

国际标准 IEC 61882
危险与可操作性分析（HAZOP 分析）
应用指南

（2001/5 第一版）

国际电工委员会

危险与可操作性分析（HAZOP 分析）应用指南

前言

- 1) IEC（国际电工委员会）是由所有的国家电工委员会组成为制订国际标准的国际组织。IEC 的目的是为了增强在电工电子领域的标准化问题方面的国际合作。至此，IEC 出版了国际标准。这些国际标准的准备工作有赖于技术委员会的努力；所有对此标准感兴趣的且领域相关的国家委员会都参与了标准制定的准备工作。与 IEC 联系紧密的国际组织、政府和非政府组织也都参与了准备工作。依照 IEC 和国际标准化组织（ISO）所协商的条款，两组织进行密切的合作。
- 2) 由 IEC 制定的有关技术方面的正式决议，都最大可能地传达了与其相关的国际上的观点，因为技术委员会中有来自各个国家委员会的代表。
- 3) 所产生的结论性文件，为技术在国际上的应用提供推荐意见，并以标准、技术说明、技术报告或指南的形式出版，而且被各国家委员会所承认。
- 4) 为了促进国际上的一致性，IEC 国家委员会承担了将 IEC 国际标准最大可能地应用于本国家或本地区标准之中。所有 IEC 国际标准与国家或地区标准之间的不同点都将由国家委员会明确地指出。
- 5) IEC 不会提供认证，并不负责确认任何设备与标准的一致性。
- 6) 值得注意的是，国际标准中可能有些涉及到专利问题。IEC 不负责与这些专利相关的问题。

国际标准 IEC 61882 由 IEC 第 56 技术委员会制定，具有可靠性。
标准的制定基于以下文件：

FDIS	Report on voting
56/731/FDIS	56/733/RVD

有关标准制定过程中的表决方式等详细信息，可以参看上表中的表决报告文件。
本出版物的起草是按照 ISO/IEC 指南第三部分进行的。
附件 A 和附件 B 仅供信息参考。

委员会决定本出版物的内容在 2005 年之前不会变更。但在这期间，本出版物将可能被：

- 重新确认；
- 撤回；
- 被新版本取代，或
- 修订。

引 言

此标准的目的是描述 HAZOP 分析的原理和步骤。HAZOP 是一个结构化和系统化的检查被定义系统的技术。它的目标是：

- * 识别系统中潜在的危险。这些危险可能包括本质上只与系统现有区域有关的危险和有更大影响范围的危险，例如，某些环境危害；

- * 识别系统潜在的操作性问题，特别的辨识操作性干扰的原因和可能导致非一致性产品的生产偏离。

HAZOP 分析的一个重大好处就是，通过结构化和系统化的方法辨识潜在危险与可操作性问题，获得的结果知识大大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”，会议期间由评价（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目的的偏离。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险与操作性问题。HAZOP 可看成是采用基于经验的方法（例如实践的规则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险和可操作性问题，从检查表，故障模式和影响分析（FMEA），故障树分析（FTA）到 HAZOP 都属此类。某些方法，例如检查表法和“如果—怎么样”分析，可用于系统生命周期的早期，因为可得到的信息很少，或在随后的阶段不需要详细的分析。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险和错误的信息。

一般而言，HAZOP 经常和其它一些危险识别技术联合（例如，检查表 HAZOP，HAZOP1 或 2，基于知识的 HAZOP）。这些技术术语的使用被认为是不恰当的，在本标准中明确排除。

在启动 HAZOP 分析之前，应保证对现行的任务而言，HAZOP 是最合适的技术（单独使用或者与其它技术结合）。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。

此标准已经开发用于提供许多工业和多种系统的指南。在一些工业中有更明确的标准和指南，特别是此技术面向的过程工业，为这些行业建立了应用的首选方法。详细资料请参看本文结尾的参考书目。

危险与可操作性分析（HAZOP 分析）—应用指南

1 范围

此国际标准提供了应用本文中定义的一套明确的引导词的系统 HAZOP 分析的指南。它还给出此技术的应用指导和 HAZOP 分析步骤的指导，包括定义、准备工作、检查会议和作为结果的文件以及后续措施。

这里还提供了阐明 HAZOP 检查的文件，以及包括不同工业的例子。

2 标准的参考书目

下面的标准文献包括通过这篇文献的参考制定的此国际标准条款的条款。对于过时的参考文献，后来的修改，或者修订没有应用。但是，基于此国际标准的协议团体被鼓励去调查应用下面指出的最新的标准文献的版本可能性。对于没有日期的参考，标准文献的最新版本参考于应用。IEC 和 ISO 的成员主持现行的有效国际标准的注册。

IEC 60300-3-9，可信度管理—第 3 部分：应用指南—第 9 节：工艺学系统的危险分析

IEC 60812，系统可靠性分析技术—故障模式和影响分析（FMEA）步骤

IEC 61025，故障树分析（FTA）

IEC 61160，有效设计综述

3 定义

为了达到此国际标准的目的，应用了在 IEC 60050（191）中包含的定义和下面的术语和定义：

3.1 特性

一个元件的定性或定量性质

注释：特性的例子如压力，温度，电压

3.2 设计目的

设计者想得到的，或者特定元件的性能范围和特性

3.3 偏离

设计意图的偏离

3.4 元件

用于识别部分基本特征的零件的要素

注释 元件的选择可能依赖于特殊应用，但是元件可以包含例如有关的物料，执行的活动，使用的设备，等特征。物料在广义上应该被考虑，还包括数据，软件等。

3.5 引（先）导词

表达和定义一种特定类型的对元件设计目的的偏离的词或短语

3.6 危害

身体伤害或对人们健康的损害或者对财产或环境的破坏

3.7 危险

潜在的危害源

3.8 部件

是当前分析的主题，该主题是系统的一个部分

注释 一个部件可能是物理的（例如，硬件）或者逻辑的（例如，在一个操作顺序中的步骤）

3.9 风险

危害发生的可能性和危害的严重性的结合

4 HAZOP 的原理

4.1 纵览

HAZOP 分析是一个详细的危险与可操作性问题的辨识过程，由一个小组执行。HAZOP 处理对设计目的潜在偏离的辨识，对偏离原因的检查和偏离后果的评估。

HAZOP 检查的主要特征包括如下几个方面：

- HAZOP 检查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目的偏离和用此偏离作为“触发装置”来激励小组成员调查偏离是怎样发生的，可能的后果是什么，以此来推动检查。

