安全系统工程资料之一

安全系统工程

（普及讲义）

北京市劳动保护科学研究所
安全系统工程课题组

序

安全系统工程是近20年迅速发展起来的新兴学科，它是以机械、设备、半成品、原材料以及相关的人和环境等综合系统为研究对象，而最终以保护人和生产资料安全为目的的。安全系统工程是以系统工程的理论和方针为指导，辅之以概率统计、图论、集合论和电子计算机技术，研究各种安全问题的综合性学科。安全系统工程起始于系统可靠性工程，迅速扩大应用于国民经济各部门的安全性分析、评价和安全管理，并取得显著成效。实践证明，安全系统工程是企业安全生产卓有成效的、科学的分析技术和管理理论、方法，是安技干部的有力技术武器。学习和应用安全系统工程是提高企业管理水平和安技干部素质的重要措施。

随着国民经济的发展，安全问题日益严肃地摆在各级政府部门和企业领导干部的议事日程上来，党和国家对职工的安全问题一向十分重视，对安全系统工程的研究、开发与应用，给予了极大的支持。自81年起，劳动人事部即责成一些科研单位开始研究这种理论，分析在我国实行的可行性。82年，劳动人事部保护局的齐英杰、苏耀勇副局长在京亲自主持召开了"安全系统工程座谈会"，提出加强研究、互通情报、搞好试点的意见。83年颁发了劳人护局13号文件"关于劳动保护干部职称评定的通知"，明确规定，安全系统工程列为劳动保护干部职称评定的考核内容。84年国家科委已把这一学科列为国家重点科研攻关项目，委托劳动人事部和全国总工会组织实施。从而，为这一学科在我国迅速发展提供了极其有利的前提条件。

目前，随着安全系统工程理论研究的深入与发展，其应用范围在不断扩大。它不仅能应用于航天和国防工业；而且能应用于国民经济的各行各业；不仅能应用于工矿企业系统的安全管理，而且能应用于规划、设计、制造等系统生命周期的各个环节；不仅应用于生产，而且能应用于科研与试验；不仅能应用于自然科学领域，而且能应用于社会科学领域……，总之，安全系统工程是一种适用范围很广的方法论。

近两年来，我们根据劳动人事部的指示，在中央各主管工业部和北京、天津、南京、包头、杭州、昆明等市从事了数次宣传活动，与会者普遍反映，这是安技部门彻底改变面貌的科学理论，各地、各部门纷纷翻印了我们的讲义，为了满足广大安技干部和生产管理人员的迫切要求，我们根据目前一般安技人员的文化程度，从实际出发编写了这本通俗的普及讲义，供自学者和学习班学员使用。

本讲义除第六章是由崔国璋同志撰写外，其余章节均由肖秦琨同志编写。由于水平有限，肯定有不少错误，恳请广大读者提出宝贵意见。

除讲义外，我们还编辑了第二部分，其内容主要介绍FTA的实际应用情况，所有作品都是近一、二年内初学者所作，可供同行参考，也可从中领悟一些作图和分析的思路，尽管可能有这样那样的问题，但仍不愧为探索者的佳作。

这个资料是本所编的安全系统工程系列丛书的第一册，所以称其为"安全系统工程资料之一"，今后将陆续出版一些指导性资料，拟于85—86年期间出版"安全系统工程资料之二"（FTA定性分析范例）和"国外安全系统工程资料选编"（安全系统工程资料之三），欢迎愿为此做出贡献的同志协助（参见征文启事）。

编　者

征 文 启 事

随着安全系统工程理论研究的深入和发展，一般知识介绍已不能满足广大读者的要求。为此，本课题组拟于85—86年期间编辑出版“FTA定性分析应用范例”，欢迎广大从事应用研究的读者踊跃投稿。

稿件内容：

1．通过FTA的应用，确实收到了明显的经济效益，如杜绝或降低了人身事故，改善了设备或工艺的安全性和可靠性，提高了产品质量等。

2．通过FTA定性分析，提出了改进系统、提高安全性的具有方向性、创造性的意见或建议。

3．通过实践，证明FTA是企业安全管理的有效手段。在企业安全管理中推动、试行FTA的经验、方法、行政管理措施等。

4．FTA，FEMA，ETA，安全检查表等结合使用，并收到较好效果的应用模式（不一定四种方法都用）。

5．FTA理论研究对应用有指导意义的创见或论文。

对文字和格式的要求：

1．文字工整，图表清晰。

2．FT图一定要交待清楚，专业术语和可能产生疑问的地方，务请加注，以便于编辑人员审核和读者理解。

3．语言精炼，流畅、通俗易懂。字数视内容而定，但不宜过长。

本资料限制在50万字以内，出版时间根据稿件多少和质量的高低而定。本资料出版的，除已在其它刊物上发表过的稿件以外，一律不予退回。

安全系统工程课题组

目　　录

第一部分　安全系统工程（普及讲义）

第一章　概论

1.1安全系统工程的发展历史……（2）
1.2安全系统工程的内容……（3）
1.3安全系统工程在工业安全中的应用……（4）
1.4安全系统工程的优越性……（5）

第二章　安全系统工程分析方法

2.1分析方法之间关系比较密切的……（6）
2.2分析方法有许多共同点的……（8）
2.3根据逻辑方法进行分析的……（10）
2.4如果……怎么办的分析方法……（12）
2.5其他的分析方法……（13）

