**中文引用格式**:王海清,张玉倩,郑威,等. 基于主次屏障的化工装置事故根因分析及"双预"机制应用[J]. 中国安全科学学报,2024,34(2):131-137.

**英文引用格式**:WANG Haiqing, ZHANG Yuqian, ZHENG Wei, et al. Root cause analysis of chemical installation accident based on primary-secondary barriers and its application on double prevention mechanism[J]. China Safety Science Journal,2024,34(2):131-137.

# 基于主次屏障的化工装置事故根因分析及"双预"机制应用*

王海清[1]教授, 张玉倩[1], 郑 威[2], 马佳雯[1]

(1 中国石油大学(华东) 机电工程学院,山东 青岛 266580;
2 杭州汉德质量认证服务有限公司,浙江 杭州 310019)

**中图分类号**:X937 **文献标志码**:A **DOI**: 10.16265/j.cnki.issn1003-3033.2024.02.1032
**资助项目**:国家重点研发计划项目(2019YFB2006305)。

**【摘 要】** 双重预防机制("双预")是当前国内危化品领域正在广泛推行的一种风险管控系统,但目前缺乏底层和运行层面的理论架构,更缺乏以根因分析(RCA)结果来指导实施"双预"的方法工具,为此,提出"主-次"屏障理论与事件与原因因素分析(ECF)相结合的可视化主-次屏障(VPSB)模型。ECF作为一种典型的RCA技术,由特定主/次屏障失效模式组成灾害事件的致因路径,为VPSB建模提供可视化框图。应用该模型对英国石油BP公司的Texas爆炸中的典型事故场景进行隐患识别和RCA,获得"双预"相关管理措施的具体失效模式,通过与美国化学品安全委员会(CSB)和英国石油(BP)公司对该事件的调查结果对比,发现CSB和BP公司将人的不安全动作作为直接原因开展深层次的原因分析,将关注点放在了人的管理上,并将根本原因宏观地总结为安全主管失职和操作工违规作业,而VPSB模型则关注的是对重大事故隐患本身和工艺过程的管理,用描述具体的次屏障失效模式来突出管理系统存在的根本性问题,其中,在机械完整性管理上的问题最多,且主要是由于管理措施未被合规执行。这为企业优化"双预"的相关工作内容提供了重点整改方向和可操作性建议。

**【关键词】** 可视化主-次屏障(VPSB)模型; 化工装置; 根因分析(RCA); 双重预防机制; 事件与原因因素分析(ECF); 事故场景

# Root cause analysis of chemical installation accident based on primary-secondary barriers and its application on double prevention mechanism

**WANG Haiqing**[1], **ZHANG Yuqian**[1], **ZHENG Wei**[2], **MA Jiawen**[1]

(1 School of Electromechanic Engineering, China University of Petroleum, Qingdao 266580, China;
2 TUV Nord China Quality Certification Service Company, Hangzhou Zhejiang 310019, China)

**Abstract**: The double prevention mechanism was a widely used risk control system in hazardous chemical fields in China. However, the theoretical framework at underlying and operational levels was missing. Especially, there was a lack of RCA results to guide double prevention. Therefore, VPSB model was proposed by integrating primary-secondary barrier theory and ECF analysis technology. Furthermore,

* 文章编号:1003-3033(2024)02-0131-07; 收稿日期:2023-08-14; 修稿日期:2023-11-18

ECF as a typical RCA method represented the causal of a catastrophic event composed of specific primary-secondary barrier failure modes, providing a visualized diagram for the VPSB model. The model was used to identify hazards and RCA for a typical accident scenario in the Texas explosion of British Petroleum (BP) company. Moreover, the failure modes of double prevention related to management measures were investigated. The comparisons of investigation results between the U. S. Chemical Safety Board (CSB) and BP indicated that people´s unsafe actions were taken as the direct cause to carry out in-depth cause analysis. Moreover, the focus was human management, and the failure of the safety supervisors and irregular operations of the operators were macroscopically summarized as the root causes. However, the VPSB model focused on near-miss and the process of major accident hazards, and detailed sub-barrier failure modes were used to highlight the fundamental problems of management systems. Specifically, mechanical integrity management had the largest number of problems because management measures were not conducted as required. This study can provide rectification directions and operability recommendations for enterprises to optimize the relevant work content of the double prevention mechanism.