- 检查是在一个训练有素，经验丰富的评价组长的指导下执行的，组长必须用逻辑的，分析的思想保证对分析系统的全面把握。分析领导最好有记录员帮助，记录员记录辨识的危险和/或操作干扰以备进一步评估和分析。

- 检查依赖具有适当技术和经验的不同部门专家，他们具有很好的直觉和判断能力。

- 检查应该在一个积极思考和坦率讨论的气氛下进行。当识别到一个问题时，应该作记录以备后续的评估和分析。

- 辨识的问题的解决方案不是 HAZOP 检查的一个主要目的，但是如果制定了就要记录，以作为那些负责设计的人员需要考虑的事项。

HAZOP 分析有四个基本的顺序步骤组成，如图 1 所示。

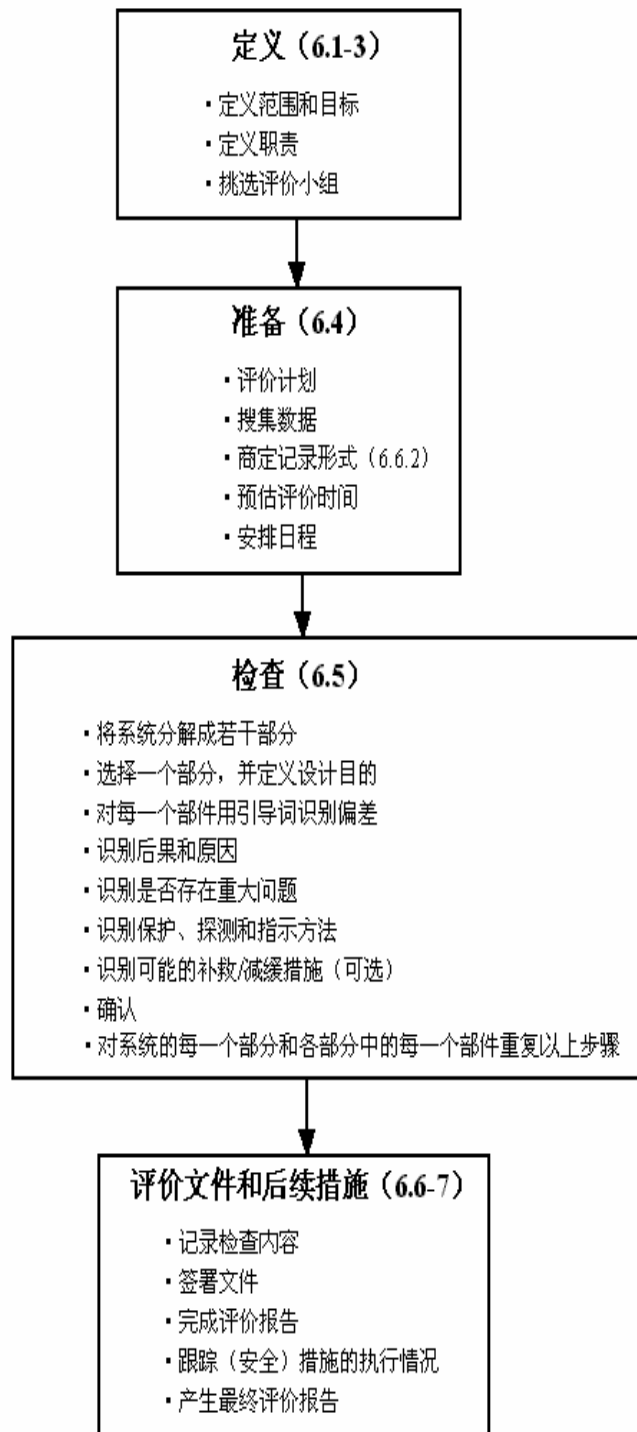


图 1—HAZOP 分析步骤

4.2 检查的原理

HAZOP 检查的基础是“引导词检查”，它是对设计目的偏离的一个从容谨慎的调查。为了方便检查，一个系统被分成几部分，分割的方法是各个部分的设计目的能被恰当地定义。选择的部分大小可能依赖于系统的复杂度和危险的严重度。在复杂系统或者那些显现有高危

险的部分可能范围很小。在简单系统或者显现低危险的系统中，采用将部分的范围扩大能加速分析。系统给定部分的设计目的用传达了部分基本特征和表示了部分的自然分割的元件表示。被检查的元件的选择在某些程度上是主观的决定，因为这里可能有几种结合能达到必须的目的，并且选择也可能依赖于特殊应用。元件可能是过程或电气系统等的控制系统，设备或组成中的一个过程，单独的信号和设备元件中离散的步骤或阶段。

在某些情况下，用下列描述表示一个部分的功能是有帮助的：

- 从一个资源中取得的输入物料
- 对该物料的一种作业活动（行动）
- 为某一目的所加工的产品

因此设计目的将包括下面的因素：物料，行动，资源和目的，它们可看作是部分中的元件。

元件经常被进一步用特性加以定义是有用的，特性可以是定量的或者定性的。例如，在一个化工系统中，元件“物料”可能进一步用例如温度，压力和组成等特性定义。对于作业活动“传输”，例如移动速率或者乘客的数量等特性可能是相关的。对于基于计算机的系统，信息比物料更可能是每个部分的主题。