第三章　安全检查表

3.1安全检查表的定义……（15）
3.2安全检查表的内容……（15）
3.3安全检查表的优点……（16）
3.4安全检查表的编制……（16）
3.5防止事故用安全检查表……（17）

第四章　危险性预先分析

4.1危险性的分级……（36）
4.2危险性予先分析的步骤……（36）
4.3危险性的辨别……（36）
4.4危险性控制……（36）

第五章　故障类型和影响分析

5.1分析步骤……（39）
5.2故障等级……（41）
5.3故障类型影响分析举例……（43）
5.4致命度分析举例……（48）

第六章　事故树分析

6.1概论与定义……（48）
6.2事故树的编制……（50）
6.2.1事故树分析程序……（50）
6.2.2事故树的符号及其意义……（51）
6.2.3事故树的编制过程……（53）
6.2.4介绍另一种事故树的编制方法……（54）
6.3事故树定性分析……（57）
6.3.1布尔代数……（57）
6.3.2概率和与积……（58）
6.3.3利用布尔代数化简事故树……（58）
6.3.4最小割集的求法……（60）
6.3.5最小径集的求法……（62）
6.3.6最小割集和最小径集在事故树分析中的意义和作用……（64）
6.3.7结构重要度分析……（65）
6.4事故树定量分析……（72）
6.4.1基本事件故障率……（72）
6.4.2顶上事件发生概率的计算（一）……（73）
6.4.3顶上事件发生概率的计算（二）……（75）
6.4.4顶上事件发生概率的计算（三）……（77）
6.4.5顶上事件发生概率的近似估计……（78）
6.4.6概率重要度分析……（80）
6.4.7临界重要度分析……（81）
6.4.8利用概率重要度求结构重要度……（83）
6.5事故树分析的应用及其展望……（38）
6.5.1几种分析方法综合使用模式……（83）
6.5.2国内外应用状况及其展望……（84）

第七章　安全评价

7.1定性安全评价……（85）
7.2定量安全评价……（86）
7.3可靠性、安全性评价法……（86）
7.4物质系数法……（95）
7.5日本劳动省制订的“化学工厂安全评价六阶段”法……（118）

第八章　事故的预防

8.1减少事故严重度……（128）
8.2减少事故频率的措施……（129）

结束语

第二部分　事故树作图及其分析方法的应用

1．高压加氢事故分析和预测……（133）
2．冲床断指事故的诸因素及其对策……（138）
3．试用FTA定性分析蒸汽锅炉爆炸事故……（140）
4．用FTA定性分析汽油混合气体爆炸事故……（151）
5．“巡道作业被机车撞轧”事故树……（162）
6．“火车与汽车相撞挤伤调车人员致死”事故树。……（163）
7．无烟药切药系统事故综合分析……（164）
8．关于螺旋压伸机安全的初步探讨……（167）
9．应用安全系统工程，提高安全管理工作的科学水平……（170）

北京市化工总公司系统九厂事故树作图有奖竞赛获奖作品选

1．三相异步鼠笼电动机烧毁事故预测FT图……（178）
2．乙炔发生器爆炸事故分析及预测FT图……（180）
3．硝化温度过高爆炸事故分析FT图……（182）
4．呈色剂粉碎着火事故分析FT图……（184）
5．酸泵房硫酸严重烫伤人事故分析FT图……（187）
6．分散黄棕车间腈化岗位爆炸事故FT图……（189）
7．γ——甲氧基丙胺高压岗位爆炸事故FT图……（191）
8．氯代反应中的毒气污染事故分析FT图……（193）
9．桃红酸解岗位皮肤过敏事故分析FT图……（196）
10．氯代氯气中毒事故分析FT图……（198）
11．分散深兰烷基化爆炸事故分析FT图……（200）
12．红鲨落地事故分析FT图……（202）
13．Ⅰ类手持式电动工具触电死亡事故分析FT图……（204）
14．低压触电后急救不当死亡事故分析FT图……（206）
15．碱表下限停车事故分析FT图……（208）
16．合成三列计算机失控事故分析FT图……（211）
17．乙炔鼓风机转子撞碎事故分析FT图……（214）
18．聚合釜防爆板爆破事故FT图……（216）
19．锅炉爆炸事故预测FT图……（218）
20．电炉油压系统着火事故FT图……（220）

第一章 概 论

安全问题是随生产的产生而产生，随生产的发展而发展的。从原始共产主义社会到奴隶社会，由于生产工具十分简单，加以奴隶所受的非人待遇，根本没有安全可言。随着封建主义农奴制度的出现，城市扩大了，在船舶、矿山、冶金等领域里，开始使用了机械代替手工劳动，生产发展同时也带来了安全问题。18世纪发明了蒸汽机，使轮船、火车和纺织机械有了动力，但是产生蒸汽的锅炉却不断发生爆炸事故。仅从19世纪初到20世纪初100年的统计中看出，美国发生了一万次锅炉爆炸事故，死亡人数超过万人。为了防止锅炉爆炸，不少人开始了对锅炉结构、材料、压力、水垢等影响的研究。19世纪中叶，英美等国相继成立了锅炉检查和保险公司，制订检验法规。美国于1880年成立了机械工程师学会（ASME），立即着手调查锅炉事故，并于1925年发表了受热压力容器标准，这在安全技术方面可以说是一个突破。

