d) 评价不同行业的管理程序；

e) 评价特定的系统，如医疗设备。

HAZOP 尤其适用于识别系统（现有或拟建）的缺陷，包括物料输送、人员流动或数据传输，按预定工序运行的事件和活动或该工序的控制程序。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：开车、备用、正常运行、正常停车和紧急停车等。HAZOP 不仅能运用到连续过程，也可用于间歇和非稳态过程及工序。HAZOP 可视为价值工程和风险管理整个过程不可分割的一部分。

5.2 与其他分析方法的关系

HAZOP 可以和其他可靠性分析方法联合使用，如：FMEA（失效模式和效应分析，参见 GB/T 7826）和 FTA（故障树分析，参见 GB/T 7829）。这种联合使用方式可用于下列情况：

a) 当 HAZOP 分析明确表明设备某特定部分的性能至关重要，需要深入研究时，采用 FMEA 对该特定部分进行研究，有助于对 HAZOP 分析进行补充；

b) 在通过 HAZOP 分析完单个要素/单个特性的偏差后，决定使用 FTA 评价多个偏差的影响或使用 FTA 量化失效的可能性。

HAZOP 本质上是以系统为中心的分析方法，而 FMEA 是以元件为中心的分析方法。FMEA 由一个元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，它是识别偏离设计目的的可能偏差，然后从两个方向进行分析，一个方向查找偏差的可能原因，一个方向推断其后果。

5.3 HAZOP的局限性

尽管已证明 HAZOP 在不同行业都非常有用，但该技术仍存在局限性，在考虑潜在应用时需要注意：

a) HAZOP 作为一种危险识别技术，它单独地考虑系统各部分，系统地分析每项偏差对各部分的影响。有时，一种严重危险会涉及系统内多个部分之间的相互作用。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。

b) 与任何识别危险与可操作性问题所用的技术一样，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应完全依赖 HAZOP，而应将 HAZOP 与其他合适的技术联合使用。在全面而有效的安全管理系统中，将 HAZOP 与其他相关分析技术进行协调使用是必要的。

c) 很多系统是高度关联的，某一系统产生某个偏差的原因可能源于其他系统。这时，仅在一个系统内采取适当的减缓措施可能不一定消除其真正的原因，事故仍会发生。很多事故的发生是因为一个系统内做小的局部修改时未预见到由此可能引发的另一系统的连锁效应。这种问题可通过从系统的一个部分的各种偏差对到另一个部分的潜在影响进行分析得以解决，但实际上很少这样做。

d) 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、经验和合作。

e) HAZOP 仅考虑出现在设计描述上的部分，无法考虑设计描述中没有出现的活动和操作。

5.4 系统生命周期不同阶段的危险识别研究

HAZOP 分析是一种结构化的危险分析工具，最适用于在设计阶段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。

5.4.1 概念和定义阶段

在系统生命周期的这一阶段，将确定设计概念和系统主要部分，但开展 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害，以便在详细设计过程中加以考虑，并有利于随后进行的 HAZOP 分析。为开展上述研究，应使用其他一些基本方法，（关于这些方法的描述，参见 IEC 60300-3-9）。

5.4.2 设计和开发阶段

在系统生命周期的这一阶段，形成详细设计，并确定操作方法，编制完成设计文档。设计趋于成熟，基本固定。开展 HAZOP 分析的最佳时机是在设计固定不变之前。在此阶段，设计信息足够详细，便于通过 HAZOP 问询方式得到有意义的答案。HAZOP 分析完成后，为评估系统设计变更对系统的影响，应建立系统设计变更管理系统。该系统应该在系统整个生命周期都起作用。

5.4.3 制造、安装和试运行阶段

如果系统试运行和操作有危险，或正确的操作步骤和说明至关重要，或后期阶段出现设计目的的较大变动时，建议在系统开车前进行一次 HAZOP 分析。此时，应结合试运行和操作说明等数据资料开展 HAZOP 分析。此外，HAZOP 分析还应重新检查早期分析时发现的所有问题，以确保它们得到解决。

5.4.4 生产和维护阶段

对于那些影响系统安全、可操作性或影响环境的变更，应考虑在变更前进行 HAZOP 分析。此外，应对系统进行定期检查，消除日常细微改动带来的影响。在进行 HAZOP 分析时，应确保在分析中使用最新的设计文档和操作说明。

5.4.5 停用和处理阶段

在本阶段可能发生正常运行阶段不会出现的危险，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，则可以迅速完成本阶段的分析。在系统整个生命周期都应保存好分析记录，以确保能迅速解决停用和处理阶段出现的问题。

6 HAZOP分析程序

6.1 分析启动

分析通常由项目负责人（本标准指项目经理）启动。项目经理应确定开展分析的时间，指派 HAZOP 分析组长，并提供开展分析必需的资源。由于法律规定或用户政策要求，通常在正常的项目计划期间已确定需要开展此类分析。在 HAZOP 分析组长的协助下，项目经理应明确分析的范围和目标。分析开始前，项目经理应指派具有适当权限的人负责确保分析得出的建议或措施得以执行。

6.2 确定分析范围和目标

分析范围和目标互相关联，应同时确定。两者应有清晰的描述，以确保：

a) 明确系统边界，以及系统与其他系统和周围环境之间的界面；
b) 分析小组注意力集中，不关注与分析范围和目标无关的区域。

6.2.1 分析范围

分析范围取决于多种因素，主要包括：

a) 系统的物理边界；
b) 可用的设计描述及其详细程度；
c) 系统已开展过的任何分析的范围，不论是 HAZOP 分析还是其他相关分析；
d) 适用于该系统的法规要求。

6.2.2 分析目标

通常，HAZOP 分析追求识别所有危险与可操作性问题，不考虑这些问题的类型或后果大小。将 HAZOP 分析的焦点严格地集中于辨识危险，能够节省精力，并在较短的时间内完成。

在确定分析目标时应考虑以下因素：

a) 分析结果的应用目的；
b) 分析处于系统生命周期的哪个阶段（见 5.4）；
c) 可能处于风险中的人或财产，如：员工、公众、环境、系统；
d) 可操作性问题，包括影响产品质量的问题；
e) 系统所要求的标准，包括系统安全和操作性能两个方面的标准。

6.3 分工和职责

安排 HAZOP 分析工作时，项目经理应明确规定 HAZOP 小组的分工和职责，并得到 HAZOP 分析组长的同意。HAZOP 分析组长应检查设计，确定可用的项目信息和 HAZOP 分析小组成员所需的技能。分析组长应制定项目 HAZOP 活动计划，做好项目进度安排，确保 HAZOP 各项建议能及时执行。

分析组长负责建立一个适当的交流机制，用于传递 HAZOP 分析的结果。项目经理负责对分析结果进行跟踪调查，并对设计小组的执行决策结果进行妥善存档。

项目经理和分析组长应确定 HAZOP 分析是仅限定于识别危险和问题（这些问题随后将反馈给项目经理和设计团队进行解决），还是 HAZOP 分析需要提出可能的补救/减缓措施。若是后一种情况，需要协定以下两方面的责任和机制：

a) 补救/减缓措施的优先选择；
b) 采取行动的适当授权。

HAZOP 分析需要小组成员的共同努力，每个成员均有明确的分工。只要小组成员具有分析所需要的相关技术、操作技能以及经验，HAZOP 小组应尽可能小。通常一个分析小组至少 4 人，很少超过 7 人。小组越大，进度越慢。当系统由承包商设计时，HAZOP 小组应包括承包商和业主两方的人员。