HAZOP 小组检查每一个元件（以及相关的特性）由于对设计目标的偏离而导致的不利后果。辨识对设计目标的偏离是采用预先定义的“引导词”通过提问方法达到。引导词的作用是激发想象的思考，集中精力分析和得出观点并讨论，从而得到最大化完备性的分析。基本的引导词和含义由表 1 给出。

表 1—基本的引导词和含义

引导词	含义
NO 或者 NOT	设计目的的完全否定
MORE	定量增加
LESS	定量减少
AS WELL AS	定性修改/增加
PART OF	定性修改/减少
REVERSE	设计目的的逻辑取反
OTHER THAN	完全替代

与时钟时间和顺序或序列有关的附加引导词由表 2 给出：

表 2—与时钟时间和顺序或序列有关的引导词

引导词	含义
EARLY（超前）	相对于时钟时间
LATE（迟后）	相对于时钟时间
BEFORE（先）	相对于顺序或序列
AFTER（后）	相对于顺序或序列

对于上面的引导词有很多种解释。附加的引导词可能对偏离的辨识有利。只要在检查开始前定义了就可以使用这样的引导词。已经选择了检查的一个部分，此部分的设计目的被分成若干元件。每个相关的引导词就用于各个元件，这样就用系统的方法执行了一个对偏离的彻底的分析。已经应用了一个引导词，给定偏离的可能原因和后果被检查，并且对故障的探测或征兆机理可能进行了分析。检查的结果记录到经过协议的格式中（看 6.6.2）。

引导词/元件关系可以看作一个矩阵，引导词定义为行，元素定义为列。对于这样构造的矩阵中的每个元素表达了一个特殊的引导词/元件的关系。为了达到全面的危险辨识，元件和它们相关的特性要覆盖设计目的的相关方面，引导词覆盖所有的偏离是必需的。不是所有组合都会给出可信的偏离，因此矩阵在考虑所有的引导词/元件组合时可能有几个空的空间。

在检查矩阵元素时有两种可能的顺序，即逐列，也就是，元素优先，或者逐行，也就是引导词优先。检查的详细步骤在 6.5 中有略述，且两种检查的顺序由图 2a 和 2b 阐明。原则上检查的结果应该是相同的。

4.3 设计陈述

4.3.1 概要

被分析系统的一个精确完整的设计陈述是检查任务的一个先决条件。设计陈述是一个充分描述了被分析系统，其部分和元件，和充分辨识它们特性的系统描述模型。此陈述可能是物理的设计或者逻辑的设计，它应该被清晰地陈述。

设计陈述应该定性或定量地传达系统各个部分和元件的功能。它还应该描述系统和其它系统、它的操作者/用户、还可能和环境的相互关系。元件的一致性或者它们设计目的的特征决定了操作的正确性，在某些情况下还决定了系统安全性。

系统的陈述有两个基本部分组成：

- 系统需求；
- 物理的和/或逻辑的设计描述。

HAZOP 分析结果的价值依赖于完备性、包含设计目的的设计陈述的充分性和精确性。因此，在准备信息包时应该谨慎细致。如果 HAZOP 的实施处于操作或者清理阶段，应注意确保任何修改都反映在设计陈述中。在开始检查前，小组应该检查信息包，如有必要就要进行修改。

4.3.2 设计需求和设计目的

设计需求由系统必需满足的定性和定量需求组成，它提供了改进系统设计和设计目的的基础。用户希望的所有合乎情理的使用和误用情况都应鉴别。设计需求和由其得出的设计目的必需满足客户的期望。

在系统需求的基础上设计者开发系统设计，即，实现系统的构架，特殊功能分派给子系统和组件。组件是被指定和挑选的。设计者应该不仅考虑设备应该做什么，还应确保在任何非正常条件下不会失效，或者在指定的生命周期内不会用坏。不良行为或特性也应该辨识，以使它们在设计中排除，或通过适当的设计减低它们的影响。上面的信息提供了基础，用于辨识被检查部分的设计目的。

设计目的作为检查的基线应该尽可能地完全和准确。设计目的的验证（详见 IEC 61160）虽在 HAZOP 分析的工作范围之外，但是分析领导人应该确保它的准确性和完整性以便使分析能够进行下去。一般的设计目的局限于在正常操作条件下系统的基本功能和参数，很少包含非正常操作条件下的情况和违规操作，而这些操作很有可能在生产过程中出现（比如，剧烈扰动、管道的水击作用、电压振荡等导致的问题）。但这些应该在检查阶段被辨识和考虑。另外，设计目的中也没有明确说明风化、腐蚀的机械或其它可能造成物质财产损失的机械的退化情况。但这些都应该在分析中使用引导词进行辨识、予以考虑。

期望的生命周期、可靠性、可维护性和维护支持也应该与危险同时考虑，因为在维护工作中很有可能遇到这些危险，如果 HAZOP 分析的工作范围包括了该项工作的话。

5 HAZOP 应用

5.1 概要

最初，HAZOP 是为了包含有处理流动介质或其它物料流动的过程工业系统所开发的技术。但是近几年，它的应用范围已经逐步地扩大了，例如将 HAZOP 用于：

- 有关可编程电子系统的软件应用；
- 有关例如道路、铁路等的人流运输模型的系统；
- 检查不同操作顺序和规程；
- 评价不同工业的管理规程；
- 评价特殊系统，例如医疗设备。

HAZOP 对辨识系统中的薄弱环节（现实存在的或假想的），包括物料流动、人流、数据流，或许多按预定的工序运作的事件或活动，或控制这种工序的程序，特别有用。HAZOP 除了是一个用于设计和开发新系统的有价值的工具外，还可以有效地用于分析一个给定系统的不同操作状态下的危险和潜在问题，例如，如开车、待命、正常操作、正常停车、紧急停车等。如同连续过程一样，也可用于批处理和非稳定状态的过程和工序。HAZOP 可被看作是价值工程和风险管理的整个过程中的一个组成部分。