**Keywords**: visualized primary/secondary barriers (VPSB) model; chemical installation; root cause analysis (RCA); double prevention mechanism; event and cause factor (ECF) analysis; accident scenario

## 0 引 言

当前,双重预防机制(简称“双预”)是我国危化品领域正在推广和实施的一种风险管控系统/制度,政府相关文件只给出框架要求和数字化建设流程,对于如何开展还缺乏理论框架和实施细则,这导致化工企业在实践中感到困惑,从而影响风险管控实效[1]。

根因分析(Root Cause Analysis,RCA)采用结构化、系统化的事故分析技术剖析安全管理系统的薄弱环节,旨在从根本上识别治理隐患、预防相同或类似事件再次发生[2]。但传统事故致因模型和 RCA 技术,如屏障模型、事件与原因因素分析(Event and Cause Factor,ECF)等,过度关注表面原因,对系统性的深层次原因笼统概括,或将促成原因(中间原因)错当作根本原因[3]。单独采用现有的 RCA 技术和事故因果模型难以为“双预”建设提供全面的工艺信息。如领结图仅列出与顶事件有关的预防、减缓性屏障及其退化因素,忽略了屏障失效模式之间的因果关系,而屏障一般存在多种失效模式,不同失效模式的后果和致因路径可能不同;保护层分析用来评估现有保护层的有效性,帮助决策者判断是否需要增加新保护层,但不能用于识别现有保护层存在的隐患,因此,该方法在“双预”机制建设过程中存在局限性。为实现事前正向预防和事后反向治理的双向风险管控,需要融合改进 RCA 技术,从理论模型层面研究如何建设“双预”机制、制定具体工作计划,此前相关研究较少。

鉴于此,笔者拟提出“主-次”屏障理论和 ECF 相结合的可视化主-次屏障(Visualized Primary/Secondary Barriers,VPSB)模型,分阶段剖析促成事故链向下一阶段演化的技术层面原因,以及与之对应的管理系统缺陷,突出不同层次/类型原因与主、次屏障的内在联系,以期为危化企业开展“双预”机制建设,优化改进工作提供模型化的管理框架和操作性建议。

## 1 “双预”实施难点与理论挑战

“双预”机制是具有中国特色的保障安全生产的长效机制和重要手段,包含风险分级管控和隐患排查治理 2 大体系,从过程安全管理(Process Safety Management, PSM)的角度出发,双重防治重大风险。通过对具体的重大事故危害(Major Accident Hazards,MAH),如具体部位的腐蚀、超温超压等(而非笼统的整个装置或单元)进行风险评估来实现分级管控;而每个 MAH 一般对应多个可能引发化工装置事故的风险事件,即重大事故事件(Major Accident Event,MAE),如带压储罐超压破裂或低压吸瘪、管道因腐蚀泄漏,进一步对其管控措施中存在的隐患排查和治理。

目前,《危险化学品双重预防机制建设指导手册》将隐患排查内容对应风险管控措施和目标,简单描述为“…是否…”,例如:液位计是否正确指示液位数据[1]。实践中,应确定风险管控主体对象,即 MAH 危害;再进一步识别其对应 MAE 事件的管

控措施中可能存在的多种不安全状态(即隐患)。因此,按照指导手册容易造成隐患识别不全面、描述不贴切等问题。

如何将“双预”机制融入到原有的安全管理体系中,如何为特定 MAH 灾害制定分级管控计划和辨识 MAE 事件的隐患排查治理措施,这些是危化品企业在建设“双预”机制的过程中亟待解决的问题,具体包括以下几个方面[4-6]:

1) 管理层对“双预”认识不足,且缺乏指导“双预”机制建设、与原有管理系统有机融合的良好工程实践和标准文件,因此,普遍存在“双预”机制与原来的安全管理体系“两张皮”的现象。

2) 风险分级管控与隐患排查治理业务独立开展或融合效果差,未能很好地形成风险管控的闭环。

3) “双预”的相关文件缺乏实操层面的细则和结构化方法模型,导致企业在开展实际工作时,对风险管控范围划分、职责分解、如何实现管控层之间的有效沟通、逐级落实各项措施等感到困惑,容易发生隐患排查治理清单类型单一(危化企业大多以工艺流程、作业步骤或设备为研究对象编制清单,缺乏对特定事故场景或风险事件的针对性)或内容遗漏、排查重点不明确或出现偏差等现象。

