第一章 概 论

安全系统工程，是以安全学和系统科学为理论基础，以安全工程、系统工程、可靠性工程等为手段，对系统风险进行分析、评价、控制，以期实现系统及其全过程安全目标的科学技术。

安全系统工程是现代科技发展的必然产物，是安全科学学科的重要分支。

第一节 基 本 概 念

安全系统工程是一门涉及自然科学和社会科学的横断科学，在定义安全系统工程之前需要弄清相关学科的有关概念。

一、系统、系统工程

系统工程的研究对象是系统。系统就是由相互作用和相互依赖的若干组成部分结合成的具有特定功能的有机整体。系统有自然系统与人造系统、封闭系统与开放系统、静态系统与动态系统、实体系统与概念系统、宏观系统与微观系统、软件系统与硬件系统之分。不管系统如何划分，凡是能称其为系统的，都具有如下特性：

（1）整体性。系统是由两个或两个以上相互区别的要素（元件或子系统）组成的整体。构成系统的各要素虽然具有不同的性能，但它们通过综合、统一（而不是简单拼凑）形成的整体就具备了新的特定功能，就是说，系统作为一个整体才能发挥其应有功能。所以，系统的观点是一种整体的观点，一种综合的思想方法。

（2）相关性。构成系统的各要素之间、要素与子系统之间、系统与环境之间都存在着相互联系、相互依赖、相互作用的特殊关系，通过这些关系，使系统有机地联系在一起，发挥其特定功能。

（3）目的性。任何系统都是为完成某种任务或实现某种目的而发挥其特定功能的。要达到系统的既定目的，就必须赋予系统规定的功能，这就需要在系统的整个生命周期，即系统的规划、设计、试验、制造和使用等阶段，对系统采取最优规划、最优设计、最优控制、最优管理等优化措施。

（4）有序性。系统有序性主要表现在系统空间结构的层次性和系统发展的时间顺序性。系统可分成若干子系统和更小的子系统，而该系统又是其所属系统的子系统。这种系统的分割形式表现为系统空间结构的层次性。另外，系统的生命过程也是有序的，它总是要经历孕育、诞生、发展、成熟、衰老、消亡的过程，这一过程表现为系统发展的有序性。系统的分析、评价、管理都应考虑系统的有序性。

（5）环境适应性。系统是由许多特定部分组成的有机集合体，而这个集合体以外的部分就是系统的环境。系统从环境中获取必要的物质、能量和信息，经过系统的加工、处理和转化，产生新的物质、能量和信息，然后再提供给环境。另一方面，环境也会对系统产

生干扰或限制，即约束条件。环境特性的变化往往能够引起系统特性的变化，系统要实现预定的目标或功能，必须能够适应外部环境的变化。研究系统时，必须重视环境对系统的影响。

系统工程是组织管理系统的规划、设计、制造、试验和使用的科学方法，是一种对所有系统都具有普遍意义的科学方法。这个定义表示：①系统工程属工程技术范畴，主要是组织管理各类工程的方法论，即组织管理工程；②系统工程是解决系统整体及其全过程优化问题的工程技术；③系统工程对所有系统都具有普遍适用性。

系统工程是 20 世纪 50 年代发展起来的一门新兴科学，它是以系统为研究对象，以现代科学技术为研究手段，以系统最佳化为研究目标的科学技术。它是发展很快、应用很广的一门管理科学，它的广泛应用为管理学的发展，为各行各业、各个领域管理现代化提供了基本理论和方法。

关于系统工程所属各子学科的命名问题，钱学森教授指出：“正如工程技术各有专业一样，系统工程也还是一个总类名称，因体系性质不同，还可以再分为门类，如工程体系的系统工程叫工程系统工程，生产企业或企业体系的系统工程叫经济系统工程，……”。这种命名原则为系统工程在各专门领域的发展提供了条件，从而免去一些关于名词术语叫法的不必要之争。

二、可靠性、可靠度、可靠性工程

可靠性是指系统在规定的条件下和规定的时间内完成规定功能的能力。这里，规定的条件都是设计规定的，规定的功能也是设计赋予的。

可靠度是衡量系统可靠性的标准，它是指系统在规定的时间内完成规定功能的概率。相反，系统在规定的条件下和规定的时间内不能完成规定功能的概率就是系统的不可靠度。

可靠性工程就是研究系统可靠性的工程技术。可靠性工程要解决的是如何提高系统可靠度，使系统在其寿命周期内正常运行，圆满完成其规定功能的问题。

就系统规定功能而言，系统整体功能除了应具备加工产品、提供服务等功能外，还必须有保障人员、设备、财产、环境不受损害的安全功能。系统可靠性与系统安全性是两个既有区别又有联系的功能，与它们相对立的是分支学科或分支系统。

三、安全系统与安全系统工程

1. 对安全的理解和认识

安全一词是人们经过抽象思维确定的一个概念或理念。目前所见到的文献对安全这个概念的诠释普遍存在两个问题：一个是缺乏科学的严密性；二是安全一词太大众化了，以致不管人们如何下定义，都很难包容一般意义上的安全理念的内涵。

安全描述的是一种客观存在的状态吗？回答并非是肯定的。因为对安全状态的描述的主要特征量是什么，在安全科学界尚难统一。有人说无事故、无隐患的状态就是安全状态；从动力学原理出发，也有人提出用系统从无序到有序，渐变与突变的统一，非畸变来描述安全动态。这样的表述虽是有一定的科学性，但由于安全因素的高度复杂性和极强的时间依赖性，上述方法所表述的安全状态必然有很大的局限性，可能与实际相差甚远，也可能带有很大的理想化色彩。但又与人们想象中的“平安无事”可能根本不是一回事。因为人

们有时说的安全、平安不过是代表一种企盼，因此是一种理想化的抽象的概念。

如果承认安全一词描述的是一种状态，但这种状态也决非是一种事故为零的所谓“绝对安全”的概念。从科学的角度讲，“绝对安全”的状态在客观上是不存在的。平安也好，安全也好，其本身就带有很大的模糊性、不确定性和相对性，所以“安全状态”具有动态特征，就是说安全所描述的状态具有动态特征，它是随时间而变化的。