5.2 与其他分析工具之间的关系

HAZOP 可以与其他可靠性分析方法联合使用，如故障模式、影响分析（见 IEC 60812）和故障树分析（见 IEC61025）。这样联合的使用，可以用在：

- 经 HAZOP 分析清楚地表明，设备某一特殊方面非常关键，需要深度地进行检查；HAZOP 此时可以用 FMEA 对该设备进行辅助分析；
- 已用 HAZOP 对单项元件或单个特性的偏离进行过检查，进而用 FTA 对多个偏离进行评估，或量化故障的可能性，还要用 FTA 辅助。

HAZOP 在本质上是一个以系统为中心的分析方法，这与以元件为中心的 FMEA 分析方法不同。FMEA 是由一个元件可能发生的故障开始，进而检查整个系统的故障后果。因此检查是单向性的由原因到结果。而 HAZOP 分析则不同，HAZOP 分析由辨识可能的设计目的偏离，进而分成两个方向，一个方向寻找产生偏离的潜在的原因，另一个方向推断它的结果。

5.3 HAZOP 的局限性

虽然 HAZOP 分析被证明在许多不同的工业领域有非常大的作用，但同时此技术也有局限性，当进一步应用时应该考虑。

- HAZOP 是一个危险辨识技术，它逐一考虑系统的部分并系统的检查偏离对各个部分的影响。但有时一个严重的危险将涉及系统几个部分之间的相互作用。在这种情况下危险可能需要用例如事故树和故障树分析等技术进行更详细的研究。
- 由于任何一种危险或者可操作性问题的辨识技术，不可能保证所有的危险或可操作性问题都能识别，HAZOP 分析也是如此。因此，一个复杂系统的分析，不应该完全依赖 HAZOP。它应该和其它合适的技术结合应用。在一个有效的全面的安全管理系统中与其它相关分析协调是必要的。
- 很多系统是高度关连的，在它们其中的一个偏离可能源于其它地方。适当的局部减缓作用可能导致无法找到真实的原因，并且仍然导致后续的事故。许多事故的发生是由于小的局部修改没有预见到其它方面的疏漏效应。虽然这种问题可以通过从一部分到另一部分进而执行偏离的推断解决，但实际上很少这样做。
- HAZOP 分析的成功很大程度上依赖于分析小组领导的能力和經驗以及小组成员之

间的知识、经验和合作。

- HAZOP 只考虑出现在设计描述中的部分。不考虑那些在描述中没有出现的行动和操作。

5.4 系统生命周期不同阶段的危险辨识

HAZOP 分析是一个结构化的危险分析工具，非常适用于后期的详细设计阶段中检查操作设备，或者是对已存在设备进行改动的阶段。下面将详细介绍对系统不同生命周期中 HAZOP 和其他分析方法的使用。

5.4.1 概念和定义（初步设计）阶段

在系统生命周期的这个阶段，设计概念和系统的主要部分被定义，但是用于指导 HAZOP 分析所必需的实际细节和文件并没有生成。但是，在这个阶段有必要对主要的危险进行辨识，以使它们在设计过程中被考虑到，也有利于随后的 HAZOP 分析。为了进行分析，其他的基本方法也应该使用（关于这些方法的详细描述，见 IEC 60300-3-9。）

5.4.2 设计和开发阶段

在系统生命周期的这个阶段，需要进行详细设计、决定操作方法和准备文件。设计趋于成熟并定型。使用 HAZOP 分析的最好时机是在设计定型之前。在这一步，设计需要足够地详细以使 HAZOP 的询问机制可以获得有意义的回答。重要的是建立一个系统用于评估进行 HAZOP 分析之后的任何改动。这个系统应该在系统整个生命周期都起作用。

5.4.3 制造和安装阶段

建议在系统开车使用之前就进行一次分析，如果系统的使用或操作有可能潜在着危险，且系统需要非常严格的操作顺序和使用规范，或者设计目的将在之后进行一系列修改时，也建议进行分析。这个时候，附加的数据，例如使用或操作说明，应该确保可用。另外，分析应该兼顾在分析的早期阶段所进行的所有活动，以确保它们被有效解决。

5.4.4 操作和维护阶段

HAZOP 分析应该在可能对系统的安全或可操作性有影响或者对环境有影响的任何改动之前进行。在对系统进行阶段性地回顾检查时，也应该对其进行分析，以使系统抵消那些逐步被改变的微小改动的影响。在分析中用到的设计文件和操作说明都应该保持更新。

5.4.5 停止使用和销毁阶段

这个阶段的分析是非常有必要的，因为危险并不一定仅在正常操作阶段才出现。如果在分析的前面阶段的记录保留的话，分析就可以很快地完成。记录应该在整个的系统生命周期中被保留，这样就可以快速完成对停止使用问题进行处理。

6 HAZOP 分析步骤

6.1 分析初始化

分析一般由负责项目的被本指南称作“项目主管”的人进行初始化。项目主管决定分析进行的时间、指定分析领导人和提供分析所需要的各种资源。由于法律要求，或由于公司的政策，这样的分析一般都会在正常的项目计划之中。在分析领导人的辅助之下，项目主管应该确定分析的范围和目标。在一个分析开始之前，需要一个权威的具有相当水平的专家来负责确保由分析得来的建议或措施被应用到实际系统中。

6.2 定义分析的范围和目标

分析的范围和目标是内部决定的，并应该同时确定。范围和目标都应该被明确地陈述，以确保：

- 系统边界，以及系统与其它系统或周围环境之间的界面被明确定义；
- 分析小组成员把注意力集中到需要解决的问题，而不会迷失于所分析问题无关的方面。

6.2.1 分析范围

这将由以下几个因素决定：

- 系统的物理边界；
- 可采用的设计陈述的详细程度和数量；
- 在系统上曾经使用过的 HAZOP 分析或其它相关分析的范围；
- 所有可用于系统的必要的规定。

6.2.2 分析目标

一般来说，HAZOP 分析寻求辨识所有的危险和可操作性问题，而不论它们的类型或后果。集中精力把 HAZOP 分析严格地应用于辨识危险，将能够使分析在较短的时间内较容易地完成。