4) 许多危化品企业在进行风险管控和隐患排查时缺乏系统的安全思维和前向思维,通常只考虑单个 MAH 的风险评估结果来制定风险管控计划,忽略 MAH 之间的风险耦合效应。

## 2　VPSB 模型及“双预”可视化建模

### 2.1　“主-次”屏障模型及功能

屏障分析是一个有效的“双预”机制建设辅助工具[2]。按照直接和间接控制能量/MAE 的方式,将屏障分为主屏障和次屏障。一般而言,直接控制能量/MAE 的物理装置、具备“检测-判定-动作”3 要素的技术系统是主屏障,如防爆墙、安全仪表系统;定期检验、测试或培训等组织管理措施是次屏障,其功能在于保障主屏障功能完整性、避免退化[7]。“主-次”屏障理论模型如图 1 所示。

在次屏障的支持下由主屏障发挥其安全功能,实现对 MAE 事件的防控。当主、次屏障缺失或功能退化时,能量沿致屏障链传播,直至作用于目标;当某个屏障实现其安全功能时,事故链被切断(发生未遂事故)。因此,主、次屏障作为能量/MAE 与目标之间的“第一道防线”和“第二道防线”,其失效模式分别为事故的间接和根本原因。

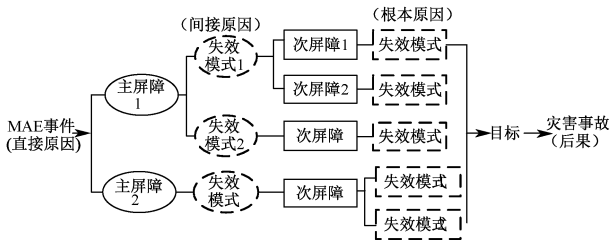



**图 1　“主-次”屏障理论模型**

**Fig. 1　"Primary-secondary" barrier theory model**

从“主-次”屏障失效原因的角度出发,将主屏障失效模式(间接原因)分为:①未设置物理设备设施或未采取技术措施;②生产、制造、设计、安装环节造成的缺陷;③误操作;④功能丧失。将次屏障失效模式(根本原因)分为:①指导安全管理活动的程序文件存在缺陷或制定不合理;②制度完善但未执行;③制度完善但执行偏差。

ECF 是一种典型的 RCA 技术,ECF 的概念模型如图 2 所示。其由主、次事件链 2 部分组成,分别描述了焦点事件的发展过程,及促成中间事件的条件/状态和次级事件。ECF 采用简单的线性思维构建事故发展与因果关系模型,没有确定不同类型原因(及对应屏障)的分类和识别方式,因此,不能清楚地识别焦点事件的直接、间接和根本原因[2]。但 ECF 为隐患识别(针对主屏障失效)和 RCA(针对次屏障失效)提供了一个整合证据、梳理事件序列的结构框架,用来描述 MAE 事件的演化顺序和致因关系,促成各阶段风险事件发生或向后演化的条件/状态(对应“主-次”屏障失效模式)。

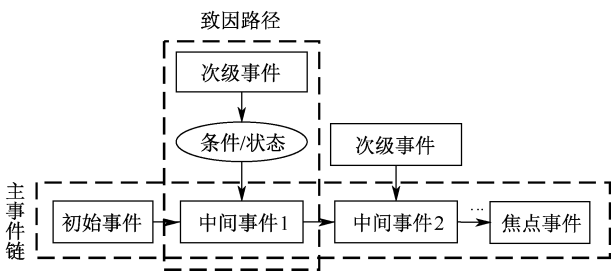



**图 2　ECF 的概念模型**

**Fig. 2　Conceptual model of ECF**

### 2.2　VPSB 模型与构建流程

结合“主-次”屏障理论和 ECF,提出 VPSB 模型,如图 3 所示。VPSB 模型在 ECF 的基础上,将致因路径的描述方式由简单的条件/状态和次级事件,改为因果关系、层次划分明确的“主-次”屏障失效模式。每个屏障可能存在多种失效模式,不同的主

