安全系统工程·课堂知识手册

09 月 08 日

课程定位与重要性

- 安全系统工程是安全工程专业的核心课程
- 作为专业基础课，与其他课程同等重要，平时要求和考试要求严格
- 大多数高校研究生招生仍以安全系统工程为考试科目
- 课程基于教材进行，考试主要考查教材内容

学科发展背景



- 早期由张铁林等老师编写安全系统工程教材，侧重矿山等传统工业领域
- 随经济社会发展，安全人才需求扩展至多个领域：机械电器、交通、建筑、过程工业、森林、景区等
- 现阶段强调韧性城市建设，体现安全工程的新发展方向

基本概念辨析

- 需要区分”工程安全”“工程系统”“系统工程”“安全系统”“安全工程”等相关概念
- 掌握基本概念的内涵与外延是学好课程的基础
- 基本概念延伸至技术、管理、人机管理、文化等多个领域

> **定义**
>
> 安全系统工程：从系统观点出发，运用工程方法和技术，防止事故发生、预防安全危害的学科

系统观点的核心理念

- 将班级、组织视为系统，个人是子系统
- 子系统状态良好，整体系统才能保持最佳状态
- 若某子系统出现问题，系统平衡被打破
- 具有韧性的系统能迅速调整并恢复新的平衡

定义

韧性：系统在灾害来袭时，在可承受范围内仍能正常运行，或能迅速适应和恢复的能力

事故处理的两种方向

- **问题出发型**：事故已发生后，汲取教训并预防再次发生（后果找原因）
  - 典型做法：四不放过原则
  - 例如：天津 812、江苏响水 321 等重特大事故后，同类作业停止并进行分析论证

注意

问题出发型虽有借鉴意义，但不是理想状态——我们不希望事故发生后再进行分析

- **问题发现型**：从系统内外联系分析薄弱环节，预防事故发生（主动防御）
  - 识别可能存在的危险或有害因素
  - 采取相应防控措施

例

自动喷淋系统：感温感烟传感器 → 视频监控 → 自动启动喷淋，形成自动灭火系统

系统安全管理的投入产出平衡

- 现代安全标准相对较高，风险阈值设置较低
- 需要相应的人力物力投入以保证风险降低
- 目标：通过系统工程方法找到薄弱环节，采取对策，达到最佳投入、最佳产出、最佳安全的状态

例

个人财务管理：当收入增加时，分散投资于基金、银行存款、零钱通等，比全部投入单一渠道风险更低、收益更优化

系统思维方式应用

- 从系统角度考虑问题，不仅涉及个人，还涉及家庭、事业发展、择业方向等
- 核心原则：能够接受自己所有决定带来的风险、机遇和挑战
- 在不断调整中维持平衡和安全

文明发展与安全需求的演进



- **原始文明阶段**：生产能力低、生活匮乏，抵御自然能力弱（狩猎阶段）
- **农业文明阶段**：出现古代文明（古埃及、古巴比伦、古希腊罗马、中华文明等），中华文明传承至今并发展光辉
- 现代社会在经济技术演进中，对安全系统工程人才的需求日益增加

新业态与安全挑战

- 低空经济成为新兴领域，对应设立新专业
- 外卖配送、电单车等新业态中的安全隐患仍需重视
- 新业态的出现意味着新问题会不断出现，需要专门机构、法规、监督教育

> **注意**
>
> 从事特种特殊行业的工作人员往往因谨小慎微而安全做得更好，而疏忽反而易导致极端情况

工业发展阶段与自动化替人的现实困境

- 机械化、自动化目标：减人、机械化换人、智慧化无人
- 现状瓶颈：机械需要人操作，无法完全替代人工
- 智能装配工地现阶段局限：
  - 柔性不足，边角工作仍需人工
  - 建筑工程仍大量采用人手工施工
  - 虽配备重型机械，但智能化水平未达预期

智慧建筑的技术挑战

- 装配式、绿色建筑特点：零碳排放、组装化
- 存在的主要问题：
  - 楼层限制（通常不超 5-20 层）
  - 材料耐久性存疑（能否维持数十年）
  - 防渗漏难题：接缝处需用泡沫材料、密封胶粘合填充

> **注意**
>
> 密封胶寿命有限，渗漏问题（特别是卫生间）是智慧建筑的技术难点，直接影响居住质量

后工业文明与服务经济的安全需求

- 经济形态：从制造向服务型经济转变
- 第三产业范畴：金融、投资、融资、股市等
- 数字技术需求：互联网、数字经济、数字货币依赖强大的安全保障
- 新兴机遇：各行业都需要专业安全技术人才投入

新能源产业的安全风险

例

汽车行业从传统燃油向新能源转变，衍生出新的安全需求：

- 电池安全（锂电池等）
- 氢能燃料电池：氢气压力达 35 兆帕（350 公斤），极高危险性
- 加氢站基础设施安全

注意

高压氢气的危险程度类似高压水切割，能穿透人体，需要更高层次的安全技术支撑

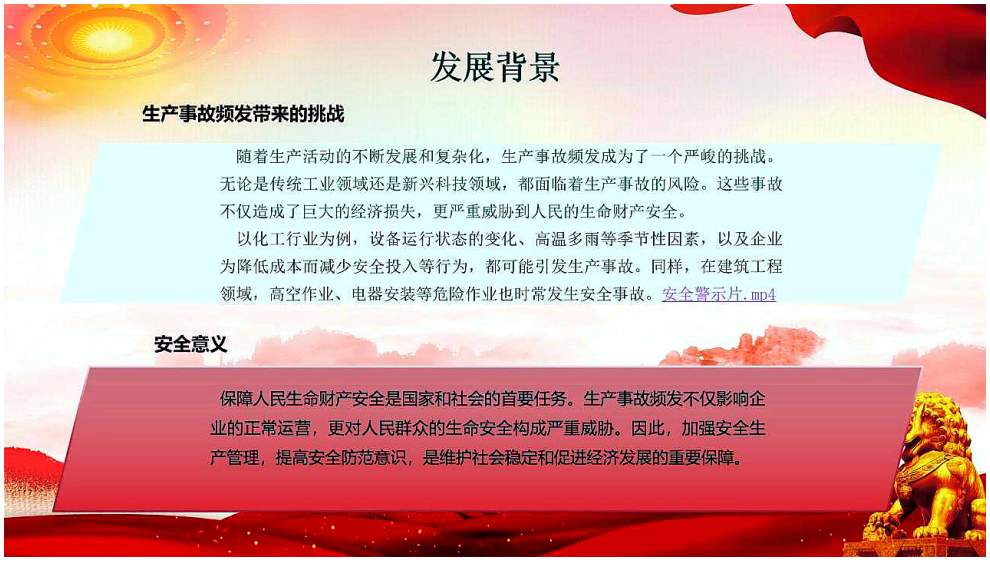
低空经济的发展与安全挑战

- 广州试点：花城广场珠江边的低空经济基地建设
- 应用场景：无人机、无人艇、无人驾驶，用于快递配送等
- 发展现状：相比深圳应用速度仍有差距

工业 4.0 时代的安全地位

- 安全技术是根本基础，其他发展无法进行
- 自动化设备出现时的误区：错以为安全工作会降低，实则需要更专业的人才
- 竞争现实：激烈的市场环保要求企业不断进步，安全专业人员需求增加

生产事故与经济损失的现实



- 事故频发带来严峻挑战
- 2019 年全国情况：虽实现三个连续下降，但隐患仍多
- 经济损失标准变化：
  - 过去：20 万左右的损失较高

- 现在：单次人身伤亡可能导致 200 万级损失

定义

生命价值提升 = 经济发展进步的表现，反映社会对人员安全的重视程度上升

雇主对员工生命安全的重视

- 原因：经济损失成本高企
- 管理方式：不能仅靠硬性管理，需结合软技术、软管理
- 行业规范：有些行业规定发生死亡案例时，片区总经理或负责人必须立即停止作业

自然灾害与隐患认识不足

- 广东频发多发自然灾害（如山体滑坡）
- 土壤液化现象：堆积土壤在特定条件下可流动，能量巨大
- 案例：深圳 1120 事故——建筑废弃物堆高引发坍塌，导致房屋被埋

注意

传统居住地虽然代代相传，但面临的自然灾害风险已改变，不能凭祖传经验判断安全

新业态与信息安全的多维挑战

- 挑战来源：经济社会发展产生的意想不到的风险
- 信息安全：手机链接随意点击可能导致费用被盗
- 系统角度：需从全方位考虑安全问题

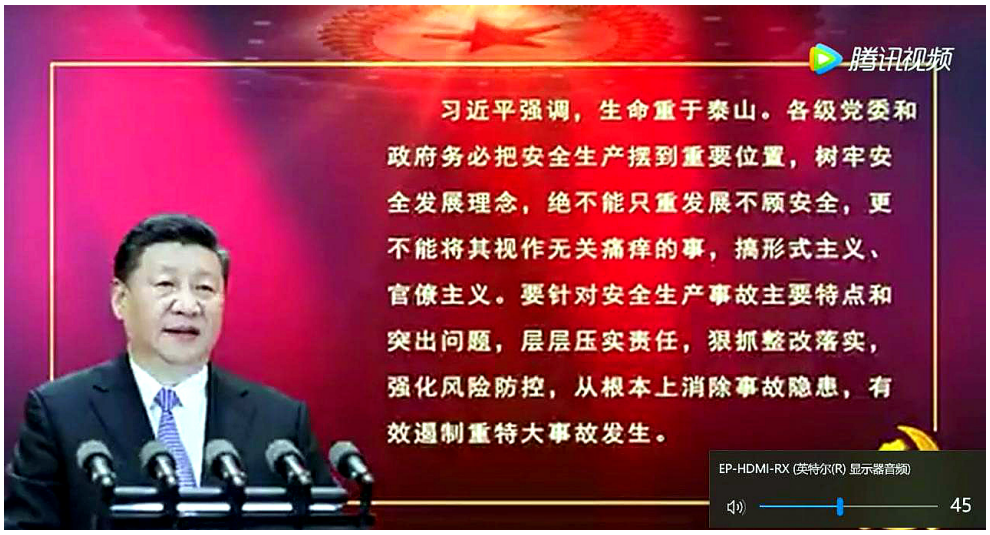
习近平总书记安全生产重要论述的核心理念

定义

核心理念框架：树牢安全发展理念、强化底线思维和红线意识、坚持问题导向、目标导向、结果导向

- 思想深邃、内涵丰富
- 系统回答：如何认识安全生产、如何做好安全生产工作
- 是经验教训的科学总结和行动指南

安全发展的不可逾越红线



定义

人命关天的红线：发展绝不能以牺牲人的生命为代价

- 2013 年 6 月 6 日提出此原则
- 体现：生命价值优先于经济发展

安全生产责任制体系



- 三级监管体系：
  - 行业主管部门直接监管
  - 安全监管部门综合监管
  - 地方政府属地监管
- 三个必须原则：管行业必须管安全、管业务必须管安全、管生产必须管安全
- 四责制：党政同责、一岗双责、齐抓共管、失职追责

注意

不履行安全责任的干部会被追责，这是前所未有的严格要求

领导干部的安全责任态度



- 要求：经常临事而惧，具有负责任态度
- 警示：当官不能潇洒，需有睡不着觉、半夜惊醒的自觉
- 后果：当官太潇洒就会出事

责任追究的严厉性



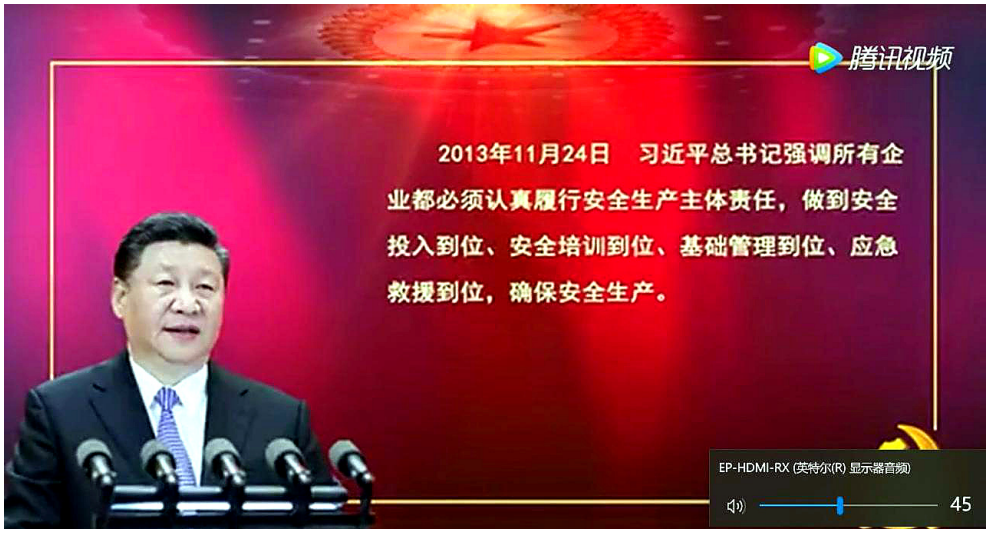
- 对责任单位和责任人要打到疼处、痛处
- 原则：真正痛定思痛、痛改前非
- 不容情：造成重大损失仍拿高薪、高额奖金、分红是不合理的

安全生产的常态要求



- 必须警钟长鸣、常抓不懈
- 丝毫放松都会导致不可挽回的损失
- 2014 年强调：必须建立健全安全生产责任体系，强化企业主体责任

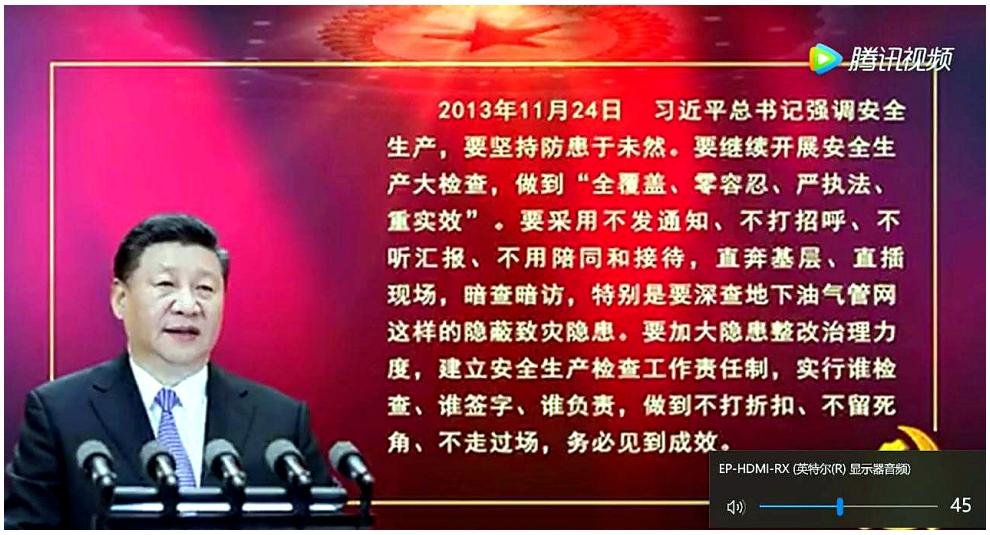
企业主体责任的四到位



定义

企业必须做到四到位：安全投入到位、安全培训到位、基础管理到位、应急救援到位

防患于未然的预防性工作机制



- 原则：坚持防患于未然
- 检查方式：采用”四不”暗查暗访（不发通知、不打招呼、不听汇报、不用陪同接待）
- 重点：深查隐蔽致灾隐患（如地下油气管网）
- 实施标准：全覆盖、零容忍、严执法、重实效
- 整改原则：不打折扣、不留死角、不走过场

> **注意**
>
> 检查工作实行谁检查谁签字谁负责制度，确保见到实效

举一反三与联动示警



- 工作机制：“一厂出事故万厂受教育，一地有隐患全国受警示”
- 目标：通过共享警示实现全面预防

血的教训与安全生产基础能力建设

- 核心认识：血的教训极其深刻，必须牢记
- 生产单位要求：
  - 强化安全生产第一意识
  - 落实安全生产主体责任

- 加强安全生产基础能力建设
- 坚决遏制重特大安全生产事故

2016 年中央政治局常委会五点要求



一、安全发展与责任制落实

- 必须坚定不移保障安全发展
- 狠抓安全生产责任制落实
- 强化党政同责、一岗双责、失职追责
- 坚持以人为本、以民为本

二、改革创新与监管改进

- 深化改革创新
- 强化开发区、工业园区、港区等功能区安全监管
- 举一反三，在标准制定、体制机制上认真考虑改革和完善

三、依法治理

- 用法治思维和法治手段解决安全生产问题
- 加快安全生产相关法律法规制定修订
- 加强安全生产监管执法
- 强化基层监管力量
- 着力提高安全生产法制化水平

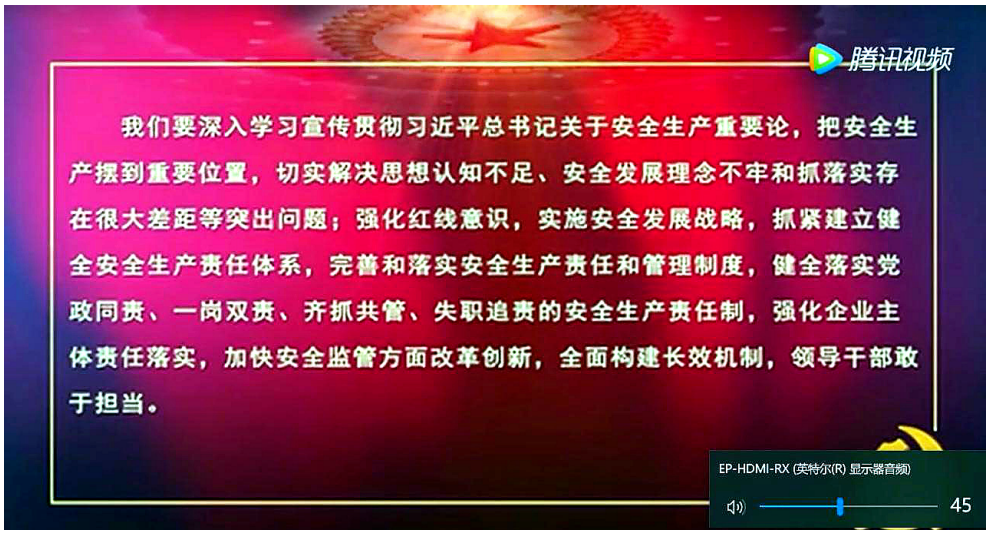
四、遏制重特大事故

- 对易发重特大事故的行业领域采取措施
- 风险分级管控、隐患排查治理双重预防机制
- 推动安全生产关口前移
- 加强应急救援工作
- 最大限度减少人员伤亡和财产损失

五、加强基础建设与安全保障

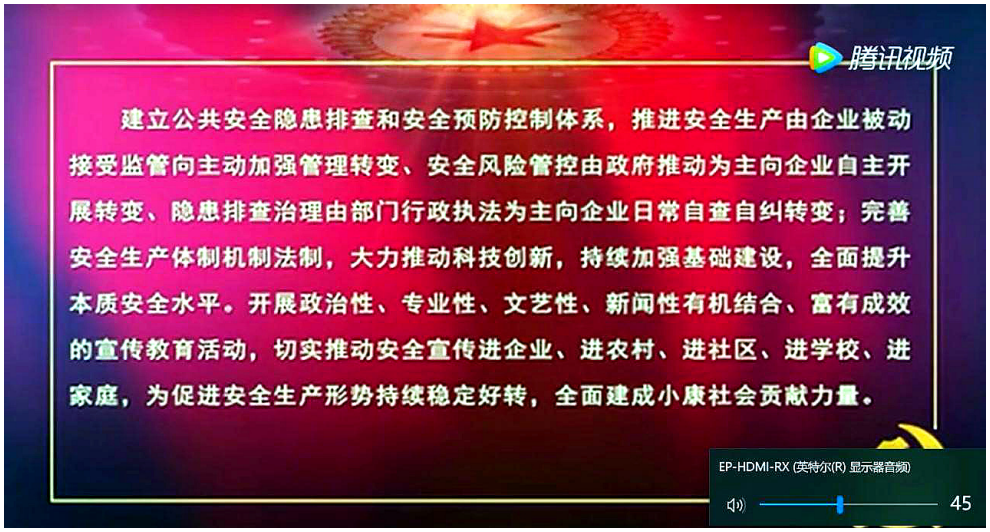
- 重点隐患：城市建设、危旧房屋、玻璃幕墙、渣土堆场、尾矿库、燃气管线、地下管廊
- 重点行业：煤矿、非煤矿山、危化品、烟花爆竹、交通运输
- 大型活动：游乐、跨年夜等群众性活动，严防踩踏事故

安全生产工作的当代方向



- 立足点：解决思想认知不足、安全发展理念不牢、抓落实存在差距问题
- 核心任务：强化红线意识、实施安全发展战略、建立健全安全生产责任体系
- 转变机制：
  - 企业被动接受监管 → 主动加强管理
  - 政府推动为主 → 企业自主开展风险管控
  - 部门行政执法为主 → 企业日常自查自纠

安全生产体系的完善



- 完善内容：体制、机制、法制
- 推动方向：
  - 大力推动科技创新
  - 持续加强基础建设
  - 全面提升本质安全水平

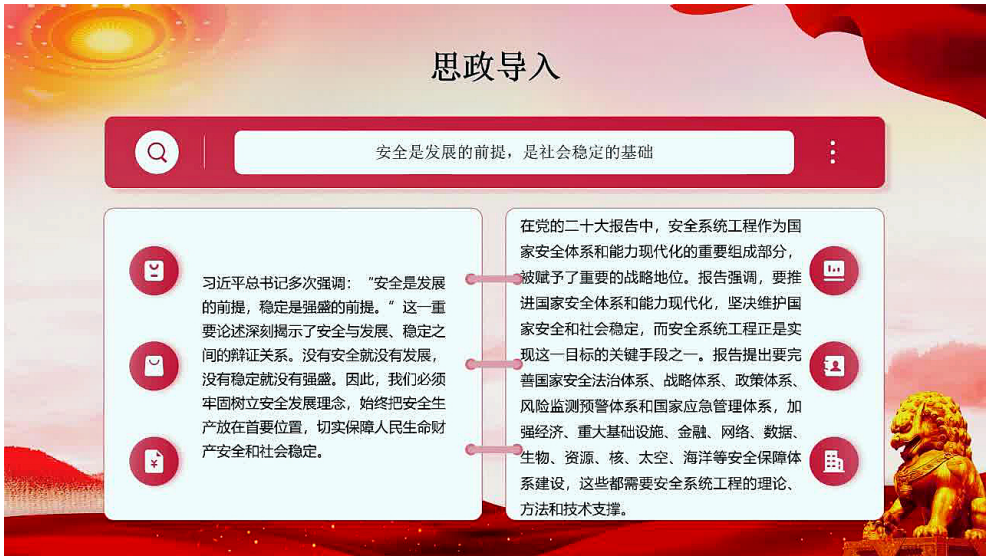
安全宣传教育的五进策略

- 五进内容：进企业、进农村、进社区、进学校、进家庭
- 宣传方式：政治性、专业性、文艺性、新闻性有机结合
- 目标：提升全社会公民的安全素质和安全意识

问题出发性与计划性的平衡

- 问题特征：既具出发性（从已发生问题出发），也具计划性（未发生时的预防态度）
- 态度转变：
  - 已出现问题 → 怎样改进或避免
  - 未出现问题 → 应有什么态度和做法

安全与发展的辩证关系



- 新理念：统筹安全和发展
- 高层次要求：高质量发展，保障高水平的安全
- 体现：安全与发展的相互促进关系
- 加强安全管理、提高安全意识是维护社会稳定和促进经济发展的重要保证
- 安全是发展的前提，稳定是强盛的前提
- 安全、发展、稳定三者构成辩证关系，而非相互对立

定义

系统安全是一个重要的观点和理念，强调用系统工程的整体观念来处理安全问题

日常生活中的安全意识

- 出发点：从校园日常开始培养安全意识
- 基本认识：自己的生命是非常宝贵的

注意

校园内常见安全隐患：

- 骑电摩托不戴安全帽
- 雨天路滑导致车辆刹不住
- 摔落时头部无保护

交通出行与安全选择的权衡

例

行人过马路 vs 司机快速通行的矛盾：
- 稍快一点：出事故风险高
- 稍慢一点：安全通过，平安到家
- 结论：谁轻谁重显而易见

多层面立体化安全宣传

- 宣传范围：不同层面、不同领域
- 投入保障：投入、应急、教育、人员等各方面
- 目标：保证整个系统的安全

专业学生的系统安全观获得

- 最大收获：建立系统的安全观念
- 适用范围：将来不管做什么、学什么都能受用
- 起点：从日常生活、学习开始实践

校园安全案例与警示

- 现象：电摩托骑行不戴安全帽的学生多
- 真实事故：校园内发生过相关事故，全校知晓
- 雨天风险：路面泥泞多、潮湿，自行车刹车失效

注意

车辆刹不住是物理现象，加上无安全帽保护，摔落时头部无异于与铁面碰撞

运动员坚持与伤病的现实

例

羽毛球女单选手陈雨菲世锦赛案例：
- 半决赛：脚踝扭伤 90 度，咬牙获胜
- 决赛：虽用止疼药、打封闭，但韧带实质性断裂
- 结果：虽坚持上场，但体能和竞技力受严重影响

注意

生理伤害无法通过意志力克服，过度坚持可能导致更严重后果

安全的重要性和战略地位

- 保障人民生命财产安全是国家和社会的首要任务
- 总书记反复强调以人为本、人民至上、生命至上
- 领导者必须树立生命财产安全意识，否则不能胜任其职位
- 安全涉及人民生命财产，同时涉及国家的保密信息、经济支柱和核心利益

国家现代化建设中的系统工程

- 二十大报告强调推进国家安全体系和能力现代化
- 系统工程是实现这一目标的关键手段之一
- 报告涵盖的主要体系：国家法制体系、战略体系、政策体系、风险监测预警体

系、国家应急管理体系
- 中国发展快是因为有坚强的领导、有系统的战略和系统的观念

> **注意**
>
> 系统性不是嘴上说的，而是需要在实际行动中体现。发达资本主义国家缺乏系统的整体观念和以人民生命财产为出发点的根本理念

安全系统工程的应用领域

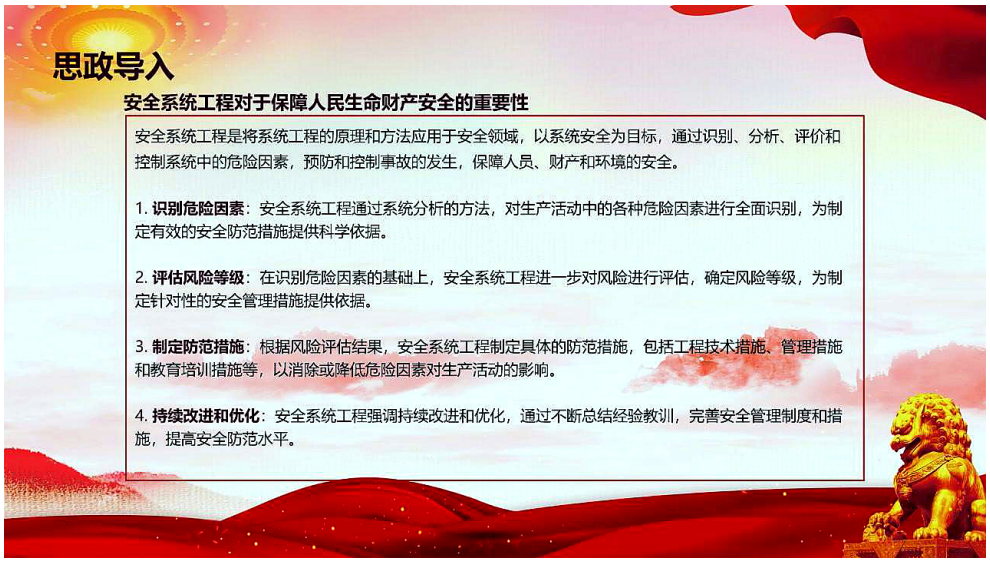
- 经济、重大基础设施、金融、网络、数据、生物资源、太空、海洋等领域
- 需要安全系统工程的理论、方法和技术支撑
- 典型应用案例：港珠澳大桥建设与运营管理

> **例**
>
> 港珠澳大桥在建设期间采用岛屿施工法，通过混凝土预制块在岛上制作，再送入海底隧道沉放。从业人员的奉献精神不可替代，后来港珠澳大桥管理局成立后，将安全咨询机构代理挖角至管理局安全部，说明运营中安全是核心

系统工程方法的核心内容

- 系统工程原理和方法应用于安全领域，以系统安全为目的
- 通过识别、分析、评价和控制系统中的危险因素
- 预防和控制事故发生，保障人员、财产和环境的安全

系统安全工程的四个主要工作阶段



识别危险因素

- 需要有意识地识别有形的、无形的及隐藏在表面背后的隐患
- 要掌握科学的分析方法和相应的技术手段
- 危险识别能力需要通过学习相关技术和知识来获得

> **注意**
>
> 缺乏危险意识往往导致防不胜防的损失。博士生获得奖学金被转账、网购退款诈骗等都是识别不足的表现

评估和监测危险等级

- 识别危险后不能立即杜绝，需要进行监测或监控
- 必须用相匹配的方式和方法对危险程度进行评估
- 根据评估结果确定危险所属的等级
- 不能随意扩大或缩小风险认知

> **例**
>
> 看病时医生用仪器检测，不会因为胳膊轻微不适就做 CT，而是用相匹配的检查方式

制定防范措施

- 在评级基础上制定相应措施
- 措施包括技术方面、管理方面和教育培训方面
- 目的是降低或消除危险因素导致的风险，减少对生产生活的影响

> **注意**
>
> 判断措施是否合理需要充分的依据。仓促决策或过度轻视都是不负责任的态度

持续改进和优化

- 不断总结经验、改进措施、提升管理水平
- 融入企业文化和安全文化建设
- 企业文化与安全文化一脉相承

安全投入的必要性和可接受风险

- 某些行业（如自来水生产）必须进行安全投入
- 液氯消毒杀菌技术的发展历程：从残留氯导致植物枯死，到现代工艺消除残留，反映了技术进步
- 自来水爆管风险是可接受的（浪费水），但燃气或油管爆管风险不可接受

> **例**
>
> 学校几十年前铺设的自来水管已超过设计寿命，虽然经常爆管，但因其内容物为水，属于可接受风险。而对于燃气管道，爆管风险则不可接受

安全文化示范企业建设

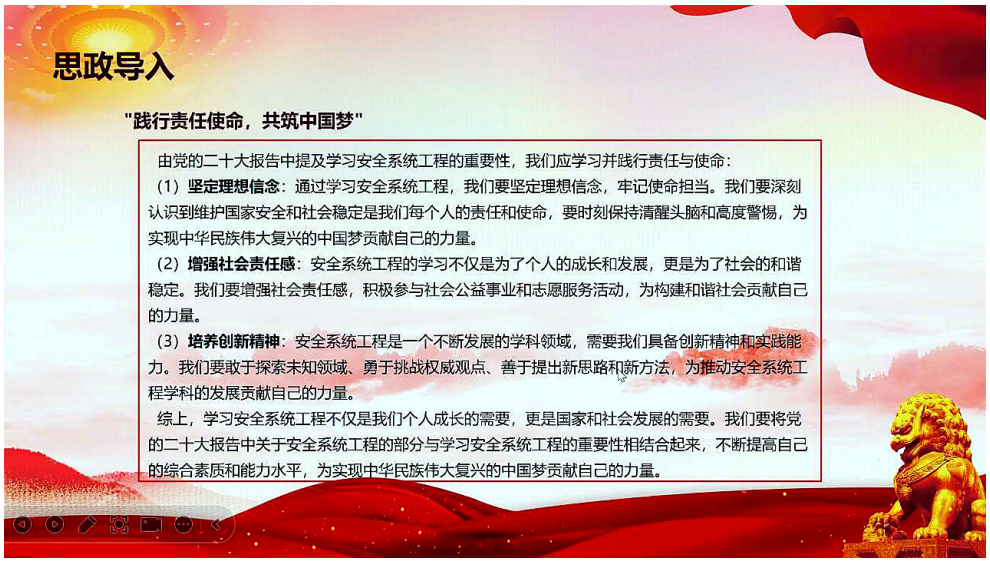
- 安全文化与企业文化相互促进、一脉相承
- 通过安全文化示范企业建设资格的多为能源企业
- 典型企业：粤电集团、供电局、发电厂、燃气厂等

> **例**
>
> 广州供电局在自然灾害后 4 小时内恢复供电需要技术、人员和装备支撑。其下属电建企业还支援海南、广西、澳门等地的应急保障工作

系统安全工程的作用

- 系统安全工程能够发挥重要的作用前提是：熟悉、会用、能在实践中应用
- 需要深入细致地理解系统安全工程的原理和方法
- 切切实实地保障人民生命财产安全

责任使命和中国梦



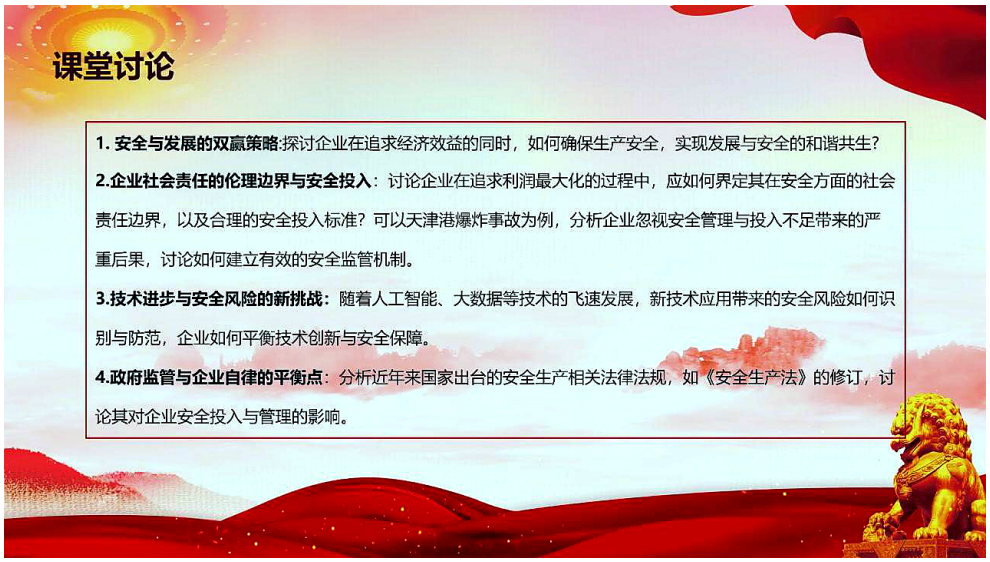
- 为实现中华民族伟大复兴贡献力量不是嘴上说说，而是实实在在的行动
- 需要践行责任和使命，而非仅停留于心理层面
- 学以致用，学习后确实能够奉献社会

> 例
>
> 中山大学博士后从华为年薪上百万的工作入伍，成为舰长，体现了学以致用的实际行动

系统安全工程学习的指导原则（二十大精神）

- 坚定理想信念，牢记使命、担当，时时刻刻保持清醒头脑
- 责任使命重大：如行业审批部门的决策直接影响企业命运和投资者利益
- 社会责任感：企业应参与公益、志愿服务，带动社区、医院、农村、学校等方面的安全进步
- 创新精神：不因危险而束手束脚，要客观应用定性定量方法探索创新，抓住机遇迎接挑战

安全与发展的双赢策略



- 安全与发展是双赢关系，而非此消彼长

- 在追求经济效益的同时重视安全，才能实现持续长久发展
- 需要在两者间找到平衡点

例

广州原液氯生产企业因周边城市化进程快，拿不到生产许可证而关闭。液氯虽然是剧毒物质但必需用于自来水消毒和供港，但当生产地周边全是居民和江边高层建筑时，风险无法控制，最终被迫停产。这反映了安全与发展需要科学平衡

注意

以前认为乡下土路、郊区的地方会因为城市发展而改变。五山地区从五十多年前的乡间小路发展为现代城区，说明任何地方都面临发展变化，原有的风险评估需要随之调整

经济社会发展与安全的平衡

- 经济社会发展迅速，如广州塔 15 年内发展，城市基础设施从农田到现代化
- 保障安全与经济发展形成和谐共生关系
- 安全发展是双赢局面，提升生活水平、幸福感和获得感

液氯生产的高危险性与风险管理

- 液氯通过电解食盐水生产，工艺简单但风险极高
- 核心风险：液氯泄露可能导致爆炸
- 安全措施演进：从早期放空处理 → 氨冷却液化 → 回收利用
- 液氯是国民经济不可或缺的杀菌剂，用于自来水处理

例

重庆天元化工厂电话线路爆炸事故

东阳光电化厂的选址与安全合规案例

- 第一厂选址：投产不到半年因不符合国家标准被政府要求关闭
  - 投资约 1 亿元
  - 违反安全距离标准：距居民区仅 800 米 ~1 公里，不符合要求
- 省应急局给予约 1 年试生产期限，要求搬迁
- 地方政府支持：在更远处提供便宜地块
- 重新选址后：企业扩大产业链，形成上下游一体化经营

注意

即使投入大、利润高的企业，也必须严格遵守安全距离标准，不能因经济效益而妥协

自来水杀菌处理工艺

- 氯气是最有效的通用杀菌方式，杀死所有微生物
- 后续处理：酸碱中和 → 过滤、沉降、分离（均为物理过程）

卫生与经济社会发展的相辅相成

- 自动化卫生设施普及（自动马桶、洗手设施）反映社会发展水平
- 分餐制与公共卫生指导提升整体卫生水平
- 卫生意识提升减少对消毒工具的依赖

企业社会责任与安全投入的关系

- 早期：粗放式发展，牺牲环保、劳动力、资源
- 现阶段：招商引资设立门槛，优先选择世界 500 强企业
- 世界 500 强企业特点：追求利润同时重视社会安全，加大安全投入

例

韩国 ABS 塑料企业，安全负责人年薪 200 万，体现安全投入的重要性和人才价值

违规安全管理的法律后果

注意

天津港 8 月 12 日爆炸事故：领导因电话指示安全评价专家出具虚假符合报告而被刑事处罚，造成 100 多人死亡

- 不能因为压力、利益而突破安全红线
- 一旦触犯法律，面临严重刑事后果

定义

安全的能力边界：不能超越法律法规和国家标准，任何人的指示也不能作为突破底线的理由

廉洁自律的重要性

- 任何形式的利益接受（打牌费用等）都会被追究
- 高层领导问责同样无法规避
- 个人风险：短期获利，长期陷入被动境地

例

广东省某事故造成 121 人死亡，相关领导因接受费用被查处，遗体无法找回

技术进步与安全的新挑战

- 新业态、新技术需要安全人才平衡创新与风险
- 核心问题：技术创新与安全保障的协调

政府监管与企业自律的原则

- 依法依规履职尽责
- 标准达不到时需要领导签名确认，但风险需要多人分担而非单人承担
- 所有工作都存在风险和压力，需要在可控范围内规范运作

注意

安全管理的闭环：法律法规 → 设计许可、选址 → 办证发证 → 遵守法规 → 若违反需按法规追责

系统的基本概念



定义

系统是由多个相互作用、相互依赖的元素或子系统组成，以一定方式结合，具有特定功能、结构有序，并向环境显示整体特性的有机整体

例

班级系统：由多个同学（元素）组成，通过班长、班委等结构组织，具有教学功能，可向外界显示整体特性

系统的主要属性

- 整体性：具有有机整体的性质
- 相关性：由若干相互作用、相互依赖的部分组成
- 目的性：完成相应功能，目的明确
- 有序性：结构不能杂乱无章，否则系统稳定性被破坏
- 环境适应性：与环境进行能量、物质交换，调整自己实现稳定

系统的多维度构成

- 物理结构维度
- 信息流动维度（如班级群信息传递）
- 能量交换与转换维度（如参加竞赛）
- 物质交换维度（如购置物资）

注意

系统概念内涵丰富，不仅体现物理结构，更包含信息、能量、物质的多维交互

系统工程的定义



> **定义**
>
> 系统工程是从系统整体出发，跨学科地运用科学方法和技术手段，对系统的构成要素、组织结构、信息流动、反馈机制等进行全面分析和综合设计，实现系统最优化的工程学科

- 强调整体性、综合性、最优化思想
- 解决复杂系统在设计、开发、运行、管理过程中的各种问题

系统工程的基本原理

系统性原理

- 系统由多个子系统组成，同时与外界发生横向联系
- 达到现代化管理优化目标需要运用系统方法进行充分分析和优化

> **例**
>
> 人体系统：具有 8 个子系统，同时与外界环境互动

反馈原理

- 在执行过程中获取灵敏、正确、有力的反馈
- 反馈机制：指挥中心发出指令 → 执行机构执行 → 反馈信息 → 与预期对比 → 识别偏差 → 再输入控制
- 本质是控制的科学理念

整分合原理

- 高效率管理必须进行整体规划、明确分工、有效综合
- 三个阶段：整体规划 → 明确分工 → 综合协调

其他原理

- 弹性原理：任何情况下保持一定弹性
- 封闭原理
- 能级原理
- 动力原理
- 激励原理（主要为正激励：奖励与精神鼓励）

系统工程的主要方法

工程逻辑方法

- 涉及布尔代数、关系代数、决策研究、数学函数
- 将逻辑学与哲学思维方法系统应用

工程分析方法

- 运用物质能量守恒、动量守恒等基本理论
- 系统有步骤地解决各类工程问题
- 涉及大量数学物理方法

统计理论与概率论

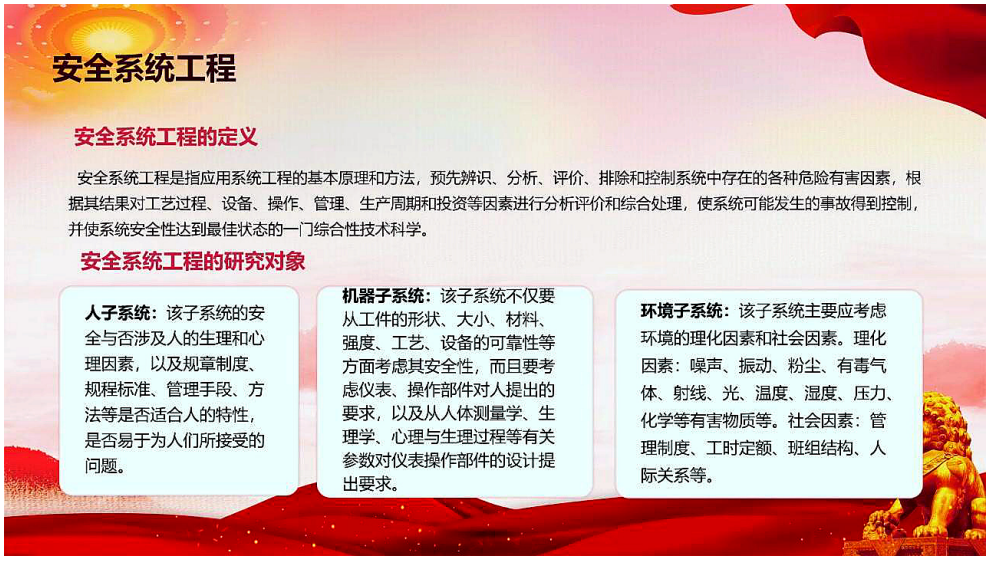
- 应对不确定性问题
- 不确定性包括两个方面：
  - 随机性不确定性（概率论处理）
  - 模糊性不确定性

> **注意**
>
> 客观世界本质上是不确定的，唯一能确定的就是世界的不确定性

运筹学

- 由华罗庚的优选方法和钱学森等大科学家建立和发展

安全系统工程的定义



> **定义**
>
> 安全系统工程是用系统工程的基本原理、方法来辨识、分析、评价、排除、控制系统中存在的各种危险有害因素，对工艺、设备、操作、管理、生产周期、投资进行综合分析、评价和处理，使系统可能发生的事故得到控制，系统安全性达到最佳状态的综合性科学技术

安全系统工程的研究对象

- 人子系统（生理和心理特征）
- 机器子系统（形状、大小、材料、强度、工艺、可靠性）
- 环境子系统（理化因素和社会因素）

注意

三个子系统相互交叉、相互影响、相互作用

人机环系统的相互影响



- 理化因素 → 影响机器寿命、精度甚至损坏
- 机器 → 产生噪音、振动影响人和环境
- 人 → 心理因素引起误操作
- 环境社会因素 → 影响人的心理状态

环境因素对人的影响

- 噪声：长期导致听力损害，影响生理心理
- 振动：经常接触对身体造成影响
- 粉尘：导致尘肺病，可能引发粉尘爆炸

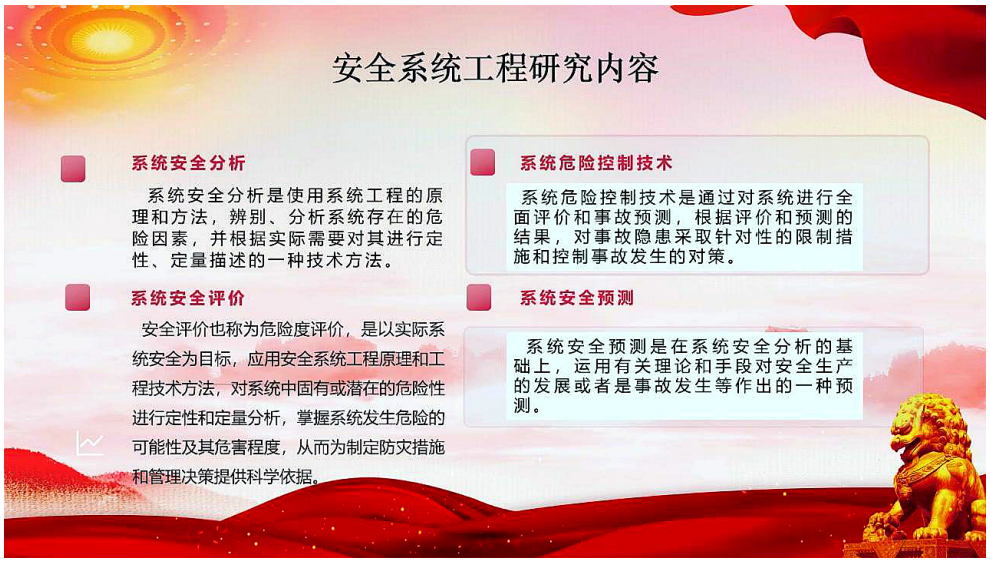
组织与人的管理模型

定义

2X4 管理模型：涉及组织和人的两个维度，每个维度包含 4 个方面

- 强调组织结构与人的心理行为两者同等重要

安全系统工程的主要内容



- 系统安全分析（辨识、分析）
- 系统安全评价（定性定量评价）
- 系统危险控制（采取技术对策与管理措施）
- 系统安全预测（分析基础上预测发展态势）

> **注意**
>
> 评价需要找到潜在危险有害因素，判断发生程度、可能性和危害程度

安全系统工程的研究方法

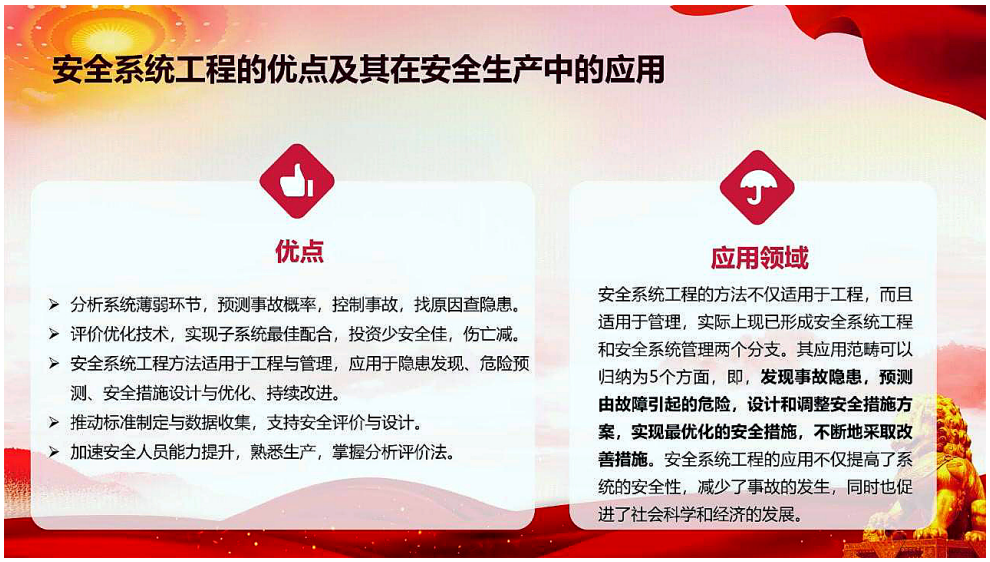
- 系统整体出发的研究方法（系统论、系统观）
- 本质安全方法：追求危险源接近零的理想状态（实际难以完全实现）
- 人机匹配：人易操作、机器易被人操作、环境相匹配
- 安全经济：追求最优投入、最佳产出、最佳安全状态的平衡

> **注意**
>
> 安全投入不是越多越好，而是要在最优产出与最佳安全状态间寻找平衡点

系统安全管理方法

- 贯穿安全规划、设计、检查、控制全过程
- “从摇篮到坟墓”的全生命周期管理

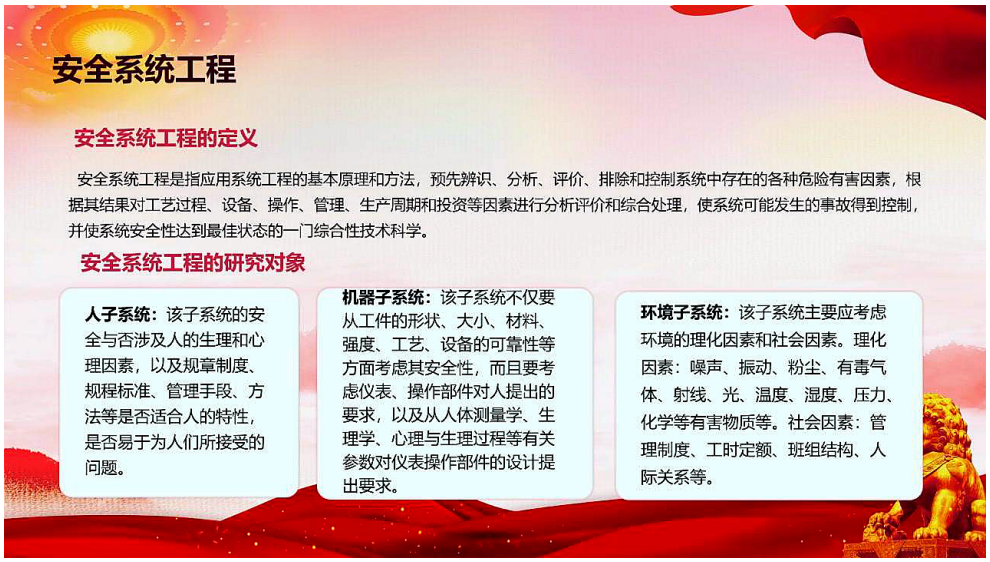
安全系统工程的优点



- 分析薄弱环节，找到”水桶最矮的板”
- 预测事故概率
- 评价和优化技术，实现子系统最佳配合
- 投资最少化同时确保安全
- 发现隐患、危险，进行优化和持续改进
- 推进标准制定与数据收集
- 加强安全人员能力提升
- 定期更新企业管理制度，进行员工培训和宣传教育

09 月 15 日

安全与风险的概念



- 安全与风险是两个不同但相辅相成的概念，安全评价与风险评估在本质上相似，但侧重点不同
- 风险评估不仅关注安全状况，还关注事故发生的可能性、事故后果的严重程度，以及采取措施后对风险的控制与降低
- 风险评估最早在国外产生，21 世纪后逐渐普及
- 从系统工程角度看，安全系统工程的核心流程是：分析 → 辨识 → 评价 → 提出

策略与控制措施

- 安全系统工程与风险评估在某种情况下可互换使用，有时称”安全评价”，有时称”风险评估”

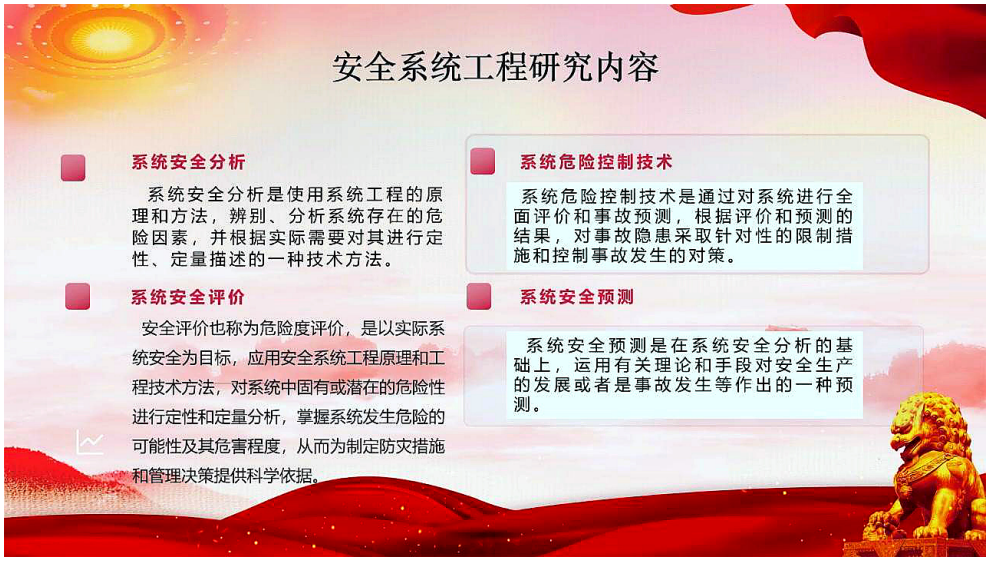
定义

安全系统工程：运用系统工程的方法，对系统进行安全分析、辨识、评价，并提出相应的策略和控制措施，以实现系统安全。

注意

安全与风险不是同一概念。安全是系统处于可接受风险的状态，而风险是事故发生的可能性与后果严重程度的综合度量。安全是目标，风险是度量对象。

安全系统工程的研究对象与内容

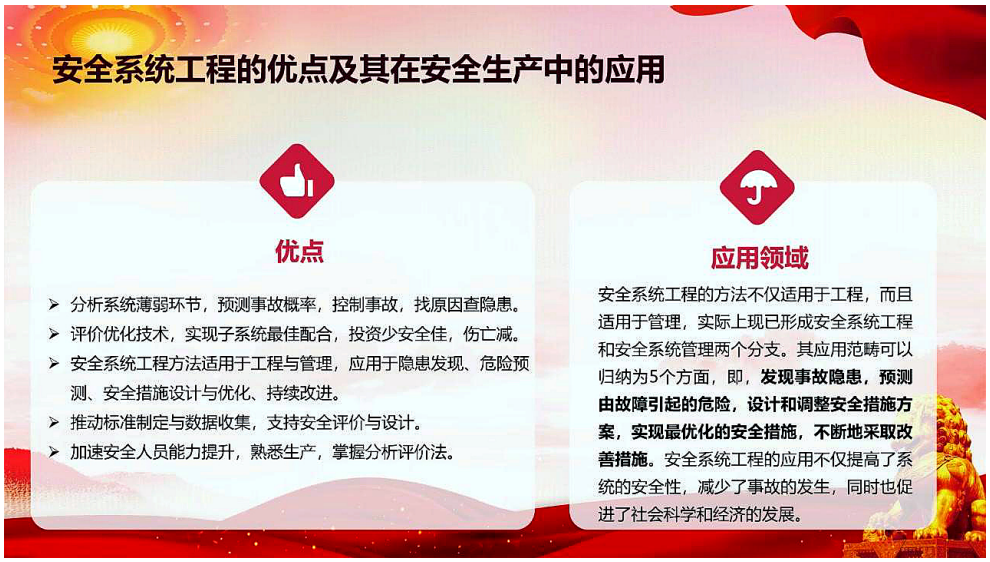


- 研究对象：人、机、物、环、管（人机物环管）
- 研究内容：分析、评价、控制、预测
- 系统具有环境适应性等特征，系统概念是安全系统工程的基础

例

以班级为例：用特征参量 A、B、C、D 描述每个同学的性格特征，若某同学 D 特征偏多，即为薄弱环节，可进一步分析是老师的问题还是学生的问题，从而改进。

安全系统工程的应用领域



- 覆盖行业：化工、交通、建筑、电力、机电、消防、航空航天等
- 电力行业（发电厂、电网、风电、燃气轮机、火电）同样需要系统安全
- 航空航天系统中有重要的”安全保障体系”子系统，发射升空与返回地面阶段均高度重视安全
- 政治、经济、国防、科技、网络空间等领域均存在风险

> **例**
>
> 广东的炼油厂（广石化、茂石化、湛江中科炼化、揭阳中石油炼化）需要大量原油，原油通过海上钻井平台或船运到达，经端点系泊转换后由海底管线输送到油库储存。

原油储罐的安全风险

- 中国最大的原油储罐可达几十万立方，如贵州炼化马鞭洲岛上的储罐群
- 储罐为常压罐，原油含硫，易腐蚀，接管泄漏可能导致火灾
- 原油罐着火事故后果严重，如青岛黄岛曾发生多次原油储罐和管线事故，死亡人数多
- 管线受地基不均匀沉降、自身重量、地震等因素影响，受力不均可能拉断或撕裂

> **注意**
>
> 原油管线泄漏后，油气沿管廊分布，相当于在地下埋设连续的”地雷”，一旦点燃后果极其严重。危险控制、后果预测、事故分析是安全系统工程的核心任务。

事故后果的定量预测

- 分析油气爆炸的影响范围，需计算相当于多少 TNT 当量的炸药后果
- 需计算影响范围、死亡半径、重伤半径等
- 预测手段包括定性分析和定量分析

高压水晶釜失效分析案例

- 高压水晶釜用于人工水晶生产：将石英砂溶解在碱性氢氧化钠溶液中，在五六百度高温、几百兆帕高压下结晶，过程约一周
- 釜体为耐高温高压耐腐蚀的钢（泡、落、裂、母矾钢），强度高
- 失效原因分析：

  - 金属低温时变脆，韧脆转变温度可能为 -20℃
  - 长期高温工作后，韧脆转变温度升高至常温约 20 多度，做实验时材料变脆
  - 长期高温导致金相析出、晶间腐蚀产生微裂纹
  - 冷热交替导致疲劳损伤
- 事故经过：反应釜泄漏后切掉一段、重新测螺纹并密封，做密封性试验时突然爆炸，炸穿墙壁，炸成几块
- 改进措施：做耐压实验前先用热水将温度升上来，避免低温脆性导致爆炸

例

高压水晶釜爆炸案例说明：材质在长期高温工作后发生性能变化（韧脆转变温度升高），工人不了解此原理，在低温下做密封性试验导致爆炸。通过宏观和微观分析可明确事故原因，判定责任不在操作人员，而在材质本身。

安全系统工程在安全生产中的应用

- 找到薄弱环节：通过分析系统各要素，识别薄弱点并改进
- 不断发现隐患、预测危险、改进设计、优化提升
- 优化标准：根据风险可接受程度确定安全距离，而非一刀切
- 提升人员技能：通过生产实习、仿真平台等提升辨识和设计能力

例

天津 812 大爆炸后，危险化学品储存标准原规定仓库周边 1000 米内不能有其他设施，浪费大量土地和成本。后修改为根据风险可接受程度确定安全距离，周边仍可利用。

安全系统工程涵盖技术、管理与文化

- 安全系统工程不仅适用于工程，还适用于管理
- 包含技术和管理两个方面，此外还有安全文化
- 安全文化体现在人员形象、庄重严肃的态度上

注意

安全文化是安全系统工程的重要组成部分，不能只关注技术和管理。人员形象、行为规范也是安全文化的体现，如进入政府机关、企业现场需着装规范。

安全系统工程的产生与发展





- 安全系统工程最早从军方提出，源于武器系统安全
- 从武器系统安全标准、系统安全程序，修订为系统安全程序要求
- 奠定了系统安全工程概念：从设计、分析、综合等基本原则出发
- 二战期间，部分武器（如飞机）经海运到前线后无法作战，原因是设计时未考虑防腐、防潮、防霉，海水中的氯离子造成腐蚀

定义

系统安全工程：将系统（如导弹）划分为多个子系统，每个子系统达到最佳状态，子系统之间良好匹配，满足整体要求后再进行组装和测试。

例

弹道导弹系统安全工程：将导弹分为多个子系统，每个子系统要求达到最佳状态并相互匹配，满足整体要求后再组装测试。由于导弹成本高（一发上百万），只能做一两个实验，因此必须设计非常完善的实验方案。

新能源电池的安全风险

- 新能源汽车最大弱点在电池，着火后很难扑救
- 新能源车使用成本低（一公里几毛钱），但存在续航问题（冬季明显）
- 电池技术仍在不断发展，质量不断提高

例

石油公司员工配两辆车：油车跑长途（一公里 1~2 元），电车上下班（一公里几毛钱），但电车着火后难以扑救，主要问题在电池。

技术发展与系统安全的关系

- 电池技术快速换代升级，从半固态电池到固态电池，风险逐步被控制
- 技术进步不断降低产品系统风险，提高产品质量与可靠性
- 科技发展（电气化、通讯、控制自动化、制造工艺）与人的因素共同推动安全水平提升

各行业安全水平对比

- 航空：整体较安全，但战争（无人机、导弹）带来新的风险因素
- 铁路：高铁速度快、舒适、准时，风险相对较低；早期绿皮车时速仅约 60 公里
- 汽车：新能源车国内数量全球第一，若无非贸易壁垒可覆盖全球市场