19世纪末期和20世纪初期，西方世界进入资本主义的发展时期，由于工业规模的扩大，化工、水运、煤矿、堤坝、土建等工程常常发生一次数百人甚至上千人的重大伤亡事故，引起了社会的很大不安。为了加强管理，各国政府纷纷制订有关安全法令。英国于1864年制订了工厂法和职业病条例，后者对职业病和生产环境作了规定。1906年制订了职业病补偿法，列出了三十一种类型的职业病。1919年国际劳工局（ILO）成立，1919、1935两年向各国发出防止灾害事故的通报，1934年提出了企业卫生标准规定。在这个期间，由于各国的努力，安全技术有了很大发展，形成了一个综合性的学科。

第二次世界大战以后，工业的技术水平和规模又有了提高，但是由于原子、航天等尖端工业，大型石油、化工、冶金等传统工业事故频繁，公害问题越来越严重，许多国家政府面临事故的惨重损失和公众的舆论压力，不得不制订一些法律约束企业对安全的重视。如美、日、英分别于1971、1972、1973年相继制订了安全卫生法。同时也加强了各级部门的安全管理工作。

我们对这一时期的劳动保护安全技术工作叫做传统安全。传统安全虽然为防止伤亡事故作出了重大贡献，但也存在不少缺点，其中最主要的就是落后于生产的发展，也就是说事故预防工作总跟不上技术的进步。为什么会产生这种情况呢？主要原因在于：

1、安全的属性问题。由于安全是依附于生产而存在的，生产中如果不发生事故，则往往使人麻痹，看不到安全工作的作用，觉得讲不讲安全也没有什么了不起，不仅企业领导人甚至工人本身也不重视安全。

2、由于工业技术处于发展阶段，还不成熟，生产中许多潜在性的危险因素还认识不清。

3、安全产生的经济效益是间接的，看不见、摸不着，只有发生事故后产生了负效益后才感觉出它的存在。这就减少了人们深入进行研究的兴趣。

当然还可能有其它的原因。

传统安全的弱点很难解决上述问题，主要由于它本身存在着弱点：

一是凭经验和直感处理生产系统中的安全问题多，由表及里的深入分析、发现潜在的事

故危险性少，难于彻底改善安全面貌。

二是定性的，即“安全”或“不安全”的概念多，而定量的概念少。如生产系统究竟有多大的安全性？事故发生的频率有大？可能的严重程度有多大？都无法回答，难以给人以实质性的概念。

三是片断地、零碎地解决安全问题大，头痛医头，脚痛医脚，而系统地、全面地解决问题少。

四是没有肯定的目标值。生产任务有目标、有奋斗的方向，而安全问题没有目标值，究竟作到什么程度才算安全问题解决得好，才能不发生重大事故，心中无数。

总之，传统安全技术越来越不适应于生产的发展，有必要进行改革，很多人已经意识到这个问题的严重性了。

我国在解放以前，由于三座大山的压迫，加以工业技术的落后，根本无劳动保护安全技术工作可言。只是在解放后才真正开始这项工作。1952年国家召开了第一次全国劳动保护会议，提出了“安全为了生产、生产必须安全”的指导方针，相继制订了三大规程和劳动保护有关法令，健全了机构，加强了工作，使我国的安全生产面貌随着生产的发展而不断改善，三十多年来取得了巨大的成绩。但是我国也和世界上其他国家一样，存在着传统安全工作不能适应四化要求的问题。

多少年来，安全工作者总想找到一个办法，能够事先预测到发生事故的可能性，掌握事故发生的规律，作出定性和定量的评价，以便能在设计、施工、运行、管理中向有关人员预先警告事故的危险性，并且能够根据评价结果，提出相应的安全措施。为了达到这个目的，安全系统工程学便应运而生了。

什么是安全系统工程？安全系统工程是采用系统工程方法，分析、评价并控制系统中的事故，调整工艺设备、操作、管理、生产周期和费用投资等因素，使系统发生的事故减少到最低限度并达到最佳安全状态。

为什么要采用系统工程的方法来研究和处理安全问题呢？我们说，世界上任何事物都可以说是由系统构成的，它有一定的目标。而系统又由若干子系统所构成。子系统之间存在着有机联系，互相依赖也互相制约，一旦失调便会影响系统目标的完成。钱学森同志曾举一个工厂的例子说明系统和子系统之间的关系。他指出，就一个工厂系统而言，就是人和物——包括三个子系统，即物资（能源、原料、半成品、成品）、设备（土木建筑、机电设备、工具仪表等）和资金（工资、流动资金等），以及事——包括两个子系统，即任务指标（上级下达的任务或与其他单位订的合同）与信息（数据、图纸、报表、规章、决策等）。由此可见系统及其子系统相互间的概貌。而系统工程方法就是为了更好地完成系统目的，对子系统按照既定顺序进行分析、评价和优化。安全工作中采用了系统工程方法，首先就可以充分地，不遗漏地揭示出系统中的危险性，然后就可以对系统中危险性大的薄弱环节加以补强，对不协调的部份加以调整，因此，就有可能消除事故的根源，并使安全状态达到最佳化。

1.1 安全系统工程的发展历史

1957年苏联发射了第一颗地球人造卫星之后，美国为了赶上空间优势，匆忙地进行导弹技术的开发，实行所谓研究、设计、施工齐头并进的方法，由于对系统的可靠性和安全性研究不足，在一年半的时间内连续发生了四次重大事故，每一次都造成了数以百万计美元的损