小组成员的分工建议如下：

a) 分析组长：与设计小组和本工程项目没有紧密关系；在组织 HAZOP 分析方面受过训练、富有经验；负责 HAZOP 小组和项目管理人员之间的交流；制定分析计划；同意分析小组的人员构成；确保有足够的设计描述和资料提供给分析小组；建议分析中使用的引导词，并解释引导词-要素/特性；引导分析；确保分析结果的记录。
b) 记录员：进行会议记录；记录识别出的危险和问题、提出的建议以及进行后续跟踪的行动；协助分析组长编制计划，履行管理职责；某些情况下，分析组长可兼任记录员。
c) 设计人员：解释设计及其设计描述。解释各种偏差产生的原因以及相应的系统响应。

d) 业主（用户）：说明分析要素的操作环境、偏差的后果、偏差的危险程度。
e) 专家：提供与系统和分析相关的专业知识。可邀请专家协助分析小组进行部分分析。
f) 维护人员：维护人员代表（若需要）。

HAZOP 分析通常需要考虑设计者和业主（用户）的观点。然而，在系统生命周期不同阶段，适合 HAZOP 分析的小组成员可能是不同的。

对 HAZOP 小组的人员应进行 HAZOP 培训，使 HAZOP 小组所有成员具备开展 HAZOP 分析的基本知识，以便高效地参与 HAZOP 分析。

6.4 准备工作

6.4.1 概述

HAZOP 分析组长负责以下准备工作：

a) 获得系统信息；
b) 将信息转换成适当的形式；
c) 计划 HAZOP 会议的顺序；
d) 安排必要的 HAZOP 会议。

此外，分析组长可以安排人员对相关数据库进行查询，收集采用相同或相似的技术出现过的事故案例。

HAZOP 分析组长负责确保具有可用的、充分的系统设计描述。如果设计描述有缺陷或不完整，分析开始前应进行修正补充。在分析的计划阶段，熟悉系统设计的人应在设计描述中确定系统各个部分、要素及其特性。

分析组长负责制定 HAZOP 分析计划，应包括以下内容：

a) 分析目标和范围；
b) 分析成员的名单；
c) 详细的技术资料：
——设计描述，该设计描述按照明确的设计目的将分析对象划分为多个部分和要素，对于每个要素，具有构成元件、物料和活动及它们特性的清单；
——建议引导词的清单，以及引导词-要素/特性组合的解释（参见 6.4.3 概述）；
d) 参考资料的清单；
e) 管理安排、HAZOP 会议日程，包括日期、时间和地点；
f) 要求的记录形式（见附录 A）；
g) 分析中可能使用的模板。

应提供合适的房间设施、可视设备及记录工具，以便会议有效地进行。

第一次会议前，宜对分析对象开展现场调查，分析组长应将包含分析计划及必要参考资料的简要信息包分发给分析小组成员，便于他们提前熟悉内容。

HAZOP 分析的成功很大程度上依赖于小组成员的机敏和专注度，因此，分析组长应负责限制每节 HAZOP 会议持续时间以及安排适当的会议时间间隔。

6.4.2 设计描述

通常，设计描述文件是下列具有清晰且唯一的审批签署和日期标识的文件：

a) 对于所有系统：
- 设计要求和描述、流程图、功能块图、控制图、电路图表、工程数据表、布置图、公用工程说明、操作和维护要求；

b) 对于过程流动系统：
- 管道和仪表流程图（P&ID）、材料规格和标准设备、管道和系统的平面布置图；

c) 对于可编程的电子系统：
- 数据流程图、面向对象的设计图、状态转移图、时序图、逻辑框图。

此外，也应提供如下信息：

- 分析对象的边界以及各个边界的分界面；
- 系统运行的环境条件；
- 操作和维护人员的资质、技能和经验；
- 程序和（或）操作规程；

- 操作和维护经验、类似系统存在的已知危害。

6.4.3 引导词和偏差

在 HAZOP 分析的计划阶段，HAZOP 分析组长应提出要使用的引导词的初始清单。分析组长应针对系统所提出的引导词进行验证并确认其适宜性。应仔细考虑引导词的选择，如果引导词太具体可能会影响审查思路或讨论，如果引导词太笼统可能又无法有效地集中到 HAZOP 分析中。不同类型的偏差和引导词及其示例见表 4。

引导词-要素/特性组合在不同系统的分析中、在系统生命周期的不同阶段以及当用于不同的设计描述时可能会有不同的解释。有些组合在既定系统的分析中可能没有意义，应不予考虑。应明确并记录所有引导词-要素/特性组合的解释。如果某组合在设计中有多种解释，应列出所有解释。另一方面，有时会出现不同的组合具有相同的解释。在这种情况下，应进行适当的相互参考。

表 4 偏差及其相关引导词的示例

偏离类型	引导词	过程工业实例	可编程电子系统实例（PES）
否定	无，空白（NO）	没有达到任何目的，如：无流量	无数据或控制信号通过
量的改变	多，过量（MORE）	量的增多，如温度高	数据传输比期望的快
	少，减量（LESS）	量的减少，如温度低	数据传输比期望的慢
性质的改变	伴随（AS WELL AS）	出现杂质 同时执行了其他的操作或步骤	出现一些附加或虚假信号
性质的改变	部分（PART OF）	只达到一部分目的，如：只输送了部分流体	数据或控制信号不完整
替换	相反（REVERSE）	管道中的物料反向流动以及化学逆反应	通常不相关
	异常（OTHER THAN）	最初目的没有实现，出现了完全不同的结果。如：输送了错误物料	数据或控制信号不正确
时间	早（EARLY）	某事件的发生较给定时间早，如：冷却或过滤	信号与给定时间相比来得太早
	晚（LATE）	某事件的发生较给定时间晚，如：冷却或过滤	信号与给定时间相比来得太晚
顺序或序列	先（BEFORE）	某事件在序列中过早的发生，如：混合或加热	信号在序列中比期望来得早
	后（LATE）	某事件在序列中过晚的发生，如：混合或加热	信号在序列中比期望来得晚

6.5 HAZOP分析

按照 HAZOP 分析计划，组织分析会议，在分析组长领导下组织讨论。HAZOP 分析会议开始时，分析组长或熟悉分析系统的过程及问题的小组成员应进行以下工作：

a) 概述 HAZOP 分析计划，确保 HAZOP 分析成员熟悉系统以及分析目标和范围；
b) 概述系统设计描述，解释会议中要使用的分析要素和引导词；
c) 审查已知的危险和操作性问题及潜在的关注区域。

分析应沿着与分析主题相关的流程或顺序，并按逻辑顺序从输入到输出进行分析。HAZOP 等危险识别技术的优势源自规范化的逐步分析过程。分析顺序有两种：“要素优先”和“引导词优先”，分别见图 2 a）和图 2 b）。“要素优先”顺序可描述如下：

a) 分析组长选择系统设计描述的某一部分作为分析起点，并做出标记。随后，解释该部分的设计目的，确定相关要素以及与这些要素有关的所有特性。
b) 分析组长选择其中一个要素，与小组商定引导词应直接用于要素本身还是用于该要素的单个特性。分析组长确定首先使用哪个引导词。
c) 将选择的引导词与分析的要素或要素的特性相结合，检查其解释，以确定是否有合理的偏差。如果确定了一个有意义的偏差，则分析偏差发生的原因及后果。有些应用中会发现，按照后果的潜在严重性或根据风险矩阵得到的相对风险等级对偏差进行分类是有用的。风险矩阵的使用在 IEC 60300-3-9 中有进一步论述。
d) 分析小组应识别系统设计中对每种偏差现有的保护、检测和显示装置（措施），这些保护措施可能包含在当前部分或者是其他部分设计目的的一部分。在识别危险或可操作性问题时，不应考虑已有的保护措施及其对偏差发生的可能性或后果的影响。
e) 分析组长应对记录员记录的文档结果进行总结。当需要进行相关后续跟踪工作时，也应记录完成该工作的负责人的姓名。
f) 对于该引导词的其他解释，重复以上 c)~e)过程；然后依次将其他引导词和要素的当前特性相结合，进行分析；接着对要素的每个特性重复 c)~e)过程（前提是对要素当前特性的分析达成了一致意见）；然后是对分析部分的每个要素重复 b) ~e)过程。一个部分分析完成后，应标记为“完成”。 重复进行该过程，直到系统所有部分分析完毕。