安全的动态特征还体现在安全描述的不只是一个相对稳定的状态特征，安全一词还可作为对事故——安全过程的一种表征。过程表征和状态表征最本质的区别就在于前者描述的是事物的发展趋势，后者描述的是一种目标。从这个角度讲，安全一词表述的又可认为是动态过程。正如有的文章所表述的：渐变对应于灾害过程的孕育、维持，突变对应于灾害过程的启动和剧烈地扩展。但灾变不仅是灾害发生，也是系统由不稳定向新的稳定（安全）跃迁的触发器。

当然从技术的角度讲，已经提出并应用的安全失效率、安全度、安全系数等定量化的计算方法、标准及其表征的安全技术状态和安全与否的结论是科学和严密的。但这和通常讲的安全的概念相比显然要狭义得多。

状态、过程、理念、技术安全都是定义安全这个概念应该考虑的内涵。可见，人们试图通过一个简单的定义就想把安全如此丰富复杂的内涵表述清楚是一件非常困难的事情。

从科学原理出发，定义事物多采用两种办法，一种是从事物的组成考虑，一种是从事物的功能考虑，或两者兼顾。

安全表述的是一个复杂物质系统的动态过程或状态，过程或状态的目标是人物将不会受到伤害或损失。安全也可表述的是人们的一种理念，即人物将不会受到伤害和损失的理想状态。安全也可表述的是一种特定的技术状态，即满足一定安全技术指标要求的物态。

在讨论对安全一词的理解和认识之后，我们再来讨论一下安全的属性问题。安全一词所涉及的纷繁复杂因素与它的自然属性和社会属性有着密切的关系。

所谓安全的自然属性可以从两个方面来讨论：一是安全是人的生理与心理需要，或者说由生命及生的欲望决定了的自我保护意识，这是天生的，是安全存在的主动因素。二是人类对天灾的无奈以及新陈代谢、生老病死的规律不可抗拒，使人们不得不把生命安全经常提到议事日程，这虽然是被动因素，但它与前一个主动因素相结合，就决定安全是自古以来人类生活、生存、进步的永恒的主题。

安全的社会属性也可以从两方面来阐述：

(1) 自从人类有组织活动以来，社会安定、有序、进步始终是各社会阶段追求的目标，而这一目标实现的重要标志之一就是安全。这是社会促动安全的主动因素。但是人类的社会活动如政治、军事、文化、社交，有的对安全直接起破坏作用，有的间接影响着安全；人类的经济活动如生产（职业）、高技术灾害（化学品致灾、核事故隐患、电磁环境公害、航天事故、航空事故）、交通灾害则是自人类开展经济活动以来就存在的突出的安全问题，如今更加突出的一个安全问题是环境问题。环境恶化（包括自然环境和人为环境）是人类生活、生存安全的重要威胁。所以在 15 届世界职业安全卫生大会上，与会专家指出：向 21 世纪人们提出的挑战性问题是“环境、安全、健康问题”，即 Q.E.&OSH 是一个严重影响国民经济可持续发展的大问题。人类的社会活动、经济活动、交通和环境一方面本身在不断制造事故，另一方面也通过技术和管理措施不断消除隐患，减少事故。但由于受政治利益

和经济利益的驱使，安全技术管理措施多数是被动的。

（2）关于安全的社会属性也有人提出人伦智的观点。人伦是在一个人群（社会性的结合）中发生的。夫妇、父子、兄弟、朋友、同事构成人际关系，人际以诚相待，共谋生命的延续、生活的充实，并以此抵制惟利是图就称为人伦智。在资本主义社会，各个人际关系上的人伦智相当低微、暗弱。然而人伦智却是“职业灾害困局”中惟一的脱困希望之所寄，它的潜在能量是可以信赖的。人伦智也应属安全社会属性中的主动因素。

如果把安全的自然属性和社会属性合起来考虑，安全代表的是什么？它可能既是理念的，又是物质的；既是抽象的概念，又是客观的、有形的；既是当前的实实在在的事物，又可能是将来的一个可望又不可及的目标。

还可看出：安全的自然属性与社会属性中都存在着很强的促动安全的主动因素，这是安全科学发展的基础。

安全问题纷繁复杂的关系正是由于安全问题的自然属性与社会属性的交融，正像人是社会的一样，而社会的复杂性正是安全问题复杂的根本原因之一。

2. 安全系统及其特点

安全问题是一个复杂的系统工程问题。或者说解决安全问题要用系统工程的理论和方法。这种认识目前已经具有广泛的共识。但是说到“安全系统”则存在着歧义。其实“安全系统”这个定义能否成立，关键还在于它的特殊性和客观性。所谓特殊性就是指它与一般系统的区别。如前所述，其客观性的问题是不容置疑的，而其特殊性或个性可以归纳为如下若干方面。

（1）系统性。与安全有关的影响因素构成了安全系统。因为与安全有关的因素纷繁交错，所以安全系统是一个复杂的巨系统。很难找到一个因素数及其相关性如此复杂的能与之相比的系统。由于安全系统中各因素之间，以及因素与目标之间的关系多数有一定灰度，所以安全系统是灰色系统。

与一般系统不同，安全系统总是把环境因素看成是其系统的组分，其典型的因素及其关系可如图 1-1 所示。

依据安全问题所涉及范围大小不同，安全系统大小之差可能很悬殊。一般地讲，纯属技术领域的安全系统比如一台设备、器具，可能只涉及机和物；而对于一个车间甚至一个工厂，考虑安全问题的系统范围，则不只是机和物，肯定要把人—机—环境都扯进来。实际上，人—机—环境的提法是考虑了安全问题的空间跨度和时间跨度两个方面。如此说来，即便是一台设备，如果把它的制造安全与使用安全考虑进来，也仍然是人—机—环境的复杂系统。

安全系统的目标不是寻求最优解。这是因为安全系统目标的多元化，以及安全目标的极强相对性、时间依赖性与其理想化理念很难协调，所以安全系统的目标解是具有一定灰度的满意解或可接受解。

（2）开放性。安全系统是客观存在的。这是因为安全系统是建立在安全功能构件的物质基础之上。但同时安全系统总是寄生在客体（另一个系统）中。在处理方法上，如果把客体看成一个黑匣子，安全系统是通过客体的能量流、物流和信息流的流入—流出的非线性变化趋势，确认安全和事故发生的可能性，因此安全系统具有开放性特点。