- 化工：风险相对较高的行业，但利润较高，因此各省市大量引进

产品性能与系统安全

- 产品性能涉及可靠性、维修性、有效性（可用性）等方面
- 这些性能与系统安全和风险密切相关
- 例：桑塔纳因耐用、易维修而长期保有品牌价值

> **例**
>
> 早期桑塔纳轿车虽简单，但耐用可靠、维修方便，体现了产品可靠性对市场的影响。

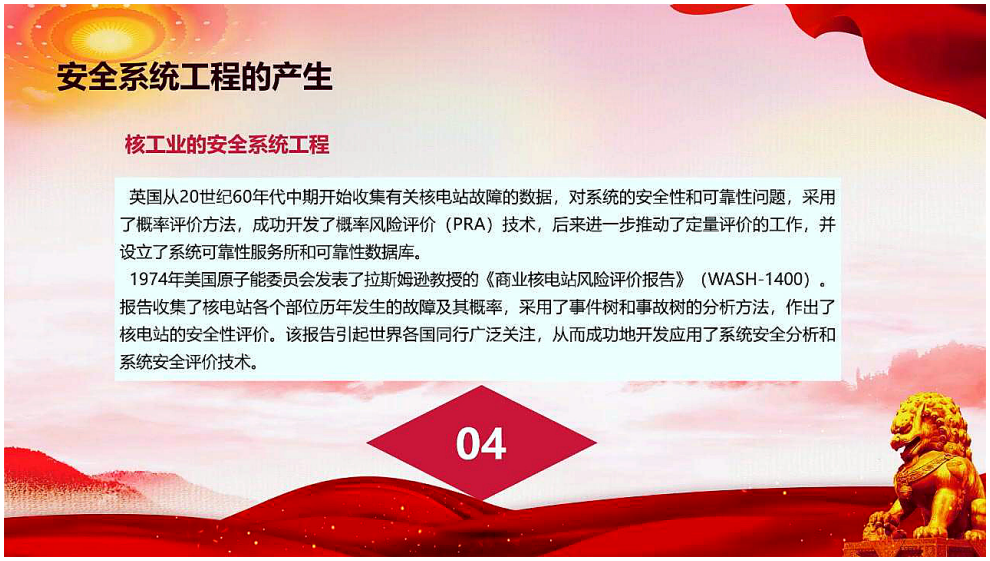
民用产品质量的进步

- 早期日本民用产品（如彩电）做得较好
- 如今中国品牌（电视机、洗衣机、冰箱）已大量出口，质量过关、价格便宜，市场认可度高

化工行业风险与评价方法

- 化工是高风险行业，但利润相对较高
- 1964 年美国提出火灾爆炸指数评价法，日本也提出相应方法
- 具体评价方法将在后续系统安全工程评价章节详细讲解

核工业安全与概率风险评价



- 核电站不容闪失，核辐射对人、动物、植物危害大
- 早期核电事故（切尔诺贝利、三里岛）后，推动了概率风险评价（PRA）的发展
- 涉及可靠性、可靠性数据库、核电站风险评价报告等

> **定义**
>
> **PRA（概率风险评价）**：通过事件树、故障树等方法分析系统故障及其概率，对核电站等高风险系统的风险进行定量评价。

- 事件树、故障树是系统安全分析和系统安全评价中最基本的方法之一
- 商业核电站风险评价报告投入大量经费，产生历史性影响
- 中国核电已与英国、法国等合作，甚至可直接到国外建核电站

安全工程专业人才培养现状

- 国内约 160~170 所高校设有安全工程专业
- 新兴专业：安全科学与工程、消防安全工程、应急管理、安全监察工程、化工安全工程、智慧安全、智慧应急、应急技术与装备（机械类）
- 广东存在的问题：专业开设学校少、培养层次不高、规模小，但社会需求大
- 曾推动建设广东应急管理学院，因经费投入大（学校年预算约 100 亿）及领导调动而未成

事故驱动到数据驱动的转变

- 早期（改革开放初期）事故频发，如 90 年代大量几十人死亡的事故、机械冲床断指事故
- 发展理念从粗放式向集约化转变（绿水青山就是金山银山）
- 安全发展阶段：机械化减人 → 自动化换人 → 智慧化无人
- 目标：从事故驱动转向数据驱动、数字驱动

注意

自动化、机械化虽能减少人员伤亡、提高效率，但需要技术支撑；国外技术不卖或价格高昂（如冲床几万元一台），而当时人工工资仅几十元，导致早期只能依赖人工。

科技支撑：人工智能与互联网

- 人工智能和互联网是当前最大的科技支撑
- 应用方向：互联网 + 工业、安全监测监控预警
- 多无人机协同：用于化工园区等高位聚集区的监测预警平台（空地协同）

例

多无人机协同平台可传输数据、图片、倾斜摄影、三维重构，实现动态态势感知与趋势预测。若发生泄漏，可结合风速、风向、湿度、气压预测扩散方向与范围，并实现溯源（定位泄漏源）以切断源头。

分布式断电减灾

定义

分布式断电减灾：针对分布式布置的燃气等管线，通过优化控制节点，在事故发生时切断源头，实现减灾。

- 分布式管线节点多、控制难度大，存在优化问题
- 科技发展无止境，多学科交叉融合是未来重点

安全系统工程教材与课程定位

- 安全系统工程行业面广，几乎每行每业都需要安全人才
- 国内安全系统工程发展约 20 年，发展迅速得益于党和政府对人民生命财产的重视
- 教材编写需融合教学、工程与应用，涵盖面广

安全的概念

1、安全

■安全：指人的身心免受外界（不利）因素影响的存在状态及其保障条件。

2、风险：

■风险：危险、危害事故发生的可能性与危险、危害事故严重程度的综合指标。

3、事故：

■事故：是指造成死亡、伤害、职业病、财产损失或其它损失的意外事件。

定义

安全：人的身心免受外界不利因素影响的存在状态，以及保障条件。身体和心理是内在因素，外界因素即环境，保障条件即机器设备。

- 安全从人的本身出发，强调人、机、环的协调共生与和谐

风险的概念

定义

风险：危险、危害事故发生的可能性与危险、危害事故严重程度的综合指标。

- 安全、风险、事故是核心概念，重点在于防止事故发生，特别是灾难性事故
- 防止事故不能无限制投资，需在风险与成本间取得平衡

例

原油储罐（如广州南沙 3 万吨外浮顶罐、20 万立方储罐）需厚钢板、牢固基础，不能有丝毫闪失，体现了高风险设施的安全投入与风险控制。

事故的定义

- 事故是造成死亡、伤害、职业病、财产损失，以及环境污染、名誉损失等其他损失的意外事件
- 事故的影响不仅限于人身和财产，还包括经济层面（如上市公司事故披露后股价下跌）和社会声誉层面
- 杜邦公司的安全哲学：所有伤害都是可以预防的

定义

事故：造成死亡、伤害、职业病、财产损失，也包括环境污染和其他损失在内的意外事件。

注意

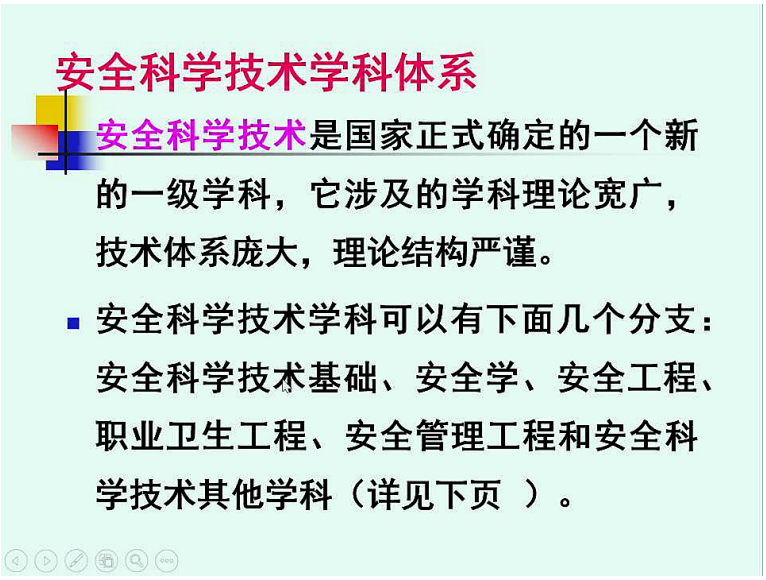
“小组内不重复发生违章”这一说法并不严谨——本小组不重复，其他小组仍可能发生。更严谨的表述是：所有危险、任何伤害都是可以预防的。

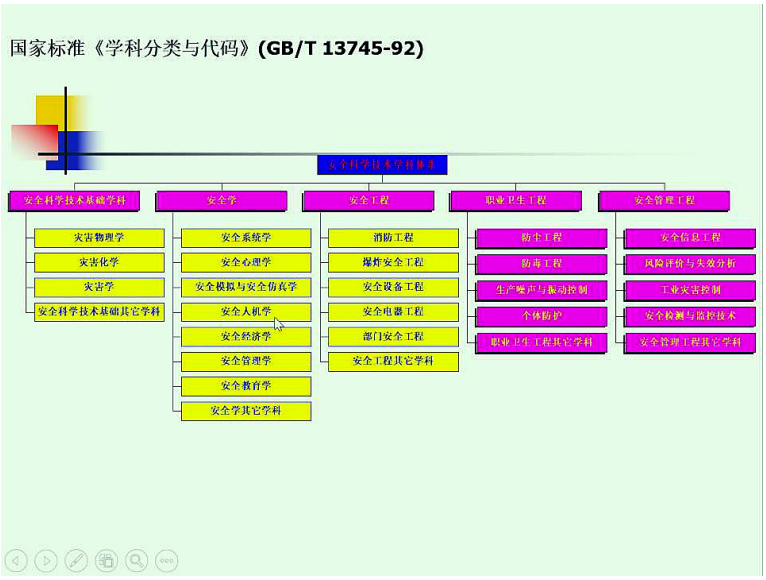
风险的定义

- 风险 = 可能性 × 严重程度
- 概念宽泛但很具体：坐飞机”风险高”是因为后果严重；说飞机”最安全”是因为发生事故的可能性最低
- 90 年代国内飞机事故多，多为人为因素，应对措施是加强安检、教育、管理和应急

> **定义**
>
> 风险：可能性和严重程度的组合。

安全科学技术学科体系





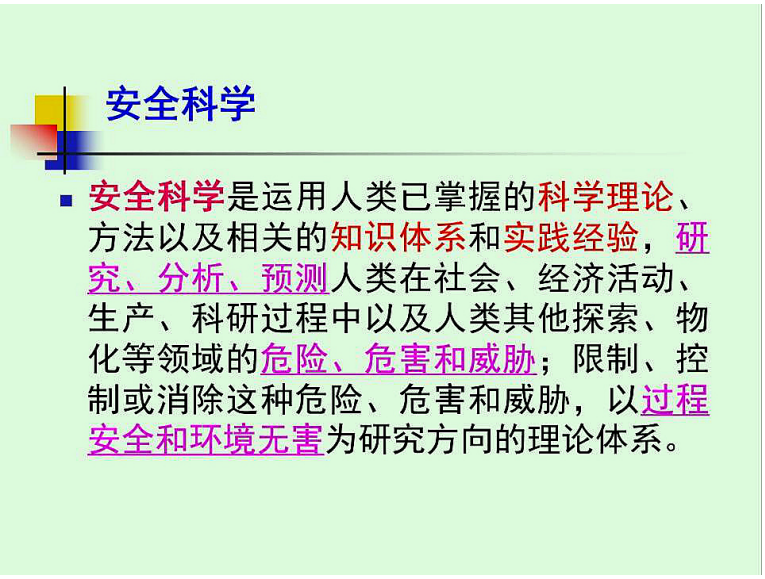
- 安全科学技术位于环境科学与管理科学之间，是介于自然科学和社会科学之间的学科
- 目前界定为工学，但部分学校的安全科学与工程专业可授予管理学学位
- 92 年国标（学科分类与代码）中仅有 5 个二级学科、约 27 个三级学科，体系单薄
- 09 年修编后，学科体系发生革命性变化，二级、三级学科大幅扩充
- 本专业已开设的课程：安全机电、人机安全系统、特种设备、火灾爆炸、消防、

智慧消防、安全工程概论、安全管理等

- 学分压缩趋势：23 级为 170 学分，25 级降至 160 学分，强调”以身为本”——重点在学了多少而非讲了多少

> **例**
>
> 北京理工大学”制药专业”实为火炸药方向（武器系统必需），华北理工、南京理工等国防院校也有类似专业。学生误以为是人用制药，实际是过程安全与化工方向，说明专业方向与名称可能存在差异。

安全科学的概念



- 用人类已掌握的科学理论方法、知识体系和实践经验，研究、分析、预测危险、危害和威胁
- 应用于社会经济、生产科研及其他探索物理化学等领域
- 以限制、控制、消除危险，实现过程安全、环境无害为研究方向

> **定义**
>
> 安全科学：运用人类已掌握的科学理论方法、相关知识体系和实践经验，研究、分析、预测危险、危害和威胁，以限制、控制、消除危险，实现过程安全、环境无害为研究方向的理论体系。

> **例**
>
> 液氢研究：液氢储存密度大，相对气氢更安全（气氢爆炸极限宽、下限低，易泄漏爆炸）。但液氢生产、储存、运输、使用各环节能耗高，使用时常需气化后加注，能耗进一步增加，相关研究仍有待开展。

安全科学的研究对象与目标

- 研究对象：事故、危险状态和存在条件
- 研究内容：以过程的正常平衡协调为目标
- 安全是相对的：相对于可接受的风险水平而言，可接受即安全
- 风险是绝对存在的，安全是相对的

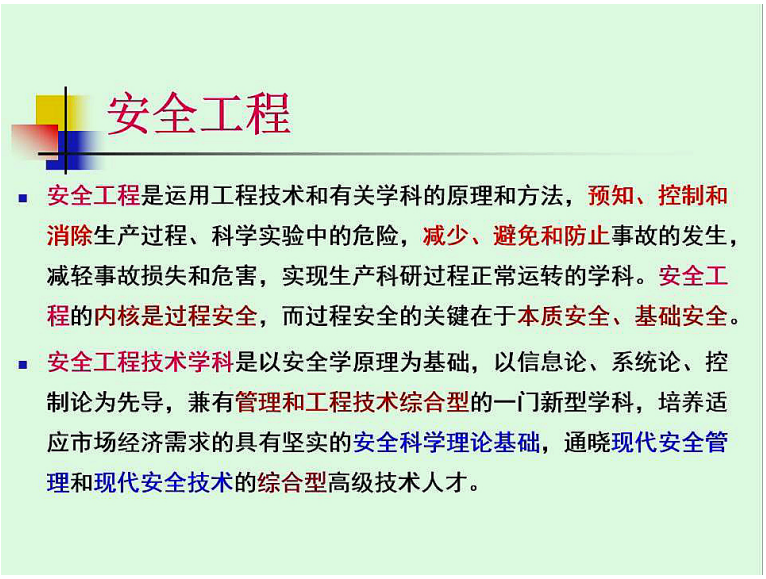
注意

事故与风险不同：风险是绝对存在的，安全是相对的——相对于”我多大风险可以接受”而言。随着经济条件、生活水平提升，可接受的风险水平也在变化（如亡人赔偿从早期约 20 万提升至现在的约 10 倍）。

安全评价指标

- 早期常用指标：亿元 GDP 死亡率、百万吨煤死亡率、万工时伤亡事故率/伤害率、因工损失工时等
- 指标随经济条件、生活水平、人的价值提升而动态调整

安全工程的概念



- 运用工程技术和有关学科的原理与方法，预知、控制和消除生产过程、科学实验中的危险
- 减少、避免、防止事故的发生，减轻损失和危害，实现过程正常运转
- 核心是过程安全、本质安全和技术安全
- 毕业生就业面广，不限于安全领域（金融、房地产、公安、消防等都需要安全）

定义

安全工程：运用工程技术和有关学科的原理和方法，预知、控制和消除生产过程、科学实验中的危险，减少、避免、防止事故的发生，减轻损失和危害，实现过程正常运转。

本质安全

- 本质安全涉及管理机构保障体系（机构、人员、投入）、制度全面性与合规性、运行机制、环境与设备、人的行为安全与意识培训、应急体系等
- 制度是动态的，需持续修编（如学生手册每年修订）
- 人是最活跃、最能动、最具有不确定性的因素
- 本质安全管理体系因行业、领域、企业原有水平不同而难以统一

例

广州燃气集团设”安全技术部”，以”制度保安全、技术保安全”为理念，级别比其他部门高半级。燃气检测从早期用肥皂泡检漏，发展到如今用便携式检测仪，

并免费更换钢制软管——这就是本质安全的体现。

安全工程技术学科

- 以信息论、系统论、控制论为基础，且需与时俱进（信息 = 互联网、大数据、人工智能）
- 兼具管理、技术、法规标准、文化等多方面
- 培养现代安全管理和现代安全技术综合性的高级技术人才
- 新修编课程引入人工智能概念（基础课为 C++），专业融合课如智慧消防、智慧应急等

注意

安全工程专业课程体系庞大，本专业所学有限，毕业后仍需通过读研或工作中持续学习，不能因科班出身就自认已掌握全部。

课程内容与考试结构

- 主要内容：安全系统工程、系统安全分析、事故树分析、系统安全评价、危险控制技术、典型应用
- 事故树分析属于系统安全分析的重要部分，单独拿出来介绍
- 事故树分析考试约 20 分，第一章约 20 分，需重点重视
- 分析、评价、控制部分可自行阅读了解

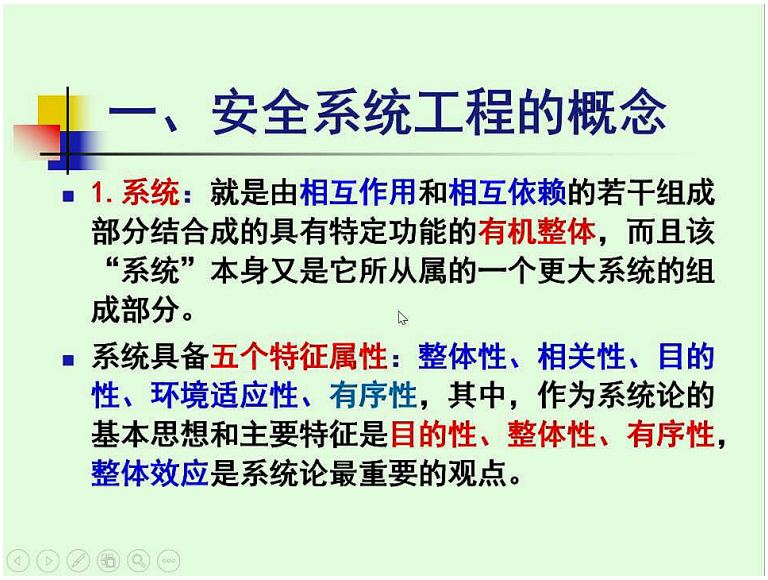
安全系统工程的研究对象

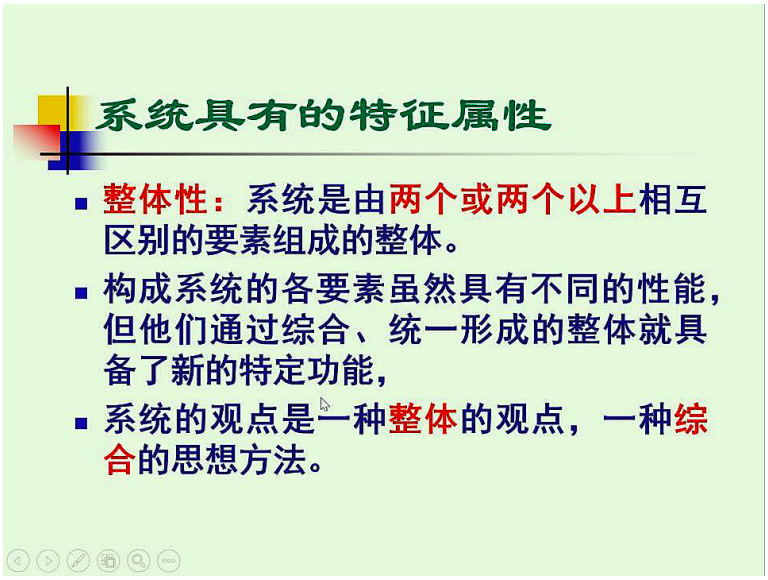
- 研究对象是人-机-环境组成的系统
- 安全科学工程、安全工程、安全技术的研究对象各不相同，不要混淆
- 需掌握系统工程、安全系统工程的定义

学习资源建议

- 推荐阅读比教材更早的经典教材（如林伯权、张景明等老教授的版本）
- 可参考其他教材，各方面侧重不同
- 有双语教材（含重庆大学版本、一位女教授的双语教材）
- 英文资料：海因里希《工业事故防控》原著（85 年版）等
- 建议：找一本英文、一本中文，配合教材使用，便于理解和做题

系统的五个属性



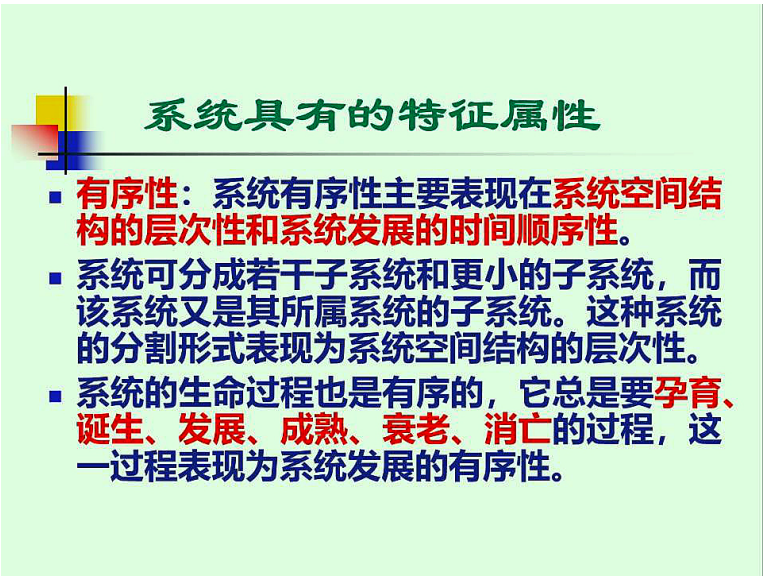


- 整体性、相关性、目的性、有序性、环境适应性（闭着眼睛都要能说出来）
- 目的性：在规划、设计、试验、制造、使用各阶段实现最优规划、最优设计、最优控制、最优管理

事故的溯源

- 事故本质是能量（机械能、电能、热能）失控作用在人体或物质上
- 根源可溯源：设备设施问题（设计、制造、工艺）或控制系统问题
- 人的问题：培训教育、知识水平、待遇保障

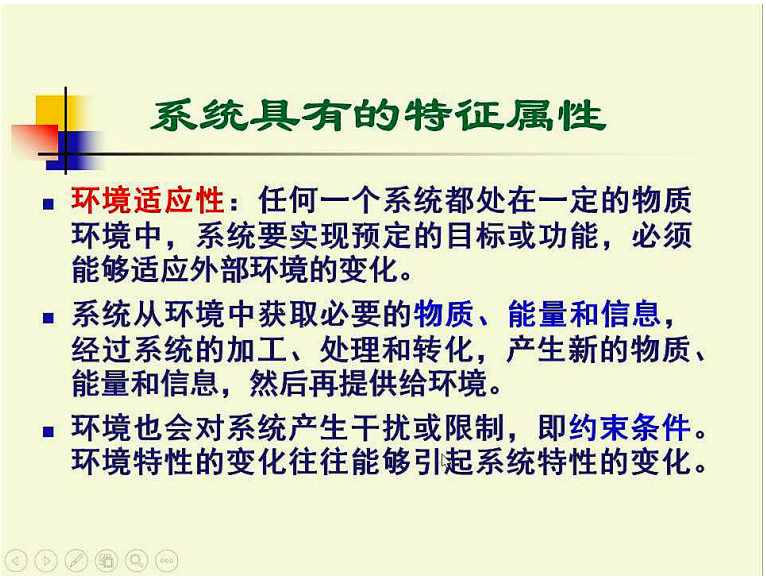
有序性



- 系统空间结构的层次性 + 时间上的过程性
- 生命周期：孕育、诞生、发展成熟、衰老、消亡
- 风险是时空演变的
- 信息物理系统融合的系统风险分析：网络攻击影响操作 → 误操作 → 产生后果
- 数字化程度越高，对信息物理融合风险分析的需求越大

> 注意
>
> 有序性可出选择题、判断题、填空题、多选、单选等多种题型，需全面掌握。

环境适应性



- 系统不能与外界独立隔绝，需进行物质、能量、信息交换
- 环境对系统产生干扰和限制，形成约束条件
- 例：黄埔云计算中心（专供公安大数据）虽物理隔绝，但仍主要面临消防安全问题

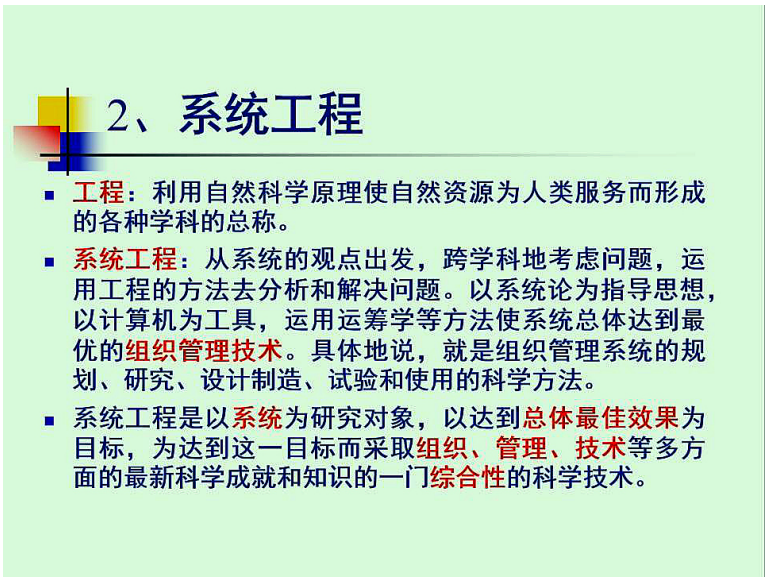
例

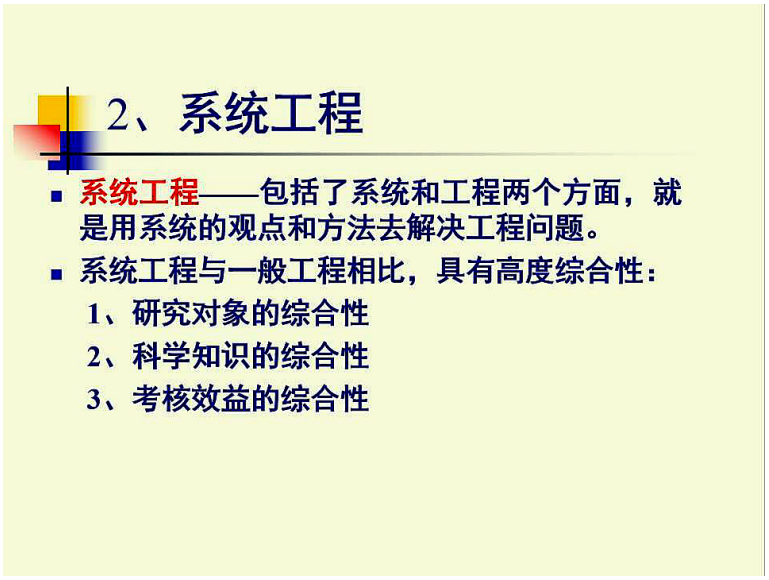
物质：人需要进食（能量交换）；信息：现代社会离不开手机（信息交换）。能做好”断舍离”、自我约束的人往往更好。

韧性

- 定义：系统受到干扰或外力作用下，能较快适应、较快恢复、较快达到原来状态
- 韧性可以后天培养（如坚强的意志）
- 社会韧性园区：在系统基础上形成韧性

工程与系统工程的概念





定义

工程：利用自然科学原理，使自然资源为人类服务而形成的各种学科的总称（如电气工程、机械工程、建筑工程）。

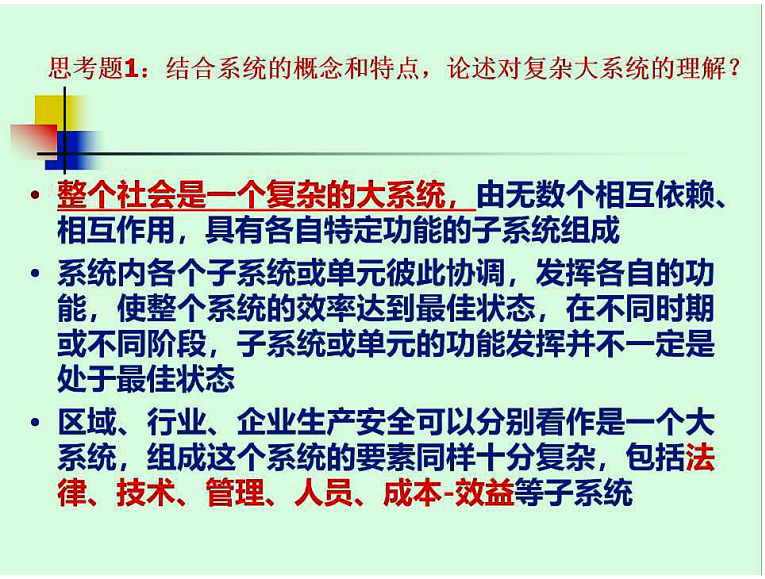
- 系统工程：用系统的观点，以系统为研究对象，追求总体最佳效果
- 总体最佳效果不是唯一的，是相对灵活的概念
- 系统工程是组织管理技术，融合技术、管理、法规、文化
- 系统工程具有高度综合性：研究对象、科学知识、考核效益的综合

- 安全系统工程除了技术知识，还要注意效益（如自动化监控投入成本过高则没必要）

例

钱学森先生提出系统工程，应用于导弹轨道全程弹道。系统工程不仅用于安全领域，还用于敦煌壁画保护等场景（数字化后无需人到现场）。

复杂大系统



定义

系统：由若干相互依赖、相互作用、具有特定功能的要素构成的具有特定功能的有机整体。

- 复杂大系统：如整个社会，由法律、技术、管理、人员、成本、效益等构成
- 具有随机性、不确定性、很大的不确定性
- 社会应在制度约束、法律约束下运行，构成和谐、稳定、向上发展的态势
- 在某阶段达成平衡，随时间推移打破平衡，形成新的持续发展过程

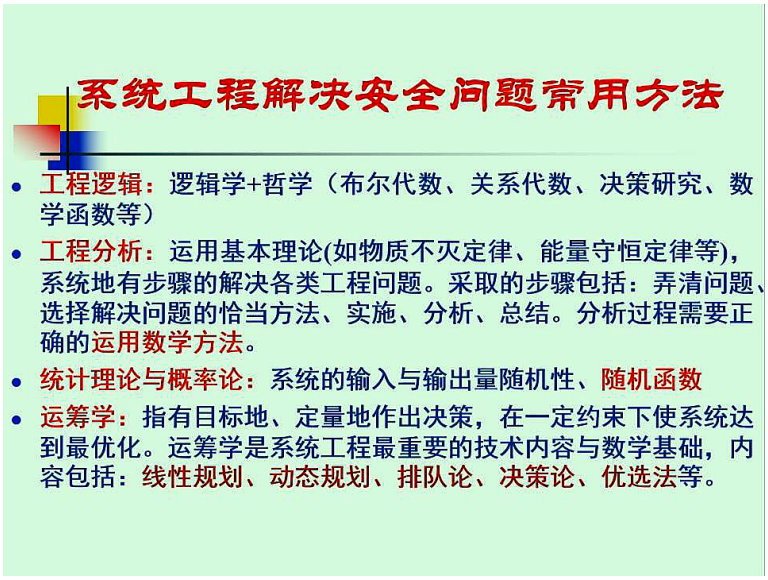
例

用”渔网”类比复杂大系统：有些区域致密稳定，有些区域脆弱（如地震、海啸、沙漠），核心节点周围衣食无忧。个人发展要选择稳定节点，避免投机”闯雷区”。

注意

对复杂大系统最好的约束是制度、法律（“尺子”）。投机、加杠杆等行为不可取，应遵从社会发展规律。

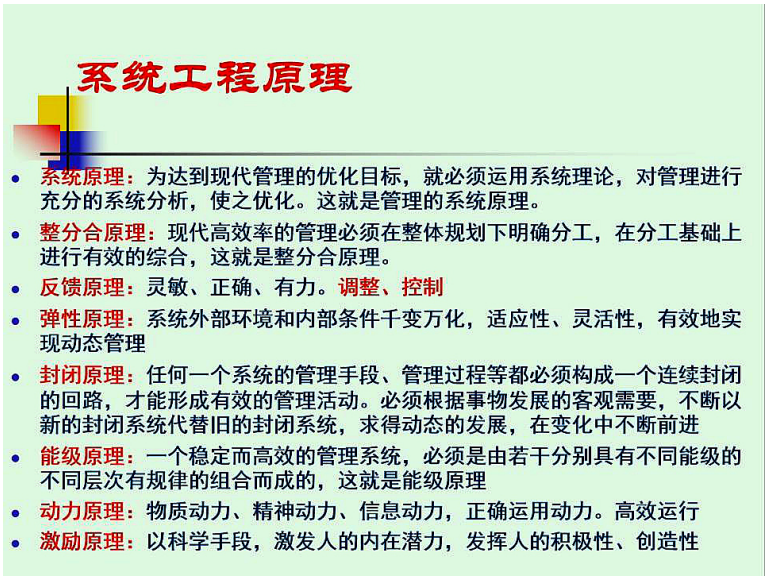
常用方法

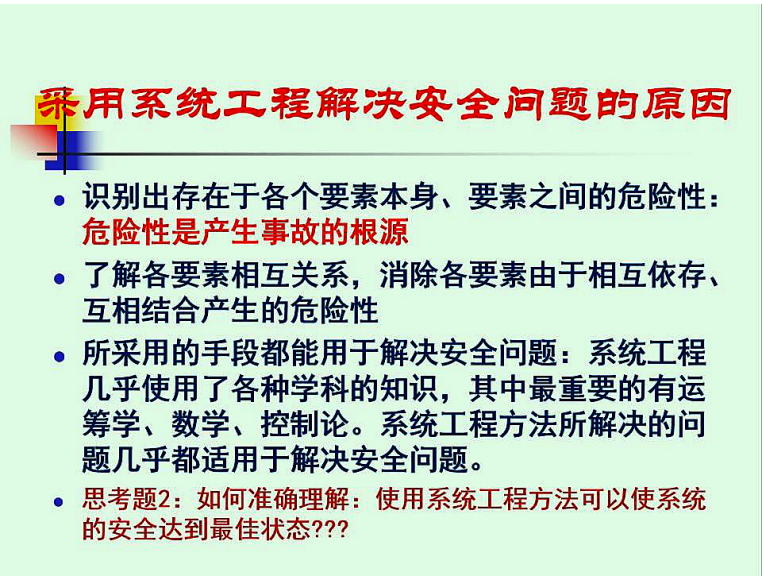


- 布尔代数（后续学习使用）
- 能量守恒、动量、质量等物理/化学/数学基础
- 概率论与数理统计、随机函数
- 运筹学（线性规划、动态规划、优化）

> 注意
>
> 多选题不要选漏；要能写出 5 个系统工程原理；要能理解”动力原理”等概念。出题不重复但都遵从书本。

系统工程方法解决安全问题的原理





- 能识别出各要素本身以及要素之间的危险性（辨识能力因人而异）
- 了解各要素的相互关系、相互依存、互相结合产生的危险性
- 运用多学科知识：运筹学、管理、线性规划、动态规划、数学、控制论
- 系统工程要解决问题的几乎都适用于解决安全问题

作业题

- 作业一：结合系统的概念和特点，论述你对复杂大系统的理解
- 作业二：如何理解使用系统工程方法可以使系统的安全达到最佳状态
- 作业三：生物圈二号为什么失败了
- 要求：手写，统一用 A4 或华工信签纸，独立完成，计入平时成绩

生物圈二号

定义

生物圈一号就是地球。生物圈二号是模拟地球的微型人工生态环境系统，位于美国亚利桑那州图森。

- 模拟地球生态：居住区、农业区、沙漠、沼泽、海洋、热带雨林、热带草原等区域
- 耗资 1.5 亿美元，历时 8 年建成（约 90 年代）
- 含 7 种生态群落和 2 个大气扩张室，主要靠光合作用，几乎自给自足
- 两次实验均失败

注意

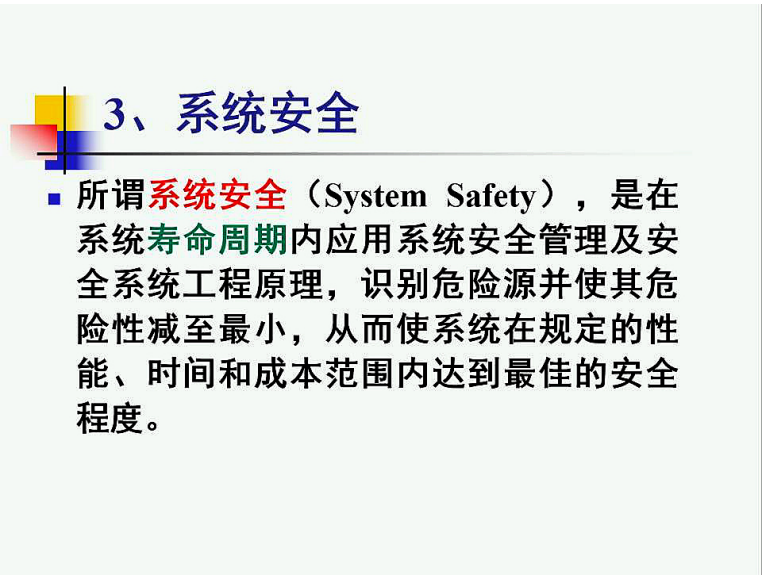
生物圈二号失败的根本原因是生态破坏。它是非常典型的生态循环系统，生态安全是重要问题。

例

生物圈二号的意义：若能在月球或其他星球建造类似系统，即可建立像地球一样的生存生活环境。联系”绿水青山就是金山银山”，更易理解生态安全的重要性。

09 月 22 日

工程的概念



- 工程是使自然科学为自然资源为人类服务的一些项目
- 属于学科范畴，是运用科学原理将自然资源转化为满足人类需求成果的实践活动

风险的本质特征

- 风险的本质是不确定性，即无法预知未来将会发生什么
- 风险需同时考虑两方面：事故发生的可能性与事故后果的严重程度
- 灰犀牛、黑天鹅等小概率事件，发生概率低但一旦发生后果严重，需综合考量
- 概率论与数理统计是处理随机不确定性的有效工具

定义

风险 = 事故发生的可能性 × 事故后果的严重程度，其本质特征是不确定性。

系统的五个特征

- 整体性
- 相关性
- 目的性
- 环境适应性
- 层次性（又称有序性）

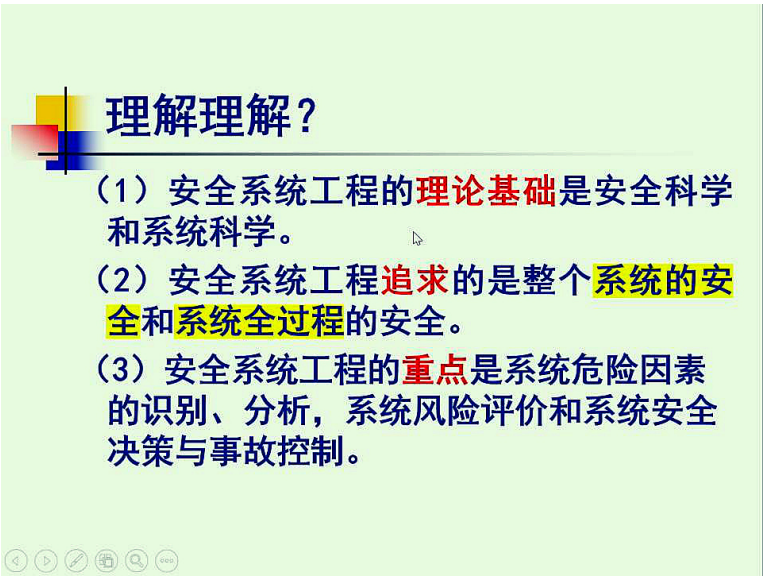
注意

系统的五个特征中，层次性常被遗漏。层次性又称有序性，指系统内部结构按一定规则组织，受系统目标指导。

环境适应性的理解

- 指系统能随外部环境变化而调整自身，以维持生存与功能
- 是系统设计的关键特点之一
- 理解环境适应性需先明确其含义，再思考如何更好地适应环境

安全系统工程的研究内容与对象



- 研究内容：系统危险因素的识别分析、系统风险的评价、系统安全的决策和事故控制
- 研究对象：复杂大系统（如城市、社会、人自身等）
- 目的：将目标系统风险控制在可接受的水平范围内

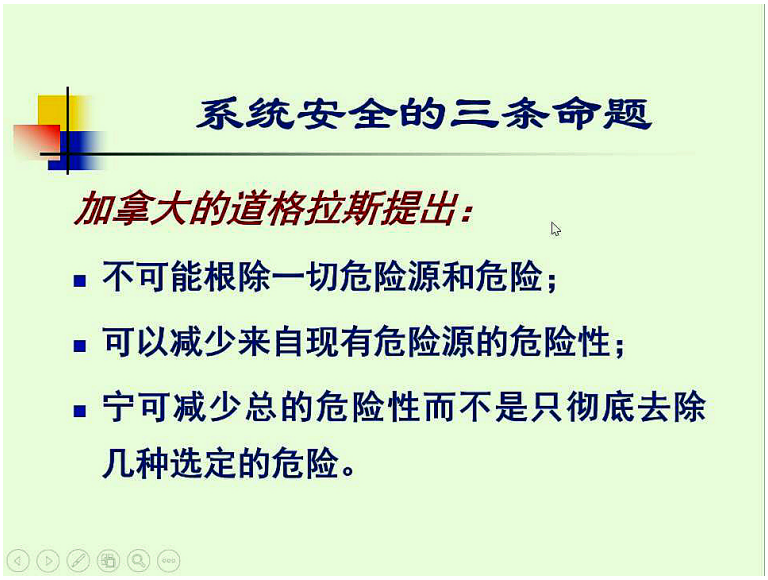
> **例**
>
> 以深圳摩天大楼（高度超 100 米）为例，需从系统角度分析其面临的风险：台风、地震、雷电、火灾等自然灾害，以及老旧小区、城中村等复杂社会情况。整个社会就是一个复杂系统，人是最能动、最活跃的因素。

系统安全寿命周期

- 寿命周期与成本密切相关，不能无限期使用
- 汽车零部件会老化，需定期维修保养；组装修复的车辆可能仅能通过初次年审，成本高
- 太空探索同样有时间和成本考量，需在寿命周期内追求最佳安全水平与最高安全效益
- 技术持续升级（如手机更新换代），用户更关注产品当前是否满足需求，不满足即被淘汰

> **注意**
>
> 不能只考虑系统”是否还能使用”，而要从全寿命周期角度综合权衡安全、成本与效益。无法无限制投入人力和物力。

系统安全的三个命题



- 命题一：完全消除所有危险源和风险是不可能的
- 命题二：系统可包含某些危险或有害因素，但风险应控制在可接受的范围内（即忽略不计的风险）
- 命题三：减少总体风险，而不是仅仅消除选定的几种风险

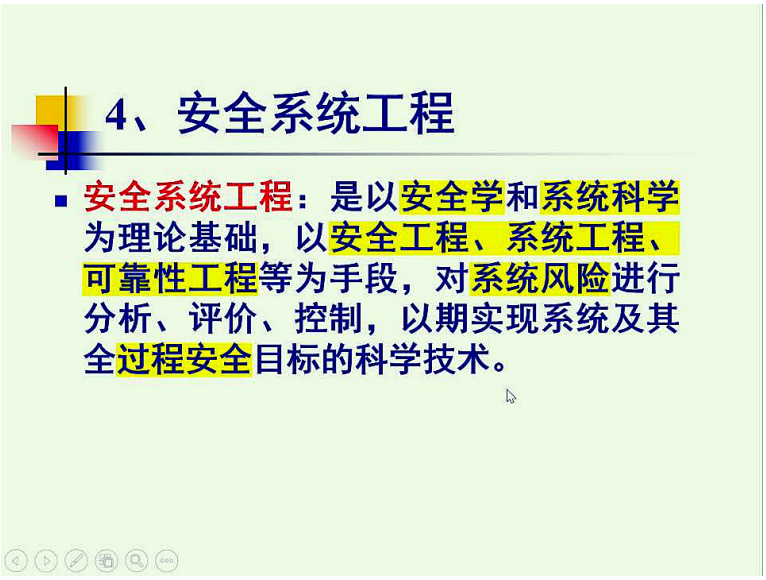
> **定义**
>
> 本质安全：产品、设备或系统在设计上达到本质安全，是追求的目标，但必须认识到完全消除所有危险源和风险是不可能的。

> **例**
>
> 相对风险防控的最优考虑：并非简单地替换掉最危险的因素，而是同时考虑和防控多个不同危险性因素，在成本或性价比上更有效。例如事故树分析中，通过定性和定量分析找到最小割集，控制其中任何一个因素即可防止事故发生。

可靠性工程

- 可靠性工程是一门独立学科，强调可靠性制造概念
- 产品在投产时就要考虑可靠性，且在整个生命周期中对可靠性有大致的预知
- 涉及选材、设计、加工、安装、使用维护及全寿命周期管理等多个方面
- 在航空航天领域，系统可靠性与安全性都是必须考虑的关键因素

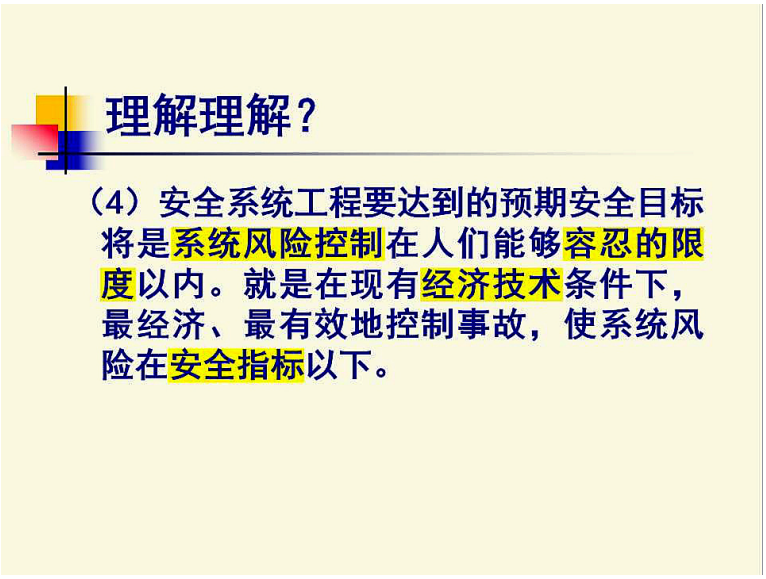
安全系统工程的理论基础



- 理论基础源自安全科学和系统科学，两者属于不同学科类别
- 系统科学的奠基人是中国科学家钱学森
- 国外在二三十年前已开展众多安全项目；我国在上世纪 70 至 80 年代引进后，安全科学逐渐发展为规范且独立的一级学科

> 定义
>
> 安全科学作为独立一级学科的标志：拥有完善的职称评价体系、覆盖本硕博博士后的完整学位体系、各级协会相继成立、产出丰富的 EI 和 SCI 收录学术成果。

系统风险控制



- 目标：在现有技术和经济条件下，采用最经济有效的事故控制策略，将系统风险保持在安全指标以下
- 可接受的风险范围取决于科技、经济、社会政治及相关发展水平

例

风险衡量指标：

- 交通事故：万车死亡率（我国已有效控制，呈线性下降趋势；美国早期每年数万人丧生）
- 煤矿开采：百万吨煤死亡率（开采 100 万吨煤过程中的人员伤亡比例）
- 经济社会：意愿 GDP 死亡率（广东较低，因 GDP 较高；绝对数值上全国较多）

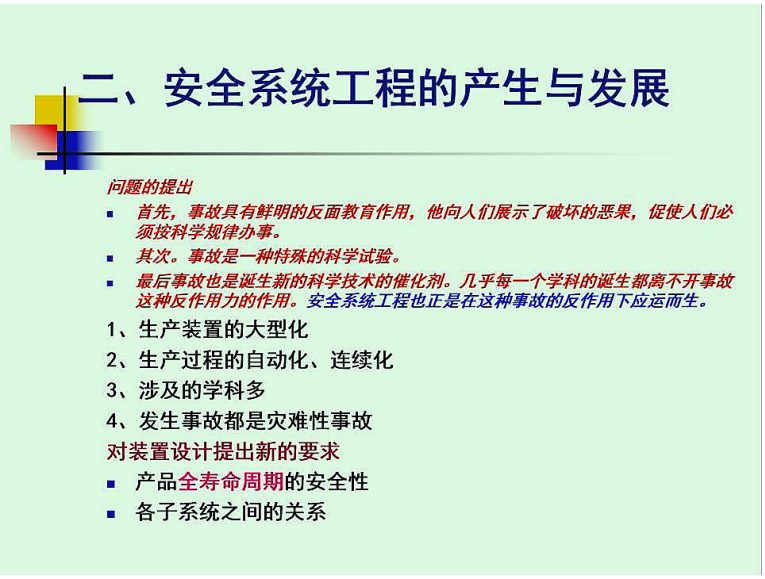
注意

经济发展水平越高，对专业技术人员的需求越大。以广州塔顶摩天轮为例，其由四个驱动装置驱动，若轨道车辆偏离或脱落会失去电力而停止——停下来是安全的（有平台支撑），但一旦出现异常，信息媒体会迅速传播，无法承受此类风险。

广州塔特种设备与安全启示

- 广州塔属于特种设备中的游乐设施，只有国家特检院有资格检验，广东省院无资格
- 跳楼机（穿梭机）上下快速移动，类似自由落体体验
- 运营者称其相对安全：无论从哪个位置掉落，人都会向下坠落，不会出现舆情问题
- 高速电梯可迅速从一层直达 100 层（广州塔约 140 层），体现特种设备安全的重要性
- 核心结论：特种设备安全至关重要，须将风险控制在可接受的范围内

事故问题与系统安全的重要性



- 事故的反作用与发现的问题是事故问题的出发点
- 随着装置大型化、生产过程自动化与连续化、学科交叉性增加，事故问题可能具有灾难性
- 对系统安全提出更高要求，系统安全/安全系统工程处于前所未有的重要地位

国家安全学学科发展

- 国家总体国家安全观由习近平总书记提出

- 国家安全学院和公共安全学院被列为安全科学的二级学科
- 国家安全学最近被确立为一级学科
- 广东省内仅一家机构提供国家安全学博士学位
- 上海交通大学、北京大学等知名学府均设有安全相关课程
- 南京大学安全科学与工程学院将安全科学、技术及管理知识应用于国家安全研究，适合偏文科学生深造

三同时要求

定义

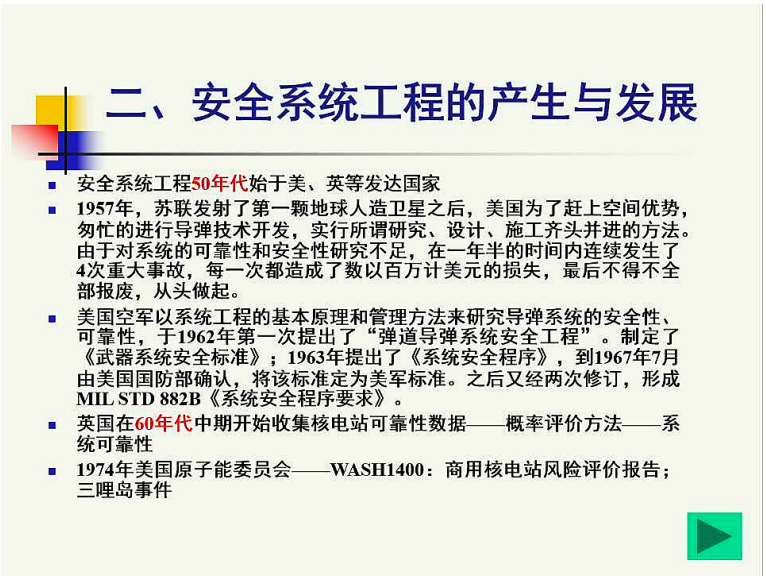
安全设备设施与主体工程必须同时进行设计、施工和验收投入使用。

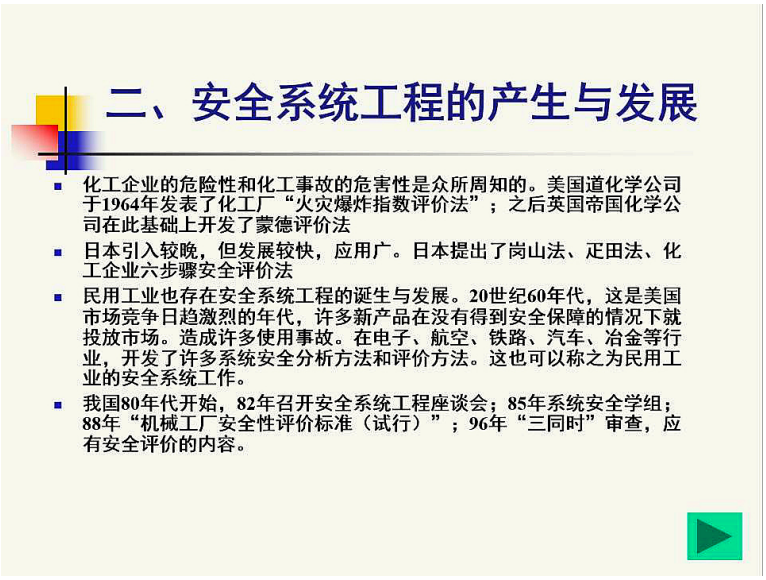
- 必须有专业机构提供技术支撑，并经过专门管理机构进行行政审批
- 安全生产许可证和危险化学品经营许可证是企业能否正常运营的关键指标
- 审批已延伸至市级行政审批层面，每个市设有专门审批处/部门
- 流程：第三方中介服务机构提供技术报告 → 专业机构评审 → 审查机构依据法律法规决定是否发证
- 危险化学品不能直接买卖，违法将面临刑事责任，严重者坐牢

例

深圳某教练场将面包车改装，把汽油桶放入车内给教练车加油（撬装式加油站），最终被举报。汽油属危险化学品，易燃易爆，移动式撬装加油站有特殊规定和条件，此类行为违法。

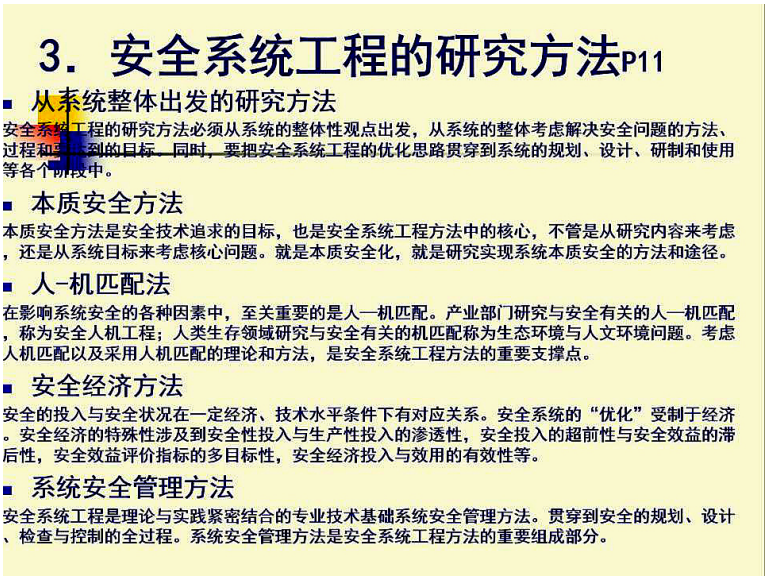
安全系统工程的发展脉络





- 起源于空间技术：美国与前苏联从空间优势到导弹系统，再到安全大纲和国防部形成
- 逐渐过渡到民用领域（环境子系统等）

安全系统工程的基本方法



从系统整体出发的研究方法

- 涵盖系统优化、思路贯穿、规划设计、研制使用等各环节
- 应用于建筑设计、道桥设计、大型机械装备设计、工艺流程设计、反应过程等
- 坚持预警控制等基本思路
- 必须基于标准规范和法规，任何设计不能低于此标准

> **例**
>
> 安全距离：仓库与工艺装置之间、甲类仓库与工艺装置之间、储罐之间的距离，必须满足规范标准要求。否则后续法规标准严格时，改扩建将面临困难。

本质安全的方法

定义

本质安全是通过设计等手段使生产设备或生产系统本身具有安全性，即使在误操作或发生故障的情况下也不会造成事故。

- 替代：用无毒物质替代有毒物质
- 减缓：用低毒物质替代高毒物质；不能完全替代时尽可能减少使用量
- 简化：尽量简化复杂系统设计，因为组成系统的部件越多，潜在风险越大

例

改革开放初期，耐克鞋用含有机溶剂的胶水粘合，劳动密集型环境下工人频繁接触，缺乏有效防护，许多工人半年左右出现贫血，病情加重甚至导致白血病。后以无毒/低毒胶水替代高毒胶水，并加强个体防护装备和通风换气。

- 本质安全发展已涵盖人、机、管、环、文化，甚至加入信息通讯
- 管理部门和化工园区管委会要求具有安全或化工专业背景的管理人员不低于75%（如总人数 15 人，需招聘 11-12 名）

例

今年真实案例：一位原在广州特种机电设备检测院工作的学生，考入一类事业单位（参公管理，身份相当于公务员），被分配到新建化工园区工作。

机械化、自动化与智能化

- 通过自动化减少人力，实现机械化换人，进而达到智能化无人操作
- 从多个角度追求机械安全

管理安全

- 管理体系：如职业健康安全管理体系（后续课程学习）

人机匹配

定义

人机工程学（人类功效学）是研究人与机器相互作用的独立学科门类，在安全领域通常称为人机工程学。

- 飞机座位间距：欧美更宽敞，考虑人的平均身高偏高
- 汽车舒适性、驾驶显示器与安全报警
- 生产过程中颜色差异提示操作者注意
- 机器设备配备声光报警器
- 操作通常要求双手操作以确保机器正确响应，单手操作机器可能无法准确执行指令

安全经济方法

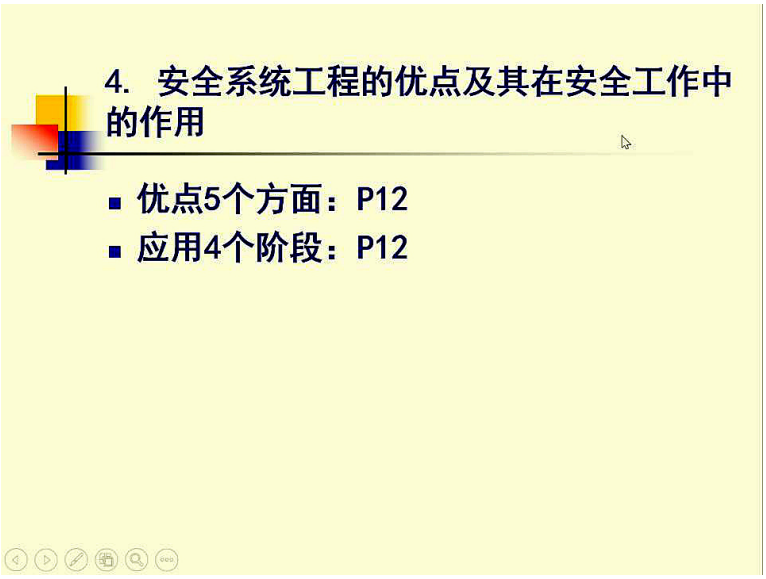
- 揭示一定经济技术水平下安全与经济的关系
- 受制于经济：有最佳投入、最好效益
- 特点：安全投入的超前性、安全效益的滞后性、安全效益评价指标的多目标性、安全经济投入与效益的有效性

> **注意**
>
> 不能简单认为化工、石化行业赚钱就粗放式发展。改革开放初期，教师凭一个配方找搅拌工/反应组，一周分装贴标签即可销售，或像医生开处方给工厂生产。但当时对人身安全、环境破坏和资源浪费明显，现在不可能再出现。行业利润高，就需要相应投入。

系统安全管理方法

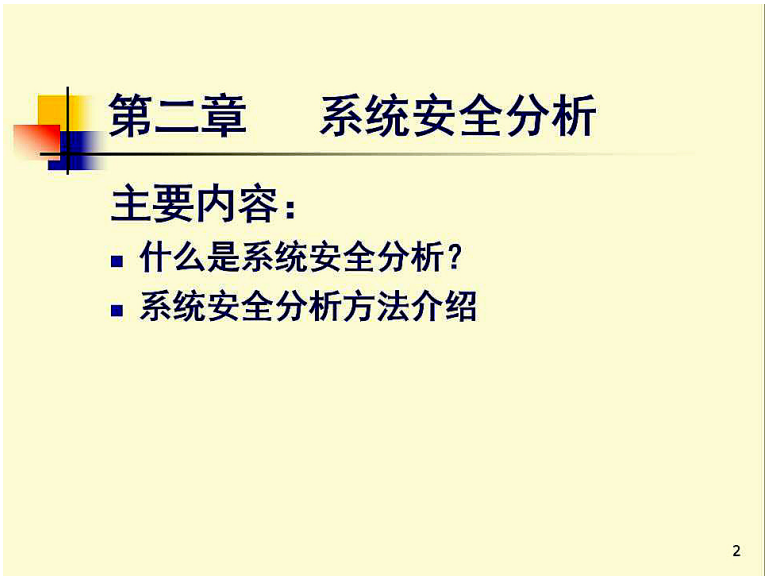
- 从系统角度阐述，将理论与实践相结合
- 涵盖规划设计与检查控制等方面
- 本课程继承安全系统工程的优点

