Q/SY

中国石油天然气集团公司企业标准

Q/SY 1362—2011

工艺危害分析管理规范

Specification for process hazards analysis management

2011-03-30 发布　　**2011-05-01** 实施

中国石油天然气集团公司　发布

目　　次

前　言

本标准由中国石油天然气集团公司标准化委员会健康安全环保专业标准化技术委员会提出并归口。

本标准起草单位：中国石油集团安全环保技术研究院。

本标准参加起草单位：大港石化公司、塔里木油田公司。

本标准主要起草人：谢国忠、李卫国、夏春英、万涛、华胜、许星。

工艺危害分析管理规范

1 范围

本标准规定了工艺危害分析的管理要求以及相关审核、偏离、培训和沟通的管理要求。

本标准适用于采油采气、油气集输、炼化生产、油气储运等具有火灾、爆炸、泄漏潜在风险的活动或过程。

2 术语和定义

下列术语和定义适用于本标准。

2.1

工艺危害分析 process hazards analysis（简称 PHA）

通过系统的方法来识别、评估和控制工艺过程中的危害，包括后果分析和工艺危害评价，以预防工艺危害事故的发生。

2.2

共因失效 common component failure（简称 CCF)

在一个系统中, 由于某种共同原因引起两个或两个以上单元同时失效。

2.3

高危害工艺 higher-hazard process（简称 HHP）

任何生产、使用、贮存或处理某些危害性物质的活动和过程。这些危害性物质在释放或点燃时，由于急性中毒、可燃性、爆炸性、腐蚀性、热不稳定性或压缩，可能造成死亡、不可康复的人员健康影响、重大的财产损失、环境损害或厂外影响。危害性物质包括任何产生上述影响的以下物质，如压缩可燃气体、易燃物、操作温度高于闪点的可燃物、反应性化学品、爆炸物、可燃粉尘、高度或中度急性中毒性物料、强酸、强碱以及蒸汽发生系统。

2.4

低危害操作 lower-hazard operation（简称 LHO）

生产、使用、贮存或处理某些物质的任何活动和过程。这些物质很少由于化学、物理或机械性危害而造成死亡或不可康复的人员健康影响、重大财产损失、环境损害或对厂界外影响。低危害性物质包括操作温度低于闪点的物质、惰性低温气体、蒸汽分配和冷凝水回用系统（所有压力等级）、低压燃料气、低毒性物质、少量的危害性物质。较低的危害性机械操作包括融化铸造、挤压、造粒或制丸、高速旋转设备、纺纱、压延、机械干燥、固体加工操作。

3 职责

3.1 集团公司安全环保部组织制定、管理和维护本标准。

3.2 专业分公司组织推行、实施本标准。

3.3 企业根据本标准制定、管理和维护本单位的工艺危害分析管理程序，企业相关职能部门具体负责本程序的执行，并提供培训、监督、考核。

3.4 企业 HSE 部门对本单位工艺危害分析管理程序的执行提供咨询、支持和审核。

3.5 企业基层单位按要求执行本单位工艺危害分析管理程序，并对实施程序提出改进建议。

4 管理要求

4.1 应用范围

工艺危害分析（以下简称 PHA）是装置生命周期内各个时期和阶段辨识、评估和控制工艺危害的有效工具。属于高危害工艺的下列情况应进行 PHA：

——研究和技术开发；
——新改扩建项目；
——在役生产装置；
——工艺技术变更；
——停用封存装置；
——拆除报废装置。

存在下列情况时也可进行 PHA：
——低危害性操作；
——设备及微小变更；
——事故调查。

4.2 应用时机

4.2.1 新改扩建项目

新改扩建项目在投用前应对所有工艺进行PHA，包括：
——在项目建议书阶段，进行危害辨识，提出对项目产生方向性影响的建议，包括考虑使用本质安全的技术，来显著地减少危害；
——在可行性研究阶段，评审自项目建议书阶段以来在项目范围或设计内容上有何变更、确认所有工艺危害均已辨识，并确定安全措施是否能足以控制所有的危害。按照国家规定必须进行安全预评价的项目，可以不再进行项目批准前PHA，但安全预评价内容必须符合本标准的要求；
——在初步设计阶段，在初步设计图纸完成后应进行PHA，对工艺过程进行系统地和深入地分析，辨识所有工艺危害和后果事件，提出消除或控制工艺危害的建议措施；
——在详细设计阶段，如出现重大变更，应补充进行PHA；
——在项目竣工验收前，应形成最终的工艺危害分析报告，此报告是项目建议书阶段、可行性研究阶段、初步设计阶段、施工图设计阶段的PHA报告的汇编。该报告应在“启动前安全检查”前完成，作为检查的一项重要内容。

4.2.2 在役装置

在役装置的整个使用寿命期内应定期进行PHA，包括：
——基准PHA。在试生产阶段，对最终的PHA报告进行再确认后，可作为基准PHA报告。PHA再确认方法参见附录A。如果期间出现了影响工艺安全的变更，应重新进行PHA。基准PHA作为周期性PHA的基础；
——周期性PHA。在生产阶段，周期性PHA至少每5年进行一次，油气处理、炼化工艺装置等高危害工艺的周期性PHA间隔不应超过3年；对于发生多次工艺安全事故或经常进行变更的工艺，间隔不应超过3年。周期性PHA可采用再确认的形式来更新，并作为下一周期性PHA的基准。

4.2.3 停用封存、拆除报废装置

停用封存的装置在停用封存前应进行PHA，辨识、评估和控制停用封存过程中的危害，保证装置封存过程及封存后的安全。

拆除报废的装置在拆除报废前应进行PHA，辨识、评估和控制拆除过程中的危害，保证装置拆除过程及结果的安全，降低环境影响。

4.2.4 研究和技术开发

涉及新工艺、新技术、新材料、新产品的研究或开发方案在实施前应进行PHA，辨识、评估和控制研究和技术开发过程中的危害，保证其过程的健康、安全、环保。

4.3 实施步骤

企业应按照直线管理的要求，根据不同的业务特点，明确工艺安全管理的部门或单位，提供实施PHA相关资源。

工艺安全管理部门或单位制定年度整体PHA计划，在具体开展PHA之前，明确PHA负责人，下达PHA工作任务书，选择工作组成员，规定PHA工作组职责、任务和目标。

PHA的实施包括计划和准备、危害辨识、后果分析、危害评价、风险评估、建议的提出和回复、

PHA报告、建议的追踪等八个阶段。PHA流程图见附录B。

4.4 计划和准备

4.4.1 工作组成员

根据PHA对象所需的专业技术和能力选择工作组成员，工作组应由多个专业的人员组成，包括设计、工艺或工程、操作、维修、仪表、电气、公用工程等，以及需要的其它专业人员。工作组实际参加人数可根据PHA的需要和目的来确定。

4.4.2 工作组成员培训

工作组组长和全程参加的人员应有PHA的经验，且每次PHA之前都应接受选择和应用的PHA方法的培训。其他成员应接受PHA步骤以及本次PHA所使用方法的培训。

4.4.3 工作职责

工作组长的职责：组织选择适当的PHA方法，按照工作计划组织实施PHA，对PHA进度、质量负责，并将PHA进展情况及结果报告PHA负责人。

工作组成员的职责：参加PHA会议，现场察看和分析，提出工艺危害清单和相应的控制措施建议，编写PHA报告，并对所分析工艺的安全可靠性做出结论。

4.4.4 工作组准备

工作组讨论PHA工作任务书，包括工作目标、范围、完成时间及所需资源等。工作组应制定PHA的工作计划，包括工作组成员任务分工、完成计划的总体时间表。

工艺技术资料的准备，主要包括危险：化学品安全技术说明书（MSDS）、工艺设计依据、设备设计依据、操作规程、操作卡片、上次PHA报告、自上次PHA以来的变更管理文件和事故调查报告等。

4.5 危害辨识

4.5.1 危害辨识清单

在PHA起始阶段，对可能导致火灾、爆炸、有毒有害物质泄漏或造成不可康复的人员健康影响的工艺危害进行辨识，并列出清单。危害辨识清单应作为下一步分析和重点讨论以及对相关人员进行培训和沟通的重要内容，并应包括在PHA最终报告中。