失，最后不得不全部报废，从头作起。后来，美国空军以系统工程的方法研究导弹系统的可靠性和安全性，于1962年第一次提出了“弹道火箭安全系统工程学”，继而制订了“武器系统安全标准”。这对后来发展多弹头火箭的成功创造了条件。1966年美国国防部采用了空军的安全标准，制订了MIL—S—38130，1969年7月发表了安全系统工程程序标准MIL—STD—882，在这项标准中，首次奠定了系统安全工程的概念，以及设计、分析、综合等基本原则，该标准于1969年和1977年进行了两次修订。

1965年美国波音公司和华盛顿大学在西雅图召开了安全系统工程的专门学术讨论会议，以波音公司为中心对航空工业开展了安全性、可靠性的分析和设计的研究，用在导弹和超音速飞机的安全性评价方面，取得了很好的效果。但是这个新生事物在初创时期，并不能为所有的人所接受，美国航空航天局就不够重视这个方法，以致造成了1967年发生的阿波罗宇航员三人被烧死的事件，受到一次惨痛的教训。

另一方面，英国以原子能公司为中心，从六十年代中叶开始收集有关原子能电站故障的数据，对于系统的安全性和可靠性问题，采用了概率论的评价方法。后来进一步推动了定量评价的工作，设立了系统可靠性服务所和可靠性数据库。它们的任务是收集原子能电站的设备和装置的数据，提供给有关单位。

1974年美国原子能委员会发表了原子能电站风险评价有关报告，这项报告是该委员会委托麻省理工学院的拉氏姆逊教授组织了十几个人，用了两年时间花了三百万美元完成的，叫作“拉氏报告”，在报告中收集了原子电站各个部位历年发生的故障及其概效，采用了事件树和事故树的分析方法，作出了原子电站的安全性评价。这个报告发表后，引起了世界各国同行的关注。

日本引进安全系统工程的方法虽为时稍晚，但发展很快。自从1971年科技联盟召开了“可靠性安全性学术讨论会以来，十余年来在电子、宇航、航空、铁路，汽车、原子能，化工、冶金等领域，研究工作十分活跃。日本劳动省于1976年公布了化工联合企业六阶段安全评价方法，就是使用的安全系统工程方法。

当前，安全系统工程已普遍引起各国的重视，国际安全系统工程学会每两年举办一次年会，1983年举办的第六次会议在美国休斯敦召开，参加国有40余个，从讨论议题涉及面的广泛，可以看出这门学科越来越引起人们的兴趣了。

我国从1982年开始在研究单位进行这门学科的介绍和研究，随即在一些工业部门所属企业进行推广试点。两年多来，已经收到了一定的效果。

1·2 安全系统工程的内容

安全系统工程主要包括三个方面：

第一是系统安全分析，系统安全分析在安全系统工程中占有十分重要的地位。为了充分认识系统中存在的危险性，那么就要对系统进行细致的分析。只有分析得准确，才能在安全评价中得到正确的答案。可以根据需要把分析进行到不同的深度，可以是初步的或详细的，定性的或定量的，每种深度都可得出相应的答案，能满足不同项目、不同情况的要求。

每一种系统安全分析方法，都有自己产生的历史和环境条件，所以并不能处处通用。要完成一个准确的分析就要综合使用各种分析方法，取长补短，有时还要互相比较，看看那些方法和实际情况更相吻合，因此就要求人们熟知各种方法的内容和长处，用起来才能得心应

手

当前已经提出的系统安全分析方法有数十种之多，是各种不同的角度对系统的安全性进行分析。当然其中不少方法是雷同或重复的。这也说明安全系统工程是一门新学科，正处在蓬勃发展的阶段，很多分析方法还没有定型的模版。

通过实践，一般认为定性的系统安全分析方法如安全检查表法（又名系统检查法），即能定性又能定量的故障类型和影响分析法、事故树分析法较为实用。我国由于起步较晚，近两年来在企业推行安全检查表法和事故树定性分析法，取得了一定的效果。

其次是安全评价，系统安全分析的目的就是为了进行安全评价。通过分析了解了系统中存在的潜在危险性和薄弱环节所在，发生事故的概率和可能的严重程度等，这些都是评价的依据。

定性分析的结果只能用作定性评价，也就是说能够知道系统中危险性的大致情况，例如数量多少和严重程度等。但这已比用传统安全方法系统和准确得多了。只有经过定量的评价才能充分发挥安全系统工程的作用。决策者可以根据评价的结果选择技术路线，保险公司可以根据企业不同的安全性规定不同的保险金额，领导和监察机关可以根据评价结果督促企业改善安全状况。

当前有两个重要的安全评价方法，其一就是对系统的可靠性、安全性进行评价，其二就是利用生产所需原料，所谓物质系数法进行评价。

第三就是采取相应的安全措施，根据评价的结果，可以对系统进行调整，对薄弱环节加以修正或加强。安全措施主要可采取预防事故的发生或控制事故损失的扩展两种方法。前者是在事故发生之前，尽可能抑制事故的发生，后者是在事故已经发生了，尽量使事故损失控制在最低限度。

