化工过程危险性分析

廖学品　编著

化学工业出版社

化工过程危险性分析

廖学品　编著

化 学 工 业 出 版 社
·北　京·

（京）新登字 039 号

图书在版编目（CIP）数据

化工过程危险性分析/廖学品编著. —北京：化学工业出版社，2000
ISBN 7-5025-2778-8

Ⅰ. 化… Ⅱ. 廖… Ⅲ. 化工过程-安全性-分析 Ⅳ. TQ086

中国版本图书馆 CIP 数据核字（2000）第 12619 号

化工过程危险性分析

廖学品 编著

责任编辑：郭乃铎

责任校对：马燕珠

封面设计：于 兵

*

化学工业出版社出版发行

（北京市朝阳区惠新里 3 号 邮政编码 100029）

http://www.cip.com.cn

*

新华书店北京发行所经销

北京市彩桥印刷厂印刷

北京市彩桥印刷厂装订

开本 787×1092 毫米 1/16 印张 13½ 字数 325 千字

2000 年 4 月第 1 版 2000 年 4 月北京第 1 次印刷

印 数：1—2000

ISBN 7-5025-2778-8/TQ・1223

定 价：28.00 元

内 容 提 要

本书系统介绍了化工过程的危险性分析方法及应用。

全书分为四大部分：第一部分介绍分析方法，包括安全审查、安全检查表分析、故障假设分析、故障假设/检查表分析、预危险性分析、危险与可操作性分析、原因-后果分析、故障树分析、事件树分析、失效模式与后果分析、人的可靠性分析；第二部分则运用这些方法对虚拟的某化工过程从概念设计到装置拆除的各个阶段进行分析；第三部分介绍安全评价方法，包括美国道化学公司火灾爆炸危险指数法、日本化工企业六阶段安全评价法、我国安全检查表-危险指数评价-系统安全分析三阶段评价法等；第四部分是附录。

本书可供从事化工过程危险性分析的人员使用，也可供高校安全工程专业的师生参考。

目　　录

绪　　言

现代化工生产的工艺过程相当复杂，工艺条件要求十分严格，介质具有易燃、易爆、有毒、腐蚀等特性，生产装置趋向大型化以及生产过程的连续性、自动化程度的提高等，使生产过程发生事故的可能性增大，而且造成的危害和损失也极为惨重。我们先来看看两个具体的实例。

联合碳化物印度有限公司（UCIL）异氰酸甲酯毒气泄漏

1984 年 12 月 4 日美国联合碳化物公司在印度博帕尔（Bhopal，Indian）的农药厂发生异氰酸甲酯（CH_3NCO，简称 MIC）毒气泄漏事故，造成 2000 人死亡、200000 人受伤的让世界震惊的重大事故。MIC 是生产氨基甲酸酯类杀虫剂的中间体。甲氨基甲酸萘酯是一种杀虫剂。

MIC 极不稳定，需要在低温下贮存。博帕尔的 MIC 贮存在两个地下冷冻贮槽中，第三个贮槽贮存不合格的 MIC。博帕尔的联合碳化物印度有限公司（UCIL）建设过程正处于城市的快速发展时期，80 年代因为对杀虫剂的需求减少，UCIL 装置关闭。

三个 MIC 贮槽的进料是用带氮气夹套的不锈钢管从精制塔送来，并用普通管道将其送到甲氨基甲酸萘酯反应器，在反应器上装有安全阀。不合格的 MIC 循环至贮槽，含 MIC 的废物送至放空气体洗涤器（VGS）被中和。每个 MIC 贮槽都有温度和压力显示仪表，以及液位指示和报警，如图 0.1。MIC 贮槽上装有固定的水监视器和致冷单元。当 VGS 中有大量释放时可使用燃烧系统，VGS 和燃烧系统的排放高度为 15～20m。1984 年 6 月不再使用贮槽的致冷系统，而且把致冷剂放出。1984 年 12 月停止生产 MIC，而且裁员 50%。

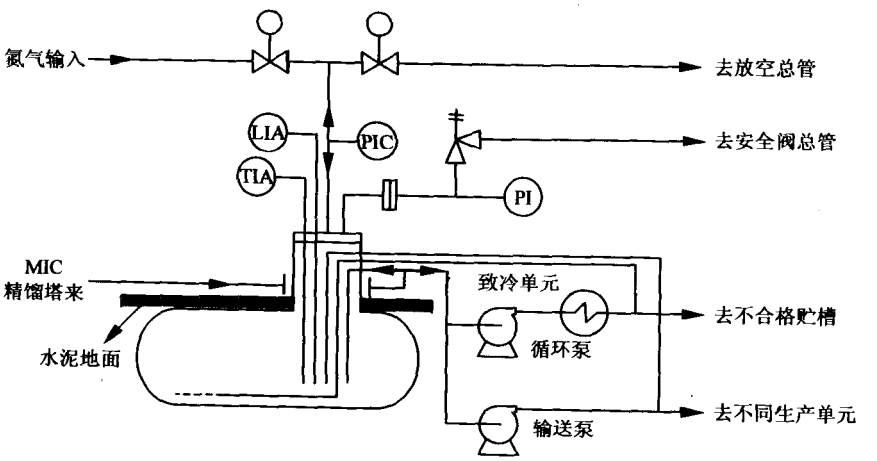

图 0.1　MIC 贮槽简图

1984 年 12 月 2 日，第二班负责人命令 MIC 装置的操作工用水清洗管道。在操作前应该进行隔离，但被忽略了；而且几天前刚进行了检修，加上其他可能性，冲洗水进入了其中一