屏障失效模式所需的次屏障也可能不同,即致因路径不同。以 MAH 或 MAE 事件为节点,分阶段进行屏障失效分析,最终由多个 VPSB 模型组成链条。以屏障框图的形式描述特定的事故场景促成风险事件向下一个阶段发展的技术系统缺陷(间接原因)和与之对应的管理系统缺陷(根本原因)。

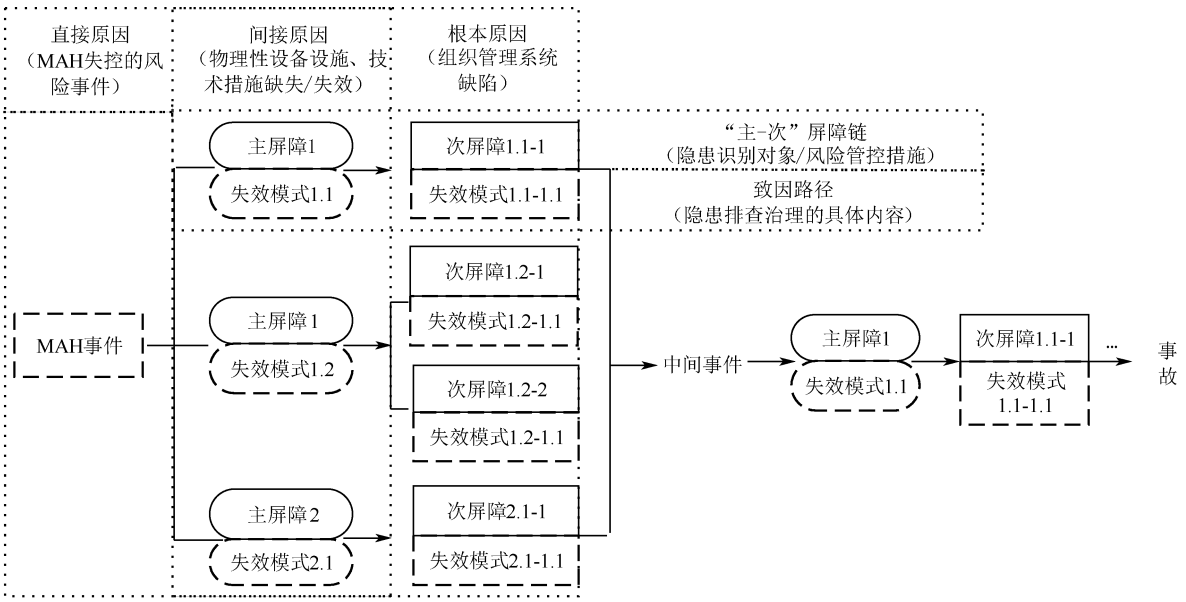



**图 3 VPSB 模型**

**Fig. 3 VPSB model**

VPSB 模型为危化企业制定和实施特定化工装置事故场景下的"双预"细化措施和具体的工作内容提供了工艺安全信息,因此,该模型可作为指导"双预"机制建设的可视化模型,其构建流程如图 4 所示。流程分为 4 个阶段,具体步骤如下:

1) 确定待分析的事故场景和 MAH,应用 ECF 技术梳理每个 MAH 可能发生的 MAE 事件之间的因果关系。每个 MAE 事件是灾害性的化工装置事故演化过程中有必要单独建模的高风险阶段。

2) 定义分析边界,确定焦点事件(主事件链中的事故或未遂事故,即中间事件)。

3) 识别预防 MAE 事件的的主屏障,详细描述其可能发生的失效模式;根据"主-次"屏障理论对不同层次/类型原因的分类方式,确定失效类型。

4) 分析促使主屏障发生特定失效模式、导致功能退化或丧失的因素,确定所需次屏障的安全功能,分析次屏障可能发生的失效模式和类型。

5) 重复步骤 2)—4),为主事件链中的每个高风险中间事件和事故后果构建 VPSB 模型。

6) 对标美国职业安全与健康管理局提出的 14 个 PSM 要素[8-9],统计与其有关的根本原因数量,实现反向确定"双预"工作的主要方向及需要重点审查的 PSM 要素。