4.5.2 危害辨识方法

危害辨识的方法如下但不限于：

——审阅待分析的工艺和类似装置的事故调查报告；

——审阅待分析的工艺和类似装置以往的PHA报告；

——审阅变更管理文件；

——通用危害辨识检查表（参见附录C1）；

——化学品相互反应矩阵（参见附录C2）；

——专家的经验。

4.5.3 现场察看

工作组应对照平面布置图、工艺流程图(工艺管道及仪表控制P&ID)，对装置现场进行察看，确定图纸的准确性，熟悉工艺和区域布置，并补充完善危害辨识清单。

4.6 后果分析

4.6.1 后果分析内容

工作组可采用定性或定量的方法，针对危害辨识清单进行后果分析，了解潜在伤害类型、严重性，可能的财产损失以及重大的环境影响。在后果分析时应考虑以下内容：

——事故、事件的类型（如火灾、爆炸或暴露于毒性物质）；

——事故、事件的后果（包括释放量；影响区域；受危害影响的人员以及伤害类型和严重性）。

4.6.2 后果分析步骤

工作组可按以下步骤进行后果分析：

——假设所有硬件和软件防护措施都失效，可能导致的如毒性物质释放、火灾、爆炸、泄漏等最坏情况；

——用定性或定量的方法分析事故、事件的后果；

——考虑现有的防护措施是否能预防或减轻事故、事件的后果影响；

——对现有的防护措施提出建议。

4.7 危害评价

危害评价包括危害分析、防护措施分析、人为因素分析、装置定点分析、工艺本质安全分析。

4.7.1 危害分析

工作组应针对工艺上可能发生的危害事件进行系统的、综合性的分析和研究。

——分析范围。辨识每个潜在事故、事件可能出现的方式、途径和原因；针对潜在事故、事件，辨识现有的防护措施，对每个防护措施的完整性和可靠性进行评估；

——分析方法。应根据项目的不同阶段、研究对象性质、危险性大小、复杂程度以及所能获得的资料数据等选择适当的方法。常用的分析方法包括但不限于：故障假设/检查表法（What If/Checklist)、危险和可操作性研究（HAZOP）、故障模式和影响分析（FMEA）、故障树分析（FTA）。危害分析方法的介绍参见附录 D。

4.7.2 防护措施分析

评估现有防护措施的完整性和可靠性，了解现有防护措施是否足够，以便提出最终工艺安全改进建议。工作组分析、评估现有的防护措施应依据以下原则：

——独立性。防护措施成功发挥作用是否取决于其它系统的成功操作；

——可靠性。防护措施是否具有高度可靠性，是否需要人的操作；

——可审核性。防护措施的设计是否易于定期检验或测试；

——完整性。防护措施是否以正确的方式安装和维护。

4.7.3 人为因素分析

工作组在PHA过程中必须对人为因素进行分析。人为因素分析主要分析人员与其工作环境中的设备、系统和信息之间的关系，辨识和避免人为失误可能发生的情况。

——分析范围。人为因素分析主要考虑人体工效学，人机界面，注意力分散，培训、技能和表现，操作程序，维修程序。工作组在现场察看、危害分析以及防护措施分析时，均应详尽考虑人为因素；

——分析方法。可以运用人为因素分析检查表辨识和评估人为因素，或者使用“故障假设/检查表”作为人为因素分析的方法。人为因素分析检查表参见附录C3；

——分析内容。潜在人为失误情况主要包括有缺陷的操作程序，不宜操作及易误导操作人员的仪表，不合理的布置或控制设计，不合理的任务分配，没有进行有效沟通，执行程序的优先顺序；

——现场察看。现场察看重点关注控制室（如中控室、DCS室)的环境（如照明、通讯能力、噪声、布局）及有人机界面的地方（如关键信息的显示、联锁按钮的位置和标识、仪表标识、警报排列和其它控制项等），听取操作人员和维修人员的现场经验。在现场察看时，还应考虑应急防护装备的有效性及是否容易获取；

——危害分析。在危害分析时，工作组应辨识以人员因素为事故起因的潜在事故、事件。在极度依赖人员操作的工艺中，对操作程序进行分析，分析人员得到的指示是否明确，重点应放在辨识可能出现人为失误的情况；

——防护措施分析。工作组在分析防护措施时，应考虑人为因素。当防护措施需要人员的干预才能发挥作用时，应考虑人员是否有能力顺利完成所要求的规定动作，以及其它可能妨碍人员完成动作的因素。

4.7.4 装置定点分析

PHA应考虑选址、平面布置、气候条件、建筑物结构和功能设计等是否符合相关法规要求，并按本标准进行周期性评审和更新。

4.7.5 工艺本质安全分析

所有新改扩建项目应进行工艺本质安全分析。工艺本质安全分析检查表参见附录C4。

——分析范围。与工艺有关的工艺物料的基本化学特性（如毒性、易燃性和反应性）、物料处理的物理条件（如温度和压力）、工艺设备的特性，或是这些因素的综合危害，应通过从根本上消

除而不是控制方法达到提高工艺本质安全水平的目的。本方法依赖于工艺和设备内在的安全性能以防止出现人员伤害、财产损失和环境影响，而不是防止事故发生的控制系统、联锁或操作规程；

——分析时机。提高工艺本质安全水平在工艺生命周期内任何阶段都可以进行，但在项目建议书、可行性研究、设计阶段考虑工艺本质安全是最好的时机，能相对容易并经济有效地加以实施，设计单位应当在项目的前期阶段充分考虑工艺本质安全，提高装置的内在安全性能；

——工艺本质安全方法。实现工艺本质安全的方法可采用以下原则：

a) 尽量不用或少用危害物质；

b) 采用低危害物料替代或消除高危害物料；

c) 采用低危害性工艺条件（如低压）或低危害性物料形态；

d) 将危害物料释放量或能量的影响降至最小（如容器制造足以承受内部能产生的最高压力）；

e) 使发生操作失误的可能性降低到最小，或增加对操作失误的容忍度。

4.8 风险评估

4.8.1 工作组应评估辨识出的潜在事故、事件的风险。根据风险等级最终确定是否应提出建议措施。

4.8.2 风险是潜在事故、事件的严重性（后果）与其出现可能性（概率）的综合度量。工作组不能仅考虑后果的严重性而提出建议措施，还应充分考虑其发生的可能性，避免资源浪费。

4.8.3 工作组可用本标准所列故障假设/检查表、HAZOP、FMEA 等 PHA 方法在危害辨识、防护措施分析、危害分析等阶段，定性或定量地确定每个危害事件发生的可能性，并运用此信息，结合潜在事故、事件的后果分析，对每个潜在事故、事件的风险进行定性或定量评估，确定该风险是否可接受。定性风险评估规则参见附录 E。

4.9 建议的提出和回复

4.9.1 提出 PHA 建议时应考虑以下关键因素：

——建议内容与工艺危害直接相关；

——风险等级；

——建议应明确。

4.9.2 PHA 建议应经过直线领导审查。直线领导应做出书面回复，可采用完全接受、修改后接受或拒绝接受的形式。

4.9.3 出现以下条件之一，可以拒绝接受建议。

——建议所依据的资料是错误的；

——建议对于保护环境、保护员工和承包商的安全和健康不是必需的；

——另有更有效、更经济的方法可供选择；

——建议在技术上是不可行的。

4.9.4 如果采取另一种解决方案、或者改变建议预定完成日期、或者取消建议等，应形成文件并备案。

4.10 PHA 报告

4.10.1 内容要求

——PHA 报告应内容详尽、文字简洁，便于相关人员清楚了解工艺危害、潜在事故、事件，控制危害的防护措施和防护措施失效的后果；

——工作组提出建议的思路和依据应在报告的相关章节中完整的描述，为制定解决方案的人员提供详细的信息，并有助于在以后的 PHA 中避免重复工作；

——PHA 报告原件应包括工作组工作的所有文件，包括所选用的危害分析方法、分析过程的记录、参考资料目录和其它有关的支持性文件等。

4.10.2 批准与分发

PHA 报告经批准后方可分发，其分发范围包括上级主管部门、所分析装置的负责人、工作组成员和同类装置负责人员。

4.10.3 PHA报告格式

PHA 报告编制指南参见附录 F。

4.10.4　沟通

应将 PHA 报告的相关内容与可能受影响的所有人员进行沟通，必要时进行培训。

4.11　建议的追踪

对于在役装置的 PHA 建议，应定期公布尚未完成的建议并提交给指定完成建议的人员及其主管；对于新改扩建设施的 PHA 建议，应由项目负责人进行监督、跟踪。如果不能保证实施建议所需的资源，应及时报告直线领导。

5　审核、偏离、培训和沟通

5.1　审核

集团公司、专业分公司和企业都应把工艺危害分析管理作为审核的一项重要内容，必要时可针对工艺危害分析管理组织专项审核。

5.2　偏离

企业依据本标准制定本单位工艺危害分析管理程序时发生的偏离，应报专业分公司批准；企业工艺危害分析管理程序执行时发生的偏离，应报企业主管领导批准。偏离应书面记录，其内容应包括支持偏离理由的相关事实。每一次授权偏离的时间不能超过一年。