在进行对分析的目标进行定义时，应考虑到下面的因素：

- 应用分析结果的目的；
- 分析所在的系统生命周期的阶段（详见 5.4）；
- 可能具有潜在风险的人身、财产，如工作组人员、一般民众、环境、系统等；
- 关系到影响生产质量的可操作性问题；
- 系统要求的标准，包括系统安全和操作性能两个方面。

6.3 角色和职能

HAZOP 分析小组成员的角色和职能应该由项目经理在分析开始前明确地指定，并得到 HAZOP 分析领导的同意。分析领导人应该纵览整个的设计以确定什么样的信息是可用的，什么样的技术是分析小组成员必须具备的。应制定对项目来说至关重要的活动计划，使得任何建议都被适时地采纳。

分析领导人负责保证一个有效的交流机制被建立，用于传达 HAZOP 分析的结果。由项目经理（主管）监督分析结果的应用，并且由设计小组所做的任何修改都被恰当地归档。

项目经理和分析领导人应该经过讨论决定是否 HAZOP 分析小组的活动被指定在辨识危险和可操作性分析的范围（这项工作完成后交于项目主管，并由设计小组来解决问题），或者是他们是否还应该提供可能的补救或减缓措施。如果是后一种情况，那么分析小组还应该负责讨论并决定选择合适的补救或减缓措施，并为活动的权限给予保证。

HAZOP 分析是集体努力的结果，集体中每一个成员都应该被赋予不同的角色。分析小组的组成应尽可能地小，只要成员们具有分析所需要的相关技术和操作技能以及经验就可以了。一般来说，分析小组由至少四个人组成，且很少超过七个人。小组越大，进程越慢。那些已经被承包商设计完成的系统，HAZOP 小组除了包括承包执行方，还应该包括客户方的成员。

建议小组成员的角色如下分配：

- 分析领导人：与设计小组和本工程项目的联系不是很紧密。对领导 HAZOP 分析经过训练且具有经验。负责 HAZOP 分析小组成员和项目管理组织之间的交流。提出分析计划。讨论决定分析小组成员的组成。确保有足够的的设计陈述信息提供给分析小组。对分析过程中需要用到的引导词和元件或特性的引导词提供建议。确保结果被归档。
- 记录员：记录会议的进程。记录危险和可操作性问题的辨识领域，记录分析所做出的建议和后续需要做的工作。辅助分析领导人进行计划和履行管理职责。在一些情况下，分析领导人可以承担这项工作。
- 设计人员：解释设计和设计陈述。解释偏离的产生原因以及对相关系统造成的影响。

- 用户：解释操作规程，其中被分析的元件将被操作，每一个偏离所导致的操作后果以及偏离可能引起的危险程度。
- 专家：提供有关系统和分析的专门知识。可以由不同领域的专家分别负责不同方面的问题。
- 维护：（如果需要）维护成员们的出席。

设计者和使用者的观点对于 HAZOP 分析通常是需要的。然而在生命周期的不同阶段，适合分析工作的专家经常是不同的。

所有的团队成员必须掌握足够的 HAZOP 技术，以使它们更有效的参与研究，如果没有那就应该向他们提供适当的介绍（培训）。

6. 4 准备工作

6. 4. 1 概要

分析小组组长负责以下准备工作：

- a)获得信息；
- b)将信息转化为合适的形式；
- c)计划会议的顺序；
- d)安排必要的会议。

除此以外，分析小组组长应当能提供一个基于资料库的查询，来证明发生的事故是由于相同或相似的技术原因。

分析小组组长应当保证有一个适当的且有效的设计说明，如果这个设计说明有缺陷或不完整，应当在分析工作开始前将其进行更正。在一个分析工作的计划阶段，单元，元素及它们的特性都应当在设计说明中由熟悉设计工作的人进行确定。

分析小组组长负责提出分析计划，一个分析计划应当包含以下几点：

- 分析的目标及范围；
- 分析小组成员的名单；
- 技术细节：
 - * 一个设计说明按照明确的设计目标分为多个单元和元素，每个元素都有一个关于组成，材料，作业活动以及它们的特性的列表；
 - * 一个被采用的建议的引导词列表，引导词的解释，即，在 6.4.3 列出的元素/特性组合；
- 适当的参考资料列表；
- 管理安排，会议计划，它们应包括具体日期、时间以及地点；
- 要求的记录表格（见 附录 A）；
- 在分析中可能要用到的样板。

应当提供充足的空间设施及影音设备来方便会议的进行。

分析计划内容的简要汇总以及必要的参考资料应当在第一次会议之前发给分析团队的成员以使它们熟悉分析内容。分析内容的检查回顾是有意义的。

HAZOP 分析是否成功在很大程度上取决于分析小组成员的对问题的机敏和专注，因此重要的是对会议持续时间应有所限制，同时在各个会议之间应有适当的间隔。以上各种要求如何实现在根本上是由分析小组组长负责的。

6.4.2 设计描述

典型的设计描述应包含以下一些文档，这些文档应被唯一地，清晰地定义和认可并标明日期：

- a) 对于所有的系统：
- 设计要求和描述，流程图，功能块图，控制图，电路回路图，工程数据单，分布图，公用工程说明，操作及维护要求；
- b) 对于过程流动系统：
- 工艺管路仪表流程图，物料说明及标准设备，管路及系统布局；
- c) 对于可编程的电子系统：
- 数据流程图，面向对象设计图，状态传递图，时序图，逻辑图。

除此以外，应当提供下列信息：

- 所分析对象的边界以及各个边界的接口界面；
- 系统操作的环境条件；
- 操作及维护的个人资格，技能熟练程度以及经验；
- 步骤和/或操作规程；
- 操作及维护经验以及来自类似系统的已知的危险因素。

