系统安全性分析

周经伦摇龚时雨摇颜兆林摇编著

中南大学出版社

内摇容摇简摇介

本书阐述了安全性系统工程学科的重要领域——系统安全性分析的理论和方法。全书共 怨章，主要内容包括系统安全性的基本概念、系统寿命周期工作内容、事故机理、危险分析方法与技术、风险评价、[illegible]网安全性建模与分析、安全性设计以及安全性分析重要信息基础的危险源，最后介绍了计算机辅助安全性分析的有关内容。

本书适合于从事安全性分析和工程设计的技术人员使用，也可作为大、中专院校可靠性与安全性工程专业学习的教材或参考书。

目录

第 员章摇概摇摇述

员.员摇引摇言

安全性概念是 圆园世纪 缘园年代提出的，并在随后的几十年中得到了迅速发展。特别是近年来随着工业技术复杂程度的不断提高，投入资金的不断增加，在设备研制和使用过程中风险也随之不断增大。美国挑战者号航天飞机的失事，前苏联切尔诺贝利核电站的泄漏事故以及欧空局阿里安 缘号运载火箭首次飞行的失事都是比较典型的例子。因此，安全性问题越来越受到世界各国工业部门的重视。

就武器装备的安全性而言，其研制、试验、生产和使用以至退役处理的整个寿命过程都可能存在着导致发生事故的潜在危险，都有可能发生事故。这是安全问题的一个方面，即从装备研制生产的纵向来研究安全问题。另一方面，武器作为一个系统是由不同分系统和操作人员组成的整体，同时武器研制涉及不同的专业学科（如光、电、机械、火工等），这些分系统及专业学科都有自己的安全问题，并且它们之间互相作用会产生复杂的后果而影响安全性，这就要从装备及其有关分系统和不同学科横向来研究安全问题。因此，研究武器装备的安全必须从上述两个方面，即从装备的全寿命周期中的各阶段和装备系统及其分系统之间的联系中找出事故发生的客观规律和内部联系，通过科学的分析，识别潜在危险，作出定性和定量的评价 提出在设计、制造和使用装备中消除潜在危险或控制这些危险使之降低到可接受程度的措施，达到安全的目的。

系统安全性是以效能、进度和费用为约束条件，在系统寿命周期内的各阶段中，应用工程管理的原则、专业技术和系统方法，识别、评价、消除或控制系统和设备中的危险，从而使系统具有最佳安全程度的工程学科。它是近 猿园年来适应大型复杂系统研制的需要而发展起来的一门综合性学科。它的重要组成部分是系统安全性分析。系统安全性分析是一种从系统研制初期的论证阶段开始进行，并贯穿工程研制、生产阶段的系统性检查、研究和分析危险的技术方法。它用于检查系统或设备在每种使用模式中的工作状态，确定潜在的危险，预计这些危险对人员伤害或对设备损坏的可能性，并确定消除或减少危险的方法，以便能够在事故发生之前消除或尽量减少事故发生的可能性或降低事故有害影响的程度。目前，系统安全性分析技术已广泛应用于核能、化工、航天和航空等领域。

武器系统安全性学科的发展史

工业生产中传统的安全技术工作已有很多年的历史，其间，预防事故的理论与实践也有不少的进展。但现代大型复杂工程系统是多学科发展的成果，单项的安全防护或单一学科的安全研究难以解决整个系统的安全问题。特别是在武器系统发展中多次严重的灾难性事故的经验与教训，促使人们认识到安全工作必须走系统分析研究的道路，从而推动系统安全性得到了应有的发展。

1950年美国防空导弹的爆炸事故，首先引起了其陆军部的重视，于1951年6月在[illegible]兵工厂建立了第一个系统安全性工程组织。经研究确定，把安全性要求纳入装备设计的规范中，以保证装备的安全性。