个贮槽。

23 时贮槽的压力在正常范围，23 时 30 分操作工发现 MIC 和污水从 MIC 贮槽的下游管道流出，0 时 15 分贮槽的压力升至 206.84kPa（30 psi），几分钟后达到 379.21kPa（55 psi），即最高极限；当操作工走近贮槽时，他听到了隆隆声并且感受到贮槽的热辐射；在控制室操作工试图启动 VGS 系统，并通知总指挥；当总指挥到来时命令将装置关闭；水喷淋系统已打开但只能达到 15m 的高度，MIC 的排放高度为 33m。他们还试图启动致冷系统，但是因为没有致冷剂而告失败。至此，开始向社区发出了毒气报警，但几分钟后报警声停止，只能用汽笛向 UCIL 的工人发出警报。据称开始时汽笛引起误会，人们以为是装置发生了火灾而且准备参加灭火；而 UCIL 的工人则错误地顺着毒气云的方向逃生。

安全阀一直开了两个小时，气、液、固三相以超过 200℃的温度、1241.06kPa（180 psi）的压力释放到空气中。因为博帕尔城市发展很快，人口多，短时间内无法完全疏散；加上贫民区已建到 UCIL 的围墙下面，简陋的屋子一点也起不到保护作用；城市的基础设施（如医院等）已无法应付这么巨大的灾难，仅有的两所医院其设施只能容纳千余人，而中毒人数是其 10 倍。

表 0.1 和表 0.2 是这次事故发生的详细过程和根本原因。

表 0.1　博帕尔毒气泄漏事故的详细过程及后果

后果——伤害和破坏： 2000 余人死亡，200000 人受伤 停产 公司将赔偿几百万美元，股票暴跌，财政危机，联合碳化物公司从世界排名第 37 位降至 200 位	**恢复系统失效：** 放空系统洗涤器能力不足
装置外保护设施失效： 无应急计划 报警系统关闭 当地居民区无保护设施 医疗设施有限	**装置出现危险故障：** 贮槽温度和压力升高
释放升级： MIC 蒸气云逸出装置外	**紧急控制系统失效：** 泄放阀放空高度 33m MIC 贮槽上无在线监视系统或高温报警
装置内的保护设施失效： 消防水只能达到 15m 的高度 因无致冷剂所以致冷单元无法工作 因为维修燃烧系统无法工作 近两个小时未察觉问题	**危险偏差：** 因 MIC 催化聚合引起温度和压力升高
大量有毒物质放出： 36t MIC 放出（气、固、液）	**控制系统失效（报警）：** 无报警
	工艺偏差： 温度和压力升高
	正常控制不当： 该系统实际上无控制 温度和压力指示器有缺陷
	事故的直接原因： 冲洗时未按规程进行隔离 水可能在管道冲洗过程或其他地方进入 MIC 贮槽

注：从表尾至表头为事故的发生、发展及结果。

根据该公司的事故调查报告，这次事故是因为贮槽中含有水和三氯甲烷，从而发生剧烈反应而引起的。贮槽中含有水和三氯甲烷的原因不太清楚，但是用危险与可操作性分析（HAZOP）方法能够找出可能的原因，并采取必要的措施避免水与异氰酸甲酯接触而导致的剧烈反应。当贮槽的安全阀打开后，应有一个独立的洗涤系统吸收所放出的蒸气，同时燃烧系统应将未被洗涤下来的毒气燃烧掉，冷却系统应使贮槽保持低温；另外一个重要问题是为什么要贮存大量的异氰酸甲酯？因为异氰酸甲酯是中间体，完全没有必要贮存那么多，如果进行 HAZOP 分析就完全能够分析到是否需要这个中间贮槽。

表 0.2 事故的根本原因

子系统	可能发生事故的条件	子系统	可能发生事故的条件
外部系统	装置附近人口激增而基础设施建设严重滞后 当发生紧急情况时与外界的联系不当 可能存在人为破坏	工程完整性	安全系统不足而且无法工作 修改不当而且修改后未进行分析 管道、阀门及仪表缺乏维修
系统环境	检查结果未得到落实 可能有更为安全的工艺路线 市政府的决定被地区政府否决 因需求不足生产不正常 扩大生产工艺过程而进入相对不太安全的领域	管理控制	目标、责任、制度不明确 对修改的管理不当而且未选择安全的工艺流程 安全责任不明确 缺乏安全训练和技术经验 无应急计划
组织和管理	未承担足够的安全义务 应对紧急情况的准备不足 印度政府安全检查不力 对公众面临的危险失察 与设在美国的总公司联系有限 员工水平不高	通讯和资料	无 MIC 的毒性资料 总公司发来的警告未得到落实
		规程和实践	对操作规程的认证不充分 未按照规程对装置进行冲洗 缺乏紧急情况处置规程
位置和装置设备	无区域规划政策 对工艺过程的预分析不当 在不当条件下长时间大量贮存工艺物料 贮槽未隔离，而且未安装阀门位置指示器 过量水进入 MIC 贮槽	工作环境	操作工裁员 50% 缺乏有经验的人员
		操作工的操作	操作工无足够的技术知识 员工因对装置的前途不定而心理紧张