引导词应用的另一种方法是将第一个引导词依次用于分析部分的各个要素。这一步骤完成后，进行下一个引导词分析，再一次把引导词依次用于所有要素。重复进行该过程，直到全部引导词都用于分析部分的所有要素，然后再分析系统下一部分，见图 2 b）。

在进行某一分析时，分析组长及其HAZOP小组成员应决定选择“要素优先”还是“引导词优先”。HAZOP分析的习惯会影响分析顺序的选择。此外，影响这一决定的其他因素还包括：所涉及技术的性质、分析过程需要的灵活性以及小组成员接受过的培训。

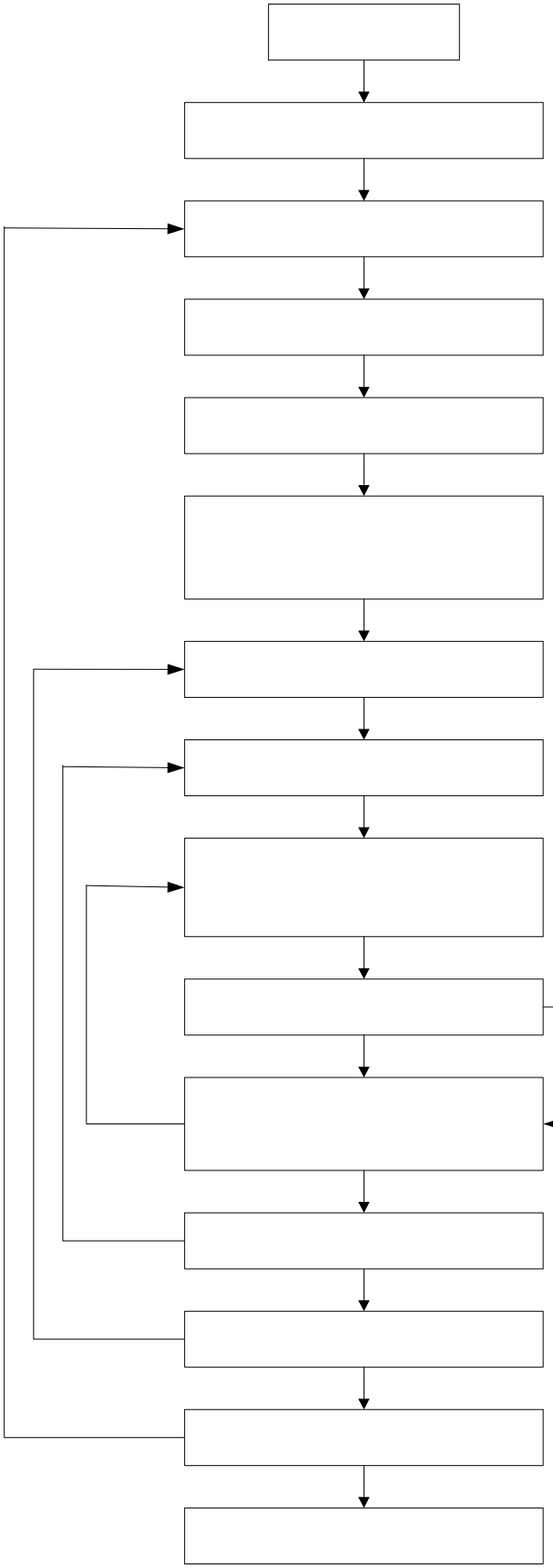


图 2 a） HAZOP分析程序流程——“要素优先”顺序

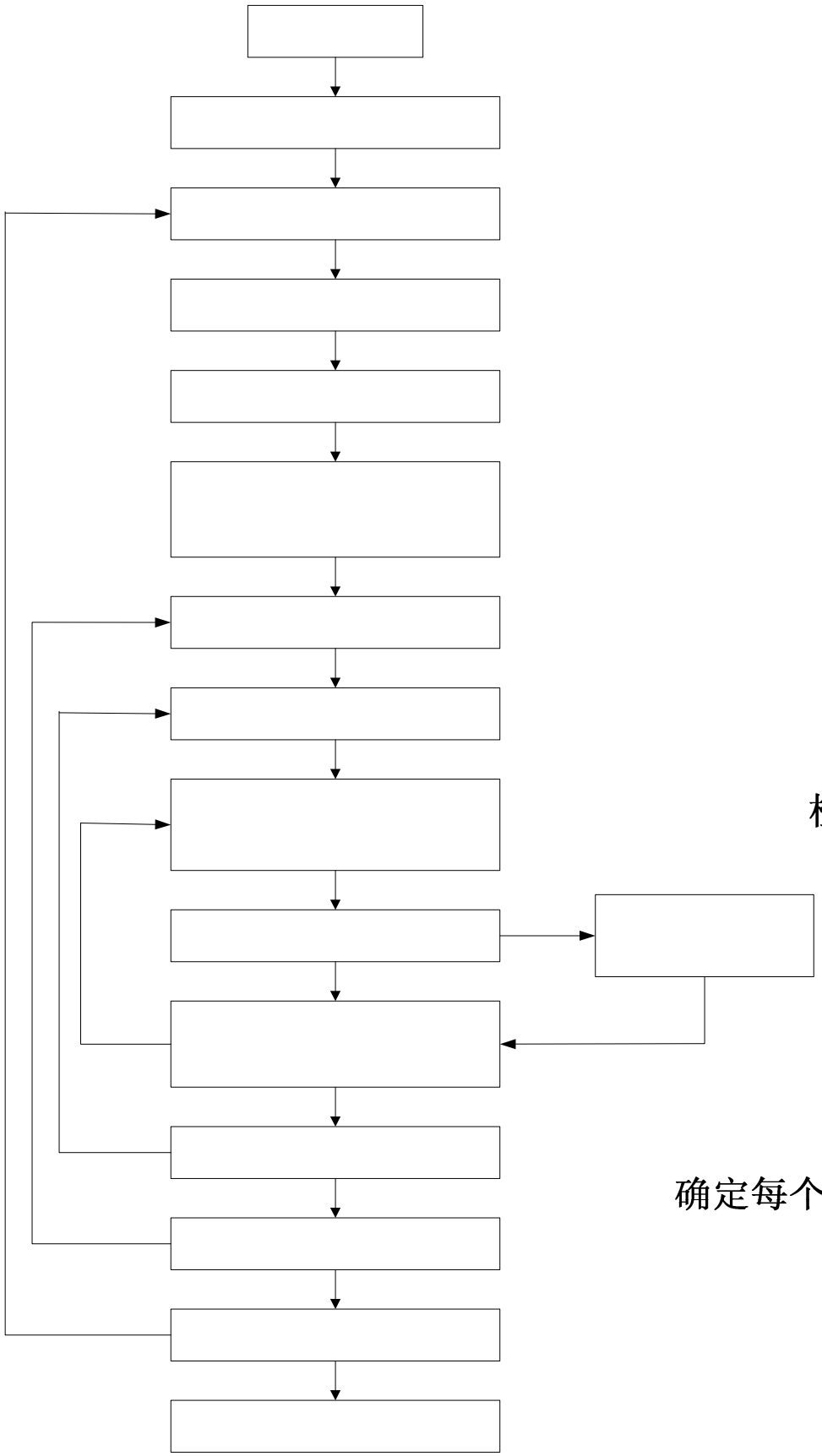


图 2 b） HAZOP分析程序流程——“引导词优先”顺序

6.6 分析文档

6.6.1 概述

HAZOP 的主要优势在于它是一种系统、规范且文档化的方法。为从 HAZOP 分析中得到最大收益，应做好分析结果记录、形成文档并做好后续管理跟踪。HAZOP 分析组长负责确保每次会议均有适当的记录并形成文件。记录员应了解与 HAZOP 分析主题相关的技术知识，具备语言才能、良好的听力与关注细节的能力。不同的报告方法见附录 A。

