普通高等教育“十一五”国家级规划教材

系统安全评价与预测

（第2版）

陈宝智　编著

XITONG ANQUAN PINGJIA YU YUCE

冶金工业出版社
Metallurgical Industry Press

普通高等教育“十一五”国家级规划教材

系统安全评价与预测

（第2版）

陈宝智　编著

北　京
冶 金 工 业 出 版 社
2011

内 容 提 要

本书在介绍系统安全的基本理论、原则和观点的基础上，从两类危险源的概念出发，重点介绍了系统安全评价与预测的理论、原则和方法，以及反映该领域新进展的内容，如重大危险源辨识和评价、防护层分析和机能安全评价等。全书共7章，包括总论，伤亡事故统计及其预测，第一类危险源辨识、控制与评价，系统可靠性分析，系统安全分析，故障树分析以及系统安全评价。各章均附有思考题或练习题。

本书除可作为高等学校教材外，还可供相关专业的科研人员、工程技术人员及管理人员参考或职业技术培训之用。

图书在版编目（CIP）数据

系统安全评价与预测/陈宝智编著．—2版．—北京：冶金工业出版社，2011.2

普通高等教育“十一五”国家级规划教材

ISBN 978-7-5024-5480-7

Ⅰ.①系… Ⅱ.①陈… Ⅲ.①系统工程—安全工程—高等学校—教材 Ⅳ.①X913.4

中国版本图书馆CIP数据核字（2011）第006235号

出 版 人 曹胜利

地 址 北京北河沿大街嵩祝院北巷39号，邮编100009

电 话 (010)64027926 电子信箱 yjcbs@cnmip.com.cn

责任编辑 马文欢 美术编辑 李 新 版式设计 孙跃红

责任校对 卿文春 责任印制 牛晓波

ISBN 978-7-5024-5480-7

北京百善印刷厂印刷；冶金工业出版社发行；各地新华书店经销

2005年10月第1版，2011年2月第2版，2011年2月第1次印刷

787mm×1092mm 1/16；11.25印张；299千字；168页

26.00元

冶金工业出版社发行部 电话：(010)64044283 传真：(010)64027893

冶金书店 地址：北京东四西大街46号(100010) 电话：(010)65289081(兼传真)

第 2 版前言

本书是根据普通高等教育“十一五”国家级规划教材出版计划，根据最新“系统安全评价与预测”课程教学大纲的要求，在普通高等教育“十五”国家级规划教材《系统安全评价与预测》的基础上，修订编写而成的。

本书第 1 版出版以来的几年里，我国转变经济发展方式，调整产业结构，进一步把经济发展建立在安全生产有可靠保障的基础上，安全生产形势发生了很大变化。建设本质安全型企业、实现本质安全逐渐成为人们的共识。国家相继制定和实施了一系列贯彻落实《中华人民共和国安全生产法》的政策、法规、技术标准。广泛开展的劳动安全卫生预评价、验收评价以及各种专项安全评价，推动了系统安全评价与预测的研究和实际应用。特别是，近年来在我国，重大危险源控制问题受到了空前的重视，国家颁布了新的重大危险源辨识的国家标准《危险化学品重大危险源辨识》（GB 18218—2009），取代原有的《重大危险源辨识》（GB 18218—2000），使之更适合中国的国情；政府和企业建立并不断完善针对重大工业事故的事故应急救援体系，制定事故应急救援预案。在编制事故应急救援预案时和实施事故应急救援过程中，往往需要定量地预测重大工业事故的影响范围和可能的人员伤亡、财产损失和环境污染情况，相应地，重大工业事故后果分析被越来越广泛地用于安全工程实践。

系统安全评价与预测在安全工程实践中不断发展，新理论、新方法不断涌现。经过几十年的发展，作为系统安全工程重要内容的危险源控制技术日臻成熟，本质安全设计、防护层和安全相关系统的功能安全等安全技术理念和原则被越来越多地应用于系统安全工程实践，形成了危险源控制的安全技术体系。系统安全评价包括对危险源的危险性的评价和对危险源控制措施效果的评价。相应地，系统安全评价又增加了本质安全评价、防护层分析和安全相关系统功能安全评价等危险源控制措施效果评价方面的新内容。系统安全评价与预测技术本身也有了新发展，在原来的定性危险性评价和概率危险性评价的基础上，定性评价与定量评价相结合的半定量危险性评价成为系统安全评价技术的新

趋势。

安全工程实践有了新需求，系统安全评价与预测理论和方法有了新发展。根据最新“系统安全评价与预测”课程教学大纲，在第1版介绍系统安全评价与预测基本理论、原则和方法的基础上，本书增加了重大工业事故后果分析定量计算的主要数学模型，以及本质安全设计、防护层分析和安全相关系统的功能安全评价等危险源控制措施效果评价等方面的内容，并采用了最新的政策规定和技术标准。