切尔诺贝利核电站爆炸事故

1986 年 4 月 26 日，切尔诺贝利核电站的 4 号反应堆发生爆炸，31 人死于放射疾病。据国际放射保护委员会估计未来几十年中整个欧洲得癌症的人数将增加 30000 人。

1970 年切尔诺贝利开始修建第一座核反应堆，但总工程师只有建设火电站的经验，整个设计由乌拉尔电力公司设计院进行。后来由莫斯科 Zukh 水电设计院接手该项目的设计，该设计院主要是水电设计。因为物质缺乏，几乎不太可能找到设计人员设计的某些特殊部件，因此设计者只好将就使用他们自己制造的部件。

1977 年第一座反应堆投入运行，与原定计划推迟了两年。管理人员和操作工并不知道 1975 年在列宁格勒与此相同的反应堆发生了熔化事故。对有关规定也进行了修改，因为它们对实际情况不适合，特别是经常移出比规定多的控制棒。操作工还发现当输出功率很低时反应堆极不稳定。

20 世纪 80 年代初，另外两个反应堆投入运行。1982 年第三座核反应堆活性区发生爆炸并将放射性物质释放到核电站区域，因为对这次事故保密，其他反应堆的操作人员并不知道此次事故的发生。这期间在整个前苏联的 ЯВМК 型反应堆还发生了几起类似的事故。1980 年在 Kursk 发生的事故引起了原子能委员会的注意：因为停电导致无动力驱动控制棒和水泵，40 秒后才启动备用电源，在此次事故中因为冷却水的自然循环量较大才避免了严重破坏。

1983 年末，估计切尔诺贝利 4 号反应堆关闭后透平机还能为反应堆水泵提供一定时间的应急电源，曾建议对该系统进行测试，但因为装置到 1983 年底前未获授权，因此对该系统的测试延期进行。在负责 ЯВМК 型反应堆的部长处还有其他的事故记录——设计的控制棒因为有裂纹当插入反应堆时引起输出功率剧烈波动，但在操作工的操作记录上没有记录。1984 年 3 月 27 日，4 号反应堆正式投入商业运行。

1985 年报纸上出现了对核电站的批评，能源部命令总工程师替换易燃的遮蔽材料和电缆。但是因为无不易燃的材料供应，这项计划被搁置。高层管理人员的注意力集中在应付商业压力，而让总工程师负责装置的操作。

1986 年 4 月，4 号反应堆停车检修，并且安排了一系列的测试计划，包括应急电源延迟测试。但仍然不知道当透平的动量下降后是否能产生足够的电能驱动水泵达 40 秒。测试由装置的制造者进行，他们的测试计划与 3 号和 4 号反应堆的总工程师讨论了 15 分钟后即获同意，并没有征求安全检查员的意见，负责反应堆的总工程师也没有到场，正式的批准文件也没有征求核专家的意见。

13 时反应堆的输出功率减为一半，两台发电机一台停车。14 时对另一台发电机的测试准备就绪。为了避免被联锁，紧急反应堆活性区冷却系统断开。开始准备测试时，Kiev 的电力调度员请求供电到 23 时。23 时重新开始根据拟定的计划对透平机的作用进行测试。控制棒的自动控制系统被断开，输出功率降低，下降到 30MW。到这一步就没有按照测试的标准规程进行（按标准规程应该放弃试验），工程师就下一步如何进行没有形成统一的意见。继续移出控制棒，4 月 26 日 1 时输出功率稳定在 200MW，但这仍然低于推荐的最小功率水平，但是被认为可以继续进行测试。

1 时过后，另一台冷却泵很快加入该系统，这就需要移出更多的控制棒。大量的水进入反应堆引起蒸汽压力降低。为了避免因为蒸汽压力低导致反应堆关闭，操作人员切断了联锁信号。1 时 22 分，实验刚刚开始，计算机打印结果表明反应性只有最小保留值的一半。1 时 23 分透平发电机的紧急调节阀门关闭，透平机无蒸汽，计算机显示反应器功率急剧上升，副控手按下紧急停车按纽试图将所有控制棒放入反应堆活性区，此时控制棒无法全部下降。爆炸发生了，爆炸掀翻了 1000t 反应堆外壳，反应堆直接向大气敞开。

工程师没有意识到反应堆已发生了爆炸，还试图用大量的水来控制反应堆，但是所有的泵都无法工作。发电机房着火，消防队也赶来，关键人物也来到现场。核电厂厂长被告知反应堆未破坏，只是需要他对产生的放射程度进行分析调查，但据说莫斯科官方拒绝授权。

4 月 26 日下午，有足够的证据表明反应堆发生了爆炸，其他的反应堆也已关闭。成千上万吨含有硼、铅等的沙石飞向建筑物。对相邻城镇 Pripyat 的调查于 4 月 27 日展开。

表 0.3 和表 0.4 是事故发生的详细过程和根本原因。

通过对该事故的分析可以得到这样的结论：如果测试计划制定更仔细一些，或者征求有关专家的意见，或者得到有关机构的认证，事故是有可能避免的。对测试计划进行危险性分析，识别可能出现的危险情况并采取相应的措施是制定测试计划的关键。这个过程应当采用某种危险分析方法，本书所介绍的分析方法如 HAZOP、检查表分析、故障假设分析都可以用来对该测试过程进行分析，使用这些方法肯定能找出测试过程可能出现的危险情况。从该例可以看出，本书所介绍的分析方法不仅适合于对化工过程进行危险性分析，而且对其他过程（如机械工业、航天工业、兵器工业、国防工业、核工业等）稍加修改也可使用。