1．3　安全系统工程在工业安全中的应用

从安全系统工程的发展可以看出，最初是从研究产品的可靠性和安全性开始的。军事装备产品有对可靠性、安全性的要求十分严格，否则不仅完不成武器的设计，而且制造过程中的某一环节也不安全。后来这种方法发展到对生产系统各个环节的安全分析，环节的内容除了包括原料，设备因素等物的因素之外，还包括了人的因素和环境因素。这就使安全系统工程的方法在工业安全（指传统的安全工作）领域中得到实际的应用。这个过程大致经历了四个阶段：

（1）工业安全和系统安全分工合作的时期。安全系统工程发展的初期阶段，工业安全工作者和产品系统安全工作者的分工是明确的，前者负责工人的安全，后者负责产品安全，两者分工合作共同完成生产任务。如果工业安全工作做得不好，发生了事故，不仅工人受到伤害，而且设备以及制造中的产品也会受到损害。又如工作环境不良，就有可能造成零部件的缺陷和质量问题，这些都能影响系统安全计划的完成。另一方面，如果零部件或产品的安全不良，制造过程中发生事故的危险性很高，也不能保证工人的安全，所以二者有极为密切的关系。

（2）工业安全引进了系统安全分析的方法。安全系统工程发展后不久，工业安全就把它的工作方法特别是系统安全分析的方法吸收了进来，由于系统安全分析是对系统各个环节根据基本事件的特点和环境条件进行安全性的定性定量分析，作出客观的评价。基础此可以

采取针对性的安全措施，这种方法对安全工作十分有用，自然就产生了上述情况。

（3）安全管理也引用了安全系统工程方法。

由于安全系统工程不仅可以评价系统的各个环节的可靠性和安全性问题，而且对系统开发的各个阶段，如计划编制、研究开发、加工制造、操作使用等都需要进行评价，取得最优效果，这些手段也完全适用于企业的安全管理，如新装置的投产或已有装置的检查、操作、维修、教育、训练等阶段，都可以使用这种方法提高系统性和准确性。

（4）在工业安全工作中广泛使用安全系统工程方法，这是传统安全工作进行改革的趋势，正从实践中不断总结出经验。

1.4 安全系统工程的优越性

综上所述，可以明显地看出在工业安全领域里引进安全系统工程的方法是有很多优越性的。它可以使安全工作从过去的凭直观、经验的传统方法改革成定性定量的方法。大致有下述各项优点：

（1）通过分析，了解系统的薄弱环节所在及危险可能导致事故的条件，可以从定量概念预测事故发生的可能性，从而可以采取相应的措施，预防事故的发生。不仅如此，通过分析，不但易于找到真正的事故原因，而且还能查到未想到的原因。

（2）通过评价和优化技术，可以找出最适当的方法使各分系统之间达到最佳配合，用最少的投资达到最佳的安全效果和大幅度地减少伤亡事故的目的。

（3）安全系统工程的方法，不仅适用于工程，而且适用于管理。实际上现在已形成安全系统工程和安全系统管理两个分支。其应用范畴可以归纳为五个方面，即 ① 发现事故隐患，② 预测由故障引起的危险，③ 设计和调整安全措施方案，④ 实现最优化的安全措施，⑤ 不断进行改善。

（4）可以促进各项标准的制订和有关可靠性数据的收集。安全系统工程既然需要评价就需要各种标准和数据。如允许安全值，故障率数据以及安全设计标准、人机工程标准等。

（5）可以迅速地提高安全工作人员的水平，真正搞好安全系统工程，必须熟悉生产，学会各种分析和评价方法，这对提高安全工作人员的质量是大有好处的。

当然，最大的优越性是减少事故，这在很多国家已用行动证明了这一点。

第二章　安全系统工程分析方法

近年来由于安全系统工程学科的发展，出现了很多分析方法，都带有各自的特点，这也说明这门学科正处于蓬勃发展的阶段。

不少方法有相似的地方，也有不同之处，很难说哪一个方法比另一个方法好，只能作为相互补充或相互比较。用一种方法也许不能表明所有的危险性，而增加另一种方法却能揭示它们。这个特点也是安全系统工程的一个特点，并且促进了这门学科的迅速发展。

作为安全系统工程工作者，应该了解各种分析方法的概貌，其中有些方法应该掌握熟练并能灵活应用。目前，见诸有关文献的分析方法多达数十种，有25种方法较为常见。本章就章此作一简明介绍。

应该说明，进行一项安全系统工程分析，并不是要全部使用这些方法，也不是说多用一种方法就会使分析结果更精确、更有效一些。其目的就是为了在特定的环境和资源条件下，分析得准确，能够更好地消除或控制危险性。

为了便于选用，各种分析方法均按下列一定次序编写：

方法　简要说明方法的内容

应用　说明使用方法的系统、子系统和元件的范围，说明适用的处理过程、生产活动和操作步骤，也说明在那些情况下不适用。

完善程度　根据某些方法的特性，有些可作广泛的、快速的表面情况分析，有些则适于详细的、深入的分析。有的可进行定性，有的不仅能够定性而且能够定量。不同的分析方法可以达到不同的完善程度。

