

石油石化员工安全环保工作必备系列知识读本

预见·风险

FORESEE RISK

石油石化员工HSE风险预控与辨识手册

《预见风险》编写组 编著

这是一本指导企业如何化解HSE风险的经典图书

深度剖析企业HSE风险源辨识与评估，力求削减与控制各类风险

也是一本石油高等院校及企业HSE培训的核心教材

集结作者多年审核评估、实地调研、事故调查、交流学习经验和心得

石油工业出版社

石油石化员工安全环保工作必备系列知识读本

预见·风险

FORESEE RISK

石油石化员工HSE风险预控与辨识手册

《预见风险》编写组 编著

这是一本指导企业如何化解HSE风险的经典图书

深度剖析企业HSE风险源辨识与评估，力求削减与控制各类风险

也是一本石油高等院校及企业HSE培训的核心教材

集结作者多年审核评估、实地调研、事故调查、交流学习经验和心得

石油工业出版社

图书在版编目 (CIP) 数据

预见风险: 石油石化员工 HSE 风险预控与辨识手册 / 《预见风险: 石油石化员工 HSE 风险预控与辨识手册》编写组编著. —北京: 石油工业出版社, 2016.5

ISBN 978-7-5183-1295-5

I . 预…

II . 预…

III . 石油工业 - 工业企业管理 - 风险管理 - 手册

IV . F407.226-62

中国版本图书馆 CIP 数据核字 (2016) 第 103647 号

《预见风险》编写组

胡月亭 刘宝林 霍国栋 牛 蕴 李 森 李建林 程连谱

出版发行: 石油工业出版社

(北京安定门外安华里 2 区 1 号 100011)

网 址: www.petropub.com

编辑部: (010) 64523550 图书营销中心: (010) 64523633

经 销: 全国新华书店

印 刷: 北京中石油彩色印刷有限责任公司

2016 年 5 月第 1 版 2016 年 5 月第 1 次印刷

710 × 1000 毫米 开本: 1/16 印张: 13

字数: 140 千字

定价: 42.00 元

(如出现印装质量问题, 我社图书营销中心负责调换)

版权所有, 翻印必究

| 前言 |

这是一本探讨如何预见和化解企业 HSE 风险的书籍。

一个企业有没有风险管理的意识和机制，是衡量一个企业是否成熟、能够可持续发展的重要标志。从本质上看，HSE 管理实质就是不断循环往复地辨识风险、评价风险与控制风险的过程。

“防为上，救次之，戒为下”，东汉时期的政治家旬悦就提出了“预防为主”的理念。今天，人们对安全生产的认识已经进入了“以人为本、超前预防”的本质安全论阶段。

这种新的安全思想和方法论推进了传统产业和技术领域安全手段的进步，也促使企业安全管理工作由粗放型向集约型转化，变“事故处理、事后防范”为“本质安全、超前预防”管理。

如何预见风险？本书通过如何“辨识”风险、如何“评估”风险、如何“化解”风险、如何“控制”风险 4 章的内容，从实践到理论，从案例到解读，向读者进行了全景式的解答。

安全生产，风险为本。安全工作的核心内容是识别、评估和控制生产作业现场的风险，如何围绕风险识别、评估、控制这条主线，眼睛盯住现场，功夫下在现场，采取一切有效的管理和工程技术措施，强化良好安全行为的养成，提高本质安全水平，最大程度地控制生产作业风险。

发现不了问题是最大的问题，意识不到风险是最大的风险。本

书的编撰正是基于这样的思路。在结构设计上，本书分别从事故预防的宏观、微观两个层面，探究了事故预防的客观规律，揭示了事故预防工作存在的问题，并通过构建宏观、微观两个模型，为解决这些问题提出了思路、方法与意见、建议。通过事故防控宏观模型，揭示了 HSE 管理体系运行中的症结所在，科学地解答了为何管理体系不能有效发挥作用的问题，同时还提出了促使管理体系有效运行的策略、模式。通过事故防控微观模型，揭示了事故发生的内在机理，指出了事故防控的关键环节，对于做好事故防控，尤其是建立长治久安的长效机制，具有重要的理论价值。