1957年前苏联发射了第一颗人造地球卫星。美国为了赶上前苏联的空间技术，匆忙地发展导弹武器。在20世纪50年代末到60年代前半期，为了缩短开发时间，美国在发展井下弹道导弹发射系统时，采取了构思、设计、制造与使用齐头并进的方针。当时，安全问题仅依靠各专业技术人员单独研究，忽视了发射系统的接口安全问题。最初运行实验的一年半时间内，在导弹地下贮存和发射基地连续发生了四次重大事故，每次损失都达到数百万美元，因而推迟了试验计划。事故调查结果表明，主要原因在于装备安全性存在重大问题，因而不得不将设备报废重新设计。因此，美国空军于1962年5月明确地提出了以系统工程的方法研究导弹系统的安全性，即“空军弹道导弹系统安全性工程”，同年8月又将系统安全性作为独立工程项目发布了“武器系统安全性标准[illegible]”，这为发展多弹头火箭创造了条件。1966年6月美国国防部对空军的标准作了修改，颁布了[illegible]，以此作为美军所有军事装备必须遵守的标准。以后，美国国防部再次修订了这项标准，并于1969年7月发布了“系统、有关分系统与设备的系统安全性大纲”，即[illegible]。在这项标准中首先建立了较完整的系统安全性概念，以及安全性分析、设计和评价等基本原则。直至1984年，[illegible]已作了多次修订，系统安全性工作的要求在装备全寿命周期内得到明确而全面的规定，并增加了软件安全性要求。这是当前不少国家引用的比较成熟的系统安全性标准。1980年美国国防部颁发的军用手册《陆军装备系统安全性工程设计指南》([illegible])，详细地论述了系统安全性概念及其设计与分析的方法。

核爆炸和核污染给人类带来不可估量的严重后果。20世纪70年代美国在核武器和核工业领域相继提出了保证安全的问题。1975年美国核能委员会（[illegible]）发表了《商用核电站轻水反应堆的风险评价》报告（[illegible]）。它是在麻省理工学院[illegible]教授领导下，组织数十名人员，历经三年完成的。该报告收集了核电站各部位历年发生的事故类型及其频率，应用事件树和故障树分析技术成功地作出了核电站安全性定量评价。这是核能安全性分析技术发展的一个重要里程碑。它说明了概率安全评价（[illegible]）是对复杂系统进行安全评价的重要方法，受到世界各国从事系统安全性工作者的普遍重视。

日本的系统安全性工作虽起步较晚，但发展较快。1969年日本科技联盟曾召开了“可靠性安全性学术讨论会”，但当时没有引起工业界的重视，以至1970～1974年前后连续发生了多起重大的事故，如濑户内海石油罐破裂造成严重污染、德山工厂乙烯装置爆炸等，震惊了世界。

日本于 [illegible]年引进了安全系统工程，在电子、宇航、铁路、公路、化工、冶金和核能等工业领域研究工作十分活跃。[illegible]年 [illegible]月日本劳动省公布的“化工联合企业安全评价指南”中的安全评价六个步骤，作为国家法令颁布执行，在其他一些产业部门和企业得到应用，提高了新产品在设计、制造和使用中的安全性。

[illegible]世纪 [illegible]年代至 [illegible]年代，我国国务院发布了一系列有关安全工作的法规，对企业安全提出了明确的要求，并在健全安全机构、开展安全工作方面做了有益的工作，安全工作不断得到改善。但这些安全要求和工作都没有从系统角度出发来研究消除和控制危险的方法。[illegible]年代我国开始进行有关系统安全性的研究，[illegible]年天津东方化工厂最早应用故障树分析方法分析了最容易发生火灾爆炸的高氯酸生产过程。[illegible]年我国首次召开了安全系统工程讨论会，研讨了我国发展安全系统工程的方向，开始对初步危险分析（[illegible]）、事件树分析（[illegible]）、故障树分析（[illegible]）等分析方法进行研究，并推广应用安全检查表。[illegible]年中国劳动保护科学技术学会成立了管理科学专业委员会以及其下属的“系统安全学组”。这个组以安全系统工程研究和应用为中心，开展攻关、开发、推广和交流成果活动，为系统安全性学科的发展作出了较大的贡献。[illegible]年我国正式颁发了国家军用标准《系统安全性通用大纲》（[illegible]）。它规定了装备系统和寿命周期各阶段的安全性要求、安全性管理工程技术内容和活动。最近颁发的国军标《系统安全性设计手册》详细地介绍了成熟的系统安全性设计与分析的内容。目前，全国有十几所高等院校开设有安全系统工程专业课程，以培养安全性系统工程的专门人才。