训练要求　有些方法未经训练的生手也能使用，有些则要通过正式的学习和实践经验，本条也说明了使用分析方法应作的准备工作。

应用难点　通过训练和实际分析，必然会产生结果。有时取得结果相对来说比较容易有的则费时费力。使用者知道这一点，选用时便会有所取舍。

讨论　介绍使用者对方法的一些评论，并提出一些应该注意的事项。

2、1分析方法之间关系比较密切的

1、子系统危险性分析（Suhsystem Hazard Analysis）

方法　对一个系统所包括的子系统、组件和元件进行分析，使用的分析方法可以选用多种方法，但分析内容不能超过子系统，也就是说分析的范围不超过子系统。

应用　只能用于子系统，例如具有单独功能的元件或元件组合。除了这条限制之外，其用除甚为广泛。

完善要求　根据选用的分析方法和分析深度而定。

训练要求　根据所选用的分析方法而定。

应用难点　根据所选用的分析方法的难度而定。

讨论　本方法并非独立的分析方法，而是在系统水平下，采用任何一种或多种分析方法的一项综合性技术。由于对安全系统工程分析的要求，为了说清问题，所以把这种综合性的技术也作为分析方法的一项，并且得到人们承认。象这样的分析方法以后还有。

2、单点故障分析（Single—Point Failure Analysis）

方法　对系统中的每一个元件进行分析研究，察明能够造成系统故障的单个元件或元件与元件的交接面故障。

应用　在硬件系统、软件系统和人的操作中都能使用。

完善程度　简单的元件或交接面用观察的方法就可以找出单点故障的所在，但系统复杂了以后，就不太容易用观察法解决问题了。用这种方法作为其他分析方法的辅助方法时，则要看其他方法的深度而定。

训练要求　有经验的设计者和工程师能够很快地掌握这种方法。作为辅助方法时，则要求对其他方法熟练掌握。

应用难点　系统复杂以后观察就有困难，作为辅助方法又需掌握为主的分析方法。

讨论　这种分析方法是事故树分析中决定最小割集时的必要手段，在事件树和故障类

型影响分析中也要求使用单点故障分析，所以说它是一个基础性的分析方法。

3、意外事故分析（Contingency Analysis）

方法　找出系统中最容易发生的偶然事故，研究紧急措施和防护设备，以便能控制事故，并避免人员和财物的损失。

应用　广泛用于系统、子系统、元件、交接面等处。使用时必须研究意外事故的发生特性和时机。一般应用中，这个方法对于哪些地方应配置备件（冗长设计），哪些地方应着重注意，以减少故障，是十分有用的。另外制订防止事故计划和评价设备的安全性时，也可用本方法。

完善程度　对意外事故是否能够充分地辩识出来是很重要的，如果疏忽了某些可能发生的意外事故，就会造成不良后果。同时所采用的辅助分析技术也很重要。

训练要求　应该熟悉系统以至元件在系统中的作用，它们发生故障后会产生什么样的后果。

应用难点　根据所选用的分析技术而定。

讨论　这个方法不是一个独立的分析技术，要根据事故的偶发特性，根据需要和可能，有针对性地选用一个或一组分析方法。

4、系统危险性分析（System Hazard Analysis）

本方法和交接面分析没有明显的区别，所有内容可见第5个分析方法。

5、交接面分析（Interface Analysis）

方法　在一个系统中，找出各个单元之间的交接面，交叉部位的各种配合不适当或不相容的情况，分析它们在各种操作条件下会产生哪些危险性，并会造成哪些事故。

应用　本法用途十分广泛，从最简单的元件直到组件和子系统都能使用。例如，交接面可以指机械内部、机械之间或人机之时，分析范围不受什么限制。

完善程度　根据已知的或预期的各种交接面是否都已辩识清楚，它们之间有哪些不适当或不相容的地方，这些情况的掌握的程度决定了使用本方法的完善程度。如果再使用一些辅助的分析技术会增加本法的完善程度。

训练要求　要熟悉各个交接面的特性，也要熟悉采用的辅助分析方法。

应用难点　根据系统的复杂性和所用的辅助技术而定。

讨论　使用辅助分析方法对完成交接面分析有很大的好处，例如用故障类型影响分析来进行交叉部位的交接面分析就能够辩识单由交接面分析发现不了的不相容性。

这个方法的主要缺点就是难于找全所有的交接面，特别是交接面之间的元件不相容性。

6、致命度分析（Criticality Analysis）

方法　系统元件发生故障后会造成多么严重的伤害，按其严重程度订出一定的等级。

应用　用于各类系统，工艺过程，操作程序和系统中的元件。

完善程度　从每一个发生故障的元件能够得出一个潜在危险性的严重等级，这是本法的特点。辩识故障要使用辅助分析技术，例如使用故障类型影响分析。因此本法的完善程度和所用的辅助方法有关。

训练要求　将故障可能造成的严重后果按等级编排起来，填入规定的表格中，使用起来甚为方便

应用难点　　如果故障类型已经清楚并很容易使用，关键是预先辨识系统元件的故障类型。因此本法需要辅助分析技术，如故障类型影响分析等。

讨论　　本法常和故障类型影响分析合用。

7、危险性预先分析（Preliminary Hazard Analysis）

方法　　非常广泛使用的方法。一般用在系统设计的开始阶段，最好是在形成设计观点的时候。当然在系统运转周期的其他阶段，如改造后开车，制订操作规程，技术改造之后，使用新工艺等情况，都可以采用这种方法。