6. 4. 3 引导词及偏离

在 HAZOP 分析的设计阶段，分析小组组长应当提出一个最初的将要被使用的引导词的列表。分析小组组长应当针对系统测试所提出的引导词并确定它们的合理性。引导词的选择应当被仔细考虑。引导词如果太具体可能会限制思路或讨论，如果太一般性又可能无法有效地集中到 HAZOP 分析中。表 3 中给出了不同偏离种类以及与它们相联系的引导词。

表 3 偏差以及与之相对应的引导词的例子

偏离类型	引导词	过程工业的解释例子	对于可编程电子系统的解释例子 (PES)
否定	NO	没有达到任何目的。 例如：没有流量	没有数据或控制信号通过。
定量改变	MORE LESS	量的增长，例如较高的温度 量的减少，例如较低的温度	数据传输比期望的快 数据传输比期望的慢
定性改变	AS WELL AS PART OF	出现杂质 同时执行了其他的操作或步骤 只有一部分目的达到，例如：只有一部分要求的流量传输（发生）	出现一些附加信号或虚假信号 数据或控制信号不完整
置换	REVERSE OTHER THAN	管道中的物料反向流动以及逆化学反应 原始的目的没有实现，而达到了完全不同的结果。例如：输送了错误物料。	一般情况下非相关的情况 数据或控制信号不正确
时间	EARLY LATE	某事件的发生比时钟时间较早，例如：冷却或过滤	信号与时钟时间相比来得太早。

		某事件的发生比时钟时间较晚，例如：冷却或过滤	信号与时钟时间相比来得太晚。
顺序或序列	BEFORE	某事件的发生比序列太早，例如：混合或加热	信号在序列中比期望来得早
	LATE	某事件的发生比序列太晚，例如：混合或加热	信号在序列中比期望来得晚

引导词-元素/特性组合当应用于不同的设计说明中时，由于分析的系统不同以及所处的系统生命周期不同，其解释也可能不同。一些组合对于给定的一些分析是没有意义的解释，应当被忽略。引导词-元素/特性组合的解释应当被详细定义并用文档说明。如果在设计文档的上下文中有多种敏感的解释，那么整个文档的解释应被列出。在另一方面，也有可能发现不同的组合中存在相同的解释。在这种情况下，应当提供相互的参考。

6.5 检查

检查会议应当在分析小组组长的领导下按照分析计划引导讨论，以实现结构化分析。在HAZOP分析会议的开始，分析小组组长或分析小组成员中熟悉检查过程及其存在问题的成员应当：

- 综述分析计划，确保分析成员熟悉系统以及分析的对象和范围；
- 综述设计文档，并解释所提出的、将会用到的元素和引导词；
- 回顾已知的危险及操作问题和所关注的潜在领域。

分析应当遵从与研究对象相关的流程流向或顺序进行，并且按照逻辑顺序跟踪输入与输出。危险识别技术例如HAZOP技术，都是依赖于有规律的一步一步的检验过程。存在两种可能的检验顺序：“元素优先”或“引导词优先”，如图2a和2b分别显示的那样。元素优先描述如下。

- a) 分析小组组长首先选择某设计说明的一部分作为起点并对它们进行标注。这部分的设计目的要被解释，与之相关的元素和与元素相关的特性应被识别。
- b) 分析领导者应选择元素中的一个，并且在是否可以将引导词直接应用于元素本身或应用于元素中某个单独特性，与团队成员达成一致。分析小组组长首先应认同哪些引导词应被使用。
- c) 在被分析的元素和特性文档的上下文中检查首先可用的引导词解释，从而确定是否存在与设计目标之间可信的偏离。如果一个可信的偏离被识别，则检查该偏离的可能的原因和后果。在某些应用中，按照因果关系的潜在强度或者按照基于风险模型的相对风险优先队列进行偏离分类是很有用的。风险模型的进一步信息将在IEC60300-3-9中讨论。
- d) 分析小组应当识别该偏离的防护、探测和指示机理。这些机理可能包含于已经选择的部分中，或者形成其他部分设计目标的一部分中。这些机制的存在不应该打断正在探索的或已列出的潜在危险或可操作性问题，同时也不应该试图减少偏离发生的可能性或减轻其后果。
- e) 分析小组组长应当总结由记录员记录的结果。当需要进行附加的后续工作时，应记录负责进行后续工作人员的名称。
- f) 对于该引导词的任何其它解释，都重复以上过程；然后依次进行其它的引导词分析；接着对元素中的每一个特性进行分析（如果分析者对于此元素在特性方面已达到一致看

法)；然后检查当前部分中的每一个元素。当一个部分被完全检查后应标明已完成。这个过程将在所有部分中重复直到所有部分都被分析。

另一种应用引导词的分析方法是：将第一个引导词逐一用于某部分的每一个元素。当第一个引导词将该部分全部检查完毕后，再用第二个引导词依次分析所有元素。重复以上过程，直到对一个特定的部分的全部元素用完所有的引导词，再转入另一个部分。(参照图 2b)

在任何特殊的分析中选择遵循哪个顺序由分析小组组长和他的小组决定，并且受到进行 HAZOP 检查的具体风格的影响。影响决定用那种方法的其它因素有：采用技术的性质；检查所需要的灵活性；以及，在某种程度上，参与的小组成员所接受到的训练。