[illegible]安全性基本概念及参数指标

[illegible]安全性概念

安全性（[illegible]）是指不发生事故的能力。系统或产品的安全性，表示在给定的条件下系统或产品无事故地完成任务的一种特性。其中事故指的是使一项正常进行的活动中断，并造成人员伤亡、职业病、财产损失或损害环境的意外事件。事故可以认为是由于未能鉴别危险或是由于控制危险的措施不合理所造成的。

可能导致事故的状态称为危险（[illegible]），它是发生事故的先决条件。可能导致事故的状态有物质状态、环境状态和人员活动状态以及它们的组合。危险可分为现实的和潜在的。现实的危险是指可能产生不良结果的固有特性，如发动机废气排出管具有高温特性，可能导致着火燃烧的危险。有毒物质也是现实的危险。潜在的危险是指原来并非为固有的危险状态，在特定条件下潜伏有导致发生事故的可能状态。如在通风良好条件下存放的煤炭并非危险状态，但长期堆放而通风不良，便有自燃的危险。油路管道和电气线路均非现实危险状态，但设计布置时，油路管道在电线上方，距离很近，则存在着油料泄漏、电路起火的潜在危险。潜在危险是系统安全性重点研究的对象。

必须指出，术语“系统安全性”并非指“系统的安全性”，而是指采用系统分析的方法和管理原则及工程工具，分析、识别和控制危险，使产品（系统、项目、设施或活动等）获得最佳安全性的工作。因此，系统安全性是一门学科，它将安全性问题作为系统工程问题进行研究，也可称其为安全系统工程或系统安全性工程。

本书中也用术语“系统”表示安全性工程中所研究的某个对象，它可以指具体的工程系统，如核电厂、军事装备等等。

安全性参数

安全性参数用于对系统的安全性进行度量，常用的安全性参数包括事故概率、平均事故间隔时间、安全可靠度和损失概率等。

事故概率

事故概率定义为：在规定的条件下和规定的时间内，系统的事故总次数与寿命单位总数之比，用下式表示：

$$P_A = \frac{N_A}{N_T} \tag{1}$$

式中：N_A——事故总次数，包括由于系统及设备故障、人为因素及环境因素等造成的事故总次数；

N_T——寿命单位总数，表示系统总使用持续期的度量，如工作小时、飞行小时、飞行次数、年、公里等。

平均事故间隔时间

平均事故间隔时间 T_A 定义为：在规定的条件下和规定的时间内，系统的寿命单位总数与事故总次数之比，它用下式表示：

$$T_A = \frac{N_T}{N_A} \tag{2}$$

式中，N_A、N_T 与式 (1) 相同。

安全可靠度

安全可靠度 R_S 定义为：在规定的一系列任务剖面中，系统无机械事故（即由于系统或其设备故障造成的事故）执行规定任务的概率。可用下式表示：

$$R_S = \mathrm{e}^{-\lambda_S t} \tag{3}$$

式中：λ_S——造成事故的系统或其设备故障的故障率；

t——执行任务时间。

安全可靠度还可用下式近似计算：

$$P_S = \frac{N_S}{N_T} \tag{4}$$

式中：P_S——在规定时间内，安全执行任务的概率；

N_S——在规定时间内，无机械事故执行任务的次数；

N_T——在规定时间内，执行任务的总次数。

损失概率

损失概率 P_L 定义为：在规定的时间内，由于系统或其设备故障造成系统灾难性事故（如严重的人员伤亡、重大的经济损失或严重的环境损害）总次数与在该时间内系统寿命单位总数之比。P_L 可用下式表示：

$$P_L = \frac{N_L}{N_T} \tag{5}$$

式中：晕缊——由于系统或其设备故障造成系统灾难性事故总次数；

晕栽——寿命单位总数，表示系统总使用持续期的度量，如工作小时、飞行小时、飞行次数、年、公里等。

系统的损失概率还可用下式表示：

孕缊越员原砸泽 （员援远）

式中：砸泽——安全可靠度。

员援猿援猿援圆 安全性指标

安全性指标是安全性的定量要求，即安全性参数要求的量值，它直接表示系统的安全性水平。例如，某航天飞机的安全性指标：在每次飞行任务中，航天飞机的灾难性事故概率不大于员园原源。其中发射阶段的灾难性事故概率为员伊员园原缘，轨道飞行阶段为苑伊员园原缘，返回阶段为圆伊员园原缘。