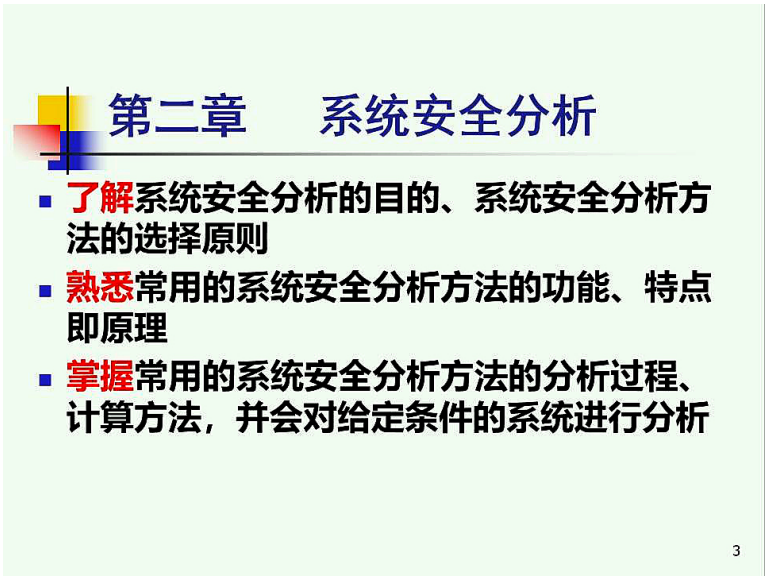
系统安全工程在安全工作中的应用



- 四个应用阶段（已了解，不再详述）
- 坚持以人为本，把人的生命安全放在首位
- 强调预防为主、综合治理等原则
- 注重环境无害、过程安全和本质安全
- 需在工程设计、工程伦理及事故预防等方面考虑

第二章：系统安全分析方法（本章重点）





- 本章目标：
  1. 阐述系统安全分析的目的和方法选择
  2. 熟悉并介绍常用系统安全分析方法的功能特点
  3. 掌握常用系统安全分析方法的分析过程和计算方法，并对特定条件下的系统进行分析
- 涵盖多种系统安全分析方法，包括适用的系统类型、生命周期阶段及基本原理
- 方法多样，包括定性与定量方法，分析过程中可能涉及计算

> 定义
>
> 系统安全分析：采用系统工程的方法和原理，识别影响系统正常运行的各种事件及其可能后果。

- 分析内容：各种事件出现的条件 + 可能产生的后果
- 系统安全分析与风险分析密切相关

安全评价与风险评估的区别

- 上世纪七八十年代美国兴起风险分析和风险评价方法，核电站中称为概率风险分析（PRA）

- 日本引进后称为安全分析和安全评价
- 中国自 80 年代起称为安全评价，后期也有风险评估

注意

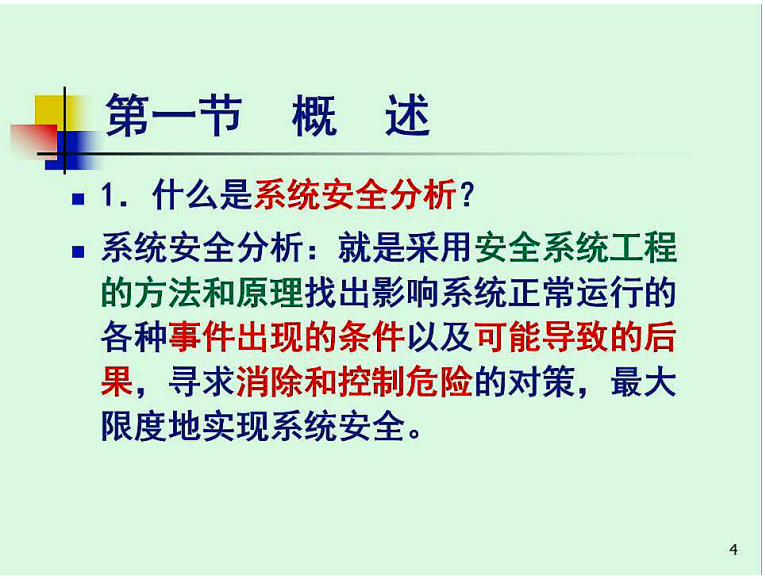
安全评价与风险评估存在明显差异：

- 安全评价：需具备专门知识和资质（安全评价资质），参与人员应为安全评价师和注册安全工程师；中介机构资质需年审和周期性复审，监管严格；人员退休会导致资质人员缺失。
- 风险评估/风险分析：可视为技术咨询，只要得到认可、工作能通过专家认证即可参与，不强制要求资格证书。

例

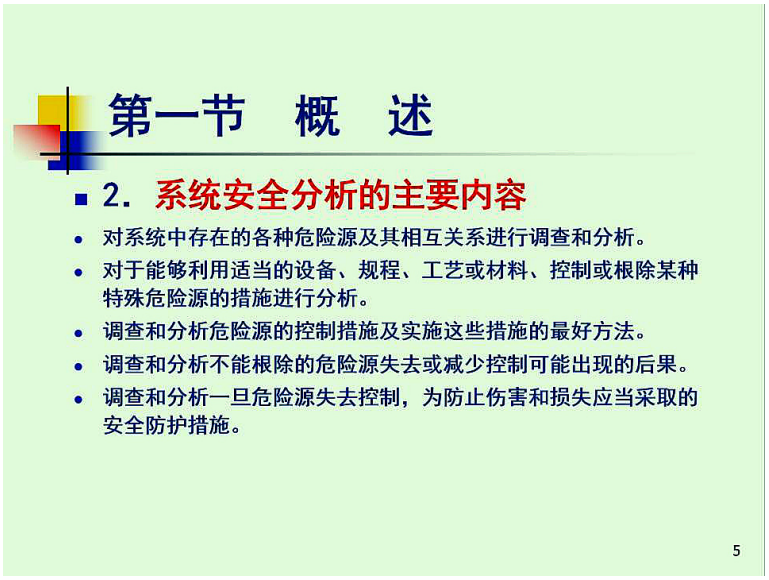
申请中介机构评价资质需具备相应专业人员：矿业领域需矿业安全技术背景人员（本科或研究生学历）；化工企业安全评价需化工过程机械等相关专业本科以上人员，可为安全评价师或化工工艺工程师。

系统安全分析的目的



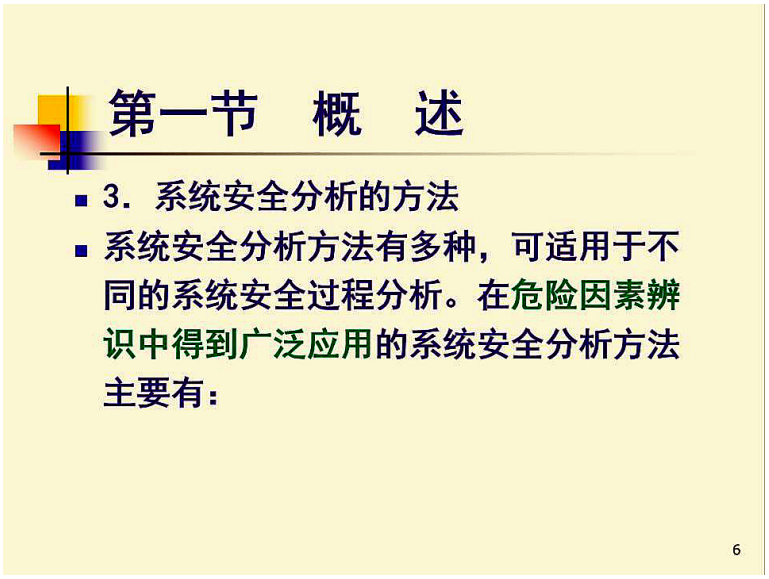
- 目的：实现系统安全
- 实现方式：采用安全系统工程的方法和原理，找出危险出现的条件及其可能后果，寻求消除和控制危险的对策

系统安全分析的主要内容



- 对系统内潜在危险源及其相互关系的调查与分析
- 利用特定设备、规程、工艺或材料控制/消除特定危险源的方法
- 考虑各种危险源之间的相互作用
- 危险源失控时防止伤害和损失的安全防护措施
- 实施措施的方法及应对可能后果的分析

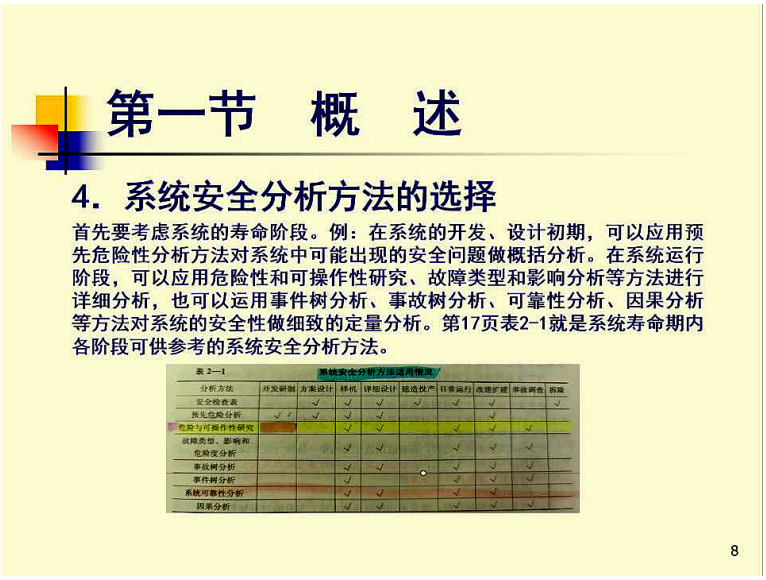
常用系统安全分析方法





- 安全检查表
- 预先危险性分析
- 故障类型和影响分析（FMEA，潜在失效模式及影响分析）
- 危险性和可操作性研究（HAZOP）
- 事件树分析
- 事故树分析（故障树分析）
- 系统可靠性分析
- 因果分析（原因后果分析）

分析方法的选择



- 针对不同分析对象和生命周期阶段，需使用不同方法
- 教材第 17 页表 2-1 列举八种分析方法在不同阶段的应用，后续需掌握

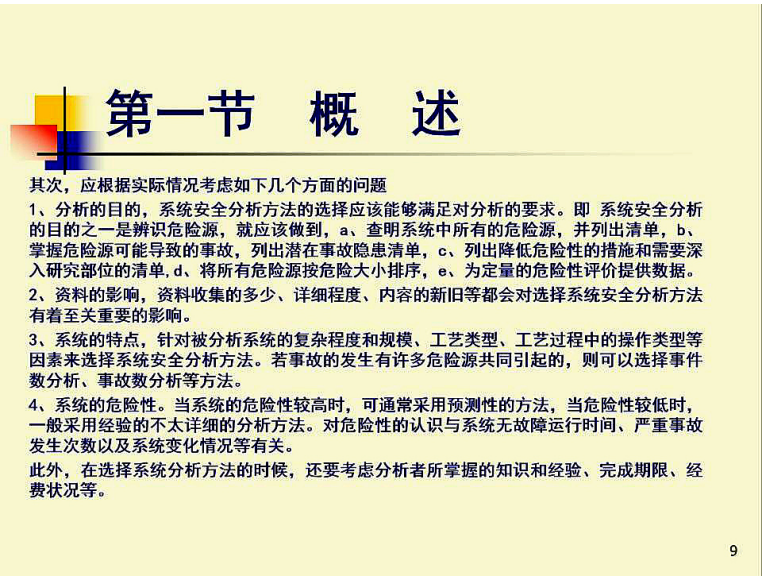
例

不同生命周期阶段的方法应用：

- 研制方案设计：可应用预先危险性分析
- 样机和详细设计阶段：八个风险分析点
- 建成投产后的安全检查表、日常运行的预先危险性分析等环节

- 改建扩建阶段：八个风险分析点
- 研制阶段特别需要进行事故调查
- 拆除环节（如储罐拆除、电厂拆除，最高部分为烟筒）也十分重要

系统安全分析方法的选择依据



- 首要考虑因素是系统的生命周期阶段
- 开发初期和设计初期：运用预先危险性分析（PHA）对潜在安全问题做概略分析
- 运行阶段：采用危险性和可操作性研究(HAZOP)、故障类型和影响分析(FMEA)等进行深入分析

可定量分析的方法

- 八种分析方法中，可定量计算的有：
  - 事件树分析（ETA）
  - 事故树分析（FTA）
  - 可靠性分析
  - 因果分析

安全分析的五个目的

- 辨识危险源：查明系统中所有危险并列出清单，避免遗漏
- 分析危险源可能导致的事故类型，列出潜在事故隐患清单
- 列出降低危险性的措施和需进一步研究的部位清单
- 将所有危险源按危险程度排序
- 为定量危险性评价提供必要数据

定义

安全分析的核心任务是识别危险源，这是首要且并不容易的工作。

危险源识别与生命线工程

- 能源和石化行业（汽油、柴油、煤电、天然气）在危险源识别方面做得较好
- 电、天然气等属于生命线工程，基本由国有企业承担
- 电网波动会导致大面积停电，需在 4 小时内完成应急抢险救援恢复供电，只有

国家层面有能力做到
- 天然气若由民营企业掌控，可能出现供应中断或抬价风险，故以国企为主

例

自来水生产最后一步杀菌通常用氯，少数发达国家用臭氧。氯与叶绿反应生成的氯化氢和次氯酸具有毒性，若叶绿泄漏扩散会引发严重后果。

危险化学品与实验室安全

- 面对两千多种危险化学品，不应简单视为恐怖物质，所有危险物品均受严格监管
- 实验室化学品必须严格按实验室安全管理规定使用和管理

收集资料的内容

- 危险源的数量、内容、新旧程度
- 生产日期、化学属性等详细记录
- MSDS 信息需记录（如新的光刻胶，即使是否属危化品尚不明确也要记录）
- 系统特点：规模、复杂程度、工艺类型、工艺流程操作
- 系统危险性：严重事故、无故障运行时间、严重事故发生次数
- 历史数据、现状及同类企业信息
- 分析人员需考虑的知识、经验、完成期限和经费状况

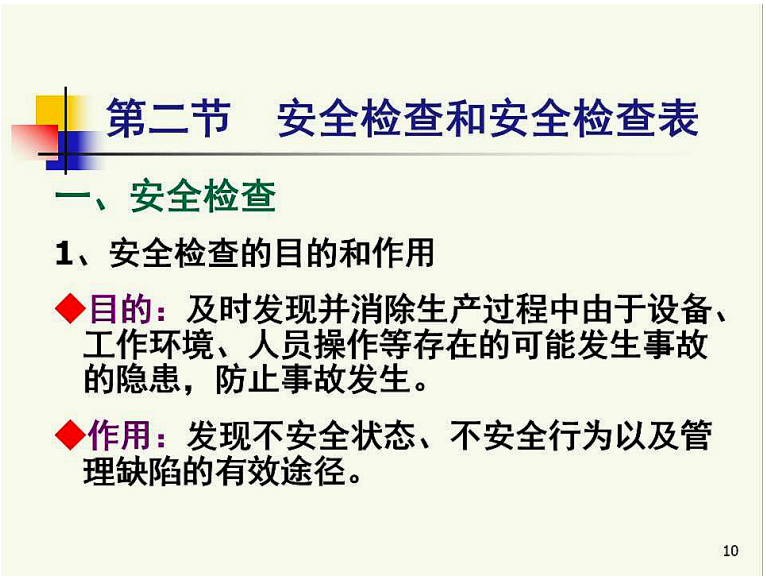
安全检查表法（SCL）概述

- 安全检查表（SCL）是安全检查的一种方式，需定期或周期性进行
- 检查不能随意，检查者需签名负责
- 检查应有明确目的，不能出现”检查了却不执行”的情况

例

水利部门领导分管城市内涝，下雨时不在办公室而在线巡查，发现堵塞或异常立即赶赴现场处理。上级询问时可回答”我在现场，正在巡查”，处理高效。下雨时最严峻的时刻总在一线。

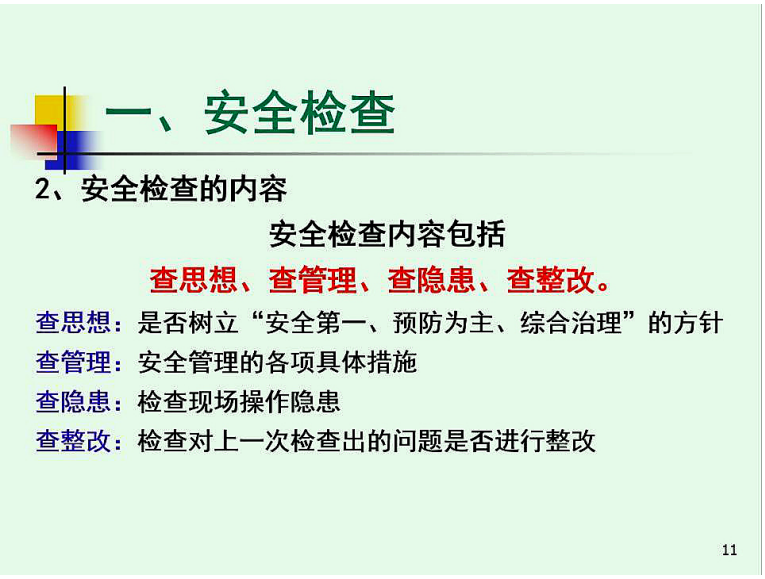
安全检查的目的与作用



- 发现并消除生产过程中设备、环境和人员可能引发事故的隐患

- 发现不安全的状态、不安全的行为以及管理缺陷

检查内容（三个层面）



1. 查思想

- 检查企业是否真正将安全置于首位，是否有”预防为主、综合治理”方针
- 领导人的承诺、培训、检查及应急演练的参与是重要标志
- 关键在领导层态度：是否具备决策层思想，能否在关注企业 3-5 年运营的同时确保安全
- 不能只问是否有政策（企业必然有，因法律法规要求），而要查政策是否真正落实

> **例**
>
> 走进一个企业所感受到的氛围，如同班级的班风学风。若每个同学都精神抖擞，班风一定良好；校风、形象、言行举止、组织乃至口号标语都反映内涵。

2. 查管理的各项具体措施

- 光有制度不够，要查运行机制
- 制度是否执行、执行中是否出现违规、对危险违规行为的处理方式及效果
- 评先评优时是否有”一票否决”、是否有扣分
- 关键在于：是否有制度、运行是否有效、是否见改进和提升

> **例**
>
> 学校有电动车使用手册，规定禁止将电池带入寝室充电、禁止使用电热炉等。但仍有同学违规使用电炉、电热丝。因此不仅要看制度本身，更要关注执行过程。

3. 查隐患

- 隐患指标准的偏离，包括管理及作业场所与法规标准不一致的情况
- 违章就是隐患，如电线老化可能打火，与标准规定大相径庭
- 包括设计规范偏离、管理制度偏离、人的行为偏离
- 通过观察作业过程、查看隐患记录及整改情况、到现场观察

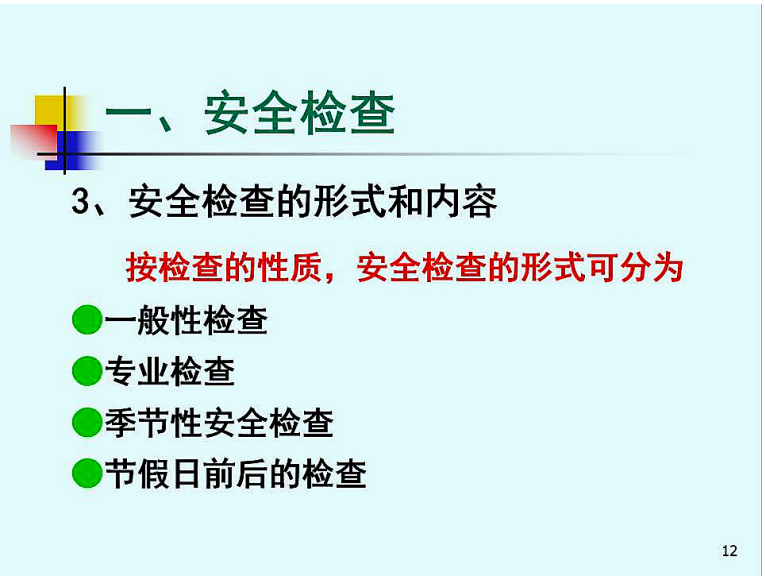
> **注意**
>
> 隐患的整改：每次整改都有相关责任人。重大事故隐患需验收和报备，有些需属地领导带队检查整改是否到位。

四不两直

- 不打招呼、不发通知、不需要陪同，直奔工作现场
- 直接询问现场情况，可检验作业人员素质
- 具备素质的作业人员能借此展现自身能力

> 例
>
> 某些化学品储存环境需保持在 26 度，若遇停电（尤其高温天气）温度会迅速升高引发严重后果。需采用双回路供电：两条线从不同变压器和变电站引来，来自不同母线。化工园区必须配备。

安全检查的形式

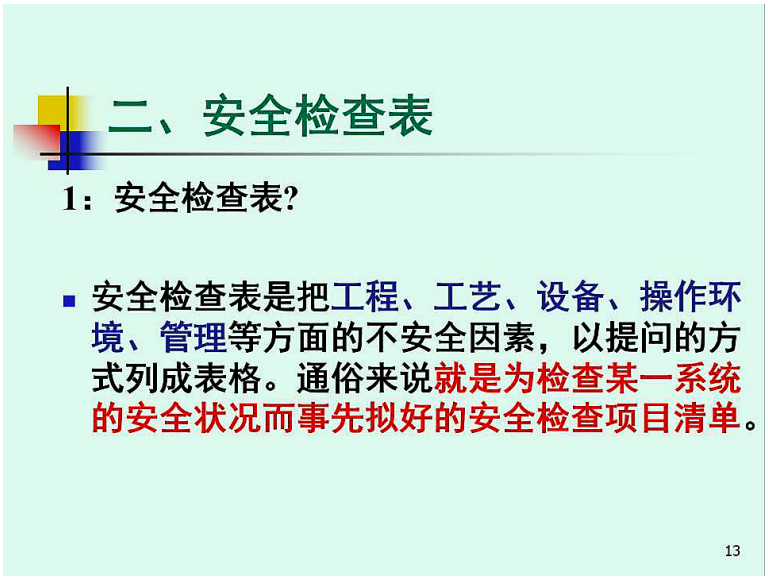


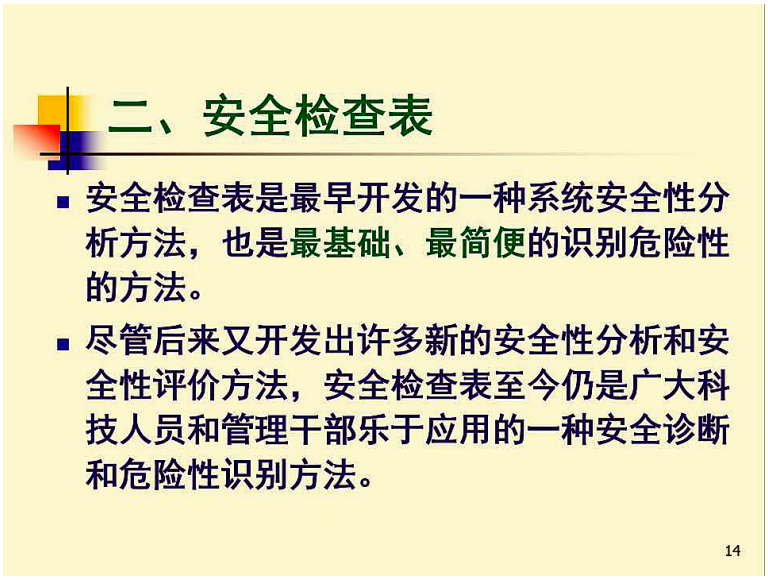
- 一般检查：如学校检查，达到一定程度即可，无需派人到现场
- 智慧监测监控预警：依靠高科技手段，如指挥中心实时显示屏监控人数
- 专项检查：国庆节、台风季节等特定时期
- 专业性检查：针对特定设备，如电梯、游乐设施、启动设备、压力容器和管道、场内运输车辆、叉车等特种设备
- 季节性检查：国庆等节假日、春夏秋冬四季交替、春节、台风季、夏季高温、秋季干燥，不同季节检查表内容不同

> 例
>
> 深圳一家生产空调的外资企业一个月内死亡三人：一人触电（临时用电最易触电）、一人被堆垛倒塌砸中、一人被集装箱内压缩重物砸中。当时缺乏相应标准和规范，群死群伤事故较常见。

> 例
>
> 高铁紧急刹车自动盘的寿命预测是重要研究方向。制动盘为铸铁制成，刹车片由合金钢、硬质合金或钢钛制成。速度过高会导致制动盘刹车时因热变形，需定期更换，如同汽车定期更换刹车片。

安全检查表（SCL）的定义与特点





定义

安全检查表（SCL）是把工艺、设备、操作环节、管理等各方面的不安全因素，以提问的方式列成表格，即事先拟好的安全检查项目清单，用于检查某一系统的安全状况。

- 检查表列出从大到小、从技术到装备到管理等各方面的项目
- 涵盖工艺、设备、操作、环境、管理等方面，若只看到部分则检查不全
- 是系统安全分析中最基础、最简便的识别危险性方法
- 被广泛采用，几乎人人能掌握，是乐于应用的安全诊断和危险性识别方法
- 没有统一格式，可自行设计，可加备注、检查人、检查时间等列
- 签名即负责：要么整改掉，要么进行 PDCA 循环，不能将问题遗漏

注意

检查发现问题必须明确指出。许多领导采取更精明的方式：组织专家团队，自己不直接参与检查，而是担任领队、组织者和协调人，参考专家意见。

安全检查表的编制依据与格式



- 从制度层面制定并更新规范标准，如《易燃易爆商品储藏养护技术条件》
- 最佳实践：将检查项目直接写入表格，并在备注栏注明标准来源
- 法规和标准每隔几年修订一次，检查表需随之更新
- 安全管理层分析检查表：项目内容、依据、备注齐全，但需注意责任人的落实

> 注意
>
> 现在做任何事情都必须考虑责任问题，检查表不能没有责任人。谁检查谁负责，专家签名同样要负责。

灭火器与初期火灾防控

- 灭火器能在初期火灾阶段发挥关键作用，防止火势扩大造成重大损失
- 一旦动用消火栓，说明火势已发展到较严重阶段
- 教室课桌等属于可燃物而非易燃物，需明确区分

配电室与照明设施检查

- 潮湿天气下配电室检查尤为重要，需特别注意防水措施
- 确保电线不会因浸泡而漏电
- 配置周围警示标识，告知人员有电危险

> 注意
>
> 照明设施检查的核心是防水与防漏电，这是潮湿地区配电安全的关键。

商场等人员密集场所的安全

- 商场即使非初期阶段发生事故，也会面临重大影响
- 一旦发生问题，可能需关闭整改，直接影响商家运营
- 人员密集场所（如东站、天河城）一旦发生事故，极易拥挤混乱

聚氨酯泡沫火灾事故案例

- 本市事故调查：六七人并非被火烧死，而是被熏死（吸入有毒气体窒息）
- 受害者所在空间四壁及顶面均覆盖聚氨酯泡沫用于保温
- 为使聚氨酯附着，部分区域添加了钢丝加固

例

仓库面积超过教学楼，业主将工程层层分包。拆除时发现仓库内有钢丝可卖钱，找来废品回收师傅。师傅到现场一看，发现作业缺乏安全保障，拒绝接收废品并录制视频留证。老板乘电梯从一楼到二楼，电梯门打开时发现三人已因吸入有毒气体晕厥在电梯门口。后续实验证实，相距 7 米处使用气割即可轻易点燃这些气体。

注意

聚氨酯泡沫燃烧产生的有毒气体是致命主因，而非明火本身。国家对动火作业要求非常严格，涉及明火的场所应尽量避免参与。

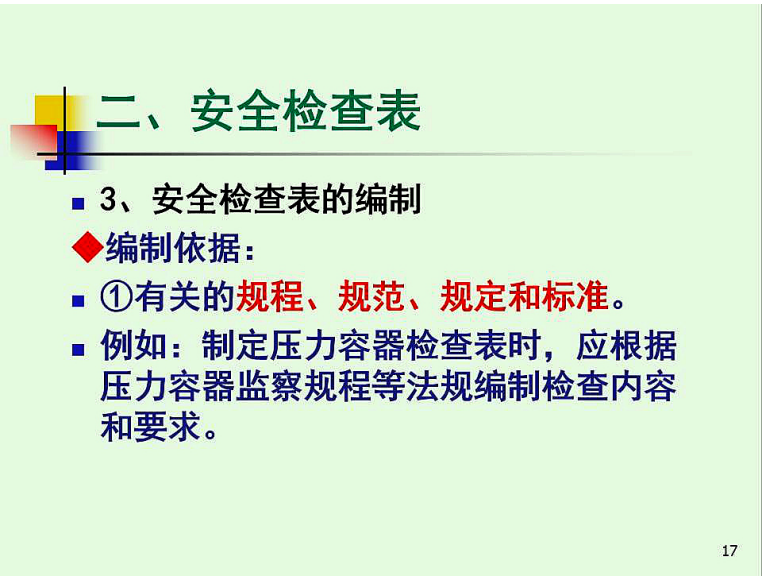
事故性质认定：消防事故与安全生产事故

- 该事故起因是消防问题（火灾导致有毒气体产生，使人窒息而亡）
- 涉及消防导致的死亡，应归类为安全生产事故，但责任主体和消防部分是明确的
- 事故调查属于应急督导范畴，由安委会的安委办设在应急管理室

注意

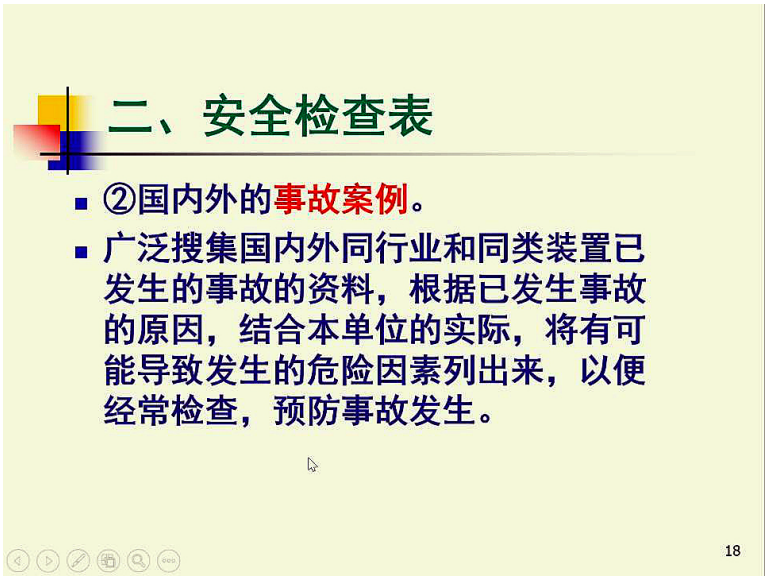
千万不能混淆消防事故与安全生产事故，两条线的责任认定是不一样的。

安全检查表的编制方法



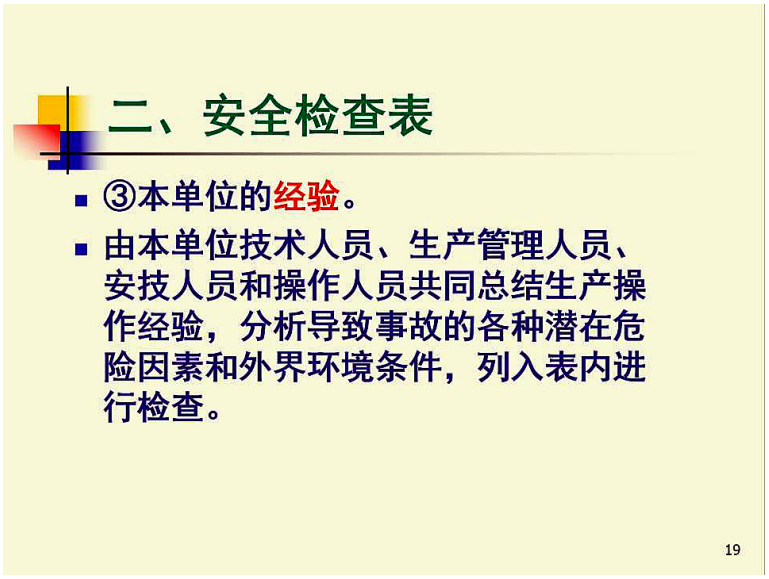
- 主要依据相关规程、规范和标准，避免遗漏任何一项
- 可参考现有网上资源，规范标准通常包含在相关标准库中
- 压力容器检查表是根据监察规程编制的

国内外事故案例学习



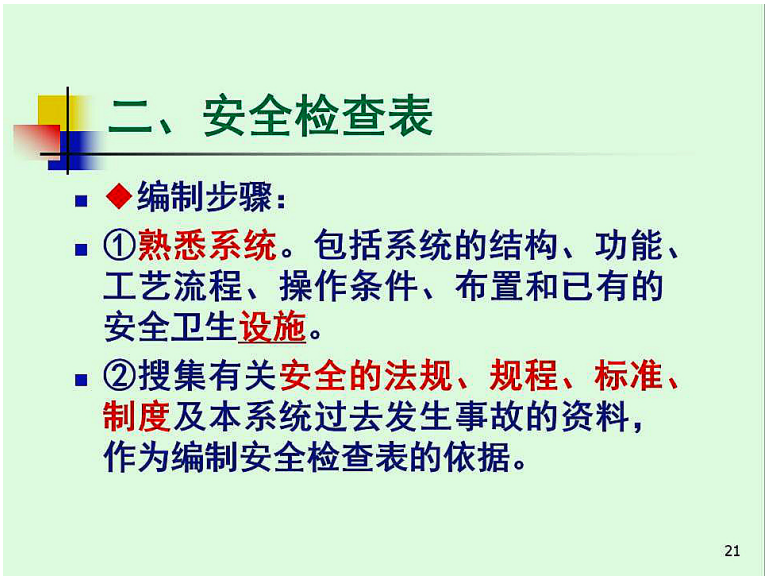
- 广泛学习国内外典型事故案例，很多新业态在国外已有先例
- 如液氢：国外电动车已广泛应用，航空领域使用液氢没有问题（不计成本保证安全）
- 国内民用领域液氢安全使用仍需努力

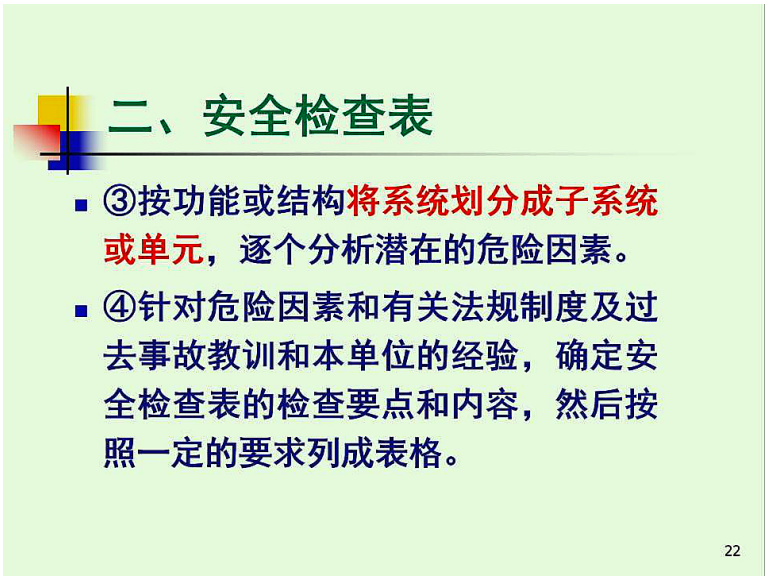
本单位实践经验的重要性



- 操作经验需被分享并记录在案，通过集体讨论优化、删减和增补
- 系统安全分析方法得出的结果（如事故树分析中最小割集）应整理到安全表中
- 确保这些事件不会发生，一旦发生可能 90 天内就会发生

编制检查表的步骤



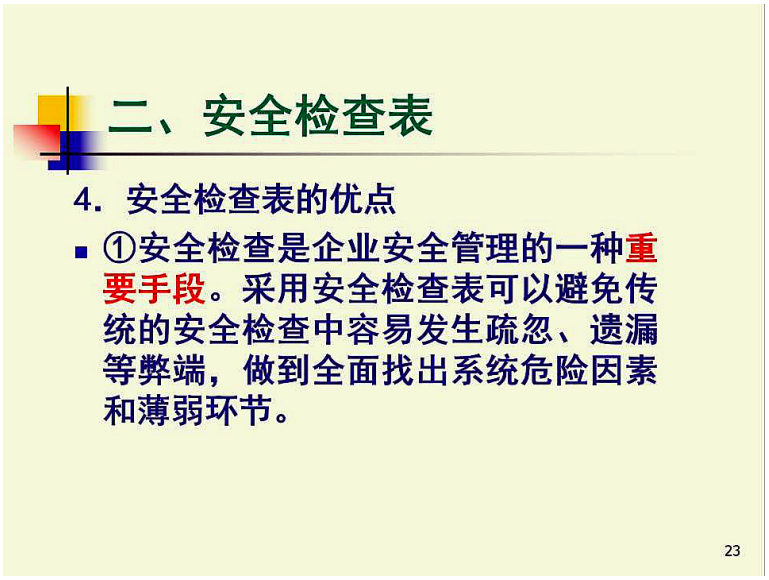


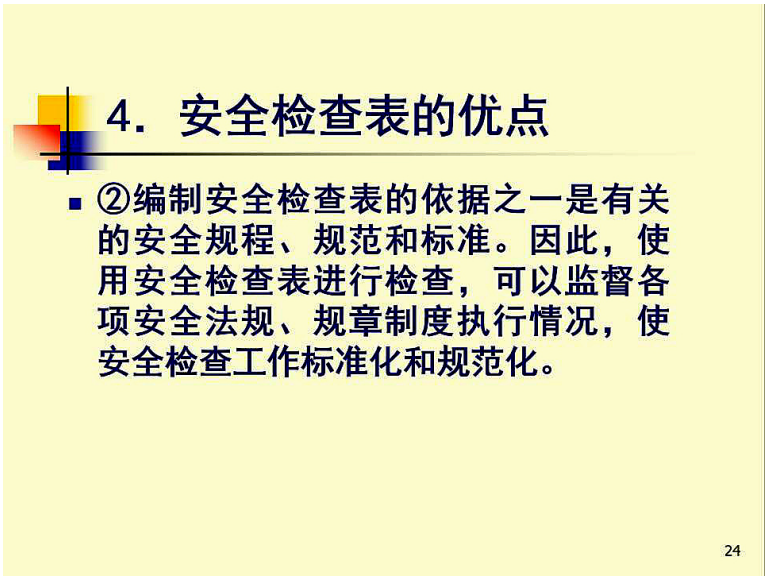
1. 熟悉系统：了解结构、功能、工艺流程图、操作条件布置和现有安全卫生设施
2. 收集安全相关法规、规程、标准和制度，以及本系统过去发生事故的资料
3. 将检查对象划分为子系统或单元，逐个进行分析
4. 将法规制度、经验教训及本单位经验融合，形成检查表格

注意

切勿认为自己刚入职两年、天天在机场工作就局限于此。基础不牢，对特殊状况缺乏了解，就不知道如何进行应急处理。

安全检查表的特点与适用范围



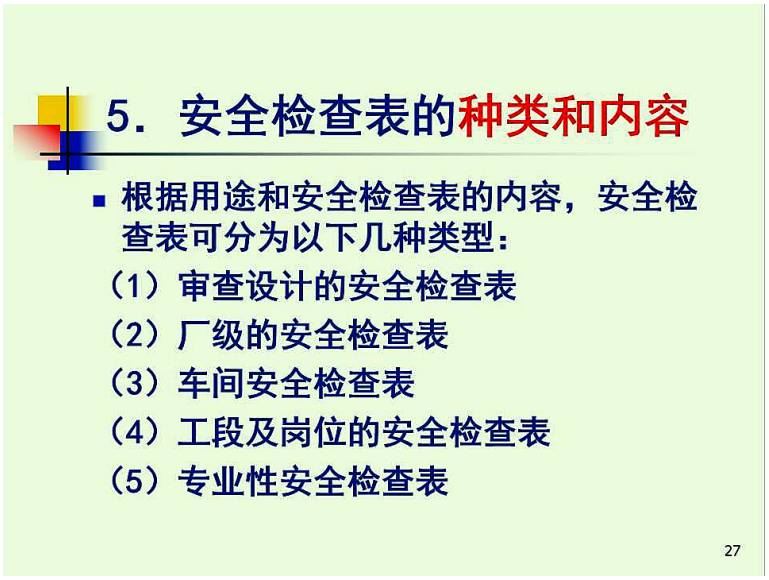


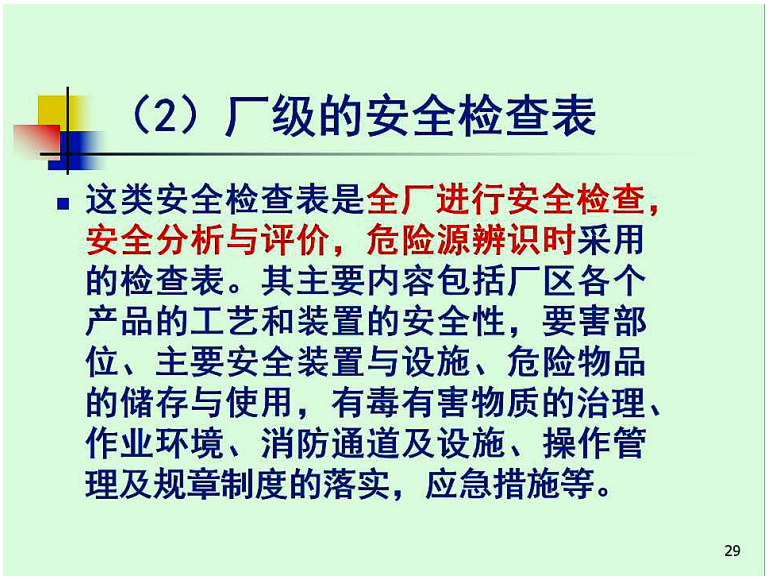
- 优点：系统性强、容易找到答案、涵盖相关安全规程标准和规范
- 不同检查对象会有不同的检查表
- 形式简洁明了，易于理解与执行
- 为检查人员提供履行职责的证据，有助于尽职免责

注意

检查表几乎涵盖所有方面，但事故调查和开发研究两个领域不适合使用，因为缺乏明确的主体和具体对象。

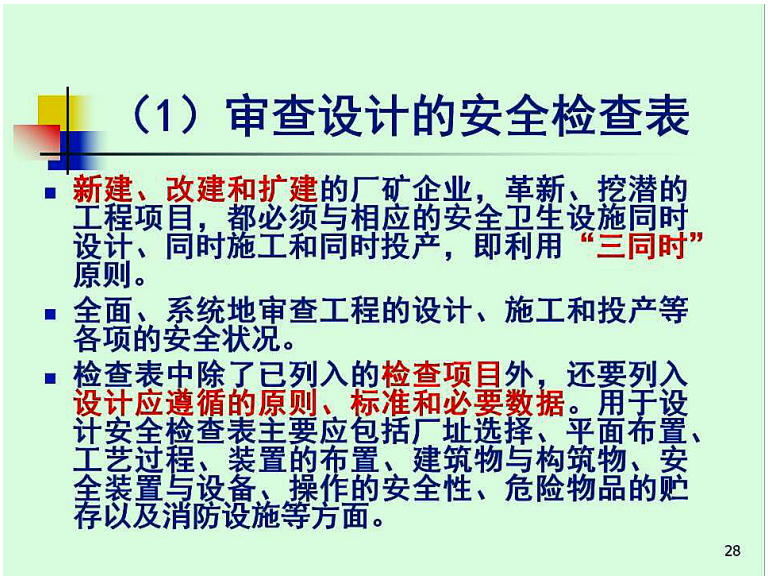
安全检查表在各层面的应用





- 工厂整体运行层面：履行相应的安全检查
- 车间层面：关注工段岗位的安全检查表
- 每个岗位确保安全，整个车间乃至工厂才能稳定运行

设计审查与新建项目



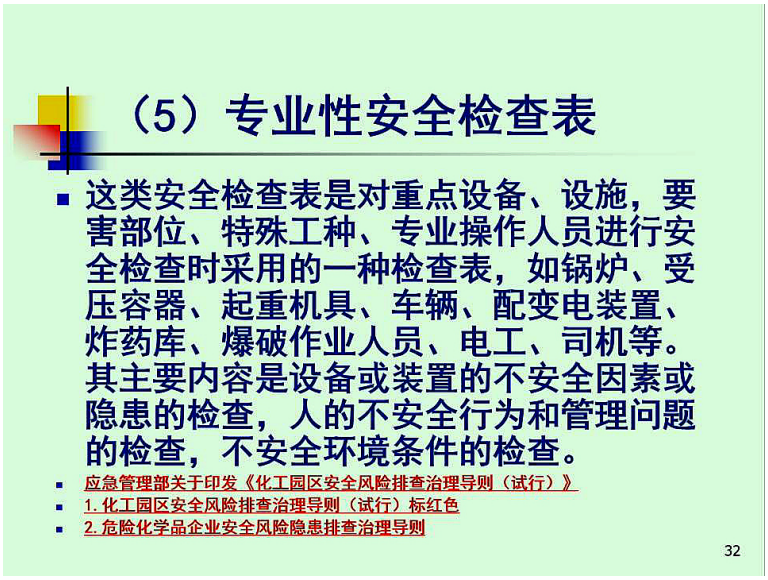
- 新改扩建项目要遵循一定的原则和标准
- 大型石化企业普遍采用安全检查表进行设计，包括工艺流程是否合理
- 在设计、施工、投产等环节，除具体检查项目外，还需遵循原则标准和必要授权
- 需对整个厂区进行安全检查、安全分析评价以及风险辨识

机械厂清洗事故案例

- 佛山某机械厂在元旦前一天发生严重事故，造成十多人丧生
- 车间清洗维修时使用天那水溶解地面油污，天那水在暗沟中挥发成气体
- 气体与空气混合形成爆炸性混合物，动火作业火星引发爆炸

> 例
>
> 清洗车间地面油污时使用天那水，溶解后的天那水在车间旁暗沟中挥发，与空气混合形成爆炸性混合物。此时若有动火作业，火星接触即引发爆炸。临近元旦假期是事故发生的可能原因之一。

工艺装置要害部位检查

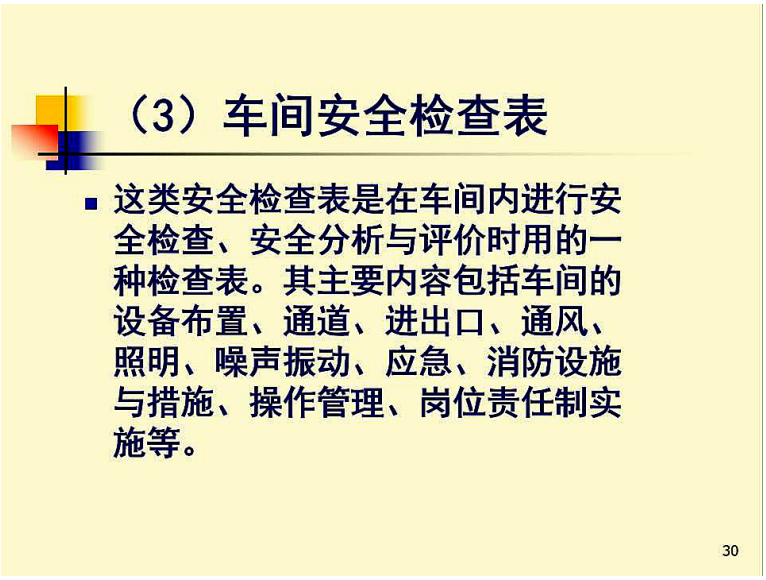


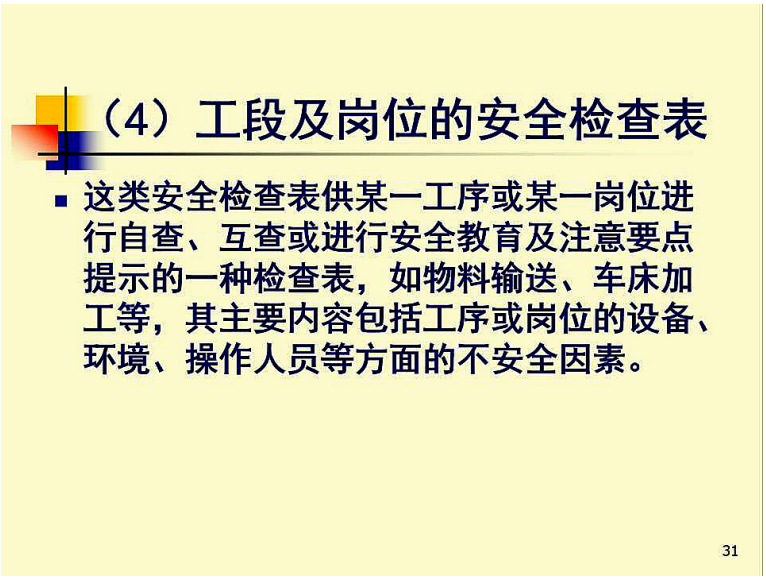
- 主要装置、危险物品储存罐、有毒有害物质治理作业环境

- 消防通道、操作管理以及应急措施

> **注意**
>
> 消防通道千万不要堵塞，很多严重事故源于简单的人为疏忽。

车间检查内容





- 设备布置：风道、进出风口、通风、照明、噪声控制、振动防护、应急消防设施
- 操作管理岗位责任制：车间主任对车间负责，工段和岗位逐级落实
- 自查复查、自学互学互纠、互助互帮

> **例**
>
> 良好的企业氛围下，岗位操作人员应互相支持、互相关心、互相照顾、互相帮助、互相提醒，而非只管自己的操作。

化工园区安全风险排查治理

- 依据《化工园区安全风险排查治理导则》，详细说明依据、适用范围和原则
- 化工园区按千亿级以上规模布局，如惠州大亚湾石化园区（全国最大之一）
- 揭阳建有中石油广东石油分公司产业园

化工园区配套设施要求

- 智能化程度高，人员撤离有保障
- 配备天然水体、消防取水点、消防车道和取水码头
- 危险化学品车辆聚集区域应建立专门停车场，实行封闭式管理
- 管理机构应配备具有化工专业背景的负责人
- 建立由化工专业人员或注册安全工程师领导带班的制度
- 安全监管人员中至少 75% 具有化工专业学历或化工安全生产实践经历

> **注意**
>
> 化工园区评分低于及格线将直接取消设立资格，园区内企业禁止新建、改建或扩建，基本失去发展空间。

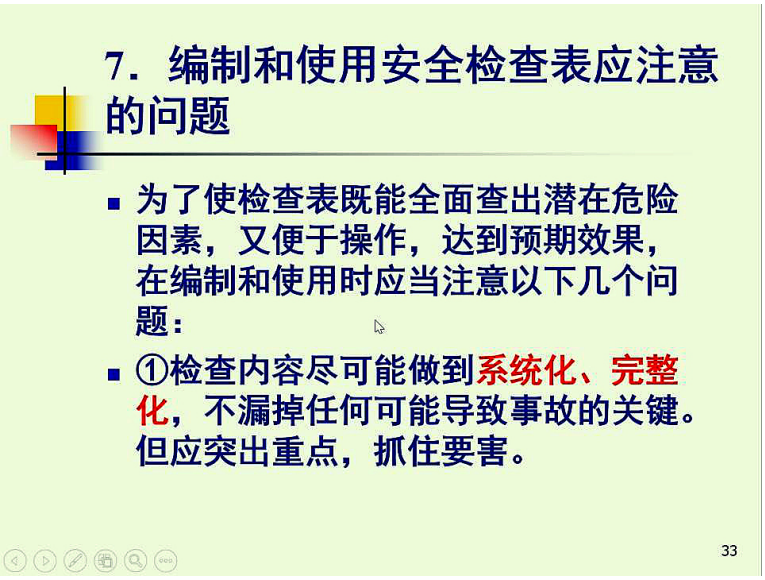
化工园区信息管理系统

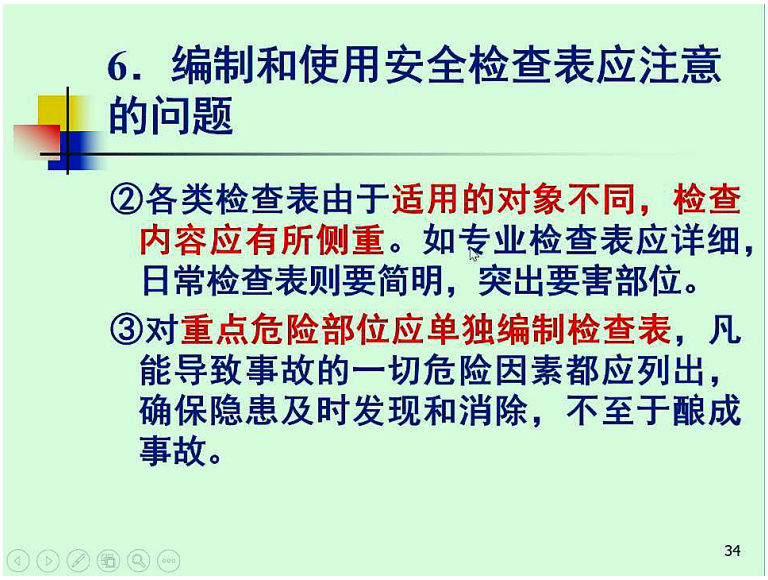
- 构建基础信息顾问、风险隐患库等
- 园区倾斜三维摄影等属于信息管理系统
- 当前工作包括：智慧化工园区风险评估、量化评估、自然灾害耦合情况下的风险评估、化工园区韧性建设、多米诺效应评估

化工园区检查表评分

- 排查项目每个 15 分，评分标准为 0-15-0-5
- 检查表有大约八十几个标准作为支撑，另有国家政策法规支撑
- 实行一企一档、一园一策

编制和使用检查表的注意事项

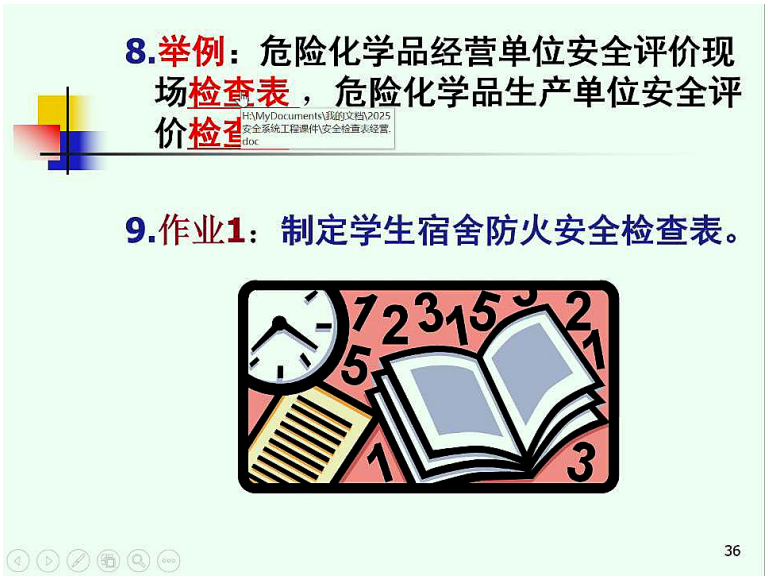




- 系统化和完整性是必须的
- 使用对象不同，检查内容需有所侧重
- 重点部位应单独编制
- 不能模棱两可，定义需要明确
- 清晰表述项目，以及工艺改造和设备变更的影响
- 完成检查后签字以明确责任

> 注意
>
> 学术论文和工作通知的撰写是完全不同的套路。即使博士毕业，到应急厅也需从头学习处理事务、起草文件和与下属沟通。

危险化学品经营与生产单位安全评价



- 危险化学品经营单位安全现场安全评价检查表
- 危险化学品生产单位评价表
- 两者均需依据相关规程规范编制

作业与考试安排

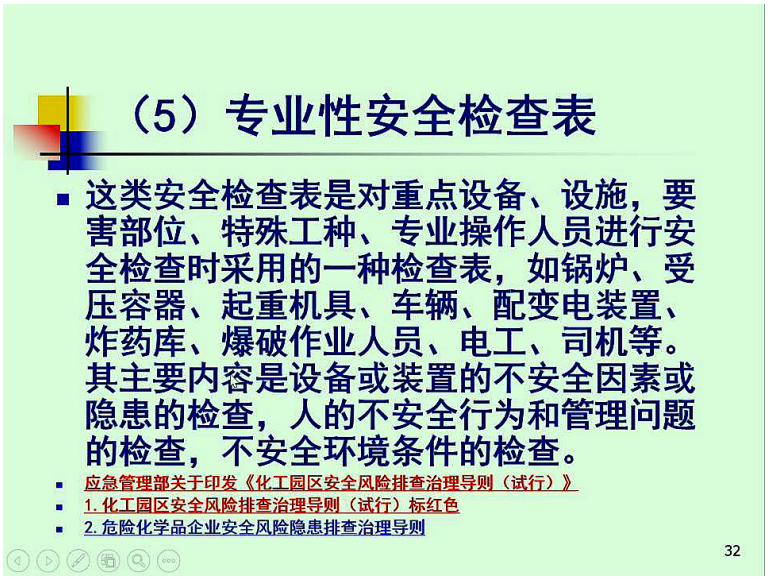
- 作业：火灾安全检查表，自行查看并完成，按讨论顺序进行，如有变更需重新排列提交
- 课程结束后一周进行考试，需平时多加用心

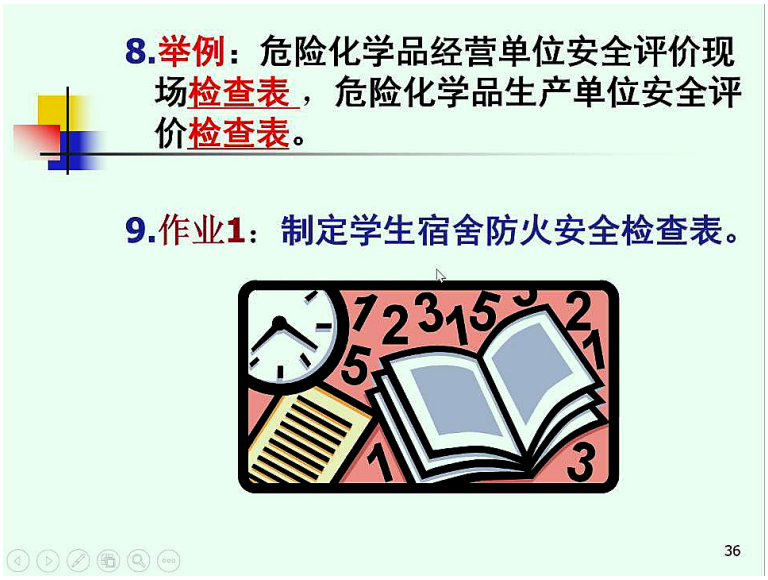
09 月 29 日

安全检查

- 安全检查是及时发现群众采集安全行为的有效途径，也是消除事故隐患的重要方法
- 检查要素包括：思想、隐患、管理、整改
- 检查内容需结合环境、设备、管理及人员状态，以及软性方面（如文化建设）形成系统

安全检查表





- 根据相关安全规范和标准制定
- 是最常用、简洁、直观、易掌握且有效的检查方法
- 能够明确责任，落实每一项法律法规标准要求

- 编制时应从危险有害因素分析开始，结合设计、日常管理及同类事故经验教训

例

宿舍安装防火墙时，需考虑的危险源包括：明火、消防通道畅通、消防指示标识、疏散方向及集结点指示、消防救援设施完备、定期消防演练等。

系统安全分析方法概述

- 系统安全分析方法涵盖约九个方面，均有标准的中英文名称
- 方法与系统所处的生命周期阶段（九个阶段）相关，不同阶段可采用不同分析方法
- 常见方法包括：安全检查表、工作危害分析（JHA）、故障类型和影响分析（FMEA）、危险和可操作性分析、风险矩阵、作业条件危险性分析等

注意

中文名称若不准确，应以对应的标准英文名称为准。

化工园区安全管理体系

- 参考《危险化学品企业安全风险隐患排查治理导则》，企业无需另行编制，应将相关要素融入自身管理
- 企业是安全风险隐患治理的主体，需落实主体责任
- 该体系由华东理工大学一位教授提出，用于协助发展和管理部进行有效管理

两重点一重大

- 重点监管的危险化学品
- 重点监管的危险化工工艺（涉及化学反应原理的流程）
- 重大危险源
- 精细化工企业也有相应监管要求
- 检查时需注意工艺设备、电气仪表、储运、消防公用工程等方面，并关注春季、秋季、冬季及重点时段、节假日的监管变化

化工园区发展与智慧化

- 广东省化工园区数量从 54 家缩减至约 23 家
- 智慧化工园区逐步发展为智慧智能自动化的办公园区，并有相应认定标准
- 中国化学石油化工协会每年公布评审结果
- 惠州大亚湾经济技术开发区、惠阳等园区经济规模位列全国前茅，产值达数千亿
- 园区发展吸引大量专业人才，待遇提升

例

上海化学工业区曾是中国最大化工基地，在发生人员伤亡事故后被广东化工区取代。目前上海化学工业区和上海石化工业园区并列第一。

乙烯产业与化工安全

- 乙烯是化工石化行业的重要产品，食品级塑料袋基本由聚乙烯制成
- 氯乙烯、聚氯乙烯、聚乙烯均由乙烯单体合成、聚合或添加后制成
- 化工行业并非”谈虎色变”，关键在于有效管理