开放性不仅是安全系统在动态中保持稳定存在的前提，也是安全系统复杂性及安全—

事故转换发生的重要机制。

（3）确定性与非确定性。.“确定性”是指制约系统演化的规则是确定性的，不含任何随机性因素。确定性的特征是演化方向及演化结果是确定的，可精确预测。“非确定性”或者具有演化方向和演化结果不确定，或者具有刻画事物运动特征的特征量不能客观精确地确定的特征。非确定性包括随机性和模糊性。

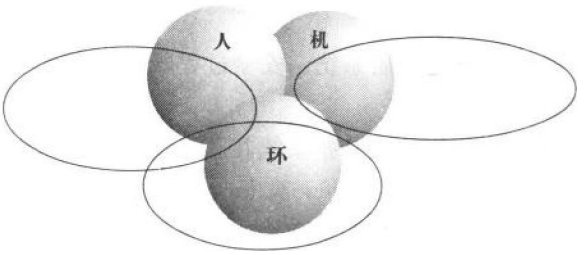

图1-1　安全系统典型的组成因素及其关系图

“随机性”可能有两个方面的来源：一是在不含任何外在的随机影响因素作用下，完全由“确定性”系统演化而产生的随机性（例如产生混沌），这种随机性称为本质随机性。二是系统还可能因其外在影响因素的随机作用而产生随机性行为，从而使系统在一定条件下表现出随机性的特征（外在随机性）。由于安全系统把环境看成是它的组分，所以对安全系统而言，本质随机性和外在随机性的区别不是绝对的。

“模糊性”是指事物的本身不清楚或衡量事物的尺度不清楚。对于安全系统，就是指系统的构成及其相互关系，以及组成与目标的关系不清楚。造成这些不清楚的可能来源在于主观和客观两个方面，即具有主观模糊性和客观模糊性。首先，刻画安全运行轨迹的以模糊数学方法建立的数学模型具有主观模糊性。因为数学模型常常不可能“严格地”确定安全系统各要素之间及其与目标之间完整的客观关系。当然，对于自然的技术因素之间的关系尚好一些。而对于社会的因素及其与技术因素的耦合关系将难于量化，因而也将难于建立准确的数学关系。应该强调的是，出现上述问题不完全是由于安全系统本身不清楚，它可能只是人们对安全系统主观模糊性的表现。

另外，对安全系统安全度的评价尺度以及构成安全度等级的评价指标体系也具有客观模糊性，即从事物的本质上无法给出其客观衡量尺度。

（4）安全系统是有序与无序的统一体。序主要反映事物的组成的规律和时域。依据序的性质，可分为有序、混沌序和无序。有序通常同稳定性、规则性相关联，主要表现为空间有序、时间有序和结构有序。无序通常与不稳定、无规则相关联。而混沌序则是不具备严格周期和对称性的有序态。现代复杂系统演化理论认为，复杂系统的演化中，不同性质的序之间可以相互转化。安全系统序的转化结果是否引发灾害或使灾害扩大，取决于序结构的类型及系统对特定序结构下的运动的（灾害意义上的）承受能力。

有序和无序，确定性和非确定性都会在系统演化过程中通过其空间结构、时间结构、功能结构和信息结构的改变体现出来。

（5）突变性或畸变性。安全系统过程的突变或畸变，或过程由连续到非连续变化在本质上还是服从于量变引起质变的哲理。

量变到质变的转化形式可以用畸变、突变或飞跃来描述，但也可通过渐变实现。所以安全系统的渐变也可能孕育着事故，而突变、畸变则肯定对应于灾害事故的启动，是致灾物质，或能量的突然释放。

综上所述，安全系统虽然与一般系统、非线性系统等有若干共同点，但安全系统的个性还是非常明显的，这是决定它客观存在并区别于其他系统的根本原因。

3. 安全的动力学特征

安全系统是物质系统。安全过程既可能是自组织的，也可能是被组织的，也可能是两者兼而有之。

所谓自组织的，是指系统在获得空间、时间或功能的结构过程中，没有外界的特定干预（所谓外界的特定干预，对安全来说主要是指社会属性中的被动因素）。它可能有两种发展形式：一种是非组织的向组织的有序发展过程，其本质是组织程度从相对较低到相对较高演化；另一种则是维持相同组织层次，但复杂性相对增长。前一种过程反映了安全系统组织层次跃升过程；后一种过程则标志着安全系统组织结构与功能从简单到复杂的组织水平的提高

对安全系统的自组织的演化过程主要是反映它的自然属性与社会属性共同作用的过程和结果。因为安全系统也是开放系统，它可以不断与外界交换物质、能量和信息，从而出现上述的两种发展形式，即从原有的混沌无序状态转变为一种在时间、空间或功能上的有序状态

一旦安全过程出现被组织的情况，如不可预见的天灾、人为诱发地震、战争、人为纵火、瞎指挥、违规操作等等，则会发生灾难或事故。

当然安全系统也是非线性系统，因而也具有非线性系统的共同特征。非线性是系统产生自组织行为的内因，没有这个内因，所谓开放性将不起作用．无序—有序的过程也就不会发生。

不少学者为了研究安全动力学而引进熵的概念。例如：引进“负熵流”以考虑安全系统与外界的物质能量和信息交换；引进“剩余熵”作为判断体系失稳与否的判据，虽然都有一定的局限性，但熵仍然是今后研究安全过程发展趋势的重要概念和方法因为熵的大小是状态自发实现的可能性的量度；同时从信息论的角度考虑，熵又是描写不肯定性大小的量．即熵愈大，不肯定性愈大，即：

$$H = -\sum P_i \log_2 P$$

式中 H——熵；

P_i——概率。

4. 安全系统工程

安全系统工程是采用系统工程的基本原理和方法，预先识别、分析系统存在的危险因素，评 价并控制系统风险，使系统安全性达到预期目标的工程技术。

对这个定义，可以从以下几个方面理解：

（1）安全系统工程的理论基础是安全科学和系统科学。它是工矿企业劳动安全卫生领域的系统工程。

（2）安全系统工程追求的是整个系统的安全和系统全过程的安全。

（3）安全系统工程的重点是系统危险因素的识别、分析，系统风险评价和系统安全决策与事故控制。

（4）安全系统工程要达到的预期安全目标将是系统风险控制在人们能够容忍的限度以

内，也就是在现有经济技术条件下，最经济、最有效地控制事故，使系统风险在安全指标以下。

第二节　安全系统工程的研究对象和研究内容

一、安全系统工程的研究对象

安全系统工程作为一门科学技术，有它本身的研究对象。任何一个生产系统都包括三个部分，即从事生产活动的操作人员和管理人员，生产必需的机器设备、厂房等物质条件，以及生产活动所处的环境。这三个部分构成一个“人一机一环境”系统，每一部分就是该系统的一个子系统，称为人子系统、机器子系统和环境子系统。