又如，某飞机的飞行操纵系统和供电系统提出的安全性指标：飞机操纵系统故障造成飞机灾难性事故的概率孕缊越缘伊员园原苑辕每次飞行，孕缊越园援苑远伊员园原苑辕飞行小时；为保证飞机安全返回，供电系统向汇流条及所有必需的用电设备供电的安全可靠度分别为园援怨怨怨愿及园援怨怨怨

员援源 系统安全性工程

员援源援员 系统安全性与传统的技术安全

系统安全性是从根本上提高工程系统安全水平的技术工作方法，是在企业传统的生产技术安全工作基础上发展起来的。面对系统日益复杂和伴随而来的事故发生可能性的增加，传统的技术安全工作，总是跟在事故后面跑，很难做到事故之前的系统分析，将事故防患于未然，这种状况不能适应现代化生产和现代工程系统发展的需要。

随着科学技术的发展，特别是系统分析方法的应用，人们从工程系统内部条件和外部环境出发，研究它们与安全问题的相互关系，掌握危险发生的规律，通过产品设计和规范使用操作来减少或控制危险，把事故发生的可能性降低到最小限度，促进了系统安全性工程的发展和应用。

系统安全性与传统的技术安全相比，主要区别如下：

（员）传统的技术安全的工作范围主要是在生产和使用场所能够保证操作人员和设备不致受到伤害或损坏，它并不直接涉及工程系统的设计（最多只是向设计反馈不安全因素）。而系统安全性则主要研究工程系统全寿命过程，包括方案论证、设计、试验、制造以及使用等方面的安全工作，并且重点在研制阶段。

（圆）传统的技术安全工作大多凭经验和直感来处理安全问题，而较少由表及里深入分析，从事物的相互联系去发现潜在危险，因而难以彻底改善安全状态。而系统安全性利用系统工程的方法，从系统、分系统和环境影响以及它们之间的相互联系来研究安全问题，从而能比较深入而全面地找到潜在危险和不安全问题，以预防事故的发生。

（猿）传统技术安全工作多从定性方面进行研究，一般只提出“安全”或“不安全”的概念，

对安全性没有定量的描述，因而难以作出准确的判断和评价，不便于控制和管理。而系统安全性利用危险严重性等级、危险可能性等级、危险事件发生概率以及人因可靠性指标来定量评价安全的程度，使预防事故的措施有了客观的度量。

(源传统的技术安全工作只是从局部的、零碎的或处于被动状态来解决安全问题的，因而不能从根本上提高安全水平。而系统安全性则从工程系统论证、设计起就开始作系统的安全性分析。它考虑到工程系统中所有可能的危险，如危险源、各分系统接口、软件对安全性的影响，并随着研制工作的进展，逐步细化安全分析的内容，使安全工作主动而全面地发挥最佳的作用。

(缘传统的技术安全工作目标值不明确、不具体，究竟做到什么程度才算安全问题解决得好，才能控制重大事故发生？这些问题目标不明，工作盲目性较大。而系统安全性通过安全性分析、试验、评价和优化技术的应用，可以找出最佳的减少和控制危险的措施，使工程系统各分系统之间，设计、制造和使用之间达到最佳配合，用最少的投资获得好的安全效果，从而有把握并在极大程度上提高工程系统安全水平。

综上可知，系统安全性分析在提高工程系统的安全性上有很大的发展和应用前景。目前由于人们认识的不足，各种数据缺乏，标准还不完善，安全性分析还只限用于一定的生产领域，系统安全性和传统的技术安全还需要分工协作。例如传统的技术安全在现场的统计资料是系统安全性定量研究的重要根据，控制危险的某些措施还有赖于技术安全的管理经验等。但随着系统安全性工作的普及与深入，必将使工业生产和工程系统使用安全水平得到更大的提高，而传统的技术安全工作也将得到改革。