园区风险隐患排查审计

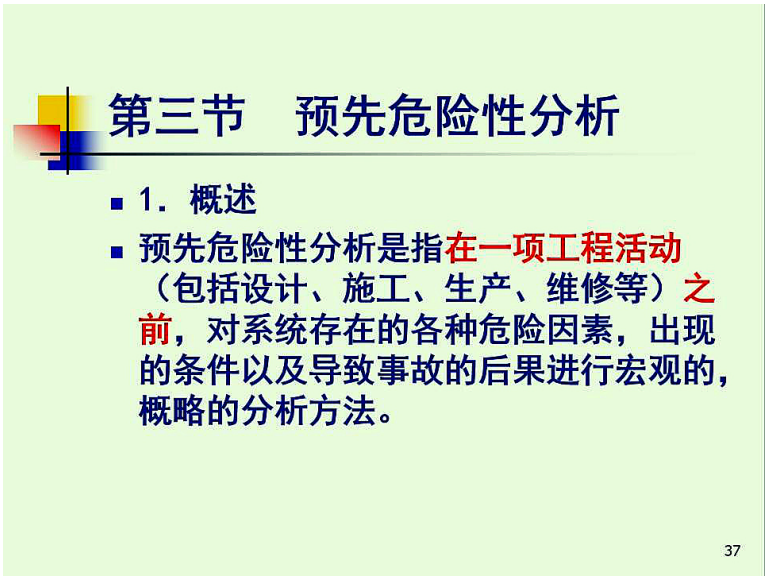
- 2019 年对 50 多个园区进行全面风险隐患排查，对照 80 多个标准规范逐项打分
- 首次审计后，第二轮审计每三年进行一次
- 2021 年对全省油气储存基地进行全面审计（涉及约十几家企业）
- 成品油行业高风险高利润，需落实安全市场责任制

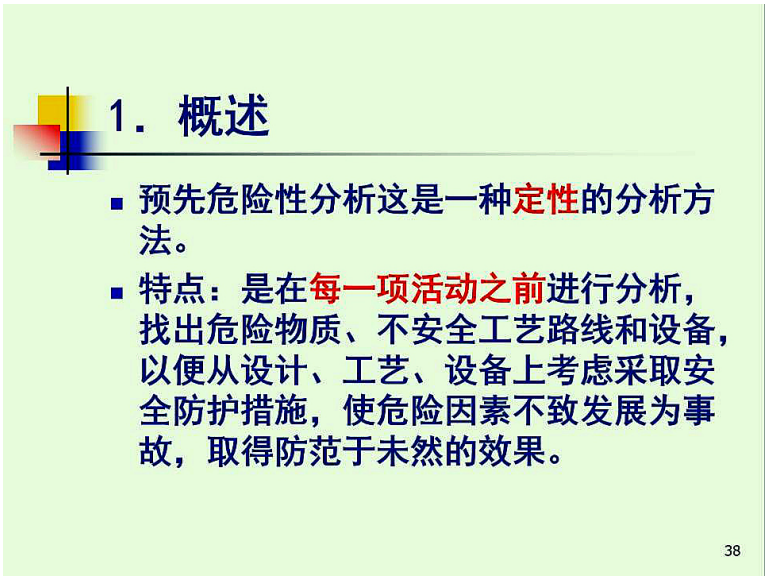
安全生产信息化管理

- 实现人人有责，在每个环节实施安全生产信息化管理
- 信息化管理不仅是使用 Excel 或编制文件夹，较好的企业已通过局域网进行信息化管理
- 使用评价表对每个要素进行评分

> 注意
>
> 不要将简单的 Excel 文件管理误认为信息化管理，真正的信息化管理需要系统化的平台支撑。

预先危险性分析（PHA）





定义

预先危险性分析（Preliminary Hazard Analysis, PHA）是指在进行一项工程活动之前，对工程活动中可能存在的各种危险因素、出现条件以及由此导致的后果进行预先的识别和分析，以评估风险。

- 涉及对风险及风险因素进行宏观的概率分析
- 工程活动主要包括设计、施工、生产、维修等方面
- 适用于新开发、研制、方案设计、样机详细设计、新建、改建、扩建等过程中固有、潜在的危险危害（共七个阶段）
- 属于定性分析方法

注意

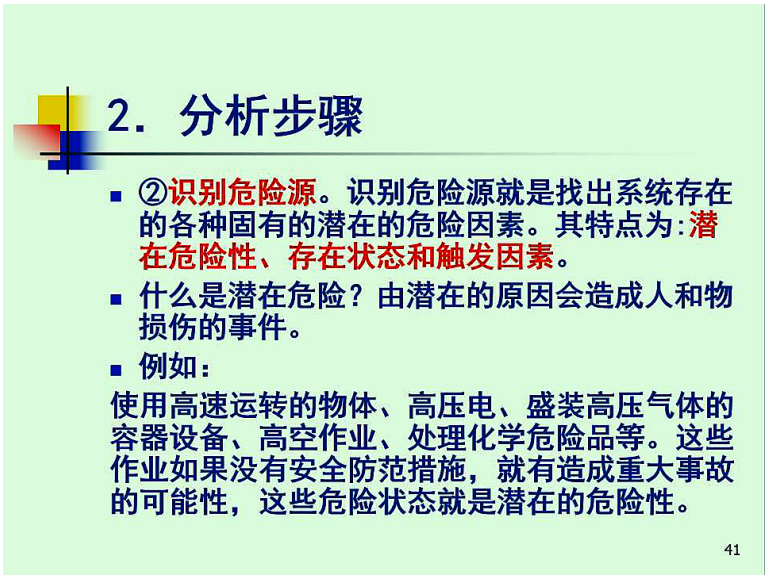
安全检查表是定性的，而系统危险性分析方法是定量的。考试中常以判断或选择题形式考查此区别。

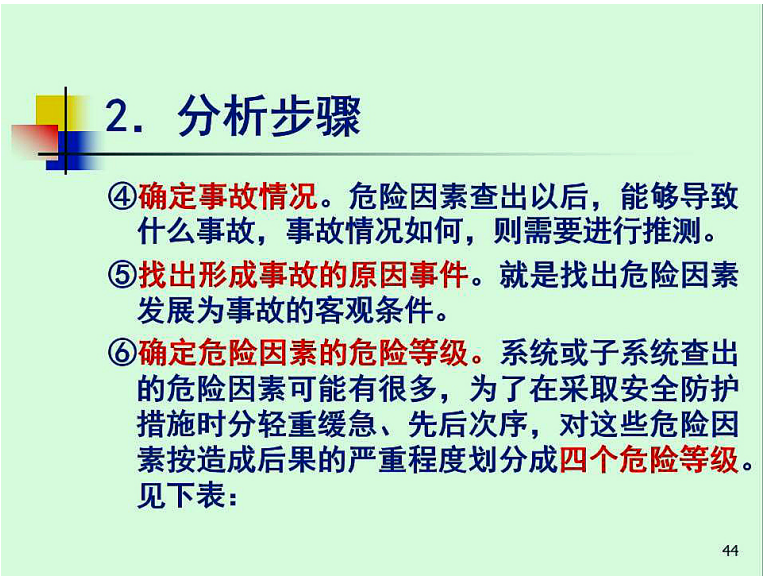
定义

预先危险性分析（PHA）是一种在项目设计、新建或工程实施之前进行的风险评估方法。

- 要求分析人员具备一定的能力和背景，含金量很高
- 专家通过桌面推演分析应急演练，利用态势感知预测可能的事故情况
- 目标是识别事故发生的链条，找出根源，采取措施切断链条以防止事故发生
- 情况复杂时采用分布式锻炼减灾策略

预先危险性分析的步骤





1. 熟悉系统：包括目的、工艺流程、操作条件、设备结构、管理状态，以及同类装置或设备以往事故的资料
2. 识别危险源：危险源具有潜在危险性，特征在于其存在状态和触发条件
3. 分析后果：考虑财产损失、人员伤亡、任务未能完成的可能性，以及能量转移和环境因素的影响

例

自来水处理工艺中，投药（氯化物）环节存在氯气泄露、过量添加或剂量不足的风险。将设备置于蓄水池旁时，需在设计工艺流程时考虑这些潜在风险。

例

广州大道旁芒果树，有人夜间摘芒果滑倒，后脑磕在石凳上。此类行为往往因缺乏危险意识而发生，属于未识别潜在危险源的情况。

危险源的潜在性

- 危险源具有潜在危险性，其特征是存在状态和触发条件
- 目前危险源状态可控，但若在工艺中不注意，就可能引发事故
- 潜在危险性指潜在的造成人或物损伤的事件
- 共性：含有能量（如旋转物体、高压电、高压气体容器设备、高空作业等）

注意

危险源辨识需要分析人员具备丰富的知识和经验，尤其是实践经验。系统过于复杂时，不能仅从系统角度解释，否则可能忽略其他重要因素。

危险有害因素辨识能力

- 基本技能之一：具备危险有害因素辨识分析的能力
- 辨识方法将在后续内容中讲解
- 分析对象的所有危险因素识别是难点所在

复杂大系统的动态平衡

- 复杂大系统包含子系统，子系统之间、内部及要素均与外界进行能量、物质和信息交换
- 若无外力约束，系统必然打破平衡，这是熵增与耗散的结果

- 班级若无组织管理，熵增加，平衡被打破
- 必须做出一定付出以维持动态平衡，系统本身也在学习和成长

定义

动态平衡：系统在熵增趋势下，通过外部约束和持续付出维持的一种相对稳定状态。

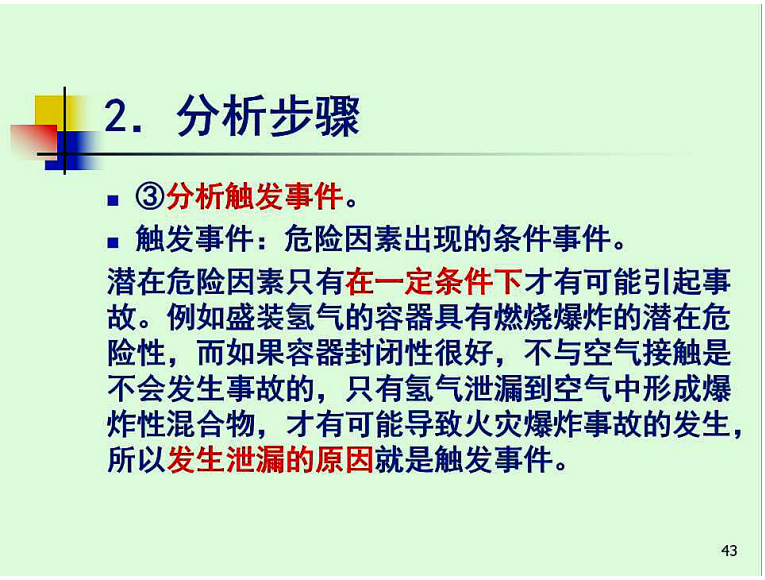
注意

动态平衡意味着存在动态风险，而动态风险比静态风险更难把控。因此研究中常提到”动态风险的态势感知”。

例

进入教室并不意味着没有风险，而是风险可控。石化企业人员需经过严格多级培训、经常接受教育，才能熟练进行电子操作、监控和预警。

触发事件与潜在危险因素



- 正常情况下不会出现问题，但一旦触发可能导致严重后果
- 许多触发条件无法预先预见，甚至超出想象
- 潜在危险因素只有在特定条件下才可能引发事故

例

爬梯子事故：工人为图方便，不从梯子一步步走，而是跳到洞的盖子上再跳下，脚下一滑，头碰到盖子导致悲剧。本可按正常作业过程安全完成，却因”偏坡”引发事故。

例

装有氢气的容器具有燃烧和爆炸的潜在危险性。

氢气的安全利用与储氢技术

- 氢气是很好的能源，可充分利用光能、风能、潮汐能（如海上风电）电解水制氢
- 海上风电机组可置于旋转平台上，无论风向如何始终正对风向
- 氢气的安全利用受爆炸极限限制

注意

氢气爆炸下限较低、上限较高、爆炸范围较宽，即便是极小的点火能量也能引发爆炸。这限制了氢气的安全利用，目前研究重点在储氢技术。

- 储氢涉及压缩储存于燃料电池中产生电力或热能
- 储氢设备需具备良好密封性
- 储氢过程中存在氢脆、氢鼓泡、氢渗透等问题
- 氢气对特定金属的相容性要好，才能用作储气材料
- 目前采用液氢作为储运介质，但液氢生产规模尚未达到大规模生产

注意

液氢需经过组装、运输、目的地再分配使用，且必须经过气化过程才能使用。航空航天领域直接使用液氢液氧不计成本，但必须确保安全性；民用方面则有记录限制。

乙炔气瓶的安全隐患

- 企业中使用乙炔气体进行气焊、气割金属或加热操作
- 乙炔气瓶输出管子（枪头部分）密封性不佳，有时导致火灾隐患
- 盖子被误认为安全遮盖物盖住后，第二天员工操作时枪头与地面摩擦产生火花

注意

移动的危险源是安全检查中必须注意的危险因素。乙炔问题并非仅此一次，而是反复出现。

事故场景与事故情景

- 危险因素出现并不必然导致事故，而是在特定危险环境下可能发生的事件及其后果
- 预防潜在事故是必要的

例

液氯泄漏：氯气扩散并在蒸发过程中进一步扩散，随风飘散，可能在一定区域造成人员中毒。叶绿素被破坏，受影响区域植被由绿转黄直至枯萎，草地、地下洞穴中的生物无一幸免。

例

作为”工业医生”，到达现场可帮助诊断制度、管理、人员、设备设施、工艺及仪器仪表等方面的问题，从而避免事故发生。

PHA 的危险等级划分

- 危险等级按照事故发生后果的严重程度来划分

注意

危险等级（PHA）按事故后果严重程度划分，而风险等级通常按风险大小划分，两者不同，需区分记忆。

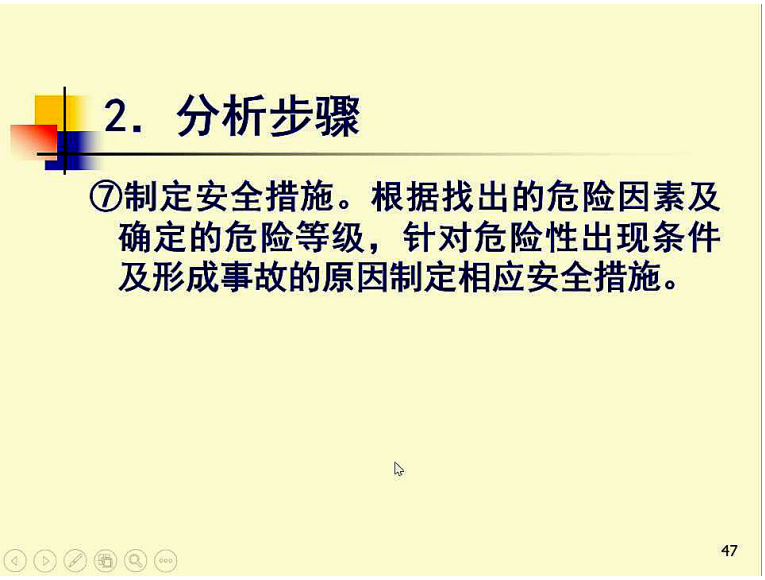
- 安全等级：尚不能造成事故
- 临界等级：处于事故边缘状态，暂时不会造成人员伤亡和财产损失，应予排除或采取措施
- 危险等级：必然会造成人员伤亡和财产损失，要立即采取措施

- 灾难性等级：后果最为严重

事故发生的可能性分级

- A 级：频繁发生
- B 级：相当可能发生，在设备使用寿命周期内出现过几次
- C 级：偶尔发生，在设备使用寿命期内有可能出现
- D 级：很少发生
- E 级：发生概率接近于零，几乎不可能发生

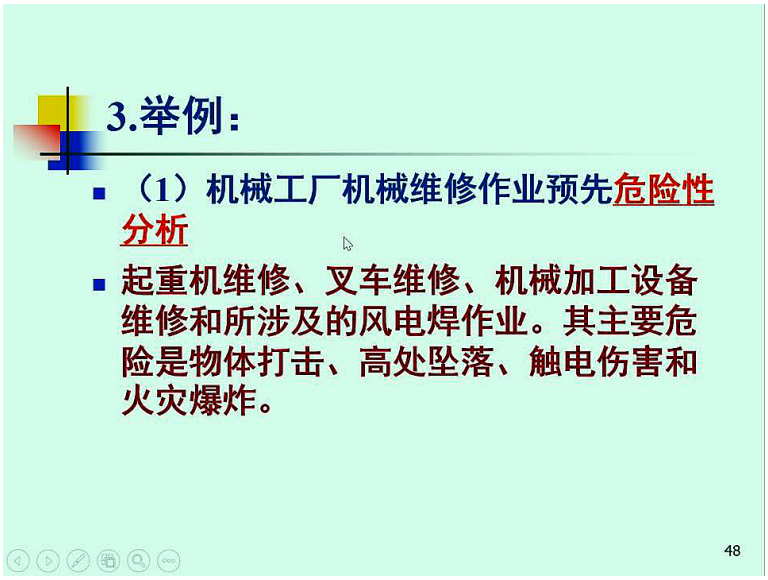
制定防范措施



- 制定措施有两个方面：降低风险发生的可能性、降低事故后果
- 重点在于尽量避免事故的发生
- 有时降低事故发生的可能性成本很高，若后果不严重，可接受风险并采取防护和隔离措施

> **例**
>
> 如需接近患者，应穿戴 PPE（个人防护装备）。

机修厂维修作业预先危险性分析



- 机修厂是航空维修中的重要环节
- 飞机维修需自行查找资料，是严格过程，缺失或多余螺丝都可能导致重新拆装
- 风险特性：发生可能性低但后果严重，风险管控重视程度高
- 涉及起重机维修、叉车维修、机械加工、设备维修、风电焊作业等

例

元旦期间发生由偏二甲肼引发的事故。该物质气味类似香蕉水，但非常易燃，只需拖布轻轻一拖便可能引发火灾。使用有机溶剂进行车间清洁、处理机油和废油时需特别小心。

焊接与动火作业风险

- 吸烟存在火种，不仅危害健康，极易引发火灾
- 气焊、气割用的枪支、液化石油气、氢气、液氨、氨气等均可购买，需严格管理
- 即使没有明火，电火花也可能引发严重后果，与其他因素混合时尤其如此

注意

多次导致多人伤亡的事故均源于风电焊操作不慎。现场混乱、烟雾弥漫，人们无法及时逃生、无法辨认方向。相关实验使用与现场类似的材质、风速和能量，证实了后果的严重性。

作业场所的多人协作与安全管理

- 作业场所不可能只有一人，一定是多人参与，需具备管理意识和能力
- 常见伤害类型：物体打击、高处坠落、触电伤害、火灾爆炸

注意

不要心存侥幸认为”碰一下应该没事”。应积极学习电工技能和消防知识，通过案例教学积累经验，即使并非专业电工也能妥善处理相关问题。

高处作业的安全监管

- 某国企对高处作业监管最为严格，甚至高管认为过于严格
- 攀爬电杆时必须使用两根安全带，永远保持一根安全带勾住才能往上爬

例

攀爬电杆时，两根安全带总有一根勾住：取下来挂上去，再爬一步，再挂上去，再爬一步，把另一根取下来挂到上面，永远保持一根安全带带着。此前曾有一根都不用直接爬的情况，因有员工从其他单位不慎坠落（原因已无法查明）才改为两根。

- 所有操作不能有空缺，人员不能空缺，必须保持全面监管
- 除人工监管外，还应加强视频监控，确保作业过程被记录并上传
- 人的生命无价，一旦失去无法挽回

例

暑假期间工人在野外冒着酷暑进行变压器维修、在电杆上安装刀闸和电线，为全运会赶工。停电后作业时间紧迫，必须迅速完成并恢复供电，否则审批失效需重新审批。电力供应局会有人管理，维修作业必须确保过程清晰明了。

例

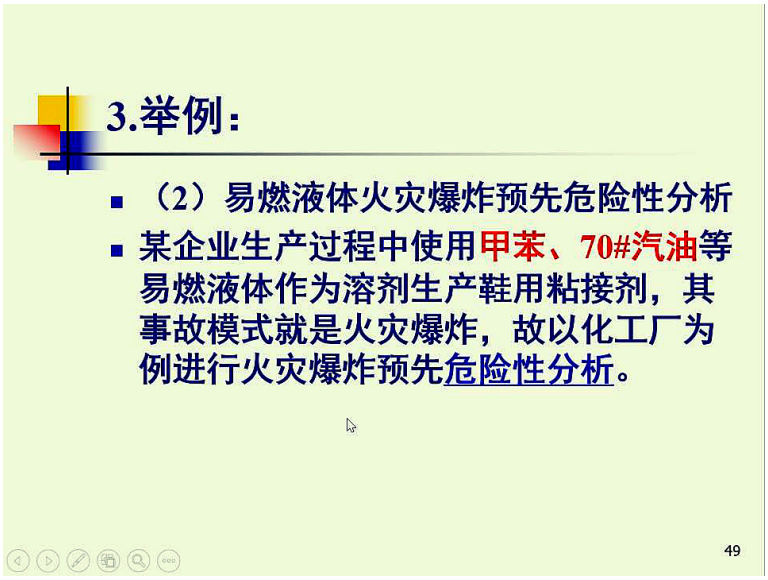
同济大学曾有教师带领学生参与塔吊项目；东北大学学生在实习期间也经历了类似假期实习。

换热器热启动事故

例

某石化企业（不必指明具体企业）刚安装的换热器，在不到 24 小时的热启动热身过程中就出现问题，第二天许多弯头出现裂纹、满是裂缝。换热器是管式或管板式的。

易燃液体火灾爆炸的预先危险性分析



- 针对某企业以甲苯、汽油为溶剂生产鞋用连接剂（胶水）的工艺进行预先危险性分析（PHA）
- 主要事故模式为火灾爆炸
- 溶剂有毒，长期接触易导致白血病，类似案例较多
- 涉及的危险有害因素：易燃易爆、甲苯泄漏、松香（作为胶水成分之一）
- 危险等级按预先危险性及后果严重程度划分为一、二、三、四级

注意

甲苯、汽油等溶剂不仅易燃易爆，还具有毒性，是职业健康的重要隐患。分析时不能只关注火灾爆炸，还要考虑中毒等职业危害。

危险有害因素来源

- 溢出、泄漏
- 雷击等自然灾害
- 摩擦、高温表面（如机械设备高温表面、法兰）
- 装卸过程
- 明火、静电火花

例

某学生在中海壳牌（惠州）工作，目睹泵送液体介质时发生泄漏引发的火灾事故，因心理阴影辞职，后转至广州市第十二人民医院（职业病防治院）从事职业卫生、风险与隐患管理工作。

燃烧三要素

- 燃烧需要三个要素：可燃物、助燃物（氧化剂）、点火源
- 明火、静电火花均属于点火源，是火灾爆炸的触发条件

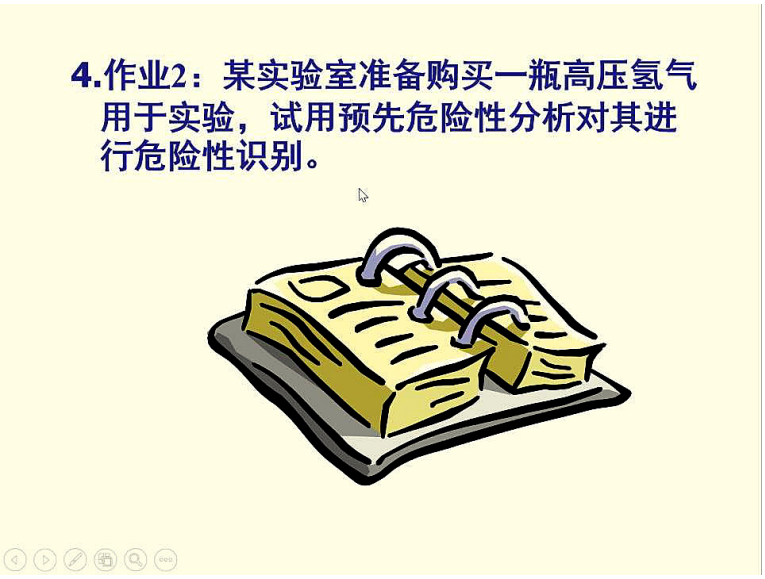
防范措施

- 当前面临人手不足的挑战
- 主要依赖视频监控、智能识别、金属探测等智能化管理手段
- 可对非法入侵进行识别并发出预警

例

海洋馆存在地面湿滑、空间狭小、下雨时外部空间受限、潜水表演等风险，需采取相应防范措施。

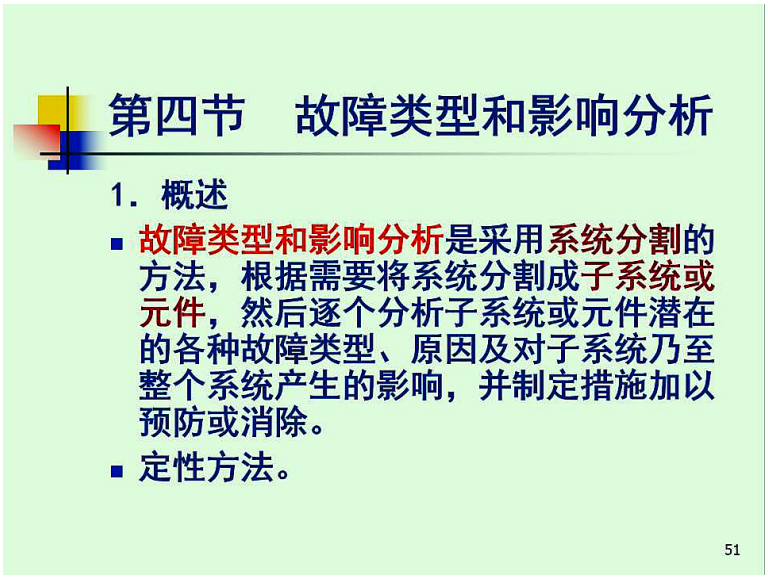
作业布置



- 作业一：对实验室购买的一瓶高压氢气进行预先危险性分析（PHA）危险识别
- 作业二：宿舍火灾安全检查表（沿用上次消防检查表）

- 作业三：FMEA（故障类型和影响分析）

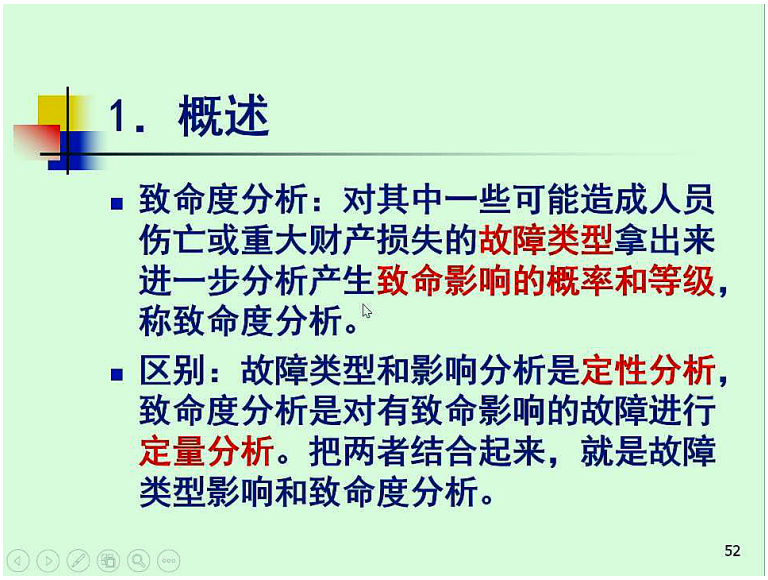
FMEA 概述



- 全称：故障类型和影响分析（Failure Mode and Effects Analysis）
- 是一种定性分析方法
- 用于识别子系统中的各种故障及其原因，以及这些故障对子系统和整个系统的影响
- 主要应用于固定设备设施（资产、固定资产），如汽车等

> 定义
>
> FMEA 是一种定性的系统安全分析方法，通过分析系统中各组成部分可能出现的故障类型、故障原因及其对子系统乃至整个系统的影响，为故障排除和预防提供依据。

FMECA 概述



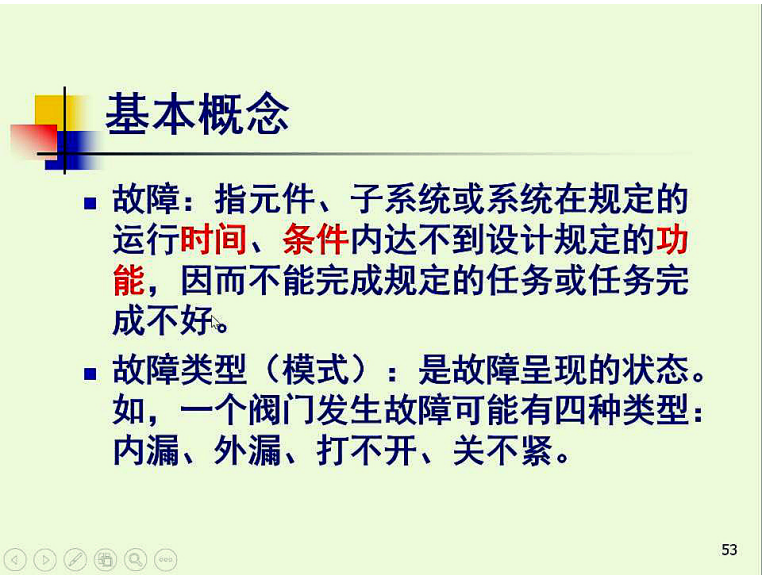
- 全称：故障类型、影响和致命度分析（Failure Mode, Effects and Criticality Analysis）
- 在 FMEA 基础上增加致命度（知名度）分析
- 致命度分析是对故障类型进行进一步量化分析，确定其导致致命影响的概率和

等级

- 结合了定性的 FMEA 与定量的致命度分析，形成更全面的分析

> **注意**
>
> FMEA 是定性方法，FMECA 是在 FMEA 基础上加入定量分析（致命度分析）。两者是递进关系，不要混淆。

故障的定义



> **定义**
>
> 故障是指元件、子系统或系统在规定时间内、规定条件下，不能达到设计规定的功能，或不能完成规定任务或功能的能力。

- 故障与可靠度是相反的概念
- 可靠度：产品、元件或子系统在规定时间内、规定条件下能够完成规定功能的能力
- 故障也可称为不可靠度

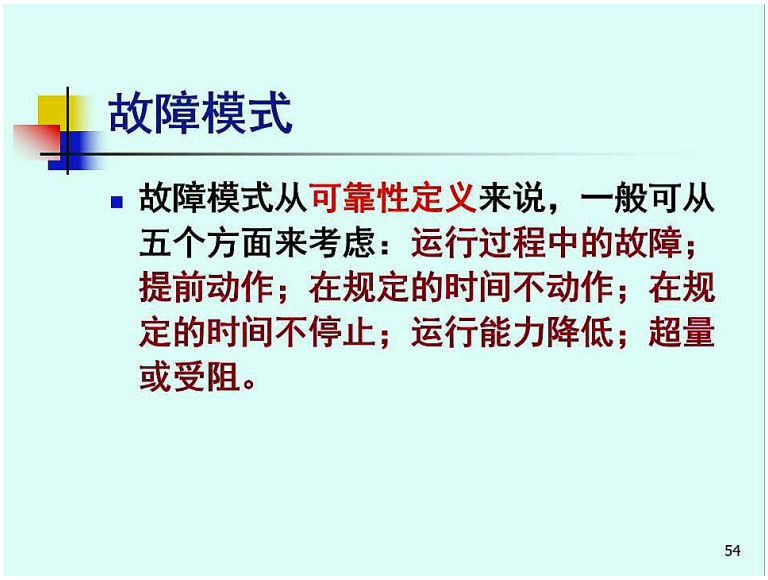
> **注意**
>
> 故障与可靠度互为反面。可靠度是”能完成规定功能的能力”，故障是”不能达到设计规定功能”，两者是同一问题的两个侧面。

故障模式

- 故障模式是指故障所呈现的状态
- 故障模式识别不准确，会导致原因分析偏差、措施缺乏针对性

> **例**
>
> 一个阀门的故障可表现为四种类型：内漏、外漏、打不开、关不紧。

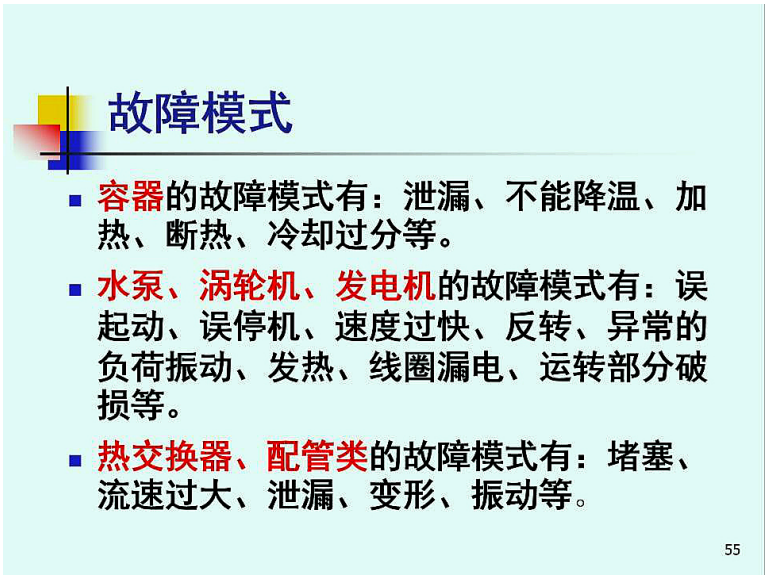
故障模式的五个主要方面

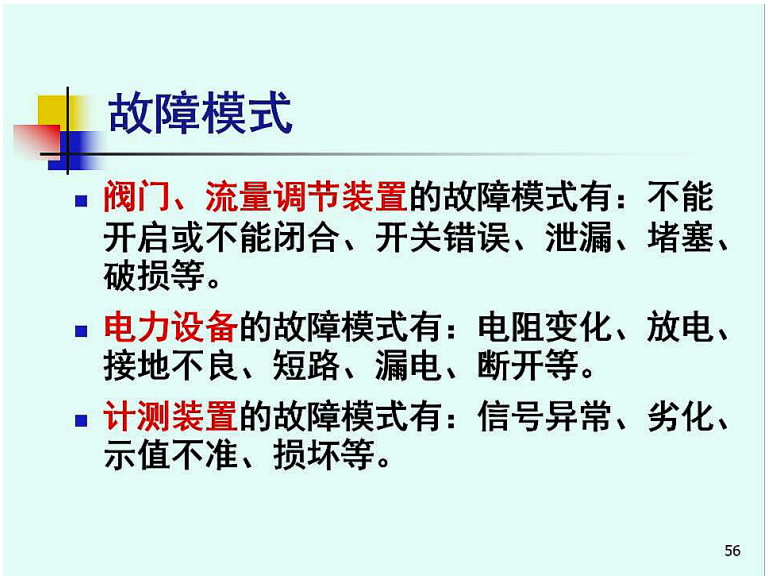


1. 运行过程中的故障：在正常运行过程中出现的问题
2. 提前动作：设备在未收到指令时突然自行启动（如机器人危险动作）
3. 规定时间内未能启动或停止
4. 运行能力降低：设备正常运行能力随使用时间增加而下降
5. 超量或受阻：设备输入或输出量超过预期范围

> **注意**
>
> “提前动作”是容易被忽视的故障模式——设备在不应动作时突然动作，可能造成严重危险，属于故障的一种。

常见设备的故障模式



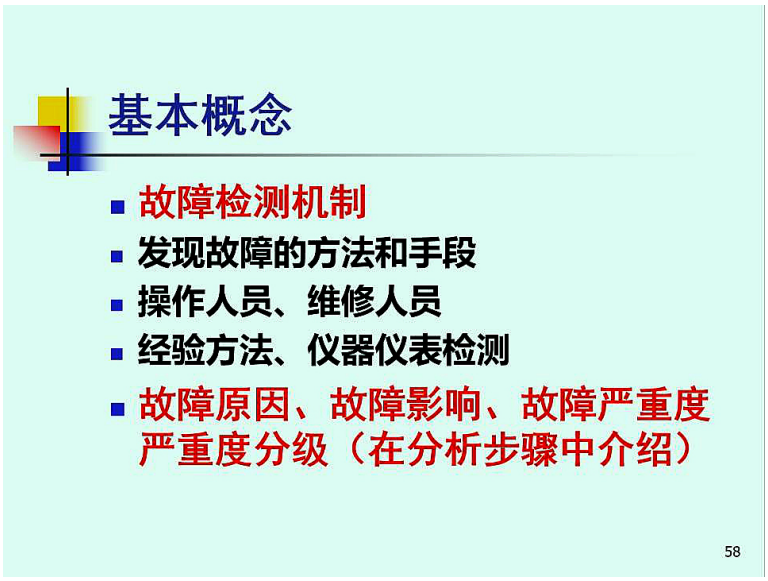


- 容器：泄漏、不利于降温、加热时断热、冷却过度等
- 热交换器（换热器）：堵塞、流速过大、泄漏、变动、震动等
- 水泵、涡轮机、发电机：各类运行故障
- 配管网：泄漏、堵塞等
- 阀门、流量调节装置、电力设备、计量装置：内漏、外漏、打不开、关不紧等
- 支撑结构：变动、松动、缺损
- 齿轮、滚动轴承：断裂、滚珠破碎、内部腐蚀产生裂纹

例

现代大型换热器的内部换热管、换热板、芯片等部件，可通过内窥镜等无损检测技术进行检查，无需拆解即可达到检测目的。

故障检测方法

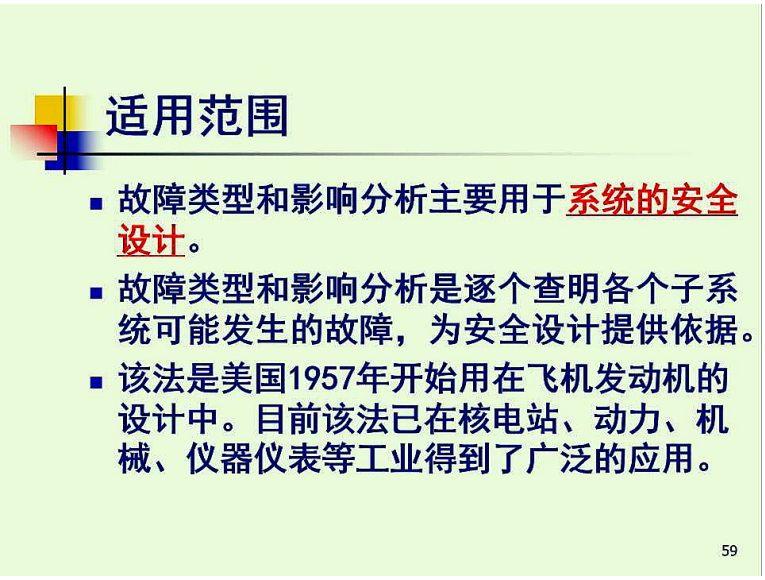


- 故障识别手段
- 操作人员和维修人员的经验
- 仪器仪表检测
- 分析故障的原因、影响、严重程度
- 进行故障严重度分级

例

特种承压设备检查可查阅广东省特种设备检测研究院相关资料；高级检验师（高检师）含金量高但要求很高；质量监督检验站负责相关检验工作。

故障类型及影响分析的应用历史



- 1957 年起应用于飞机发动机设计
- 随后在核电站、动力机械、仪表等领域广泛应用
- 主要用于系统安全设计

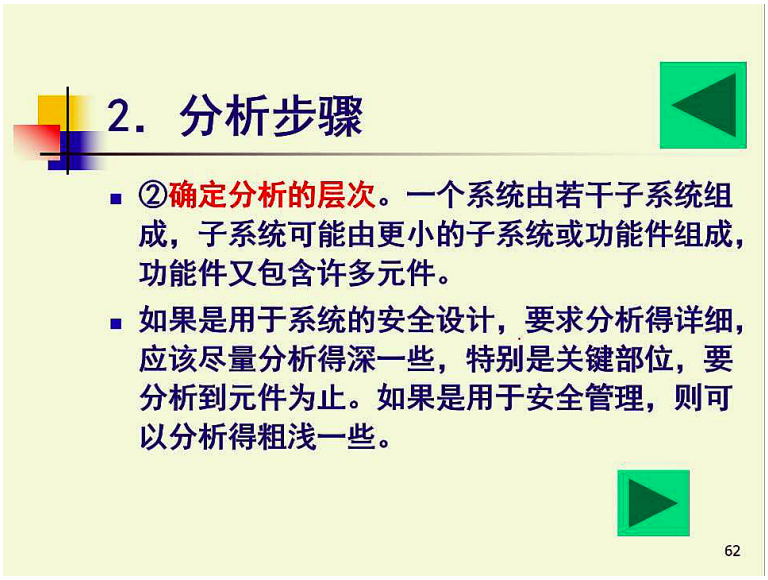
FMEA 分析流程

1. **明确系统并确定分析层次**：梳理子系统和组成部分
2. **确定故障模式**：根据各层次和对象确定可能的故障模式
3. **理解功能框图**：明确子系统及其功能、各功能组件之间的连接方式（串联、并联、桥式连接等）
4. **分析模式及其影响**：深入分析故障模式对系统的影响
5. **确定故障严重程度**
6. **制定预防措施**

注意

可靠性框图中的连接方式（并联、串联、桥式连接等）在可靠性讨论中并非重点，但理解功能框图至关重要——它有助于明确子系统功能及组件间的连接关系。

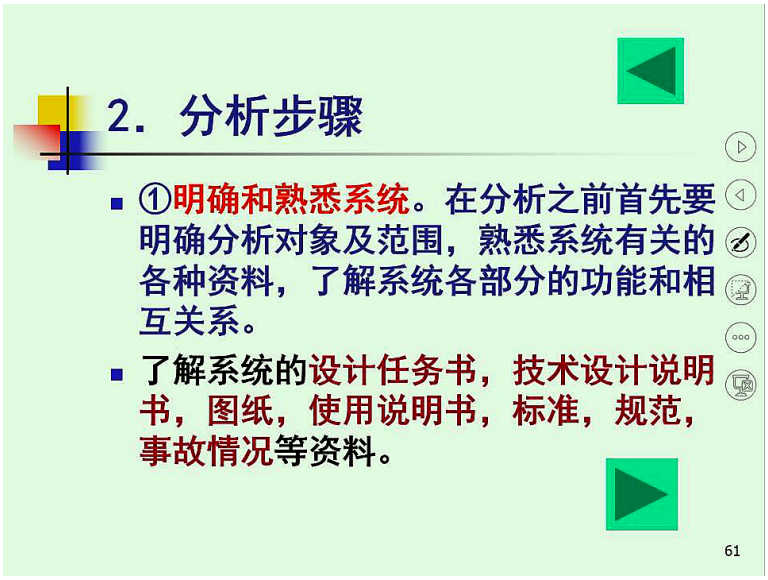
分析层次的选择



- 设计阶段：需进行更详细、深入的分析，对关键部位细化到元件，工作量、人员和时间成本更高，但更准确
- 安全管理阶段：可相对粗略，不必分解到元件细节

> 例
>
> 空调本质上就是一个换热器，将室内热排到室外、冷气进入室内。但因其需 24~72 小时连续运行，对能量损耗、噪音控制提出更高设计要求，体现了系统设计中对细节的讲究。

明确和熟悉系统



- 进入相关行业后需学习该行业特定知识（如化工行业总平面布局中不同符号代表不同设备设施）
- 设计文件通常包括：设计任务书、设计说明书、图纸、使用说明书、标准规范等
- 通过审阅设计资料，全面理解系统功能、构成、子系统连线与功能
- 分析各元器件在系统中的重要性、可能产生的影响及后果严重程度

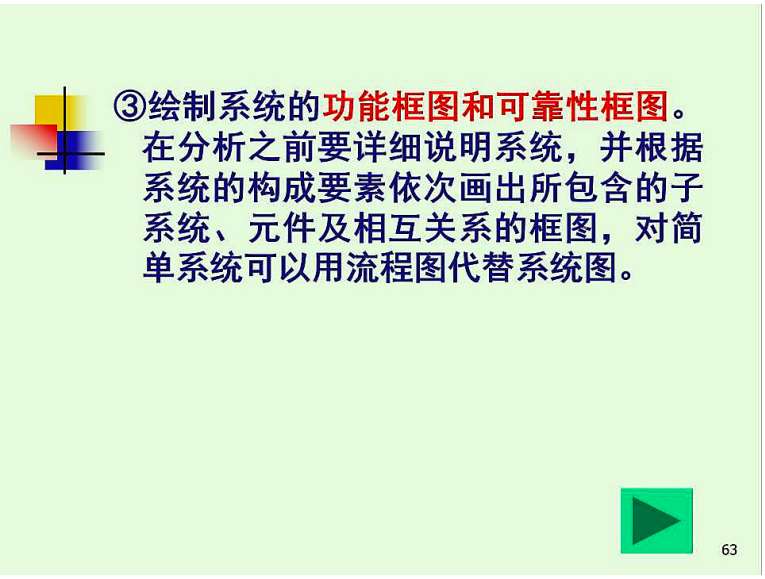
例

电厂选择：电厂待遇优厚但需离开广州；广州市内单位稳定但电力系统稳定性更好。现代电厂多采用天然气发电，环保干净，机组国产化程度高，控制运行几乎全自动化，采用超超临界技术，转速高，实现气电热冷联供，综合效益高。

变频空调与压缩机原理

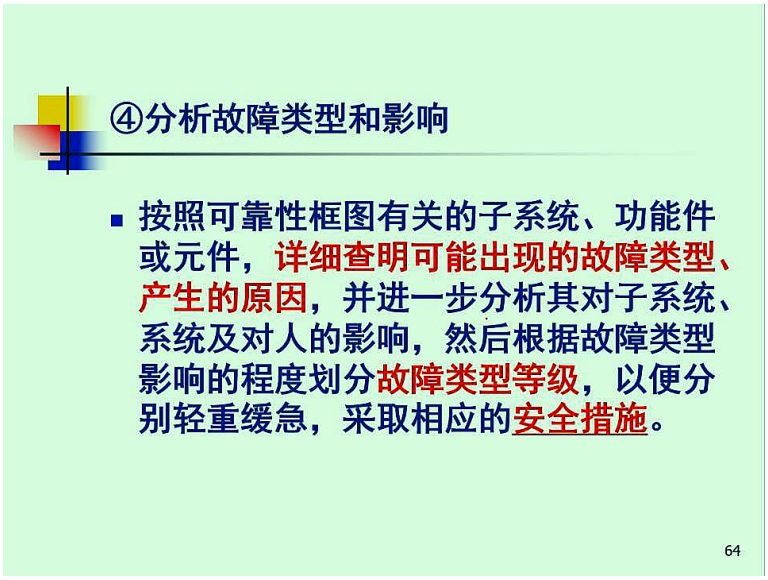
- 室外机通过压缩将气体变为液体，传输至室内机，经节流阀膨胀变为气体，吹出后再压缩，循环往复
- 变频空调核心是压缩机转速可变：需要温度高时压缩机减少工作量、降低转速
- 变频技术依赖变频器和变频电机，成本较高
- 温度控制曾是”卡脖子”技术，现国产已能解决

功能框图与子系统连接



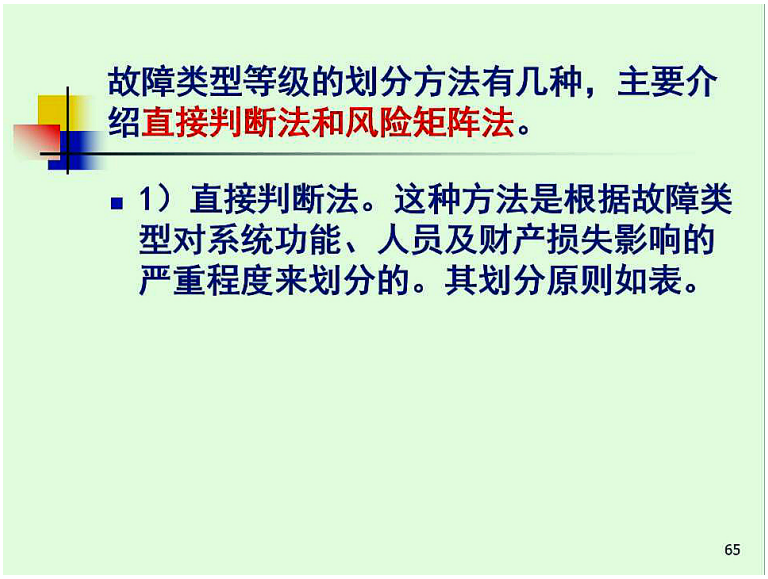
- 子系统和组件之间存在相互联系与连接方式，即功能的关联性
- 简单系统通常表现为流程，可用框图表示
- 可靠性框图将在后续可靠性章节专门讲述

故障类型分析（FMEA 核心步骤）



- 分析可能的故障类型，即预设的故障场景
- 故障场景可来自凭空假设，也可借鉴传统经验（如易燃易爆场所）
- 动设备故障类型通常更多
- 通过监测元器件了解运行状况，如噪音来源可能与磨损或泄露有关
- 对故障进行等级划分，再按轻重缓急采取措施

故障等级划分

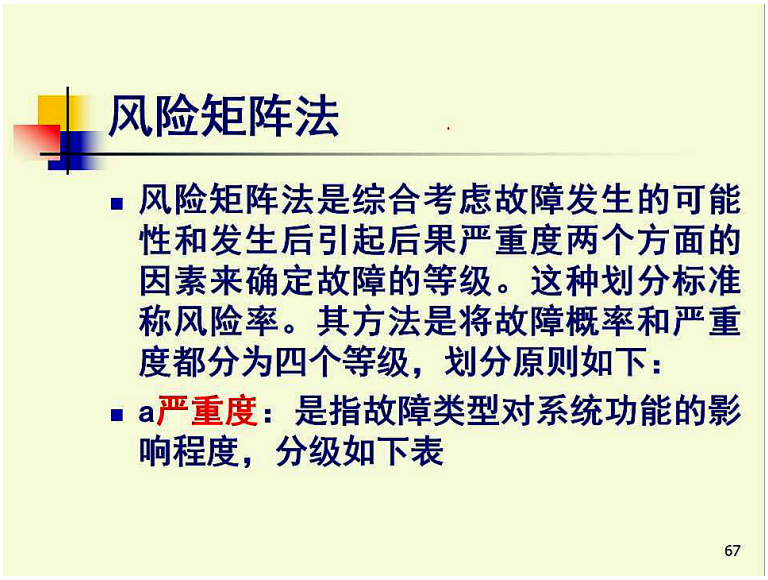


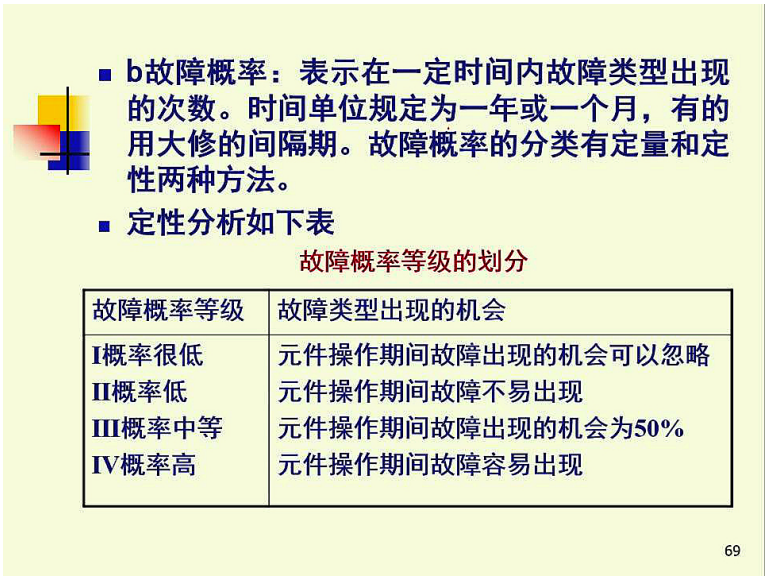
- 故障分级主要依据严重性划分，包括严重、致命、临界、灾难性等级
- 前两种为主要，第三种为关键，第四种为灾难性
- 关键和灾难性故障概率很低，二级概率较低，三级中等，四级高
- 故障概率数据来自统计结果和同类产品的统计分析，尽量定性判断

定义

若已知元器件在使用过程中的所有故障概率，则可计算系统的失效概率，进而从可靠性角度计算出系统的可靠度。

风险矩阵





- 基于两个关键因素：故障概率和严重程度
- 严重度标号 1、2、3、4，故障概率标号 1、2、3、4
- 根据对角线判断风险水平：确定严重度和发生概率后，焦点位置代表分析对象的风险水平
- 高风险、中风险、低风险区域划分取决于判断准则的设定

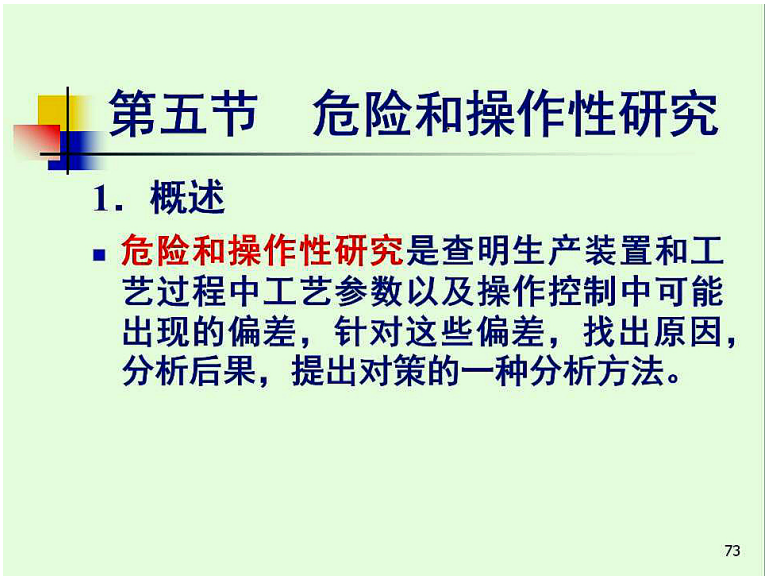
降低风险的途径

- 减少风险的严重性
- 降低风险发生的可能性
- 这是 FMEA 分析的基本过程

注意

元件正常工作期间，任何单一故障类型出现的概率必须小于所有故障类型的总概率。故障概率定级量化原则共四个等级，通常若未超过 20% 的最大概率，该概率已相当高。

危险可操作性研究（HAZOP）概述

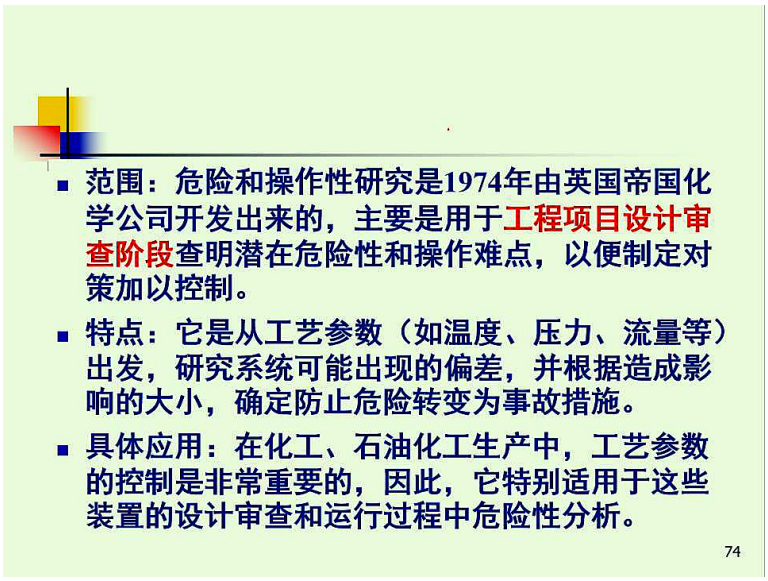


- 前三种系统安全分析方法：检查表、预先危险性分析、FMEA、FMECA
- 第四种方法为危险可操作性研究（HAZOP），适用于流程工业
- FMEA 主要关注设备、设施和机械装置；HAZOP 关注管道、压缩、泵、储罐等输送流体介质的设施
- 关注生产装置和工艺过程中可能出现的偏差，找出原因、分析后果、采取对策

定义

危险可操作性研究（HAZOP）主要关注在生产装置和工艺过程中，工艺参数和操作控制中可能出现的偏差，即寻找偏差、分析原因、评估后果以及确定如何避免这些后果。

HAZOP 的应用范围与特点



- 起源于 1974 年英国帝国化学公司（ICI）的工程项目设计审查
- 在项目开始前即可用于分析危险和操作性
- 涉及阀门、储罐和监控系统等
- 工艺参数包括温度、压力、流量等，如人体体温、血压、心率、血氧浓度（需保持 94% 或 95% 以上）、血糖等

- 系统相互关联，一个参数异常可能影响其他参数
- 从工艺参数出发查找偏差、分析影响、采取预防措施
- 特别适用于化工和石油化工生产的设计审查和运行过程中的危险性分析

例

天然气管道检测：若管道中发现流动的天然气，可分析可能的原因。水管也可用此方法，但水不像天然气那样危险，可在检测后进行抢修。

HAZOP 的关键概念与术语

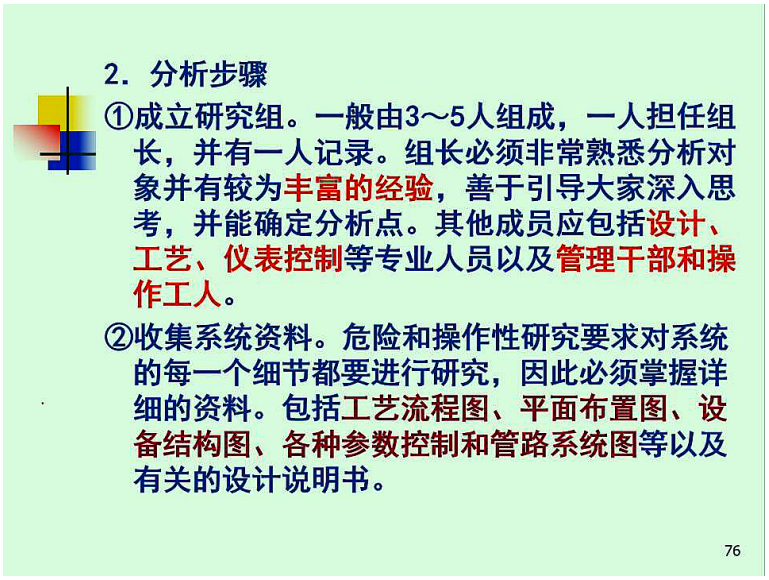


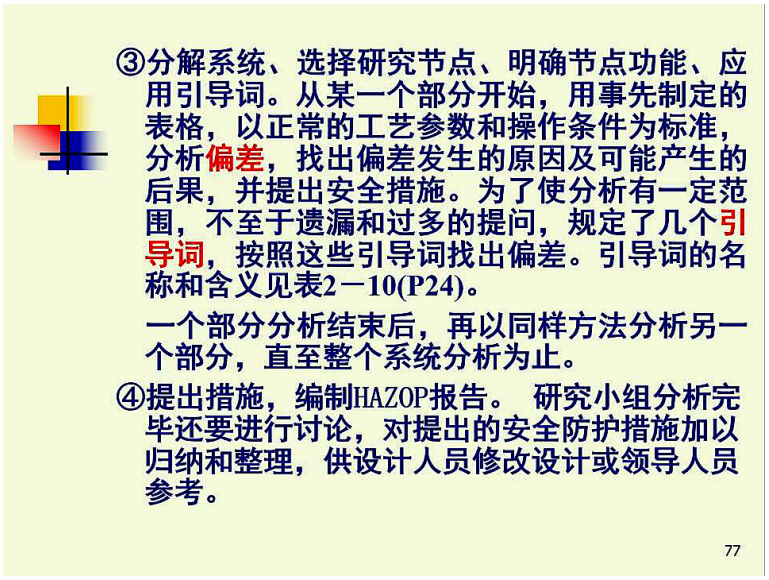
- 目的：要实现的功能
- 偏差：设计意图与实际结果之间的不一致
- 产生偏差的原因
- 后果：偏离设计意图所导致的影响
- 引导词：对设计意图进行定性和定量描述，如大小、高低等，引导分析偏差的产生

注意

偏差可能表现为偏大、偏小、偏高、偏低、偏左、偏右、偏正、偏负等，这些情况更加严重。

HAZOP 的操作流程



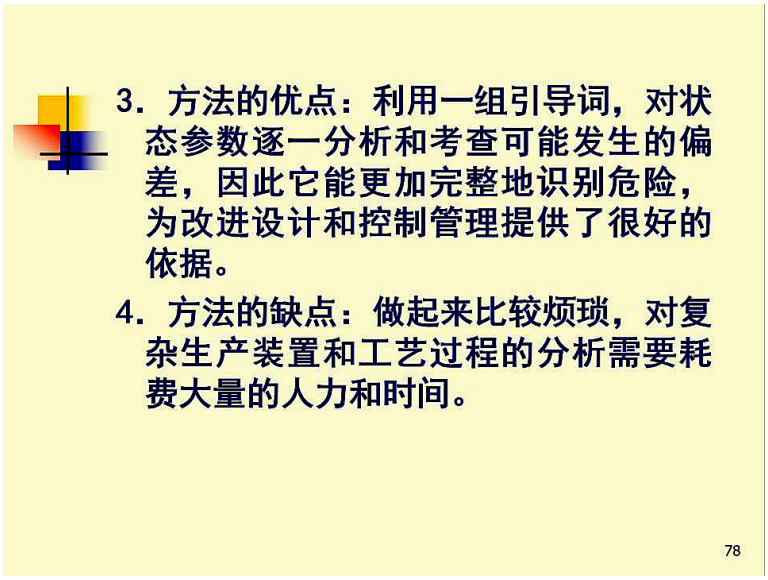


- 成立研究组：根据系统复杂程度，小组可由 3 人组成，复杂系统可增至 5 人或更多
- 组长需经过培训、通过考试获得证书（主席证书）后执行分析任务
- 收集系统资料：包括工艺流程图、平面布置图、设备结构图、各种参数控制图（PID 图）以及管路系统图
- 分解系统，选择研究节点：通常选择一个单元的前后两个点作为分析节点，对所有节点完成分析后再看整体情况，形成循环
- 应用引导词分析偏差，找出所有可能原因，判断是否有对策
- 若无对策，提出建议改进设计
- 反复进行，开会讨论达成共识，整理成报告，反馈给设计人员参考