现代化工生产的工艺过程相当复杂，工艺条件要求十分严格，介质具有易燃、易爆、有毒、腐蚀等特性，生产装置趋向大型化，以及生产过程的连续性、自动化程度的提高等，使生产发生事故的可能性很大，而且造成的危害和损失也极为惨重。1989 年原化工部科学技术情报研究所出版的《全国化工事故典型案例分析》一书，将化工过程发生的事故分成 15 大类，在所选的 316 个案例中，火灾、物理爆炸、化学爆炸、中毒和窒息占了 159 例，这与化工过程的生产特点有关，即高温、高压、有毒、危险品。化工生产过程的安全性问题越来越受到

政府或企业的高度重视，制定了相应的法律和法规，这无疑大大地提高了化工生产过程的安全性。

表 0.3　切尔诺贝利核反应堆爆炸事故的发生过程

后果——伤害和破坏： 31 人死亡，短期内发现 300 例放射污染疾病 欧洲癌症发病率将明显上升 30 公里范围内 135000 人将被疏散 大面积土地受到污染	**装置的危险波动：** 可能是“正空穴系数”所致
减轻措施失效： 无第二层保护 对紧急救援队缺乏保护设备 因为政治原因未迅速作出反应	（紧急）**状态控制失效：** 当出现与测试计划背离的情况时未放弃测试 因疏忽让“滞留电力”进入，使功率降到很低的水平 操作工严重降低了功率设定值 **危险偏差：** 14 时 5 分因为 Kiev 控制员请求继续向电网供电，使装置在 50%的功率下运行了 9 个小时，可能产生氙
事故升级： 1 时 24 分装置达到超临界状态 输出功率每秒上升 100 倍，结果是反应堆爆炸	**状态控制失效：** 反应堆的大部分保护系统不能工作 维修测试违反操作规程
状态恢复系统失效： 将反应堆剩下的防护设施关闭后继续进行测试 1 时 22 分反应堆活性区控制棒少于 8 根 1 时 24 分当反应堆出现故障时试图“紧急刹车”	**工艺（过程）偏差：** 1986 年 4 月 25 日降低输出功率，当输出功率达 25%时作为测试条件 操作工降低功率所使用的紧急活性区冷却系统已断开
装置的危险波动： 反应堆输出功率为 7%时虽然是稳定的，但低到设计规定最小值的 20%是非常危险的	**事故的直接原因：** 试验企图分析可能对活性区熔化保护系统造成危险障碍的设备

注：从表尾至表头为事故的发生、发展及结果。

表 0.4　切尔诺贝利事故的根本原因

子系统	可能发生事故的条件	子系统	可能发生事故的条件
外部系统	工人的居住区靠近装置 从上级公司得到的支持不够	工程完整性	自建设开始未对修改后的标准进行更新 缺乏工程安全设备以避免操作工失误 系统的安全系数不当
系统环境	项目预算紧张，资源短缺 专家假定 ЯBMK 型反应堆不可能发生爆炸 因在其他反应堆发生事故所以才进行测试 因为政治原因未直接进行分析	管理控制	测试计划不周 管理者对测试的技术理解有差异 改正措施不当 违反规定 缺乏安全训练，安全责任分工不明 紧急情况处置不当
组织和管理	测试未经俄罗斯核建设委员会批准 设定工作顺序的方法错误 物资和工程设备的管理不当 紧急反应物资和设备不足 对其他装置发生的事故保密	通讯和资料	提供的紧急情况应对资料不充分
		规程和实践	未提供参考资料
位置和装置设备	装置未经授权——不应进行测试 反应堆的设计使得当输出功率低于 20%时不稳定 大型活性区需要复杂的控制系统 因为管线复杂，因此为每个通道提供紧急冷却比较困难	工作环境	为准备测试员工已工作了 24 小时 负责试验的工程师对核反堆知之甚少 程序的质量低
		操作工的操作	操作工的操作未达到设计的装置条件 偏离规定的操作规程，忽视安全规程 操作工过分自信 违反一系列的操作规定 总工程师过于“热心”

人们在进行事故调查时总是从违章操作、设计不合理以及安全管理混乱等方面找原因，当然这些都是导致事故的主要原因。但是假如能够事先对工艺过程和装置的操作进行分析，找出可能存在的危险，并对所存在的危险采取相应的措施（如修改设计、增加安全设备等），就

能够大大地提高系统或工艺过程的安全性。如果能识别出可能存在的危险，安全问题就解决了一半，再加上对可能存在的危险采取了措施，则发生事故的可能性将大为降低。很多事故都与操作工的操作有关，但是一味地指责操作工是不恰当的，也是不公平的，既然某个地方如果操作工误操作就有可能导致事故，那为什么不采取相应的安全措施呢？按现代化工生产过程的观点，所设计的生产过程应该是“用户友好”的，所谓的“用户友好”，至少应该是当发生误操作时不至于导致人员伤亡，系统能安全停车。另一方面是如何判定所设计的工艺过程本身是否合理或是安全的。这就需要按照一定的方法和程序对项目发展的各个阶段以及对装置的操作（如开停车、正常操作、维修等）进行危险性分析。用化工过程危险性分析方法对化工过程的设计、安装、试车、开车、停车、正常运行、检修等阶段进行分析，几乎可以发现过程所存在的所有危险。