5.3　培训和沟通

本标准应在集团公司范围内进行沟通。企业所有相关的管理、技术人员都应接受本标准培训。

附 录 A
（资料性附录）
PHA 再确认方法

A1 概述

A1.1 在初始 PHA 完成后，按本标准规定的周期（3 年或 5 年），应由一个符合本标准要求的工作组对 PHA 进行再确认，以保证 PHA 与装置的实际情况相符。对于多次发生工艺安全事故、具有重大危害或经常发生工艺技术变更的装置，应考虑将再确认的周期调整到 3 年以内。

A1.2 下文所述是对以前的 PHA 进行再确认的过程。首先应确定上一次的 PHA 是否符合 PHA 基准的要求，以及是否按照本标准要求进行的。然后，检查自上一次 PHA 以来已实施的所有变更和工艺安全事故，确认是否对这些变更的相关危害及事故原因进行了充分分析。再确认的结果应当是一个新的、准确反映了工艺设备状况的 PHA 基准。

A2 程序

在启动再确认过程前，工作组应确定先前的 PHA 是否符合 PHA 基准的要求。如果确定上一次的 PHA 中有严重的不足和疏漏，应做一次新的 PHA，而此程序也不再适用。

A2.1 资料收集

A2.1.1 必须收集大量的资料以评估自上次 PHA 以来实施的变更和工艺安全事故资料。

A2.1.2 工艺安全技术信息应齐全并符合实际情况。

A2.2 评估工艺变更

工作组的经验有利于确定自上次 PHA 以来进行变更的数量和重要性。必须对以上要求收集的资料进行审阅，以便辨别和评估已实施的变更。如果发现工艺上有重大变更，应重新做一次 PHA。

A2.3 核实上一次 PHA 的质量

可以用 PHA 再确认检查表（参见附录 C5）来检查上一次的 PHA 的质量。对没有完全符合检查表要求的条目应标记出来，并在再确认的过程中加以更新和补充。此外，PHA 工作组应查看上一次 PHA 中所用的分析方法（如故障假设法或 HAZOP 方法）及提出的问题和建议，判断其是否仍然适用于现有的工艺设备状态。

A2.4 PHA 完整性

上一次的 PHA 可能未包括所有的 PHA 要素，如：

——后果分析；

——装置定点分析；

——人为因素分析；

——工艺本质安全分析。

如果未使用这些分析方法，应作为补充内容加入到更新后的 PHA 中。

A2.5 工艺变更评审

A2.5.1 应对自上次 PHA 以来工艺流程中实施的变更进行评审，检查是否在危害控制方面对这些变更进行了充分的分析。

A2.5.2 如果有些变更项目已做过 PHA 分析，应首先检查这些 PHA，确定是否所有的危害已得到辨识，是否已经确定潜在的严重后果，并制定了相应的防护措施。然后将这些 PHA 作为一项更新内容包含在再确认的文件中。