例

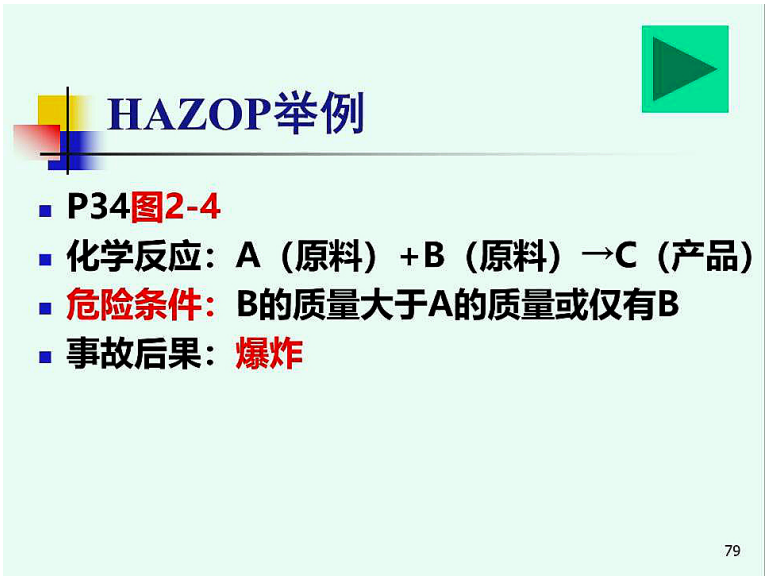
教材第 33 页提到九个步骤，第 34 页图 2-4 为阿德伯案例。A 与 B 反应生成 C 产品，当 B 的质量大于 A 的质量或仅 B 存在时会发生爆炸。因此需确保 A 总是先于 B 进入反应容器，且 A 的量稍多于 B。

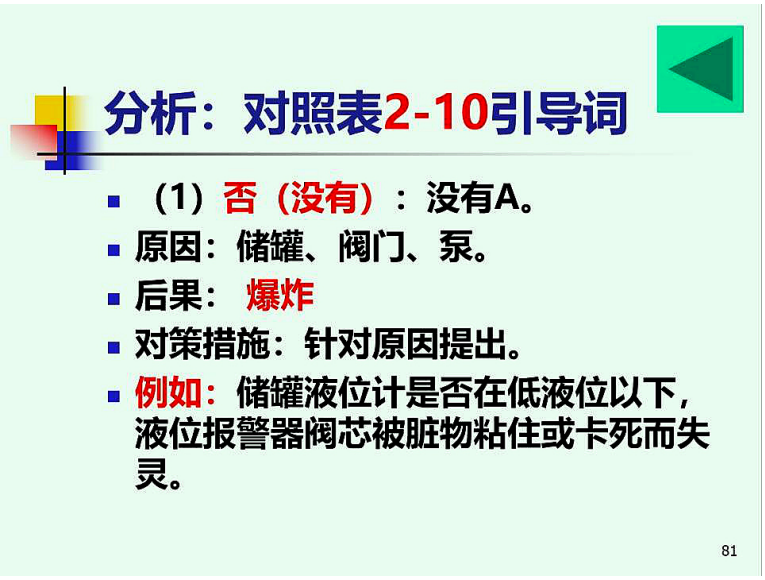
HAZOP 的优缺点



- 优点：通过引导词对各个工艺参数逐一分析和考察，识别可能产生的偏差及其原因，据此进行危险识别、改进设计和管理
- 缺点：很麻烦，需要耗费大量人力、物力和时间

HAZOP 案例分析（阿德伯案例）





- 系统分为四部分：A、B、C、D
- 首选 A 部分为研究节点，应用引导词分析：
  - 否（A 没有）：A 是空的，阀门一或阀门二没有打开，泵一堵住，泵一没有工作，或管道破裂，导致爆炸
  - 少（A 太少）：分析可能原因
  - 多（A 太多）：分析可能原因
  - 或者：尽管按设计要求原料 A 被泵入反应罐，但其他物质被送入反应罐，导致污染，产品含杂质
  - 部分：原料罐缺少某种组分，比例不大，可能导致爆炸
  - 相反：A 从反应罐被供入储罐，可能性不大但确实存在
  - 其他：许多其他原料没有被泵入反应罐，导致其他物质被放入，可能导致爆炸
- 只有第一个步骤全部完成后，才能分析结果并撰写报告

> **注意**
>
> 阿德伯案例属于考试范围，需掌握。分析 B 部分时，教材上的图只显示一个泵和一个阀门，而课件上的图显示两个阀门，以教材为准。

作业

- 作业一：实验室准备进行高压空气分离实验，利用预先危险性分析方法对其危险性进行分析
- 作业二：将阿德伯案例中的 A 改为 B，分析原料 B 的输送部分，选择研究节点进行分析

10 月 13 日

课程考核与平时成绩构成

- 平时作业（V90+V95，约 50-60 页）的平均分即平时作业分
- 点名共 10 次，每次 10 分；请假酌情扣一半，无故缺席扣 5 分
- 平时成绩对最终结果有决定性影响：平时保持 A，期末略降至 B，总分仍可能较高；平时不理想，期末再努力也难以弥补
- 第一次作业需扫描提交，属严肃任务，类似平时测验，各占总评 20%
- 第二次作业多数同学成绩提升（有两位从 B+ 升为 A），少数从 C 降为 C-，说明

并非理解有误而是思路完全偏差
- 成绩在 75-90 之间的同学可清楚看到 CC 关系；大部分同学成绩在 B 以上，其余在 CC-或更低
- 已提交作业按第一次提交标准计算，但允许成绩不理想者重新提交

系统安全分析的作用

- 评估系统可能存在的潜在风险
- 识别事故发生的可能性及可能产生的后果
- 为后续评价及寻找最佳安全投资效益的最优防控方案提供依据

系统安全分析方法概述



- 两次课程涉及的方法包括：故障类型及影响分析（FMEA）、危险性分析、危险可操作性研究（HAZOP）、事件树分析（ETA）等
- 需掌握每种方法的基本特点、分析程序及优缺点
- 需明确各方法是定性还是定量，以及哪些方面需要考虑定量分析
- 需掌握各方法的分级标准（如危险分析按什么标准分级）

文献检索与数据库资源

- 常用中文数据库：万方、中国知网（CNKI）、维普、人大复印资料（人文社科）
- 常用英文数据库：SCI（科学引文索引）、SSCI（社会科学引文索引）、EI（工程索引）、JCR（期刊引用报告）
- 学术团体期刊：ACS（美国化学学会）、IEEE（电气与电子工程师学会）等
- 大型出版公司：Springer、Elsevier 等
- 检索方式：可按作者名、标题、关键词（如”安全”）等进行检索
- 检索示例：输入”危险可操作性研究”或”氯气化”等关键词，可检索到大量期刊、学位论文、会议论文等文献
- 检索结果示例：84 篇文献中包括 84 个学术期刊、69 个学位论文、5 个会议论文、1 个报纸、1 个图书、4 个标准、2 个其他
- 图书馆资源及数据库使用是提高研究能力的重要途径，需自行探索学习

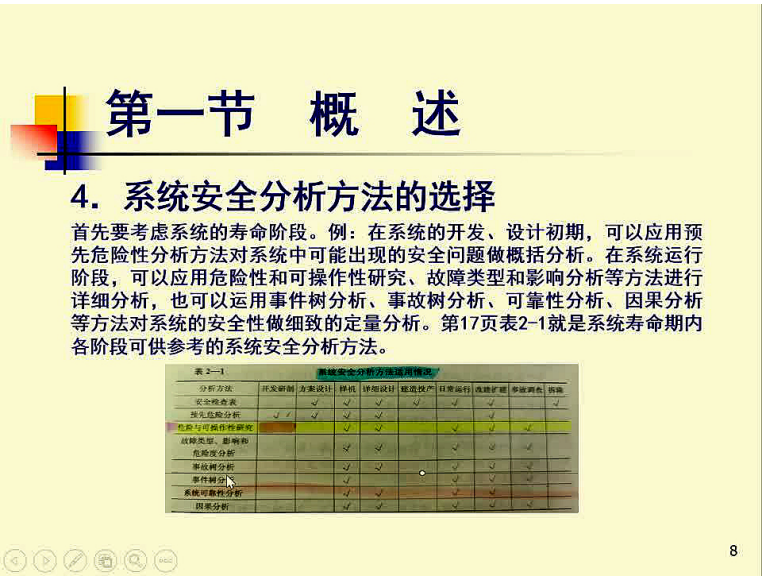
安全系统工程专业英语学习

- 安全系统工程理论源自国外，建议查阅英文原版教材
- 国内相关著作：重庆大学傅师傅老师、中国矿业大学朱传杰老师、中国地质大

学范蠡晓教授

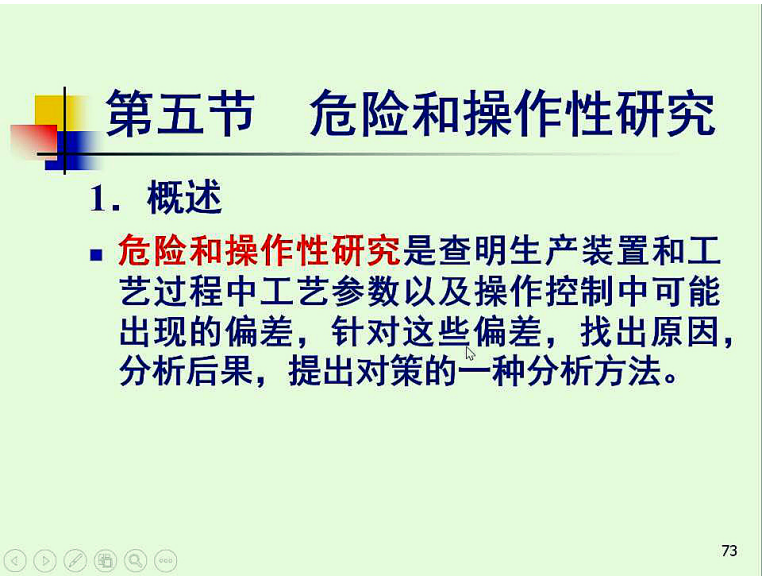
- 建议通过英文教材学习专业英语，虽不作作业要求，但值得了解

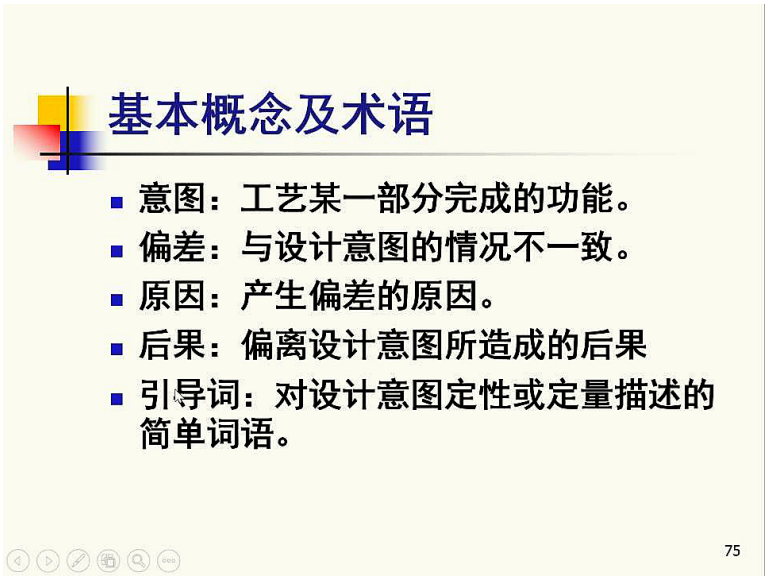
系统安全分析方法的应用阶段



- 各种方法在系统寿命周期各阶段均可参考使用
- 方法选择需结合系统所处阶段（如设计、运行等）

危险可操作性研究（HAZOP）核心术语



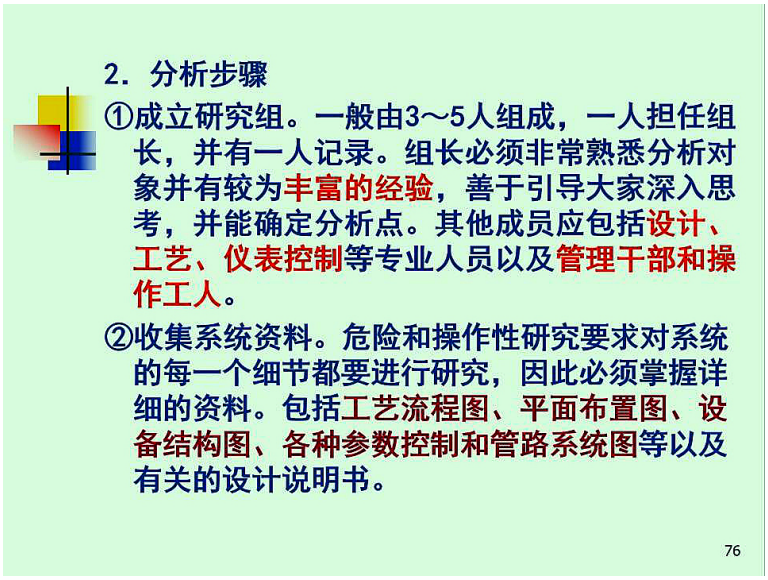


定义

危险可操作性研究（HAZOP）是一种系统化的危险分析方法，通过引导词对设计意图进行定性、定量描述，识别偏差及其原因和后果。

- 关键术语：引导词、偏差、原因、后果、对策（措施）
- 引导词是分析的关键要素，书上列有相关内容
- 设计流程从明确意图开始：工艺某部分完成的功能和目的应清晰界定
- 若业主需求与设计意图不符，即产生设计偏差
- 偏差产生的原因可能引起相应后果，后果即偏离设计意图

HAZOP 分析所需资料



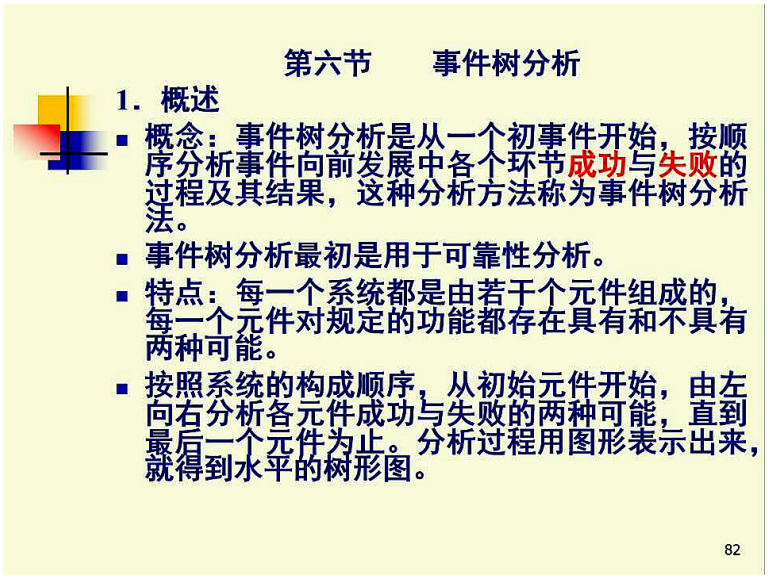
- 工艺流程图（PHA 中的流程图，如自来水净化和消毒杀菌流程图）
- 平面布置图（设备设施按总平面布局规范放置）
- PID 图、各种参数图、管路线路图等
- 设计单位工作需重新培训学习，但安全工程师是设计单位所需人才

HAZOP 报告与优缺点

- 引导词在书末有列出，形成 HAZOP 报告（哈扎本）

- 组长需经过专门培训并获得分析主席证书
- 优点：能对整体进行逐一分析和考察
- 缺点：投入的工作量非常大（人力和时间）

事件树分析法（ETA）基本概念

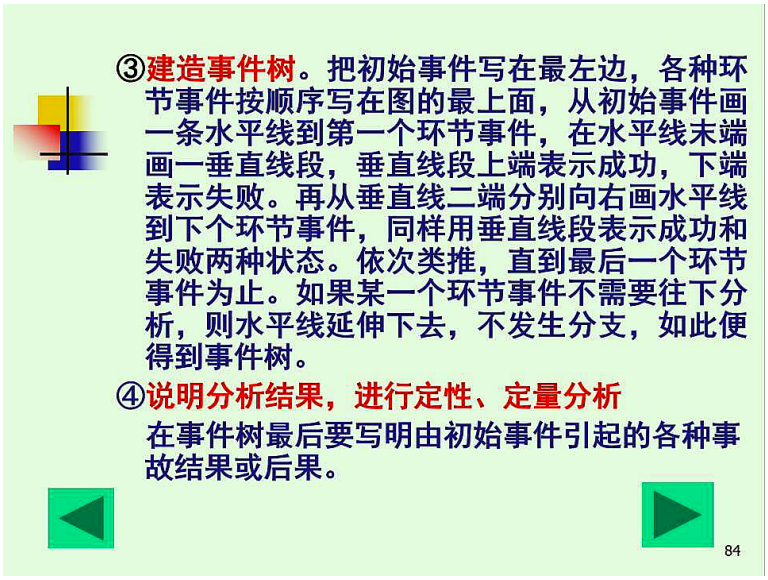


定义

事件树分析法（ETA）是将事故发生的整个过程从起点开始按顺序展开，在发展的各个环节中，成功或失败构成一个系统，从左到右展开形成分叉的树状结构。

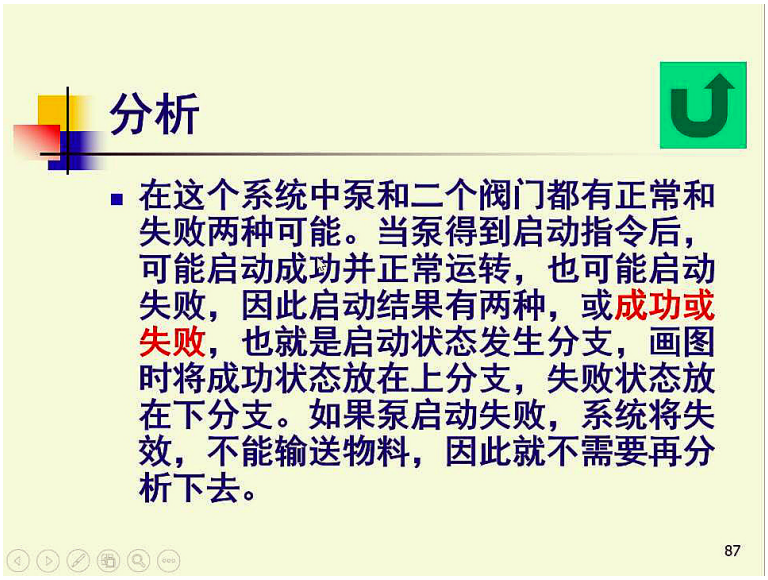
- 最初用于可靠性分析，后应用于故障树分析以计算系统可靠性或可靠度
- 每个系统由多个元件组成，每个元件对规定功能有”有/无”（成功/失败）两种可能性
- 按系统构成元件的顺序从左到右分析，形成分支众多的树状结构
- 初始事件可以是系统故障、设备失效、操作失误或工艺过程异常等，可为已发生或设想的情况

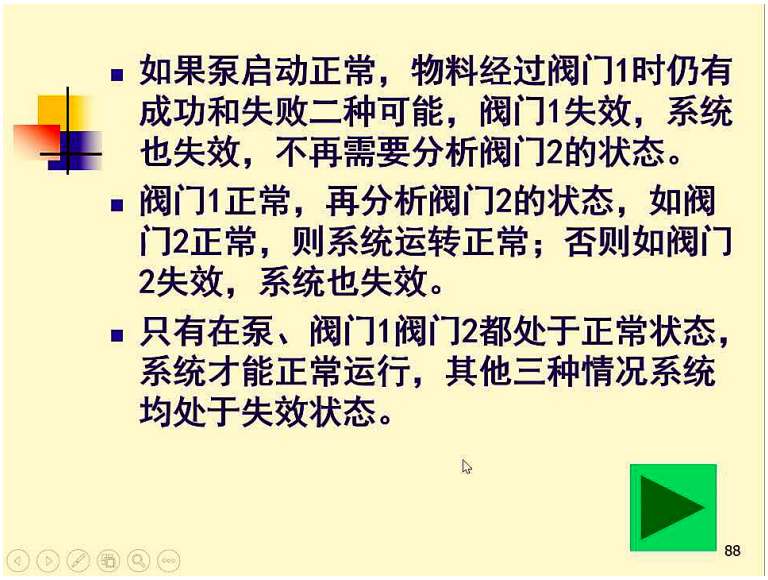
事件树分析步骤



- 明确初始事件
- 确定与初始事件相关的各元件及其连接关系，判断连接是成功还是失败
- 构建决策树：初始事件放左边，上下分支代表成功和失败，递归展开
- 细节分析程度取决于目标，当继续细分无意义时停止
- 定性分析：判断哪些分支是成功的
- 定量分析：计算某条线路成功的概率及相应的不可靠度

事件树分析示例：泵与阀门串联系统



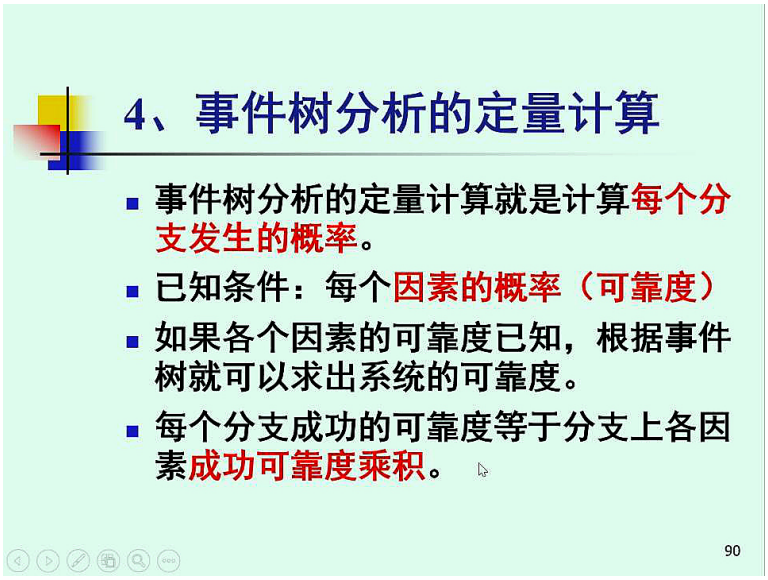


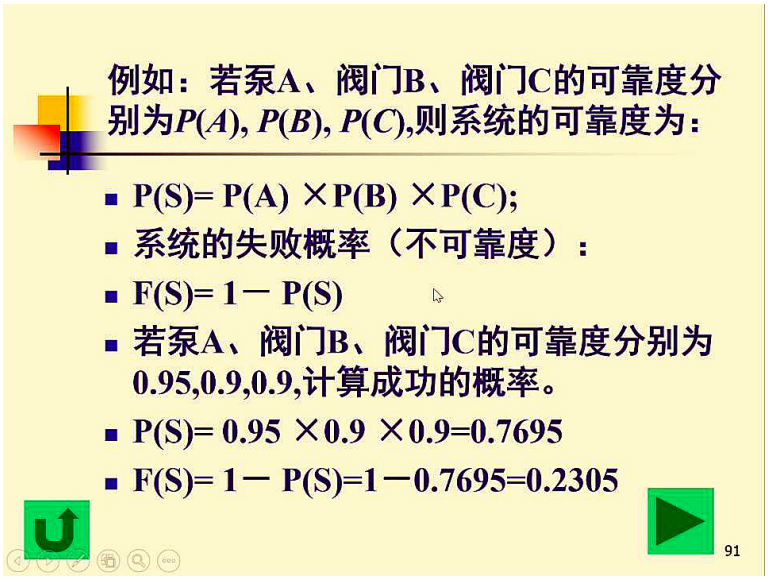
例

泵输送物料（如剧毒物质）时，采用泵-阀门 1-阀门 2 串联的双重保险设计。给电信号后泵启动，成功则继续判断阀门 1、阀门 2 的状态，失败则系统失效。按逻辑连接路径顺序为泵 → 阀门 1→ 阀门 2，弄反会出错。

- 串联系统中，所有元件都成功系统才成功
- 成功路径：泵成功 + 阀门 1 成功 + 阀门 2 成功
- 其余分支均为失败路径

串联系统可靠度计算





注意

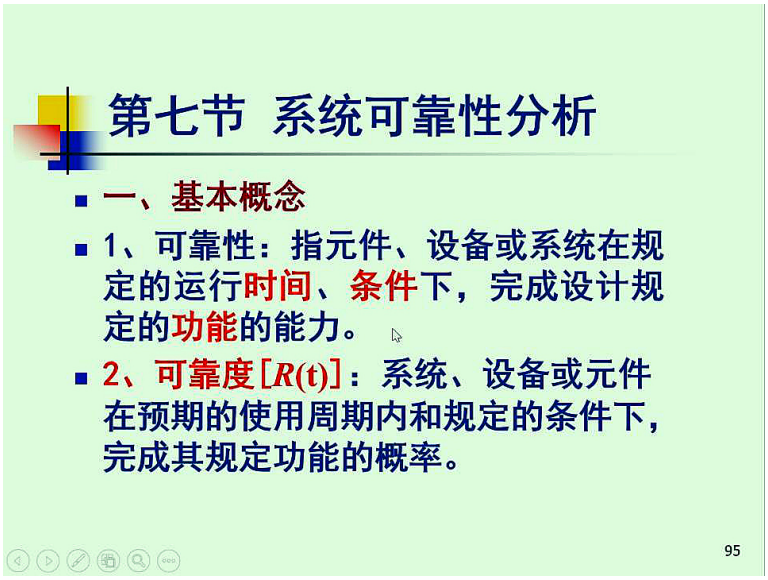
串联系统的可靠度等于各元件可靠度的乘积，但各分支概率之和必须等于 1，需仔细核对。

- 系统可靠度 = 各成功分支可靠度的乘积
- 失败概率 = 1 - 可靠度
- 示例：三个元件可靠度分别为 0.95、0.9、0.9，系统可靠度 = 0.95 × 0.9 × 0.9 = 0.7695
- 各分支概率相加应等于 1，需注意核对

课堂作业

- 计算给定串联系统的可靠度（如 0.95、0.9、0.9 组合，结果为 0.7695）
- 在原有基础上再加一个阀门 D（可靠度 0.9），重新计算系统可靠度
- 将阀门串联或并联组合，观察可靠度与成本的变化
- 工业阀门成本高（动辄几十万、上百万一个），可靠度提升与成本需权衡

可靠度与可靠性的定义



- 可靠度是可靠性的量化，可靠性本质上是一种能力
- 可靠性涉及五个关键要素，需完整理解才能围绕可靠性展开讨论

定义

系统或元件的可靠度定义为：在预期的使用周期内，在规定的条件下，系统或元件完成其规定功能的概率。

- 五个基本要素：
  - 研究对象：元件、设备或系统
  - 规定运行时间（即寿命）
  - 规定运行条件（即环境）
  - 设计功能是否满足规定
  - 能力

例

一副简单的眼镜也存在可靠性问题：撑脚易掉落、镜片易摔花、颜色随时间变化（如从黄色变绿）。可靠性高的产品其价格也会不同，说明小部件同样蕴含可靠性设计。

概率的概念

- 概率是描述可能性发生的度量，不能简单地用”可能性”来解释概率
- 概率可通过发生次数与总次数的比值来体现
- 概率是《数据统计》课程中已学过的概念，属于常考内容

维修度



定义

维修度是指系统发生故障后，在维修允许的时间内完成维修的概率。

- 维修度考虑的是在一定时间内能够完成维修的概率，而非无限期拖延
- 维修时间过长则维修度低

有效度

定义

有效度是指在规定的使用条件和时间内，系统保持正常状态的概率。

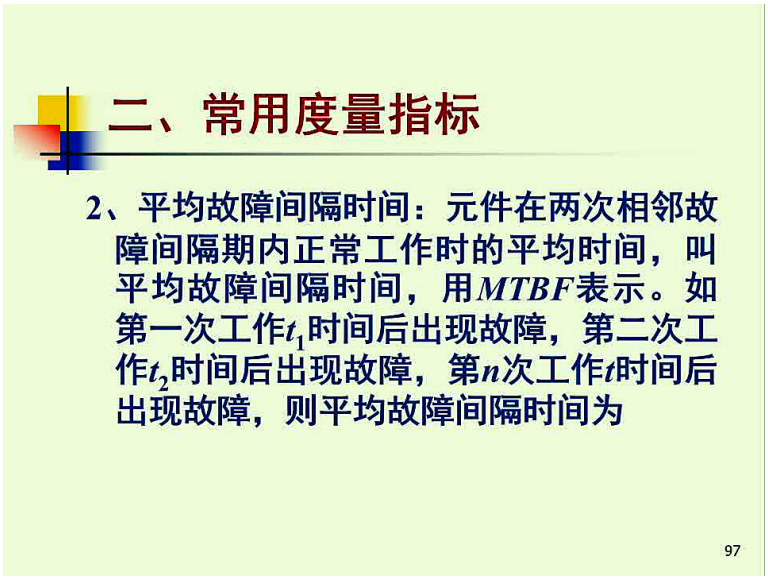
例

电动汽车充满电可行驶 300 公里，但实际只行驶了 280 公里，这便是有效度问题。因此许多人选择同时拥有电动车（日常通勤）和燃油车（长途出行），因为电动车长途行驶可能需中途充电。随着电池技术（如固态电池）进步，这一问题已有所改善。

可靠性的基本度量概念

- 可靠度、维修度、有效度是可靠性的三个基本概念，需清楚理解

平均无故障时间（MTBF）



定义

MTBF（Mean Time Between Failures）指从故障发生到下一次故障的平均工作时间，即系统发生故障前连续正常工作的平均时间。

例

将 100 个灯泡放入教室使用 100 小时，其中 3~4 个在 50 小时内烧坏。将所有灯泡的正常工作时间相加并平均，即可计算 MTBF。

- 注意：TTF（Time To Failure）指首次故障发生的时间，通常针对不可修复系统；对于可修复系统，指首次故障到再次故障的发生时间

平均故障间隔时间与平均故障修复时间



- 平均故障间隔时间（MTBF）：对于可修复系统，将故障修理时间从总时间中剔除后，再除以故障发生次数
- MTBF 与 MTTF 物理意义无显著差异，但引入 MTBF 是为了处理可修复系统
- MTTF（Mean Time To Failure）：平均故障修复时间，也称 TTR，指可修复系统

出现故障到恢复正常工作平均所需的时间

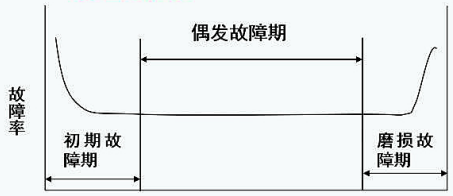
> **注意**
>
> MTBF 与 MTTF 是两个不同概念，需区分：MTBF 是平均故障间隔时间，MTTF 是平均故障修复时间（TTR）。

故障率

- 可靠度的补事件故障概率（或不可靠度），用$F(t)$表示。故障概率由下式表示：

$$F(t)=1-R(t)=1-e^{-\lambda t}$$

- 上述两式只适用于故障率稳定不变的情况。但许多元件故障率随时间而变化，显示出如下图所示的浴盆曲线。



100

> **定义**
>
> 故障率是指设备在一段时间内正常运行后，单位时间内出现故障的概率。

- 当故障率 λ 为常数时，可靠度 R(t) = e^(-λt)
- 不可靠度 F(t) = 1 - R(t) = 1 - e^(-λt)
- 故障率在稳定状态下不变，仅适用于特定时间段

故障率曲线（浴盆曲线）

- 由图可见，元件故障率随时间变化有三个时期，即
  - 初期故障期
  - 偶发故障期
  - 磨损故障期

101

- 故障率随时间变化分为三个阶段：

例

故障率曲线类似洗澡的过程，分为三个阶段：

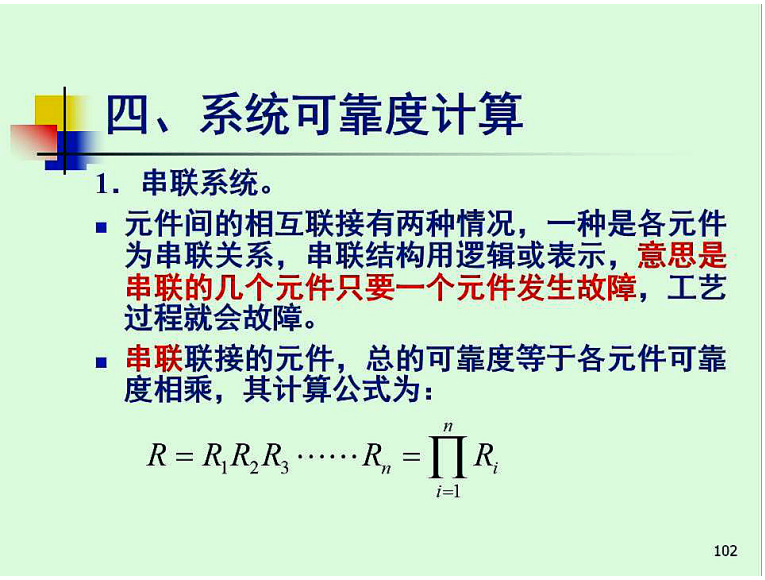
1. 早期故障期（磨合期）：故障率较高但随时间下降，产品在这一阶段出现的故障通常会被排除。新车交付时基本已度过磨合期。
2. 偶发故障期（有效寿命期）：故障率稳定且较低，是产品的最佳使用阶段。
3. 磨损故障期：故障率随时间上升，产品老化。通常车辆使用到寿命的三分之二时，维修保养费用将达到车辆原始成本的三分之二。

故障概率与故障率的区别

注意

故障概率与故障率不是同一概念。故障概率指的是不可靠度（1 - 可靠度），而故障率是另一个概念，指单位时间内发生故障的概率。

串联系统

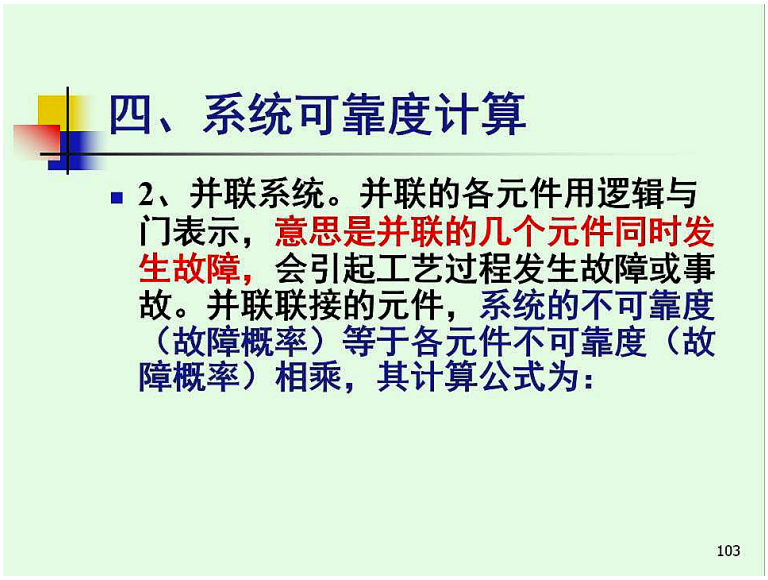


- 各元件两两相连形成串联，只要有一个元件失效，整个系统就受影响
- 串联系统的总可靠度等于各个元件可靠度的乘积

例

教室中的电压是一定的，但需避免某些情况导致串联电路中断。串联系统可靠度计算可直接应用各元件可靠度相乘，无需通过事件分析。

并联系统



- 几个元件并联，只有当所有并联元件同时发生故障时，整个系统才受影响
- 只要有一个元件是好的，系统就能正常运行
- 并联系统的可靠度计算为 1 - F，其中 F 为各元件不可靠度的乘积（即 1 减去各元件可靠度相乘）

复杂系统连接方式

- 电路连接方式包括串联、并联以及更复杂的串并联混合连接
- 无论电路如何复杂，均可采用基本分析方法
- N 中取 K（N 中取 M）系统：并联情况下，若 N 个元件中有 M 个正常运行且未发生故障，系统则被视为正常

事故树分析概述



- 事故树分析（FTA）是一种既定性又定量的重要分析方法
- 在查找控制事故途径及识别事故发生路径方面相对更为准确
- 可定量计算顶上事件发生的概率，存在多种计算方法（可借助计算机或专用小程序）

注意

事故树与事件树不同：事件树涉及的是事件的数量（成功/失败两种状态），而事故树涉及的是故障或事故的数量。事件树从原因推导结果，事故树从结果追溯原因，二者是归纳与演绎的关系。

- 事故树分析既可定性分析，也可定量分析，定量难度高于事件树
- 本章内容对事故预防至关重要，通常在考试中占 30 分左右，需重点掌握

事故树（故障树）的定义

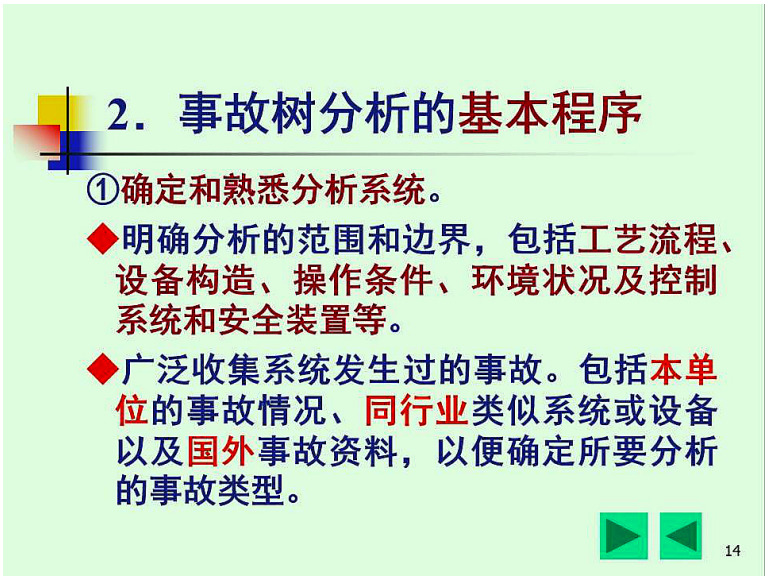


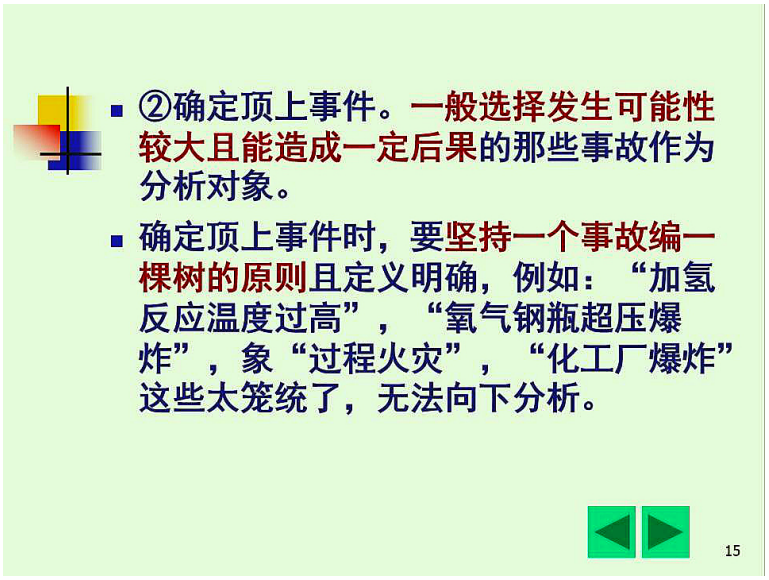
定义

事故树（又名故障树）是一种从结果到原因分析灾害事故中各种因素之间的因果关系和逻辑关系的工具。

- 通过绘制事故树，可形象地理解事故与原因之间的因果联系
- 采用演绎分析方法分析事故因果关系
- 假设事故场景后，可找到潜在的危险因素，为安全设计和防错管理提供依据
- 简洁形象地表示事故和各种原因之间的因果关系

事故树分析的基本程序





- 熟悉基本程序和系统
- 进行调查分析（与相关人员交流）
- 需明确管理、标准制定、法规遵循、制度执行及教育培训的目的
- 对未按规定执行的情况进行分析

事故树分析的应用案例



例

LPG（液化石油气）槽车事故分析：

- 事故涉及超车、着火，LPG 是可燃物，需同时具备可燃物、助燃物、点火源三个条件
- 泄露原因可能包括焊缝或接头设计缺陷、车辆翻覆或焊接质量不佳、超载和转弯过快导致翻车
- 处理措施：喷淋降温、防止局部聚集性气体、确保火势完全燃烧并控制在原地、及时疏散周边区域
- 与氢气相比，LPG 的最小点火能更大，但一旦发生事故后果严重

例

打火机火灾事故：打火机内塑料制品及气体，点火时先按按钮让气流出来，只需一点火星即可点燃，是典型的小型火灾事故。

例

机械厂地面火星事故：机械厂老板误以为地面脏，实际是地面容易产生火星（非防静电地面），鞋容易产生火星但无防止措施，导致火灾隐患。

事故树的定量分析

- 定量分析包括评估事件发生的概率，以及计算概率重要度和临界重要度
- 事故后果的计算通常非常庞大，需借助计算机处理
- 准确知道事故中每个事件发生的概率是挑战，但目前已能获取许多故障发生的概率数据

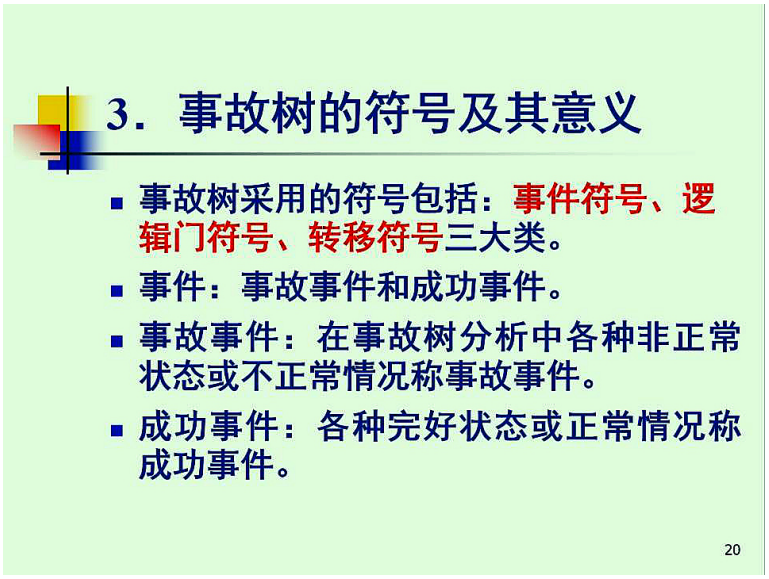
事故树分析的应用领域

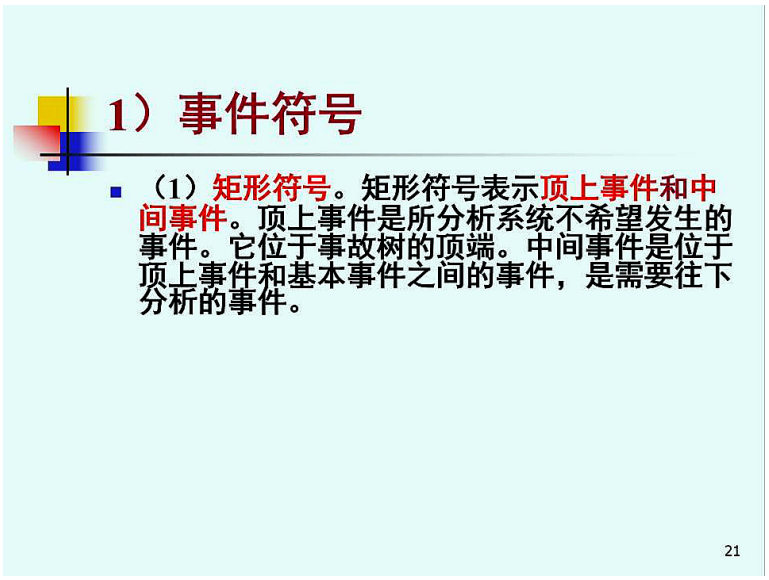
- 许多事件已经发生，有些是设想的情景
- 在军事领域常用于模拟作战场景，如防止无人机攻击的作战产品研发
- 民用领域应用广泛，如低空经济示范点（无人机、无人船、无人艇、无人车）

事故树分析的基本概念与流程

- 事故树分析（FTA）以顶上事件为起点，通过逻辑符号和逻辑门构建图形，形成事故树
- 编制流程：收集资料 → 确定顶上事件 → 简化 → 修改 → 定性分析 → 定量分析 → 制定安全措施
- 分析深度取决于细化程度：越细越深，但越深越复杂，人力物力投入越大
- 现代系统常采用模块化诊断：设备故障通过电脑诊断确定具体模块后直接更换，无需深入内部零件（如阀芯、法兰等）
- 电器继电器、开关、马达等组件故障可直接通过计算机诊断，无需分解到内部零件

事故树的事件符号

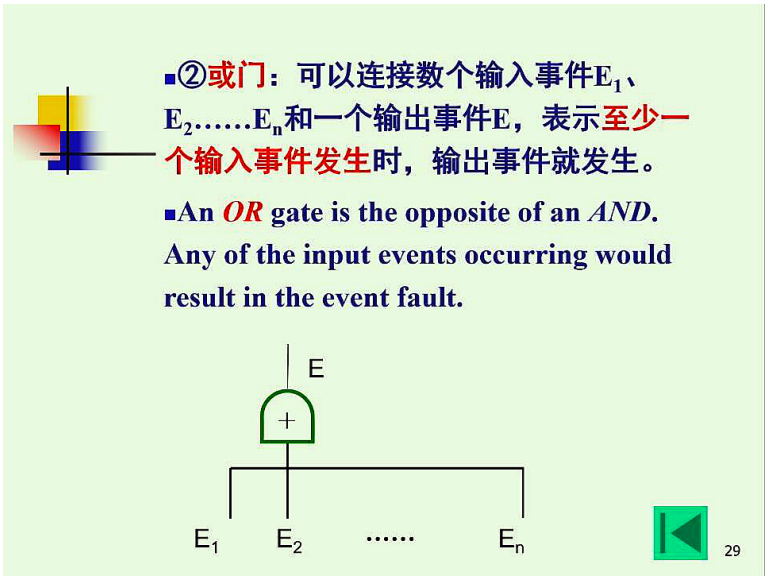




- 矩形符号：表示顶事件和中间事件，需要进一步分解
- 圆形符号：表示不能再细分的基本事件，位于事故树底部
- 菱形符号：表示需要进行分析的事件
- 环形符号：代表正常事件和开关事件，正常事件无需进一步细分
- 三个基本事件（底事件）合在一起构成一个复合事件

逻辑门符号



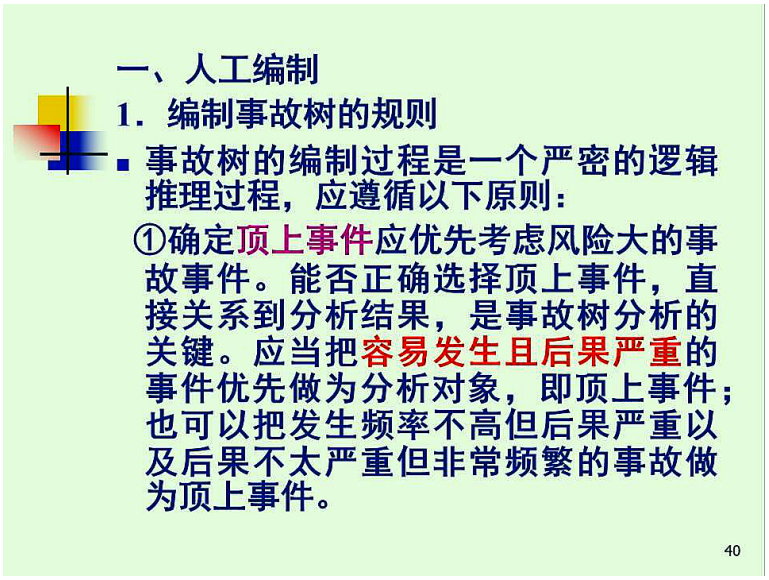


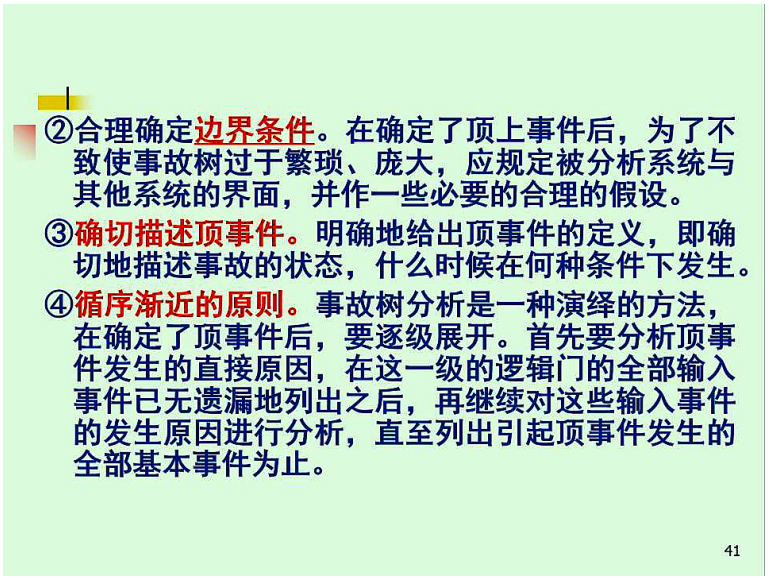
- 与门：所有输入端都必须发生，输出才发生
- 或门：至少有一个输入端发生，输出就发生
- 条件与门：输入事件不仅同时发生，还必须满足特定条件，输出才发生
- 条件或门：至少有一个输入发生，且满足条件 V 时，输出才发生
- 表决门：当输入事件数量 M ⩽ N 时，输出事件发生
  - M=1 时相当于或门（只要有一个发生）
  - M=N 时相当于与门（所有都发生）
- 异或门：仅当单个输入事件发生时，输出事件才发生（不同时发生）
- 禁门：当条件事件发生时，输入事件的发生才导致输出事件的发生
- 转移符号：从三角形图形中转移，再导出三角形，用于简化重复结构

例

爆炸极限：爆炸发生必须达到爆炸极限，即存在火源和油气聚集两个条件同时满足。氧气瓶超压爆炸：只要存在气体或热源（如火源或太阳暴晒），就可能达到其强度极限。

事故树编制的原则



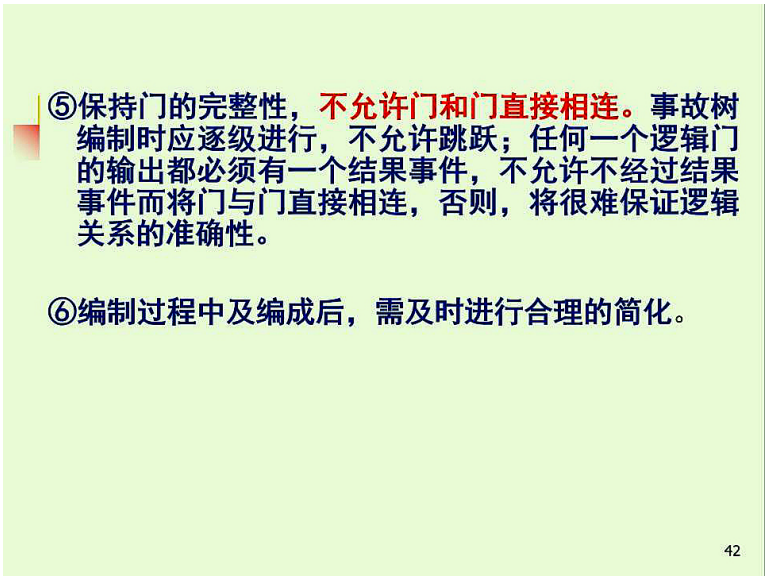


- 选择顶上事件要遵循基本原则，坚持”一棵树到底”，不能太笼统
- 顶上事件描述应具体，如”LPG 储罐爆炸”或”氧气瓶超压爆炸”，而非”过程火灾”或”化工厂爆炸”等宽泛表述
- 确定边界条件时，应合理设定标准
- 既要考虑发生频率高且后果严重的事故，也要关注频率低但后果严重、以及后果不严重但频率高的事故
- 准确描述事件非常重要，表述不能模糊不清

注意

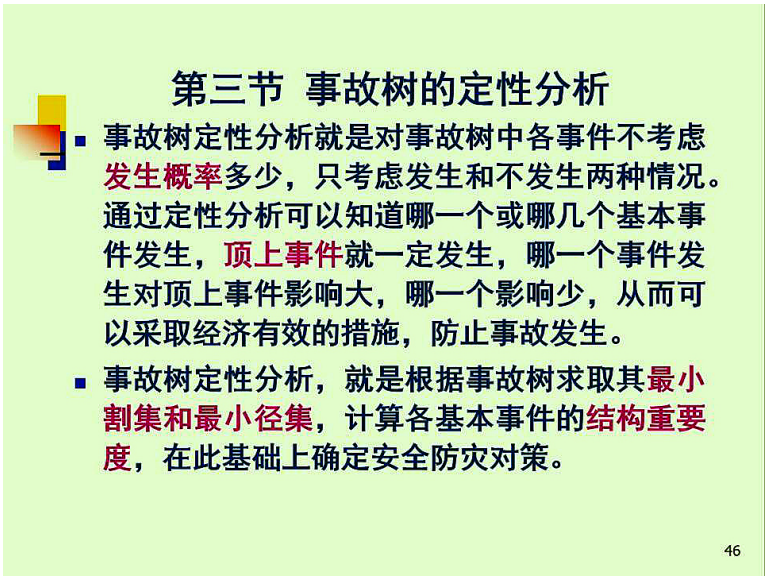
表述准确性示例：说”应急管理基础薄弱”与”应急管理基础仍显薄弱”含义不同。前者暗示五年内几乎没有采取措施，后者则承认不足的同时强调已取得的进步。对他人的工作不能全盘否定，表述上要准确。

事故树编制的注意事项



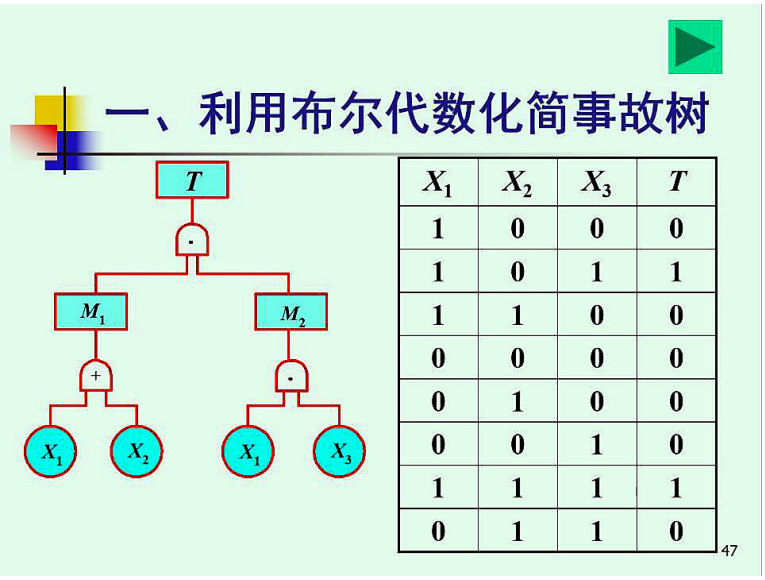
- 逻辑门的简化：用演绎方法编制，可能一开始不完全正确，需经讨论后修改完善
- 保持门的完整性：不允许门和门之间直接相连，必须有一个基本事件
- 事故树编制是否完善，直接影响定性定量分析的准确性，关系到事故处理的成败
- 需要设计人员、操作人员和可靠性分析人员的参与，需要一定专业知识
- 事故调查小组会指派专业人士进行调查

定性分析与定量分析



- 定性分析：不考虑基本事件发生的概率，只关注事件发生与否
  - 求解最小割集和最小径集
  - 计算各个基本事件的结构重要度
  - 确定哪些事件对顶事件影响最大、哪些最小
- 定量分析：从量化角度分析每个基本事件对顶事件的影响程度
  - 引入轻重缓急和优先级概念进行控制
  - 为安全措施提供依据，是经济合理的选择

最小割集与化简



X_1	X_2	X_3	T
1	0	0	0
1	0	1	1
1	1	0	0
0	0	0	0
0	1	0	0
0	0	1	0
1	1	1	1
0	1	1	0

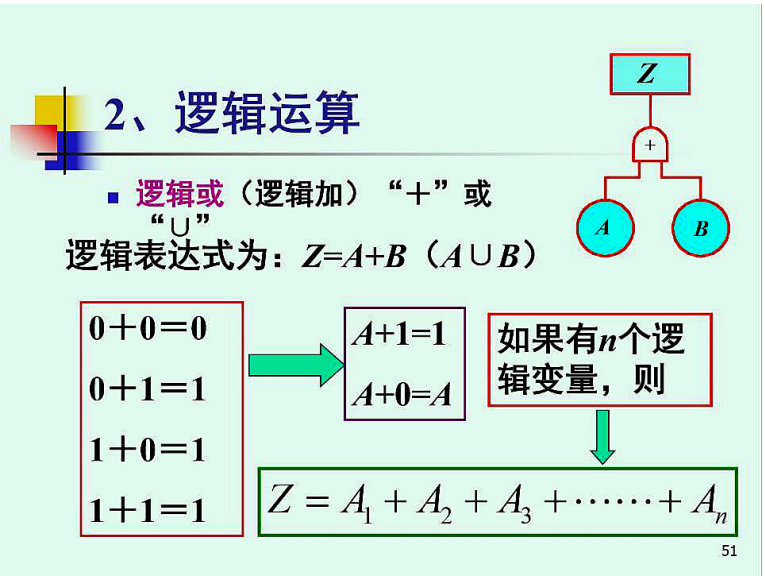
- 最小割集：导致顶事件发生的最少基本事件的集合
- 化简方法：利用布尔代数进行逻辑运算
- 化简示例：若 M1、M2 中包含了 X1、X2、X3，则 M1 · X1 · X2 · X3 不再需要，可简化
- 当基本事件数量较多时，不能一一列举，需通过布尔代数化简

注意

给出的四个数字（基本事件组合）并非最简形式。若是最简形式，就不会出现”X1 发生而 X2、X3 未发生时顶事件是否发生不确定”的情况。化简后，某些基本事件（如 X2）可能被吸收消除。

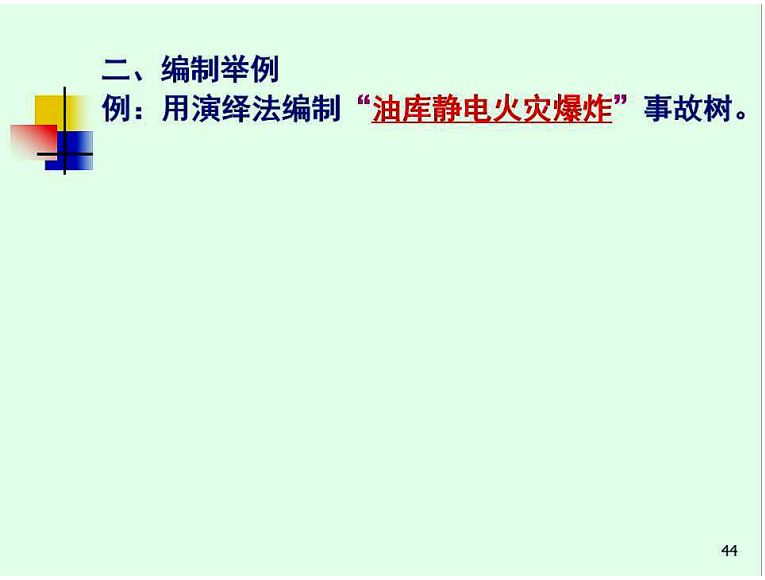
布尔代数基础

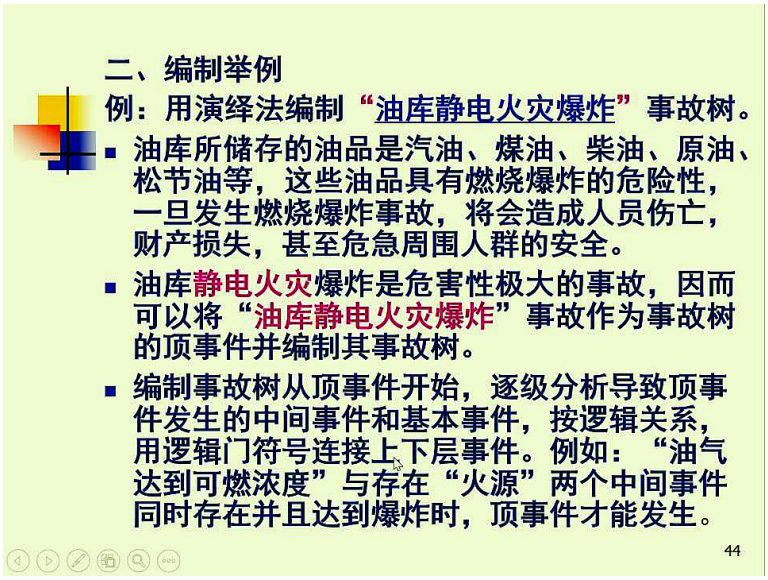




- 逻辑运算与传统计算方式不同
- 逻辑值：0 和 1
- 基本运算规则：
  - 0+0=0，0+1=1，1+0=1，1+1=1（逻辑或）
  - 逻辑与、逻辑或（不是”陈”或”交”，而是逻辑乘和逻辑加）
- 逻辑运算使事故树分析变得简单

