

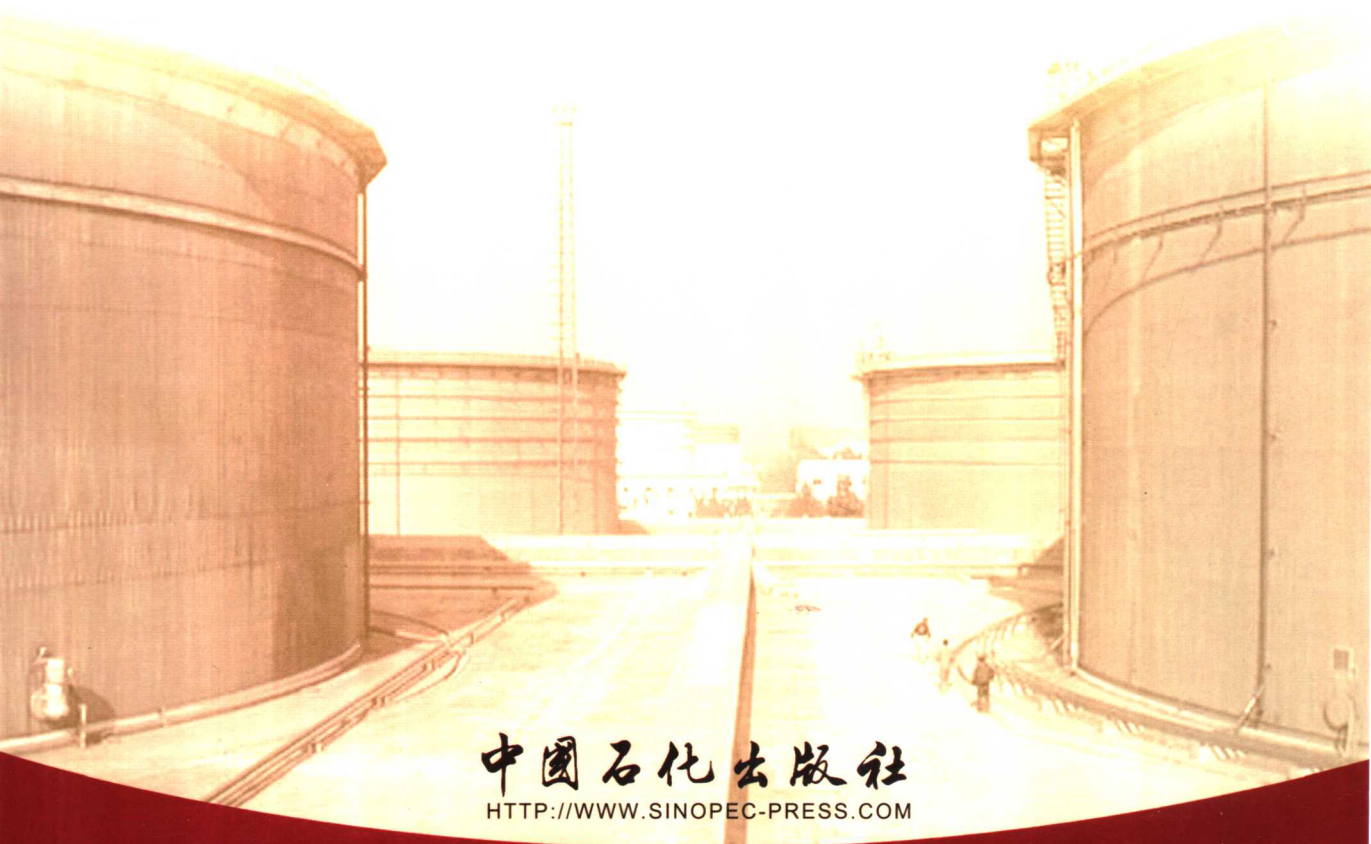


油库安全丛书

油库安全系统工程

OIL DEPOT SAFETY SYSTEM ENGINEERING

母元江 王 丰 编著



中国石化出版社
[HTTP://WWW.SINOPEC-PRESS.COM](http://www.sinopec-press.com)

油库安全丛书

油库安全系统工程

母元江 王 丰 编著

中国石化出版社

内 容 提 要

本书是油库安全丛书之一,内容主要包括事故致因理论、事件树分析、事故树分析、油库安全检查表、作业条件危险性分析、预先危险性分析、故障类型及影响分析、危险和可操作性研究、原因—结果分析、管理疏忽与危险树、安全目标管理、故障假设分析、安全决策、油库安全防护评估与决策系统等内容。

本书力求将安全系统工程理论和方法应用于油库安全管理工作之中,为油库安全科学化管理寻求新的方法,与油库实践结合紧密,内容系统,通俗易懂,可操作性强,具有较高的实用价值,可作为油库业务培训教材和参考书,也可作为大中专院校相关专业的参考书。