7) 根据描述的特定化工装置事故场景发展过程和因果关系的 VPSB 模型,制定"双预"的分解工作(责任人、内容/性能要求、考核指标等)细化措施、隐患排查治理清单等,根据 MAH 的风险等级确定管控层级、分级管控措施和隐患排查治理周期。

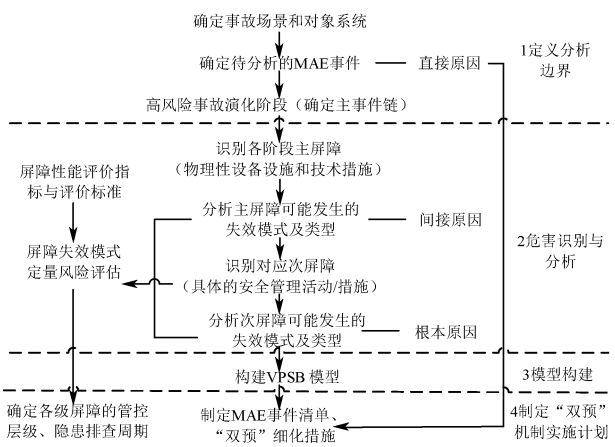



**图 4 VPSB 模型构建流程**

**Fig. 4 VPSB model construction process**

## 3 案例应用

2005 年,BP 公司 Texas 炼油厂在异构化 ISOM 装置开车的过程中发生蒸气云爆炸,造成 15 人死亡、170 人受伤[10-11]。以该事故为例,采用所提出的 VPSB 模型进行"双预"开发,识别 PSM 系统缺陷,验证相关屏障措施,揭示预防此类事故的具体对策。

### 3.1　定义分析边界

在 ISOM 开车过程中过度进料、控制液位的关键仪表设备失效,这些会导致液位失控,分馏塔内液位持续升高。当管线内压力超过泄压阀起跳值时,液体被泄放至放空罐,但罐内液位报警系统失效、人员响应失败、未连接火炬系统,导致易燃易挥发的烃类液体溢出,形成可燃蒸汽云,但未设置相应的气体检测装置和紧急切断系统,最终被引燃爆炸[10-11]。

根据图 4,将 Texas 事故的演化过程划分为物料失衡、液位失控、储罐溢流和蒸气云爆炸 4 个阶段,当主屏障失效时,风险沿着主事件链向后传播,如图 5 所示。针对第一阶段,以“液位失控”为焦点事件,根据“主-次”屏障理论,确认其直接原因是“进料量大于出料量”(MAE 事件),间接原因是主屏障“液位调节回路”和“液位报警与人员响应”失效。

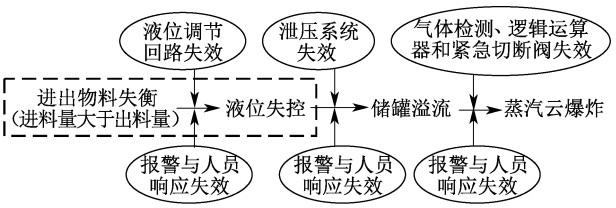



**图 5　Texas 事故的主事件链**

**Fig. 5　Primary events chain of Texas accident**

### 3.2　主次屏障失效分析与 VPSB 模型构建

液位调节回路由液位计、控制器和调节阀(Level Valve, LV)组成。液位计将检测到的液位信号发送给控制器,并以百分比的方式指示液位高度,控制器根据接收信号与设定值的偏差向 LV 发送控制信号,通过改变阀门开度调节液位以保持进出物料平衡[10-11]。现以“液位调节回路”为例,对“液位失控”危害事件进行“主-次”屏障失效分析,构建 VPSB 模型。

针对设计不符合工艺要求(无法检测 3 m 以上液位)这一主屏障失效模式,提出建议性措施:①依据工程标准进行设计审查;②对液位调节回路可能发生的故障模式及原因进行工艺危害分析;③定期结合液位数据、操作记录、涉及液位异常的事件调查报告等工艺信息排查隐患,确认其功能完整性;④开车前检查、维护、测试,确认是否满足开车条件;⑤冗余液位监控系统;⑥超高液位(3 m 及以上)报警和紧急切断阀(Emergency Shutdown Device, ESD)。