这本书是企业风险管理的同仁对风险预控知识和专业技术进行总结、思考、探索的思想结晶。希望本书的出版，对企业提升 HSE 业绩水平，夯实企业安全发展基础提供借鉴，同时也为广大员工提供 HSE 管理行之有效的方法及工具。

目 录

CONTENTS

第1章 如何“辨识”风险

/ 1

1.1 常用风险辨识方法 / 3

1.2 如何选择辨识方法 / 11

1.3 做好辨识前的准备工作 / 14

1.4 根据危害因素特征辨识风险 / 18

1.5 根据事故、事件类型辨识风险 / 23

1.6 传统业务活动的危害因素辨识 / 25

1.7 新型业务活动的危害因素辨识 / 28

1.8 多时态、多状态、多角度、全方位辨识危害因素 / 32

1.9 动员全体员工参与危害因素的辨识 / 37

拓展案例：危害因素辨识示例 / 39

延伸阅读：源头类危害因素与衍生类危害因素 / 44

- 2.1 对危害因素进行分级、排序 / 55
- 2.2 剥离低风险和发现高风险危害因素 / 58
- 2.3 “二拉平”评判原则的应用 / 60
- 2.4 注重风险评估的可能性与严重性 / 63
- 2.5 风险评价应该注意的准则 / 65
- 2.6 风险评价的注意事项 / 67
- 拓展案例：常用风险评估方法介绍 / 72
- 延伸阅读：风险评估方法的比选 / 79

- 3.1 风险削减与控制的原则 / 89
- 3.2 风险防控策略 / 93
- 3.3 奶酪模型与防控措施 / 95
- 3.4 风险防控措施的层级 / 97
- 3.5 选择风险防控措施类型 / 104
- 3.6 风险防控措施制定的注意事项 / 107
- 3.7 小事故、未遂事故风险的防控 / 115

3.8 致命性事故风险的防控 / 117

3.9 灾难性事故风险的防控 / 126

拓展案例：事故发生的机理 / 133

延伸阅读：事故发生的特点 / 139

第4章 如何“控制”风险

/ 145

4.1 三类危险源划分的背景意义 / 147

4.2 重新划分三类危险源 / 149

4.3 科学的事事故防控模式 / 152

4.4 传统安全管理下的事故防控模式 / 163

4.5 事故防控宏观模型的构建 / 165

4.6 事故防控微观模型（“3×3”模型）的构建 / 170

4.7 风险防控方法——蝴蝶结模型 / 174

4.8 安全文化与安全文化建设 / 188

拓展阅读 1：风险的宏观方面原因 / 196

拓展阅读 2：风险的微观方面问题 / 197

参考文献 / 200

第1章 如何“辨识”风险 >>

要做好风险管理，最关键的就是要做好危害因素辨识，即全面彻底系统地开展危害因素辨识活动，尽可能把客观存在的危害因素都辨识出来。由于系统地开展危害因素辨识，很可能辨识出的危害因素的数量很多，尤其对于大型作业项目，将会辨识出大量的危害因素，如果不分主次都进行管理，胡子眉毛一把抓，势必会在风险管理方面捉襟见肘。因此，要想在管理上有所侧重，就必须分辨出哪些为主，哪些为次，从所辨识出的众多危害因素中找出并抓住“主要矛盾”，进而实现对风险的有效管控。



1.1 常用风险辨识方法

1. 安全检查表法

安全检查表（Safety Check List）是运用安全系统工程的方法所开发的用于发现系统以及设备、机器装置和操作管理、工艺、组织措施等方面的各种不安全因素的一种表格式检查工具。它原本是由于现场安全检查、隐患排查以及督促各项安全法规、制度、标准落实的一种实用检查工具。