图书在版编目(CIP)数据

油库安全系统工程/母元江,王丰编著.
—北京:中国石化出版社,2006
(油库安全丛书)
ISBN 978-7-80229-178-2

I.油… II.①母… ②王… III.油库-安全管理-系统工程 IV.TE972

中国版本图书馆 CIP 数据核字(2006)第 107736 号

中国石化出版社出版发行

地址:北京市东城区安定门外大街 58 号

邮编:100011 电话:(010)84271850

读者服务部电话:(010)84289974

<http://www.sinopec-press.com>

E-mail:press@sinopec.com.cn

北京精美实华图文制作中心排版

北京大地印刷厂印刷

全国各地新华书店经销

*

787×1092 毫米 16 开本 14.5 印张 353 千字

2007 年 1 月第 1 版 2007 年 1 月第 1 次印刷

定价:36.00 元

前 言

安全是油库生产活动得以正常进行的重要条件。我国现代化建设正处在新世纪、新时代，国民经济迅猛发展，对石油产品的需求量与日俱增，油库数量和油品储备量的大幅度增加，油库呈现大型化趋势，油库运行过程中人、物 and 环境的危险因素引发的油品火灾爆炸事故的概率也相应增大，特别是大型油库，一旦发生火灾爆炸，就会造成惨重的人员伤亡和巨大的财产损失。多次重大油库事故给人们带来一次次惨痛的教训，不断就油库安全问题向人们敲响警钟。因此，如何建设本质安全型油库，如何安全有效地对油库进行管理和维护，如何保证油库的安全运营，已成为当前油品储运系统面临的艰巨任务。

随着科学技术的迅速发展，人们更加重视油库事故的预防工作，油库安全系统工程思想逐步形成和完善。油库安全系统工程是应用安全科学和系统工程的原理与方法，分析、评价油库生产系统与过程中的危险有害因素，采取预防与控制措施，防止重大事故的发生。近年来，油库安全系统工程的研究得到了快速发展，系统安全的思想和方法改变了传统安全技术与管理工作的思路，通过对油库系统或过程固有危险和潜在危险的早期预测与分析评价，可以有效地防止或减少事故的发生。本书是对近年来油库安全系统工程研究成果的科学总结，详细介绍了事故致因理论、事件树分析、事故树分析、油库安全检查表、作业条件危险性分析、预先危险性分析、故障类型及影响分析、危险和可操作性研究、原因—结果分析、管理疏忽与危险树、安全目标管理、故障假设分析、安全决策、油库安全防护评估与决策系统等内容，并力求将安全系统工程理论和方法应用于油库安全管理工作中，为油库安全科学化管理寻求新的方法。本书与油库管理实践结合紧密，内容系统，通俗易懂，可操作性强，具有较高的实用价值，可作为油库业务培训教材和参考书，也可作为院校相关专业的参考书。

本书由成都军区 38 分部军交运输油料处母元江处长和解放军后勤工程学院王丰教授编著，后勤工程学院龙军讲师、冯剑讲师和杜振华副教授参加了部分内容的编写。在本书编写过程中参阅和研究了许多资料，主要参考文献列于书后，在此一并对这些作者表示感谢。由于作者水平所限，书中难免存在不妥之处，欢迎读者批评指正。

编著者

目 录

第一章 概述	(1)
第一节 系统及系统工程	(1)
第二节 安全系统工程及其发展过程	(2)
第三节 油库安全系统工程的研究对象和内容	(7)
第四节 油库系统安全因素分析	(10)
第五节 油库事故模型	(12)
第六节 油库安全分析方法选择	(15)
第二章 事故致因理论	(22)
第一节 概述	(22)
第二节 事故因果论	(24)
第三节 能量转移理论	(28)
第四节 人失误的事故模型	(31)
第五节 轨迹交叉理论	(39)
第六节 动态变化理论	(42)
第七节 根据事故致因理论如何预防事故	(44)
第八节 油库事故致因机理分析	(48)
第三章 事件树分析	(50)
第一节 事件树分析的作用及程序	(50)
第二节 事件树分析的方法及特点	(51)
第三节 事件树分析步骤	(53)
第四节 油库应用实例分析	(53)
第四章 事故树分析	(57)
第一节 概述	(57)
第二节 事故树的符号及意义	(58)
第三节 事故树分析方法	(59)
第四节 事故树定性分析	(63)
第五节 事故树定量分析	(72)
第六节 油库应用实例分析	(73)
第五章 安全检查表	(84)
第一节 概述	(84)
第二节 安全检查形式	(85)

第三节	油库安全检查的内容与方法	(86)
第四节	油库安全检查表的编制	(87)
第五节	油库安全检查的组织实施	(88)
第六节	用安全检查表进行危险性评价	(89)
第七节	油库安全检查表实例	(91)
第六章	作业条件危险性分析	(106)
第一节	基本原理及评价步骤	(106)
第二节	赋分标准	(106)
第三节	图解法	(108)
第四节	油库应用实例分析	(108)
第七章	预先危险性分析	(112)
第一节	概述	(112)
第二节	危险性的辨识	(112)
第三节	预先危险性分析步骤	(116)
第四节	危险性控制	(117)
第五节	油库应用实例分析	(118)
第八章	故障类型和影响分析	(128)
第一节	概述	(128)
第二节	FMEA 方法及步骤	(129)
第三节	致命度分析	(131)
第九章	危险和可操作性研究	(134)
第一节	概述	(134)
第二节	危险和可操作性研究的目标及基本概念	(134)
第三节	危险和可操作性研究的分析步骤及程序	(138)
第四节	油库应用实例分析	(139)
第十章	原因—结果分析	(143)
第一节	原因—结果分析方法	(143)
第二节	油库应用实例分析	(144)
第十一章	管理疏忽和危险树	(146)
第一节	MORT 的产生与发展	(146)
第二节	MORT 的基本原理	(147)
第三节	MORT 的结构	(148)