A2.5.3 变更如没有进行详细评审，应对变更重新进行一次新的 PHA 分析。

A2.6 运行经验

如果自上一次 PHA 以来多次发生了工艺事故或事件，应重新做一次 PHA。如果只有少数意外事件，可以把事件或事件的分析内容应用到现有 PHA 中。

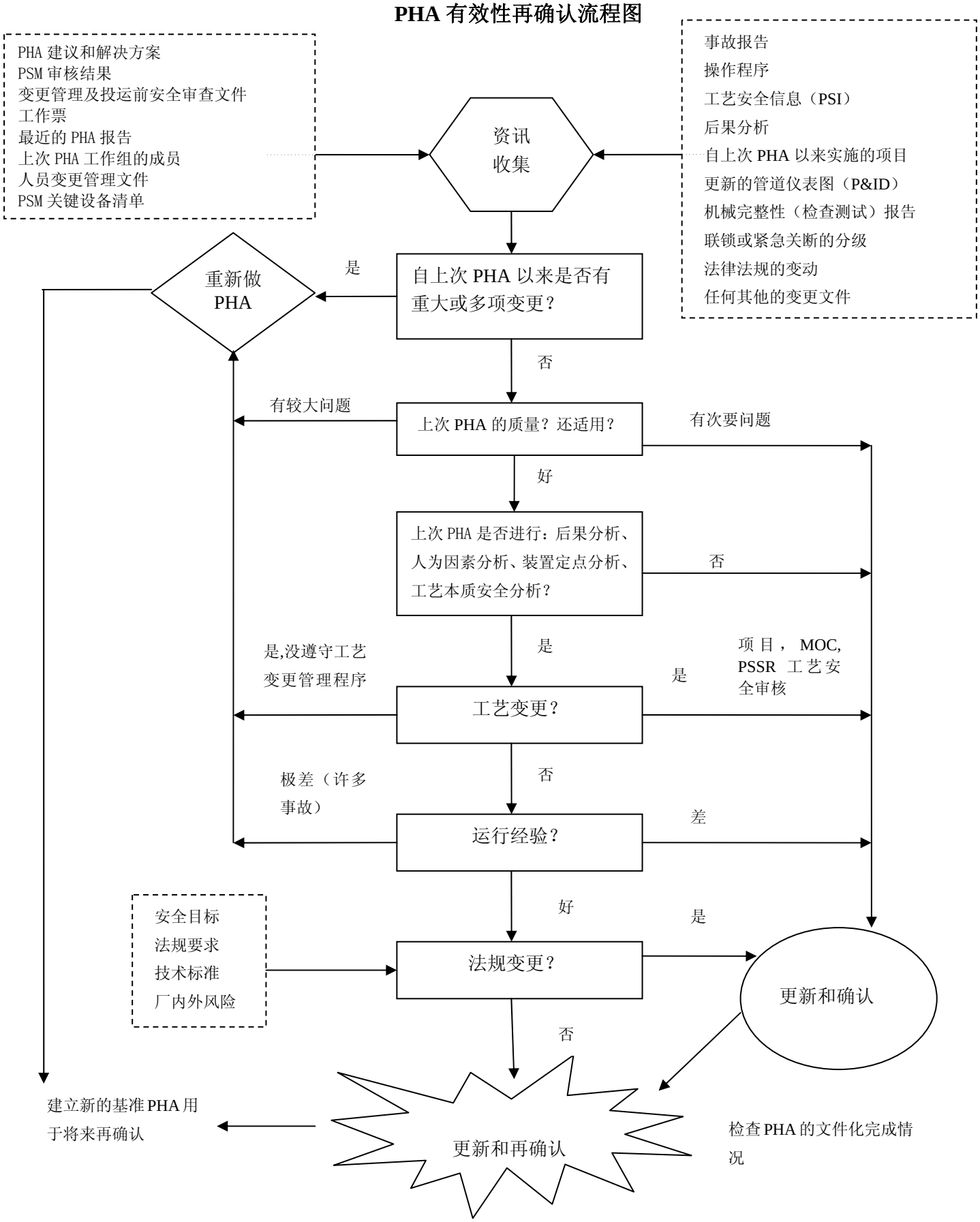
A2.7 法规变更

如果自上次 PHA 以来，出现了法律法规方面的变化，这些变化应应用到再确认过程中。

A2.8 新的 PHA 基准

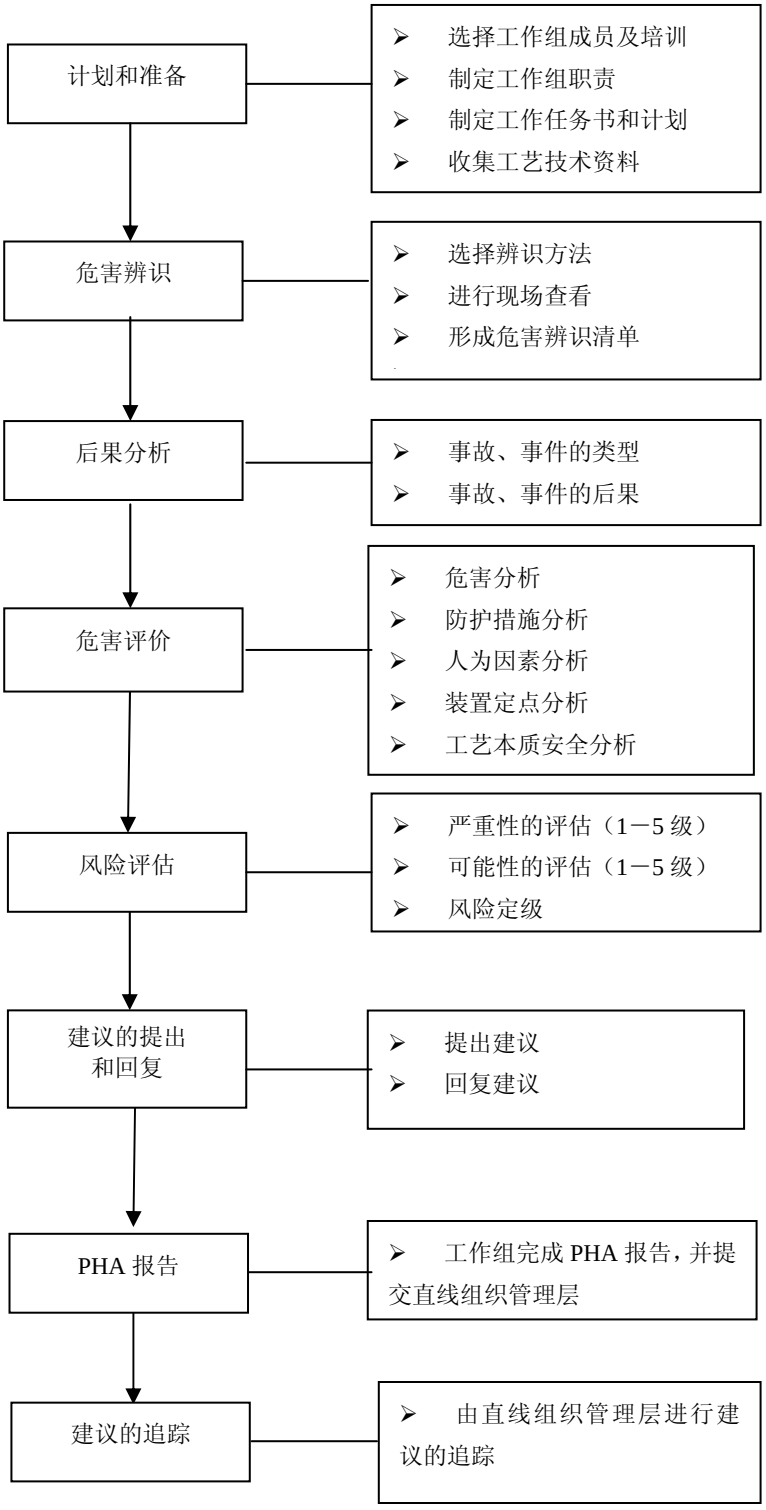
有效性评估的目的是建立一个新的 PHA 基准。如果可能，通过修改、更新、补充上一次 PHA 基准的方法发布新版本。如果以修改原 PHA 文件的方式更新 PHA 困难时，可行的方法是编写补充文件以附件形式附在原 PHA 文件后。在本周期结束时，这个新的基准 PHA 应是下一次有效性再确认工作的起点。

PHA 有效性再确认流程图



备注：PSM——工艺安全管理　MOC——变更管理　**PSSR**——启动前安全检查

附 录 B
（资料性附录）
PHA 流程图



附 录 C
（资料性附录）
PHA 检查表示例

C1 通用危害辨识检查表

危害辨识是辨认可能造成火灾、爆炸、超压、中毒、冻伤、化学灼伤、核辐射、高温、环境污染等重大事件的原因。

通用危害辨识检查表（范例）

序号	危害	问题
1	火灾	是否涉及可燃/易爆的物料？
		这些物料是否根据相关的标准采用合适的火灾编码进行标志？
		是否存在显示出上述某方面不完全、不充分的特殊情形？
		回答这些问题我们是否需要知道一些东西？如果是，我们怎样才能获得这些信息？
		列出所有的火灾危险及其潜在危害。
		……
2	爆炸	是否存在由于物理性的过高压力而带来的潜在爆炸？
		是否存在由于易燃物在空气中的燃烧而带来的潜在爆炸？
		是否存在由于流程液体的混合造成的燃烧而带来的潜在爆炸？
		是否存在由于非正常反应、分解、放热、聚合等而带来的潜在爆炸
3	物理性超压	高压气体是否会窜入低压容器？
		超压的机理是否正常并被很好的理解？
		按照常规标准设计的泄压、排放设施是否能提供足够的保护？
		超压的机理是否不正常或太复杂，以至常规的安全装置不够？
		为理解此危险我们是否需要知道一些信息？如果是，我们怎样才能获得？
4	易燃物在空气中的燃烧	控制适当的比例（如燃烧器管理系统）、防止空气泄漏（如惰性气体化）和消除点火源（如区域分类，防静电措施）等传统方式是否足够以预防爆炸？
		我们是否知道所有用以界定爆炸界限的必需资料？如果没有，我们将怎样获得它？
5	工艺流程中液体的混合而引起的燃烧	每个工艺流程（包含温度、压力、化学试剂、凝固点等）都具有特殊性，因此需要为其设计特定的预防措施。我们是否掌握了所有用以避免不同液体混合的界面，以及确定界面的必要数据？
6	非正常反应等	这些需要给予特别的关注加以理解和识别所有潜在的原因，因此这些通常都被列为流程危险而需要特别的关注。我们是否拥有所有用以界定这些危险的信息，如果没有，我们怎样才能获得它？
7	中毒	列出所有涉及到的毒性试剂。
		进入受限空间作业时，是否会暴露于有毒气体中？
		为避免人员接触毒性物质，采取了哪些好的工程设计和传统的安全实践？
		哪些释放的毒性气体会对雇员造成致命的危险或让邻居讨厌？
		我们是否拥有足够的毒性数据以界定危险的程度并且决定需要多少额外的工作（而不仅仅依赖于好的工程设计以保证化学试剂完全密闭）？
		我们是否需要引入毒物、卫生或工业安全方面专家？
8	噪声	通常噪声并不意味着流程危险，但是通过提问也许会引起新的发现。通常的噪声问题应该由 PHA 之外的努力加以关注。为雇员评估潜在的噪声问题。必须达到规定要求。很多时候工程解决方案会比行政方案带来更好的效果。存在哪些噪声危险？

序号	危害	问题
9	辐射－核	诸如水平测试装置的传感器中的放射源只要密闭良好通常就不认为是流程中的危险。处理这些问题已经确立了一些程序，而且这些良好的设计和操作程序应该足够处理这类问题。是否存在一些核辐射需要特殊而不寻常的预防措施？如果是的话，把它作为流程危险记录下来，并确定我们需要什么信息来界定危险的界限。我们在哪能得到这些信息？
10	辐射－电磁	是否存在电磁辐射？它是否覆盖有能明显识别的预防措施？向合适的管理人员咨询这些预防措施并确保它们融入了设计。
		流程中是否存在特别的电磁辐射，没有覆盖如下能良好识别的预防措施？如果是，把该电磁辐射记录成流程危险并确定需要哪些信息来界定危险的界限，并且在哪能得到这些信息。
11	辐射－热	确保这种发热表面在设计和安全中考虑了操作者的防护。是否存在某些对操作者、邻居、设备等具有特别危险的发热源（如火焰）？如果是，把它们该电磁辐射记录成流程危险并确定需要哪些信息来界定该危险的界限
12	污染	许多污染方面的考虑不是流程危险，应该由良好的设计程序来解决并通过正常的环保努力加以处理。是否存在重大的污染问题？我们是否拥有处理这些问题的信息？
13	污染－外观	是否存在一些详细说明了美观，限制了高度、颜色或其它视觉效果的规章或构建代码？这些是否会成为潜在的流程危险？
		其它的视觉效果，如蒸汽云、闪亮的火光等，也许会让邻居觉得惊慌，应该被看成流程危险并加以相应的处理。是否存在重大的视觉冲击？
14	污染－泄漏	所有因偶然或故意而可能发生泄漏、溢出或排放的东西，不管是持续的、固定的还是突然的，都应该被认为是流程危险。这包括排放阀的泄漏、清洗口、排水管、密封管和法兰泄漏、密封圈的溢流等。这也包括用完的催化剂，柱状封装，空的圆桶，洗涤物，从管道、水管、热交换器等清洗下来的污物，或流程中没有耗完而需要处理的东西。此流程会排放出哪些化学物质？
		我们需要请教哪些顾问人员来帮助我们确定哪些排放需要管制而应加以许可或进行报告？
15	污染－灰尘	灰尘，不管是产品还是如矿石和焦炭的原材料，如果迷漫的话都会造成邻居相当的不愉快。释放这些物料时潜在的危险是什么？
16	污染－气味	是否存在一些有害的气体，会或感觉会对雇员和邻居带来危险？
17	财产损失	尽管财产损失不一定是工艺流程的危险，对考虑之下的主要工艺流程所有部分的偏离或失效，都应该考虑其是否会因为质量问题、停工期或设备的不可使用而造成重大的财产损失。所有这些关键的设备都应该记录，而给予可能超出 PHA 的努力之外的特殊关注。存在哪些重大的财产损失的风险？