（1）人子系统：该子系统的安全与否涉及到人的生理和心理因素，以及规章制度、规程标准、管理手段、方法等是否适合人的特性，是否易于为人们所接受的问题。研究人子系统时，不仅把人当作“生物人”、“经纪人”，更要看作“社会人”，必须从社会学、人类学、心理学、行为科学角度分析问题、解决问题；不仅把人子系统看作系统固定不变的组成部分，更要看到人是一种自尊自爱、有感情、有思想、有主观能动性的人。

（2）机器子系统：对于该子系统，不仅要从工件的形状、大小、材料、强度、工艺、设备的可靠性等方面考虑其安全性，而且要考虑仪表、操作部件对人提出的要求，以及从人体测量学、生理学、心理与生理过程有关参数对仪表和操作部件的设计提出要求。

（3）环境子系统：对于该子系统，主要应考虑环境的理化因素和社会因素。理化因素主要有噪声、振动、粉尘、有毒气体、射线、光、温度、湿度、压力、热、化学有害物质等；社会因素有管理制度、工时定额、班组结构、人际关系等。

三个子系统相互影响、相互作用的结果就使系统总体安全性处于某种状态。例如，理化因素影响机器的寿命、精度甚至损坏机器；机器产生的噪声、振动、温度、尘毒又影响人和环境；人的心理状态、生理状况往往是引起误操作的主观因素；环境的社会因素又会影响人的心理状态，给安全带来潜在危险。这就是说，这三个相互联系、相互制约、相互影响的子系统构成了一个“人—机一环境”系统的有机整体。分析、评价、控制“人一机—环境”系统的安全性，只有从三个子系统内部及三个子系统之间的这些关系出发，才能真正解决系统的安全问题。安全系统工程的研究对象就是这种“人一机一环境”系统（以下简称‘系统’）。

二、安全系统工程的研究内容

安全系统工程是专门研究如何用系统工程的原理和方法确保实现系统安全功能的科学技术。其主要技术手段有系统安全分析、系统安全评价和安全决策与事故控制。

1. 系统安全分析

要提高系统的安全性，使其不发生或少发生事故，其前提条件就是预先发现系统可能存在的危险因素，全面掌握其基本特点，明确其对系统安全性影响的程度。只有这样，才有可能抓住系统可能存在的主要危险，采取有效安全防护措施，改善系统安全状况。这里所强调的“预先”是指：无论系统生命过程处于哪个阶段，都要在该阶段开始之前进行系

统的安全分析，发现并掌握系统的危险因素。这就是系统安全分析要解决的问题。

系统安全分析是使用系统工程的原理和方法，辨别、分析系统存在的危险因素，并根据实际需要对其进行定性、定量描述的技术方法。

根据有关文献介绍，系统安全分析有多种形式和方法，使用中应注意：①根据系统的特点、分析的要求和目的，采取不同的分析方法。因为每种方法都有其自身的特点和局限性，并非处处通用。使用中有时要综合应用多种方法，以取长补短或相互比较，验证分析结果的正确性。②使用现有分析方法不能死搬硬套，必要时要根据实用、好用的需要对其进行改造或简化。③不能局限于分析方法的应用，而应从系统原理出发，开发新方法，开辟新途径，还要在以往行之有效的一般分析方法基础上总结提高，形成系统性的安全分析方法。

2. 系统安全评价

系统安全评价往往要以系统安全分析为基础，通过分析，了解和掌握系统存在的危险因素，但不一定要对所有危险因素采取措施。而是通过评价掌握系统的事故风险大小，以此与预定的系统安全指标相比较，如果超出指标，则应对系统的主要危险因素采取控制措施，使其降至该标准以下。这就是系统安全评价的任务。

评价方法也有多种，评价方法的选择应考虑评价对象的特点、规模，评价的要求和目的，采用不同的方法。同时，在使用过程中也应和系统安全分析的使用要求一样，坚持实用和创新的原则。过去 20 年，我国在许多领域都进行了系统安全评价的实际应用和理论研究，开发了许多实用性很强的评价方法，特别是企业安全评价技术和重大危险源的评估、控制技术。

3. 安全决策与事故控制

任何一项系统安全分析技术或系统安全评价技术，如果没有一种强有力的管理手段和方法，也不会发挥其应有的作用。因此，在出现系统安全分析和系统安全评价技术的同时，也出现了系统安全决策。其最大的特点是从系统的完整性、相关性、有序性出发，对系统实施全面、全过程的安全管理，实现对系统的安全目标控制。最典型的例子是美军标准《系统安全程序》，美国道化学公司的安全评价程序，国际劳工组织、国际标准化组织倡导的《职业安全卫生管理体系》。系统安全管理是应用系统安全分析和系统安全评价技术，以及安全工程技术为手段，控制系统安全性，使系统达到预定安全目标的一整套管理方法、管理手段和管理模式。

三、安全系统工程的方法论

安全系统工程的方法是依据安全学理论，在总结过去经验型安全方法的基础上日渐丰富和成熟的。概括起来可以归纳为如下三个方面：

1. 从系统整体出发的研究方法

安全系统工程的研究方法必须从系统的整体性观点出发，从系统的整体考虑解决安全问题的方法、过程和要达到的目标。例如，对每个子系统安全性的要求，要与实现整个系统的安全功能和其他功能的要求相符合。在系统研究过程中，子系统和系统之间的矛盾以及子系统与子系统之间的矛盾，都要采用系统优化方法寻求各方面均可接受的满意解；同时要把安全系统工程的优化思路贯穿到系统的规划、设计、研制和使用等各个阶段中。