第十二章 安全目标管理	(152)
第一节 目标管理	(152)
第二节 安全目标管理原理	(157)
第十三章 故障假设分析	(166)
第一节 概述	(166)
第二节 What-If 法分析步骤	(166)
第十四章 安全决策	(169)
第一节 决策概述	(169)
第二节 安全决策程序	(170)
第三节 安全决策的方法	(172)
第四节 油库安全决策实例分析	(178)
第十五章 油库安全防护评估与决策系统	(184)
第一节 绪论	(184)
第二节 油库安全评估理论及其模型的建立	(186)
第三节 油库安全防护与决策系统评估指标体系的建立	(197)
第四节 油库安全防护评估系统数据的处理方法	(205)
第五节 油库安全防护评估与决策系统的软件集成	(212)
参考文献	(223)

第一章 概述

系统科学的产生与应用,促使人们用一个全新的观念来解决生产中的安全问题,即从系统的概念出发,用系统的思想方法来考察和解决生产中的安全问题。因此,20世纪60年代迅速发展起一门新兴学科——安全系统工程,它是以系统工程的方法研究、解决生产过程中安全问题的工程技术。

第一节 系统及系统工程

一、系统

系统广泛应用于生产和生活的各个领域。对它有多种解释,在古希腊语中,它是有条理、有秩序地放在一起的意思。韦氏大词典称系统为“有组织或被组织化的整体,由有规则的相互作用、相互依存的形式组成的诸要素的集合”。国际标准化组织技术委员会称系统为能完成一组特定功能的,由人、机器以及各种方法构成的有机集合体。钱学森描述系统的概念时说,极其复杂的研究对象称为系统,即由相互作用和相互依赖的若干组成部分结合成的具有特定功能的有机整体,而且这个系统本身又是它所从属的更大系统的组成部分。总之,系统是由相互作用、相互依赖的若干组成部分结合而成的具有特殊功能的有机整体。描绘一个系统应包括以下四部分内容:系统元素;元素间的关系;边界条件;输入及输出的能量、物料、信息等。

系统按形式划分为:自然系统、人工系统和复合系统。按结构复杂程度划分为:简单系统和复杂系统。

为了实现系统自身的正常运行和功能,系统需要以一定的方式构成,应具有保持和传递能量、物质和信息的特征。系统种类繁多,根据控制论观点,可由三部分组成,即输入、处理和输出,如图1-1所示。任何系统都具有输出某种产物的功能,而且一定是先有输入,再经处理,才能得到输出。可见,输出是处理的结果,代表着系统的目的。处理是使输入变为输出的一种活动,通常由人和设备分别完成或联合承担。比如汽车制造厂生产汽车是由入口输入了原材料,经过加工和作业,进行整体装配,这就相当于处理部分,装配好的汽车再由出口输出。这种以物质流动为主的系统称为生产系统。一项计划也可视为输入,经过执行,即处理阶段,最后得到了结果,就是输出。这种以信息流为主的系统称为管理系统。系统处理后的结果,不一定是理想的,这就需要验证和修正计划,改善执行环节来达到预期的目的。这在系统上称为反馈。

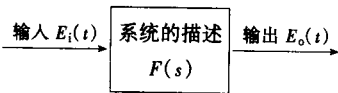


图 1-1 系统构成示意图

一般来说,系统具有四个属性。

(1) 整体性。系统至少由两个或两个以上的要素(元件或子系统)组成。组成系统的各个元素虽然具有不同的性能,但它们是根据整体要求按照一定方式构成的一个具有特定功能的集合体,因而系统不是各要素性能的简单相加。组成系统的各个要素并不都很完善,但它们

可以综合、统一成为具有良好功能的系统。反之，即使每个元素是良好的，而构成整体后并不具备某种良好的功能，也不能称之为完善的系统。

(2) 相关性。系统内部要素之间是有机联系和相互制约的，而且这种依赖关系具有一定的规律性。例如，一台计算机就是由主板、电源、CPU、硬盘、软驱、键盘、显示器等硬件通过特定的关系，有机地结合在一起所形成的一个系统。

(3) 目的性。任何一个系统，不论其大小都具有特定的功能，没有目的的系统是不存在的。特别是人类创造的系统，总是为了实现某一目的而设计、制造出来的。

(4) 环境适应性。任何一个系统都存在于一定的环境之中，因此它必然要与周围环境发生物质、能量和信息的交换，以适应外部环境的变化。在研究系统的时候，环境往往起着重要的作用，必须予以重视。适者生存就是这个道理。

二、工程

工程是指服务于特定目的的各项工作的总体。例如机械工程、电力工程、电子工程、土木工程、化工工程、计算机工程、宇航工程、环境工程、安全系统工程等。我们这里讲的工程具有更广泛的意义，不仅指与物质、能量等有关的工作，而且包括信息处理、人的行为、心理研究等各个方面。

三、系统工程

系统工程是近几十年来发展起来的一门有关组织管理技术的新兴科学。系统工程是指为了更好地达到系统目标，而对系统的构成要素、组织结构、信息流动和控制结构等进行分析与设计的技术。简言之：以系统为研究对象的工程。钱学森称为组织管理技术。