这些次屏障均不具备独立阻止液位失控的能力,但能够强化液位调节回路的功能,降低液位失控风险。若次屏障发生以下失效模式,将形成事故路径:①未测试液位高于液位计量程时液位调节回路的功能完整性;②忽略设计缺陷与液位计误报之间的因果关系;③工艺信息管理不善、人员沟通不畅,导致信息不足以支持员工预先识别设计缺陷;④开车前未校验液位计;⑤玻璃观察窗模糊不清;⑥未设置超高液位报警和 ESD 阀。

同理,分析以违规变更 LV 操作条件/步骤(将 LV 开度设为 50%的自动模式且未在规定时间内打开至合适开度)为起点的致因路径。根据上述分析结果,构建液位失控危害事件的 VPSB 模型(以液位调节回路失效为例),如图 6 所示。

### 3.3　与 CSB、BP 对比“液位失控”事件 RCA 结果

对比 VPSB 模型、美国化学品安全委员会(U. S. Chemical Safety and Hazard Investigation Board, CSB)、BP 公司对液位失控事件的原因分析结果,CSB 和 BP 将关注点放在人的因素上,得到了一致的直接原因,即过度进料(人的不安全行为),且将促成该行为的管理系统缺陷分别以详细描述和总结概括的方式描述为间接原因和根本原因,但宏观的 RCA 结果对开展“双预”相关工作的指导作用不大,这往往导致管理系统的根本性问题难以有效解决。

相比之下,VPSB 模型将大型装置的具体部位 MAH 可能发生的 MAE 事件视作焦点事件的直接原因,间接原因是物理装置或关键技术系统的特定故障模式,将根本原因详细描述为与之对应的各种安全管理活动、制度、措施偏离预期的状态。

根据 VPSB 模型对“液位调节回路”2 种失效模式的 RCA 结果,得出在 PSM 各个方面促成“液位失控”MAE 事件的根本原因数量及类型,如图 7 所示。对比发现,“执行偏差”占比最大,且主要涉及机械完整性和合规审查,表明 BP 公司在设备全生命周期内的完整性管理和绩效审核方面存在显著隐患,主要表现在程序文件未执行,这为事后优化“双预”的相关工作内容提供了重点和整改方向。当考虑更多主屏障失效模式时,得到的 RCA 结果和 PSM 系统重点审查要素可能不同。

### 3.4　“双预”相关工作重点的改进建议

1) 将 MAH 作为独立的风险分析单元,如装有易燃易挥发烃类液体的分馏塔,根据 VPSB 对特定的化工装置事故场景的 RCA 结果,对应特定的“主-次”屏障失效模式来优化/制定管控措施和隐患排查清单。