2. 本质安全方法

这是安全技术追求的目标，也是安全系统工程方法中的核心。由于安全系统把安全问题中的人一机（物） —环境统一为一个“系统”来考虑，因此不管是从研究内容来考虑还是从系统目标来考虑，核心问题就是本质安全化，就是研究实现系统本质安全的方法和途径。

3. 人一机匹配法

在影响系统安全的各种因素中，至关重要的是人—机匹配。在产业部门研究与安全有关的人机匹配称为安全人机工程，在人类生存领域研究与安全有关的人机匹配称为生态环境和人文环境问题。显然，从安全的目标出发，考虑人一机匹配，以及采用人—机匹配的理论和方法是安全系统工程方法的重要支撑点。

4. 安全经济方法

由于安全的相对性原理，所以，安全的投入与安全（目标）在一定经济、技术水平条件下有对应关系。也就是说，安全系统的“优化”同样受制于经济。但是，由于安全经济的特殊性（安全性投入与生产性投入的渗透性、安全投入的超前性与安全效益的滞后性、安全效益评价指标的多目标性、安全经济投入与效用的有效性等）就要求安全系统工程方法，在考虑系统目标时，要有超前的意识和方法，要有指标（目标）的多元化的表示方法和测算方法。

5. 系统安全管理方法

安全系统工程从学科的角度讲是技术与管理相交叉的横断学科；从系统科学原理的角度讲它是解决安全问题的一种科学方法。所以，安全系统工程是理论与实践紧密结合的专业技术基础，系统安全管理方法则贯穿到安全的规划、设计、检查与控制的全过程。所以，系统安全管理方法是安全系统工程方法的重要组成部分。

第三节　　安全系统工程的产生与发展

事故给人类带来无数灾难，严重地制约了经济发展和社会进步，甚至对人类生存构成巨大威胁。然而，事故的影响也并非都是消极的。它和其他事物一样，也有积极的一方面。首先，事故具有鲜明的反面教育的作用，它向人们展示了破坏的恶果，教人们必须按照科学规律办事。其次，事故是一种特殊的科学实验。一个系统发生事故，说明该系统存在这样那样的不安全、不可靠的问题，从而以事故的形式弥补了设计时应做而没做，或想做而没敢做（没钱做）的实验。人们通过对事故的调查、分析，找出事故原因，研究并采取了有效控制事故的措施，改变了系统工艺、设备，从而提高了系统的性能，发展了专业技术。第三，事故也是诞生新的科学技术的催化剂。事故的强大负面效应对人类产生巨大的冲击作用，从而激发人类以更大的决心和更大的力量研究事故。通过对事故信息、资料的收集、整理、分析、研究，也就是充分开发利用“事故资源”，一个崭新的自然科学学科就在人们这种不懈努力与坚苦卓绝的斗争中诞生了，这就是作用力与反作用力的作用机制。在科学技术发展的历史长河中，几乎每一个学科的诞生都离不开事故这种反作用力的作用。

安全系统工程也正是在这种事故的反作用下应运而生的。安全系统工程产生于 20 世纪 60 年代初期美英等工业发达国家。这一时期，由于美国在导弹系统研发过程中仅仅一年半

的时间就连续发生四起重大事故，造成惨重损失，从而迫使美国空军以系统工程的基本原理和管理方法来研究导弹系统的安全性、可靠性，并于 1962 年提出了“ 弹道导弹系统安全工程 ”，制定了“ 武器系统安全标准 ”；1963 年提出了“ 系统安全程序 ”；到 1967 年 7 月由美国国防部确认，将该标准提格为美军标准；之后又经两次修订，成为现在的 MIL-STD-882B“ 系统安全程序要求 ”。它以标准的形式规范了美国军事系统的工程项目在招标以及研发过程中对安全性的要求和管理程序、管理方法、管理目标。这就是由事故引发的军事系统的安全系统工程。

原子弹是可怕的，从而在人们的心里存在着对以放射性物质为动力的核电站的恐惧心理。因此，在社会压力下各国的政府对核电站的要求极其严格，同时在核安全方面的研究投入了巨大的人力、物力。英国在这方面的研究开始比较早，到 20 世纪 60 年代中期就已建成了系统可靠性服务所和可靠性数据库，成功开发了概率风险评价（PRA）技术，从而以概率来计算核电站系统风险大小以及是否可以接受。到 1974 年美国原子能委员会发表了拉斯姆逊教授的“ 商用核电站风险评价报告 ”（WASH-1400），从而成功地开发应用了系统安全分析和系统安全评价技术。该报告的科学性和对事故预测的准确性得到了“ 三浬岛事件 ”（核电站堆芯熔化造成放射性物质泄漏事故）的证实。这就是核工业的安全系统工程。

化工企业的危险性和化工事故的危害性是众所周知的。随着工业规模的扩大和事故破坏后果的日益严重化，迫使化工企业加倍努力，严格控制事故，特别是化工厂的火灾爆炸事故。为此，美国道化学公司于 1964 年发表了化工厂“ 火灾爆炸指数评价法 ”，俗称道氏法。该法经过多年的实用，修改了 6 次，出了第七版，并出版了教科书。该法是以根据化学物质的理化特性确定的物质系数为基础，综合考虑一般工艺过程和特殊工艺过程的危险特性，计算系统火灾爆炸指数，评价系统损失大小，并据此考虑安全措施，修正系统风险指数。之后，英国帝国化学公司在此基础上开发了蒙德评价法，日本提出了岗三法、疋田法。20 世纪 70 年代日本劳动省发表的评价方法，另辟蹊径，它是以分析与评价，定性评价与定量评价相结合为特点的“ 化工企业安全评价指南 ”，亦称“ 化工企业六步骤安全评价法 ”。该评价法是一种对化工系统的全过程如何进行评价的管理规范。它不仅规定了评价方法、评价技术，也规定了系统生命周期每个阶段用哪种评价方法，如何进行评价等。这就是化工系统的安全系统工程。