C2 化学品相互反应矩阵

评估化学品相互反应的方法是编制一个矩阵图，通常矩阵应包括所有的物料，并应考虑管道系统和容器的材质与物料可能发生化学反应的情况。下表给出了编制化学品相互反应矩阵的示例。

化学品相互反应矩阵

A / B	Cl_2	丁二烯	HCl	空气	过氧化物	润滑油	钢
Cl_2	N	Y	N	N	Y	Y	Y
丁二烯		Y	Y	Y	?	?	N
HCl			N	N	Y	Y	Y
空气				N	Y	N	N
过氧化物					Y	Y	?
润滑油						N	N
钢							N

注：1.A 与 B 反应会造成问题吗？Y=是，N=否，?=不知道；

2.列表中应包括原料、中间产物、产品、废弃物等所有物料；

3.对于每个“Y”，该反应和反应必需的条件应被记录。

C3 人为因素分析检查表

人为因素检查表(范例)

人为因素是贯穿于工艺安全管理系统每个方面的一个普遍因素。相应的，人为失误在工艺安全事故中就成为一个重要的因素。这份检查表提供的问题，目的是促进小组讨论人为因素。它的目的不是要覆盖工艺安全管理每个要素里的所有情形，而是对通常包括在工艺安全分析范围内的部分，协助分析小组对易于诱发人为失误的情况进行辨识和消除。而其余部分则更适于归在工艺安全管理的分析组的工作范围里。

PHA 小组应当关注发现有整改需要的发展趋势。这里提供了一些问题的例子，这些例子的目的不是限制讨论，相反是帮助澄清提出这些问题的目的。

检查内容	问题
管理体系 通过建立和管理展示，来减少人为失误易发情况的管理承诺的政策，管理层对日常操作中人为因素的重要性定下基调并建立清晰的责任预期同时提供资源，以促进员工对人为因素的理解，以及最重要的一点——建立一个不以追究责任为目的的氛围，通常是达到上述目标的最佳做法。通过下面的问题发掘出的，也许正是表明管理体系范围内问题的症状。	1、管理层是否对员工的违章行为或违背操作规程的做法采取默认和置之不理的态度？是否以随意的口头指令来指导员工的操作？
	2、工作环境，如设备、设施总体的整洁和拥挤情况是否维持在一个可接受的程度；或是否习惯性的容忍，直到情况变得不堪忍受？是否有证据表明情况有恶化的趋势？
	3、是否所有意外事件都被确认（例如是否存在未经正式调查的关于夜间发生事件的传言）？事故调查报告是否发现了根本的原因(不是肤浅的或表象的)？随后的改进工作是否完成并确认？
	4、是否对工艺安全管理的各种要素进行过审查？管理层对做出的建议的反应如何？
	5、是否所有的人都理解安全规章？员工是否对其执行负有责任？员工是否充分了解安全的重要性和违反程序的纪律处分？
	6、是否有有效的方法来发现和改正由于酗酒或药物滥用造成员工不在工作状态的现象？
	7、是否有有效的方法来发现并更正员工的身体和精神能力已经不能满足生产任务要求的情况？
	8、当员工感觉到他们的工作表现可能受过度疲劳影响时，管理层是否有有效的方法来减轻他们的疲劳？
	9、有没有方法来识别在某一方面是否存在容易诱发人为失误的情形？如果发现了管理层反应速度如何？
	10、员工是否有清晰的、成文的指南判断何时采取措施来关闭一个单元或中断一项行为，以免因为担心事后被质疑决定的正确性而干扰了决策过程？
	11、人员变动频率是否维持在可接受的水平？是否有程序控制人员变更，来保持管理和技术队伍的稳定性？

检查内容	问题
操作规程 一个内容清晰、写得好的操作规程会显著降低出现人为失误的风险。下面的问题能够帮助 PHA 小组判断对工艺安全有明显影响的操作规程的完整性和质量。	1、相关的操作规程是否存在？例如开车、停车、闲置、正常运行和紧急情况等？
	2、是否确定了主要的紧急情形？是否有相应的操作规程用于这些紧急情形的控制，与现场操作人员的协调，并将人员和财产的损失降到最小程度？员工是否能方便的获取并理解使用这些操作规程？
	3、操作规程是否清晰和完整？术语的使用上是否统一并与使用者的理解水平相匹配？
	4、操作规程是否保持更新？是否对操作规程进行例行审查（如工作循环分析 JCA），与使用者的行为进行对照，并进行适当的修正？
	5、操作规程的编写和审核工作是否有操作规程使用者的参与？
	6、岗位配备的操作规程是否是最新修订版本？操作规程是否作为受控制的文件得到维护，并且严禁未经授权的复制而导致混乱？
	7、员工获取操作规程是否容易和快速？操作规程是否编有合适的索引？
	8、是否有用于核对关键或复杂操作的检查表？检查表是否与操作规程上的指导保持一致？
	9、如果操作程序文件中某些章节的页面带有颜色，纸张的颜色编码是否统一，并被使用者理解？患有色盲的员工是否能辨认这些颜色编码？
	10、操作规程是否指出了“为什么这么做”而不仅是“怎么做”？ 操作规程里是否包含了关于危险源的警告、注意事项或解释？
	11、是否有“程序陷阱”（也就是说操作顺序是否按照合适的顺序描述，例如在要求的操作步骤前先给予解释性的警告，而不是在这之后）？
	12、如果同样的工艺或设备有不同的配方或配置，操作规程是否清晰的表述了什么时候和如何使用这些操作指导？是否有检查方法来确保所使用的程序是对应某配方或配置的正确程序？
	13、故障排查、工艺异常的响应或应急程序中留给诊断和更正问题的时间是否实际可行？（也就是说，情况是否会在组织起有效的响应之前失去控制？）
	14、是否有太多的变更文件（例如检验授权，临时程序）以至于员工无法对每个文件的情况都充分掌握？
	15、关于操作规程改动的信息，其交流的质量和效果如何？
培训 良好培训的效果超出了对操作规程的遵守和实践。它融合了对程序设计理由的理解以及对偏离操作规程可能造成的后果的了解。	1、人员是否理解： a. 工艺的潜在危险源和危害？ b. 对危险源和危害的防护措施是什么？ c. 哪些是关键的安全装置、联锁、事故控制设备和管理控制措施？ d. 为什么设置这些控制措施，以及它们是如何实现控制作用的？
	2、进入一个区域的员工，他的培训内容是否同时包括通用的和针对具体区域的安全规章，以及关键的应急程序？
	3、是否为如何使用各工种专门的应急装备提供了培训？
	4、纠错程序（在操作失误后使用）是否包含在综合培训内容内？
	5、信息交流和交接责任方面的培训是否组织操作小组一起接受培训？
	6、培训内容中是否包括不经常使用但是非常重要的技能和知识？
	7、故障排查技巧是否包括在培训内容中？
	8、操作者是否就如何发觉紧急情况得到相关培训？是否组织过符合实际情况的演习以检测员工对这类事件的反应？
	9、某个岗位员工的培训需求（或应掌握技能）是否准确的反映了包括例行的和非例行的操作要求？
	10、人员是否根据岗位所需的技能进行工作分配？
	11、对于在职培训的操作员是否有一个有效的监督和导师计划？
	12、是否确定哪些是关键的维修保养程序，这些程序内容是否易懂、准确？