2) 分别对起点为“液位计无法监控 3 m 以上液

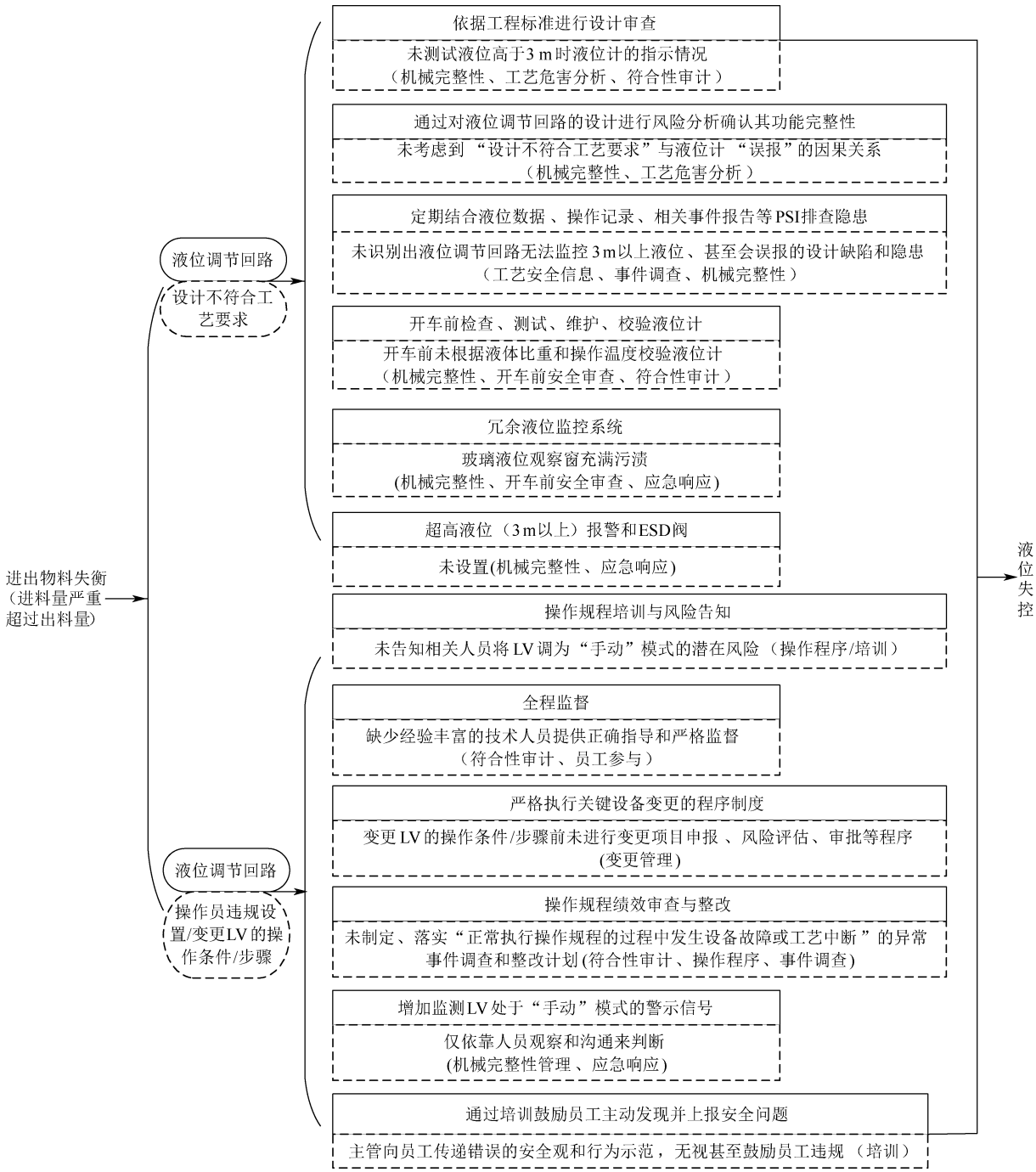



**图 6 “液位失控”危害事件液位调节回路失效的 VPSB 模型**

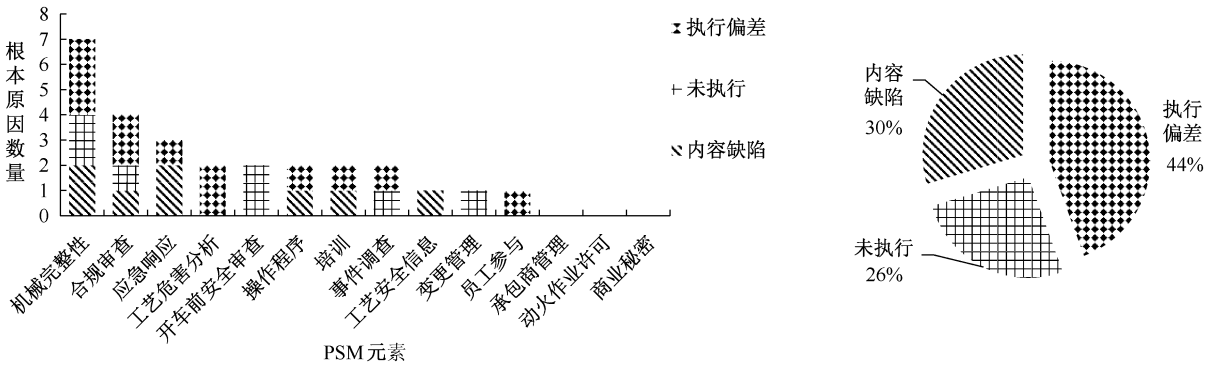
**Fig. 6 VPSB model for liquid level adjustment circuit failure in "liquid level out of control" hazard event**