这种方法，首先要把明显的或潜在的危险性查找清楚，再研究控制这些危险性的可行性以及控制措施，常用安全检查表帮助分析。

应用　　如前所述这种方法都是在各种行动的最初阶段使用，所以叫作危险性预先分析，它对于决策人选用技术路线时特别有帮助。

完善程度　　依赖于分析者的经验多少和分析深度而定。

应用难点　　根据分析的深度而定。

讨论　　本法并非一个独立的分析方法，而是使用一种或多种分析技术的综合性方法，只是在使用时间上有其特殊性，即在运转周期之前选用。

2.2 **分析方法有许多共同点的**

（1）**程序分析**（Procedure Analysis）

方法　　检查每一步操作程序，包括完成任务的项目，所用的设备和人所处的环境等因素，找出由于操作造成的事故概率，例如系统对操作人员造成伤害的概率及操作人员对系统造成损害的概率。

应用　　只限于有人员操作的系统，其操作程序必须有充分的资料或者已经正规化，并能保证用逐项的检查法不致漏检项目。除此之外，最好还用交叉检查的方法防止检查结果漏项。

完善程度　　根据程序步骤和各个元件的研究深度以及失误被选择出来的程度而定。例如遗忘了程序的阶段、省略了程序中的步骤、插入了错误程序等情况。

训练要求　　熟练人员也要先进行单元分析。程序越复杂越会发生错误。因而需要学习正规的技术并经过训练，取得经验后才能适应这类复杂性。

应用难点　　如果操作程序很少发生失误，用这种方法十分容易。如果程序中可能发生多重失误，或者发生多处单点故障，或者在分离操作时还要考虑其综合情况，这时用起本法来困难就大了。

（2）**作业安全分析**（Job safety Analysis）

方法　　对各种工作，包括工作过程、系统操作等一个单元一个单元地进行分析，辨识每一个单元带来的危险性。经常由工人、工长和一个工程师组成一个组来完成此项任务。

应用　　只限于有人操作的情况，操作应该已经正规化并不会有突出的变化。如果预料到有改变时，应该事先考虑。

完善程度　　根据各单元的研究深度和规定程序的变化程度决定。

训练要求　　熟练人员可立即进行工作。对复杂的工作或有许多因素有变化时，则要学习正规的分析方法，以适应其复杂性。

应用难点　如果是个人操作而且很少变化的工作，用起来很容易。如果变化很多而且必须加以考虑时，用起来就比较困难了。如果有变化但不加考虑，则分析方法的完善程度将会受到影响。

讨论　有人员操作的系统用本法辨识危险性很有用，也可在工业安全中使用此法进行系统安全分析

（3）操作和后勤危险性分析（Operating Support Hazard Analysis）和程序分析全同

（4）流动分析（Flow Analysis）

方法　研究流体或能量的流动情况，由一个元件、子系统或系统流向另一个元件、子系统或系统，查出哪些是不希望的流动。不希望的流动系指能造成受伤或财物损失的流动。

应用　用在传送和控制流体及能量的系统中，有时还需要辅助的技术方法，例如不希望的流动模型和发生概率。

完善程度　把系统中的流体及流量和能量列成表。如果流动是正常的，列表时不易发生漏项。如果流动不正常或者还有一些多因素的综合性影响，则发生的漏项可能性会很大。

训练要求　为了列表，需要作准备工作，对于不正常的流动也要找出原因和防止措施，还要掌握辅助的技术方法。

应用难点　把流动列表比较容易，找出防护措施也不难。一般可以按照法令、规范和标准的要求与系统特性相比较。如果还要求能控制不希望的流动，则要困难得多。这种控制无论是手动的或自动的，都不能用本法直接分析，必需使用辅助技术。

讨论　本法多用于分析系统内部的流体和能量流动。系统外部的流动影响，例如来自邻近系统或自然环境　则经常不预考虑。

（5）能量分析（Energy Analysis）

方法　找出系统中使用的全部能源，考察会造成伤害的不希望的能量流动，研究防护它们的措施。

应用　本法适用于使用或贮存任何形式能量的系统，或者系统本身就具备一定能量。（例如机械能、位能、电能、离子辐射能、化学能、热能等），配合其他方法，也可用于控制能量的使用、贮存或传送。应用这种方法应注意与能量无关的危险性，例如密闭空间的氮气不足，或缺氧造成的窒息等，都与能量无关，但十分危险。

完善程度　列出系统中的能量项目，可以使用检查表辅助查找，一般不会漏项。如果能量来自系统外部，则有漏项的可能。另外还应注意能量利用率、周期和频率，如振动和疲劳负荷以及各种能量的综合影响，如容器壁受到的瞬时压力和温度差的影响等。

训练要求　了解能量的存在和转变，以便列出能量项目。另外还要熟悉不希望能量流动的防护措施知识

应用难点　列出能量项目比较容易，一般按照有关法令、规范、规程和标准的要求对系统的特性进行简单比较就可找出适当的防护措施。这项工作在系统开始设计时就应进行，并应整理出资料。

讨论　查找系统中存在的危险性，首先可使用本法，通过初步观察，就容易发现能量可能存在的危险性。但系统外部来的能量往往被忽视。作出“安全入内”的决定时，要考虑

环境情况，虽然环境和不希望能量的散逸无关，但环境和生命关系密切，象上面说的窒息事故，因此必须对这类情况作出特别的预防措施。

2．3根据逻辑方进行分析

（1）事件树分析（Event—Tree Analysis）

方法　选出希望或不希望的事件作为开始事件，按照逻辑推理推论其发展结果。发展趋势只有两种可能性，即失败或成功。把每一个结果都作为新的起始事件，不断交互推论下去，直到找出事件的发展所有可能的结果。