检查内容	问题
任务设计和组织 任务的正确设计和对责任的清晰理解能极大的减少出现人为失误易发情况的风险。	1、操作员的工作描述是否清晰明确（例如是否存在职责的交叉和空白，由于相关职责的模糊不清而出现重要任务被遗漏的可能性）？
	2、是否有部分工艺流程存在界面不清的情况进而可能导致职责不清？
	3、当几个不同的任务分配给同一个人时，这些任务能否在一段有限的时间内无人照顾自行运行，而操作员在做分配的其他任务？
	4、员工精神和身体上的工作负担是否在合理的水平上（就是说在一个持续几个小时而不会感到过度疲劳的水平上）？如果有高强度工作负担的话，是否局限于较短的时间内，并在两次之间给员工留有充足的恢复时间？
	5、工作环境是否会出现长时间持续的精神或身体上的无动作状态或个人独处情况（例如，在需要时得不到帮助，有离开原处寻求同伴/帮助的冲动，长时间平静无事的看守造成的感觉迟钝）？
	6、对于需要持续监看的“系统”（例如面板，DCS，进入受限空间作业的监护人，动火作业的监护人），是否有一个强制执行的制度，确保该系统在运行时候一直被监看到？
	7、是否有一些高速、高精度的或高度重复的工作由手动完成？发生错误的可能性是否因此而增加？失误的后果是否可以接受？
	8、手工操作的配料工作（例如给一个反应器加料），是否设计有办法避免加料数量错误或多次重复加料？
	9、手工操作的配料工作，是否对原料的称量和计量装置实行控制（就是说根据设定的频率校验精度）？
	10、当操作顺序被打断时，是否有辅助手段帮助员工找到他们进行到工序中哪一步？工序一旦混淆其后果是什么？
人体工程学 关注操作环境，人－机界面以及人－系统界面，在避免人为失误易发情况方面是非常重要的。	1、关键性的设备控制件（例如停车开关、阀门）是否设置在发生紧急情况时能顺利够触到的地方？（例如，员工是否需要穿过泄漏物料或火场，才能够到紧急切断部件？）
	2、是不是有的操作员的身体状况或能力不能操作或者佩带应急装备
	3、在设施的设计时是否考虑到环境条件（温度、照明和气候）？它们对成功的启动或应急装备的影响是否被评估过？
	4、是否有任何操作需要长时间穿戴过多的或繁重的个人保护装备，造成身体上的束缚或精神无法集中，以至于妨碍操作员在适当的时间内安全的完成一项操作？
	5、对于完成速度是关键因素的任务，空间的拥挤是否对其有影响（例如到关断装置的应急通道，撤退路线等）？
	6、在设备的周围是否预留了足够的空间以便进行需要的维修任务？（例如，拧紧某个法兰上的一个螺栓是否因为周围的空间太拥挤而变得很困难？）
	7、是否为要求的任务提供了合适的工具？（例如，在某个工段，因为没有人力气够大可以拧紧螺栓，易燃性气体经常性从高压热交换器里泄漏出来，购买一个液压螺栓紧固器就能解决这个问题。）
	8、员工在不误动操作面版的前提下能否方便顺利的跨越、经过操作面版（例如，紧急停车按钮上是否有罩板？如果有，还应保证在紧急情况下，罩板不会限制按钮的使用。）？
	9、相同或相似的设备会不会容易引发误操作（例如：①应在 A 单元进行的工作放在 B 单元上进行；②把槽车卸货管线误接到错误的位置。）
	10、对于关键的管道、阀门、罐槽和现场指示灯这类设备，是否有清晰明确的标识？有无专人对这些标识的维护工作负责？责任是否明确？
	11、是否有背景噪声或其它的分散/打断注意力的因素？听力保护装备是否妨碍了交流？
	12、员工是否对现有系统自行做出一些改动，说明设计中有人为因素方面的缺陷？（例如把一块纸板盖在电视屏幕上减轻屏幕反光，或者在不必要警报喇叭上贴上封带。）

检查内容	问题
控制系统	1、是否有不必要的警报分散了工人的注意力或使得更重要的警报被忽视了？
	2、控制方案是否进行了适当的记录归档，使用者是否理解？
	3、控制系统的标识用语是否统一并清晰易懂？
	4、对于警报、警示灯和警报喇叭这样的装置，其外观（声音）在流程的不同区域是否保持统一？
	5、如关键的控制器和手动干涉之类的装置是否有可能与普通的控制器相混淆？（提示：观察控制器的布置和互相之间的靠近程度。）
	6、在紧急情况中，当很多警报声同时响起时，操作者是否会有效的判断？如果是那样，是否有方法区分出最重要的警报？
	7、在紧急情况时，采取相应的对策是简单容易还是复杂困难?（需牢记的是在紧急状态，一个过于复杂的响应计划不太可能被成功的执行。）
	8、控制器的设计是否与人的直觉相反或违反了大多数人的习惯？ **注意**：大多数人的习惯指的是在人群中一种根深蒂固的行为风格；例如习惯将顺时针方向认为是关闭阀门的方向。
	9、是否有的区域过程控制/警报的颜色或声音用法与其它工段的用法相反？ **注意**：这对调入或调出该区域的工人将是一个很大的问题。
	10、用手动控制取代自动控制的判断指南是否清晰和明确？系统能被设置为自动或手动控制模式的条件是否被使用者所理解？
	11、是否提供了在正常和异常的情况下正确操作所需的相关信息？
	12、当选择警报设置时，是否考虑了反应时间（仪器/DCS 系统的延迟时间和人的反应时间）？
	13、仪器(或视频显示终端)延迟/刷新时间是否太长以至于操作者有可能出现过度调节的问题？
	14、是否有有效的方法发现仪器的故障？如果关键仪器给出错误的读数，可能会造成什么样的操作失误？
	15、指示器（(例如条形图表制图笔、刻度盘、视频显示)是否可能卡住，从而导致不能显示工艺的实际参数值？
	16、在控制系统设计中是否有隐含的假设在工艺条件异常的情况下可能变得不成立(例如当流体密度发生变化时液位信号出现失真)?
	17、如果控制设置或显示有改动，使用者是否总能得到通知？
	18、有权限调节控制设置的员工是否得到有效的培训？
	19、系统设计是否避免了过度敏感的过程控制?换而言之，控制器是否有一个合理的动作范围？（例如，如果试图用每半转流量值就变化了 1000GPM 的控制旋钮将流量控制在 50GPM，操作失误就很可能会发生。）
	20、仪器是否定期校准或检查？
	21、仪器检查是否校验了整个的仪器回路？（例如，测试警报时，要从现场传感器发送信号，而不是从同在控制室（CCR）里的压力开关发送信号。）
	22、仪器故障能否得到及时修复？是否有长期将联锁/警报旁路的迹象？
	23、控制系统中是否有自动的联锁旁路或警报抑制设计？如果有的话，有什么样的控制措施防止这些设计被滥用？
	24、关于面板和就地仪器的控制： a. 控制器是否清晰而不杂乱拥挤？是否对其进行维护？ b. 需要的地方实行颜色编码了吗？颜色编码是否是统一？（色盲会引发问题吗？） c. 对相似的设备布置是否也是相似的？（类似设备之间是否有相当的区别以避免混淆？） d. 控制和显示是否读取容易？ e. 警报声调/信号是否可区分？

检查内容	问题
	25、关于视频界面： a. 如果显示屏出现故障，是否有冗余渠道可以获取信息？ b. 同一个控制面板可以控制多个控制屏幕时，是否可能出现一面看着错误的屏幕一面进行控制调节的情况？不同的（但看起来是一模一样的）单元是否有相似的控制屏幕？ c. 如果屏幕停止刷新信息，使用者能否很快的意识到？ d. 使用者是否有时间来确定警报的来源，还是警报信息在屏幕上上翻得太快？ e. 屏幕显示的信息是否太多？ f. 视频显示器的数量是否够用来同时显示需要显示的工艺过程？
	26、关于可编程电子系统: a. 是否有适当的检查来避免计算机编程错误？ b. 是否有程序，在安装商业软件或更新软件版本后负责相关的介绍和后续工作？ c. 是否有适当的控制措施来确保软件修改工作只能由有资格的和有能力的人员进行？ d. 如果可编程电子系统里包括安全联锁，是否实行了不同的冗余逻辑方案？ e. 如果有旧的手动（或低级的半自动）控制系统被保留作为主系统的后备系统，关于如何使用这些旧设备/控制的的复习培训和操作者技能展示是否进行过？ f. 软件安全联锁是否有完善的记录存档，记录中是否包括其工作原理的书面描述？ g. 可编程电子系统的故障是否会产生随机的输出信号？发生这种情况后操作者如何才能发觉？是否有相应的修复程序？ h. 系统如何避免数据输入错误？

C4 工艺本质安全分析检查表

本检查表可用来指导设计、PHA、事故调查以及其它工艺改进工作，可采用“头脑风暴”方式进行充分思考和分析，对不能在现有装置中使用的想法，若不被采纳，也应记录并保留，为将来的工艺改进工作提供参考。