位”和“手动调节 LV”的致因路径进行风险等级评估,以确定分馏塔这一 MAH 对应物料失衡、液位失控 MAE 事件的管控层级和排查周期等。

3）根据 VPSB 模型对“液位失控”事件部分根本原因的统计分析结果,确定与液位调节回路“设计不符合工艺要求”和“违规操控”有关的 PSM 重点审查要素和整改方向。如 BP 公司应优先对 MI 管理和管理系统审计作出优化整改,并根据 VPSB 模型对 2 方面问题的具体描述,制定相应的整改和验收计划,实现对管理系统缺陷的闭环管理。

## 4 结 论

1）区别于传统 RCA 技术和事故致因模型,VPSB 模型基于前向思维,对特定化工装置事故场景的管控措施(“主-次”屏障)及其可能出现的隐患(失效模式)进行预测性分析和可视化建模,并将




(a) 按照PSM元素和失效原因对“液位失控”的根本原因的分类统计结果　　(b) “液位失控”3种类型根本原因所占的比例

**图 7　VPSB 模型得出“液位失控”的根本原因的数量及类型统计**

**Fig. 7　Root cause number and type statistics of "liquid level out of control" obtained by VPSB model**

RCA 结果与整个 PSM 系统建立联系。这为事前优化制定或事后改进“双预”分解工作的细化措施提供了实操性建议和管理框架。

2) 通过对比 CSB、BP 公司和 VPSB 模型对“液位失控”事件的 RCA 结果,验证了 VPSB 事故模型的原因划分方法,及其以非人为因素的客观 MAE 事件为起点,先从直接控制 MAH 处于安全限值的技术措施入手,再从过程风险管控系统的根源性问题入手的建模思路,对于企业开展系统的安全审计工作、编制特定事故场景下 MAH 的管控方案和隐患排查治理清单的实操性指导意义。

3) 由于 MAH 通常对应多个 MAE 事件,每个屏障又存在多种失效模式,应用 VPSB 模型对复杂化工装置事故进行 RCA 时,往往包含的信息量较大,因此,建议在实际应用时,以事件序列中的某个阶段、甚至以某个主屏障为节点,细化模型。

## 参 考 文 献


[1] 中华人民共和国应急管理部. 危险化学品双重预防机制建设指导手册(2021 版)[Z]. 2022-10-11.

[2] IEC 62740-2015, Root cause analysis(RCA) [S].

[3] BAYBUTT P. Insights into process safety incidents from an analysis of CSB investigations[J]. Journal of Loss Prevention in the Process Industries, 2016, 43: 537-548.

[4] 国务院安委办. 实施遏制重特大事故工作指南构建双重预防机制的意见[EB/OL]. 国家安全生产监督管理局,(2016-10-13). https://www.gov.cn/xinwen/2016-10/11/content_5117487.htm.

[5] 国务院. 中共中央国务院关于推进安全生产领域改革发展的意见[EB/OL]. (2016-12-09). https://www.gov.cn/gongbao/content/2017/content_5156728.htm.

[6] LIU Yejiao, TENG Ting, CHEN Ying, et al. Research on construction method and information system of double prevention mechanism in iron mine[J]. IOP Conference Series: Earth and Environmental Science, 2022, 983(1): 657-667.

[7] Center for Chemical Process Safety, Energy Institute. Bow ties in risk management: a concept book for process safety[M]. New York: John Wiley & Sons Incorporate, 2018: 12-42.

[8] BEHIE S W, HALIM S Z, EFAW B, et al. Guidance to improve the effectiveness of process safety management systems in operating facilities[J]. Journal of Loss Prevention in the Process Industries, 2020, 68: DOI: 10.1016/j.jlp.2020.104257.

[9] 29 CFR 1910.119-1992, The OSHA process safety management (PSM) Standard [S].

[10] U.S. Chemical Safety and Hazard Investigation Board. Investigation report[R/OL]. [2023-04-20]. https://www.csb.gov/bp-america-refinery-explosion/.

[11] HENDERSHOT D, WIEGMANN D A, BAKER J A, et al. The report of the BP U.S. refineries independent safety review panel [R]. British Petroleum(BP), 2007.


**作者简介:** 王海清　(1974—),男,云南普洱人,博士,教授,主要从事安全管理体系建设、过程安全管理(HAZOP/FMEA 等)、安全仪表系统(LOPA/FGS 等)、报警管理和可靠性分析等方面的研究。E-mail: wanghaiqing@upc.edu.cn。