应用　广泛应用于各种系统，能够分析出事件发展的各种可能结果。

完善程度　可为分析得很完全，能够作到所有事件都能进行分析，而且通过分析都能看出结果。

训练要求　方法较难。须经几天到几星期的学习，还要结合实践经验，否则就难在复杂的系统中得到顺利应用。

应用难点　受过训练后用起来并不太困难，但很费时间。不过使用了事件树分析以后研究了所有希望的和不希望的事件，将来再应用事故树分析或故障类型影响分析等方法时，更能取得实际效果。

讨论　在以逻辑理论为基础的分析方法中，不管是逻辑分析、事件树分析，还是未加防护的人的分析，都能进行得很彻底，但是需要大量的资料和时间，因此只有在风险高或隐患深的系统中才使用这种方法。例如用简单分析方法不能胜任时）。

（2）管理监督和风险树分析（Management Oversight and Risk—Tree Analysis）

方法　先画一个预先设计好的和系统化了的逻辑树，概括系统中的全部风险，这类风险是在设备、工艺、操作和管理中存在的。

应用　事先设计好的树可以列出安全问题的各个方面，所以它是一个比较有用的工具，在各种系统和工艺过程中，用树与实际情况对照检查，可为发现薄弱环节或由环境造成的事故原因，这种方法有广泛的应用。

完善程度　由于事先设计好了树的模型，使用时逐项对照，所以可以分析得比较彻底，被研究对象的分析深度影响分析的完善程度。

训练要求　通过一天的正式讲解，并进行一星期的反复实践就可学会。

应用难点　这个方法耗费时间而且枯燥乏味，但经过训练，使用并不困难，利用图形说明更易于了解。

讨论　研究事故和异常现象时使用这个方法，已经逐步普及并引起了人们的重视。

（3）故障类型和影响分析（Faiiuic Modes and Effects Analysis）

方法　对系统中的元件进行逐个研究，查明每一个元件的故障类型，每一个元件可能有一个或一个以上的故障类型，然后再进一步查明每个故障类型对子系统及系统的影响。类型可以单一起作用也可以组合起作用。

应用　本法广泛用于系统、子系统、组件、程序、交接面等分析中。分析时要用一定的表格排列各种故障类型，并需准备足够的资料。

完善程度　这种分析方法的完善程度取决于下述条件①故障类型能否不遗漏地查找清

楚，②每一个故障类型能够造成的影响是否清楚。③故障类型存在的组合情况。

训练要求　查找故障类型对于复杂系统较为复杂，因此需要几天到几星期的训练和实际工作，另外还要知道一些布尔代数的知识。

应用难点　经过训练掌握此项技术并不困难，但很费力耗时。它只需要对故障类型推论其影响，不象事件树分析那样，无论是否会造成伤害都要分析到底。

讨论　这个方法曾经风行一时，但逐渐已被耗时较少的事故树分析方法所代替。不过此法仍有其特定的用途，例如分析重要的机器时，如飞机发动机等，仍用这个方法。在系统可靠性设计时，这是很效的方法。

（4）网络逻辑分析（Network Logic Analysis）

方法　将系统操作和元件绘成逻辑网络图，并用布尔代数式表示系统功能，对网络加以分析，找出哪个系统元件易于导致事故。

应用　本法广泛用于所有人工或非人工控制系统，所有元件和操作都能以二值表示时就能用。

完善程度　本法分析程度较为彻底，主要看所画的网络是否能完全代表系统的元件和操作。但外围设备的故障，例如公用工程以及交接面的影响，在本法中常被忽视。

训练要求　较难使用，特别需要布尔代数的知识，不经过几天到几个星期的学习和实际进行操作，就很难完成复杂系统的分析工作。

应用难点　一旦通过必要的训练，这个方法使用起来并不太难。由于要涉及系统中所有可能发生的偶然事件，所以比故障类型影响分析和事故树分析用起来要难些。

讨论　网络逻辑分析、事件树分析和未加防护的人的分析都是适用于彻底分析的方法。但要消耗大量时间和资料，因而只在风险高和隐患大的情况下使用。

（5）事故树分析（Fault Tree Analysis）

方法　找出不希望事件（顶上事件）的所有基本原因事件，把它们通过逻辑推理方式用逻辑门（与门、或门等）连接起来。这样能清楚地表示出哪些原因事件及其组合发展成为顶上事件的动态过程。

应用　广泛用于安全系统分析，但要求两个先决条件（1）顶上事件要设定得正确，同时能分析到真正的原因事件。（2）各个顶上事件应独立进行分析。

完善程度　可进行定性也可进行定量。分析结果的好坏要看逻辑推理的完善与否，对基本原因事件的理解深度。在定量方面，则要看所用原因事件发生概率的精确程度。

训练要求　初学者要经过40小时或更多一些时间的学习和实习。事先学一点布尔代数和逻辑门的使用是有好处的。

应用难点　虽然耗费时间，但经过训练后用起来并不太困难。近来使用计算机的情况已逐渐增多。这个方法和事件树及故障类型影响分析不同，它只需要分析导致事故的故障条件和原因条件，不需要对全部故障都作分析。

讨论　本法虽然能够计算出顶上事件发生的概率，但容易产生一个偏向，即千方百计地追求概率数字。但原因事件的故障率和人的失误率估计置信度不高，因而消耗大量时间而收效不大。

但是，用事故树分析，可以找出导致事故的基本事件的最小组合，即最小割集。有几个最小