系统工程就是从系统的观点出发，跨学科地考虑问题，运用工程的方法去研究和解决各种系统问题。具体地说，就是运用系统分析理论，对系统的规划、研究、设计、制造、试验和使用等各个阶段进行有效的组织管理。它科学地规划和组织人力、物力、财力，通过最佳方案的选择，使系统在各种约束条件下，达到最合理、最经济、最有效的预期目标。它着眼于整体的状态和过程，而不拘泥于局部的、个别的部分。这是因为系统工程采用了新的方法论，这种方法论的基础就是系统分析的观点，即一种“由上而下”、“由总而细”的方法。它不着眼于个别单元的性能是否优良，而是要求巧妙地利用单元间或子系统之间的相互配合与联系，来优化整个系统的性能，使其从整体上成为技术先进、经济合算、运行可靠、时间节省的实际可行的系统。

第二节 安全系统工程及其发展过程

一、与安全有关的基本术语

1. 安全

安全是指客观事物的危险程度能够为人们普遍接受的状态。人们从事的某项活动或某系统，即某一客观事物，是否安全，是人们对这一事物的主观评价。当人们均衡利害关系，认为该事物的危险程度可以接受时，则这种事物的状态是安全的，否则就是危险的。万事万物都存在着危险因素，不存在危险因素的事物几乎是没有什么的，只不过危险因素有大有小，有轻有重而已。有的危险因素导致事故的可能性很小，有的则很大；有的引发事故后果非常严重，有的则可以忽略。因此，我们从事任何活动或操作任何系统，都有不同的危险程度。

人们常把危险程度分为高、中、低三个档次。发生事故可能性大且后果严重的为高危险程度；一般情况为中等危险程度；发生事故可能性小且事故后果不严重者为低危险程度。当客观事物状态处于高危险程度时，人们是不能接受的，是危险的；处于中等危险程度和低危险程度时，人们往往是可以接受的，则这种状态是安全的。中等以上的危险程度称危险范围，中等及其以下危险程度为安全范围。

2. 危害

危害是指可能带来人员伤害、疾病、财产损失或作业环境破坏的根源或状态。危害也可理解为危险源或事故隐患。从本质上讲，就是存在能量、有害物质和能量、有害物质失去控制而导致的意外释放或有害物质的泄漏、散发这两方面危害因素。对于危害因素的分类方法有多种，如按事故的直接原因进行分类，则可根据 GB/T 13816—92《生产过程中的危险、危害因素》分为六类：物理性、化学性、生物性、心理生理性、行为性及其他危害因素。此外，也可根据事故类别、职业病类别进行分类。

3. 危险

危险是一种状态，它可以引起人身伤亡、设备破坏或降低完成预定功能的能力。当存在危险性时，就存在产生这些不良影响的可能性。

4. 危险性

危险性表示危险的相对暴露。可能存在危险，但由于采取了预防措施，危险性可能不大。例如高压变压器组，只要通了电，就有使人触电死亡的固有危险性。如果这个变压器组不加防护，放在人员比较集中的地方，就有高度危险性。

5. 事故

事故是指造成主观上不希望出现的结果意外发生的事件，分为死亡、疾病、伤害、财产损失或其他损失共五大类。这里所说的疾病包括职业病和与工作有关的疾病。

6. 风险

特定危害性事件发生的可能性与后果的结合就称为风险。

风险可认为是潜在的伤害，可能致伤、致命、中毒、设备或财产等损害。风险具有两个特性，即可能性和严重性。如果其中任一个不存在，则认为这种风险不存在。如电击风险，如果能保证在有电击可能性的地方，不许人员进入，就可认为这个风险是不存在的。风险性可按其严重程度进行分类，对系统的风险性应进行风险评价。

7. 职业病

职业病是指企业、事业单位和个体经济组织的劳动者在职业活动中，因接触粉尘、放射性物质和其他有毒、有害物质等因素而引起的疾病。

职业病的分类和目录由国务院卫生行政部门会同国务院劳动保障行政部门规定、调整并公布。

8. 风险评价

评价风险程度并确定其是否在可承受范围的全过程，即称为风险评价，也称为危险度评价或安全评价。如果风险分析过程中发现系统中存在风险性，就必须估价它在系统运行中的可承受性，即评价其严重程度或可能性，以确认其是否在可承受的范围。

9. 危害辨识

识别危害的存在并确定其性质的过程，称为危害辨识。危害辨识就是确定危害的存在和

性质, 辨识时应识别出危害因素的种类与分布、伤害(危害)的方式、途径和性质。对于用人单位来说, 应辨识的主要部位为厂址、厂区平面布局、建筑物、生产工艺过程、生产机械设备、有害作业部位(粉尘、毒物、噪声、振动、辐射、高温、低温等)和管理设施、事故应急救援设施及辅助生产生活卫生设施等。

10. 危险因素、有害因素和事故隐患

在生产过程中存在着各种与人的安全与健康息息相关的因素, 其中, 能对人造成伤亡或对物造成突发性损坏的因素称为危险因素; 能影响人的身体健康, 导致疾病, 或对物造成慢性损坏的因素, 称为有害因素; 事故隐患泛指现存系统中可导致事故发生的物的危险状态、人的不安全行为及管理上的缺陷。通常, 通过检查、分析可以发现和察觉它们的存在。事故隐患在本质上属于危险、有害因素的一部分。

11. 系统安全

在生产过程中, 导致事故发生的原因是很多的, 必须从系统的观点出发, 运用系统的方法去分析、评价和消除系统中的危险, 消除产生事故的根源, 才能实现系统的安全。所谓系统安全, 是指在系统使用期限内, 应用安全科学的原理和方法, 分析并排除系统要素的缺陷及可能导致灾害的潜在危险, 使系统在整个寿命周期内保持最佳安全状态。