在人们的固有观念中，化工过程安全无非就是加强安全的管理与检查，制定一系列的安全管理法规，在过程设计中引入安全装置等，毫无疑问这些都是很重要的，但问题是在设计和操作过程中是否考虑到了所有可能导致事故的危险情况？所设计的系统的安全性如何？特别是新的工艺过程的设计，无经验可供借鉴，又如何在设计过程中考虑到所有的危险情况呢？既然在化工过程存在着危险性，为什么不在设计过程中尽可能地发现这些危险并加以消除，让过程本身就是安全的（即固有安全）呢？而且在装置建成之后，或者装置的改造之后进行危险性分析，根据对装置的操作及安全管理经验可以进一步发现安全问题，经过改进，可以进一步提高过程的安全性。在现代科学技术发展的今天，发现问题比解决问题更重要，对化工过程安全而言，重要的是找出所有的危险情况，这就是危险性分析的目的；针对这些危险情况提出相应的改进措施，如采用危险性小的工艺过程、使用新的安全技术等。如果在过程的概念设计阶段就引入危险性分析，而且在项目发展的各个阶段都进行危险性分析将大大提高过程的安全性。作者认为对过程的危险性进行分析是整个化工过程安全的重要组成部分，这种分析将对系统客观地、全面地进行分析，分析内容包括：物料、设备、操作、仪表、维修、分析等整个工艺过程的各个方面以及安全管理，其分析结果作为进一步设计和安全管理的依据。美国政府以法律的形式规定所有的化工企业在1996年前必须进行危险性分析，否则不能进行生产；英国也作出了相同的规定，在英国的许多高校化工系的课程中都开设有过程安全课程，有一系列的专著出版。英国的拉夫伯勒大学化工系长期开展化工过程安全方面的研究，化工过程危险性分析是其主要研究内容之一。

作者在英国利兹大学访问进修期间阅读了大量的有关化工过程安全方面的资料，对欧美等国对安全的重视感触很深。本书的目的在于系统、全面地介绍化工过程危险性分析方法。本书的名词术语可能在翻译上存在差异，而且因为基本采用国外资料，某些内容或提法不符合我国国情；加之作者水平有限，收集资料遗漏，错误和不妥之处敬请各位专家批评指正。

在本书的编著过程中得到了英国利兹大学化工系教授王学重博士的大力支持，云南工业大学牛存镇教授和角仕云教授对本书提出了许多宝贵意见并审稿，在此表示感谢。

第一部分　化工过程危险性分析方法

1　化工过程危险性分析方法概述

本章的目的是对各种危险性分析方法作一简要介绍，在以后的各章中将对这些方法作详细说明，读者可根据需要选读其中的某一部分。所列出的分析方法并不是对所有分析对象都适用，换句话说，对不同的分析对象应选用不同的分析方法，各种分析方法适用于项目发展过程中（或称工程项目发展过程）的不同阶段，如“安全检查（Safety Review）”、“安全检查表分析（Safety Checklist Analysis）”、“故障假设分析（What-If Analysis）”等分析方法适用于项目发展的初期阶段，如概念设计阶段；而“危险与可操作性分析（Hazard and Operability Analysis，简称 HAZOP）”则适用于过程详细设计阶段和正常操作时对过程进行分析，“故障树分析（Fault Tree Analysis，简称 FTA）”及“事件树分析（Event Tree Analysis，简称 ETA）”是对某一个或几个特定的分析对象进行定性或定量的分析。某些过程危险分析方法如故障树分析、事件树分析、原因-后果分析、人的可靠性分析则需要经过专门的学习并具有实践经验的分析人员才能完成。正确选用这些危险性分析方法对项目发展过程的各个阶段进行危险性分析，可以发现设计、生产过程中可能产生的危险，并提出改进措施，这样可以大大的提高过程的安全性。

对每一种分析方法的简介包括以下内容：方法描述、目的、分析结果，以及所需资料。这些信息有助于选择合适的危险分析方法。

另一个重要因素是分析对象的大小和复杂程度，为了估计这种影响并让分析人员大致估计完成某一分析所需时间，将分析问题分成两类，即简单/较小的系统和复杂/较大的系统。

（1）简单/较小系统—如化学品的卸料和贮存系统，需要考虑卸料平台、输送管线、泵、贮槽，压力控制以及蒸气返回管线等。

（2）复杂/较大系统—如化学反应过程要考虑进料系统、反应系统、产品的分离与回收、紧急释放系统，以及与之相连的管路和控制系统。该过程一般有 10～20 个主要的容器，包括反应器、塔器、贮槽等。

上述两种类型的系统可作为估计危险性分析所需时间的基准。用某一种危险分析方法对某特定分析对象进行分析包括三个步骤：分析的准备、分析、分析报告。分析的准备包括资料的收集、确定分析范围以及分析的组织；分析就是按照选定的分析方法进行实际分析的过程，如采用 HAZOP 分析，则整个分析过程则必须以会议的形式进行。对特定的分析方法应当包括复杂故障逻辑模型的建立，以及模型的发展阶段；分析报告不仅应当包括分析会议（过程）的记录，而且应当包括对主要工艺过程的描述、重要结果的讨论、表格或逻辑模型、对拟采取的重要措施作简要的解释。

通常以小时、天、周来估计分析所用的时间。某些分析组成员可以只参加整个分析过程的一个或两个阶段，如 HAZOP 分析，而某些分析成员特别是分析组的领导或组织者必须参加整个分析过程。此外还应当考虑其他一些因素，如分析组对某一分析方法的熟练程度。