6.6.2 记录样式

HAZOP 记录有两种基本样式：完整记录和“问题记录”。应在会议前确定好记录方法，记录员随后据此进行记录。

a) 完整记录指将每个引导词-要素/特性组合应用于设计描述上每个部分或要素，对得到的所有结果进行记录。这种方法虽然繁琐，但可证明该分析非常彻底，能够符合最严格的审查要求。
b) “问题记录”只记录识别出的危险与可操作性问题以及后续行动。“问题记录”会使记录文件更容易管理。但是，这种记录方法不能彻底地记录分析过程，因此在审核时作用较小。此外，在以后的某些研究中，还会再次进行相同的分析。因此，“问题记录”法是 HAZOP 记录的最低要求，使用时应谨慎。

在确定采取的记录样式时，应考虑以下因素：

a) 规章要求；
b) 合同要求；
c) 用户政策；
d) 跟踪和审核需要；
e) 所关注系统的风险等级；
f) 可用的时间和资源。

6.6.3 分析报告

HAZOP 分析的报告应包括以下内容：

a) 识别出的危险与可操作性问题的详情，以及已有的探测和（或）减缓措施的细节；
b) 如果有必要，对需要采取不同技术进行深入研究的设计问题提出建议；
c) 对分析期间所发现的不确定情况的处理；
d) 基于分析小组具有的系统相关知识，对发现的问题提出的减缓措施建议（若在分析范围内）；
e) 对操作和维护程序中需要阐述的关键点的提示性记录；
f) 参加每次会议的小组成员名单；
g) 系统中已做 HAZOP 分析的内容说明及未做 HAZOP 部分的原因；
h) 分析小组使用的所有图纸、说明书、数据表和报告等的清单（包括引用的版本号）。

使用“问题记录”法时，上述 HAZOP 报告的内容将非常简明地包含于 HAZOP 工作表中。使用完整记录法时，HAZOP 报告的内容需要从整个 HAZOP 分析工作表中“提取”。

6.6.4 报告要求

记录的信息应符合以下要求：

a) 应分条记录每一个危险与可操作性问题；
b) 应记录所有的危险和可操作性问题以及它们产生的原因，不考虑系统中已有的保护或报警装置；
c) 应记录分析小组提出的需要会后研究的每个问题以及负责答复这些问题的人员姓名；
d) 应采用一种编号系统以确保每个危险、可操作性问题、疑问和建议等有唯一的标示；
e) HAZOP 分析文件应存档以备需要时检索，并可作为系统危险日志（若存在）的参考。

HAZOP 最终报告的发送对象取决于业主的内部政策或规章要求，但一般应包括项目经理、分析组长以及后续行动/建议的负责人（见 6.1）。

6.6.5 文档签署

HAZOP 分析结束时，应生成 HAZOP 分析报告并经小组成员一致同意。若 HAZOP 小组不能达成一致意见，应记录原因。

6.7 后续跟踪和职责

HAZOP 分析的目的并非要对系统进行重新设计。通常，分析组长没有权限要求 HAZOP 分析小组提出的建议能得到执行。

依据 HAZOP 报告提出的危害辨识结果，项目经理应在完成系统的重大的设计变更（修订）文件后，在执行设计变更前，考虑再召集 HAZOP 小组对重大的设计变更进行分析，以确保不会出现新的危险与可操作性问题或维护问题。

在某些情况下（见 6.3），项目经理可授权 HAZOP 小组提出建议并开展设计变更。在这种情况下，可要求 HAZOP 小组完成以下工作：

a) 在关键问题上达成一致意见，以修改设计或操作和维护程序；
b) 核实将进行的修改和变更，并向项目管理人员通报，申请批准；
c) 对将进行的修改部分（包括系统界面）开展进一步的 HAZOP 分析。

7 审查

HAZOP分析的程序和分析结果可接受业主（用户）内部或法律规定的审查。须审查的标准和事项应在业主（用户）的程序文件中列明，其中包括：人员、程序、准备工作、记录文档和跟踪情况。审查还应包括对技术方面的全面检查。

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：

a) 在准备好的表格上进行手工记录，这种形式尤其适合小型研究，只要满足清晰易读的基本要求；
b) 手稿式 HAZOP 记录可以在会后进行文字处理，并生成质量良好的副本，供分发使用；
c) 可在会议期间使用具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；
d) 可使用各种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，使用软件包显示分析记录有助于节省分析成本。

A.2 HAZOP工作表

应制定记录分析结果和跟踪结果的工作表。不论采取何种报告形式，工作表应包括下文所述的基本特征以满足特定要求。工作表的版面设计各有不同，取决于它是手工的还是电子化的。手写完成的工作表通常包括表头和表列。

表头中可包括下列信息：项目、分析对象、设计目的、分析的系统部分、小组成员、分析的图纸或文件、日期和页码等。

各列的标题可为以下各项：

a) 分析期间完成的内容：
   1） 编号；
   2） 要素；
   3） 引导词；
   4） 偏差；
   5） 原因；
   6） 后果；
   7） 需要采取的措施。

也可记录其他信息，如保护措施、严重程度、风险等级和注释等。

b) 在后续跟踪过程中完成的内容：
   1） 建议措施；
   2） 优先权/风险级别；
   3） 行动的负责人；
   4） 状况；
   5） 注释。

注：b)中 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（包含责任和状态）。

使用现有的文字处理系统，可较容易地生成符合客户要求的报告。此外，多种商业化的软件包能简化数据记录和报表生成。这些软件包在协助记录员完成任务时可起到很大作用。不过，有些软件包也在尝试承担分析组长的角色，通过使用引导词-要素（或特性）对的检查清单，取代引导词直接用于要素（和特性，若需要）产生偏差的方法。尽管这些软件包可以识别很多危险，能形成和人工 HAZOP 分析结果类似的输出结果，但它们缺乏从“工作系统”中识别危险的严密性。这些软件包应用于连续处理单元以外领域时，具有一定的局限性。尤其需要指出的是，本导则不提倡使用计算机集成软件包完全代替分析组长。特定检查清单的随机应用不能视为本导则定义的 HAZOP 分析。

A.3 HAZOP分析报告

应编制 HAZOP 分析的最终报告，包括以下内容：

a) 概要；
b) 结论；
c) 范围和目标；
d) 逐条列出的分析结果（见 6.6.3）；
e) HAZOP 工作表；
f) 分析中使用的图纸和文件清单；
g) 在分析过程中用到的以往研究成果、基础数据等。

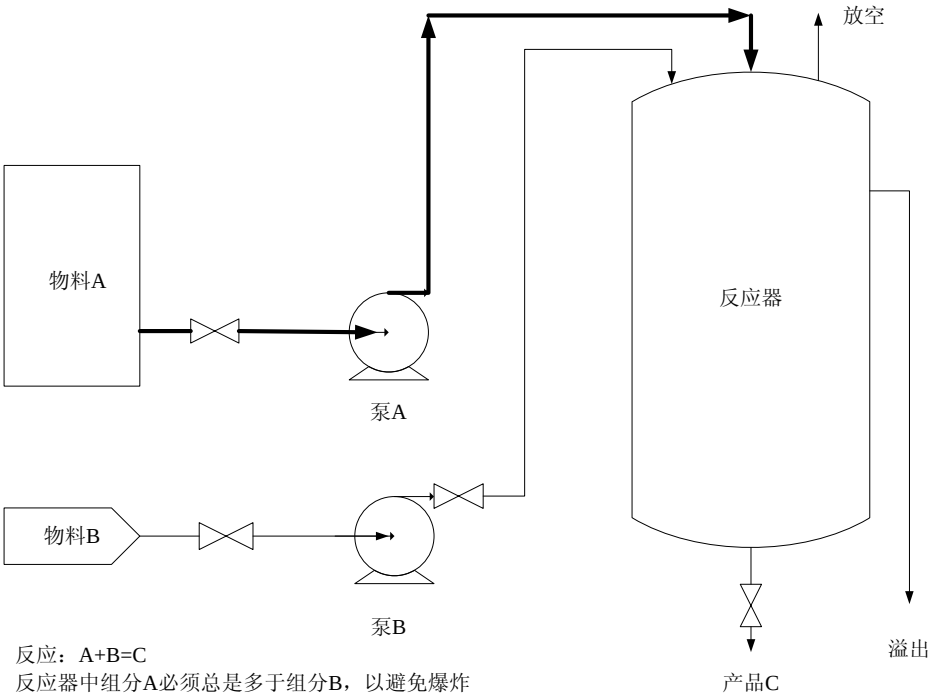
附录B
（资料性附录）
HAZOP示例

附录 B 包含的示例旨在举例说明本导则中描述的 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。还应注意，此处仅提供输出结果的示例。