民品工业也存在安全系统工程的诞生与发展问题。 20 世纪 60 年代正是美国市场竞争日趋激烈的年代，许多新产品在没有得到安全保障的情况下就投放市场，造成许多使用事故，用户纷纷要求厂方赔偿损失，甚至要求追究厂商刑事责任，迫使厂方在开发新产品的同时寻求提高产品安全性的新方法、新途径。这期间，在电子、航空、铁路、汽车、冶金等行业开发了许多系统安全分析方法和评价方法，这也可以称之为民品工业的安全系统工程。

在我国，安全系统工程的研究、开发是从 20 世纪 70 年代末的开始的。天津东方化工厂应用安全系统工程成功地解决了高度危险企业的安全生产问题，为我国各个领域学习、应用安全系统工程起了带头作用。其后是各类企业借鉴引用国外的系统安全分析方法，对现有系统进行分析。到 80 年代中后期，人们研究的注意力逐渐转移到系统安全评价的理论和方法，开发了多种系统安全评价方法，特别是企业安全评价方法，重点解决了对企业危险程度的评价和企业安全管理水平的评价。

这期间，许多专家学者的相关专著也相继问世了，以系统的观点、方法，系统地总结了国内外安全系统的理论与方法，这些论著的共同观点是：

(1) 安全系统工程是在事故逼迫下产生的。安全系统工程也好，系统安全工程也好，都是在人类从事社会经济活动中由于发生事故的规模如此巨大，事故损失如此惨重，以致人们再也承受不起这么严重的灾难，不得不在现有安全工程技术基础上，寻找能够预测、预防、预控事故的科学技术，安全系统工程就是在这样的背景下诞生的。即，预先的系统安全分析、系统安全评价技术和对系统整个生命周期实施全过程安全控制的系统安全管理工程。

(2) 现代科学技术的发展为安全系统工程的产生提供了必要条件。20世纪40年代产生了系统可靠性工程，50年代出现了系统工程，以及这一期间现代数学和计算机技术的迅速发展，使安全系统工程在20世纪60年代产生成为科学技术发展的必然产物，也是相关学科相互影响的必然结果。

(3) 美国导弹技术的开发促使安全系统工程的诞生，但它不是安全系统工程产生的惟一策源地。美国导弹技术的开发深入地研究了系统的安全性和控制系统安全性的手段与方法，从而出现了空军标准“系统安全程序”和“系统安全程序要求”。同时也必须看到，在同一时期，还有核电站的概率风险评价技术，化工企业的火灾爆炸指数安全评价法，以及涉及产品安全的系统安全分析技术，如FTA、ETA、FMEA等，这些行业的安全系统工程都是在20世纪60年代短短几年时间产生的，因此，我们把所有这些成功的理论通过科学的总结形成一个完整的学科——安全系统工程，应当说是顺理成章的。

(4) 安全系统工程不仅包括分析与评价技术，也应包括管理程序、管理方法等管理科学的内容，它也是以系统工程为基础的安全工程。

各类有关安全系统工程的论著，其内容都是以系统工程为基本原理，包括系统安全分析、系统安全评价和系统安全管理三部分内容。通过分析和评价认识风险，通过工程技术管理控制风险，使系统安全性达到预定的目标。

基于这种思想，迄今国外发表的系统安全分析、系统安全评价、系统安全管理技术与方法属于安全系统工程范畴；国内已经实践证明对预先控制事故、提高系统安全性确有实效的，具有系统工程鲜明特点的安全分析、安全评价和安全管理技术与方法也应当属于安全系统工程范畴。在安全系统工程的发展进程中，应当有我们中国人的贡献！

第四节　安全系统工程的应用特点

安全系统工程是一门应用性很强的科学技术学科。几十年来，许多经典的应用范例始终激励人们进行不懈的探索，不断充实和发展其自身的理论体系，以期实现更好的应用效果，这是安全系统工程始终保持快速发展的重要原因。为了进一步促进学科发展，提高其实用性，有必要进一步明确安全系统工程的应用特点：

(1) 系统性。无论是系统安全分析、系统安全评价的理论，还是系统安全管理模式和方法的应用都表现了系统性的特点，它从系统的整体出发，综合考虑系统的相关性、环境适应性等特性，始终追求系统总体目标的满意解或可接受解。

(2) 预测性。安全系统工程的分析技术与评价技术的应用，无论是定性的，还是定量

的，都是为了预测系统存在的危险因素和风险水平。它是通过这些预测来掌握系统安全状况如何，风险能否接受，以便决定是否应当采取措施，控制系统风险。所以，安全系统工程也可称作是系统的事故预测技术。

（3）层序性。安全系统工程的应用是按照系统的时空两个跨度有序展开，管理规范的执行，一般是按照系统生命过程有序进行，而且贯彻到系统的方方面面。因此，安全系统工程具有明显的“动态过程”研究特点。

（4）择优性。择优性的应用特点主要体现在系统风险控制方案的综合与比较，从各种备选方案中选取最优方案。在选取控制风险的安全措施方面，一般按下列优先顺序选取方案：设计上消除→设计上降低→提供安全装置→提供报警装置→提出专门规程。因此，冗余设计，安全联锁，有一定可靠度保证的安全系数，是安全系统工程经常采用的设计思想。

（5）技术与管理的融合性。前面述及安全系统工程是自然（技术）科学与管理科学的交叉学科，随着科技与经济的发展，人们对安全的追求目标（特别是生产领域）是本质安全。但是，一方面由于新技术的不断涌现，另一方面由于经济条件的制约，对于一时做不到本质安全的技术系统，则必须用安全管理来补偿。所以在相当长的时间内，解决安全问题还必须把技术与管理通过系统工程的方法有机地结合起来。