安全检查表不仅具有安全检查工具的功能，而且已演变为危害因素辨识的索引、指南，通过安全检查表对照查找可能存在的危害因素，使其成为危害因素辨识的方法和工具，这就是危害因素辨识中的安全检查表法。所谓安全检查表法，就是把某项作业活动、某个工作系统、某种装置可能存在的危害因素，根据有关标准、规程、规范、规定以及本行业国内外有关事故案例等，进行系统分析及研究，并将其结果结合运行经历，归纳、总结所有的危害因素，按顺序编制成类似安全检查所使用的安全检查表格。这样，员工在辨识危害因素时，通过对照事先编制的安全检查表，可弥补知识、经验不足的缺陷，或认识上的偏差，具有方便、实用、不易遗漏的优点，同时，结合现场实际情况，可以最大限度地现场可能存在的危害因素都辨识出来。安全检查表法适用于产品、过程或系统的生命周期的任何阶段。

2. 头脑风暴法

头脑风暴法出自“头脑风暴”一词。所谓头脑风暴（Brain Storming），最早是精神病理学上的用语，指精神病患者的精神错乱状态。现在已成为无限制的自由联想和讨论的代名词，其目的在于产生新观念或激发创新设想，故其又称智力激励法或自由思考法（畅谈法，畅谈会，集思法）。

在群体决策中，由于群体成员心理相互作用影响，易屈于权威或大多数人意见，形成所谓的“群体思维”。群体思维削弱了群体的批判精神和创造力，损害了决策的质量。为了保证群体决策的创造性，提高决策质量，管理上发展了一系列改善群体决策的方法，头脑风暴法是较为典型的一个。头脑风暴法又可分为直接头脑风暴法（通常简称头脑风暴法）和质疑头脑风暴法（也称反头脑风暴法）。前者是在专家群体决策时尽可能激发创造性，产生尽可能多的设想的方法，后者则是对前者提出的设想、方案逐一质疑，分析其现实可行性的方法。采用头脑风暴法组织群体决策时，要集中有关专家召开专题会议，主持者以明确的方式向所有参与者阐明问题，说明会议的规则，尽力创造融洽轻松的会议气氛。主持者一般不发表观点，以免影响会议的自由气氛，主要靠专家们“自由”提出尽可能多的方案。

头脑风暴法是由专家参与的辨识方法，适用于对新型业务领域以及新技术、新工艺、新材料、新设备等的危害因素辨识。

3. 预先危险分析法

预先危险分析也称初始危险分析（Preliminary Hazard Analysis，简称 PHA），是在一项活动之前，特别是在设计的开始阶段，对系统存在危险类别、出现条件、事故后果等进行概略地分析，以评价

出可能的潜在危险性。该方法一般用在设计、施工、检维修、改扩建之前，作为实现系统安全危害分析的初步或初始的计划，是在方案开发初期阶段或设计阶段之初完成的，其目的是辨识系统中存在的潜在危险，确定其危险等级，防止这些危害因素失控而酿成事故。此外，也可为进一步利用HAZOP、FMEA、ETA、FTA等方法进行深入、系统的分析工作做好准备。

预先危险分析一般用于项目评价的初期，通过预先危险分析，过滤一些风险性低的环节、区域，同时，也为在其他风险性高的环节、区域，进一步采用其他方法进行深入的危害因素辨识创造了条件，适用于固有系统中采取新的方法，接触新的物料、设备和设施的危险性评价。当只希望进行粗略的危险和潜在事故情况分析时，此方法也可以用作对已建成的装置进行分析。

4. 危险与可操作性分析法

危险与可操作性分析法（Hazard and Operability Analysis，简称HAZOP）是以系统工程为基础的一种可用于定性分析或定量评价的风险管理方法，用于探明生产装置和工艺过程中的危害因素及其原因，寻求必要对策。通过分析生产运行过程中工艺状态参数的变动、操作控制中可能出现的偏差，以及这些变动与偏差对系统的影响及可能导致的后果，找出出现变动可偏差的原因，明确装置或系统内及生产过程中存在的主要危害因素，并针对变动与偏差的后果提出应采取的措施（图1-1）。