12. 劳动保护

劳动保护是指依靠技术进步和科学管理, 采取技术措施和组织措施, 来消除劳动过程中危及人身安全和健康的不良条件和行为, 防止伤亡事故和职业病危害, 保障劳动者在劳动过程中的安全与健康。劳动保护实际上就是站在政府的立场上, 强调为劳动者提供人身安全与身心健康的保障。

13. 劳动安全健康

劳动安全健康是指以保障职工在劳动过程中的安全与健康为目的的工作领域以及在法律、技术、设备、组织制度和教育等方面所采取的相应措施。劳动安全卫生与职业安全卫生作为同义词使用。

14. 安全信息

安全信息是安全活动所依赖的资源, 是按安全事物在时间和空间定性或定量的表达。安全信息类型分为一次安全信息和二次安全信息。一次安全信息是指生产过程中的人机环境客观安全性; 二次安全信息包括安全法规、条例、政策、安全科学理论、总结、分析报告等。

15. 安全收益

安全收益即安全产出。安全的实现不但能减少或避免人员伤亡和财产损失, 而且能通过维护和保护生产力, 实现促进经济生产增值的功能。由于安全收益具有潜伏性、间接性、延长性、迟效性等特点, 因此研究安全收益是安全经济的重要课题之一。

16. 安全目标管理

安全目标管理就是在一定时期内(通常为一年), 根据企业经营管理的总目标, 从上到下地确定安全工作目标, 并为达到这一目标制定一系列对策措施, 开展一系列的组织、协调、指导、激励和控制活动。

17. 职业安全健康管理体系

职业安全健康管理体系(occupational safety and health standard management system, OSHMS)是指为建立职业安全健康方针和目标并实现这些目标所制定的一系列相互联系或相互作用的

要素管理体系。其运行模式按戴明模型，具体包括：计划（PLAN）、行动（DO）、检查（CHECK）、改进（ACT）等四个相关联的环节。

18. 绩效测量

绩效测量是 OSHMS 中的一个基本术语，是指用人单位根据职业安全健康方针、目标，在控制和消除职业安全健康风险方面所取得的可测量的结果，也可以说，绩效测量是职业安全健康管理活动和结果的测量。绩效测量可分为主动测量和被动测量两种。绩效是职业安全健康管理运行的结果与成效，是根据安全健康方针、目标、指标的要求控制危险危害因素得到的。因此，绩效可用各单位的安全健康方针、目标及指标的实现度来描述，并可具体体现在某一或某类危险危害因素的控制上。

19. 可承受风险

可承受的风险是 OSHMS 中的一个基本术语，是指根据用人单位的法律义务和职业安全健康方针，已将危害性事件发生的可能性与后果降至可接受的程度。风险一般是不能转化为安全的，但可以减小风险的可能性或严重性或者两者均减小来降低风险的程度。

20. “三同时”原则

我国劳动法第五章第 53 条规定的劳动安全卫生设施必须符合国家规定的标准，并要求遵循“三同时”原则，即，“新建、改建、扩建工程的劳动安全卫生设施必须与主体工程同时设计、同时施工、同时投入生产和使用”。

21. “三不放过”原则

国务院第 34 号令规定：伤亡事故应在 90 日内结案；特殊情况下不超过 180 日；必须采取“三不放过”原则：原因分析不清，不放过；责任者和职工没有受到教育，不放过；没有防范措施，不放过。

22. 系统安全

系统安全，是指在系统运行周期内，应用系统安全管理及安全工程原理，识别系统中的危险性并排除危险，或使危险减至最小，从而使系统在操作效率、使用期限和投资费用的约束条件下达到最佳安全状态。简言之，系统安全就是系统在一定的功能、时间和费用的约束条件下，使系统中人员和设备遭受的伤害和损失为最少。也可这样说，系统安全是一个系统的最佳安全状态。

要达到系统安全，就必须在系统的规划、研究、设计、制造、试验和使用等各个阶段，正确实施系统安全管理和安全工程。人们在运用系统时，总是希望在人力、物力、财力和时间等约束条件下，所设计的系统具有最佳工作状态，如最佳性能、最大可靠性、最小重量和最大期望寿命等。寻求这种最佳效果的愿望，几乎渗透于产品的规划、研究、设计、制造、运行等各个阶段，这就需要应用优化理论。

要使系统能达到安全的最佳状态，应满足：①在能实现系统安全目标的前提下，系统的结构尽可能简单、可靠；②配合操作和维修用的指令数目最少；③任何一个部分出现故障，保证不导致整个系统运行中止或人员伤亡；④备有显示事故来源的检测装置或警报装置；⑤备有安全可靠的自动保护装置并制定行之有效的应急措施。

23. 安全系统工程

安全系统工程是应用系统工程的原理与方法，识别、分析、评价、排除和控制系统中的各种危险，对工艺过程、设备、生产周期和资金等因素进行分析评价和综合处理，使系统可

能发生的事故得到控制,并使系统安全性达到最佳状态。简单地说,安全系统工程就是用系统工程的知识、方法和手段解决生产中的安全问题。它的最终目的是消除危险,保证人身财产安全。由于安全系统工程是从根本上和整体上来考虑安全问题,因而它是解决安全问题的具有战略性的措施。为安全工作者提供了一个既能对系统发生事故的可能性进行预测,又可对安全性进行定性、定量评价的方法,从而为有关决策人员提供决策依据,并据此采取相应安全措施。