B.1 介绍性示例

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[1]。

假设一个简单的工厂生产过程，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。工厂中待分析的部分用粗线条表示。



图B.1 简化流程

分析部分是从盛有物料 A 的供料罐到反应器之间的管道，包括泵 A。这部分的设计目的是连续地把物料 A 从罐中输送到反应器，A 物料的输送速率（流量）应大于 B 物料的输送速率。根据 4.2 建议的要素，设计目的可通过如下表头给出：

表B.1 设计目的

物料	活动	来源	目的地
A	输送（转移） （A速率>B速率）	盛有物料A的供料罐	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“问题记录”样式，仅记录了有意义的偏差。在分析完与系统这部分相关的每个要素的每个引导词后，可以再选取另一部分（如：物料 B 的输送管路），重复该过程。最终，该系统的所有部分都会通过这种方式分析完毕，并对结果进行记录。

表B.2　过程的HAZOP工作表示例

分析题目：过程								表页：1/2	
图纸编号：			修订号：					日期：1998 年 12 月 17 日	
小组成员：劳伦斯、狄克、艾略特、尼克、马科斯、贾斯汀								会议日期：1998 年 12 月 15 日	
分析部分：从供料罐 A 到反应器的输送管道									
设计目的：		物料：A　　功能：以大于物料 B 的输送速率连续输送 来源：装有原料 A 的供料罐　　目的地：反应器							
序号	引导词	要素	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
1	无 NO	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	情况不能被接受	考虑在 A 供料罐安装一个低液位报警器外加液位低/低联锁停止泵 B	马科斯
2	无 NO	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	情况不能被接受	物料 A 流量的测量，外加一个低流量报警器以及当 A 低流量时联锁停泵 B	贾斯汀
3	多 MORE	物料 A	物料 A 过量使罐溢出	当没有足够的容量时，向罐中加料	物料从罐中溢出到边界区域	无显示	备注：可以通过对罐的检测加以识别	如果没有预先被识别出来，考虑高液位报警	艾略特
4	多 MORE	输送 A	输送过多； 物料 A 流速增大	叶轮尺寸选错； 泵选型不对	产量可能减少； 产品中将含过量的 A	无		在试车时检测泵的流量和特性； 修改试车程序	贾斯汀
5	少 LESS	物料 A	更少的 A	A 供料罐液位低	不适当的吸入压头； 可能引起涡流并导致爆炸； 流量不足	无	同 1，不可接受	同 1，在 A 供料罐安装一个低液位报警器	马克斯
6	少 LESS	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	不可接受	同 2	贾斯汀

表B.2（续）

分析题目：过程								表页：2/2	
图纸编号：			修订号：					日期：1998 年 12 月 17 日	
小组成员：劳伦斯、狄克、艾略特、尼克、马科斯、贾斯汀								会议日期：1998 年 12 月 15 日	
分析部分：从供料罐 A 到反应器的输送管道									
设计目的：		物料：A 来源：装有原料 A 的供料罐		功能：以大于物料 B 的输送速率连续输送 目的地：反应器					
序号	引导词	要素	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
7	伴随 AS WELL AS	物料 A	在供料罐中除了物料 A 还有其他流体物料	供料罐被污染	未知	所有罐车装的物料在卸入罐前应接受检查和分析	认为是可接受的	检查操作程序	劳伦斯
8	伴随 AS WELL AS	输送 A	输送 A 的过程中，可能发生侵蚀、腐蚀、结晶或分解	根据更具体的细节，对每种潜在的可能都应该加以考虑					尼克
9	伴随 AS WELL AS	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	采用可接受的管道规范或标准	接受合格品	将能联锁跳车的流量传感器尽可能靠近反应器安装	狄克
10	相反 REVERSE	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	装有反应物料的供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	马斯汀
11	异常 OTHER THAN	物料 A	原料 A 异常； 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	在供给物料前对物料进行检验分析	情况可以接受		
12	异常 OTHER THAN	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	建议规定流量联锁跳车应有足够快的响应时间以阻止发生爆炸	马斯汀

B.2 程序

考虑一个安全关键塑料元件的小批量生产过程。元件必须严格满足材料特性和颜色的规范要求。加工顺序如下：

a) 取 12 kg 粉末“A”；
b) 放在搅拌器中；
c) 取 3 kg 着色剂粉末“B”；
d) 放在搅拌器中；
e) 启动搅拌器；
f) 混合 15 min，停止搅拌器；
g) 取出搅拌的混合物，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) 在 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规范要求。作为程序化的顺序，HAZOP 分析的部分是相关的连续指令。对这一顺序的 HAZOP 分析的部分内容见表 B.3。本示例采用了“问题记录”报告形式。

表B.3　程序的HAZOP工作表示例

分析题目：程序									表页：1/2
程序题目：X 元件的小规模生产						修订号：			日期：
小组成员：比克、史密斯									会议日期：
分析部分：					指令 1：取 12kg 粉末 A				
序号	要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
1	取粉末 A	无 NO	没有取 A	操作失误	最终产品不合格	操作人员会注意到搅拌机中颗粒太小，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 AS WELL AS	有其他原料和 A 一起添加	原料 A 被杂质污染	颜色不合格，最终混合物不合格	使用前对所有交付的样品 A 进行检验		检查生产商的质量保证程序	比克
3	取粉末 A	异常 OTHER THAN	取用了除 A 之外的物料	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	比克
4	取 12kg 粉末 A	多 MORE	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 个月保养一次称重设备		史密斯对操作人员强调精确称重的重要性	史密斯
5	取 12kg 粉末 A	少 LESS	取了过少的 A	错称重误/操作人员失误	同上	同上		同上	史密斯

表B.3（续）

分析题目：程序								表页：2/2	
程序题目：X 元件的小规模生产			修订号：					日期：	
小组成员：比克、史密斯								会议日期：	
分析部分：					指令 2：放入搅拌器				
序号	要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
6	搅拌器	异常 OTHER THAN	原料 A 没有正确的放在搅拌器内，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器		如果需要安装其他搅拌器，那么要对安装位置进行审查	比克
7	加硬化剂	无 NO	未加入硬化剂	操作人员失误	最终混合物不合格； 财产损失	操作人员必须签署一系列表格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	比克
8	加硬化剂	伴随 AS WELL AS	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	厂商提供的质量保证书； 对所有样品进行检测		无	
9	加硬化剂	异常 OTHER THAN	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	硬化剂提前称好并袋装，错误的几率会大大降低	等待硬化结果； 采购询问和审查	史密斯
10	取 0.5kg 硬化剂	多 MORE	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； 可能导致灾难性的后果	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 0.5kg 预先称好的袋装催化剂的可能性； 对每一交付样品进行检查	史密斯
11	取 0.5kg 硬化剂	少 LESS	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	史密斯