员圆圆遥系统安全性工程与其他学科

系统安全性涉及设计、制造与使用维修各个方面，它与工程系统硬件和使用方面的软件(如操作规程)以及硬件和软件之间有着密切的关系。有害的环境和人为差错对工程系统的安全性有着直接影响。与安全性有关的专业技术主要有：设计工程、人素工程、可靠性工程、维修性工程、试验工程、制造工程、工业卫生和保健、质量检验和控制以及综合保障工程(其中包括：维修工程、使用维修人员培训、包装、贮存和运输等)，等等。系统安全性工程技术人员要把与安全性有关的这些专业中已做过的或将要做的有关安全性的工作(技术的和管理的)综合起来研究，以便在保证安全上形成全面和系统的见解和正确的结论。因此，系统安全性工程是最近新提出的并行工程中的一项专业工程。

员圆员设计工程

对系统安全性影响最大的是设计工程。产品设计的不完善或有缺陷将会造成人员伤亡、职业病、设备损坏或财产损失等事件发生，或不便于对已知危险进行有效的控制。设计方案本身可能引入较严重的潜在危险，如内燃机采用汽油还是柴油，前者发生火灾的概率比后者大；安全设计的计算错误会使产品发生灾难性的危险，如高压容器设计中的计算差错而发生爆炸等；产品上没有预防差错的设计将导致使用时发生事故等。

过去设计人员往往只重视产品的物理性能和功能，而对安全性问题多数是通过曾发生过类似或相近的事故的经验教训才逐步认识的。不同的设计人员所设计的产品的安全性水平差别较大，经过系统安全性技术人员的专门研究，提供了产品安全性设计准则，参加安全性设计评审，并协同或指导设计人员分析产品设计中的潜在危险，可大幅度减少设计中对安全性考虑

不周而造成的差错，能显著提高设计的安全性水平。

㈣人素工程

人素工程对系统安全性的贡献主要在于，研究工程系统与人的接口，防止由于人的原因（心理的、生理的以及人体外形量度的）造成的事故，消除由于不适应人员的要求而造成的职业病和伤亡。人素工程技术人员的工作包括分析产品的设计以尽量减少导致事故的人为差错；在制定安全操作规程上尽量减少可能产生偏离规定的操作程序；从人素工程的观点和要求鉴别设计图纸中的缺陷，提出更改建议等。

㈤可靠性工程

可靠性研究的对象是故障，安全性研究的对象是危险。故障和危险有时是等同的，例如工程系统的致命性故障也就是一种危险，但并非所有的故障均与危险有关。反过来，危险也不一定是由于故障造成的，例如在使用危险材料时，即使工程系统没有任何故障，也存在危险。所以说可靠性与安全性是密切相关但又有所区别的两门学科。

可靠性工程通过工程技术措施尽量减少工程系统的故障。虽然故障并非都与安全性有关，但当故障的后果会导致不安全时，可靠性问题也就是安全性问题。可靠性有时同安全性会有矛盾，例如，对某一功能来说，冗余设计可以显著地提高可靠性，但有时增加的部分会增加不安全因素，如某内燃机设有电起动与高压气体起动两套装置，保证了起动的可靠性，但增加了一种危险源，可能会降低安全性。

在研究系统的安全性时要全力找出影响安全性的故障，分析故障的安全性后果，然后提出纠正措施和建议。对于复杂工程系统可以从过去发生故障后导致事故的类似部件中分析原因，提高可靠性以减少或防止故障的发生；也可通过分析与安全性有关的关键件，改进其可靠性设计。

㈥维修性工程

维修性工程与系统安全性有两个接口：一是在产品设计中，保证硬件的结构和材料或工艺的设计不会由于保养和修理不当、装配的差错而引起事故；二是保证所设计的硬件不会因进行正常的维修作业而伤害维修人员。

㈦试验工程

系统安全性技术人员对工程系统研制生产的各项试验过程应作出安全性分析，以鉴别在试验中可能出现的危险。试验工程人员根据安全性分析的结果制定适当的防护措施，防止事故的发生，或改变试验程序，以保证安全。