这些安全系统工程的应用特点应在该学科的理论研究和实际应用中得到充分重视，使安全系统工程发展更快些，应用效果更明显些。

思考题

1. 名词解释：

风险、风险度、系统、系统工程、可靠性、可靠度、安全、安全系统。

2. 安全系统工程产生的客观背景与条件是什么？

第二章 系统安全分析

第一节 概 述

系统安全分析(System safety analysis) 的目的是为了保证系统安全运行，查明系统中的危险因素，以便采取相应措施消除系统故障或事故。

一、系统安全分析的内容和方法

系统安全分析是从安全角度对系统中的危险因素进行分析，主要分析导致系统故障或事故的各种因素及其相关关系，通常包括如下内容：

(1) 对可能出现的初始的、诱发的及直接引起事故的各种危险因素及其相互关系进行调查和分析。

(2) 对与系统有关的环境条件、设备、人员及其他有关因素进行调查和分析。

(3) 对能够利用适当的设备、规程、工艺或材料控制或根除某种特殊危险因素的措施进行分析。

(4) 对可能出现的危险因素的控制措施及实施这些措施的最好方法进行调查和分析。

(5) 对不能根除的危险因素失去或减少控制可能出现的后果进行调查和分析。

(6) 对危险因素一旦失去控制，为防止伤害和损害的安全防护措施进行调查和分析。

目前，系统安全分析方法有许多种，可适用于不同的系统安全分析过程。这些方法可以按实行分析过程的相对时间进行分类，也可按分析的对象、内容进行分类。按数理方法，可分为定性分析和定量分析；按逻辑方法，可分为归纳分析和演绎分析。

简单地讲，归纳分析是从原因推论结果的方法，演绎分析是从结果推论原因的方法，这两种方法在系统安全分析中都有应用。从危险源辨识的角度，演绎分析是从事故或系统故障出发查找与该事故或系统故障有关的危险因素，与归纳分析相比较，可以把注意力集中在有限的范围内，提高工作效率；归纳分析是从故障或失误出发探讨可能导致的事故或系统故障，再来确定危险源，与演绎方法相比较，可以无遗漏地考察、辨识系统中的所有危险源。实际工作中可以把两类方法结合起来，以充分发挥各类方法的优点。

在危险因素辨识中得到广泛应用的系统安全分析方法主要有以下几种：

(1) 安全检查表法 (Safety Checklist)；

(2) 预先危险性分析 (Preliminary Hazard Analysis，PHA)；

(3) 故障类型和影响分析 (Failure Model and Effects Analysis，FMEA)；

(4) 危险性和可操作性研究 (Hazard and Operability Analysis，HAZOP)；

(5) 事件树分析 (Event Tree Analysis，ETA)；

(6) 事故树分析 (Fault Tree Analysis，FTA)；

(7) 因果分析 (Cause-Consequence Analysis，CCA)。

此外，尚有 What If （如果出现异常将会怎样）分析，MORT （管理疏忽和风险树）分析等方法，可用于特定目的的危险因素辨识。

二、系统安全分析方法的选择

在系统寿命不同阶段的危险因素辨识中，应该选择相应的系统安全分析方法。例如，在系统的开发、设计初期，可以应用预先危险性分析方法；在系统运行阶段，可以应用危险性和可操作性研究、故障类型和影响分析等方法进行详细分析，或者应用事件树分析、事故树分析或因果分析等方法对特定的事故或系统故障进行详细分析。系统寿命期间内各阶段适用的系统安全分析方法见表 2-1。

表 2-1　系统安全分析方法适用情况

分析方法	开发研制	方案设计	样　机	详细设计	建造投产	日常运行	改建扩建	事故调查	拆　除
检查表		√	√	√	√	√	√		√
预先危险性分析	√	√	√	√			√		
危险性与可操作性研究			√	√		√	√	√	
故障类型和影响分析			√	√		√	√	√	
事故树分析		√	√	√		√	√	√	
事件树分析			√			√	√	√	
因果分析			√	√		√	√	√	

在进行系统安全分析方法选择时应根据实际情况，并考虑如下几个问题：

1. 分析的目的

系统安全分析方法的选择应该能够满足对分析的要求。系统安全分析的最终目的是辨识危险源，而在实际工作中要达到一些具体目的，例如：

（1）对系统中所有危险源，查明并列出清单；

（2）掌握危险源可能导致的事故，列出潜在事故隐患清单；

（3）列出降低危险性的措施和需要深入研究部位的清单；

（4）将所有危险源按危险大小排序；

（5）为定量的危险性评价提供数据。

在进行系统安全分析时，某些方法只能用于查明危险因素，而大多数方法都可以用于列出潜在的事故隐患或确定降低危险性的措施，但能提供定量数据的方法并不多。

2. 资料的影响

关于资料收集的多少、详细程度、内容的新旧等，都会对选择系统安全分析方法有着至关重要的影响。

一般来说，资料的获取与被分析的系统所处的阶段有直接关系。例如，在方案设计阶段，采用危险性和可操作性研究或故障类型和影响分析的方法就难以获取详细的资料。随着系统的发展，可获得的资料越来越多、越详细。为了能够正确分析，应该收集最新的、高质量的资料。

3. 系统的特点

针对被分析系统的复杂程度和规模，工艺类型，工艺过程中的操作类型等影响来选择系统安全分析方法。

对于复杂和规模大的系统，由于需要的工作量和时间较多，应先用较简捷的方法进行筛选，然后根据分析的详细程度选择相应的分析方法。

对于某些工艺过程或系统，应选择恰当的系统安全分析方法。例如，对于分析化工工艺过程可采用危险性和可操作性研究；对于分析机械、电气系统可采用故障类型和影响分析。因此，应该根据分析对象的类型，选择相应的分析方法。

对于不同类型的操作过程，若事故的发生是由单一故障（或失误）引起的，则可以选择危险性与可操作性研究；若事故的发生是由许多危险因素共同引起的，则可以选择事件树分析、事故树分析等方法。

4.系统的危险性

当系统的危险性较高时，通常采用系统、严格、预测性的方法，如危险性与可操作性研究、故障类型和影响分析、事件树分析、事故树分析等方法。当危险性较低时，一般采用经验的、不太详细的分析方法，如安全检查表法等。

对危险性的认识，与系统无事故运行时间和严重事故发生次数，以及系统变化情况等有关。此外，还与分析者所掌握的知识和经验，完成期限，经费状况，以及分析者和管理者的喜好等有关。