B.3 列车自动保护系统

本节的目的是给出系统方块图式的典型 HAZOP 分析示例，以说明本导则中一些要点。该示例分两部分进行描述：

a) 简单介绍该系统及其方块图；

b) 辨识一些潜在偏差，进行 HAZOP 分析，采用“问题记录”报告形式（见表 B.4）。

应注意，本例中对所分析系统的设计未提供太多细节。设计和 HAZOP 分析工作表示例仅做说明之用，并非取自真实系统，将它们包含在内是为了说明整个过程，并不一定完整齐全。

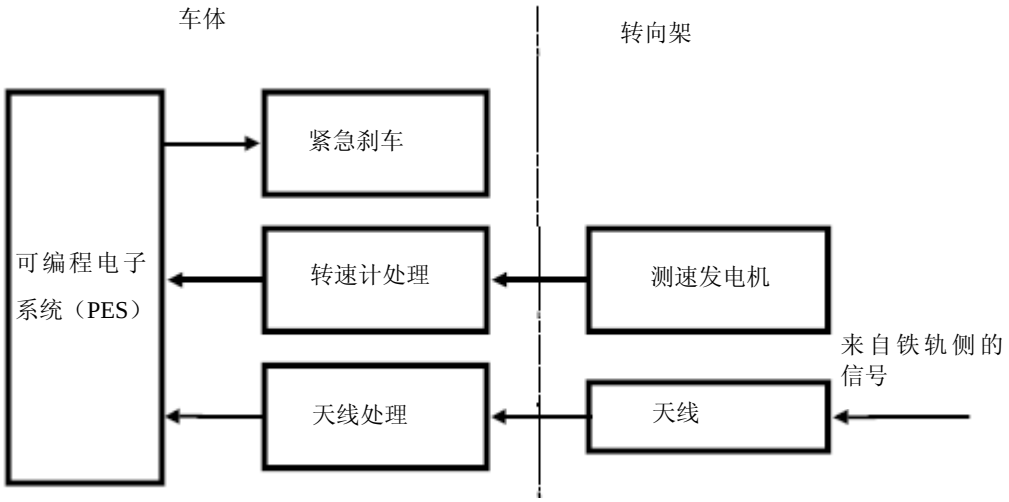
B.3.1 应用

B.3.1.1 系统目的

本例关注车载列车自动保护系统（ATP），该系统在很多地铁列车和一些主干线列车上都得到了应用。ATP 监控列车的速度，并将其与列车的预定安全速度相比，一旦识别出超速情形，自动启动紧急刹车。在所有 ATP 系统上，列车和铁轨侧均安装有设备，可以把信息从铁轨侧传输给列车。目前有很多不同的 ATP 系统，这些系统只是在实现基本功能的细节上有区别。

B.3.1.2 系统描述

在列车上有一条或多条天线，可以接收铁轨侧设备发出的关于安全速度或停车点信息的信号。这类信息先经过处理，再传输到可编程电子系统（PES）。PES 的其他主要信息输入来自转速计或测量列车实际速度的其他方式。PES 的主要输出是发往安全继电器的信号，如控制紧急刹车的信号。图 B.2 给出了一个相关的简单方块图。



图B.2 车载ATP设备

表B.4　列车自动保护系统HAZOP工作表示例

分析题目：列车自动保护系统										表页：1/2
图纸编号：ATP 方块图					修订号：1					日期：
小组成员：丹尼尔、杰弗瑞、鲍比										会议日期：
分析部分：轨道侧设备的输入										
设计目的：通过天线向 PES 发出关于安全速度和停车点的信号										
序号	要素	特性	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
1	输入信号	振幅	无 NO	未检测到信号	发射器故障	考虑对轨道侧设备进行单独分析			重新审查轨道侧设备的分析结果	丹尼尔
2	输入信号	振幅	大 MORE	大于设计振幅	发射器安装位置离轨道过近	可能损坏设备	安装过程中进行检查		对安装程序进行检查	丹尼尔
3	输入信号	振幅	小 LESS	小于设计振幅	发射器安装位置离轨道过远	可能漏失信号	同上		对安装程序进行检查	丹尼尔
4	输入信号	频率	异常 OTHER THAN	检测到不同频率的信号	接收的是邻近铁轨的信号	向处理器传递错误的值	目前没有		检查对此是否需要保护措施	丹尼尔
5	天线	位置	异常 OTHER THAN	天线不在正确位置	支架故障	可能碰撞轨道并被损坏	电缆应能提供二次支撑		确保电缆能使天线不与轨道接触	杰弗瑞
6	天线	电压	大 MORE	电压过高	天线和带电铁轨间短路	天线和其他设备将导电			检查是否需要防护措施防止此现象发生	丹尼尔

表B.4（续）

分析题目：列车自动保护系统									表页：2/2	
图纸编号：ATP 方块图						修订号：1			日期：	
小组成员：丹尼尔、杰弗瑞、鲍比									会议日期：	
分析部分：轨道侧设备的输入										
设计目的：通过天线向 PES 发出关于安全速度和停车点的信号										
序号	要素	特性	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
7	天线	输出信号	异常 OTHER THAN	传输的是不同的信号	收集到了邻近电缆的杂散信号	不正确的信号可能会被使用			确保对电缆干扰有合适的保护措施	杰弗瑞
8	转速计	速度	无 NO	未测到速度	车轮突然卡住	可能显示零速度			检查相应的保护措施	丹尼尔
9	转速计	速度	异常 OTHER THAN	检测到不正确的速度	被卡的轮子突然松动，发出干扰信号	可能显示错误的速度			检查相应的保护措施	鲍比
10	转速计	速度	伴随 AS WELL AS	检测到很多速度	由轮子旋转引起输出的突然改变	可能根据错误的速度引发一些行为			检查这是否是个实际问题	鲍比
11	转速计	输出电压	无 NO	无输出电压	车轴被锁	可能显示零速度			检查其隐含意义	丹尼尔
12	转速计	输出信号	伴随 AS WELL AS	输出信号有干扰	混入了其他信号	可能显示错误的速度			检查这是否是个可信的故障	鲍比

B.4 应急计划的HAZOP分析示例

组织需要制定计划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。这些计划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，识别应急计划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。

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，并送往安全之地。有效的 EER 安排是整个海上设施系统必不可少的部分。在典型的 EER 计划中，通常有很多不同的阶段（要素）如：

a) 通过自动仪表或任一操作员手动发出通用报警（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 应急计划HAZOP工作表示例

分析题目：报警系统									
设计目的：发出通用报警（GPA）信号									
要素：　　输入：触发信号；电能 人员：　　来源：所有警报发生器 　　目的：平台上所有人员									
序号	要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
1	GPA 触发信号和电能	无 NO	无输入	1) 仪器或人员并未启动 GPA	未能警告人员	无	不太可能，但是有可能性	无	
				2) 人员试图启动 GPA，但信号未能到达报警器	同上	双重连接和故障安全模式，即，“电流接通，弹簧关闭”	不太可能		
				3) 没有电能	同上	不间断电源	同上		
2		多 MORE	过多的输入	1) 虚假的报警	人员收到不必要的警告	无	可能	启动报警是否需要两个按钮?	
				2) 恶作剧性质的报警	同上	纪律和守则	不太可能	无	
3	输入	多 MORE	过多的输入	电能过载	损坏报警系统	专用电源保护	不太可能	无	
4		少 LESS	触发信号较少	触发信号只到达部分报警器	某些人员未听到报警	报警器的例行检查		无	
5			过少的电能	能量部分损失	警报可能不响	专用电源	不太可能	无	
6		伴随 AS WELL AS	伴随启动发生	启动触发其他活动		不可能有其他专门的硬连接线路		无	
7			伴随着电能	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 PART OF	部分输入	有信号无电能或有电能无信号	人员没有警惕性		上面均已考虑到		
9		相反 REVERSE	相反的输入	反向报警启动			系统不包括“解除警报”	开发“解除警报”系统	