以上内容只是让分析人员了解完成某一分析过程大致需要作哪些工作和大致所用的时

间。然而因为还有很多其他的因素，分析人员在估计分析过程所用的时间时应当慎重，实际分析过程所用的时间通常比估计的时间要多得多。如果分析人员及分析的组织者对分析方法富有经验，将大大提高分析过程的效率。下面简要介绍主要的危险分析方法。

1.1 安全检查

1.1.1 说明

毫无疑问，安全检查（Safety Review）是第一个危险分析方法，这种方法又称为过程安全检查(Process Safety Review)、设计检查(Design Review)、避免危险检查(Loss Prevention Review)，这种方法可用于工艺过程发展的各个阶段。当分析对象为已投入运行的装置时，安全检查可以是非正式的、感性的，也可以是正式的、由专门的分析组花上几个星期完成的工作；对正在进行设计的工艺过程，项目设计组可对图纸进行安全检查。

安全检查用来识别可能导致人员伤亡、财产损失、环境破坏等事故的装置条件或操作程序。典型的安全检查包括与装置有关的人员座谈，这些人员包括：操作人员、维修人员、工程技术人员、管理人员、安全人员及与装置有关的其他人员。安全检查应该致力于提高整个系统的安全和操作性能，而不是去干扰正常的操作或者制定一系列的惩罚条款。各方面的合作是开展工作的基础，在认识到对装置人员和设计者带来的好处之前人们通常会固执己见，因此整个分析过程都应取得各方面的支持。

安全检查通常瞄准主要的危险，枝节问题不是安全检查的目的，当然这些枝节问题也是需要进一步改进的。安全检查还应吸收其他工艺过程的安全经验，如常规安全检查以及其他危险分析方法（安全检查表、故障假设分析）。

安全检查结束时，分析人员应对存在的安全隐患提出相应的处理方案，对处理方案进行评价，推荐负责人，以及完成日期，接下来的工作是督促检查是否按要求完成了所提出的处理方案。

1.1.2 目的

安全检查可用于保证装置和操作以及维修符合设计要求和建设标准，安全检查过程的目的是：①让操作人员对过程危险保持警惕；②对操作程序进行检查并作必要的修改；③发现由于设备或工艺改变所带来的新的危险；④对控制和安全系统的设计依据进行评估；⑤对新的安全技术应用于已存在危险进行检查；⑥检查维修及安全检查是否适当。安全检查还常常用于过程开车前的安全检查。

1.1.3 分析结果

安全检查是对过程潜在安全问题的定性描述，并提出改正措施。安全检查报告包括若偏离设计的工艺条件所引起的安全问题、偏离规定的操作规程所引起的安全问题、新发现的安全问题，以及确认改正措施的负责人。

1.1.4 所需资料

对工艺过程进行安全检查之前，分析组成员应获得并研读以下资料：

(1) 规范或标准；

(2) 以往的安全分析报告；

(3) 详细的工艺和装置描述，PID（带控制点的工艺流程图）和 FID（工艺流程图）；

(4) 开停车、正常操作、维修、紧急情况下的操作规程；

(5) 人员伤害报告；

(6) 危险事故报告；

(7)维修记录，如关键设备的检查，安全阀的测试，压力容器的检测；

(8) 工艺物料性质，如毒性和反应活性。

表 1.1 安全检查需用时间

范　围	准　备	分　析	报　告
简单/较小系统	2～4 小时	6～12 小时	4～8 小时
复杂/较大系统	1～3 天	3～5 天	3～6 天

参加安全检查的人员需对安全标准和程序非常熟悉，同时需要建筑、电气、压力容器以及其他特定项目的具有专业知识和丰富实践经验的人员参加。表 1.1 是估计完成安全检查所用时间。

1.2 安全检查表分析

1.2.1 说明

安全检查表分析（Safety Checklist Analysis）是将一系列分析项目列出安全检查表进行分析以确定系统的状态，这些项目包括设备、操作、控制、环保、安全等各个方面。传统的安全检查表分析方法所列项目差别很大，而且通常用于检查各种规范和标准的执行情况。安全检查表分析方法很容易掌握，可用于项目发展过程的各个阶段，通过将工艺过程与安全检查表进行对比，可使无经验的人员熟悉工艺过程，分析人员对工艺或操作的评估还为管理检查提供第一手资料。

详细的安全检查表为过程危险性的标准评价提供依据，它也可以对某些特殊情况进行分析，但它应当用于那些需进一步考虑的问题。安全检查表分析方法通常与其他分析方法配合使用来对危险情况进行估计。安全检查表分析受分析人员经验的限制，因此，需由对分析系统具有丰富经验的人员来完成安全检查表分析。通常，安全检查表内容包括规范、标准和规定，并随时关注并采用新颁布的有关规范、标准和规定。

许多机构使用标准的安全检查表对项目发展的各个阶段（从初步设计到装置报废）进行分析，换句话说，安全检查表内容是一定的。但是完整的安全检查表应当随着项目从一个阶段到下一个阶段而不断完善，这样，安全检查表可作为交流和控制的手段。

1.2.2 目的

传统的安全检查表分析主要用于确保有关规定和标准得以实施，某些情况下，分析人员将安全检查表分析方法与其他危险分析方法结合起来去发现只用安全检查表分析可能无法发现的危险（如故障假设/安全检查表分析）。