第二节　安全检查及安全检查表

一、安全检查

安全检查是运用常规、例行的安全管理工作及时发现不安全状态及不安全行为的有效途径，也是消除事故隐患、防止伤亡事故发生的重要手段。

1. 安全检查的性质

安全检查除了进行经常性的检查外，还应定期地进行群众性的检查。检查的性质可分为普遍检查、专业性检查和季节性检查等。

开展安全检查工作，要做到有计划、有组织、目标明确、内容要求具体，并且必须由领导负责、有关人员参加的安全生产检查组进行实施。安全检查自始至终应贯彻领导与群众相结合的原则，做到边检查、边整改。

2. 安全检查的内容

安全检查的内容主要是查思想、查管理、查隐患、查事故处理。

（1）查思想：检查企业领导和各级管理人员的思想认识，是否把职工的安全健康放在首位，对安全法规、政策和安全生产方针是否认真贯彻执行。

（2）查管理：主要是检查企业领导是否把安全生产列入议事日程；企业主要负责人在计划、布置、检查、总结、评比生产的同时是否将‘五同时’的要求落到实处 新建、改建、扩建的工程项目与安全卫生设施是否执行同时设计、同时施工、同时投产的“三同时”原则；安全机构、安全教育制度、安全规章制度以及特种作业人员的培训制度是否健全。

（3）查隐患：通过检查生产设备、劳动条件、安全卫生设施是否符合安全要求以及劳动者在生产中是否存在着不安全行为等，找出不安全因素和事故隐患。

（4）查事故处理：检查企业对伤亡事故是否及时报告，认真调查；是否按“三不放过”的要求严肃处理；是否采取了有效措施，避免类似事故重复发生。

二、安全检查表

安全检查表是分析和辨识系统危险性的基本方法，也是进行系统安全性评价的重要技术手段。早在20世纪中期，安全检查表在许多发达国家的保险、军事等部门得到了应用，对系统安全性评价起到了很大作用。随着科学技术的进步和生产规模的扩大，安全检查表引起了人们的高度重视，在各部门和行业生产中得到了广泛应用。我国机械、电子等部门首先用来开展企业安全评价工作，并于1988年1月颁布了《机械工厂安全性评价标准》，对保证安全生产起到了积极作用。

1. 安全检查表的形式

安全检查表的形式很多，检查表可根据不同的检查目的进行设计，也可按照统一要求的标准格式制作，如危险等级划分表、安全性评价项目表、安全性评价检查表等。安全检查表的基本格式见表2-2。

在进行安全检查时，利用安全检查表能做到目标明确、要求具体、查之有据；对发现的问题做出简明确切的记录，并提出解决的方案，同时落实到责任人，以便及时整改。

表2-2 安全检查表的基本格式

检查时间	检查单位	检查部位	检查结果	安全要求	整改期限	整改负责人

序　号	安全检查内容	结论与说明

2. 安全检查表的类型

根据用途和安全检查表的内容，安全检查表可分为以下几种类型：

（1）审查设计的安全检查表。新建、改建和扩建的厂矿企业，革新、挖潜的工程项目，都必须与相应的安全卫生设施同时设计、同时施工和同时投产，即利用“三同时”原则全面、系统地审查工程的设计、施工和投产等各项的安全状况。检查表中除了已列入的检查

项目外，还要列入设计应遵循的原则、标准和必要数据。用于设计的安全检查表主要应包括厂址选择、平面布置、工艺过程、装置的布置、建筑物与构筑物、安全装置与设备、操作的安全性、危险物品的贮存以及消防设施等方面。

（2）厂级的安全检查表。主要用于全厂性安全检查，也可用于安全技术、防火等部门进行日常检查。其主要内容包括主要安全装置与设施、危险物品的贮存与使用、消防通道与设施、操作管理及遵章守纪等方面的情况。

（3）车间的安全检查表。用于车间进行定期检查和预防性检查的检查表，重点放在人身、设备、运输、加工等不安全行为和不安全状态方面。其内容包括工艺安全、设备布置、安全通道、通风照明、安全标志、尘毒和有害气体的浓度、消防措施及操作管理等。

（4）工段及岗位的安全检查表。用于工段和岗位进行自检、互检和安全教育的检查表，重点放在因违规操作而引起的多发性事故上。其内容应根据岗位的操作工艺和设备的抗灾性能而定。要求检查内容具体、易行。

（5）专业性安全检查表。此类表格是由专业机构或职能部门所编制和使用的，主要用来进行定期的或季节性的安全检查，如对电气设备、起重设备、压力容器、特殊装置与设施等的专业性检查。

3. 安全检查表的编制

安全检查表应由专业干部、有关部门领导、工程技术人员和工人共同编写，并通过实践检验不断修改，使之逐步完善。

安全检查表可以按生产系统、车间、工段和岗位编写，也可以按专题编写，如对重要设备和容易出现事故的工艺流程，就应该编制该项工艺的专门的安全检查表。

安全检查表的编制过程，也是对系统进行安全分析的过程。通过对系统的全面分析，结合有关资料，找出系统中存在的隐患、事故发生的可能途径和影响后果等，然后根据有关法规、规章制度、标准和安全技术要求，完成检查表的制定工作。为了清楚地列出检查表中的检查项目和检查重点，可通过事故树分析找出导致事故的基本事件和最小割集，然后进行逐一审查并确定出它们之间的逻辑关系。

4. 安全检查表的特点

安全检查表是进行系统安全性分析的基础，也是安全检查中行之有效的基本方法，具有以下明显的特点：

（1）通过预先对检查对象进行详细调查研究和全面分析，所制定出来的安全检查表比较系统、完整，能包括控制事故发生的各种因素，可避免检查过程中的走过场和盲目性，从而提高安全检查工作的效果和质量；

（2）安全检查表是根据有关法规、安全规程和标准制定的，因此检查目的明确，内容具体，易于实现安全要求；

（3）对所拟定的检查项目进行逐项检查的过程，也是对系统危险因素辨识、评价和制定出措施的过程，既能准确地查出隐患，又能得出确切的结论，从而保证了有关法规的全面落实；

（4）检查表是与有关责任人紧密相连系的，所以易于推行安全生产责任制，检查后能够做到事故清、责任明、整改措施落实快；

（5）安全检查表是通过问答的形式进行检查的过程，所以使用起来简单易行，易于安