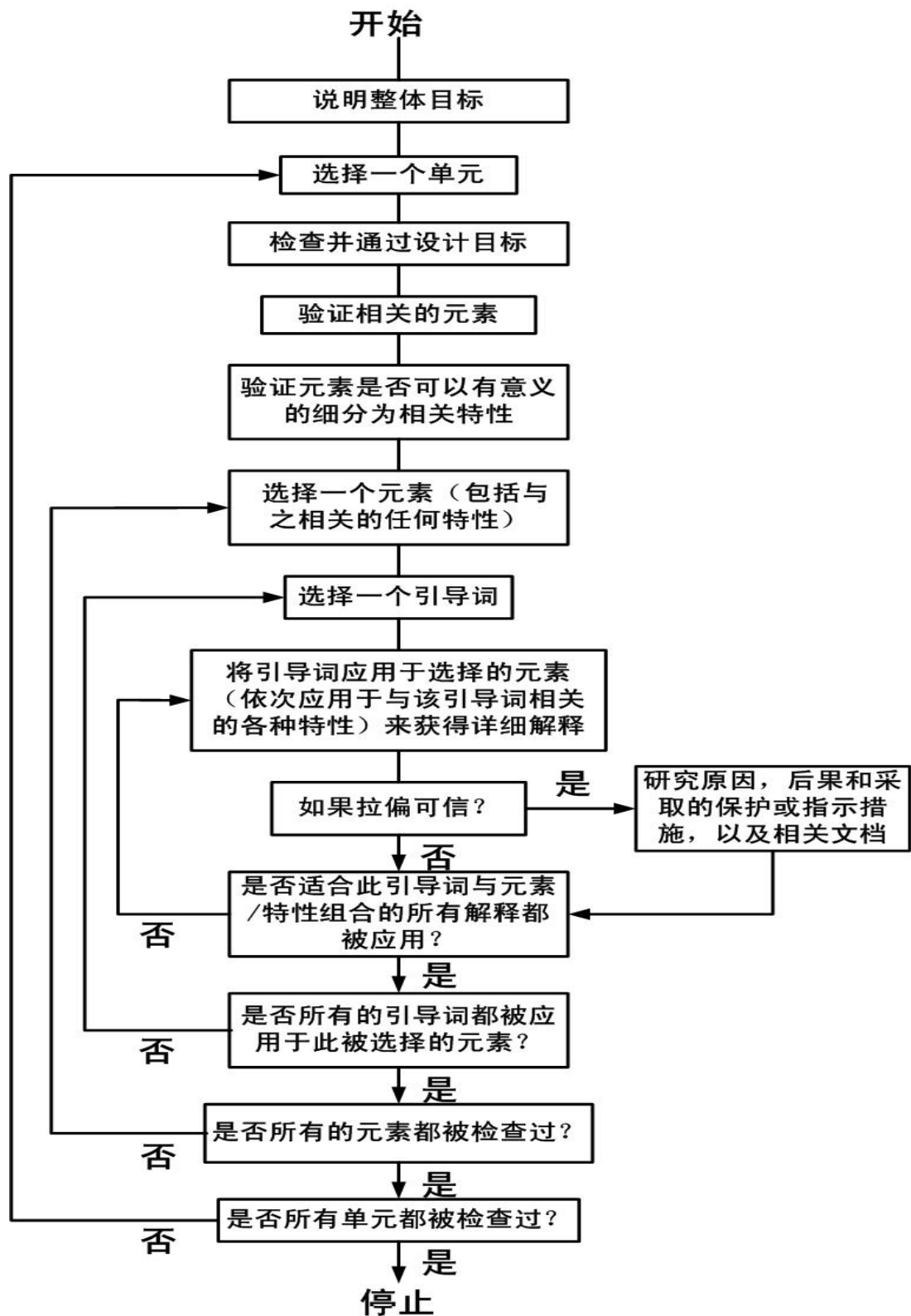


图 2a -元素优先的HAZOP方法流程图

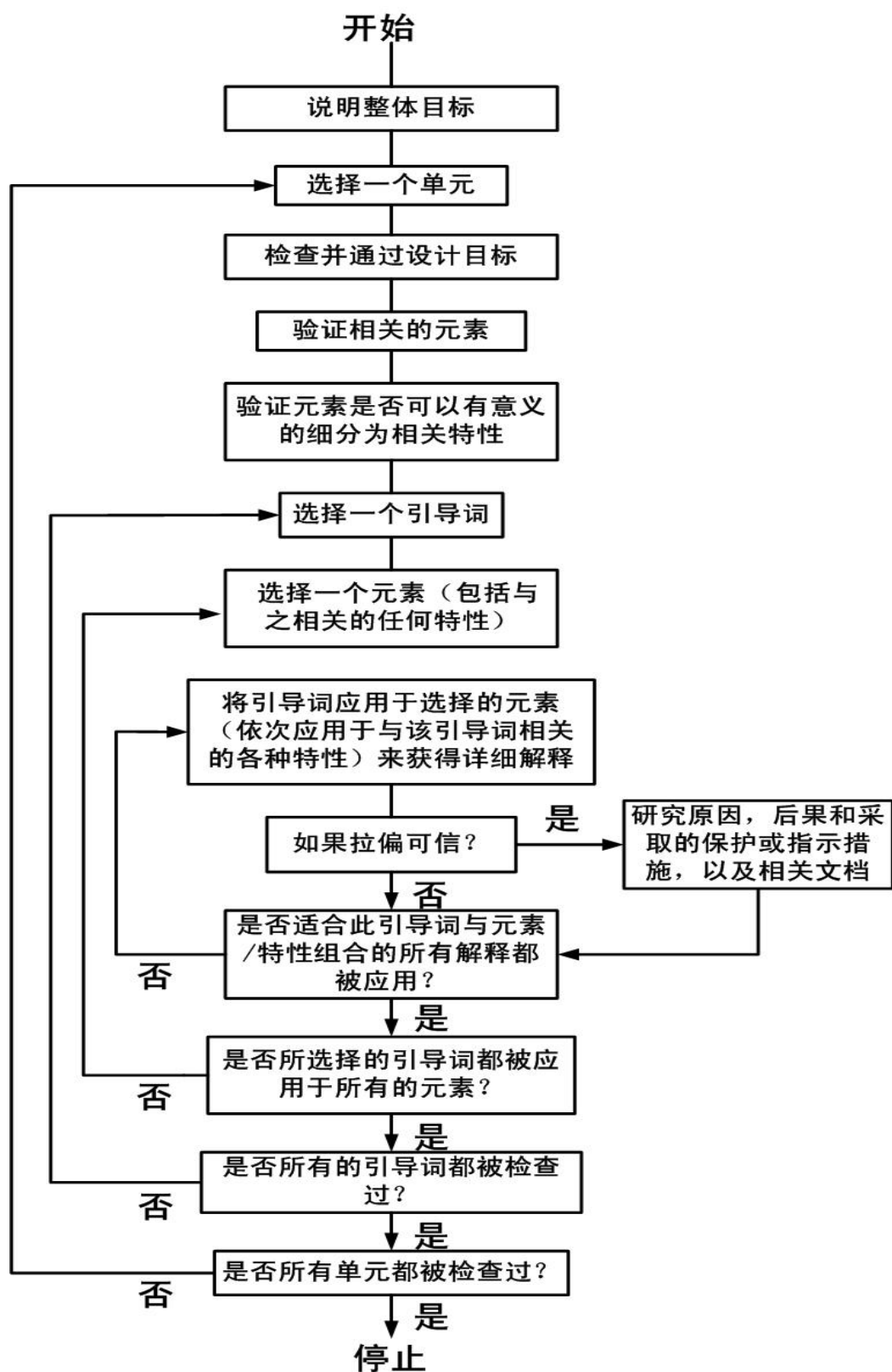


图 2b -引导词优先的HAZOP方法流程图

6.6 文档

6.6.1 概述

HAZOP 主要的优势在于它给出了一个系统的，有规律性的和文档化的方法。为了从 HAZOP 分析中充分获得效果，HAZOP 分析必须以恰当的形式存档并坚持到底。分析小组组长应当保证每次会议都产生适当的记录。记录员应当具有专业的有关分析课题的技术知识、熟练的语言能力和很好的倾听与关注细节的能力。多种记录报告的方法在附录 A 中有所讨论。

6.6.2 记录的样式

有两种 HAZOP 记录的基本方法：全部记录和只记录异常（故障）的方法。在召开任何会议之前，应当首先决定记录方法，然后相应的决定记录人员。

- “全部记录”包括记录设计说明中的每个单元或元素中的每一个引导词-元素/特性组合应用的结果。这种方法尽管比较麻烦，但它提供的这种方法很彻底，可以满足最苛刻的审查要求。
- “只记故障方法”只记录被证明了的危险以及可操作性问题（包括后续工作）。“只记故障方法”使管理文档更简单。然而这种方法没有将所分析的所有内容存档，因此对于审目的目的的作用相对较小。它同样可以在相同范围进一步的分析中起作用。通过“只记故障方法”是一种最小要求的实现，因此应当谨慎使用。

在考虑所使用的记录方式时，下列方面应当被考虑。

- 规章要求
- 合约要求
- 企业政策
- 追踪和审查要求
- 与系统有关的危险大小
- 可用的时间和资源

6.6.3 分析结论

HAZOP 分析的结论应当包含以下内容：

- 已识别的危险和可操作性问题的细节，以及相应的探测和/或减缓措施的细节；
- 如果有必要，应对进一步的特殊方面的分析给出使用不同技术的建议；
- 在分析过程中对于已发现的不确定性所采取的措施；
- 分析小组在自身所拥有知识的基础上，对已发现的系统问题的减缓方法的建议；（如果是在分析的范围内）
- 在操作和维护程序中存在的特殊点，应被标出提醒注意；
- 每一次会议的成员列表。