油库静电火灾爆炸事故树案例





- 顶上事件：油库静电火灾爆炸
- 发生条件：静电火花 + 油气达到爆炸极限（可燃浓度）
- 静电火花的产生原因：
  - 人体放电（人体与化学品摩擦、作业中与导体接触）
  - 油液流速过高（高速抽水产生静电）
  - 接地不良（接地电阻超标、接地线损坏）
  - 静电积聚
- 油气存在的正常事件：油库中无明火，管理严格
- 通风不良是基本事件
- 油库储存的油品包括汽油、煤油、柴油、原油、松节油等，对周边人员和设施构成安全威胁

例

油罐抽油不能简单抽干：油罐有低液位和低低液位报警。低低液位时不能继续抽，否则真空度过高会导致油罐瘪掉。解决方法是在油罐中加水，使油浮起，只抽取上部的油。

注意

水射流与空气混合产生静电：水从水龙头喷出形成水射流时，与空气中气体混合物接触，因摩擦产生静电，可能导致蒸汽爆炸。杂质含量越高，爆炸风险越大。

生产车间燃烧爆炸事故

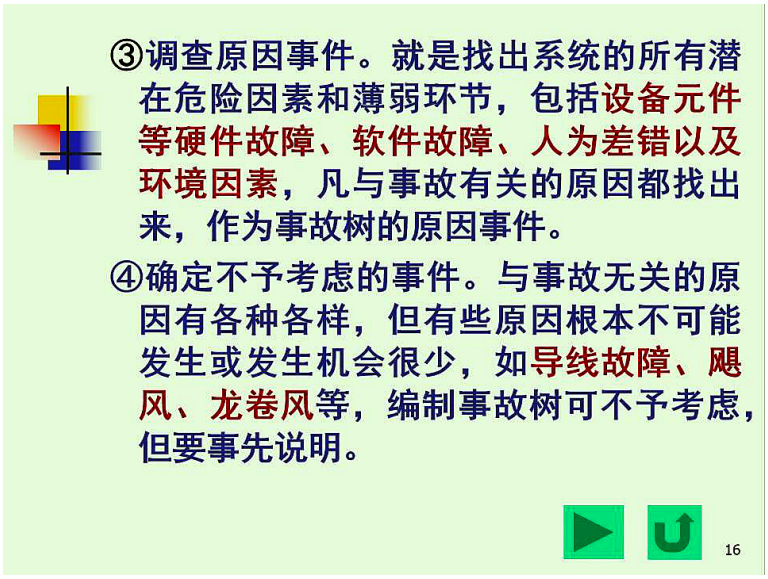
- 甲类生产车间（易燃易爆火灾危险场所）易发生燃烧爆炸事故
- 典型案例：LPG 气瓶火灾爆炸事故
- 钢瓶内液化气泄漏导致爆炸（LPG 泄漏燃爆），钢瓶放置在室内（如厨房）非常危险且常见

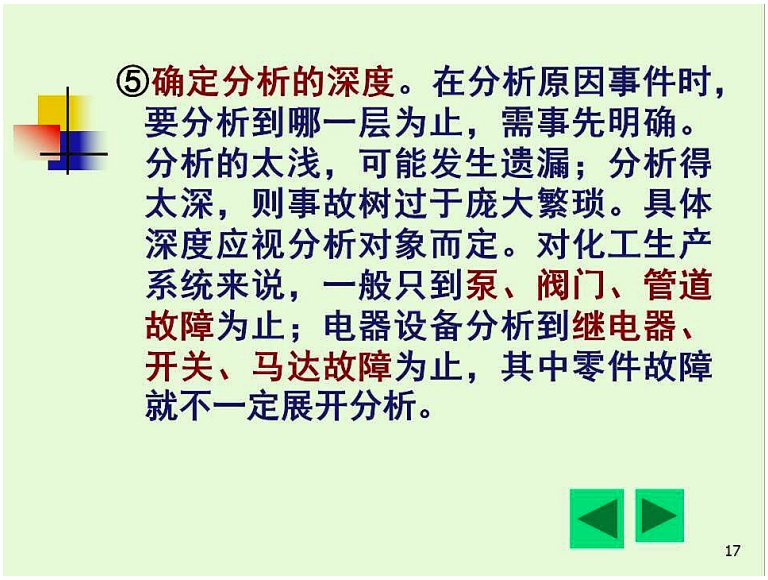
作业内容



- 并联和串联情况的事故树分析
- 钢瓶内液化气泄漏导致的爆炸（LPG 泄漏燃爆）事故树编制
- 油库静电火灾爆炸事故树编制

事故调查与原因分析





- 调查事故主要分析可能的原因
- 分析方法：经验、技术、量化模拟
- 参考同类事故：本单位、同行业、国内外类似事故
- 国内外有公开的事故数据库可供查询（法国、美国、欧盟/英国等），约六七个事故资料可供参考
- 需确定并熟悉分析系统：工艺流程、设计构架、设计条件、管理状况、控制系统及安全措施

多灾种耦合风险研究

- 考虑不被考虑的因素：导线故障、飓风、龙卷风等灾害
- 考虑过多会使情况复杂、结果不准确、针对性不强
- 欧洲专门机构资助多灾种耦合风险研究，具有系统性和灾难性特征
- 典型案例：日本地震引发海啸，导致核电站泄漏

例

早茶店火灾案例：使用液体燃料（柴油或煤油）储存在地下 2 楼，通过泵抽取至地上 3 楼灶头。液体燃料比重较小，渗透到各灶头燃烧。若燃料含二甲醚等成分，橡胶密封件过期会渗漏引发火灾。传统早餐店使用小气瓶加热，推车移动时发生爆炸。

注意

逃生方向：火灾时人员跑反方向是因为没有考虑清楚。应往有路的方向跑，若被困应靠近窗户并倒下。这体现了安全素养的重要性。

安全管理的实践与素养

- 安全管理效果好的企业：岗位责任、直线责任明确，考核到位
- 安全管理人员待遇相对较高，招聘专业人才（如安全总监）
- 许多安全问题依赖于人的素养和精神
- 学习安全知识后必须到现场实践，用心发现细节，才能勇敢面对并解决问题

新业态的安全挑战

- 低空经济：存在系统安全约束，需要研究
- 氢能产业：液氢需达到零下 253 度以下的低温，不仅对人危险，对所有生物都有

危险
- 锂电池安全状况已有所改善
- 这些新业态存在技术性挑战，需要深入研究

10 月 20 日

课程要求与作业制度

- 作业成绩取最好的三次成绩
- 不认真、不交作业、不重视平时任务的同学，平时成绩可能照顾不到
- 提醒大家重视课堂练习，提前准备好白纸等工具
- 尽量不要坐到最后一排，保持课堂认真态度
- 第二学期为小班教学，人员构成相对固定，需重视团队协作

事故树分析（FTA）的基本概念

- 事故树分析是一种**演绎方法**，从结果到原因进行分析
- 既可用于**定性分析**，也可用于**定量分析**
- 将因果关系和逻辑关系用图形（倒置树形）表示出来
- 分析过程中涉及的主要程序：如何准确设计、构建、分析到什么程度
- 需要掌握的基本概念：偏差、意图、目的、引导词
- 对于复杂系统，需要明确分析人员构成、背景知识要求，以及如何判断和分析

定义

事故树分析（Fault Tree Analysis, FTA）是从结果到原因，用图形表示导致与灾害事故有关的各种因素之间的因果和逻辑关系的一种分析方法。

事故树分析的目的

- 通过对系统进行定性定量分析，找出顶上事件发生的路径
- 明确典型事件发生的原因、逻辑和因果关系
- 确定系统中需要重点关注的基本要素
- 有效控制风险的两个方面：
  - 发生的可能性（在预防方面作用显著）
  - 发生可能引起的后果
- 目标是达到**优化的最佳状态**，而非无穷尽地降低风险

注意

风险控制不是无限度的。技术达不到或经济达不到时，需要权衡是否冒这个风险。例如有人以房产做抵押贷款，一旦杠杆失衡，后果严重——这就是风险观念的体现。

事故树分析的特点

- 可能发生的事故（顶上事件）放在树的顶部
- 中间设计基本设备（中间事件）
- 基本事件是**相对的**，不是绝对的——分析到某一程度即可停止，但实际还可继续细分

例

油罐车在高速公路高架桥上着火事故：
- 第一层次：可燃物
- 第二层次：助燃物
- 第三层次：法兰连接处断裂导致泄漏
- 翻车导致法兰破坏进一步分析：转弯时超速 → 车速过快 → 可能原因包括路面摩擦小（雨天）、司机主观因素、刹车故障等，说明基本事件还可继续细分。

事故树分析的优点

- 详细找出系统各种固有的危险因素，为安全设计、安全技术措施、安全教育提供依据
- 简洁形象地表示出因果关系和逻辑关系
- 通过分析原因来控制顶上事件
- 具有预防预测功能：即使事件尚未发生，也可预想并检查是否有相应措施
- 可对感兴趣的事件进行顶上事件分析
- 可进行定量分析，确定各种危险因素对系统影响的大小
- 若已知各基本事件发生概率，可计算顶上事件发生的概率

事故树分析的缺点

- 需要分析人员经验非常丰富、对系统非常熟悉
- 系统复杂时，定量分析和定性分析都比较困难（现在计算机一般可实现）
- 基本事件发生的概率有时难以准确掌握，影响计算结果

注意

事故树分析最大的缺点是：对分析人员的经验要求高，且基本事件发生概率难以准确获取，这会影响定量计算的准确性。

事故树分析的基本程序

- 基本程序分为两个阶段，共五个步骤：

1. **确定顶上事件**：选择可能性较大或后果较严重的事件
   - 需收集同行业、本单位、国内外的类似事故资料
   - 例如：危险品运输车需考虑司机、路线、时间、装载量、车辆状况、押运等条件
2. **确定边界条件**：明确分析范围
3. **定义要明确**：顶上事件的定义必须清晰具体
   - 例如：“加氢反应器温度过高”比“化工厂爆炸”更明确
4. **调查事故原因**：分析导致顶上事件的各种原因
5. **确定分析深度**：根据分解程度决定
   - 例如：生产系统 → 电气设备 → 继电器/马达/开关 → 马达内部故障

例

确定顶上事件时需考虑可能性与后果：
- 高空坠落（脚手架上）
- 物体打击（建筑工地吊杆操作）
- 这些事件发生的可能性较大或后果严重，应作为重点分析对象

注意

有些原因可以不予考虑，例如龙卷风导致家庭火灾爆炸这类可能性极小的因素，属于预先排除的范围。

事故树的基本符号

- **事件符号**：圆形符号表示基本事件，矩形符号表示顶上事件或中间事件
- **逻辑门符号**：与门、或门、条件门、表决门、非门等
- **管理符号**：用于表示转移等

注意

逻辑门中，与门和或门是计算题中一定会用到的，必须掌握。条件门、表决门、非门等特殊情况也要了解。表决门需明确什么情况下与门、什么情况下过门。

事故树的编制

- 由较多人员构成：系统设计人员、操作人员、符合性培训人员、管理人员等
- 可采用人工编制和计算机编制
- 编制过程需循序渐进，遵循基本编制原则

编制基本原则

1. 风险大的作为顶上事件（风险大 = 容易发生 + 后果严重）
2. 合理确定边界条件
3. 准确描述事件
4. 提出改进建议
5. 中间事件必须有一定的时间采取相应措施

事故树的定性分析

- 定性分析包括：**最小割集、最小径集、结构重要度**
- 结构重要度：在已知系统树的基本逻辑关系和因果关系基础上，分析每个基本事件的重要程度
- 定性分析首先需要弄清楚布尔代数的分析过程

定义

结构重要度：不考虑基本事件发生概率，仅从系统树的结构（逻辑关系）出发，分析各基本事件对顶上事件影响程度的大小。

逻辑运算基础

- 逻辑变量取值只有 0 和 1，分别代表事件不发生与发生
- 三种基本逻辑运算：逻辑或（+）、逻辑与（·）、逻辑非（¬）
- 逻辑或：$Z = A + B$，任一输入为 1 则输出为 1
- 逻辑与：$Z = A \cdot B$，所有输入为 1 才输出为 1
- 逻辑非：输入取反，如 $\neg 0 = 1$，$\neg 1 = 0$

定义

逻辑或（OR）：只要有一个输入为真，结果为真。逻辑与（AND）：所有输入为真，结果才为真。逻辑非（NOT）：对输入取反。

逻辑代数基本定律

- 交换律：$A + B = B + A$，$A \cdot B = B \cdot A$
- 结合律：$(A + B) + C = A + (B + C)$，$(A \cdot B) \cdot C = A \cdot (B \cdot C)$
- 分配律：$A \cdot (B + C) = A \cdot B + A \cdot C$，$A + B \cdot C = (A + B) \cdot (A + C)$
- 同一律：$A + 0 = A$，$A \cdot 1 = A$
- 互补律：$A + \neg A = 1$，$A \cdot \neg A = 0$
- 幂等律：$A + A = A$，$A \cdot A = A$
- 吸收律：$A + A \cdot B = A$，$A \cdot (A + B) = A$
- 双重否定律：$\neg(\neg A) = A$
- 德摩根定律：$\neg(A + B) = \neg A \cdot \neg B$，$\neg(A \cdot B) = \neg A + \neg B$

注意

逻辑代数中的”加”和”乘”与普通代数不同：$A + A = A$（不是 $2A$），$A \cdot A = A$（不是 A^2）。运算时务必按逻辑定律，不能套用普通代数规则。

事故树的化简

- 复杂事故树先写出布尔代数表达式，再按逻辑定律逐步化简
- 化简过程要严格按逻辑运算规则，一步步进行，不能跳步
- 化简到最简形式后，可画出等效事故树
- 化简结果用于后续的定量计算，若此处出错，后续量化计算（约 15 分）会连带出错

例

展开 $(A + B)(A + C)$：$= A \cdot A + A \cdot C + B \cdot A + B \cdot C = A + A \cdot C + A \cdot B + B \cdot C = A + B \cdot C$（利用吸收律化简）

割集的概念

- 凡是能导致顶上事件发生的基本事件的集合，称为割集
- 割集是系统发生故障的途径或模式
- 若割集中所有基本事件都发生，顶上事件必然发生
- 事故树中所有基本事件都发生时，顶上事件必然发生，但通常只需少数几个基本事件发生即可导致顶上事件发生

定义

割集：能导致顶上事件发生的基本事件的集合，即系统发生故障的模式或途径。

最小割集的概念

- 割集的数目可能很多，内容上可能包含、重复或有多余事件，需要去除
- 除去多余事件后的割集称为最小割集
- 最小割集是能导致顶上事件发生的最低限度的基本事件集合，去掉其中任何一个事件就不再是割集

定义

最小割集：能导致顶上事件发生的最低限度的基本事件的集合。去掉其中任一基本事件，顶上事件就不再发生。

注意

割集与最小割集的区别：割集可能包含多余事件，最小割集不含任何多余事件。化简事故树的目的就是找出最小割集，去掉冗余事件。

最小割集与系统危险性

- 事故树中有一个最小割集，顶上事件发生的可能就有一种途径
- 最小割集越多，顶上事件发生的可能途径越多，系统越危险
- 通过最小割集可找出控制事故的最佳途径——控制最少的基本事件即可防止顶上事件发生

例

某等效事故树的最小割集为 {x1, x3}、{x3, x5}、{x3, x4}、{x1, x5}。只需控制 x3 和 x5 两个基本事件，即可防止顶上事件发生，这是控制事故的最佳途径。

集合的基本概念

- 集合：满足某种条件或具有某种属性的事物的全体
- 集合的每一个成员称为该集合的元素
- 割集中的每个基本事件就是该集合的一个元素
- 并集：把两个集合合在一起，对应逻辑”或”
- 交集：两个集合的公共元素，对应逻辑”与”

最小割集的求法

- 求最小割集有两种主要方法：布尔代数法和行列法
- 布尔代数法：先列出事故树的布尔代数表达式，用逻辑运算定律化简，最后得到若干交集（每个交集即一个最小割集）
- 行列法：按行和列的方式逐层展开求最小割集
- 布尔代数法较为通用，是常用的求解方法

注意

行列法不是”行列式法”，而是按行和列逐层展开的方法，两者不要混淆。

例

用布尔代数法求最小割集：设 $T = A \cdot B$，其中 $A = x1 + x2$，$B = x3 + x4$，则 $T = (x1 + x2)(x3 + x4) = x1 \cdot x3 + x1 \cdot x4 + x2 \cdot x3 + x2 \cdot x4$，得到 4 个最小割集：{x1, x3}、{x1, x4}、{x2, x3}、{x2, x4}。

求解最小割集的注意事项

- 化简过程较复杂，必须细心，一步一步按逻辑定律进行
- 前面一旦出错，后续量化计算会连带出错
- 事故树分析是安全系统工程的重要学习要点，需熟练掌握
- 化简到最简形式后，可画出等效事故树，便于直观判断控制途径

布尔代数法化简事故树

- 布尔代数法是求最小割集的方法之一，依据布尔代数运算法则，对事故树逐步展开、逐步化解，最终得到等效最简事故树
- 运算中：或门对应”加”（逻辑或），与门对应”乘”（逻辑与）
- 化简过程要一步一步按原理和准则进行，不可跳跃，避免遗漏或失误

- 门与门之间不能直接连接，中间必须经过中间事件

行列法（富塞尔法）求最小割集

- 行列法又称富塞尔法，由学者富塞尔提出
- 基本原理：与门使割集的大小增加（横向展开），或门使割集的数量增加（纵向展开）
- 操作方式：或门纵向列出，与门横向列出，逐层替代直至全部为基本事件
- 展开后如有交集，再用布尔代数进一步简化，最终得到最小割集
- 与门 → 割集大小增加；或门 → 割集数量增加（平行行数增多）

注意

用行列法展开时，应一次只展开一个门，逐步进行。若同时把多个门一起展开，容易在计算中出现遗漏或失误。例如先展开 g1（或门）保留 g2，再展开 g2，而不是同时展开。

例

某事故树用行列法求得最小割集为 {1,4}、{3,5}、{1,2,3}。展开过程中若跳跃步骤，容易漏掉 {1,2,3} 这一项，需仔细核对每一步展开结果。

径集与最小径集

- 割集表示顶事件发生的模式或路径；最小割集一旦发生，顶事件必然发生
- 径集：不导致顶上事件发生的基本事件的集合，表示系统不发生故障、正常运行的模式
- 径集越多，系统成功运行的可能性越大，系统越安全
- 径集中若存在相互包含或重复的事件，去掉后形成最小径集

定义

最小径集：顶上事件发生的最低限度的基本事件的集合。去掉其中任何一个基本事件，它就不再是径集。

- 最小径集越多，顶上事件不发生的途径越多，系统越安全；但系统越安全，投入也越大

对偶树（成功树）与最小径集的求法

- 将原事故树转化为对偶数（成功树）：与门变或门、或门变与门，事件取其非
- 求成功树的最小割集，即为原事故树的最小径集
- 依据布尔代数法则：合的非等于非的合（德摩根定律），积的非等于非的和

注意

若原事故树中含有条件与门、条件或门或限制门，在转化为成功树（对偶数）时，应将这些条件作为基本事件处理。教材未涉及此内容，其他教材有详细过程。

例

某事故树求最小径集：先画出其对偶数（成功树），再求成功树的最小割集。如某事故树的最小割集为 {x1, x3}，其最小径集需通过成功树的最小割集求得，结果可表示为三个最小径集。

最小割集与最小径集在事故树分析中的作用

- 最小割集的作用（4 个方面）：

  - 表示系统的危险性
  - 表示顶事件发生的原因组合
  - 为降低系统的危险性提出控制方向和预防措施
  - 判定事故树中基本事件的结构重要度，方便计算顶事件发生的概率
- 最小径集的作用（3 个方面）：
  - 表示系统的安全性
  - 依据最小径集选取确保系统安全的最佳方案
  - 判定事故树中基本事件的结构重要度，计算顶事件发生的概率

注意

最小割集与最小径集的作用中，前两点不同（割集侧重危险性/原因组合，径集侧重安全性/最佳方案），但第三点相同——两者都可用来判定结构重要度和计算顶事件发生概率。

结构重要度的概念与本质

- 结构重要度：不考虑基本事件发生概率的大小，只定性考虑各基本事件发生对顶事件发生的影响程度
- 作用：明确基本事件对顶事件发生的影响程度，从而确定优先采取措施的方面，有针对性地防控顶事件
- 属于**定性分析**范畴，但非常重要

定义

结构重要度是指在不考虑基本事件发生概率的情况下，分析各基本事件发生对顶事件发生的影响程度，用于判断哪些基本事件更值得优先控制。

结构重要度的两种分析方法

- **精确法**：计算各基本事件的结构重要度系数，从大到小排序，相对精确
- **近似法**：用最小割集和最小径集近似判断基本事件结构重要度的大小并排序，简便但可能有偏差
- 当事故树复杂、割集多时，精确法计算量大，宜采用近似法

事故树的结构函数

- 顶事件是基本事件的状态函数，基本事件只有两种状态：发生（1）和不发生（0）
- 基本事件从 0→1 变化时，顶事件可能有三种变化：
  - 0→0：顶事件始终不发生
  - 0→1：顶事件随基本事件变化而变化
  - 1→1：顶事件始终发生
- 有 n 个基本事件时，组合总数为 2 的 n 次方；固定一个基本事件变化、其余不变时，对照组为 2 的 n-1 次方

例

3 个基本事件时，组合总数为 $2^3=8$ 种；固定 X1 从 0→1、其余不变时，对照组为 $2^2=4$ 种。

结构重要度系数的计算

- 结构重要度系数用函数表示，反映某一基本事件变化时顶事件随之变化的组合所占比例
- 以图 2-13（4 个基本事件）为例：n=4，2 的 n-1 次方 =8 个对照组

- 当 X2 由 0 变为 1 时顶事件由 0 变为 1 的情况有 5 种，则其结构重要度系数为 5/8
- 其余基本事件系数分别为 3/8、1/8、1/8
- 当 n 很大时，精确计算困难，需用简化方法

结构重要度的近似判断公式

- 设最小割集中有 k 个，含有 m 个基本事件，基本事件 Xi 的结构重要度系数用简化公式近似计算
- 公式可不必死记，但要会判断排序

例

三个最小割集 {X1}、{X1,X2}、{X1,X3}：

- X1：$1/3\times1 + 1/2\times1 + 1/2\times1 = 10/9$
- X2：$1/3\times1/2 = 1/9$
- X3：$1/3\times1/2 = 1/9$ 排序：X1 > X2 = X3

近似判断的四条原则

1. **单事件最小割集（径集）中的基本事件结构重要度最大**
   - 如最小割集 {X1}，则 X1 的结构重要度系数最大
2. **仅出现在同一个最小割集（径集）中的所有基本事件结构重要度相等**
   - 如 {X2,X3} 中 X2 与 X3 相等；{X4,X5,X6} 中三者相等
3. **仅出现在基本事件个数相等的若干个最小割集（径集）中的各基本事件，结构重要度依出现次数而定**
   - 出现次数多的结构重要度大，出现次数少的相等
4. **两个基本事件出现在基本事件个数不等的若干个最小割集中，需按具体情况比较**

注意

这 4 条原则必须按顺序进行判断，不能单纯使用近似判别式，否则会得到错误结果。最基本、最重要的是第一条。

例

最小割集为 {X1,X2,X3}、{X1,X4}、{X2,X5}、{X2,X6}：

- X1 出现次数多，结构重要度大
- X3 与 X4 相等，X2 与 X5 相等
- 排序：X1 > X3 = X4 > X2 = X5

近似判断的另一种公式

- 当最小割集为 {X1,X2}、{X1,X3}、{X2,X4}、{X2,X5} 等结构时，可用 2 的 (m-1) 次方形式的近似公式判断
- 如 5 个最小割集 {X1,X2}、{X1,X3}、{X2,X4}、{X2,X5}、{X2,X6}，用 2 的 (m-1) 次方近似计算
- 此方法不一定准确，一般了解即可

注意

用最小割集和最小径集判断结构重要度，两者的结果应该一致；若不一致，需仔细核对。

结构重要度分析的应用

- 用于确定安全检查表中需要重点反映的项目
- 用于日常检查、日常管理控制的基本要点
- 为选择控制事故的最佳方案提供依据

事故树定量分析的基本认识

- 最基本要求：求顶事件发生的概率
- 前提：必须知道基本事件发生的概率，否则计算顶事件概率没有依据
- 求出顶事件概率后，可与系统目标值比较，判断是否超标
- 若超标，需分析降低哪些基本事件的发生概率（结合结构重要度、概率重要度、关键重要度等）

> **注意**
>
> 结构重要度在定量分析中表现不出优势，因为还需要考虑概率重要度、临界重要度等敏感性指标——即某个基本事件概率降低一点点，顶事件概率就降低很多的情况。

事故树定量分析的基本条件

- 各基本事件的参数或故障率已知，且数据可靠
- 事故树中应完全包括主要的故障模式
- 对全部事件用布尔代数做正确描述

定量分析的假设条件

1. **基本事件相互独立**：彼此之间没有关联性，相关系数为 0
   - 若存在相关性（如 X1 与 Y1 相关），则假设不成立，前述分析不成立
2. **基本事件和顶事件只考虑两种状态**：发生和不发生
3. **故障分布为指数函数分布**：故障率函数为常数（U 形曲线底部平坦部分）

> **定义**
>
> 故障率函数为常数时，可靠度 R = e^(-λt)，不可靠度 F = 1 - e^(-λt)，此时故障服从指数分布。

> **例**
>
> 故障率函数呈 U 形（浴盆曲线），其底部平坦，说明故障率为常数，因此故障服从指数分布。

平均无故障工作时间 MTBF

- MTBF（平均无故障工作时间）= 1/λ，为常数
- 在故障率为常数的假设下，MTBF 也是常数

系统单元的故障概率

- 单元故障概率：$q = \lambda / (\lambda + \mu)$
  - λ：单元故障率（单位时间内故障发生的频率）
  - μ：修复率
- 由于 λ 远小于 μ，故 $q \approx \lambda/\mu$
- λ = 1/MTBF（平均故障间隔期）
- μ = 1/MTTR（平均修复时间）

- MTBF 远大于 MTTR

> **注意**
>
> K 为修正系数，与温度、湿度、振动及其他环境条件密切相关，用于修正故障概率。

人的失误概率

- 人的失误是导致事故发生的重要原因，但事故树分析中很少将人作为基本事件，这是薄弱环节
- 人的失误概率受温度、环境压力、疲劳、社会因素等复杂因素影响，难以准确确定
- 人因工程学、人机工程学、后勤工程学（logistics）对此有深入研究
- 若有统计数据，可用统计结果；否则更多考虑元件或部件的故障概率

> **注意**
>
> 元器件故障概率与人的失误概率之间有关系，但人的失误概率通常不准确，需专门研究。

10 月 27 日

布尔代数与摩根定律

- 事故树化简最终归结为摩根定律的两个基本形式
- 摩根定律是事故树化简中最核心、最常用的工具
- 逻辑值运算需掌握：等幂率、吸收率、交换率、结合律、分配律等
- 化简过程中需注意基本事件的吸收、合并

> **定义**
>
> 摩根定律（De Morgan's Law）：
> - 和的非等于非的积：$\overline{A+B}=\overline{A}\cdot\overline{B}$
> - 积的非等于非的和：$\overline{A\cdot B}=\overline{A}+\overline{B}$

> **例**
>
> 无条件时，与门可直接变为或门，或门变为与门，同时加上一个”非”。若有条件时，需把条件变成一个基本事件再处理。

割集与最小割集

- 割集：能导致顶事件发生的基本事件的集合
- 最小割集：最低限度的基本事件构成的割集，去掉任何一个基本事件就不再是割集
- 割集表示顶事件发生故障的模式或路径
- 割集越多，系统失效的可能性越大，事故的危险程度越高

> **定义**
>
> **割集**：能导致顶事件发生的基本事件的集合。**最小割集**：若割集中任意去掉一个基本事件后就不再是割集，则称该割集为最小割集。

注意

割集越多 → 失效可能性越大 → 危险性越高。这是考试中常考的判断/选择点。

径集与最小径集

- 径集：不导致顶事件发生的基本事件的集合（即成功）
- 最小径集：不导致顶事件发生的最低限度的基本事件的集合
- 径集越多，系统越安全
- 控制事故可从两方面入手：控制割集不让其发生，或利用径集保证成功

定义

径集：不导致顶事件发生的基本事件的集合（成功集）。**最小径集**：不导致顶事件发生的最低限度的基本事件的集合。

注意

割集对应”事故/失败”，径集对应”成功”，两者互为对偶关系，注意区分。

最小割集与最小径集的求解方法

- 方法一：布尔代数化简法
- 方法二：行列法（行列式法）

注意

行列法两个原则：

- 与门：增加割集（或径集）的**个数**，不增加元素
- 或门：增加割集（或径集）的**元素**，不增加个数

从左到右展开时，要分清是增加个数还是增加元素，不要混淆。

结构重要度分析

- 结构重要度：反映基本事件发生对顶事件发生的影响程度，不考虑基本事件发生概率
- 两个基本求解思路：
  1. 通过结构函数分析（较准确）
  2. 近似判断（利用最小割集或最小径集）

定义

结构重要度：不考虑基本事件发生概率，仅从结构上分析基本事件发生对顶事件发生的影响程度。

注意

近似判断不一定准确，结果可能有偏差。若近似方法能完全符合要求，可不采用结构函数法；否则需用结构函数法验证。

结构重要度系数的求法

- 基本事件从 0→1 变化时，观察顶事件状态是否随之变化
- 顶事件状态随基本事件变化而变化的次数，即为结构重要度判断依据
- 需罗列基本事件从 0→1 时顶事件变化的全部状态（共 2^{n-1} 种）

例

4 个基本事件时，$n=4$，需考察 $2^{4-1}=8$ 种状态。若某基本事件从 0→1 时顶事件有 5 个状态发生变化，则其结构重要度系数为 $5/8$。

结构重要度的近似判断

- 利用最小割集或最小径集进行近似判断
- 基本思路：看基本事件在最小割集（或径集）中出现的次数和位置
- 单事件割集（或径集）中的基本事件结构重要度最大
- 出现次数相同的基本事件，结构重要度相同

例

若基本事件 x_1 在最小割集中出现次数最多，则其结构重要度最大。若 x_1、x_2、x_3 出现次数相同，则三者结构重要度相等。排序示例：$I_1 > I_4 = I_2 > I_2 = I_5$（依具体割集结构而定）。

注意

近似判断时若出现模棱两可（无法直接判断大小）的情况，需通过近似计算（如 $1/k$ 求和）来比较，不能仅凭直观判断。

最小割集与最小径集的应用

- 可选择控制事故的最佳方案
- 结合结构重要度分析，可进行定量分析
- 为事故预防和系统优化提供依据

定量分析的前提条件

- 基本事件故障参数（故障率）已知且数据可靠
- 可参考相关故障数据库（需注明数据来源）
- 事故树已化简，可用布尔代数表示（存在函数关系）
- 需注意化简后可能出现的相同基本事件（如 x_1 与 x_2 相同），代入数据前必须合并

注意

布尔代数写出后，若中间出现相同的基本事件（如 x_1 或 x_2 重复出现），必须化简到最简形式后才能代入数据，否则计算结果错误。

定量分析的教学假设

- 基本事件之间相互独立
- 基本事件只考虑两种状态（发生/不发生）
- 故障分布假定为指数函数分布

定义

指数分布假设：假定故障分布为指数函数分布，这是定量分析的重要前提假设。

注意

为什么假定故障分布为指数函数分布？因为指数分布具有无记忆性，便于数学处理，是可靠性分析中的常用假设。此假设是考试重点，需理解其意义。

指数分布与有效寿命期

- 指数分布是可靠性分析中常用的故障分布模型，其故障率 λ 为常数
- 假定故障率恒定（指数分布）的前提是设备处于有效寿命期
- 有效寿命期指故障率保持稳定的阶段，处于早期故障期与耗损故障期之间

定义

有效寿命期：设备故障率保持稳定、处于恒定状态的阶段。它位于早期故障期（偶然故障）和后期老化（耗损故障）阶段之间。

注意

只有假定故障率为常数（指数分布），后续分析中求偏导数、进行概率计算才可行。若故障率随时间变化，计算将变得复杂，因此定量分析前必须做此假定。

平均无故障工作时间（MTBF）

- MTBF 指两次故障之间正常工作的平均时间，即平均无故障工作时间
- 可通过实验或统计获得
- 是衡量可修复系统可靠性的重要指标

定义

MTBF（Mean Time Between Failures）：平均无故障工作时间，指可修复系统两次相邻故障之间正常工作的平均时间间隔。

人的失误概念

- 人的失误概念与设备可靠度概念类似，只是将对象从元件、器件、产品、设备替换为”人”
- 人的失误指人未能在规定条件下、规定时间内完成规定功能

定义

人的失误：人的作业实际完成的功能与系统要求的功能之间的偏差。

注意

人的失误概率难以像设备那样通过实验或统计精确获得，因为人受众多复杂因素影响，因此需要专门的人因工程方法进行分析。

人的可靠度五要素

- 人的可靠度概念与设备可靠度一致，包含 5 个基本要素
- 这 5 个基本要素是可靠性分析的基础，应熟练掌握

定义

人的可靠度：人在规定条件下、规定时间内完成规定功能的能力。

人的失误概率预测方法

- 将一项工作分解为多个步骤（作业单元、动作）
- 分析每个动作与预期偏差的可能性
- 将各动作的可靠度相乘，再用 1 减去该乘积，得到人的失误概率

例

把被分析的作业程序分解成单元作业，作业再分解为动作。对每个动作分析其失误概率，将各动作可靠度相乘，再用 1 减去乘积，即得到整个作业的失误概率。

人机系统信息处理环节

- 人机系统中人的反应包含三个环节：输入、判断、输出
- 即接受信息、处理信息、操控信息
- 一线岗位操作人员（如驾驶员）需特别重视这些环节

注意

人的反应速度与计算机相比差距很大，人可能忽略信息、反应不过来，且受作业环境影响，因此不能按计算机的速度来要求人。

作业环境对失误概率的影响

- 人的舒适温度一般为 19~22℃
- 环境温度超过 27℃ 时，人的失误概率约上升 40%
- 作业条件、作业自身因素、作业环境都会对人的行为产生影响

例

广州 11 月气温处于 19~22℃ 的舒适区间，因此全运会、学校审核评估等重大活动常选在此时段，此时人最容易发挥出最佳状态。

人的可靠度修正系数

- 人的可靠度受多方面因素影响，需用修正系数 1-2×k 进行修正
- k 包含以下因素：
  - 作业时间
  - 作业频率（操作频率）
  - 危险状况（如高速作业、潜水、带电作业、受限空间作业）
  - 心理和生理条件
  - 环境条件（如台风、大雨等抢修作业）

注意

修正系数（如表 3-3）的意义不在于精确计算，而在于帮助从系统角度考虑如何高效衔接、匹配和管理人机系统，做到物尽其用、人尽其才、因人而异。

例

心理脆弱的人、环境敏感的人、恐高的人，其失误概率会更大。安排岗位时应考虑个体差异，否则会降低团队协作效率。

顶事件发生概率的计算

- 已知基本事件发生概率和事故树逻辑结构（含最小割集）后，可计算顶事件发生概率
- 这是事故树定量分析的核心目标

定义

顶事件发生概率：在已知基本事件发生概率和事故树逻辑结构的前提下，计算出的顶上事件发生的概率。

与门与或门的顶事件概率计算

- 与门连接：顶事件发生概率 = 各基本事件失效概率的乘积
- 或门连接：顶事件发生概率 = 1 - 各基本事件可靠度的乘积

注意

事故树的与门/或门计算不能完全套用可靠度框图的并联/串联系统公式。可靠度框图有并联、串联、串并联、混联、桥式、N 中取 k 等结构，而事故树是按逻辑门（与/或）连接，二者有本质差别。

最小割集与顶事件概率计算

- 当事故树有多个最小割集时，需先写出完整表达式并展开化简，才能代入数值计算
- 若最小割集之间存在交集（重复基本事件），不能直接代入数值

注意

必须先将表达式展开、化简到最简形式，才能代入基本事件概率计算。若直接代入，结果会产生偏差。

例

当两个最小割集都含有同一基本事件 q_2 时，展开后会出现 $q_2 \times q_2$，应化简为 q_2 而非 q_2^2。若直接代入数值，会得到错误结果。

容斥原理（展开公式）

- 多个最小割集时，顶事件概率按容斥原理展开：
  - 两个割集：各割集概率之和减去两割集的交集
  - 三个割集：各割集概率之和，减去两两交集，再加回三者的交集
- 展开过程中，偶数个割集交集取减号，奇数个割集交集取加号

定义

容斥原理：计算多个事件并集概率时，先加各事件概率，减去两两交集，再加回三交集，依此类推，奇数次交集加、偶数次交集减。

注意

事故树概率计算是逻辑运算，不是普通数学运算，与可靠度框图的并联/串联计算不同。展开化简到最简形式后才能代入数值。

顶事件发生概率的展开计算规则

- 计算顶事件发生概率时，先列出顶事件发生概率的表达式，再进行展开
- 展开的目的是消除每个概率集中重复的概率因子
- 若各最小割集（或最小径集）之间不存在重复的基本事件，则可忽略展开步骤，直接代入计算
- 展开后需将各基本事件的概率值代入，才能最终计算出顶事件发生概率

注意

展开消除重复概率因子这一步不能省略。若存在重复的基本事件（如两个最小割集都含 k12），必须消去重复项，否则最终结果错误。

最小割集展开公式（容斥原理）

- 两个最小割集：各元素乘积之和，减去它们的交集
- 三个最小割集：三个割集各自元素乘积之和，减去两两交集，再加上三个割集的交集

例

三个最小割集时：第一项 + 第二项 + 第三项 − (第一 ∩ 第二) − (第一 ∩ 第三) − (第二 ∩ 第三) + (第一 ∩ 第二 ∩ 第三)

注意

割集数量越多，展开项数越复杂。一般考试不超过 4 个最小割集，3 个必须掌握，4 个只需会写表达式，不必展开计算。

最小径集计算顶事件概率

- 最小径集与最小割集原理相同，只是用对偶（或门）公式
- 两个最小径集时，展开结果为：q1 · q3 − q1 · q2 · q3 + q2
- 每个径集用一减的形式（1 − qi），因为径集对应或门
- 化简后规律：一次项、二次项、三次项依次排列，再减去交集项

注意

最小径集计算时，不能直接把概率值代入，必须先化简表达式，否则会出错。

概率重要度（Probability Importance）

- 定义：基本事件发生概率的变化引起顶事件发生概率变化的程度
- 数学表达：对顶事件概率函数 P(T) 关于基本事件概率 qi 求偏导，即 ∂P(T)/∂qi
- 求偏导后需将各基本事件概率值代入，得到概率重要度系数
- 作用：可快速确定哪个基本事件的概率能迅速有效地降低顶事件发生概率

定义

概率重要度系数：第 i 个基本事件发生概率的变化引起顶事件发生概率变化的程度，即对顶事件概率函数关于 qi 求偏导。

注意

概率重要度只考虑了基本事件对顶事件的影响幅度，未考虑基本事件自身发生概率的大小。若某基本事件影响大但本身发生概率已很小，再去改变它投入大、效果差。

临界重要度（关键重要度）

- 定义：基本事件发生概率的变化率引起顶事件发生概率的变化率
- 数学表达：I_c(i) = (qi / P(T)) × ∂P(T)/∂qi
- 其中 ∂P(T)/∂qi 即概率重要度系数，qi 为基本事件概率，P(T) 为顶事件概率
- 相比概率重要度更合理、更具实际意义，因为它反映了基本事件概率的相对变化对顶事件的影响

定义

临界重要度系数：第 i 个基本事件发生概率的变化率引起顶事件发生概率的变化率，等于概率重要度系数乘以 qi/P(T)。

例

某事故树两个最小割集，各基本事件概率已知。先求顶事件概率表达式，再对 qi 求偏导得概率重要度系数，最后代入公式 I_c(i) = (qi/P(T)) × ∂P(T)/∂qi 求临界重要度，并排序。

概率重要度与临界重要度的区别

- 概率重要度：看基本事件概率变化对顶事件概率的影响幅度，不考虑基本事件自身概率大小
- 临界重要度：看基本事件概率变化率对顶事件概率变化率的影响，考虑了基本事件自身概率大小
- 临界重要度更能从本质上反映各基本事件在事故树中的重要程度

注意

计算临界重要度时，必须先正确写出顶事件概率表达式 P(T)，再求概率重要度系数，最后代入临界重要度公式。任何一步出错都会导致最终结果错误。

完整解题步骤

- 第一步：化简事故树，求最小割集（或最小径集）
- 第二步：写出顶事件发生概率的表达式（展开消除重复概率因子）
- 第三步：代入各基本事件概率值，计算顶事件发生概率
- 第四步：求各基本事件的概率重要度系数
- 第五步：求各基本事件的临界重要度系数并排序

注意

题目通常包含多个步骤，稍不注意就会遗漏。结果算错基本不得分，务必细心。

事故树分析中的与门、或门运算

- 与门、或门连接时，割集与径集的运算关系要区分清楚
- 或门对应割集，顶事件发生条件按或门逻辑展开
- 若对运算规则不清楚，必须严格按照最原始的定义式推导，否则中间过程容易出错
- 偏导数可直接求，也可按定义式展开求，两种方式均可

原因后果分析（Cause-Consequence Analysis）

- 本质是把事件树和事故树结合起来的方法
- 事件树从左到右展开，事故树从上到下展开
- 将每个”电机过热”等中间事件既当作事故树的顶事件，又当作事件树的初始事件
- 既可用事件树计算概率，又可用事故树计算顶事件发生概率
- 理解其结合思路即可，属于综合分析方法

系统安全预测（第四章概述）

- 本章不作详细讲解，有兴趣可自行阅读

- 内容包括：预测类型、预测基本原理、预测方法
- 具体方法：时间序列预测、灰色模型预测、回归预测、灰色预测、马尔可夫预测

系统安全评价的基本概念

- 安全系统工程的核心环节：分析 → 预测 → 评价
- 评价是对系统安全状况或水平进行判断，判断其是否处于可接受的风险边界之内
- 评价方法分为定性、定量两大类；定量中又含指数法、模拟仿真法等
- 早期也称”风险评估”或”风险判断”

定义

系统：由两个或两个以上相互关联、相互依存的要素构成的、具有特殊功能的有机整体。其性质包括整体性、完整性、有序性、相关性。

定义

风险：系统可能出现危险，由危险有害因素导致事故发生的可能性，以及一旦发生之后导致的事故后果的严重程度，并包含风险防控措施对系统风险的削弱或补偿。

定义

安全评价（危险度评价/风险评价）：对系统内存在的危险性及其严重程度，以既定的指数、等级或概率值进行分析和评估，并判断其是否达到可接受标准；若超过标准，则制定相应的安全对策措施，使安全性达到社会公众所需的水平。

例

量化判断的常见形式：万车死亡率（指数）、事故发生的概率值（如 10^{-n}）、工时损失等。

安全评价的分类（按阶段）

- 评价分类依据项目或系统所处的不同阶段
- 各阶段评价均有相应法规要求，须在法规规定的阶段进行

定义

安全预评价：在可行性研究阶段、园区规划阶段或生产经营活动组织实施之前，辨识分析建设项目、工业园区、生产经营活动潜在的危险有害因素，检查其符合法规标准规章规范的符合性，预测事故发生的可能性和严重程度，提出建议并作出结论。

例

埋地天然气管线铺设于公路下方，需预先评价其受载荷和外界因素影响下多长时间内会发生破坏，即属于安全预评价。

定义

安全验收评价：在工程竣工、试生产、园区建设完成后，检查建设项目或园区内的安全设施设备装置与主体工程”三同时”（同时设计、同时施工、同时投入生产和使用）情况、安全生产管理措施到位情况、规章制度健全情况、应急预案建立情况，审查其满足安全生产法规规章标准规范的符合性，从运行状况和

安全管理作出验收评价结论。

注意

验收评价通过后，评价结论在有效运行期（如 3 年或 6 年）内不能出现问题，因此验收评价风险高、含金量高。不能仅凭”已建设完成”就做验收评价，还需经过试运行阶段；若试运行（如投料升温）中发生事故，则不能通过验收。

定义

安全现状评价：在生产经营过程中，对事故风险、安全管理状况进行评价，确定其与法规要求的符合性，并提出符合性结论。

例

石油化工行业等危险性较高的行业，每三年需做一次现状评价，检查管理、人员、设备设施（工艺、控制、仪表、特种设备等）是否仍符合安全要求。设备设施随使用进入耗损期（浴盆曲线老龄期）材料老化，故现状评价属于寿命周期内的评价。

定义

专项安全评价：针对特定情况或改变进行的评价，如加装设备、对原有系统进行调整，或发生意外事故后需停工评价，符合要求后再继续推进。

注意

评价分类名称（预评价、验收评价、现状评价、专项评价）统属于 AQ 标准 AQ 8001-2007《安全评价通则》。该通则是所有安全评价最上层、原则性的标准，规定了基本概念和原则性内容；不同行业另有实施导则（如建筑工程安全评价实施导则、危险化学品建设项目安全评价导则）和更细的细则。做危化品安全评价不能用建筑行业的实施导则，但建筑行业可以用通则中的概念性、原则性内容。

注意

AQ 8001-2007 发布时间较早（2007 年）。2022 年应急部曾就修改该标准征求意见，但截至当前未查到重新颁布的定稿，故在无新标准发布前，该标准仍有效，应依法执行。

定义

实现安全目的：对工程系统、生产经营行为、社会活动中的危险有害因素，预测发生事故或造成职业危害的可能性和严重程度，再提出科学、合理、可行的安全风险管理对策措施建议。

定义

评价对象：可以是一个相对独立的对象，也可以是一个区域范围。例如整个石化园区（区域）、园区内某一企业（相对独立对象）、企业内某一套装置（更小对象）均可作为评价对象。

例

安全评价中介机构早期大量承接预评价业务，因经济快速发展、企业不断注册投资。评价师资格早期为认定制，后转为培训考试制；现主要考注册安全工程师（注安），分初级、中级、高级，高级相当于安全高级工程师。持有中级注安师证书在各单位含金量较高、待遇较好。

安全评价的分类（按量化程度）

- 按评价结果量化程度分为：定性评价、定量评价、半定量评价
- 半定量评价因含部分定性内容，本质上仍属定性范畴

注意

半定量评价属于定性评价的一种，因其包含定性成分。

重要度概念（需熟练掌握）

- 需熟练掌握：结构重要度、概率重要度、关键重要度、临界重要度
- 本次无作业，但要求比平时更高，须滚瓜烂熟

11 月 03 日

割集与最小割集

- 割集：故障树中若干基本事件的集合，当这些基本事件都发生时，顶事件必然发生
- 最小割集：若割集中任意去掉一个基本事件后就不再是割集，则该割集为最小割集
- 最小割集之间为逻辑”或”关系，任一最小割集发生即可导致顶事件发生
- 顶事件发生概率的表达式需完整、准确并尽可能简化

概率重要度与临界重要度

- 概率重要度：基本事件发生概率变化对顶事件发生概率的影响程度
- 临界重要度（关键重要度）：综合考虑基本事件自身概率大小及其对顶事件的影响
- 计算公式由概率重要度结合基本事件概率推导得出，需理解逻辑推导过程而非仅记结果
- 计算过程需仔细操作，部分考试不允许携带计算器，应提高手算准确性

最小割集与最小径集的求解方法

- 基本运算规则为布尔代数
- 最小割集求解方法（本课程介绍两种）：
  - 布尔代数法：利用布尔代数运算规则化简
  - 行列法：通过行列展开方式求解
- 最小割集与最小径集在事故分析及实际应用中作用不同，需掌握各自特性
- 应学会分析典型事故案例，辅助事故分析

大作业要求

- 分组进行（原计划五至六个小组，自行分配）
- 基本要求：对故障树/事故树进行分析
- 进阶要求：

- 寻找计算机软件自动绘制事故树
- 用软件直接计算顶事件发生概率

系统安全评价的分类（AQ 标准）



定义

AQ 8001-2007《安全评价通则》将系统安全评价分为三类：安全预评价、安全验收评价、安全现状评价。

- 分类依据相关法规（如《危险化学品安全管理条例》）确定
- 安全预评价：企业设立阶段进行
- 安全验收评价：即将投产时进行
- 安全现状评价：正常运行过程中每三年进行一次

例

危险化学品企业全生命周期管理：设立时做预评价 → 投产前做验收评价 → 运行中每三年做现状评价，实现从孕育到生产结束的全方位管理。

安全评价与安全生产许可证

- 安全评价是法定动作之一，是企业获得安全生产许可证的必要条件
- 仅靠安全评价不够，还需日常设备维护、工艺装置维护、监测监控系统维护、员工培训及岗位管理等
- 选址阶段需进行安全条件认证与安全评估，评估土地规划性质（工业园区用地、城市一般工业用地等）是否适合设厂

专项安全评价

- 生产作业中遇到异常情况导致局部或全部停产时，恢复生产前需进行专项安全评价
- 用于确认恢复生产前是否符合安全基本要求

评价对象——系统

- 评价对象为系统，系统至少具有五个方面的特点（此前课程已介绍）
- 评价基于风险展开，需熟悉风险概念

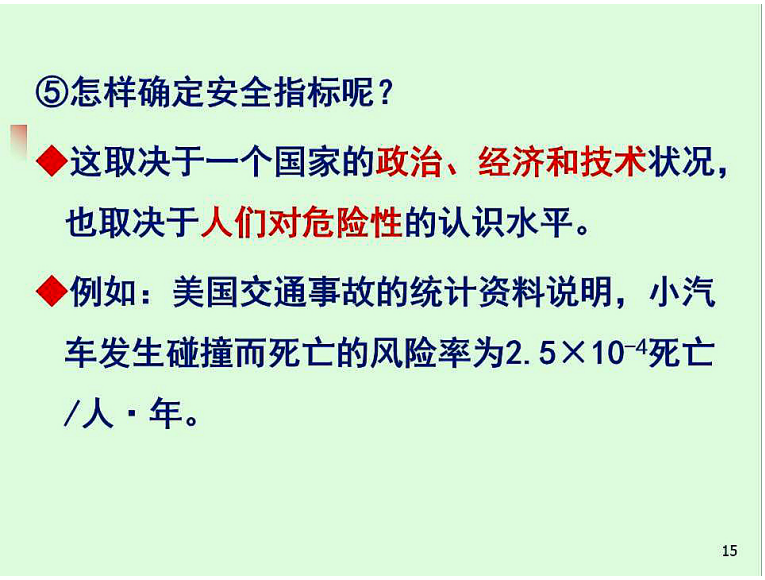
风险的概念

- 风险影响源于两个方面：
  - 可能性的大小
  - 发生后对系统或系统与外部环境交互的严重影响程度
- 定性评估与定量分析各有相应方法
- 定量手段包括：计算机模拟、仿真实验、工具性软件、统计软件等

例

隧道火灾时烟气传播需量化；易燃易爆液体/气体与空气混合达爆炸极限后，一点热源即可引发爆炸，该过程是三维冲击波超压动力学的传播过程，可通过工具软件模拟分析。

风险的表征与评价基准



- 量化风险结果需与标准或指标进行对比
- 需明确：风险如何定量表示、如何定性表示、定量表示的水平或指标依据、接受高低标准取决于哪些因素
- 确定指标需考虑政治、经济、技术及其他相关因素

例

建国初期我国人均寿命较低，如今已显著提高，公众对自身安全的要求和期望值随之上升，因此必须降低风险以满足更高期望。

需求层次理论与安全管理

定义

马斯洛需求层次：生理需求 → 安全需求 → 爱与归属感 → 尊重需求 → 自我实现。其中生理需求和安全需求属于缺失性需求（最基础），其余三个属于成长性需求。

- 公众需求随社会发展持续上升
- 安全需求是基础性需求，政府若忽视民众生命将失去民心
- 安全工作的目的之一是满足高层需求（自我实现），通过管理、技术及安全审批体系，使作业环境、人机环系统达到高度和谐

安全评价通则与标准更新

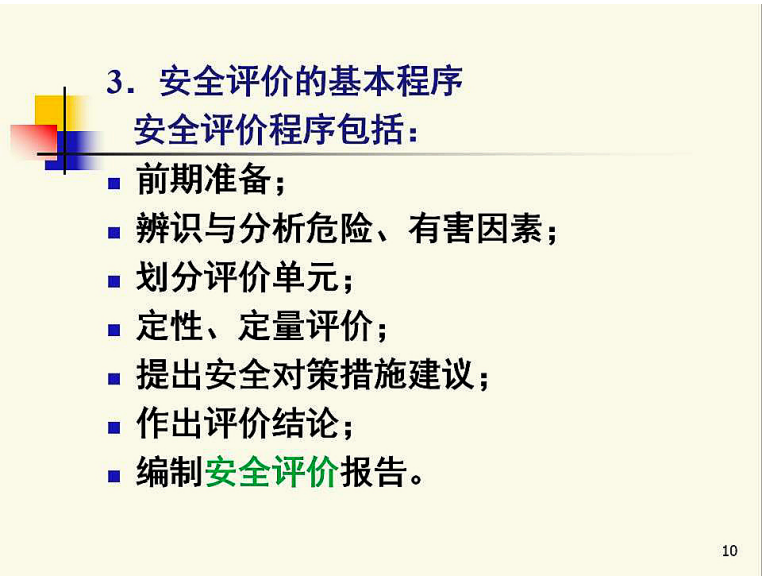
- 安全评价必须遵循国家标准，国家标准处于修改或征求意见阶段时，新标准发布后应予以采用
- 验收评价与现状评价的区别：
  - 验收评价：依据竣工时现行有效的法律法规和标准规范
  - 现状评价：依据当前现行有效的法规标准，要求可能更严格

> **注意**
>
> 不能认为验收通过后一切就符合要求。整个运行过程是动态的，标准规范不断变化，人们需求水平持续提升，设备设施性能需优化。若设施符合旧标准但排放不达标，仍不可接受；若需重新建设，必须按新要求执行。

三同时原则

- 项目竣工时需满足”三同时”：同时设计、同时施工、同时投入生产和使用
- 同时包括管理措施和应急救援
- 法规层次：法律法规（国家、地方、部门）→ 规章 → 标准规范 → 规范标准的符合性
- 验收人员若未发现危险有害因素即签字通过，存在明显漏洞需追责，监管体系严格科学

安全评价的基本程序



- 基本程序（以周保成同学回答为例）：
  1. 确定评价单元
  2. 识别和分析危险有害因素
  3. 编写安全评价报告
- 每一步都包含许多细节，逻辑框架大致如此

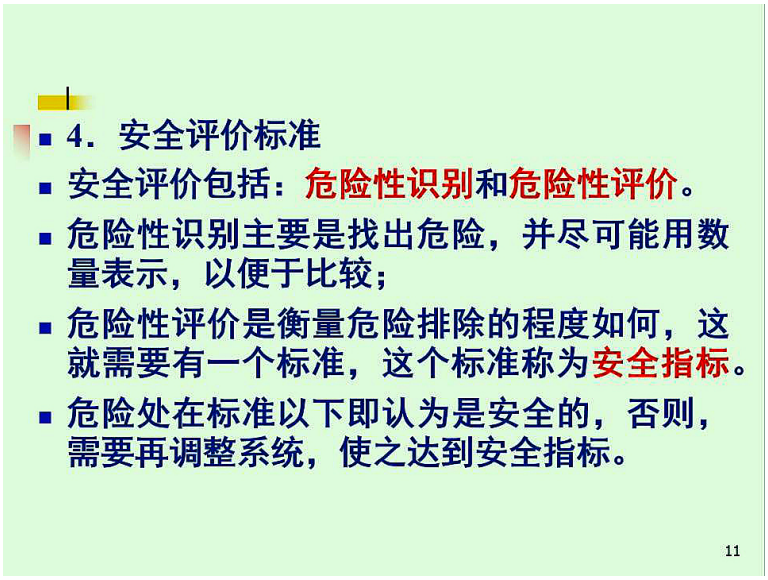
前期准备与危险有害因素识别

- 前期准备需两人同时到现场调研，携带录音、拍照设备，收集佐证材料
- 避免因准备不足导致危险有害因素识别出现偏差或遗漏
- 识别依据包括：相关法规和标准、专业知识和经验、同类企业事故案例、公司自身运营中的突发情况及未遂事件
- 还需在工艺、管理制度、人员培训等方面做好准备

- 老专家凭借丰富经验具备”态势感知”能力，能像传感器一样收集并处理现场信息

> **注意**
>
> 有限空间作业可能存在早期辨识遗漏；涂料或原材料添加过程中可能产生静电，应避免使用铁锤等易产生静电的工具。若相关细节未在报告中记录，后续出现问题会造成麻烦。

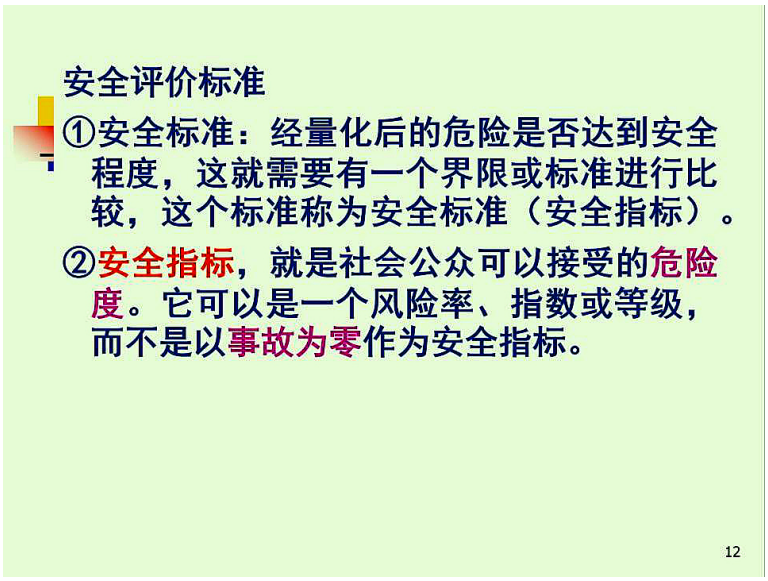
安全指标



> **定义**
>
> 安全指标是衡量危险排除程度的标准，反映公众可接受的危险水平。危险程度低于该标准即可认为安全，否则需建立相应管理制度。

- 安全指标可基于概率、指数或其他方式，不以事故数量作为唯一衡量
- 安全指标应反映公众可接受的危险水平

事故的特性与安全指标确定



- 事故具有偶然性、必然性、隐蔽性和危害性

- 事故背后潜藏着一个过程，发生既包含偶然因素也遵循必然规律
- 认知能力有限，无法完全理解某些现象，因此事故为零难以作为安全指标

例

神舟二十一号任务时间不到三个半小时，体现载人飞船高可靠性要求；尽管认知有限，但在该范围内已实现重大突破，未来认知将逐步深入。

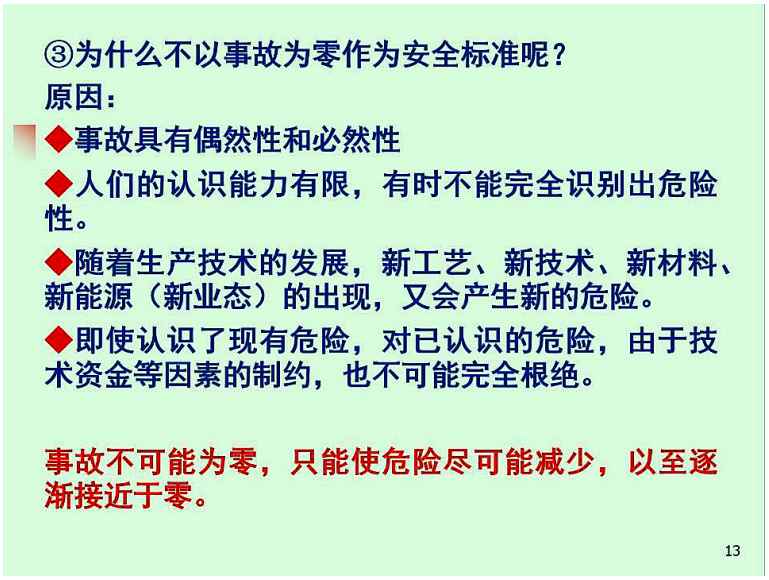
新技术、新业态带来的安全挑战

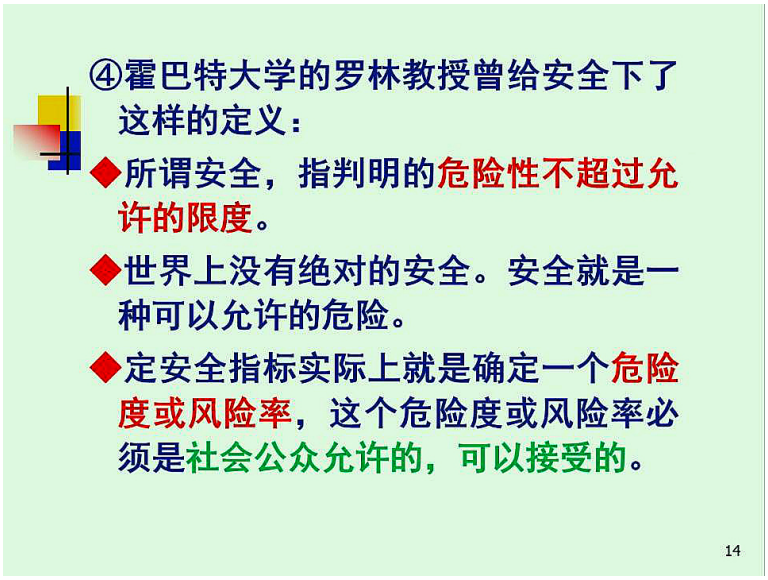
- 新技术、新工艺、新材料、新能源带来新的安全要求：
  - 低空经济：无人机、无人船、无人艇、无人车等新业态
  - 新能源：氢能安全使用、锂电池技术
  - 新材料：柔性显示屏、可任意折叠材料等，难以界定是否属于危险化学品或微毒物质
- 若发现安全隐患或设备带病运行，务必提交报告