1.2.3 分析结果

分析人员确定标准的设计或操作以建立传统的安全检查表，然后用它产生一系列基于缺陷或差异的问题。所完成的安全检查表包括对提出的问题回答“是”、“否”、“不适用”或“需要更多的信息”。定性的分析结果随不同的分析对象而变化，但都将作出与标准或规范是否一致的结论。此外，安全检查表分析通常提出一系列的提高安全性的可能途径并提供给管理者考虑。

1.2.4 所需资料

为了较好地完成安全检查表分析，需要一份适当的安全检查表、工程设计程序及操作方法，以及完成安全检查表分析的人员应当具有待分析过程的基本知识。如果根据以往的工作能得到一份可靠的安全检查表，只要它还具有指导意义，分析人员应当尽量使用它；如果没有，必须由一人（有时是几个人）来准备安全检查表并完成分析。有经验的管理者或总工程师应当检查安全检查表分析结果并指导下一步的工作。建立安全检查表时可参考本书附录 B。

安全检查表分析的弹性很大，既可用于简单的快速分析，也可用于更深层次的分析，它是识别已知危险的有效方法。表 1.2 是完成安全检查表分析需用时间。

表 1.2 安全检查表分析需用时间

范　围	准　备	分　析	报　告
简单/较小系统	2～4 小时	4～8 小时	4～8 小时
复杂/较大系统	1～3 天	3～5 天	2～4 天

1.3 预危险性分析

1.3.1 说明

预危险性分析（PHA，Preliminary Hazard Analysis）由美国 MSSSPR（U. S Military Standard System Safety Program Requirement）衍变而来。PHA 主要用于对危险物质和装置的主要工艺区域进行分析。它常常在过程发展的初期，当无详细设计和操作程序资料时进行，而且是进一步危险分析的先导，在过程发展的初期使用这一方法非常有效。因为该方法有军工背景，PHA 有时用于检查非受控状态下有能量释放的工艺区域。

通过考虑以下工艺特点，PHA 将危险和危险状态列表：

- 原料，中间和最终产品，以及它们的反应活性；
- 操作环境；
- 装置设备；
- 设备布置；
- 操作活动（测试、维修等）；
- 系统之间的连接。

一个或几个危险分析人员对主要的过程危险进行评估，并对每一个特定危险状态划分等级，以区分为提高安全性所提出的意见或建议的先后顺序。

1.3.2 目的

PHA 常用于过程发展的初期阶段的危险性分析，通常在工艺装置的概念设计或研究和发展阶段使用，而且在进行厂址选择时非常有用，它还经常作为 PID 设计之前的设计检查工具。

虽然 PHA 方法一般用于项目发展的初期阶段，此时对潜在的安全问题无经验可借鉴，但当分析大型的已投入运行的装置或者对危险划分先后次序时也是很有帮助的。

1.3.3 结果

PHA 定性说明与过程设计有关的危险；PHA 还提供危险状态的定性等级，为在项目发展过程的后续阶段消除或减少危险所提出的意见或建议划分先后顺序。

1.3.4 所需资料

使用 PHA 方法需要分析人员获得装置设计标准、设备说明、材料说明及其他资料。可由一个或两个具有过程安全知识的人员完成 PHA，对于缺乏经验的人也可完成 PHA，但不太可能进行详细的分析，因为这种方法需要分析人员进行大量的判断。表 1.3 列出了 PHA 方法所需时间。表 1.3 列出了 PHA 所需时间。

表 1.3 PHA 需用时间

范　围	准　备	分　析	报　告
简单/较小系统	4～8 小时	1～3 天	1～2 天
复杂/较大系统	1～3 天	4～7 天	4～7 天

1.4 故障假设分析

1.4.1 说明

故障假设分析（What-If Analysis）方法是一种创造性的分析方法，它是由熟悉工艺过程、富有经验的人员所组成的分析组，通过提出问题（故障假设）来发现可能潜在的事故隐患。它不同于其他的分析方法（如 HAZOP 和 FMEA），它需要分析人员将基本概念用于特定对象。

有关故障假设分析方法的资料很少，然而几乎在项目发展的各个阶段都可以使用故障假设分析方法，并取得满意的效果。

故障假设分析方法实质上是要求危险分析小组从思考问题入手。然而，任何对过程安全的考虑都必须指出，即使不以问题的方式提出来。例如：

我考虑提供的原料不对（不以问题的方式）

如果开车过程中泵停止运行会发生什么情况（以问题的方式）

如果操作人员打开阀门 B 而不是 A 会发生什么情况（以问题的方式）

通常由记录人员将所有问题制作成图表、卡片等，然后分门别类，如电气安全、防火、人员安全等，然后分成几个分析小组分头进行分析。所提出的问题基于实际经验、图纸及工艺说明；对正在运行的装置，应与分析组以外的人员座谈（不拘形式，除非组织者将过程分为不同的功能系统）。所提出的问题涉及任何与装置有关的非正常条件，而不仅仅是设备故障或工艺变量。在进行故障假设分析时可参考本书附录 B。

1.4.2 目的

故障假设分析的目的是识别危险或隐患，或可能导致不良后果的事故事件。有经验的分析组将找出事故隐患，分析可能的后果，已有的安全保护措施，提出降低或消除危险的方法。分析方法包括检查设计、安装、技改或操作过程中可能产生的偏差，它需要对整个工艺过程有一个基本的了解，能预测可能产生的与设计要求不同的偏差及其可能导致的后果。这就要求分析人员具有丰富的经验，否则其分析结果将是不完整的或根本达不到预期效果的。