危险与可操作性分析法可按分析的准备、完成分析和编制分析结果报告等步骤来完成。由各种专业人员（如工艺、设备、自控、现场操作人员等）按照规定的方法对偏离设计的工艺条件进行过程

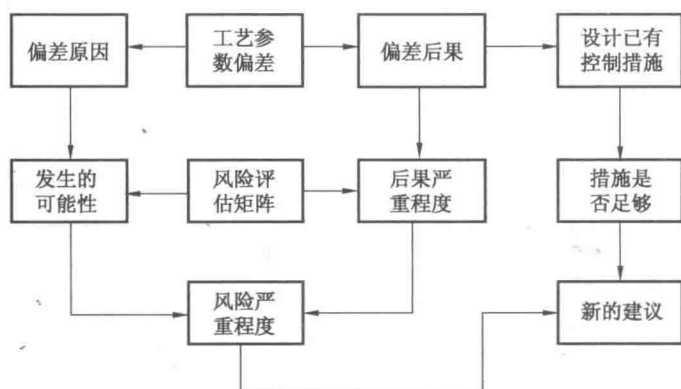


图 1-1 危险与可操作性分析法原理图

危险与可操作性研究。危险与可操作性分析法和头脑风暴法类似，不能由某人单独使用，必须由一个多方面的、专业的、熟练的人员组成的团队来完成。

危险与可操作性分析法适用于连续性生产工艺过程（连续生产装置、复杂的工艺流程等）的危害因素辨识，通过对危险与可操作性分析法的适当改进，该方法也能应用于间歇化工生产工艺过程的危险性分析。该方法既适用于设计阶段，也适于现有的生产装置的评价。危险与可操作性分析法特别适合于化工系统、装置设计和运行过程分析，如油气处理、炼油化工、储运等装置，还可以用于水利系统的安全分析。

5. 故障类型与影响分析法

故障类型与影响分析（Failure Mode and Effect Analysis, 简称 FMEA）又称“失效模式与影响分析”、“失效模式与后果分析”、“失效模式与效应分析”、“故障模式与后果分析”或“故障模式与效应分析”等。因为英文“Failure”可译作“故障”、“失效”等，

而英文“Effect”则可译作“影响”、“后果”、“效应”等，它们属于同义或近义词，由此出现了诸多中文称谓。它是以一种深入浅出的分析方式，通过分析系统基本组件潜在的问题，以及分析研究这些问题对系统的影响情况，进而发现其中需要防范的高风险危害因素的一种危害因素辨识方法。具体来说，通过 FMEA 方法，把一个系统分解为若干个子系统、单元，然后逐个分析每个部分可能发生的故障及其类型，进而推断各种故障类型对相邻单元、子系统和整个系统的影响，在此基础上，针对需要管控的问题，提出避免或减少这些影响的措施。故障类型与影响分析法因果模式如图 1-2 所示。