试验工程人员除了试验产品的有关性能要求是否合格外，还要验证硬件、软件（包括规程）或环境中是否有潜在危险，研究对已有的危险控制是否完善，是否有未预见的危险；还应评价使用与维修的规程在安全上是否合理。

㈧制造工程

制造工程是以最小的费用和完善的制造计划生产出符合设计要求的产品为目的。制造计划主要包括：工艺设计及工艺规程的编制、工艺装置设计、生产设备（如机床、试验设备、自动生产线等）的选用和设计以及调试和检验、测试和检验的程序和标准、生产制造技术文件、人员培训与考核等。这些问题都对安全性有直接的影响。

设计人员和系统安全性技术人员都应考虑产品制造中有关安全性的问题。产品制造工程技术人员除了控制执行制造工艺本身的安全外（如焊接安全、机床操作安全等），必须了解与

安全性有关的零部件（包括安全性关键件及产品材料、工艺和环境对安全的影响），听取设计与安全性部门的意见，防止制造上的差错导致在生产和使用时发生事故。

(6) 工业卫生和保健

工业卫生和保健工作人员要熟悉工程系统、材料和环境（包括工业毒物、不良气象条件、生物环境以及不合理的劳动组织等）对人员身体健康的有害影响，收集现场已发生过的对人员健康有害影响的事例，向设计人员提出消除或控制这些影响的建议。

(7) 质量检验和控制

质检部门要防止或尽量减少生产有安全性缺陷的产品。设计与系统安全性技术人员必须将安全性关键件的主要要求通知质检人员，通常是在图纸或其他文件上作出专门的标注，以便制定详细的检查方法和指出在检查时特别要注意的问题，防止产品产生影响安全的缺陷。

(8) 维修工程

维修工程人员应保证所制定的工程系统维修计划在实际执行时符合安全性要求。预防性维修计划中所确定的预防性维修工作类型和维修间隔期要防止发生事故的故障。所制定的详细预防性和修复性维修规程中要有防止发生事故的措施。

(9) 使用和维修人员的教育

工程系统的硬件必须按规定的操作程序和要求使用与维修，这样才能保证安全。工程系统设计者拟定了符合安全要求的操作规程，使用和维修人员也要懂得这些要求的含义，按要求去操作。因此需要对操作者进行安全操作的教育。设计和系统安全性工作人员要提供安全性教育与培训的内容和基本要求，其中包括：工程系统安全性特点、安全操作规程、安全报警标志的识别与操作要求、演练时发生事故后的应急措施等。这些要求要准确，不含糊，不复杂并易于使操作者所接受。

(10) 包装、贮存和运输

设计人员和系统安全性人员应对产品包装、贮存和运输中有关安全问题（如大型设备起吊和搬运安全要求、化工品贮存安全规定、包装及容器安全要求等）拟定详细的规程，并将此规程向贮存、运输工作人员介绍，同时考虑工作现场的实际和工作人员的经验和意见，修改安全规程，以防止贮存和运输中发生事故。

系统安全性是一项系统工程，需要各方面的协调与合作，这样才能使工程系统获得经济而有效的安全性水平。

(三) 系统安全性大纲

为规范系统安全性工作和要求，采用科学和工程的方法进行系统安全性设计、分析评价与管理，使系统安全性工作有章可循。当前不少国家都制定并颁发了各自的有关系统安全性的国家或军用的标准文件——《系统安全性大纲》。如美国国防部 1969 年颁布的系统安全性大纲 MIL-STD-882 作为美军所有军事工程系统必须遵守的标准，在这项标准中完整地建立了系统安全性的概念、安全性分析、设计和评价的基本原则，以及工程系统全寿命周期内系统安全性工作的明确要求和规定。该标准自 1969 年颁发至今，已先后作过四次大的修改，是当前不少国家引用的比较成熟的系统安全性标准。

我国在 1984 年正式颁发了国家军用标准 GJB 900《系统安全性通用大纲》。它是我国工程系统安全性工作的顶层标准，其中规定了装备系统（包括装备硬件、软件、使用、保障以及有关