注意

新技术、新工艺、新材料的使用有时难以界定其危险性（如某些材料是否属于危险化学品或微毒物质），这对安全评价提出新的要求。

安全与风险的本质





- 绝对的安全是不存在的，安全实质上是一种可接受的危险
- 安全是指判断的危险性保持在社会可接受的限度内
- 安全与风险是相对的，确定危险度和风险率时必须考虑社会公众的接受程度
- 事故无法完全消除，目标是尽可能减少事故发生，并逐步趋近于零
- 理想状态是实现全面的自动化、智能化、机械化和智慧化，消除人的直接作业，但资金是制约因素

定义

安全：指判断的危险性保持在社会可接受的限度内。安全与风险是相对的，安全实质上是一种可接受的危险。

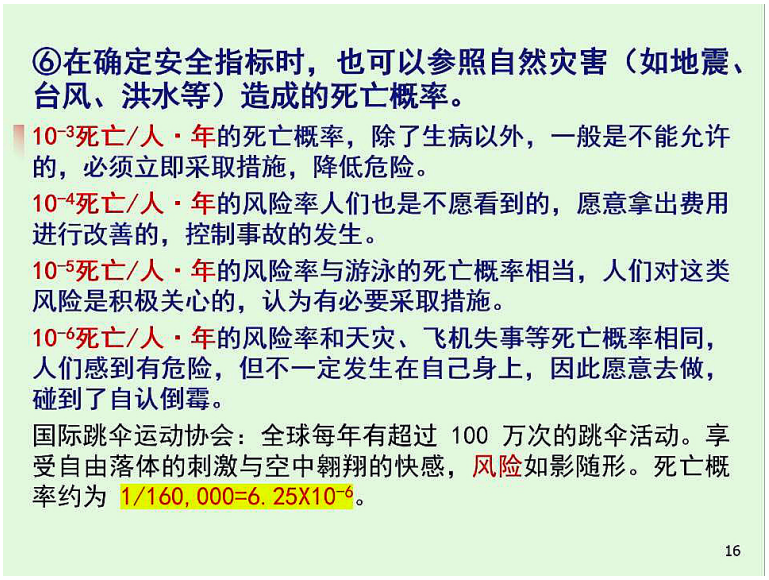
例

美国对交通事故的分析非常细致，涉及路况、车型、驾驶员的学历、性别等因素，分析出事故概率约为 2.5×10^{-4} （即 2.5万分之），相当于每 400 次中有 1 次。而自然灾害造成的死亡概率约十万分之一，这样的概率是不可接受的。

注意

2.5万分之 并不是”每 10 万次中有 2.5 次”，而是”每 400 次中有 1 次”，两者含义不同，注意区分。

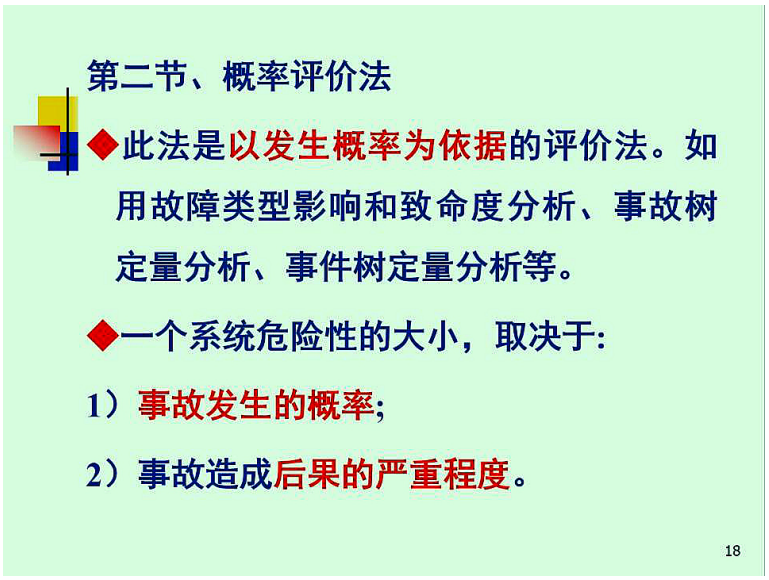
不同行业与活动的风险差异

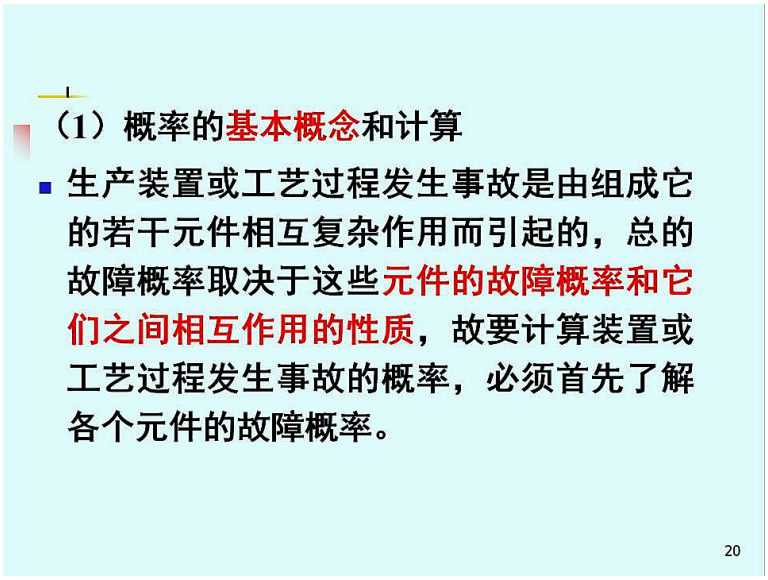


- 不同行业之间存在风险差异，如公安、交警、消防、建筑行业等属于风险较高的范畴
- 高风险行业通过购买安全险、责任险等保险来转移风险
- 跳伞运动虽相对较少发生事故，但从事人数较少

> 例
>
> 跳伞事故概率约为 16 万分之一，换算后约 6.25万分之。跳伞只要按照严格的规程、经过训练，风险是可以接受的。

可靠性基础概念回顾

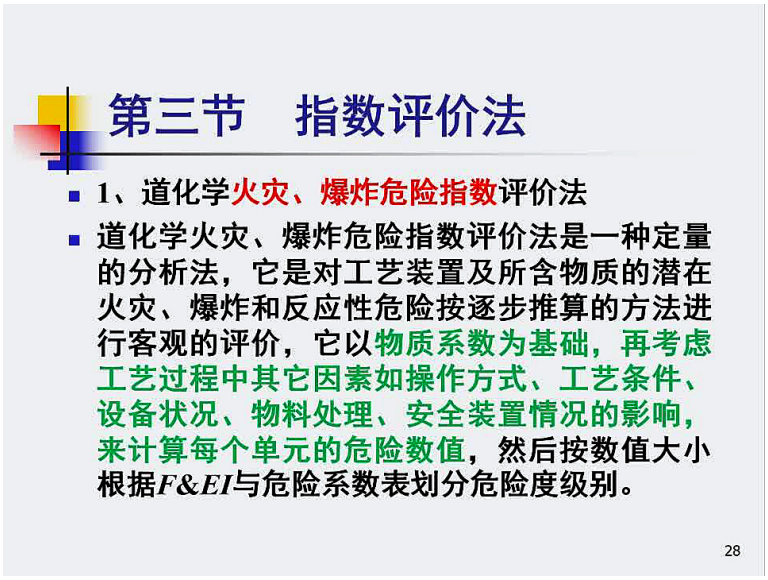




- 概率评价基于 FMEA 中的相关数据
- 涉及 MTBF（平均故障间隔时间）等可靠性指标
- 产品故障分为三个时期：初期故障期、偶发故障期（偶然故障期）、磨损故障期（老年故障期）
- 教材中给出了基本事件或事件发生的概率，通过赔付率表来反映
- 连接方式（串联、并联）是确保可靠性的关键，串联可靠度与并联可靠度不同

> **注意**
>
> 偶发故障期是产品处于稳定运行的时期；到了磨损故障期，产品应尽量淘汰。

道化学火灾爆炸危险指数评价法概述

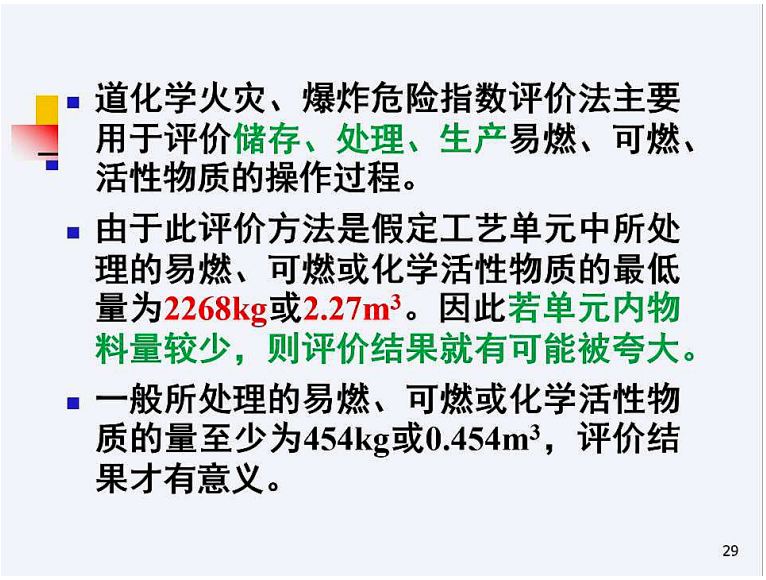


- 是化工行业发展中形成的重要评价方法，属于指数评价法中的重中之重
- 主要针对工艺装置及其所含物质的火灾、爆炸和反应性危险进行量化评估
- 通过计算得到一个客观的量化值，以此评定危险度分级
- 根据计算结果将危险性分为五级，便于进行有效的风险管理

定义

道化学火灾爆炸危险指数评价法：针对工艺装置及其所含物质的火灾、爆炸和反应性危险进行量化评估，通过计算得到客观量化值，评定危险度分级的方法。

道化学法的适用范围与物质系数

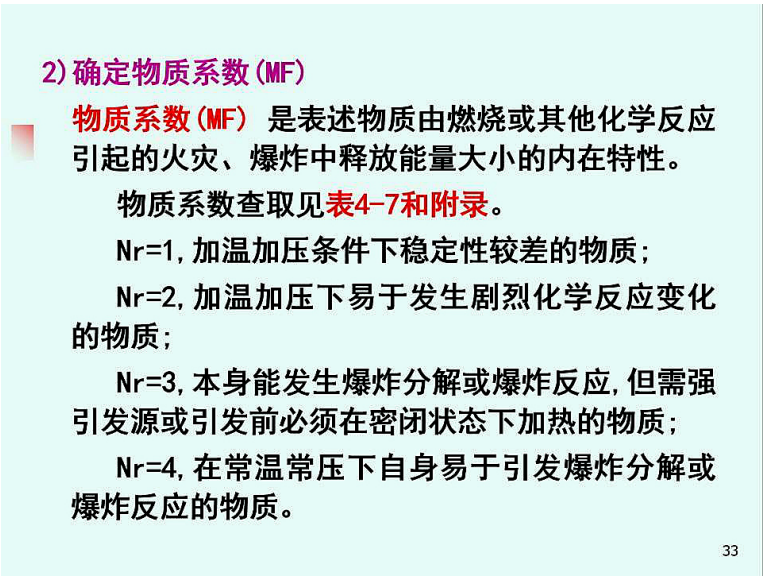


- 该方法适用于储存、处理和操作含有可燃活性物质的设备
- 对设备的量有明确要求：应尽可能不少于 2268（或体积 2.27），最低量为 454（或 0.454）
- 如果量太小，该方法就没什么意义，不需要使用

注意

如果设备中物质数量过少，可能导致评估结果偏下，从而造成评估结果偏大。量太小时不适用该方法。

物质系数的确定

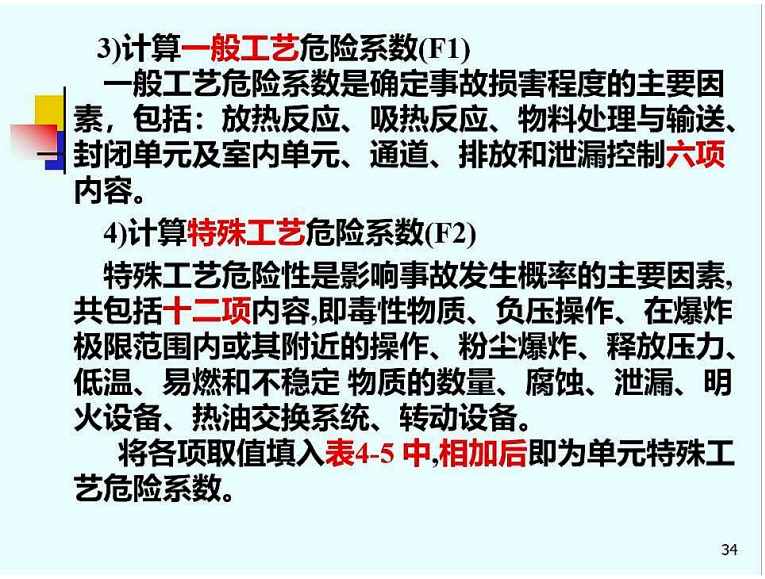


- 物质系数基于物质的火灾爆炸特性和化学反应活性（热稳定性）确定
- 物质系数通过查表获取，其中涉及的 NNR 值在附录中明确说明（约 262 页）

- 不同消防协会的参数不同，需要确定具体使用哪一种

> **例**
>
> N=1 表示在加热条件下稳定性较差；N=4 表示在常温常压下物质容易自发引发爆炸或分解，且情况会随条件变化而逐渐恶化。

一般工艺危险系数与特殊工艺危险系数

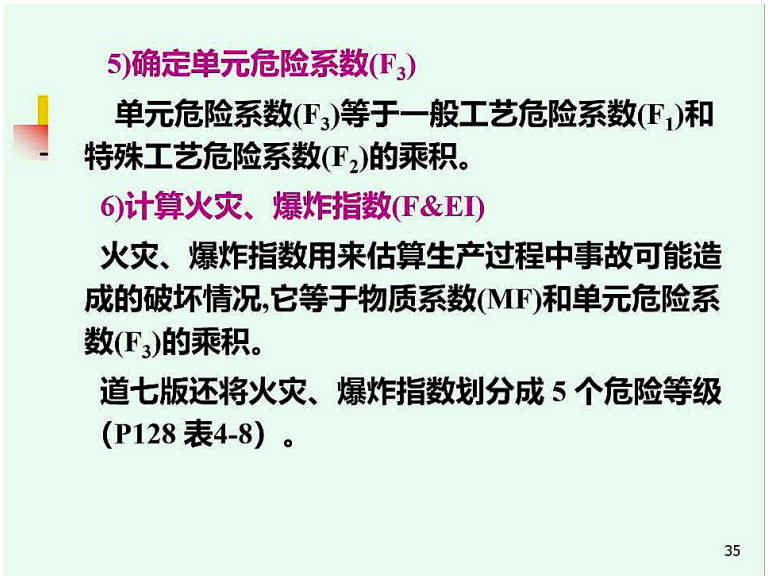


- 一般工艺危险系数有 6 项，特殊工艺危险系数有 12 项
- 一般工艺系数与常规工艺参数一致，包括热辐射引起的封闭单元、室内单元、通道的排放和泄露等
- 特殊工艺系数包括：毒性物质在爆炸极限范围内或附近、粉尘爆炸释放的压力增大、低温不稳定性、腐蚀性、泄露明火控制等

> **注意**
>
> 一般工艺系数中的”排放和泄漏”与特殊工艺系数中的”泄露”表述不同，容易混淆，需仔细区分。一般工艺系数中的排放涉及 50 或类似密封等概念，两者不一样。

> **例**
>
> 粉尘爆炸属于一般工艺系数，而不是特殊工艺系数，判断题中需注意区分。

工艺单元危险系数与火灾爆炸指数



- 工艺单元危险系数 = 1 + 一般工艺危险系数 + 特殊工艺危险系数，因此大于等于 1
- 火灾爆炸指数 = 工艺单元危险系数 × 物质系数
- 火灾爆炸指数分为五个等级，从很大到中度

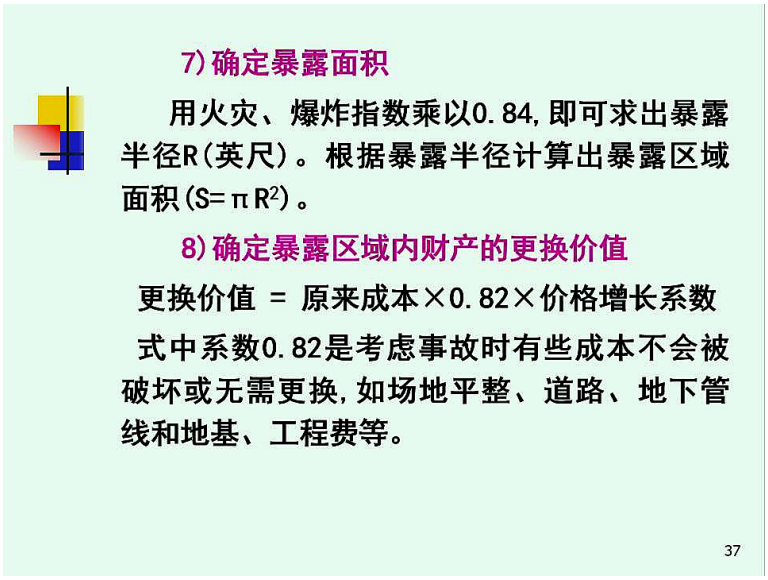
注意

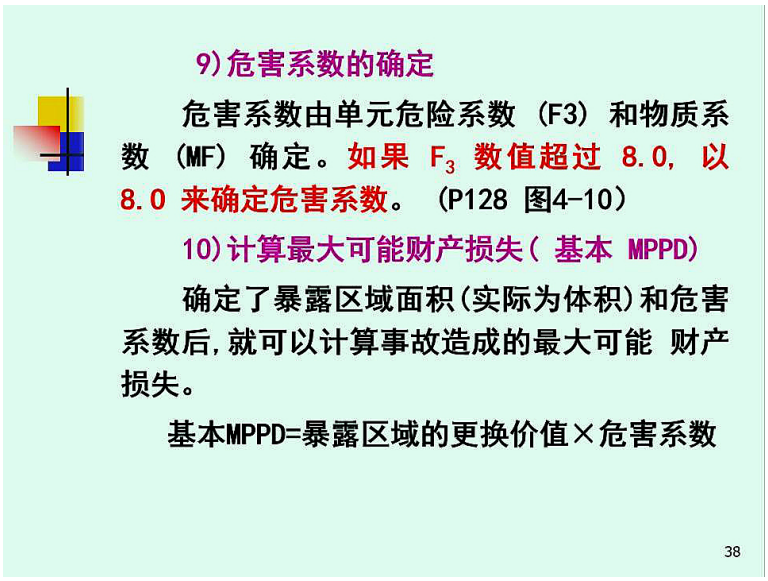
工艺危险系数是引起风险增大的，因此大于等于 1（即 1 加上各项系数之和）。大于 1 的数值相乘，结果大于等于 1。

注意

火灾爆炸指数的五个等级尚未考虑修正和控制措施，修正后的指数需通过安全措施补偿系数计算。

暴露面积与最大可能财产损失



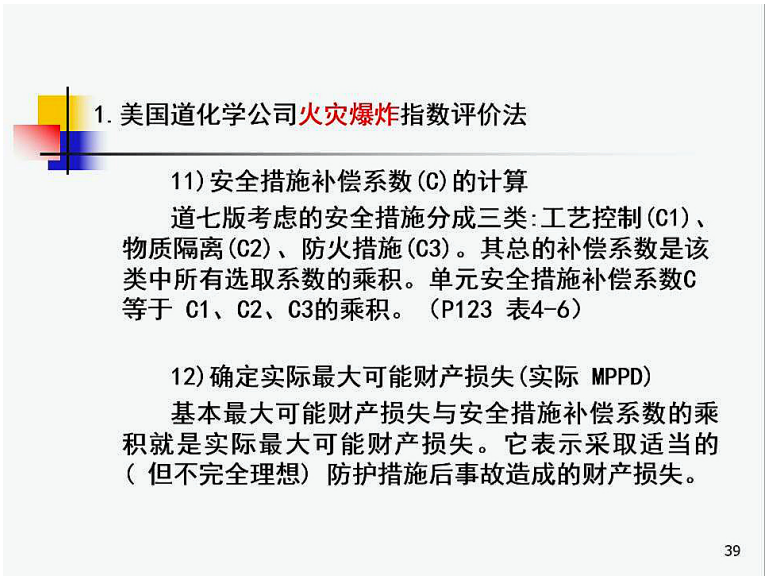


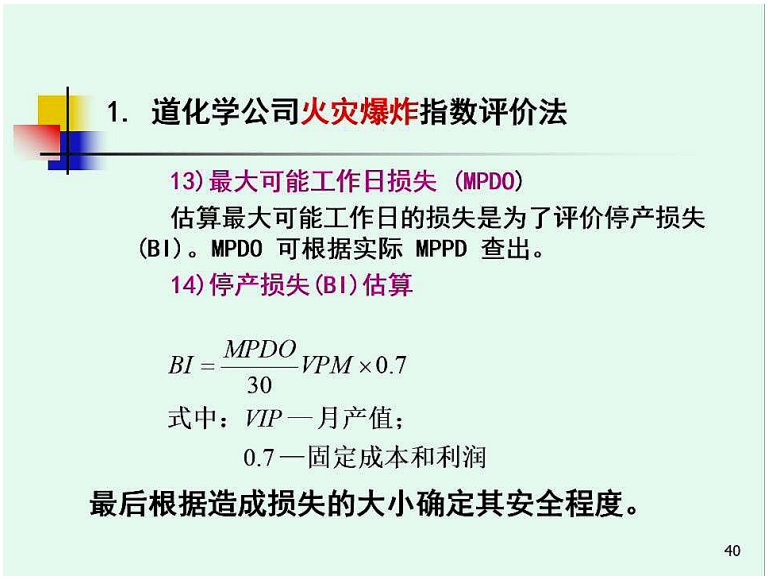
- 计算出火灾爆炸指数后，乘以 0.84 得到暴露面积
- 暴露面积 × 0.82 × 价格增长系数 = 区域内设备和设施的成本（原值）
- 危害系数通过查阅图 4-14-10 确定，基于单元危险系数和物质系数
- 当单元危险系数超过 8 时，应使用 8.8.0 来确定危害系数
- 基本最大可能财产损失 = 未经修正的指数 × 0.84 面积内的成本
- 最大可能财产损失 = 更换价值 × 危险系数

定义

基本最大可能财产损失：未经修正的火灾爆炸指数乘以 0.84 得到的暴露面积内，设备和设施的成本。

安全措施补偿系数

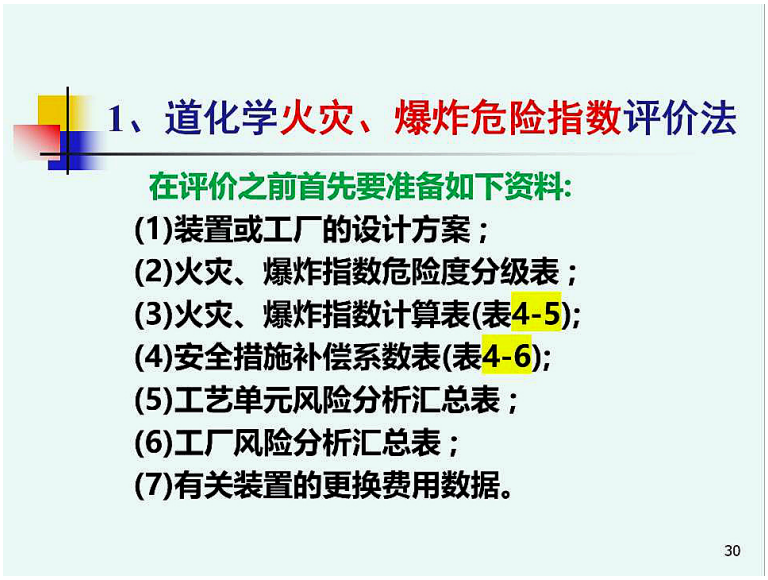


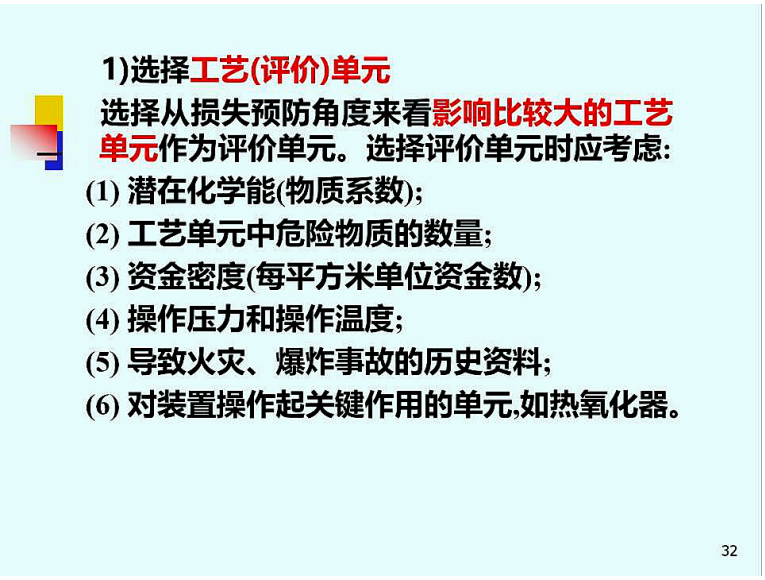


- 有三类安全措施补偿系数：工艺控制、物质隔离、防火措施
- 补偿系数均小于等于 1
- 修正后的火灾爆炸指数 = 火灾爆炸指数 × 补偿系数 C
- 修正后的指数反映火灾爆炸风险降低的程度，分级评估后可看到实际风险水平
- 还需考虑最大可能工作日损失和停产损失，可依据具体工作情况估算，也可用国内数据换算

> **注意**
>
> 安全措施补偿系数小于等于 1，因为补偿措施是降低风险的。三个补偿系数确定后，其层级是单元安全措施的补偿性。

道化学法评价的基本流程

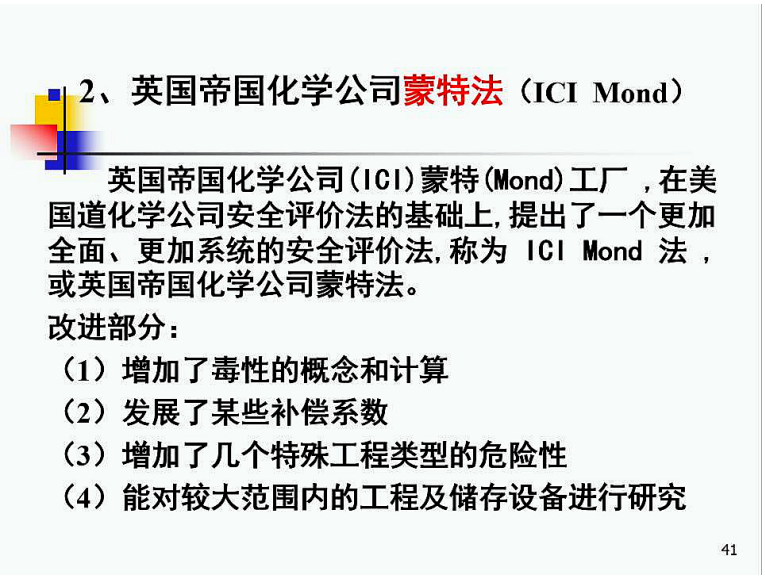




- 划分评价单元：根据不同的单元生产工艺流程进行划分
- 审查装置和设计方案，进行指数分析
- 计算指数 → 补偿 → 修正 → 汇总（单元层面）
- 每个单元完成后，再汇总成工厂层面的风险分析汇总表
- 工厂评估完成后，火灾爆炸指数乘以特定系数得到受影响面积
- 单位面积资产金额 × 受影响面积 = 设备更换费用

> 例
>
> 选择工艺单元时，从损失预防的角度看，影响较大的工艺单元被视作平台单元。这些单元通常具有潜在危险物质、工艺上存在超重压力和超高温等特征，容易导致火灾爆炸事故。

蒙德法（SI 蒙德法）概述

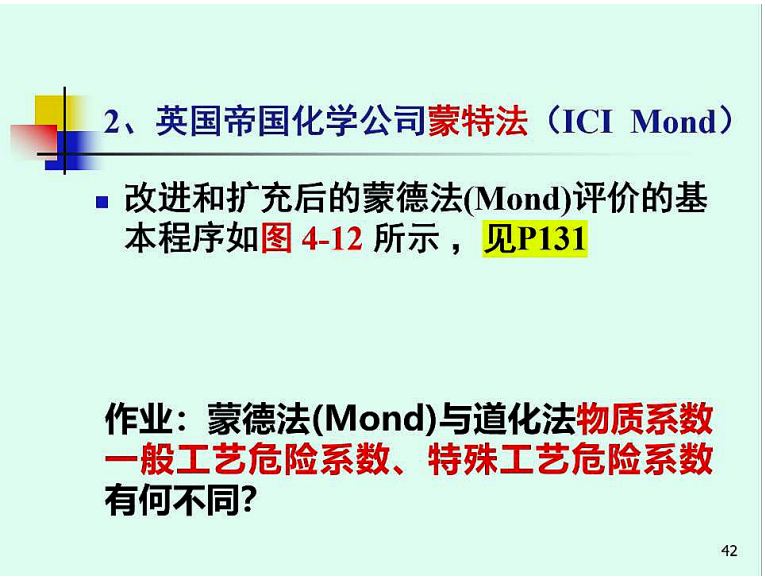


- 帝国化学公司（ICI）提出的蒙德法，是在道化学法第三版基础上改进而来
- 属于跨国公司早期对安全较为重视的产物

定义

蒙德法（SI 蒙德法）：帝国化学公司（ICI）在道化学法第三版基础上改进和扩充的评价方法。

蒙德法对道化学法的改进



- 增加了毒性因素的考虑：道化学法主要关注火灾爆炸，但某些介质还具有毒性
- 补偿措施方面有所改变
- 特殊工程类型方面，重点仍是毒性
- 较大范围内的工程和处置设备的布局

蒙德法特殊工艺危险指数新增因素

- 密封接头和垫圈造成的泄漏
- 震动和金属使用
- 强氧化剂
- 泄露易燃物的着火点
- 静电危害

注意

蒙德法与道化学法在物质系数、一般工艺危险系数、特殊工艺危险系数方面存在不同，需作为作业仔细对比。

多米诺效应

- 多米诺效应指一个企业发生事故后，对相邻区域产生影响，进而引发连锁事故
- 常见于化工园区

定义

多米诺效应：一个区域发生事故后，对相邻区域产生影响，而该区域再去影响其他区域，形成连锁的事故升级效应。

注意

多米诺效应有三个关键点：

1. 存在一个初始的、首发的事故——如果能够防止首发事故，后续事故就不会发生
2. 首次事故可能引发二次事故升级，升级向量包括冲击波、热辐射、碎片等
3. 二次事故的后果比第一次事故更严重

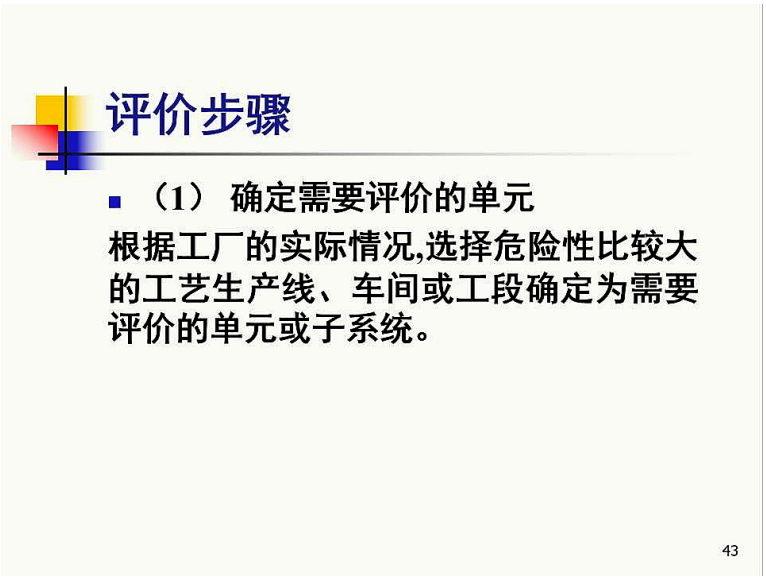
多米诺效应的防控

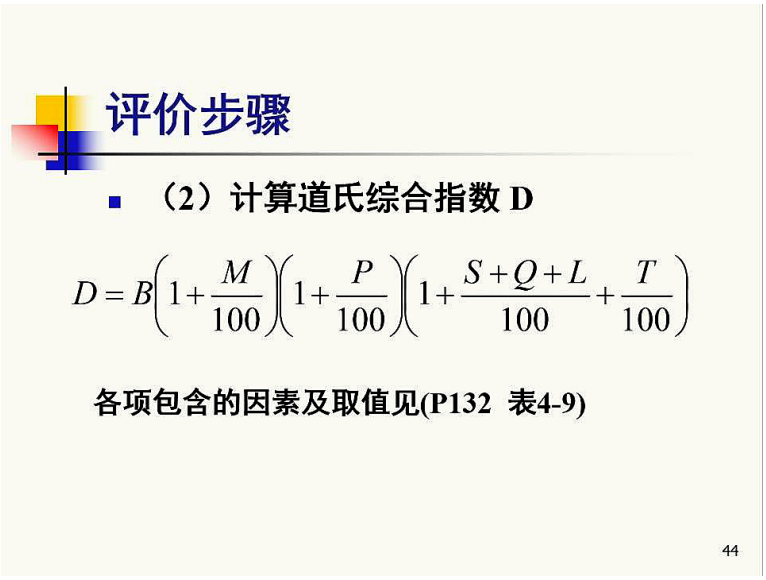
- 涉及首次事故发生的概率
- 涉及多米诺效应传播路径的问题——如果知道传播路径，可以在该路径上采取措施进行切断（锻炼减灾）
- 路径本身带有概率性，需采用分布式方式：对发生概率高的路径进行更多干预，低概率路径较少干预，更为经济
- 可通过消防系统、自动化连锁控制、安全屏障来有效防止多米诺效应
- 可细分为一级多米诺、二级多米诺、三级多米诺等

园区韧性与韧性城市

- 国际上的发展方向是做园区韧性：面临外部冲击时，能够抵御、吸收并恢复
- 国家提倡振兴城市，注重韧性城市建设
- 韧性城市与园区韧性中蕴含丰富的研究课题
- 其基础是当前所掌握的基本概念，将变得越来越复杂

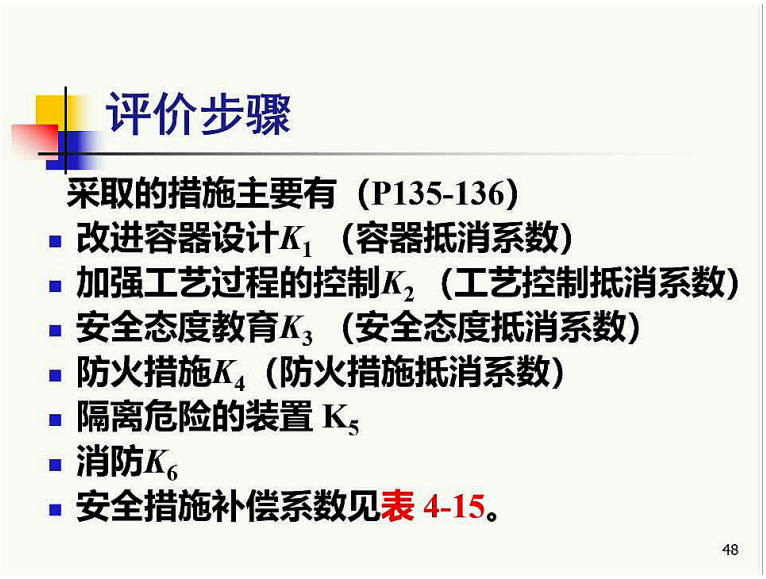
蒙德法综合指数计算

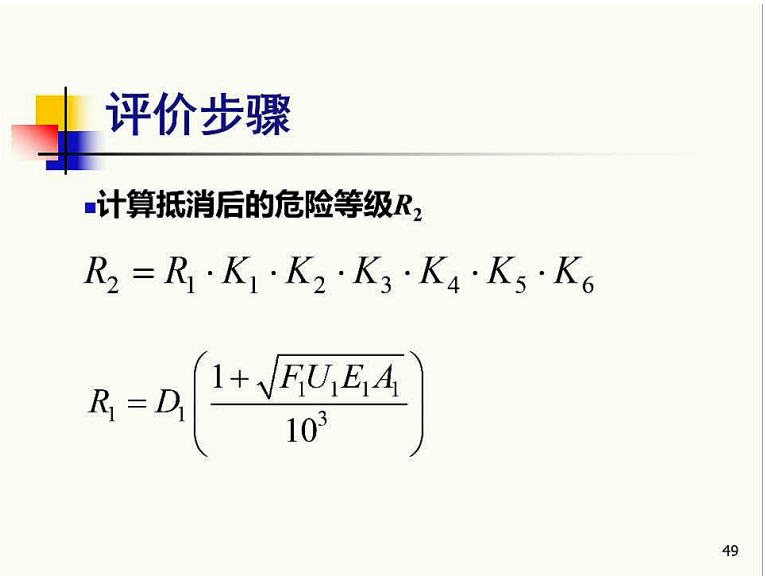




- 综合指数 R 由 D（火灾、爆炸和毒性指标）与右侧表达式相加得到
- 右侧表达式数值范围在 10^{-4} 到 10 之间，分类在 4-12
- 各参数物理意义：U 为单面毒性指数，C 为主读性指数
- 火灾荷载系数涵盖范围为 4 至 11，依据相关规范取值
- 计算出各系数后即可进行分级，分级后再采取相应措施
- 确定措施时需综合考虑事故率和后果严重程度两个方面
- 若某项指标危险性仍偏高（如综合危险性分级），需进一步采取措施修正

蒙德法补偿措施

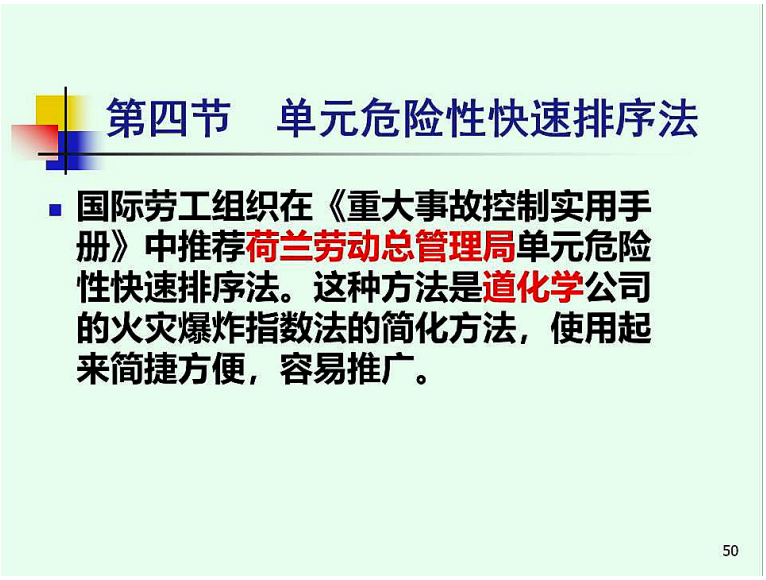




- 补偿措施依据《4-15 案件补偿措施技术》标准，总体在 135 至 136 页之间
- 补偿措施包括：改进容器设计、容器抵消系数、加强工艺过程控制、安全态度教育、防火措施、隔离措施等
- 安全措施的补偿系数应 ⩽ 1，危险系数则 > 0.1
- 基于第三版蒙德法，通过计算六个方面的有效性，得到抵消后的危险本金，即 R1 乘以这六个方面的有效性

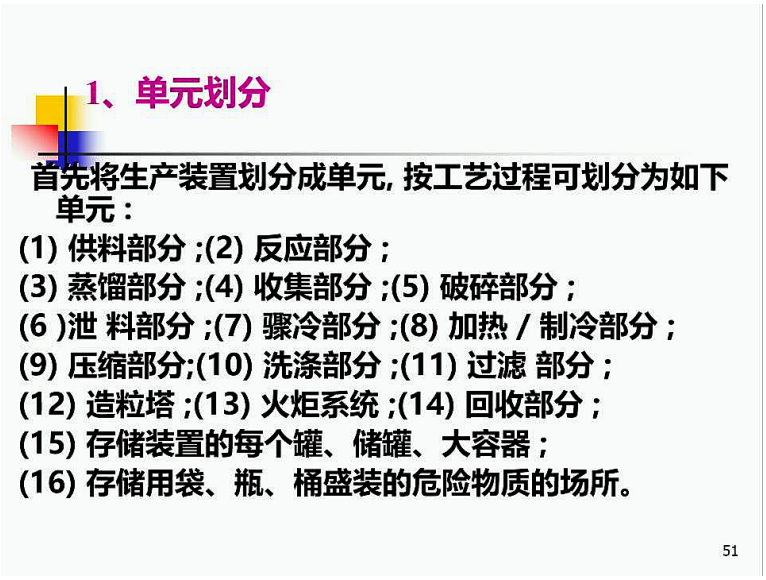
> **注意**
>
> 补偿系数与危险系数的取值范围容易混淆：安全措施补偿系数 ⩽ 1，危险系数 > 0.1，两者方向相反。

单元危险性快速排序法概述



- 该方法在道化学方法文献基础上简化得到，由河南省劳动总局和河南省劳动总管理局推广
- 核心步骤：单元划分 → 确定各系数 → 计算火灾爆炸指数 → 划分危险等级 → 按面积排序 → 优先关注高危险单元

单元划分与火炬系统

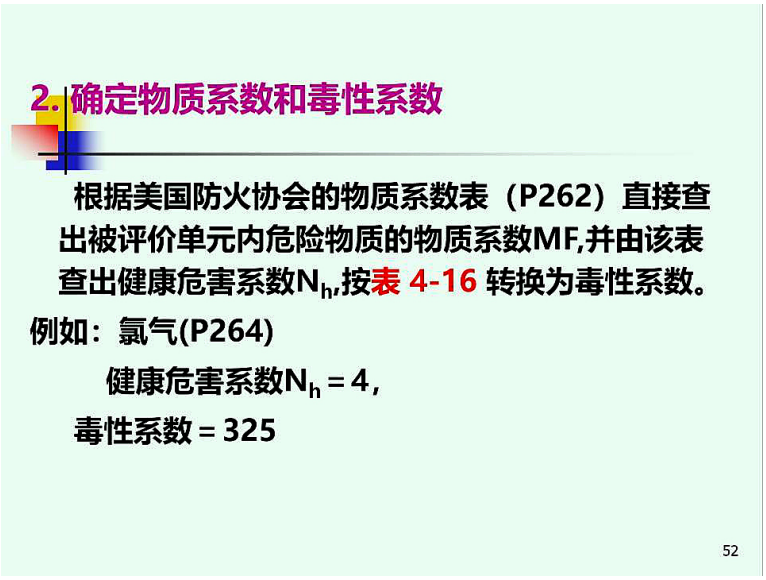


- 单元划分可从 16 个方面进行，依据设计说明书判断各工艺单元
- 设计说明书中未提及的方面，即视为未涉及
- 火炬系统主要用于紧急情况（如紧急停车时），将未反应或中间产品排放出去，防止污染大气或引发二次事故

> 例
>
> 火炬系统：若燃料未完全燃烧且比空气重，可能对周边环境造成污染、火灾等问题。我国规定紧急情况下任何问题都可排入火炬系统。火炬分为高架火炬和地面火炬，高架火炬直径可达 120 米，燃烧范围在厂区内占很大区域；地面火炬占地面积大，高架火炬相对较小。

> 注意
>
> 火炬燃烧产物并非通常理解的二氧化碳和水。火炬平时火焰并不涉及太多原材料或反应物，但必须保持不熄灭，以确保紧急排放和事故状态下能正常运作。

物质系数与毒性系数查取



- 物质系数 MF 查表（教材 1262 页），表中同时给出健康危害系数
- 查到健康危害系数后，再按表 4-16 查取毒性系数
- 示例：氯气的健康危害系数为 4，对应毒性系数为 325

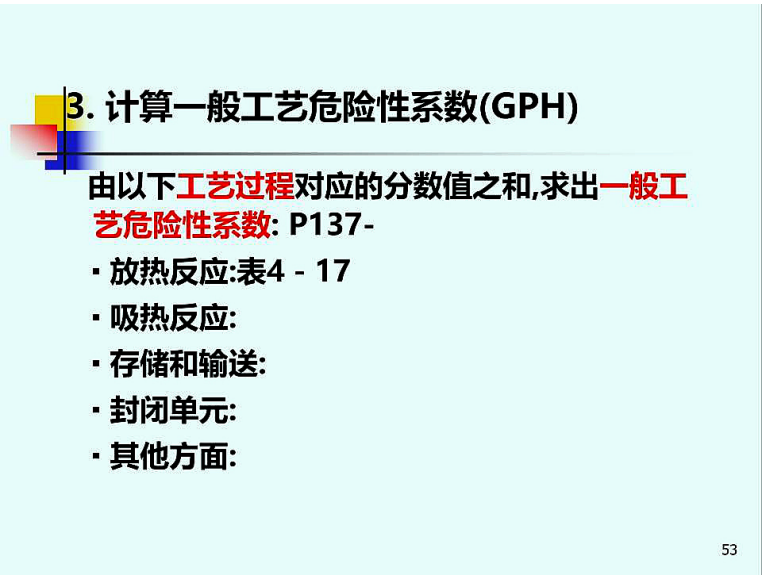
例

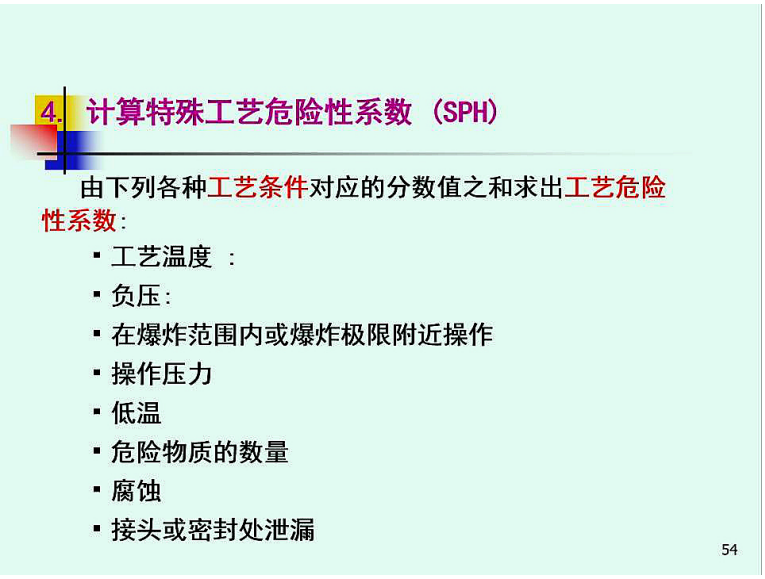
氯气：健康危害系数 = 4 → 查表 4-16 → 毒性系数 = 325。

定义

NFPA：美国防火协会（消防协会）的缩写。美国环保署等机构定期更新危化品理化特性参数并共享至数据库，便于查询。

工艺系数确定



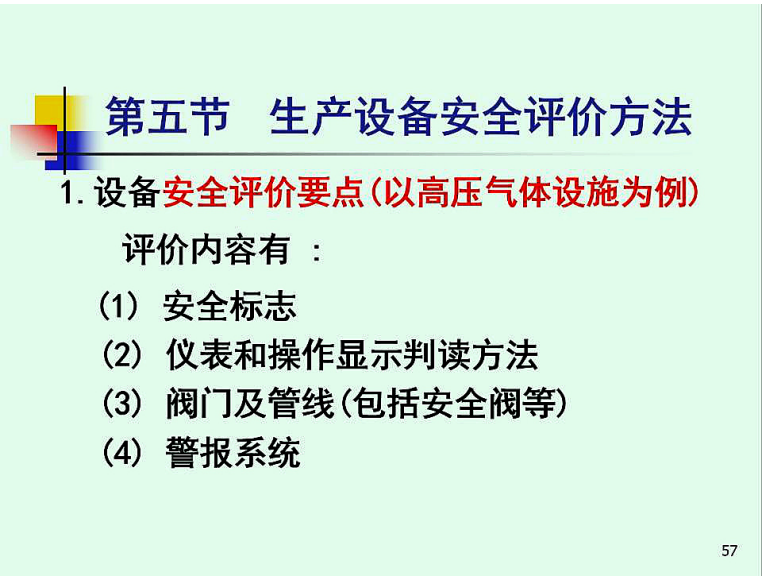


- 放热反应有特定表格（4-17 表），详细列出不同情况下的具体取值，使用方便
- 特殊工艺包括：温度变化、极限操作范围接近极限、操作压力、低温、腐蚀结构、密封处泄漏、危险物质数量等，与道化学方法基本一致
- 计算火灾爆炸指数时公式有所变化，并考虑毒性及有毒物质的最高允许浓度
- 计算后外部危险性划分为三个等级，毒性也分级，取等级更高者优先关注

注意

单元快速排序法相对简单，关键在于确定哪个等级更高，便优先关注哪个单元。

生产设备安全评价方法概述



- 该方法主要针对生产设备，区别于之前讨论的工艺参数和设计
- 本质安全：设备本身的安全是第一位的，即使设备稍微超压仍能正常运行最好
- 但设备在非正常情况下仍保持安全，设计投入大、成本高、安全系数高，市场竞争中需权衡
- 对生产设备需进行客观评价，高压设备是特别重要的类别
- 随着技术发展，有智能装备和智能过程设备等不同阶段，但高压设备风险相对较高

注意

设备安全与成本之间存在矛盾：追求本质安全（非正常工况下仍安全）会大幅提高设计成本和安全系数，影响市场竞争力。因此需在保证安全要求的前提下平衡成本。

高压设备安全标准要点

- 相关标准明确要求设置安全标志和警告标志
- 重点内容：安全标志、仪表的操作显示判读方法、阀门及管线（包括安全阀和警报系统）的操作

例

房间入口挂有不同颜色或类型的牌子即可判断能否进入：牌上写”高压危险”则不能靠近，标示”有毒”则选择远离。警示牌的存在是为了保护人员安全。

仪表与阀门管线安全

- 现代仪器仪表已数字化，准确性显著提高，但不能存在误差或读数错误
- 飞行员操作飞机需依赖密集复杂的仪表盘，需全面掌握仪表信息才能确保飞行安全
- 飞行员培养过程艰辛，需严格学术训练、出色身体素质（跑步、俯卧撑、仰卧起坐等）及定期体检
- 阀门和管线是重点：现场阀门很大，包括单向阀、电磁阀、远程开关、气动阀

等，需精准控制
- 安全阀是最后一道关卡：设备超出正常或安全状态数据时发出警报；若出现物料或可燃气体泄露，情况更紧急

> **注意**
>
> 生产设备最终产品出现问题，最可能的原因是设备故障。虽然可能源于操作不当或设计缺陷，但根本上设备是问题所在。问题发生后需分析原因、改进设计和工艺。

氢气储运设备安全

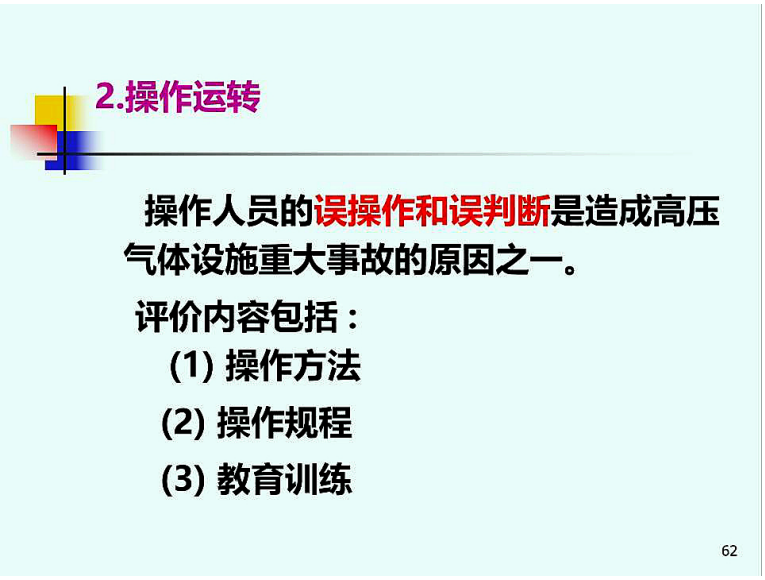
- 高压气体设施对氢气储运至关重要
- 氢气是清洁且易获取的自然资源，应用潜力巨大，但目前储运效率不高
- 现有加氢站中采用液氢方式的数量不多
- 气芯压力为 35 兆帕或 70 兆帕，储存工艺要求高
- 需掌握的技术包括：材质、快速接头、加注枪等，均需自主生产，并有一定可靠性要求

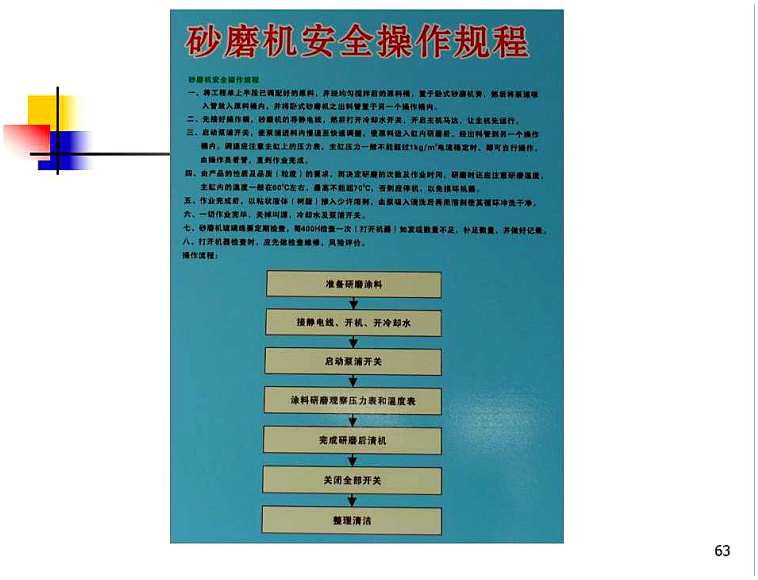
设备布置与现场检查

- 检查设备布置是否规整，包括设备、管道和地面的间隔是否清洁整洁
- 红色标记区域需注意，绿色和黄色标记区域可能涉及气体性质
- 三氯化铁具有腐蚀性，需注意 MSDS 应急信息
- 压力表需在两个红线之间，检定压力表有严格规定，每年校验一次
- 现场阀门众多，需注意识别和操作

> **注意**
>
> 压力表读数必须在两个红线之间，且需每年校验一次，这是严格规定。

操作运转与操作规程

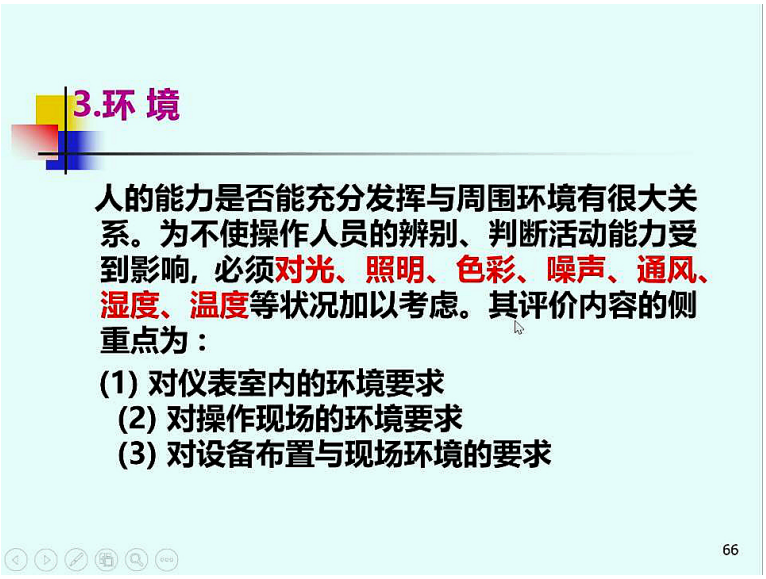




- 操作运转包括：操作方法、操作规程、教育培训等
- 操作方法应按照安全规程执行，需进行考核
- 操作不当可能导致严重事故后果

> **例**
>
> 涂料生产中的过滤机：通过控制温度进行生产，是涂料生产工艺过程中必不可少的设备。现在基本可自动化整个生产线，提高产品竞争力、性能更稳定、市场战略更稳固。

作业环境要求



- 作业环境温度有最高和最低范围要求
- 原料和生产工艺需在恒温恒湿环境中进行
- 环境因素包括：照明、色彩、噪声、通风、湿度和温度等
- 照度、色彩、噪声等均对作业环境有影响

> **注意**
>
> 作业环境温度有明确范围（最高温度约 27℃，最低温度需查 PPT 确认具体数值），需在恒温恒湿条件下进行生产。

车间标准化与定制化管理

- 放置车产品的车间遵循严格标准化规范，包括高度、间距以及地面防静电处理
- 从门口到室内区域设计有逐渐降低的斜坡（而非较高斜坡）
- 室内高度范围需参考具体标准（如 1.8-2.2 米或 2.2-2.7 米等，需查证）
- 工作持续时间、心理身体因素等也是修正因素
- 作业时间长、难度大、危险性高，作业危险性环境需综合考虑

现场安全标识与应急设施

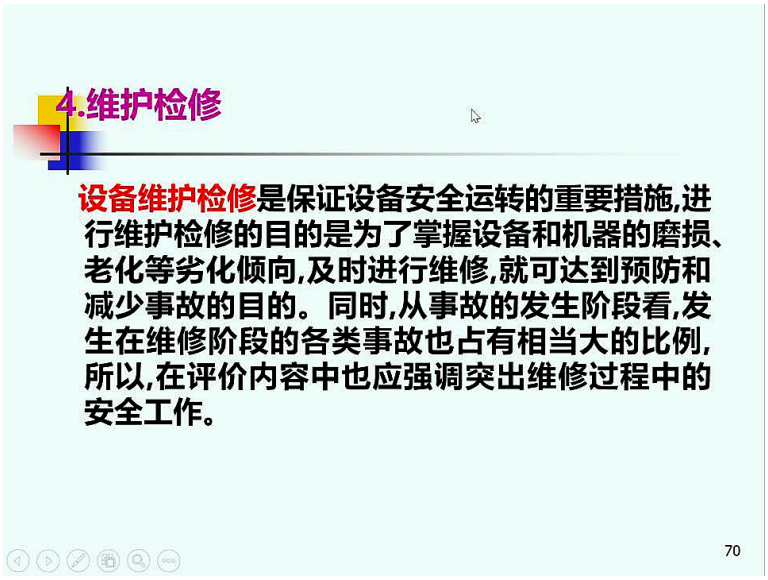


76

- 现场应配备 M 登记表以便快速识别潜在风险
- 重大危险源门口应有显示牌，显示物质的量、重大危险源等级及应急措施
- 现场地面标识清晰度需加强，路径及应急设施指示需完善
- 所用灯具必须是防爆型的
- 喷淋系统之外，还有泡沫灭火系统（真正的灭火设备）
- 主要红色管道用于输送水，特定条件下可使用泡沫灭火，需满足相应环境要求

> 例
>
> 油漆/涂料制作车间：有楼梯、栏杆、破损的桶等，楼板边上放置踢脚板以防止人员跌落，脚正好挡在踢脚板处。

设备维修的重要性



- 设备运行过程中会面临老化、裂化、腐蚀、材质变化等问题
- 提倡预防性维修，尽量避免事后维修
- 事后维修往往伴随更高的成本和风险
- 最佳维修状态是最经济、最安全的

> **定义**
>
> 预防性维修：在设备发生故障前进行的计划性维修，相比事后维修成本更低、风险更小，是最佳的经济状态。

七氟丙烷灭火系统

- 七氟丙烷可作为灭火剂，属于气体灭火剂
- 灭火剂用量取决于空间大小：空间大则需求量大，需多瓶
- 所有灭火剂瓶汇集到一根管线，再分配到需要的地方
- 系统采用远程控制，使用气动装置打开阀门，也可人工操作

> **例**
>
> 七氟丙烷灭火系统：只需一瓶即可的小空间，若空间巨大则需多瓶，所有瓶汇集到一根管线，再根据需求分配到各区域。

UPS 不间断电源与排汇流间

- UPS 是不间断电源，使用蓄电池
- 排汇流间：将多个电源排在一起、汇聚在一起
- 采用远程控制，使用气动装置打开阀门，是远程控制的自动设计，也可人工操作

无人机消防监控系统

- 无人机已完成巡航任务后返回机场并充电，为二代产品（早期机型体积较大）
- 用于消防监控和检测特定区域是否存在火源
- 装载红外热像仪，能自动定位火源，无需人工操作，由程序控制
- 在大面积林地上空飞行，选择特定区域监测，将异常位置及周边环境地图信息发送至相关人员手机

例

无人机消防监控：覆盖 1 万亩山林区域，装载红外热像仪自动定位火源，将异常位置及周边地图信息发送至相关人员手机，便于直观了解现场情况。

广州塔安全案例



- 广州塔首要任务是确保安全，一旦发生任何情况（哪怕一点舆情影响）都可能造成重大后果
- 核心安全之一是消防安全：设有多个避难层（共 5 个），配备消防报警系统
- 广州塔紧邻珠江，周边有财富论坛码头（王子号、公主号、红船）、银线旅、越剧等特色项目