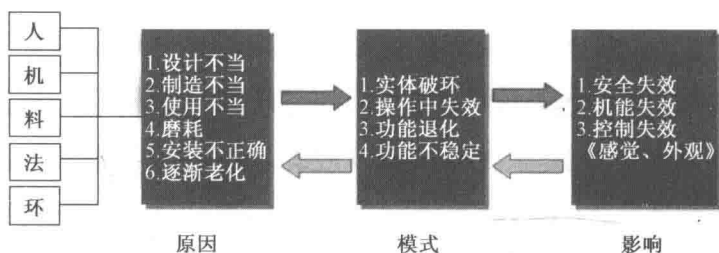


图 1-2 故障类型与影响分析法因果模式

FMEA 方法最早是由美国国家宇航局（NASA）形成的一套分析模式，美国国家宇航局（NASA）曾经在研制一种卫星系统时，由于设计时考虑不周，导致发射失败，造成 1 亿多美元的巨额损失，事后，NASA 开始了故障类型与影响的分析。FMEA 方法是一种实用的解决问题的方法，可适用于许多工程领域，目前世界许多汽车生产商和电子制造服务商（EMS）都已经采用这种模式进行设计和生产过程的管理和监控。当然，FMEA 方法也可作为一种很好的危害因素辨识方法，ISO 31010《风险管理—风险评估技术》把 FMEA 方法作为一种全能的风险评估工具而着重推荐，FMEA 方法可用作

HSE 风险管理活动中的危害因素辨识、风险分析和评价等各项工作。

FMEA 方法广泛应用于制造行业产品生命周期的各个阶段，尤其适用于产品或工艺设计阶段的危害因素辨识。同时，其他业务领域也可参照该方法进行危害因素辨识。

如果说要做好作业活动的危害因素辨识需要细化活动步骤，那么，设备、装置的危害因素辨识就要细化其功能单元，在此基础上，才能做好设备、装置的危害因素辨识，FMEA 方法就是有效工具。

6. 事故树分析法

事故树分析法（Accident Tree Analysis，简称 ATA）起源于故障树分析法（Fault Tree Analysis，简称 FTA），是安全系统工程的重要分析方法之一，它是从要分析的特定事故或故障开始（顶上事件），层层分析其发生原因，直到找出事故的基本原因，即故障树的底事件为止。这些底事件又称为基本事件，它们的数据是已知的或已经有过统计或实验的结果。它能对各种系统的危险性进行辨识和评价，不仅能分析出事故的直接原因，而且能深入地揭示出事故的潜在原因。用它描述事故的因果关系直观、明了，思路清晰，逻辑性强，既可定性分析，又可定量分析。

事故树分析法是一个逆向逻辑推理过程，即由结果逆向推理，追溯事故发生的原因，通过分析找出事故原因，采取相应的对策加以控制，从而可以起到事故预防的作用。所以说，事故树分析法是一种很好的危害因素辨识方法。

事故树分析法能对各种系统的危险性进行识别评价，既适用于定性分析，又能进行定量分析，是安全分析评价和危害因素辨识的

一种先进的科学方法。非常适合于高度重复性的系统，但要求分析人员必须十分熟悉所分析研究的对象系统，且具有丰富的实践经验。

7. 事件树分析法

事件树分析法（Event Tree Analysis，简称 ETA）起源于决策树分析法（简称 DTA），它是一种按事故发展的时间顺序由初始事件开始推论可能的后果，从而进行危险源辨识的方法。一起事故的发生，是许多原因事件相继发生的结果，其中，一些事件的发生是以另一些事件首先发生为条件的，而一些事件的出现，又会引起另一些事件的出现。在事件发生的顺序上，存在着因果的逻辑关系。事件树分析法是一种时序逻辑的事故分析方法，它以一初始事件为起点，按照事故的发展顺序，分成阶段，一步一步地进行分析，每一事件可能的后续事件只能取完全对立的两种状态（成功或失败、正常或故障、安全或危险等）之一的原则，逐步向结果方面发展，直至出现系统故障或事故为止。该法所分析的情况用树枝状图表示，故叫事件树分析法。它既可以定性地了解整个事件的动态变化过程，又可以定量计算出各阶段的概率，最终掌握事故发展过程中各种状态的发生概率。

事件树分析法与事故树分析法正好相反，是一种从原因到结果的自下而上的分析方法。从一个初因事件开始，交替考虑成功与失败的两种可能性，然后以这两种可能性为新的初因事件，如此继续分析下去，直至找到最后的结果为止，它是一种归纳逻辑树图，能够看到事故发生的动态发展过程，可看做事故树分析法的补充，可以将严重事故的动态发展过程全部揭示出来，可以用来分析系统故