工艺本质安全分析检查表（范例）

序号	检查内容	问题
1	消减	是否减少危害物料的使用或使用量？
2	替代/消除	是否能用其他的工艺或化学反应来替代或消除危害原料、工艺中间体或副产品？
		是否能用改变工艺条件来替代或消除危害原料？
		是否能用较低危害的原料替代（如不燃的、低活性的、更稳定的、低毒性的等）？
3	减少/缓和	能否保持原料供应压力低于接收容器的额定工作压力？
		能否通过加催化剂或使用更好的催化剂使反应条件（如压力、温度）更为缓和？
		是否能通过其它途径使工艺条件更为缓和？例如:通过设计升级提高反应器的热力学或动力学效率（如改善混和或传热）以降低操作温度和（或）压力。
4	限制影响	能否将容器设计或制造成足以承受工艺过程中可能产生的超压？
		设计是否考虑设备由于温度变化造成的影响（如强度的降低、耐腐蚀性等），从而避免依赖外部系统（如冷冻、加温）来控制工作压力超出设计范围？
		能否用被动的限制泄漏技术限制可能出现的封闭性失效？
5	程序简化、操作失误容忍	能否通过简化工艺流程减少危害相互作用的可能性？
		是否在设备设计时考虑因操作或维修失误而引起的危害？
		通过程序设计降低因操作或维修错误而引起的危害？
		是否在设计时考虑设备的布置？（如便于操作和维修）

C5 PHA 再确认检查表

PHA 再确认检查表（范例）

序号	检查内容	问题
1	对危害清单的复核	是否包括了所有的危害？
		所有的危害的定义和特征描述是否仍然适合？
2	适用的 PHA 方法的运用情况	先前 PHA 中分析方法是否得到正确运用？
		结论是否正确？
3	重新进行 PHA 的情况	自上一次 PHA 后发生的或任何可能会导致灾难性后果的事件，是否重新进行 PHA?
4	预防或减轻灾难性后果的硬件和软件控制措施	所有的控制措施是否仍然落实有效？
		自上次 PHA 分析以来是否做过修正？
5	人为因素	有没有会影响到先前 PHA 结论的控制措施或人员的变动？
6	工艺本质安全	是否有一些新的建议能提高工艺的本质安全性？
7	对上一次 PHA 后所有的工艺变更进行复核情况	每一个改动对安全有什么影响？
		改动之间的相互作用是否产生新的危险源？如何产生？

C6 What If/Checklist 检查表

此检查表用于故障假设后，完善补充危害辨识，确保其充分性。

What If/Checklist 检查表（范例）

工艺单元	单元流程	分析主体	设计	工艺	操作	管理	其他
原料与半成品的储运	储罐 输送设备 管道系统 电气系统 控制系统 消防设施 排放系统 ……	设计 容量 自动控制 环境影响 物料 MSDS 工艺参数 检查程序 应急程序 ……	储罐间距是否符合防火安全要求？ ……	储罐内油品含水是否符合工艺要求？ ……	储罐的液位是否在安全高度范围内？	罐区是否建立巡回检查制度？ ……	储罐安全附件是否定期检查？ ……
……							

附 录 D
(资料性附录)
危害分析方法介绍

危害分析一般采用危险和可操作性研究（HAZOP）、故障假设/检查表法（What If/ Checklist)、故障模式和影响分析法（FMEA）、故障树分析（FTA）等方法。

1、危险和可操作性研究（HAZOP）是一种用于辨识设计缺陷、工艺过程危害及操作性问题的分析方法。对工艺或操作的特殊点进行分析，这些特殊点称为“分析节点”，或工艺单元/操作步骤。通过分析每个“节点”， 识别工艺参数的偏离，以及偏差产生的原因及其对整个工艺系统的影响。

2、故障假设/检查表法（What If/ Checklist) 是两种分析方法的组合。首先用故障假设法，对研究的对象提出各种可能故障问题的假设，然后辨识现有的防护措施并判断其完整性和可靠性，需要时提出建议措施。然后再利用预先准备的检查表，对研究对象进行逐项查对，需要时提出建议措施。

3、故障模式和影响分析（FMEA）法是有条理地研究个别组件失效模式及其对整个系统的影响。可用于辨识共因失效和单一组件失效导致的危害事件、事故。FMEA 也是帮助辨识、研究防护措施、故障概率和风险的方法；

4、故障树分析（FTA）是使用逻辑图来描述所有导致特定顶端事件故障路径的方法。顶端事件通常是由故障假设/检查表法、HAZOP 等方法识别出来的。分析是从一特定的顶端事件开始，逻辑推导出产生顶端事件所需的多系列子事件（或分支）。

这些方法的选择参见下表：

		故障假设/检查表分析	故障模式和影响分析	危险和可操作性研究	故障树分析
建设项目	项目建议书阶段	X			
	可行性研究阶段	X		O	O
	初步设计	X	O	O	O
在役装置定期 PHA		X	O	O	O
工艺变更 PHA		X	O	O	O
停用封存、拆除报废 PHA		X			

X=必须　　O=可选

附 录 E
（资料性附录）
定性风险评估规则

E1 概述

该规则适用于评估潜在的工艺危害事故、事件的风险。在这个规则中，首先确定事故、事件的后果级别，分 1 级到 5 级；然后再评估现有的能阻止事故、事件发生的系统的失效频率，也分 1 级到 5 级。综合考虑后果和频率确定风险等级。该风险等级用于确定建议措施的优先次序。

E2 声明

本规则只适用于定性风险评估，不能用于定量风险评估。当某个事故、事件的潜在后果严重或是灾难性时，需慎用本规则。

E3 评估程序

E3.1 步骤 1

应对危害事故、事件进行定义，并对危害事故、事件的后果进行定性评估。

E3.2 步骤 2

应对该事故、事件发生的途径进行分析。通常情况下，应使用危害分析方法。

E3.3 步骤 3

如果难以确定危害事故、事件的风险水平，就应使用本定性风险评估规则。

E3.4 步骤 4

使用“表 E1 风险矩阵”，选择最贴近事故、事件的后果级别描述来确定后果的级别。

E3.5 步骤 5

使用“表 E1 风险矩阵”，选择最贴近事故、事件发生率的级别描述来确定频率级别分数。

该矩阵应用于对正在讨论的事故、事件进行针对性的评估，而不能用于整个厂区的总体评估。矩阵的对象应是某件具体的事故、事件，而不是用来对整个工厂进行工艺安全管理体系审查，因为它可能对一个要素或事故、事件评分很高但对另一个的评分却很低。

E3.6 步骤 6

使用“表 E1～表 E3 风险矩阵”，综合后果级别和频率级别，评估出一个最终的风险等级。

E3.7 步骤 7

使用“表 E4 风险等级划分标准”，采取相应的行动和 PHA 改进建议。

E4 定性风险评估方法

下文提供了使用后果评估矩阵或事故、事件频率评估矩阵的指导方法。

如何应用后果评估矩阵或频率评估矩阵有三种方法。工作组应自行判断、选择合适的方法。

E4.1 薄弱环节法：这种规则假设整个安全链的强度取决于最弱的一环。因此，用最差的单项分数（即最高分值）进行风险评估。当工作组认为硬件和软件系统中任何一个控制环节失效而可能发生评估的事故、事件时，可使用这种方法。

E4.2 目标分类法：这种方法假设几个影响频率的因素分类中的仅有一些（或一种）直接适用于所评估的危险源。在这种情况下，选择目标类别中的最差的单项分数。当某些种类比其它的类别更重要时，这种方法比较适用。

例 1：列车槽车的卸货操作，其危险源是意外地卸错物料。这里硬件控制措施可能相当少，而安全主要取决于卸货员的培训和操作纪律。事故、事件频率评估应着重在人为因素类别里。

例 2：对于一个高度自动化、有多重联锁，很少需要操作员介入的系统，硬件控制类别（如检测、可靠性）是最重要的。

E4.3 平衡法：分析者只需简单地求出各项分数的平均值，然后调整为整数作为综合分数。当工作组觉得在整体的防护措施中存在冗余的时候，可以使用这种方法。例如，一个联锁的失效可能通过高水平操作者的培训和（或）管理系统得到更正。

风险矩阵图示例

表E1　风险矩阵表

事故发生概率等级	5	I 5	III 10	IV 15	IV 20	IV 25
	4	I 4	II 8	III 12	IV 16	IV 20
	3	I 3	II 6	II 9	III 12	IV 15
	2	I 2	I 4	II 6	II 8	III 10
	1	I 1	I 2	I 3	I 4	II 5
风险矩阵		1	2	3	4	5
		事故后果严重程度等级				