安全系统工程的理论基础除了有系统论、控制论、信息论、运筹学、优化理论等外,还有如预测技术、可靠性工程、人机工程、行为科学、工程心理学、职业卫生学、劳动保护法规、法律以及相关的各工程学等多门学科和技术。

二、安全系统工程发展概况

自从有了人类社会以后,安全与健康就成了人类社会关心的问题。作为人类最基本的需求,安全伴随着人类经济生活水平的不断提高越来越受到人们的重视。

安全系统工程是现代科学技术发展的产物。它的发展是与军事工程、尖端技术的迫切需要紧密相连的。1957年,前苏联发射了第一颗人造地球卫星,在全世界引起了很大反响。美国为了和前苏联争夺空间优势,匆忙地进行导弹技术的开发,实行所谓研究、设计、施工齐头并进的方法。由于对系统的可靠性和安全性研究不足,在一年半的时间里,在导弹的地下储藏库和发射基地连续发生了四次重大事故,每次都造成数百万美元的损失,最后不得不全部报废,从头做起。这一惨痛教训,使这些国家逐渐认识到系统安全的重要性。1961年,美国贝尔实验室在系统安全的基础上创造了事故树分析方法,促成了美国民兵式导弹的研制。美国空军以系统工程的方法研究导弹系统的可靠性和安全性,于1962年提出了“导弹火箭系统安全工程学”,继而制定了“武器系统安全标准”。这为后来发射多弹头火箭的成功创造了条件。1966年美国国防部采用了空军的安全标准,制定了“MIL-S-38130”。1967年7月又发表了安全系统工程计划标准 MIL-STIL882。在这个标准中,首次奠定了安全系统的概念,以及设计、分析、综合等基本原则。

1965年,美国波音公司和华盛顿大学在西雅图召开安全系统工程专门学术讨论会议,以波音公司为中心对航空工业开展安全性、可靠性和设计的研究,在导弹和超音速飞机的安全性评价方面取得了很好的效果。但是,美国航空航天局对这种方法不够重视,以致造成1967年发生了三名阿波罗宇航员被烧死的事故。英国以原子能公司为中心,从20世纪60年代中期开始收集有关核电站故障的数据,对系统的安全性和可靠性问题采用了概率评价方法,后来进一步推动了定量评价的工作,并设立了系统可靠性服务所和可靠性数据库。

1972年,美国三里岛核电站发生了泄漏事故,引起了公众的恐慌和指责。美国原子能委员会组织了以麻省理工学院拉斯姆逊教授为首的14名专家,用了两年多的时间,耗资300多万美元,对核电站的危险性进行了研究和评价。1974年,美国原子能委员会发表了拉斯姆逊报告,称作“拉氏报告”,即 WASH-1400。报告收集了核电站各部位历年发生的故障及其概率,采用了事件树和事故树的分析方法,做出了核电站的安全性评价。该报告的发表,对世界各国影响很大,促进了安全系统工程的发展。

日本引进安全系统工程的方法虽然较晚,但发展很快,已在电子、宇航、航空、铁路、公路、原子能、汽车、化工、冶金等工业领域大力开展了研究与应用。

当前,安全系统工程已引起了各国普遍重视,曾多次召开过安全系统工程的学术会议,

出版了许多学术刊物和专著。国际安全系统工程学会每两年举办一次学术年会,1983 年在美国休斯敦召开的第六次会议,有 40 多个国家参加,讨论的议题涉及国民经济各个行业。可以看出,这门学科正得到越来越广泛的应用,并起到了越来越大的作用。

我国从 20 世纪 70 年代末期开始研究安全系统工程及其应用。1982 年北京市劳动保护研究所召开了安全系统工程座谈会,由研究单位、大专院校和重点企业等部门同志参加。会上交流了国内开展研究和应用的情况,探讨了在我国发展安全系统工程的方向,并组织分工进行事故危险性预先分析、故障类型和影响分析、事件树分析和事故树分析等分析方法的研究,同时开展了安全检查表的推广应用工作。研究如何长期进行学术交流等,这次会议为我国开展安全系统工程的研究与应用打下了良好的基础。

1985 年,中国“劳动保护管理科学专业委员会”成立,在会上建立了“系统安全学组”,该学组以安全系统工程为中心,进行开发研究和推广应用等活动,为安全系统工程学科的发展和推进安全管理做出了贡献。

我国各产业部门、地方劳动局和工业部门在所属企业,积极推广应用安全系统工程的活动,并取得了较好的效果。例如天津市原机械局于 1988 年贯彻《机械工厂安全性评价标准(试行)》,当年在行业内部就取得无一人死亡的成绩。这是天津市机械行业历史上从未有过的大事。根据原劳动部 1996 年第 3 号令,规定今后“三同时”审查,应有“安全评价”的内容。另外全国几十所高等院校增设了安全工程专业。这些都为普及和推广安全系统工程知识,推进现代安全管理创造了有利条件,同时也为创造出适合我国国情的安全系统工程打下了良好的基础。

经过几十年的发展,目前安全系统工程在冶金、煤炭、化工、交通、能源、航空航天等部门得到了广泛应用。我国成立了中国安全科学学会、中国劳动保护学会、安全系统工程学会等学术机构,有多种含有安全系统工程内容的学术期刊,几十种安全系统工程的专著,有几十所高等院校设有安全工程专业,开设了安全系统工程课程。安全检查表、预先危险性分析、事件树分析、事故树分析等安全分析方法和安全评价技术得到了普遍应用,计算机也应用于安全系统工程,可用于事故统计分析、事故树分析、安全预测、安全评价、安全专家系统、安全数据库的建立和安全管理信息系统等方面。