			相反的电能	没有任何建设性意义					
10	输入	异常 OTHER THAN	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	行动发出报警并传送给人员	无 NO	未听见任何警报	声音设备故障 电缆损坏	未能警告人员	双扩声系统 双电缆 双电源 多声道扬声器	不太可能	无	
12		多 MORE	报警声音过大	音响设备动力过大	人员听力受到损伤	音响设备音量不能超过安全水平		无	
13		少 LESS	报警声音过小	声音太过微弱	一些人员未听到报警	无		确保系统提供最小 15 分贝以上的音量	
14		伴随 AS WELL AS	有其他报警和传输	报警失真、泛音或回音	对人员缺乏明确的信号	无		调查是否需要声学工程	
15		部分 PART OF	部分报警传输	传输警报不足	人员未收到信号		如上述报警声过小		
16		相反 REVERSE	反向报警传输				见以上关于触发和“解除警报”的注释		
17		异常 OTHER THAN	未启动 GPA 报警，声音未传输	系统发出“啪啪”的错误声响	人员慌乱，一些人可能错误地撤离平台	无		重新检查信号逻辑，使发出的“啪啪”声响仅能在 GPA 报警后发出	
18		早 SOONER	报警和声音传输过早	在需要采取行动前过早地启动 GPA 报警	不必要的恐慌和工作中断	无		对平台上人员制定明确的指导方针	
19		晚 LATER	报警和声音传输过晚	在需要采取行动前过晚地启动 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（见图 B.3）描述了 HAZOP 如何应用于详细的电子系统。

压电阀是一种由压电陶瓷驱动的阀门。陶瓷成分通过电力驱动，带电状态下可变长。充电的压电陶瓷关闭阀门，放电的压电陶瓷打开阀门。如果压电陶瓷没有失去或得到电荷，阀门状态保持不变。

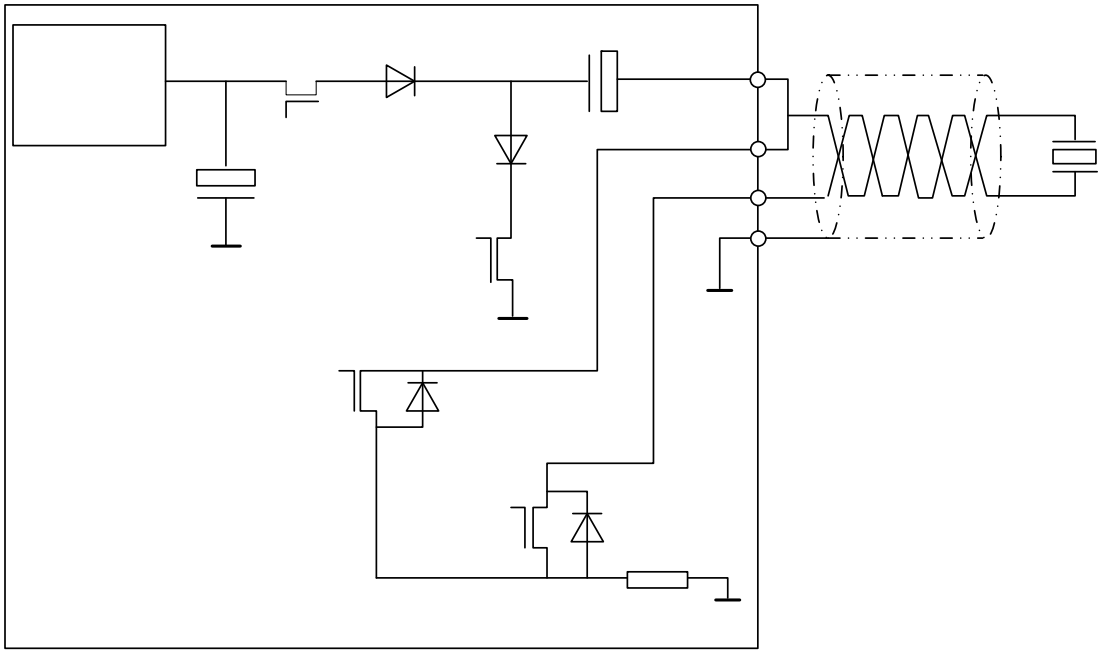
该系统将一种易燃易爆的液体喷洒到反应容器（未显示）内。完整的系统包括反应器、管路和泵等，这些作为 HAZOP 分析的一部分。此外，这里只描述了电子部件的 HAZOP 分析。

该部件的操作是两种状态的切换过程，其设计是需要关闭阀门时为“状态 1”，需要开启阀门时为“状态 2”。

源自电容器 C1 的电荷通过晶体管 T1 传导到耦合电容器 C2，并通过线路传导给压电阀并关闭阀门。这种情况下，晶体管 T2 和保护型晶体管 T3 关闭（高阻抗）。

电容器 C2 通过晶体管 T2 放电，打开阀门。为防止压电阀不均匀充电（例如受到机械应力或热应力），晶体管 T4 将低侧接地。

电缆采用静电屏蔽的双绞线以防止电磁干扰对阀门的影响。



图B.3 压电阀控制系统

状态 1 描述：关闭阀门。

分析部分：从交流/直流转换器和电容器 C1 通过晶体管 T1、二极管 D1 和电阻器 R 到达阀门的动力侧、从阀门的接地侧通过晶体管 T4 和电阻器 R 到达地面的电缆。

状态 2 描述：打开阀门。

分析部分：从阀门的动力侧通过晶体管 T3、二极管 D3 和电阻器 R 到达地面的电缆。

设计目的如下。

表B.6　状态 1 和状态 2 设计目的

输入		功能	来源	目的地
状态 1：关闭阀门	1.电容器 C1 充电 特性： 电压 电容	1.经晶体管 T1、二极管 D1、电容器 C2 传递电荷	C1 和转换器	1.向阀门动力端提供动力
		2.经晶体管 T4 和电阻器 R 把电荷转移到地面	阀门低端	2.低端对地放电
	2.至 T1、T3 和 T4 的控制信号	3.从接地端经 T1 和 T4 控制开	来自控制器的信号	T1、T3 和 T4 过度对地放电
		4.通过 T2 隔离		
		5.通过 T3 防止过度充电		
		6.防止电荷经 D2 回流	阀门电源端	
状态 2：打开阀门	1.阀门放电侧 特性： 电压 电容	1.通过 T1 隔离 C1 和转换器	阀门和 C2 的电源端	地面
		2.经 D2 和 T2 转移电源电荷		
		3.经 D3、D4 和 R 转移阀门的任何电荷		
	2.至 T1、T2 和 T4 的控制信号	4.通过 T4 隔离阀门的低电荷侧	从控制器来的信号	T1、T2 和 T4