- 进行了分析的所有部分的列表以及任何一部分所用到的基本原理；
- 所有的图表，说明书，数据单，报告，及其它如团队所引用的修订版本号；

使用“只记故障方法”，这些输出一般情况下在 HAZOP 工作单中会被很简明的记录。

使用“全记录方法”，符合要求的输出可能需要从全部的分析工作单中提炼出来。

6.6.4 报告要求

记录下的信息应当符合以下要求：

- 每一个危险和操作性问题应分条被记录；
- 无论系统中是否已设置保护或报警装置，所有危险和操作问题和产生它们的原因都应当被记录。
- 在分析会议后，分析小组提出的每一个问题以及连同负责回答该问题人的名单应当

被记录；

- 应当采用一个记数系统，从而保证每一个危险、操作问题、疑问、建议及其他等都是唯一可识别的。
- 分析文件应该存档以便检索，如果需要，在系统危险日志中索引（如果存在的话）。

确切地说，最终的报告由谁接受，很大程度取决于公司内部政策或（安全）标准的需要，通常也包括项目经理、分析组长和分派负责执行后续工作及实施建议的人员应当得到最终报告。

6. 6. 5 文档的签字

在分析结束时，应当产生分析报告并且在分析小组中达到共识。如果意见不能达到统一，应当将原因记录下来。

6. 7 后续工作及职责

HAZOP 分析的目的并不是重新设计一个系统，同样对于分析小组组长而言，也没有授权保证分析小组的建议被采纳。

当对于已经进行过 HAZOP 分析所得出的结论要进行重要的更改，一旦需要修改文档之前，项目经理应当考虑再集合 HAZOP 小组讨论，以便保证没有引入新的危险或可操作问题或维护问题。

正如 6.3 所指出的，在某些情况下，项目经理可能授权 HAZOP 小组执行建议并完成设计更改。在这种情况下，HAZOP 小组被要求做以下额外工作：

- ◆ 在关键问题上小组要达成一致并要修订设计或操作维护规程；
- ◆ 验证修订版及所做的改动，并应将它们向项目经理汇报等待批准；
- ◆ 实施进一步的修订 HAZOP 分析，包括系统界面。

7 审查

HAZOP 分析的程序及结果应当服从于公司内部的或管理专家的审查。审查的标准和问题应当在公司运作程序中进行说明。这些可能包括：人员，程序，准备，文档及后续工作。也应当包括技术方面彻底的检查。