第三节 油库安全系统工程的研究对象和内容

一、油库安全系统工程

油库是由多个部门、多类人员、多种设备设施和物资组成一个互相关联的有机整体,具备了构成系统的基本要素。从影响油库安全的诸多因素分析中抓住其主要矛盾,用安全系统工程的方法和理论,建立油库安全系统并实施有效的管理,对提高油库系统安全性是十分重要的。

油库安全系统工程是采用系统工程的原理与方法,识别、分析、预测、评估油库系统中的危险性或事故,据此采取技术和管理等各种措施或对策,从而使油库系统可能发生的故事得到控制,并使油库安全性达到最佳状态。

油库安全系统工程的方法与安全工程方法相比,主要的差别就是两者的出发点和工作方法不同。两种安全管理工作方法的基本过程如图 1-2 所示。油库安全系统工程的方法

法主要是从系统的内部出发去发现和解决油库存在的安全问题。

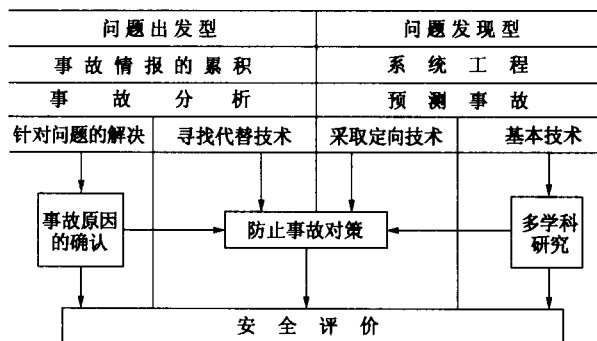


图 1-2 两种安全工作方法的基本过程

油库安全系统工程作为一种科学的安全管理方法体系，改变了以往凭直观经验和事后处理的被动局面，具有以下优点：

(1) 预测和预防事故的发生，是现代安全管理的中心任务。运用系统安全分析方法，可以识别油库系统中存在的薄弱环节和可能导致事故发生条件，而且通过定量分析，预测事故发生的可能性和事故后果的严重性，从而可以采取相应的措施，预防事故发生。

(2) 油库系统日趋复杂，各子系统、各作业、各环节之间相互联系、相互制约。通过系统分析方法，全面地、系统地、彼此联系地以及预防性地处理油库系统中的安全性，而不是孤立地、就事论事地解决油库系统中安全性问题。

(3) 对安全进行定量分析、评价和优化技术，为油库安全管理事故预测提供了科学依据，根据分析可以选择出最佳方案，使各子系统之间达到最佳配合，用最少投资得到最佳的安全效果，从而可以大幅度地减少燃烧爆炸、人身伤亡和设备损坏等事故。

(4) 油库安全系统工程要作出定性和定量的安全评价，就需要有各项标准和数据。如许可安全值、故障率、人机工程标准以及安全设计标准等。因此，油库安全系统工程可以促进各项标准的制定和有关可靠性数据的收集。

(5) 通过油库安全系统工程的开发和应用，可以迅速提高安全技术人员、操作人员和管理人员的业务水平和系统分析能力，同时为油库管理工作提供了一套完整的参考资料。

二、油库安全系统工程的研究对象

油库安全系统工程作为一门科学的安全管理方法，有它本身的研究对象。在油库生产活动中，始终存在着安全与危险这一对矛盾，油库安全系统工程的基本任务就是要解决这一对矛盾，促使矛盾向安全方面转化。油库生产系统主要包括三部分，即从事油库生产活动的操作人员和管理人员，油库储存的油料等物资和生产必须具备的设备设施等各种物质条件，以及油库生产活动所处的环境。这三个部分构成了一个“人—物—环境”系统，每一部分是其中的一个子系统，称之为“人子系统”、“物子系统”和“环境子系统”。这也正是油库安全系统工程的研究对象。

人子系统，涉及到人的生理因素和心理因素，以及规章制度、规程等如何适合人的特性、易于为人们所接受的问题。不仅把人看作“生物人”、“经济人”，而且也是“社会人”，必须从安全心理学、行为科学等方面科学地解决这些问题，以充分发挥人的主观能动性。

物子系统,不仅要考虑油库工艺设计、油库设备可靠性、油库安全设施等各方面考虑其安全性,而且要考虑设备设施操作对人提出来的要求,以及从人体学、生理学、心理学研究人在正常作业条件下,人体参数、结构特点、运动特点、心理与生理过程等有关参数对设备设施的设计提出要求。

环境子系统,主要包括环境的物化因素和社会因素。物化因素主要有噪声、振动、有毒气体、光、温度、湿度、压力、热、化学有害物质等;社会因素有管理制度、班组结构、人际关系等。

在“人—物—环境”系统中,这三个子系统相互联系、相互制约、相互影响,构成了一个有机的整体。油库安全系统工程就是从系统思想出发,研究“人—机—环境”系统,提高其整体的安全功能。