例

广州塔顶部装有两台大型跳楼机，每台有 16 个波波球，可容纳 4 人同时旋转。一旦发生断电，将有几十名游客受影响，后果严重。

摩天轮设备事故案例

- 摩天轮在慢慢旋转过程中，托垫供电跟不上，导致华数片跟不上，凸显设备安全问题
- 该摩天轮临近江边，是博士后安全工程研究的一部分，专注于多米诺效应系统的安全性
- 目前还有两个项目在其他站点进行联合培养

注意

设备事故往往发生在看似正常运转的过程中（如摩天轮供电跟不上），需重视设备安全监控与应急措施。

参观场所安全提示

- 参观地点包括海洋馆和岭南印象园，其中岭南印象园的安全问题尤为突出
- 海洋馆安全情况后续详细讨论

11 月 10 日

课程考核与复习提醒

- 本课程共 5 次作业，平时成绩取群里最高的 3 次
- 若作业均为 A，平时成绩基本为 A（请假或旷课除外）
- 考试时间地点由张泽宇在群里通知
- 考试范围不超出课堂 PPT、书本知识与作业，需认真复习

第四章内容的重要性

- 第四章内容相对较多，是重点章节
- 引导词（否、多、少、大、小、不分、相反等）需区分”相反”与”部分”两种情况，要非常熟悉
- 安全领域没有不重要的方法，忽视任何一方面都可能涉及人的行为心理、环境、作业过程、操作岗位等风险

风险分级与应对

- 风险具有”急迫性”与”重要性”两个维度
- 急迫且重要 → 立即落实防控或改进措施
- 急迫但不重要、重要但不急迫、不重要也不急迫 → 需区分对待
- 需掌握相应的基础知识、基本概念、基本原理和方法

安全工程的专业体系

- 目前课程达到的是教育部规定的安全工程主要课程与专业方向领域
- 矿山等领域内容基本未覆盖，需重视交叉融合与动态变化
- 安全工程是系统工程，涉及多学科交叉（结构、力学、布局、法律法规等）

安全评价的类型

- 涉及安全管理评价、安全设备评价、综合安全评价等
- 与整个系统密切相关

火灾爆炸指数评价法基本流程

- 从第一步开始：确定评价单元 → 划分评价单元 → 确定物质系数
- 考虑一般工艺系数、特殊工艺系数、安全危险系数等
- 最终得出火灾爆炸指数及危险等级

管涵（涵洞）防护措施

- 高铁与输油气管线交叉时，采用管涵（钢筋混凝土）将管线罩住，从地下穿过
- 管涵两头设置泄爆装置，爆炸时压力从两端卸掉
- 设计管涵时需计算管壁承受的压力

例

地下管廊比人高几米，有照明、通风、监测设施，管线铺设在管廊两侧的架子上。

管涵防护的工程应用案例

- 中德合资医院距 19 米处有两根高压燃气管线（天然气、汽油）
- 天然气压力大，泄漏爆炸对人员聚集场所（医院）后果严重
- 采用箱涵将管线包起来，设计时需进行计算

- 这类工程问题其他专业无法完成，需安全专业人员进行计算与分析

例

切尔诺贝利核电站最终采取用水泥将反应堆全部封住的措施，属于后果风险分析后的对策措施。

火灾爆炸指数评价法的意义

- 火灾爆炸指数是基本但重要的方法
- 计算出危险等级后，可采取相应方式削弱事故发生可能性或减轻事故后果
- 涉及火灾爆炸学、有限元流体、爆炸动力学、流体动力学等计算仿真

安全评价的早期实践

- 2006 年作者在广东省较早开展安全评价工作（学校层面）
- 早期评价单位领导是作者的学生，邀请其参与恒基达鑫项目
- 火灾爆炸指数法第七版年份需自行查阅（考试内容）

火灾爆炸指数法的计算机化

- 作者第一个硕士生将方法计算机化（远程 B/S 架构，服务器 + 浏览器）
- 将全部程序化，可自动输出表 4-2、表 4-5、表 4-6 等
- 可生成单元级和工厂级评价结果

蒙德法（Mond 法）

- 在火灾爆炸指数法（含第三版）基础上发展而来
- 做了改进，增加了一些概念，提出了修正系数
- 基本程序见图 4-12
- 涉及装置工厂的整体布局考虑
- 提出了多米诺效应概念

定义

多米诺效应：一个事故引发连锁反应，导致后续一系列事故发生的现象。

快速排序评价方法

- 当其他方法较复杂时，可用简单方法对单元危害性进行快速排序
- 排序范围 137~141
- 用于生产设备安全评价

员工操作与安全管理

- 员工操作较机械，按安全规则作业，效率相对较低但安全
- 领导若抱怨安全要求不对，会放大员工的负面效应
- 安全要求来自上级，需严格执行

注意

电线塔作业时，上下塔必须使用两根安全带，不能悬空。下来时因疲劳易图快只用一根安全带，属严重违章作业（A 类违纪）。

生产设备安全评价

- 将生产过程全部分解为约 16 类，每类用快速风险/危险度评价方法进行排序
- 需清楚物质系数和毒性系数

- 不同行业（制药厂、化工厂、机械制造厂）要求不同

例

大型机械制造厂（国企）的压力容器：立式容器一节节焊接，若地面有碎屑，表面受轻微磨损，核电压力容器受内压大且疲劳循环，易萌生裂纹，检测精度要求高，出现问题至少停产 20 天。

高压气体设施安全评价（142 页）

- 对仪表及操作提出安全要求，列出两三个即可

仪表操作安全要求

- 仪表读数单位能直接应用，原则上不再换算
- 阀门用不同色彩涂色，区分抛物光盘和开关光盘
- 阀门有远程控制（电动最快、气动也快），同时保证能手动

注意

储罐（油罐）下面的阀门必须有紧急切断阀，且具备自动控制（气动或电动），一旦泄漏立即切断。老旧储罐未预留紧急切断阀安装位置，改造困难，不符合新标准。

报警系统与操作运转

- 报警系统需自行复习
- 操作运转涉及人的因素，包括指令、人的动作、辅助要求
- 需有操作方法、操作规程、教育培训/教育训练

航天领域的安全案例

- 挑战者号与哥伦比亚号航天飞机失事
- 哥伦比亚号：发射升空时保温陶瓷掉落一块未维修，返回大气层时因高热融化
- 挑战者号失事发生在高考那年

例

航天飞机表面被太空微尘垃圾碰撞，或保温陶瓷脱落，返回大气层时因高热融化导致事故。

设备维修与培训的重要性

- 培训环节不能掉以轻心，必须不断改进
- 飞机维修必须严格按程序执行，装拆后必须完全匹配，不能有任何闪失
- 设备设施（如高速旋转的动设备、仪表盘、操作杆）操作需严格规范

自动化改造的技术支撑与可靠性

- 气雾剂等产品若改为自动化生产，需要技术设计与支撑
- 改造一条生产线约需投入六七百万，企业需评估投入产出
- 自动化后需考虑：可靠性、可控性、故障后能否及时维修
- 这些都是系统安全必须考虑的问题

人机环境与操作规程的适配

- 操作规程需更好地适应人机环境
- 环境要求多样，不能只考虑舒适的办公室环境

- 水利部门领导暴雨时必须在现场，体现岗位环境适配的重要性

例

暴雨内涝场景：积水处安装水位监测系统，一旦异常立即应急报警。以前广元路曾因暴雨导致车辆被冲走、人被淹（如送高考途中遇一米深积水），现在通过监测系统已能有效应对。

地面标识与警示标志

- 作业现场地面标识不清晰、警示标志不足
- 涂料生产车间存在设备维护薄弱、物品随意乱丢的问题

大型设备设施的维护与诊断

- 大型设备（发电厂汽轮机、电动机、锅炉）一旦叶片或震动出现小问题，可能导致严重后果
- 维护方式：通过震动、故障诊断监测位移、震动、频率
- 发展方向：远程智能诊断、自动判断

定义

治愈（自愈）：设备设施在出现基本问题时能够自动恢复的功能，类似人生病后自愈。特别适用于航空航天等极端环境。

- 可通过远程维护维修保证运行可靠性，减少自动化风险

预防性维修与以可靠性为中心的维修

- 预防性维修工程：以可靠性为中心的维修
- 核心问题：设备维修后可靠度能恢复到多少

定义

可靠度：产品、设备或系统在预定的使用周期内完成其规定功能的概率。

- 可靠度达到要求时，不会发生故障；即使发生故障也不会引发事故，风险可控

注意

可靠度是概率概念，不是”绝对不出故障”。达到一定可靠度要求后，故障概率低且故障后果可控，才是风险可控的本质。

RBI（基于风险的检测）

- 大型设备（价值几百万甚至上千万）停产前必须做 RBI 或类似评估
- RBI = Risk-Based Inspection，基于风险的检测
- 结合 CM（维修）等，使整个系统始终可控
- 信息化管理：每个元器件/零部件的故障概率可统计，进行系统综合

设备事故案例分析

- 测试时设备爆炸，碎片飞出击穿墙壁，所幸无人
- 事故后收集碎片做原因分析，目的：
  1. 找到原因，避免再次发生
  2. 区分技术原因与管理原因（非领导责任）
  3. 判断材料是否适合该工况

例

人造水晶（手机晶振片材料）在高温下长期工作，常温下已失去韧性，韧脆转变温度升高。做密封测试时必须先升温，否则会脆裂。该厂曾是全国最大的人造水晶生产商。

无人机巡山与设备故障应对

- 无人机充电后巡山，可识别火苗、定位并立即采取措施
- 成本较高，但社会关注度在提升
- 设备一旦出故障，需考虑能否维修、是否有备用方案

游乐设施（摩天轮）的检修与安全

- 摩天轮每天早晨检修约 2 小时，每周有一天长时间检修（上午到下午）
- 检修时无外人，但若运行中突然停机，每个球内有 4 人，后果严重
- 建议：统计分析华硕片（关键部件）的可靠寿命，在快到更换周期时主动更换，而非等故障发生

注意

设备故障不能只靠”实验做不了就分析”，要量化分析可靠寿命，用预防性更换替代事后维修。本质安全角度出发，避免 PDF（概率性故障）真的发生。

跳楼机与摩天轮的风险差异

- 跳楼机停机影响相对较小：乘客本就处于激动状态，且设备可靠性高
- 摩天轮停机影响大：缓慢运行中突然停止，乘客被困高空
- 省特检院会派专业人员定期指导，保证正常运行

重大危险源公示

- 广州塔附近江边有游船（公子号、公主号、王子号、红船号）
- 相关水域属广州港集团/广州港务局管理
- 需进行重大危险源公示

设备安全评价的总体要求

- 设备安全涉及：基本要求、安全评价、操作运行、环境形成、维护检修
- 承压设备是书中介绍的重点示例

特种设备的分类

- 8 大类：承压设备、压力管道、起重设备、场内运输车辆、压力容器、索道等
- 监管部门：市场监管局（原质检部门与工商、市场合并），国家层面为市场监管总局
- 广东省特种设备检测研究院、广州特种设备检测中心（机电 + 承压设备合并）

例

行业人才需求：高级检验师年薪可达 142 万，需检验士约 10 年经验、获带国徽的科技进步奖、主持完成至少一项项目。有特检院院长从基层逐步晋升，也有部门负责人跳槽到民企获 120 万年薪。

安全管理的重要性

- 安全生产的重要方面是管理

- 安全管理评价涉及：安全管理体系是否健康、可持续、不断改进提升

体制与机制

- 十五五规划由习近平总书记亲自任组长，在二十届四中全会作编制说明
- 我国体制与国外不同：国外 4 年换届，我国体制为多数人服务

例

上甘岭战役中的邱少云、堵机枪的英雄事迹，体现我国体制下战士的奉献精神，这是管理有效可靠的基础。

- 机制：制度、体系如何运行高效合理
- 发展要求：从粗放式转向相对稳定、高质量

法治与组织措施

- 法治是管理的基础
- 在体制基础上做组织措施，控制不安全行为

注意

不能以”事故为 0”为目标，总会或多或少有事故。管理目的是把工作做好，而非为难管理人员。

事故分级边界

- 死亡 50 人以上，或受伤 3~9 人（含 3、9，不含 10）为特别重大事故
- 边界事故的部门领导需先停职

注意

事故分级边界易混淆：受伤人数为”3~9 人”（大于等于 3，小于等于 9），不包括 10 人。注意”3~10”与”3~9”的区别。

安全管理在安全因素中的比重

- 安全管理占影响企业安全因素的 24%
- 机务因素的危险性控制占其余部分

本质安全

定义

本质安全：通过设备设施本身的设计（材料、结构）实现安全，而非依赖外部管理。如钢杯掉地不碎，玻璃杯掉地会碎。

- 本质安全不足时，可通过加强安全管理来弥补
- 特殊环境中工作介质旁的材料选择可提升本质安全水平

例

手机屏幕：钢制屏幕看不清字体，可折叠塑料屏幕不怕摔但成本高。本质安全需在功能与安全之间权衡。

现代安全管理方法

- 安全管理评价第一方面：现代安全管理方法的应用
- 包括：安全行为心理学、人机工程、信息管理、PDCA、目标管理、三级危险点、

网络管理、计算机管理、电话管理、教学、安全评价
- 管理科学、运筹学方法也可用于安全管理

安全教育与三级教育

- 三级教育是必要的
- 操作规程、培训教育是安全管理的重要环节

安全生产责任制与职责分解

- 安全生产法明确要求落实”一岗双责”“三管三必须”，职责分解不到位就要承担责任
- 安全管理部门是”安全生产监督管理综合协调部门”，核心职责是协调、组织、指挥、控制
- 要把每个部门的职责划清楚，并检查其是否落实，而不是只做传达
- 各级人员都要建立安全生产责任制，职能部门安全指标需分解到岗到人
- 企业应张贴各级人员安全生产责任书（如消防安全责任书），便于对照检查

注意

管安全不是”有责任”的问题，而是”愿不愿意承担责任”的问题。真正做安全是管理角色，要主动去检查、去追责，而不是等政策来了才告知别人”你们要被追责”。

安全生产制度汇编的时效性

- 最新《安全生产法》为 2021 年修订，制度汇编应随之更新
- 若法规修订后企业未完善自身安全生产制度汇编，说明领导不重视、标准滞后

注意

安全生产法修订后，企业必须同步修订自己的安全生产制度汇编，不能拿旧版制度应付检查。

安全管理到位与否的判定

- 判断安全管理是否到位，看是否做到：该签名的签名、该培训的培训、该学习的学习、防护用品已准备、演练已按计划组织
- 若以上全部做到位，工人仍出事故，则属于其他原因，而非管理失职

例

某领导被提拔到市里，并非因出了事故而”没事”，而是因为他把该做的全部做到位——签名、培训、学习、防护用品、演练都落实，即使出事也不是其工作失职。

安全生产费用管理

- 安全生产费用必须有专项费用，并制定管理办法
- 必须提取安全生产措施费用的行业：建筑施工、矿山（煤矿）、化工（石化）、交通运输、机械制造

注意

安全生产措施费用提取是法规强制要求，不同行业有明确范围，需按行业规定执行，不能以”没查到”为由忽略。

安全机构与人员配备

- 《安全生产法》对安全机构设置和人员配备有明确规定
- 安全工程做风险评估，本质是”从法律来到法律去”——法律泛指法规、标准、政策

安全管理评价方法

- 将各要素分解，逐项判断是否符合要求，符合给分、不符合扣分，最后分级
- 安全管理在系统工程中作为其中一个方面，核心的管理方法理论在《安全管理》课程中深入学习

系统安全综合评价

- 综合评价把各方面综合起来，核心是”意外能量的意外释放”
- 事故类型多样：火灾爆炸、高处坠落、物理打击、机械伤害、物理爆炸、中毒窒息等，均与能量相关
- 能量形式包括有形和无形能量，如势能转化为动能、机械能之间的转化

例

从高处坠落是势能转化为动能；机械制造过程中物体挫伤是机械能转化到人体，都属于能量意外释放。

设备设施与安全文化

- 设备设施安全状态、完好率是安全管理的重要条件
- 安全文化是重要的”软实力”，看不见摸不着，但能反映企业真实管理水平
- 观察企业文化：参加一次会议、到食堂、看技术措施即可感知

注意

安全文化看似”没用”，实则是非常有用的软实力；看似”有用”，抓起来又看不见摸不着。到企业实地感受一次会议或食堂，就能判断其文化水平。

安全评价方法应用实例（第 8 节）

- 教材第 152 页第 8 节为”安全评价方法应用的实例”，基于生产过程的企业安全评价
- 传统安全管理存在不足，需建立基于生产过程的安全管理模型

职业健康安全管理体系

- 早期提法：职业安全健康管理制度
- 现行提法：职业健康安全管理体系（GB/T 45001-2020，推荐性国家标准）
- 45001-2020 与 ISO 45001-2020 等效

定义

职业健康安全管理体系：按照 GB/T 45001-2020 标准构建的管理体系，将职业健康、安全、环境（E）、质量（Q）等要素融合在一起，企业可几个标准一起做认证，也可分开认证。

基于生产过程的安全管理模型

- 优点：保证管理的连续性，安全与生产过程紧密相连，便于建立安全评价指标体系
- 安全评价体系构建：系统化体现在图 4-18，包含危险识别、评价、管理过程、安

全培训、应急响应等要素，每个要素可打分
- 图 4-9 给出指标体系的三级指标：设备设施、领导重视程度、安全培训、员工素质、环境等
- 新方法包括人工智能、AI、大语言模型（LLM）等

注意

安全生产法中的部分提法（如重大危险源现场登记）在教材中可能已过时，属早期版本，但重大危险源登记等要求仍然存在。

生产工艺过程安全评价

- 评估单元：原料、中间产物、工区连续性，共 4 个评估单元
- 从人、机、环、管理 4 个方面分析危险源和安全隐患
- 每个作业过程做危险有害因素分析，识别隐患
- 危险等级确定后，给出相应控制措施

油库安全评价案例分析

- 油库储罐含汽油、煤油、柴油，属易燃介质场所，易发生火灾，汽油可能引起爆炸
- 油品通过海上管道输送至储罐，码头有单管专用或共用管道至转换坑，再经岸上泵打入储罐
- 部分化工品有剧毒，需专用管道
- 油库远离人口密集区，周围无铁路和高压输电线

定义

重大危险源：指长期或临时生产、加工、搬运、使用或储存危险物质，且危险物质数量等于或超过临界量的单元。

例

油库危险有害因素分析：
- 物料方面：易燃、易蒸发、易扩散、易受热膨胀、不可压缩、有毒性
- 工艺过程方面：装卸区（火灾爆炸、车辆伤害、机械伤害）、主储区（火灾爆炸、中毒窒息、冲撞、机械伤害）、输送区（管道火灾爆炸）

注意

油库评价要考虑全面：布局、设备设施位置、人员、建筑等，不能只想到火灾爆炸。油库中石油、中石化员工平时风险较低，但油库本身风险高，油一泄露即形成爆炸性混合气体。

油库适用的安全评价方法

- 安全检查表法
- FMEA（故障模式与影响分析）
- 道化学法（火灾爆炸指数法）
- 其他：事故树、事件树等

注意

油库必然构成重大危险源，评价时需系统考虑布局、设备、人员、建筑，不能只关注单一危险因素。

11 月 17 日

课程思政与安全发展理念

- 总书记强调”安全是发展的前提，稳定是强盛的前提”，要求树立安全发展理念，将安全放在首位
- 安全系统工程保障人民财产安全与社会稳定，是平安中国建设的重要任务
- 学习要求：掌握基本概念、基本理论、基本原理、基本方法、基本控制及应用
- 核心目标：识别危险因素、评估风险等级、制定防范策略、持续改进优化
- 讨论题（考试范围内）：安全与发展的双赢策略、企业社会责任与安全投入的边界、科技进步带来的新型风险、政府监管与企业自律的平衡

注意

企业追求利润最大化与安全投入之间存在张力，安全投入是企业的基本责任，不能以利润为由削减。

安全工程师的职业素养与责任

- 爱国情感：融入国家安全大局，守护家园安全
- 敬业精神：精益求精，安全绝不能断，人命关天
- 法治与科学精神：敬畏法律、尊重科学、诚实守信、生命至上、以人为本
- 成为坚定的法治捍卫者、职业道德的崇高践行者、科学精神的忠诚者
- 主动预防事故，保障个人职业安全

系统安全中的新技术应用

- 新兴技术：VR、大数据、互联网技术、智慧消防、智能监控
- 信息化安全管理技术、课程设计等将在系统安全领域发挥重要作用
- 构建大格局：全球化、信息化，超越传统安全观的局限

安全文化建设（示范企业创建）

- 四个保证：组织保证、机构保证、投入保证、人员保证
- 理念体系：核心理念、安全理念、愿景、目的、使命、道德价值观
- 强调以人为本、生命至上，采用多方法（技术、管理、环境、人文）综合手段

危险控制技术概述

- 本章目标：了解控制的基本方法和原则，掌握决策方法（技术/管理/综合），熟悉宏观与微观控制及运行模式
- 危险控制的目的：降低事故发生的可能性、减少事故严重程度、减少事故经济损失（伤亡 + 经济损失）
- 其他影响：名誉、社会影响、环境污染等，最终可折算为经济损失

定义

危险控制：以系统工程原理为指导，对危险进行控制，防止事故发生或减轻事故后果。

宏观控制技术

- 以整体系统作为控制对象，运用系统工程原理对危险进行控制
- 采取的手段：法制、经济、教育

例

法制手段（法律约束）、经济手段（惩罚或激励措施）、教育手段（对员工特别是新员工进行持续安全教育）。

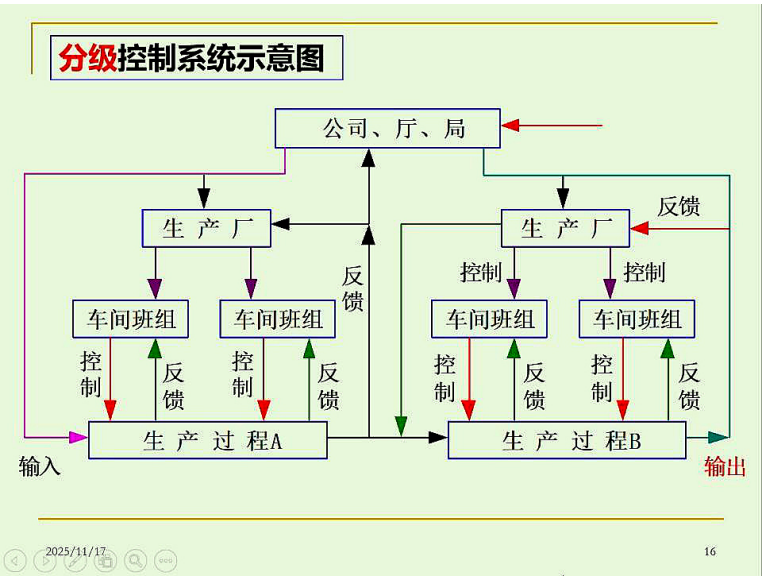
微观控制技术

- 以具体的危险源为控制对象
- 以系统工程原理为指导，对危险进行控制
- 对需要监控、自动化、接触较高的危险源，必须采取保证技术或补偿技术，否则会产生严重后果

注意

没有危险源就不符合控制对象的要求。危险源可能导致事故，但发展较慢，必须重视。

危险控制的原则



- 闭环控制：相对闭环，没有绝对闭环，系统与外界存在环境适应性，本身是动态变化的
- 实时控制：系统是运动变化的，需采用实时控制，现代采样频率很高
- 分级控制：不同层级、范围、性质、个人不同，可自行调整并实现优化目的

例

爆炸实验中，从 0 秒到 0.01 秒可采集四五千至上万个压力变化数据点，用高速摄像机记录全过程，体现实时控制的高采样频率。

例

煤气灶、热水器等自动控制系统：点火不燃、温度达不到、压力过低时自动关闭。但使用 8-10 年后水箱腐蚀、燃气泄漏等问题仍存在，说明自动控制并非根本性措施。

决策的基本概念

- 决策是对事物主客观条件的认识与判断过程
- 决策包括决策的准备和选择两个环节

- 狭义决策：方案选择；广义决策：准备、方案、优选方案、实施等全过程

> **定义**
>
> 决策：在求生与发展过程中，对事物主客观条件进行认识、分析、判断，并选择方案的过程。

决策的分类

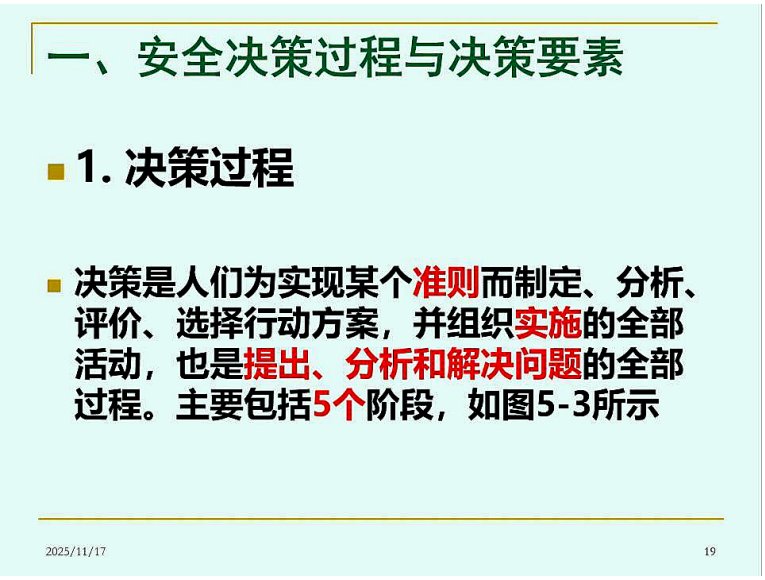
- 按约束性：约束性决策、随机性决策
- 按确定性：确定性决策、不确定性决策

> **注意**
>
> 确定性决策好做，但世界往往是不确定的。不确定性决策占主导，包括风险性不确定性和完全不确定性。

风险型决策的 5 个条件

- 风险型决策问题通常有 5 个条件（教材 169 页）
- 决策者面对大量不确定性，需要很强的抗洪（抗风险）能力
- 涉及经济社会、政治、资源、个人化等多方面因素

决策的基本过程（5 个阶段）



- 明确目标
- 构造模型
- 分析评价
- 实施
- （决策流程：提出问题 → 了解待解决的决策问题 → 明确目标（含标准、准则）→ 构造模型并估计参数 → 分析评价 → 选择方案 → 组织实施）

> **定义**
>
> 决策过程：从总则制定、分析评价、选择方案到组织实施的全部活动，用于解决问题。

决策的要素（4 个）

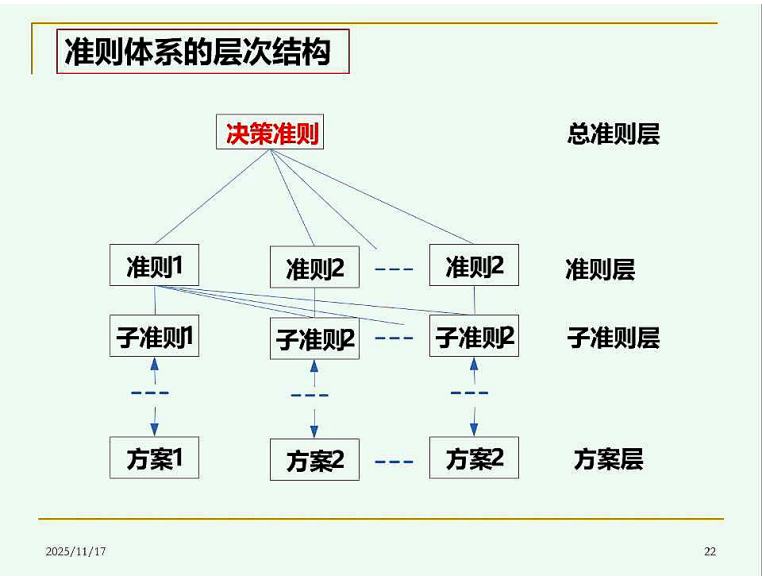
- 决策者

- 决策的发言（方案）
- 决策的结构环境
- 决策规则

定义

决策者：掌控全部决策过程，规定总任务、总需求，确定价值判断和决策规划（如倾向性意见），最终确定方案并组织实施。

决策的层次结构



- 常用层次结构表示决策准则体系或指标体系
- 从总目标到中间准则层，再到最底层的方案层
- 用于评价和选择方案

决策准则体系

- 决策需要一套准则体系来判断和确定方案
- 决策还涉及决策的环境和结构
- 决策态势受多种因素影响，如举办地点、举办方式等（进博会、博鳌论坛、广交会等案例）
- 广交会已举办 100 多届，采用线上线下结合的方式
- 决策中不存在绝对最优，只有相对更优

例

江苏城市足球联赛（苏超）：门票约 10 元，从 5 月持续到 10-11 月，带动了当地经济发展。说明决策中”最优”是相对的，通过低成本高带动效应实现更优结果。

决策目标与方案

- 决策目标：预防事故发生，协调民事或安全利益，避免伤害
- 决策方案：为达到目标制定一系列措施，而非直接执行
- 安全生产与生产进度存在矛盾（如赶工期），但不能因此放弃安全
- 决策方案后果需考虑潜在问题：
  - 人身安全方面
  - 精神思想方面

- 行为方面
- 实施反馈

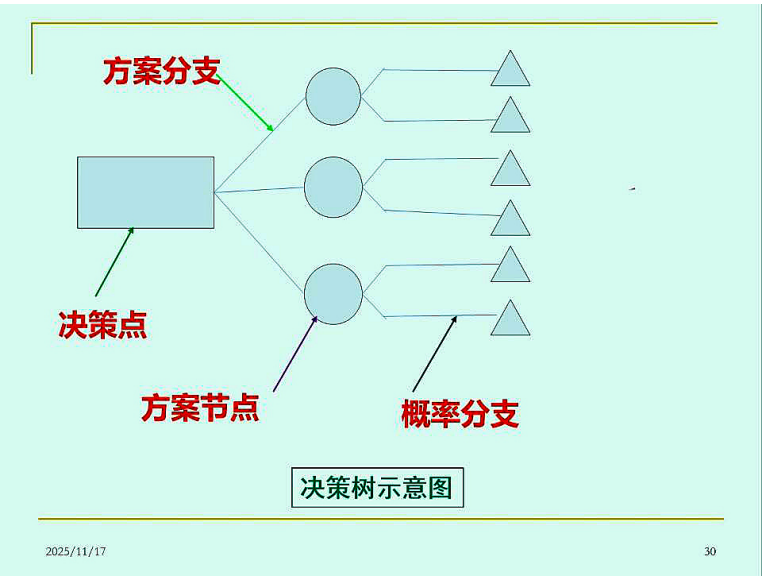
> **注意**
>
> 决策方案的后果涉及”人、能量、人的心理、人的行为”四个方面，实施反馈是重要环节，不能只关注直接后果。

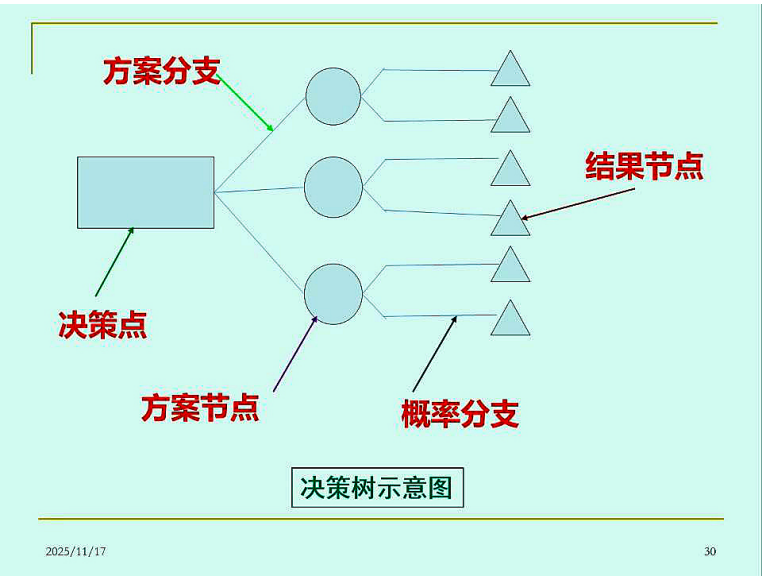
决策方法分类

- 定性与定量相结合的决策方法
- 模糊多属性决策方法
- 常用方法：决策评分法、决策树法

> **定义**
>
> 决策评分法：通过找到相关人员对照比较，对方案进行相对客观准确的评分，从而确定最优方案。

决策树法





- 绘制决策树，计算各分支的概率

- 计算相应结果节点的收益
- 计算各概率点的收益期望值
- 通过比较期望值大小选择方案

例

教材 176 页应用举例：独立研制成功的期望值为 12，企业研究的期望值为 14.4，取较大值 14.4，因此选择与外部协作共同研制。

定义

决策树法优点：

- 形象直观
- 易于比较方案
- 可定性也可定量分析，量化结果准确

固有危险源的概念

定义

固有危险源是生产中导致事故和损失的不安全条件，包括物质因素和环境因素。采取控制措施后，它就不一定是危险源了。

危险源按性质分类（5 类）

- 化学方面
- 电气方面
- 机械方面
- 辐射方面
- 其他方面（化学、机械、电气、辐射之外的归入此类）

注意

这 5 类危险源是考试重点，必须记住。分类原则是：化学、机械、电气、辐射之外的都归入”其他”。

化学危险源

- 包括生产过程中涉及的原料、成品、半成品、催化剂等
- 分为 4 个小类：
  - 火灾爆炸
  - 工业污染
  - 毒害
  - 大气污染、水污染

电气危险源

- 引起触电危险
- 漏电危险
- 着火危险（前提是有电）

注意

电气着火危险与化学火灾爆炸不同，电气着火的前提是”有电”，两者发生频次不同，但后果都很严重。

机械危险源

- 包括土木基建类
- 重伤、重物伤害
- 速度和加速度伤害
- 运行、旋转、往复运动、冲击等运动形式带来的危险

注意

事故伤害类型有 20 种归纳（企业职工伤害事故），但危险源分类是基本原理，两者不要混淆。

其他危险源

- 噪声
- 强光
- 高压气体
- 高温、高温源（如运行中机械表面烫）
- 特别潮湿的地方
- 三种危害

危险源控制措施（6 个方面，按顺序记忆）

1. **消除**：本质安全，从根本消除危险源
2. **减弱**：控制危险源，如超压安全阀、安全电压、保险丝、安全评估、设置报警
3. **预防**：在无法消除、减弱、预防危险环境时，将人与危险因素分开
4. **隔离**：禁止入位、颜色标识标记、安全距离、安全罩、固定距离限制
5. **保留**：所有措施都采用后仍存在的风险，只能保留
6. **转移**：将风险转移到其他方面

例

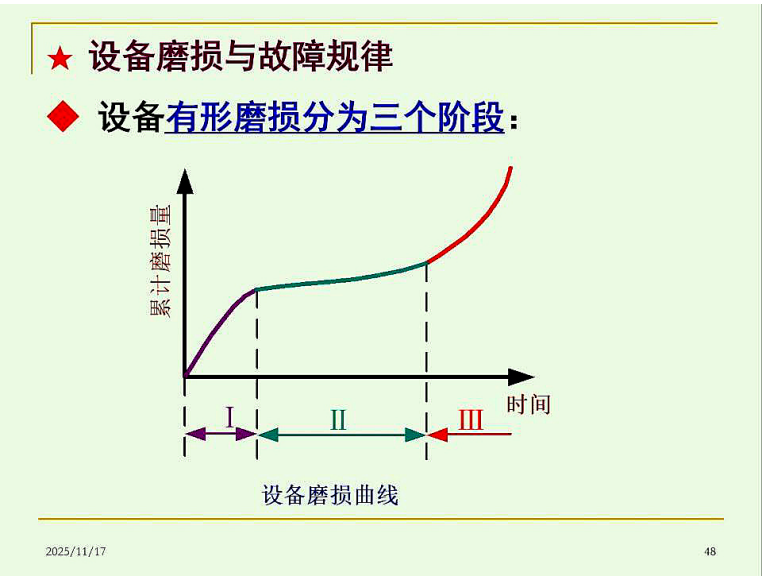
1998 年长江上游荆江分洪工程：为保护武汉等大城市，在新疆（应为荆江）南面分洪，牺牲局部保全全局，是”转移危险”的典型例子。

注意

6 个措施的顺序（消除、减弱、预防、隔离、保留、转移）必须记住，考试常考。对任何事故风险，可综合利用这些措施。

降低事故发生概率的措施

1. 提高设备运行可靠性

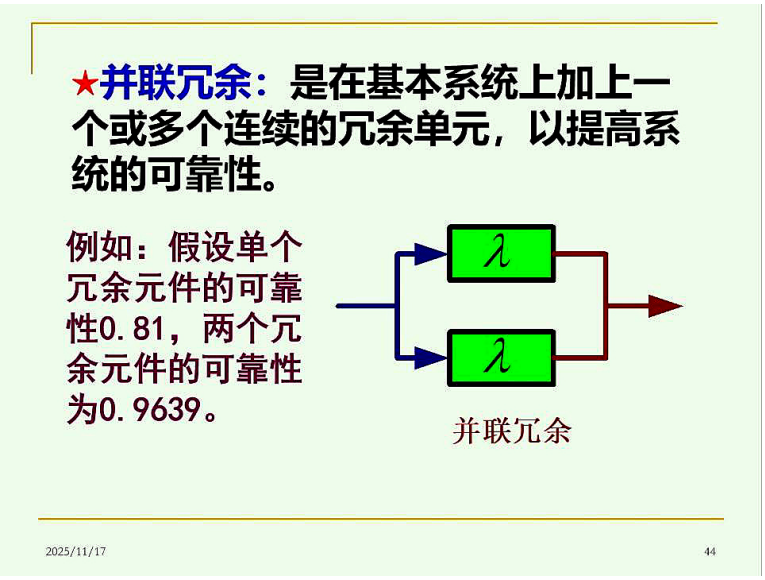


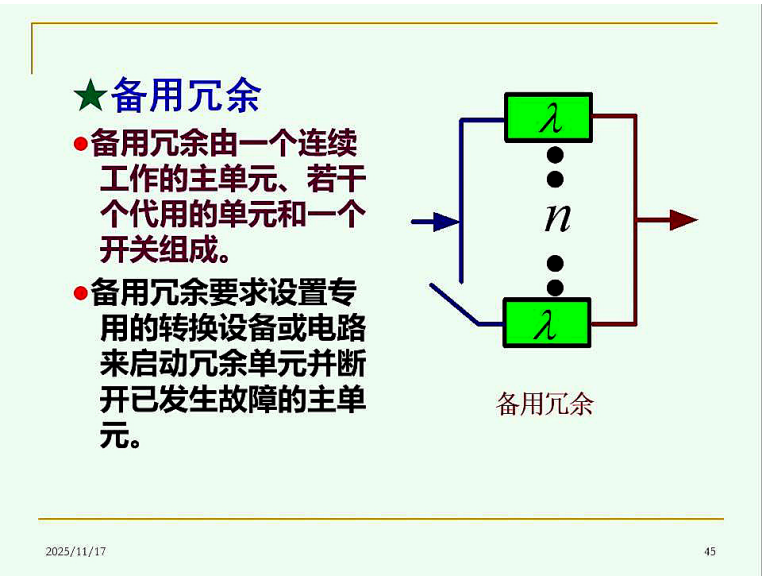


- 设备可靠性取决于元件的结构和性能是否符合设计要求
- 选用高可靠性元件会增加成本，需综合权衡
- 设计时采用可靠寿命概念，到寿命期及时更换

> **例**
>
> 早期电子设备多依赖进口，现在基本国产化，元器件专业度高，可靠性大幅提升。

2. 采用冗余系统





- 平行冗余：多个通道完成同一功能，只要一个正常即可
- 表决冗余：如 3 个中 2 个或 3 个正常即可
- 串联冗余：如毒性液体用两个开关，一个坏了另一个仍可关闭

> 例
>
> 水龙头装两个开关：万一第一个坏了，第二个还能关住，便于维修。

3. 采用可靠工艺

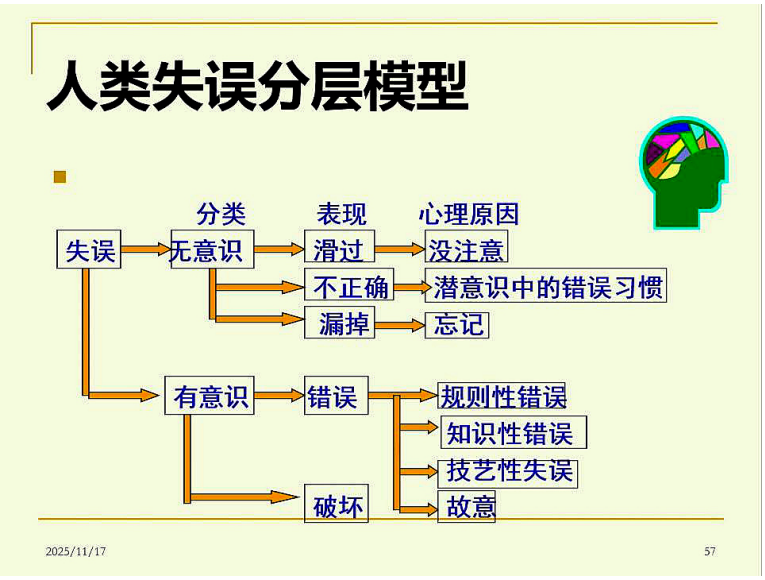
- 金属材料经热处理后性能不同
- 焊接接头与母材性能不同，需通过工艺处理保证整体性能
- 生产工艺选择需权衡：高温高压 vs 常压常温（效率与风险）

4. 提高系统抗灾能力（系统韧性）

> **定义**
>
> 系统韧性：在自然灾害或外界事物干扰时，自动抵抗而不发生事故的能力。包括：
> - 较强的吸收能力
> - 适应能力
> - 恢复能力

5. 减少人的失误





- 对人进行充分培训：安全知识、安全技能、安全态度
- 以人为中心，改善作业环境，提供安全性较高的劳动条件
- 提高机械化程度，用机械代替人工，减少井下作业人员
- 用人机工程学原理改善接口安全状态
- 使工作性质与工作人员性格特点相匹配

> **注意**
>
> 机械化是”换人”，自动化是”减人”，智慧化是”无人”，本质安全水平逐级提升。

例

人的信息处理模型：视觉输入很快（15%），但处理很慢，输出相对较快，信息数据跟不上，导致输出错误。这是人失误的分层基本模型。

降低事故严重程度的措施

1. **限制能量或分散风险措施**
   - 如储罐设计容量 15,000 立方，实际只装 500 立方
   - 限制汽车行驶速度（如校园内限速 25km/h）
   - 分散风险：化简化小、能量零散
2. **防止能量蓄积的措施**
3. **加装缓冲能源装置**
   - 安全帽、安全带等防护装置
   - 建筑工地因安全带使用不当导致伤亡的案例

注意

降低事故严重程度的三个途径是考试重点：限制能量或分散风险、防止能量蓄积、加装缓冲能源装置（避免人身伤亡）。

加强安全管理的措施

- **建机构**：安全生产法规定必须建立安全生产管理机构
- **配备人员**：高危行业需配备专门管理人员、注册安全工程师，有学历和职业经历要求
- **考核兑现**：该奖就奖、该罚就罚，考核指标与结果挂钩
- **安全生产责任制**：每个岗位、每个人员、各级领导都有相应责任
- **安全技术落实与操作规程**：企业需制定安全操作规程
- **加强安全监督检查**
- **安全教育**：需考试合格才能上岗，不包庇，外协人员也有相应要求

注意

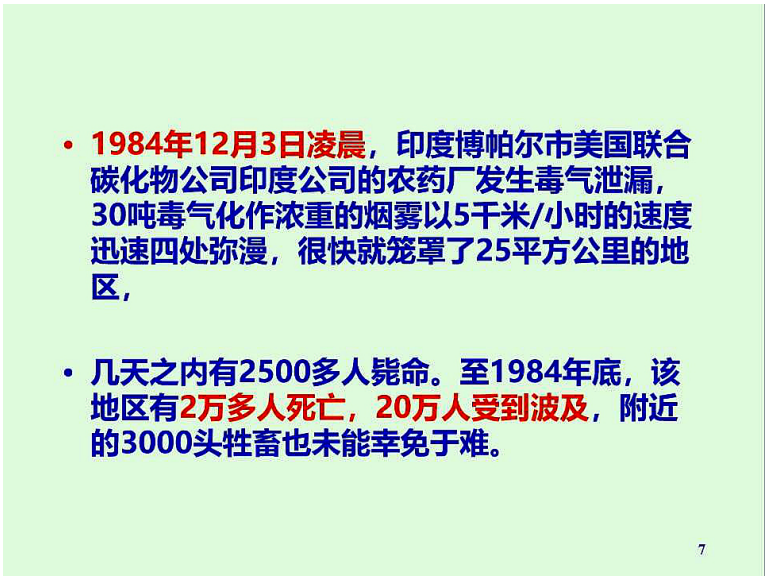
企业安全管理要求往往高于安全生产法的最低规定，如配备比例、学历、职业经历等都有更高标准。

重大危险源控制方案

- 重大危险源作为危险化学品类型，风险过于危险，需专门控制方案

重大危险源监控管理的依据与背景



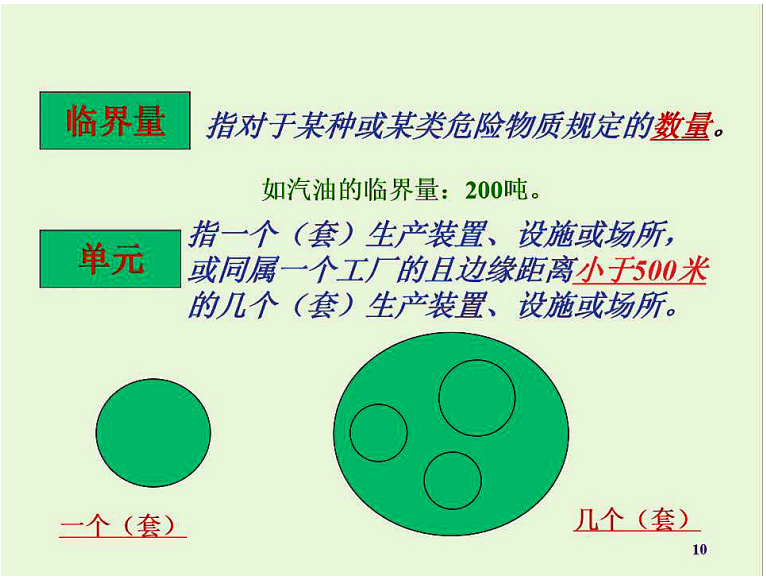


- 依据：危险化学品重大危险源相关标准、危险安全执法与危险源监督管理相关办法，以及近年危险化学品管理措施。
- 20 世纪 70 年代起，预防重大工业事故成为全球关注重点；印度博帕尔毒气泄漏等灾难性事故促使国际社会重视。
- 1993 年国际劳工大会通过《预防重大工业事故公约》，首次对重大事故给出定义。

定义

重大事故：在重大危害设施内的一项活动过程中，意外突发的事件，造成严重泄漏、火灾、爆炸及人员伤亡等后果。

重大危险源（重大危害设施）的定义



- 重大事故发生在重大危害设施中，因此需先明确重大危害设施的概念。

定义

重大危害设施（重大危险源）：长期或临时地加工、生产、处理、搬运、使用或储存数量超过临界量的一种或多种危险物质的设施。军事核设施及非管道设施现场除外。

重大危险源辨识标准

- 现行有效标准：GB 18218-2018《危险化学品重大危险源辨识》（正在修编，修编完成前按 2018 版执行）。
- 辨识核心：某种或某类危险物质实际储存量是否超过规定的临界量。
- 单一品种：实际储存量超过该品种临界量即构成重大危险源。

例

汽油临界量为 200 吨，比重约 0.89。若油库储存汽油超过 5000 立方米（约 4450 吨），远超 200 吨，构成重大危险源。城市加油站因无储存库，一般不构成。

多品种重大危险源的辨识（临界量比值法）

GB18218—2009

辨识基准：

（1）对于某种或某类危险化学品规定的数量（即临界量），若单元中的危险化学品数量等于或超过该数量，则该单元定为重大危险源；

（2）单元内存在的危险化学品为多品种时，则按下式计算，若满足下面公式，则定为重大危险源：

$$\sum_{i=1}^{n} \frac{q_i}{Q_i} \geq 1$$

式中：$q_1,q_2...q_n$——每种危险化学品实际存在量，t；

$Q_1,Q_2...Q_n$——与各危险化学品相对应的临界量，t。

11

请辨识

- 《危险化学品重大危险源辨识》（GB18218-2009）中将汽油的临界量定为200吨，甲苯的临界量是500吨。
- 现有一储罐区储存汽油、甲苯各140吨，该罐区构成危险化学品重大危险源吗？

- 140／200+140／500=0.7＋0.28=0.98＜1

18

- 多个品种共存时，需计算各品种实际储存量与其临界量的比值之和。

定义

辨识公式：将每种危险化学品的实际储存量除以对应临界量，再将各比值相加。若总和 ⩾ 1，则构成重大危险源。

例

某罐区储存汽油 140 吨（临界量 200 吨）、甲苯 140 吨（临界量 500 吨）。比值 = 140/200 + 140/500 = 0.7 + 0.28 = 0.98 < 1，不构成重大危险源。

注意

临界量因物质而异：汽油 200 吨、液化石油气 50 吨、乙烯 50 吨、甲烷/天然气 53 吨、丁二烯 33 吨、氢气临界量很小。爆炸品等按危险化学品分类及敏感度确定临界量。

重大危险源分级

1.3 危险化学品重大危险源的分级管理

- 《危险化学品重大危险源监督管理暂行规定》（国家安监总局令40号）规定：

  危险化学品重大危险源由高到低分为四个级别，一级为最高级别。

  分级指标***R***：单元内各种危险化学品实际存在量（在线量）与其在《危险化学品重大危险源辨识》中规定的临界量比值，经校正系数校正后的比值之和。

19

校正系数α的取值

根据重大危险源的厂区边界向外扩展500米范围内常住人口数量，设定厂外暴露人员校正系数*α*值，见表3：

表3 校正系数*α*取值表

厂外可能暴露人员数量	*α*
100人以上	2.0
50人～99人	1.5
30人～49人	1.2
1～29人	1.0
0人	0.5

23

- 分级目的：不同级别对应不同管理职责与要求，便于差异化监管。
- 分级依据：危险化学品重大危险源监管暂行规定、安全评价结果。

定义

分级指标 R = α（校正系数）× β（厂区边界外 500 米范围内人口数量校正系数）× 各品种临界量比值之和。按 R 值分级：R ⩾ 100 为一级，50 ⩽ R < 100 为二级，10 ⩽ R < 50 为三级，R < 10 为四级。

注意

一级、二级重大危险源需进一步计算个人风险和社会风险；三级、四级不需要。分级越高，监管越严格，一级由中央/省级检查，二级由设区的市级政府管理。

例

某企业液氯 5 吨、LPG 200 吨、汽油 5000 吨，周边常住人口 65 人。经辨识构成重大危险源。计算得 β2=1.5、β3=5、α=1.5，分级指数 = 52.5，属于二级重大危险源，需计算个人风险和社会风险。

个人风险与社会风险

定量风险评价

（1）可容许个人风险标准

- 个人风险是指因危险化学品重大危险源各种潜在的火灾、爆炸、有毒气体泄漏事故造成区域内某一固定位置人员的个体死亡概率，即单位时间内（通常为年）的个体死亡率。
- 通常用个人风险等值线表示。

34

（2）可容许社会风险标准

- 社会风险是指能够引起大于等于N人死亡的事故累积频率（F），也即单位时间内（通常为年）的死亡人数。
- 通常用社会风险曲线（F-N曲线）表示。



36

- 个人风险：某固定位置人员因事故死亡的概率（横坐标）。
- 社会风险：累积频次与死亡人数的关系（纵坐标），用 F-N 曲线表示。
- 风险分区：超过上限为不可接受区，中间为尽可能降低区（ALARP），下限以下为可接受区。
- 计算需借助商业软件，学生可学习计算。

> **注意**
>
> 个人风险、社会风险属于本课程未深入介绍的内容，但属于事故影响分析的重要部分，可计算得出。

重大危险源管理流程

2.3登记建档

重大危险源档案应当包括下列文件、资料：

（一）辨识、分级记录；
（二）重大危险源基本特征表；
（三）涉及的所有化学品安全技术说明书；
（四）区域位置图、平面布置图、工艺流程图和主要设备一览表；
（五）重大危险源安全管理规章制度及安全操作规程；
（六）安全监测监控系统、措施说明、检测、检验结果；
（七）重大危险源事故应急预案、评审意见、演练计划和评估报告；
（八）安全评估报告或者安全评价报告；
（九）重大危险源关键装置、重点部位的责任人、责任机构名称；
（十）重大危险源场所安全警示标志的设置情况；
（十一）其他文件、资料。

38

- 流程：辨识 → 登记 → 评估 → 建档 → 备案 → 核销。
- 核销：原为重大危险源，经管理后储量降低或停用（如罐内改装消防水），可申请核销。
- 档案管理：一、二级重大危险源档案报送设区的市级人民政府；一级报送省级。

> **注意**
>
> 内部管理档案中不得将安全生产许可证放入，一旦发放给企业，后续管理将非常被动。

重大危险源监测监控系统

2.5 安全监测监控体系

- 危险化学品单位应当根据构成重大危险源的危险化学品种类、数量、生产、使用工艺（方式）或者相关设备、设施等实际情况，按照下列要求建立健全安全监测监控体系，完善控制措施。



42

2.5 安全监测监控体系

- （一）重大危险源配备温度、压力、液位、流量、组份等信息的不间断采集和监测系统以及可燃气体和有毒有害气体泄漏检测报警装置，
- 并具备信息远传、连续记录、事故预警、信息存储等功能；
- 一级或者二级重大危险源，具备紧急停车功能。记录的电子数据的保存时间不少于30天；

43

- 一级、二级重大危险源必须建立在线监测监控体系。
- 要求：紧急停车系统、紧急泄漏处置装置、独立避雷防雷电系统、静电接地系统、紧急切断系统（约 4 个紧急处置系统）。
- 视频监控系统需符合规定。
- 所有存档电子数据不少于 30 天。
- 发展趋势：从早期系统分析评价、多级监控计算机辅助评价系统，向智能化、智慧化发展（虚拟现实、监测预警、态势感知、风险分析等）。

城市重大危险源监控管理措施

便携式气体检测仪





空气呼吸器

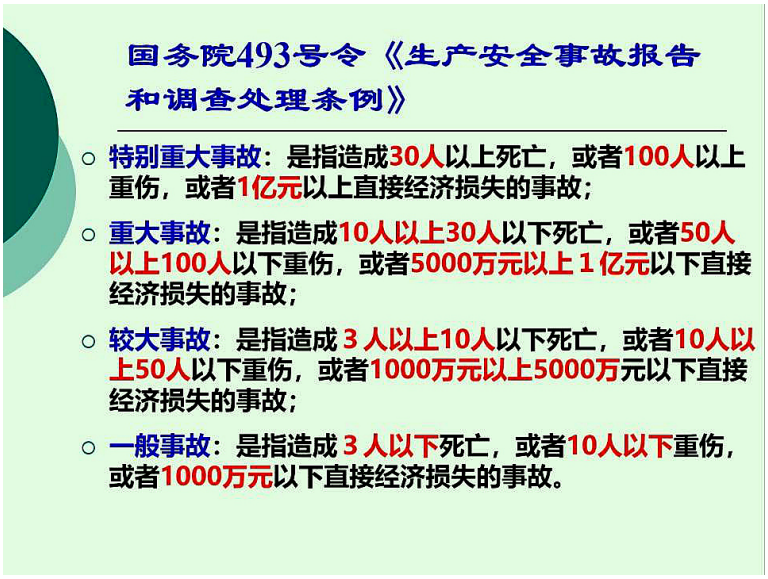
50



- 应急管理：包括应急预案编制、应急资源调查、应急演练。
- 应急预案编制核心：针对本单位风险，明确主要危险因素，进行风险分析（可参考评价报告）。
- 需调查周边应急资源，在此基础上编制预案。
- 预案形式、理念、报备备案；每 3 年或发生重大变动时修订，无重大变化则修编后重新报备。
- 应急设备设施（如变压器系统、通风）需随时可调用，平时必须演练。
- 应急预案演练与评估：按应急预案管理办法执行，编制后 2 年进行评估。

> 注意
>
> 应急设备设施不能只停留在纸面，专家现场检查会要求立即安排到位，平时不演练将无法应对。

灾难性事故概述

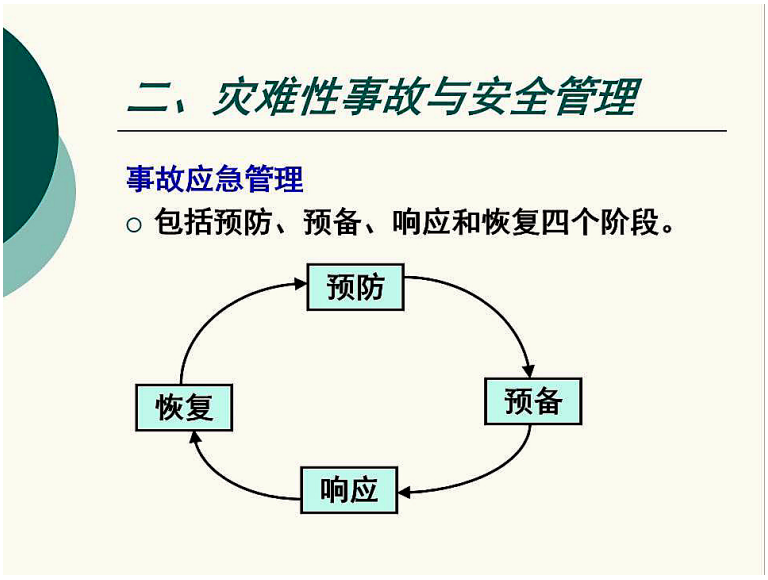


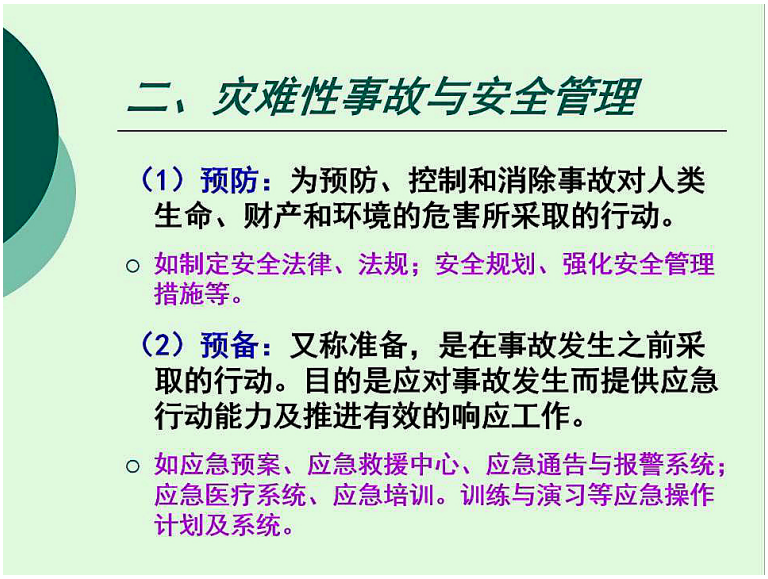
- 灾难性事故包括火灾、爆炸等重大事故，具有普遍性、随机性、必然性、因果性、多变性、潜伏性、危害性及广泛的社会性。
- 按种类分为 15 类，严重度分级分为 10 级。

定义

严重度分级依据三个指标：死亡人数、重伤人数、经济损失。三个指标中任一达到相应标准即判定为该级别。

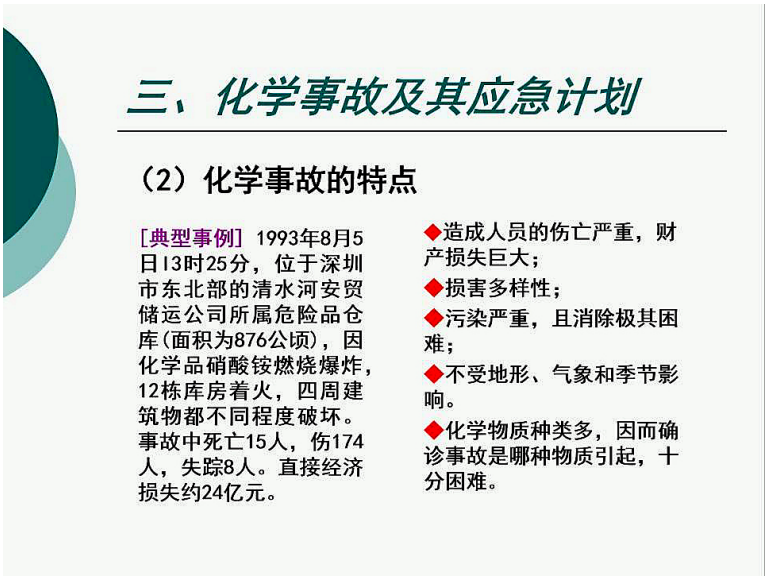
灾难性事故应急管理四阶段

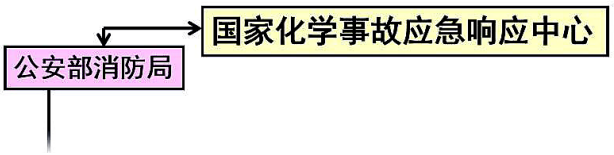




- 预防：系统工程是预防的根本工具，控制风险。
- 预备：训练、演练、应急报警系统、医疗准备等。
- 响应：事故发生时采取行动减少损失，包括医疗、疏散、救援等（可借助无人机等辅助系统）。
- 恢复：改善重建、保险理赔、修改完善、沟通总结。

化学事故应急救援体系





- 针对化学事故的应急预案，适用于石化企业（如老石化、茂名石化、湛江石化、中科炼化等）。
- 国家化学事故应急救援中心设在现场，公安部及各地省市设有专业骨干、通信网络。
- 特点：组织严密、专家协助、行政与技术结合，形成分层组织的网络专家库。