表 E2 事故发生概率等级表

频率等级（L）	硬件控制措施	软件控制措施	频率说明（F）/年
1	1.两道或两道以上的被动防护系统，互相独立，可靠性较高；2.有完善的书面检测程序，进行全面的功能检查，效果好、故障少。3.熟悉掌握工艺，过程始终处于受控状态。4.稳定的工艺，了解和掌握潜在的危险源，建立完善的工艺和安全操作规程。	1.清晰、明确的操作指导，制定了要遵循的纪律，错误被指出并立刻得到更正，定期进行培训，内容包括正常、特殊操作和应急操作程序，包括了所有的意外情况。2.每个班组上都有多个经验丰富的操作工。理想的压力水平。所有员工都符合资格要求，员工爱岗敬业，清楚了解并重视危险源。	现实中预期不会发生（在国内行业内没有先例）<10-4
2	1.两道或两道以上，其中至少有一道是被动和可靠的。2.定期的检测，功能检查可能不完全，偶尔出现问题。3.过程异常不常出现，大部分异常的原因被弄清楚，处理措施有效。4.合理的变更，可能是新技术带有一些不确定性，高质量的PHAs。	1.关键的操作指导正确、清晰，其它的则有些非致命的错误或缺点，定期开展检查和评审，员工熟悉程序。2.有一些无经验人员，但不会全在一个班组。偶尔的短暂的疲劳，有一些厌倦感。员工知道自己有资格做什么和自己能力不足的地方，对危险源有足够认识。	预期不会发生，但在特殊情况下有可能发生（国内同行业有过先例）10-3至10-4
3	1.一个或两个复杂的、主动的系统，有一定的可靠性，可能有共因失效的弱点。2.不经常检测，历史上经常出问题，检测未被有效执行。3.过程持续出现小的异常，对其原因没有全搞清楚或进行处理。较严重的过程（工艺、设施、操作过程）异常被标记出来并最终得到解决；4.频繁的变更或新技术应用，PHAs不深入，质量一般，运行极限不确定。	1.存在操作指导，没有及时更新或进行评审，应急操作程序培训质量差。2.可能一班半数以上都是无经验人员，但不常发生。有时出现的短时期的班组群体疲劳，较强的厌倦感。员工不会主动思考，员工有时可能自以为是，不是每个员工都了解危险源。	在某个特定装置的生命周期里不太可能发生，但有多个类似装置时，可能在其中的一个装置发生（集团公司内有过先例）10-2至10-3
4	1.仅有一个简单的主动的系统，可靠性差。2.检测工作不明确，没检查过或没有受到正确对待。3.过程经常出现异常，很多从未得到解释。4.频繁地变更及新技术应用。进行的PHAs不完全，质量较差，边运行边摸索	1.对操作指导无认知，培训仅为口头传授，不正规的操作规程，过多的口头指示，没有固定成形的操作，无应急操作程序培训。2.员工周转较快，个别班组一半以上为无经验的员工。过度的加班，疲劳情况普遍，工作计划常常被打乱，士气低迷。工作由技术有缺陷的员工完成，岗位职责不清，员工对危险源有一些了解。	在装置的生命周期内可能至少发生一次（预期中会发生）10-1至10-2
5	1.无相关检测工作。2.过程经常出现异常，对产生的异常不采取任何措施。3.对于频繁地变更或新技术应用，不进行PHAs。	1.对操作指导无认知，无相关的操作规程，未经批准进行操作。2.人员周转快，装置半数以上为无经验的人员。无工作计划，工作由非专业人员完成。员工普遍对危险源没有认识。	在装置生命周期内经常发生〉10-1

表E3 事故后果严重程度等级表

等级	员工伤害	财产损失	环境影响
1	没有员工伤害或只有轻伤，但没有重伤和死亡。	一次造成直接经济损失人民币不足 50 万元。	事故影响仅限于生产区域内，没有对周边环境造成影响。
2	造成重伤、急性工业中毒，但没有死亡。	一次造成直接经济损失人民币 50 万元以上、100 万元以下。	因事故造成周边环境轻微污染，没有引起群体性事件。
3	一次死亡 1-2 人，或者 3-9 人中毒（重伤）。	一次造成直接经济损失人民币 100 万元以上、500 万元以下。	1、因事故造成跨县级行政区域纠纷，引起一般群体性影响。 2、发生在环境敏感区的油品泄漏量 1 吨以下，以及在非环境敏感区油品泄漏量 10 吨以下，造成一般污染的事故。
4	一次死亡 3-9 人，或者 10-49 人中毒（重伤）。	一次造成直接经济损失人民币 500 万元以上、1000 万元以下。	1、因事故造成跨地级行政区域纠纷，使得当地经济、社会活动受到影响。 2、发生在环境敏感区的油品泄漏量 1-10 吨，以及在非环境敏感区油品泄漏量 10-100 吨，造成较大污染的事故。
5	一次死亡 10 人以上，或者 50 人以上中毒（重伤）。	一次造成直接经济损失人民币 1000 万元以上。	1、事故使得区域生态功能部分丧失或濒危物种生存环境受到污染。 2、事故使得当地经济、社会活动受到严重影响，疏散群众 1 万以上。 3、因事故造成重要河流、湖泊、水库及海水域大面积污染，或县级以上城镇水源地取水中断。 4、发生在环境敏感区的油品泄漏量超过 10 吨，以及在非环境敏感区油品泄漏量超过 100 吨，造成重大污染事故。

表 E4 风险等级划分标准

风险等级	分值	描述	需要的行动	PHA 改进建议
IV 级风险	15 至 25	严重风险（绝对不能容忍）	必须通过工程和/或管理上的专门措施，限期（不超过六个月内）把风险降低到级别 II 或以下。	需要并制定专门的管理方案予以削减
III 级风险	10 至 14	高度风险（难以容忍）	应当通过工程和/或管理上的控制措施，在一个具体的时间段（12 个月）内，把风险降低到级别 II 或以下。	需要并制定专门的管理方案予以削减
II 级风险	5 至 9	中度风险（在控制措施落实的条件下可以容忍）	具体依据成本情况采取措施。需要确认程序和控制措施已经落实，强调对它们的维护工作。	个案评估。评估现有控制措施是否均有效。
I 级风险	1 至 5	可以接受	不需要采取进一步措施降低风险。	不需要。可适当考虑提高安全水平的机会。（在工艺危害分析范围之外）

附 录 F
(资料性附录)
PHA 报告编制指南

PHA 报告可包括以下内容，但章节可根据实际情况进行增减。

F1 封面

应提供的信息：名称、单位名称、分析单元、时间、批准人。

F2 目次

应提供的信息：章节名称、对应页码。

F3 工作组成员的签名页

该签名页必须声明分析对象能否安全运行，所有的工作组正式成员应在此签名。如果工作组认为该对象不能安全运行，应提出关闭建议。

F4 企业领导对建议措施的回复

企业领导应把对建议措施的回复形成文字记录，指出对每条建议措施是接受还是拒绝，并对接受的建议措施明确责任人和完成时间。

F5 工作组的成员和资格

列出姓名、职务、专业领域，现场和所评估工艺方面的经验年限，PHA 的经验和培训（至少有一个成员对所评估的工艺具备专门的经验和知识，至少有一个成员对使用的工艺安全分析方法非常了解）。

F6 分析小结

—— 工艺过程描述和评估范围总结（说明评估的界限）；

—— 建议措施小结（工作组所作建议的一个简明列表）；

—— 实地考察（实地考察的日期和任何重大的发现）。

F7 分析过程

F7.1 工艺过程描述

工艺过程的详细描述，提供足够的信息让相关人员对工艺有清晰的了解。包括工艺原理、使用的物料、储存的数量、设备规格。这部分必须对评估的界限作详细的描述。

F7.2 工艺图纸

说明工艺单元之间的连接方式，标明工艺流程方向。

F7.3 危害清单

对已确定的事故、事件和可能发生的后果以及降低或消除事件发生可能性的主要的防护措施进行总结。列明针对不同危害的硬件和软件上的控制措施以及它们之间的相互关系。

F7.4 对建议措施的详细描述

记录每条建议措施背后的详细信息和思路。并考虑在暂时无法整改前是否需要采取监控等措施。

F7.5 对无建议措施条目的描述

目的是突出已分析的且情况令人满意的重要条目。讨论应提供足够的细节，说明无建议的理由，以便将来的评估小组能从中受益。

F7.6 人为因素分析描述

这部分总结了在整个分析过程中人为因素是如何被考虑的。对人为失误、人机界面和人的工作要求等因素如何控制进行描述。

F7.7 装置定点分析描述

应记录装置定点分析的详细内容。

F7.8 工艺本质安全分析描述

工作组应从工艺本质安全的角度考虑工艺技术并提出相应的建议。

F7.9 报告附录

下面所列的是可以包括在报告附录中的文件：

——工作任务书；

——危害辨识所采用方法（如化学品反应矩阵、通用危害检查表、封闭性检查表等）；

——技术文件包；

——变更管理文件；

——重大事故报告；

——先前的 PHA 和建议措施的实施状况列表；

——人为因素检查表；

——风险评估方法及分析记录；

——PHA 结果培训和沟通计划；

——其他。