三、油库安全系统工程的内容

油库安全系统工程是以预测和防止事故为中心,以检查、测定和评价事故为重点,按照安全分析、安全评价和安全对策三个基本程序展开工作。

1. 安全分析

为了保证油库系统的安全,必须仔细地寻找可能引起油库系统发生事故的潜在危险因素,确定导致危险的各个事件的发生条件及相互关系,观察各种危险因素之间的数量关系及其变化规律,估计事故发生的概率和可能产生伤害及损失的严重程度,以充分认识油库系统中的危险性。系统安全分析是油库安全系统工程的核心,分析结果的正确与否,关系到整个安全工作的成败。可见,系统安全分析在油库安全系统工程中占有十分重要地位。根据实际需要和油库系统完善的不同程度,可以把分析进行到不同深度,可以是初步的或详细的,定性的或定量的,每种深度都可以得出相应的结论,来满足不同项目、不同情况的要求。当前系统安全分析的方法有几十种,它们从各种不同的角度对系统的安全性进行分析。每一种系统安全分析方法都有其产生的历史背景和适用条件,所以并不能处处都通用。要完成一个准确的分析需要综合使用多种分析方法,取长补短,有时还要相互比较,看哪些方法和实际情况更为吻合。因此,应当熟悉各种分析方法的内容和长处,用起来才能得心应手。通过实践,比较实用的系统安全分析方法主要有安全检查表、预先危险性分析、故障类型和影响分析、事件树分析、事故树分析和因果分析等。

2. 安全性评价

系统安全评价是对系统的危险性进行定性和定量分析,得出系统发生危险的可能性及其程度的评价,以寻求最低事故率、最小的损失和最优的安全投资效益。安全评价分为定性安全评价和定量安全评价两大类,包括对油料、设备设施、作业流程、人—物—环境系统等的安全评价。其主要内容包括确定系统的评价方法、评价指标和安全标准;评价系统的各种潜在危险,并把它减少到允许的范围之内;当引进新材料、新技术、新设备或改变工艺流程时,要使危险减少到最少;参照类似系统的事故例证,预防类似事故的重复发生;当系统在技术和经济上难以或不可能达到预期效果时,应对计划或设计进行修改,反复评价,直到达到安全标准。定性安全评价通过定性分析油库系统中的危险性,能揭示油库系统中的危险因素并对危险性进行重要程度的分类。定性安全评价比起用传统安全方法来,已经系统和准确多了。只有经过定量的评价才能充分发挥安全系统工程的作用。决策者可以根据评价的结果选择技术路线,上级业务部门可以根据评价结果督促油库改进安全状况。当安全评价的结果

表明需要改进系统的安全状况时,就必须采取安全措施,减少危险因素及其发生概率,重新进行安全评价,直到达到安全要求。安全评价的方法很多,如油库安全度评价法、火灾爆炸危险评价法、可靠性评价法、模糊综合评价法等。

3. 安全对策

根据安全性评价的结果,可以对系统进行调整甚至修改设计,以消除和控制系统中的危险有害因素,提高系统的安全性。安全措施主要有两个方面:一是预防事故发生的措施,即在事故发生之前采取适当的安全措施,排除危险因素,避免事故发生;二是控制事故损失扩大的措施,即在事故发生之后采取补救措施,避免事故继续扩大,使损失减到最小。具体措施有增设安全防护装置,改进工艺过程或修改设计,改善作业环境,加强安全教育和管理等方面。

第四节 油库系统安全因素分析

分析油库系统安全,必须知道影响油库安全的主要因素。这些因素中,凡可能导致人员伤亡和物质损失而形成事故的因素都称之为危险因素。它是导致油库事故的基础。影响油库系统安全的主要因素包括油料自身的因素、设备设施因素、人的因素、管理因素和环境因素等。

一、油料自身的因素

油料自身的危险性决定于本身的组成以及它的物理、化学性质。如易挥发、易流失、易燃烧、易爆炸、有毒、不导电等。油料的这些特性一方面是其造福人类的基础,另一方面它也危及自身及油库系统的安全。

就油料本身而言,不同油料其易燃、易爆、易挥发、易流失等性能也不相同。汽油和重油虽然都是易燃物资,但是两者能量转换的程度和速度不同,汽油与重油相比,汽油闪点低,更容易燃烧,因此有更大的危险性。轻油除了易燃、易爆的特性外,挥发性、流动性也高于其他油料。

物质条件的危险性随着物质条件的存在而存在,随着物质条件的变化而变化。一瓶汽油敞开放置经过一段时间之后,其轻质组分逐渐减少,挥发性降低,其燃烧、爆炸性也随之改变。物资的危险还与危险物资转化所能释放的能量有关。一瓶汽油、一桶汽油、一罐汽油,显然后者一旦发生事故危险性更大。汽油、煤油、柴油、润滑油、润滑脂其能量转化的条件各不相同,同样多的油料燃烧释放的能量也不尽相同。

物资危险性转化为事故是有条件的,是具有可控性的。混合气过稀、过浓、缺氧、缺火源时都不会燃烧、爆炸。因此可以采取隔离火源、密封储存、监测油气浓度、及时通风等控制措施,防止事故发生。油流产生静电若控制流速、减少水杂、做好接地、加防静电添加剂都可以减少静电的产生和积聚。对油料自身危险性的可控性没有一个清醒的认识,是得不到安全管理的主动权的。

二、设备、设施的因素

设备、设施是完成任务的物质手段。如果设备、设施齐全,技术状况良好,位置适当,就具备了完成任务的物质条件。如果设备、设施不全,质量低劣,位置不当,任务就难以完成,而且有酿成事故的可能。设备、设施影响油库安全主要表现在对设备设施建造的可靠性