1.4.3 分析结果

故障假设分析方法首先提出一系列的问题，然后回答这些问题。分析结果可以表格的形式出现，主要内容包括：问题、对问题的回答（可能后果）、安全措施、降低或消除风险的可能方法。

1.4.4 所需资料

因为故障假设分析方法非常灵活，在项目发展的任何阶段均可使用。因此与过程有关的材料都可能用到。对任意一个局部过程，由 2～3 人即可完成分析，当然也可组织较大的分析组，视具体的分析对象确定具体的参加人员。对复杂的系统，最好组织由各方面人员参加的分析组，并且将复杂问题尽可能分解成若干小的问题。

表 1.4 故障假设分析所需时间

范　围	准　备	分　析	报　告
简单/较小系统	4～8 小时	4～8 小时	1～2 天
复杂/较大系统	1～3 天	3～5 天	1～3 周

故障假设分析所需时间与装置的复杂程度及分析区域的数量成正比，当然还与分析组的组织及成员的经验有很大的关系。表 1.4 列出了使用故障假设分析方法所需时间。

1.5 故障假设/安全检查表分析

1.5.1 说明

故障假设/安全检查表分析（What-If/Safety Checklist Analysis）是将具有创造性的故障假设与具有系统性的安全检查表分析方法结合起来的分析方法。这种分析方法吸收了各自的优点和长处，弥补了各自的不足。例如，安全检查表分析方法是基于经验的方法，使用这种分析方法主要依靠安全检查表分析者的经验，如果所列安全检查表不完整，分析人员就不能有效地找出危险情况；而故障假设分析方法鼓励分析人员思考潜在事故事件及后果，它不受分析人员经验的限制，因此可以分析到安全检查表分析无法分析到的问题；反过来安全检查

表分析方法使故障分析方法更具系统性。故障假设/安全检查表分析方法可用于项目发展的各个阶段。

与大多数的其他分析方法一样，故障假设/安全检查表分析同样需要对工艺过程具有丰富经验的人才能很好的完成。该方法常用于分析存在于过程中的最普通的危险，虽然它能分析几乎所有层次的事故隐患，但该方法一般不作更为详细的分析，而不像后面将介绍的 FMEA 分析方法。通常，故障假设/安全检查表分析方法用于过程危险的初步分析，然后再用其他分析方法对发现的问题进行详细分析。

1.5.2 目的

故障假设/安全检查表分析的目的是识别潜在危险，考虑过程或活动中可能发生的事故类型，定性估计这些事故的可能后果，确定已有安全保护措施是否对潜在的事故起作用。通常，分析人员还应提出降低或消除过程操作风险的方法。

1.5.3 分析结果

危险分析组使用故障假设/安全检查表分析方法将得到一份分析结果表，内容包括事故情况、后果、已有的安全保护、拟采取的措施，该分析结果还包括完整的安全检查表。不同的机构对结果文件有不同的要求。

表 1.5 故障假设/安全检查表分析所需时间

范　围	准　备	分　析	报　告
简单/较小系统	6～12 小时	6～12 天	4～8 小时
复杂/较大系统	1～3 天	4～7 天	1～3 周

1.5.4 所需资料

大多数情况下，故障假设/安全检查表分析由对过程有经验的设计、操作、维修人员组成。所需人数取决于待分析过程的复杂程度、内容及阶段。通常，使用这种分析方法所需人员和时间比使用 HAZOP 分析方法少。表 1.5 列出了这种分析方法所需时间。

1.6 危险与可操作性分析

1.6.1 说明

危险与可操作性分析（HAZOP）方法是用来识别和估计过程的安全方面的危险以及操作性问题，虽然这些操作性问题可能并没有什么危险性，但通过可操作性分析以保证装置达到设计能力。该分析方法最初是为缺乏预报危险和操作性问题经验的分析组设计的，但发现该方法同样适用于已投入运行的工艺过程。使用 HAZOP 分析技术需要有关过程设计和操作的详细资料，因此它总是在详细设计阶段过程中或详细设计阶段完成之后用该方法对过程的危险与操作性问题进行分析，在化学工业实际应用中有多种 HAZOP 分析方法。

HAZOP 分析，是由各学科组成的分析组运用创造性的、系统的方法识别由于偏离过程设计要求（称为偏差）而引起的危险与操作性问题，这些危险与操作性问题可能导致不希望的后果。有经验的分析组的组织者将使用一些固定词组（称为“引导词”或“关键词”），引导分析组系统地对装置的设计进行分析，将这些引导词应用于装置设计的特定单元或分析节点，并与设计的工艺参数组合起来识别那些与装置的设计和操作规程不符的偏差。

例如，引导词“空白（NONE）”与工艺参数“流体流动”组合起来就构成偏差“无流体流动”。一般地，作为分析组的组织者应使用安全检查表或对过程的经验，为分析组提供在 HAZOP 分析会议上必须讨论的偏差项目。然后分析组对引起偏差的原因（如：操作人员关闭泵的出口阀门）、偏差的后果（如：泵过热）、为防止这种偏差所使用的安全装置进行讨论。如果原因和后果比较重要，而且安全装置也不适当，则分析组应当提出相应的措施提供给管理人员考虑。某些情况下，分析组分析到了某种偏差的原因，但不知道将产生什么样的后果，此