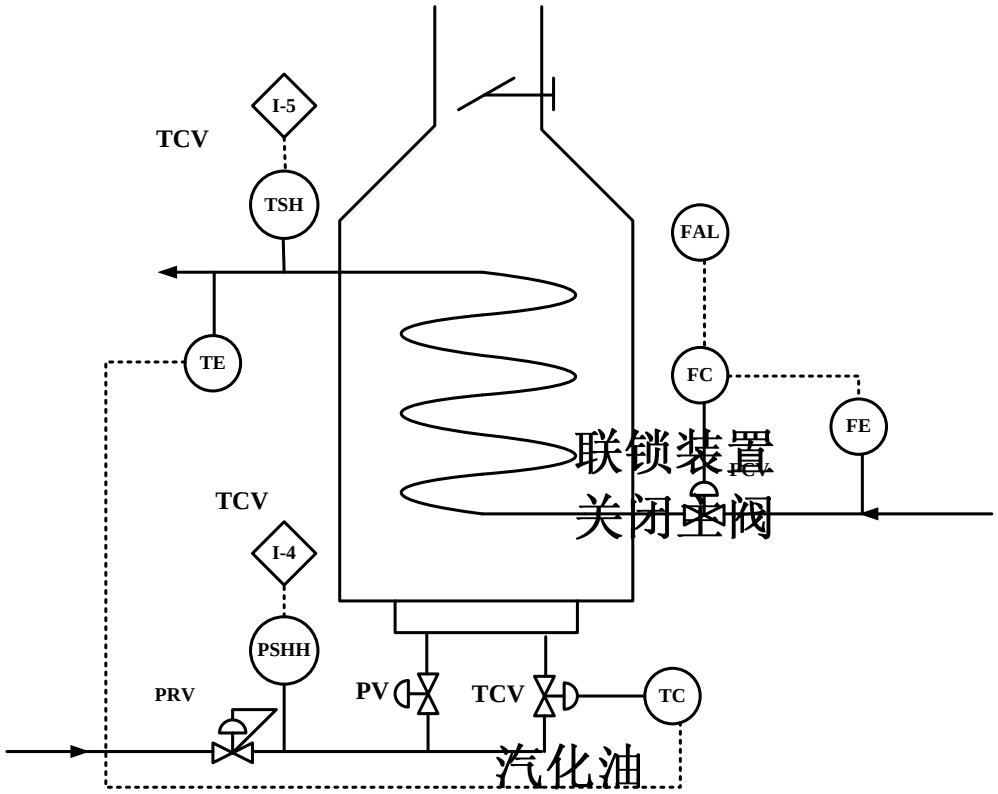
表B.7 压电阀控制系统HAZOP工作表示例

分析题目：压电阀控制系统							表页：1/2	
图纸编号：			修订编号：				日期：	
小组成员：开发工程师、系统工程师、质量经理							会议日期：1997 年 11 月 4 日	
分析的部分：	状态 1：系统关闭阀门							
设计目的：	在规定时间内把规定数量的电荷转移到压电执行器关闭阀门							
要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
输入： 电容器 C1 充电	无 NO	未充电，包括未传递电荷	电力断供 转换器故障 C1 故障 T1 永久关闭 T2 永久打开 T1 故障 二极管（D1、D3）故障： 1）二极管 D1 电路断开；无电流流动 2）二极管 D3 短路；经 D4 到压电阀低端短路或经电阻器 R 到地面短路 C2 故障 断线 T4 故障 R 故障 T3 故障	没有电流经 C2 进入压电阀； 阀门不能关闭，永久打开； 反应物质窜入容器	无	该情况不可接受 要求变更设计	高液位报警 测试程序	史密斯

表 B.7（续）

分析题目：压电阀控制系统							表页：2/2	
图纸编号：			修订编号：				日期：	
小组成员：开发工程师、系统工程师、质量经理							会议日期：1997 年 11 月 4 日	
分析的部分：	状态 1：系统关闭阀门							
设计目的：	在规定时间内把规定数量的电荷转移到压电执行器关闭阀门							
要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
输入： 电容器 C1 充电	较多 MORE	电荷比规定多	C2 充电过高 转换器故障 晶体管 T1 未及时关闭 C2 故障 交流直流转换器释放过高的电压 晶体管 T1 未及时关闭故障保护 T3	压电阀早于规定的时间关闭 压电阀损坏	流量计显示流量过高，通过晶体管 T3 给压电阀放电 无显示	该情况不可接受	考虑高液位报警	彼得森
输入： 电容器 C1 充电	较少 LESS	电荷比规定少	没有足够容量； 电缆绝缘故障，电荷消失 T1 关闭太早 T2 部分打开	C2 充电不足 阀门关闭比规定时间晚	无	该情况不可接受	报警	史密斯
输入： 电容器 C1 充电	伴随 AS WELL AS	T1 及 T2 均打开	C2 充电不足 阀门没有关闭 反应物质进入反应容器	不可控的化学反应	无显示	小差异可以接受	报警 测试程序 重新设置 确定可以接受的差异	史密斯

B.6 油蒸发器



图B.4 油蒸发器

油蒸发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。

油以液态进入加热盘管，蒸发气化，离开加热盘管时成为过热蒸气。

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。

油流量的控制装置包括：流量控制阀 FCV、油流量检测元件 FE、流量控制器 FC 和油流量减少到一定值时的低流量报警器 FAL。

天然气流经一个自力式减压阀 PRV，到达主燃烧器控制阀 TCV、导向阀（副操作阀）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 测量的是油蒸气排出的温度。高/高限压力开关PSHH在天然气管线上是联锁的，如果气化气体压力过高，将通过1-4关闭主燃烧器控制阀TCV。如果油被加热超过最高允许温度，气化油出口的高温开关将通过联锁关闭主燃烧器控制阀TCV。此外，还有一个火焰探测装置（图中没有画出），它在火焰熄灭时将关闭两个天然气阀门。

联锁装置
关闭主阀

燃

燃

导向阀

天然气

表B.8　油蒸发器HAZOP工作表示例

分析题目：油蒸发器									
图纸编号：						修订号：		日期：	
小组成员：马克斯、尼克、狄克、爱德华、劳伦斯								会议日期：	
分析部分：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）									
设计目的：输入：油由进料线流入，由加热炉加热 功能：气化，使其过热并将油蒸气输送到处理装置									
序号	引导词	要素	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
1	无 NO	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； 高温联锁跳车 TSH	安全措施取决于操作人员的快速反应	考虑低流量元件 FE 联锁关闭主燃烧器控制阀 TCV	劳伦斯
				--盘管堵塞； --蒸发器出口被堵塞	油在蒸发器中沸腾； 可能过热并导致加热盘管结焦	低流量报警 FAL； 高温联锁跳车 TSH		检查这些安全措施是否足够并考虑如何方便地清洗盘管	尼克
2	无 NO	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； --考虑油输出温度低报警	狄克
3	大 MORE	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	使蒸发器负荷过大，导致对油不能充分加热（见第 6 点）	无		--检查 FCV 控制高压油流量的性能； --考虑油输出温度低报警	马克斯
4	多 MORE	加热	加热过多	炉温过高	--加热盘管过热：可能导致油结焦并堵塞	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	爱德华
					--温度过高的油蒸气输送到后续系统	高温联锁开关 TSH 关闭主燃烧器控制阀 TCV		检查油蒸气温度过高对后续加工系统的影响	狄克
5	小 LESS	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 LESS	加热	加热不足	炉输出温度低	可能导致不能气化，油在低温下进入后续系统	无	考虑是否构成安全问题	检查油未气化或低温油对后续系统的影响	狄克
								考虑油输出温度低报警	爱德华

表 B.8（续）

分析题目：油蒸发器									
图纸编号：						修订号：		日期：	
小组成员：马克斯、尼克、狄克、爱德华、劳伦斯								会议日期：	
分析部分：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）									
设计目的：输入：油由进料线流入，由加热炉加热 功能：气化，使其过热并将油蒸气输送到处理装置									
序号	引导词	要素	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
7	伴随 AS WELL AS	油	油性质改变	油混入杂质，例如： --带水 --固体、不挥发物、腐蚀物或不稳定的混合物	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	狄克
					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	狄克
8	相反 REVERSE	油流量	反向流动	进油装置损坏可能导致油蒸气从后续加工系统倒流入盘管和进油系统	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	狄克
9	异常 OTHER THAN	油	其他物质	错误地将其他物质输入蒸发器	取决于何种物质	前一工序的输入控制		检查控制措施是否合适	爱德华
10	异常 OTHER THAN	蒸发	在炉子中可能发生爆炸	点燃天然气与空气的混合气	损坏蒸发器； 导致供油系统起火	炉子上的联锁装置等	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	尼克
11	异常 OTHER THAN	油流量	油气不是流向后续加工装置入口	--泄漏； --盘管故障	导致供油系统起火，油蒸气会从后续加工系统倒流； 散发浓烟； 可能损坏燃烧室	无		--考虑在供油系统安装火焰切断阀门； --向炉内提供紧急情况的灭火气体； --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	尼克

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.