本书吸取了东北大学安全工程专业教师们多年来在讲授该课程中积累的宝贵经验；张培红教授，毛宁、林秀丽、苑春苗、郭尹亮等诸位博士参与了本书编写并根据教学过程中发现的问题提出了修改意见，使本书更臻完善。本书参考、引用了大量国内外文献资料。在此向诸位老师们、文献作者们表示诚挚的谢意。

作　者

2010年12月

第 1 版前言

“系统安全评价与预测”是安全工程专业的主要专业课程之一。本书在介绍系统安全的基本理论、原则和观点的基础上，重点介绍了系统安全评价与预测的理论、原则和方法。

系统安全是为了解决大规模复杂系统安全性问题而产生的理论、原则和方法体系，与以往的安全工程理论相比，在安全观念和方法论方面有许多创新，丰富和发展了安全工程的理论和方法。例如，它认为系统中存在着的危险源是事故发生的原因，人类的任何活动都存在着潜在的危险，安全只是一个相对的、主观的概念，所谓的安全是一种可以被人们接受的危险；它的一个基本原则，是从一个新系统构思、可行性研究阶段开始，直到系统报废为止的整个系统寿命期间内，都要辨识危险源、预测系统事故并采取相应措施控制危险源，评价其危险性是否在可接受的范围内。于是，事故预测与系统安全评价就成为系统安全工程的重要内容。事故预测与系统安全评价紧密地联系在一起，相辅相成。根据系统内存在危险源的情况预测可能发生的事故；通过对系统内危险源的危险性评价以及对危险源控制措施的评价，定量地预测事故发生的可能性，以及一旦发生事故时其后果的严重程度。

随着系统安全评价与预测的理论在实践中不断发展，新理论、新方法不断涌现，课程知识体系有了较大的变化，原有的教材内容已经不能适应教学的要求。为了适应新的教学要求，及时反映本学科的最新科研成果，满足工程领域的需求，笔者根据新的“系统安全评价与预测”课程教学大纲和工程实际应用的需要，在系统总结多年来的教学经验和科研成果的基础上，编写了本书。

编写过程中，在将系统安全评价和预测基本知识加以系统化的同时，增加了一些反映该领域新进展的内容，如两类危险源的概念，重大事故危险源的辨识和评价等。系统安全预测与评价具有很强的实践性，它产生于安全工程实

践，并在实践中不断发展。本书在介绍理论、原则和方法的同时，注意了可操作性的问题。书中除了引用一些典型例子之外，每章还附有一些练习题和思考题，以帮助学生学习运用这些理论、原则和方法。

本书汲取了东北大学安全工程专业教师们二十多年来在讲授该课程中积累的宝贵经验，参考、引用了大量的国内外文献。张培红、李刚、钟茂华、肖国清等博士参与了本书的编写，并根据教学过程中发现的问题提出了修改意见，使得内容更臻完善。在此谨向诸位同事、文献作者表示诚挚的谢意。

由于本人学识所限，书中有不当之处，敬请读者批评指正。

作　者

2005年6月

目　录

1 总　论

1.1　系统安全评价与预测概述

我们生活在一个充满“危险”的现实世界中。安全工程领域涉及的危险，主要是人们在生产活动和生活活动中意外发生的各种事故造成的人员伤亡、财产损失或环境污染的危险。面对这些危险，人们做出种种努力回避危险而追求安全。相应地，安全工作的根本目的就是防止事故和事故造成的人员伤亡、财产损失或环境污染。

为了防止事故，需要预测事故；只有预测了事故，才能有针对性地采取措施防止事故发生。

人们希望充分利用已有的科学技术知识认识事故发生规律，在事故发生前预测事故的发生和事故可能造成的后果，从而先行采取措施防止事故发生，或者在一旦发生事故的场合最大限度地避免、减少人员伤亡、财产损失或环境污染。

很久以来，人们在事故预防方面，基本上是“从事故学习事故”，即分析、研究以往事故发生的原因和总结防止事故的经验，来得到预测这些种类事故再发生的知识，指导事故预防工作。例如，根据人员操作机器时曾经发生机械伤害事故的经验，人们可以预测机械工厂里发生机械伤害事故的可能性。在民用航空领域，曾经采用了“飞行—修改—飞行（fly—fix—fly）”模式，根据发生的事故经验修改设计，防止由于同样的原因再引起事故。

这种“从事故学习事故”的方式在一定程度上是科学的、必要的，在今后的事故预防工作中仍然要继续采取这种方法。然而，事故是一种随机发生的小概率事件，依靠事故后留下的有限信息来分析、研究其发生原因是一件非常困难的工作。这种根据“从事故学习事故”的方式进行的预测只能是定性的，即对未来事故发生可能性的预测。

随着科学技术的迅速进步，新材料、新能源、新技术、新工艺、新产品不断涌现，新种类的事故发生的可能性和事故后果的严重程度也在增加。事故的经验往往是人们用鲜血和生命换来的，其代价是非常昂贵的。人们不能等到发生事故、造成严重人员伤亡及财产损失或环境污染之后才来总结经验，研究预防事故的办法。

事故会造成损失，预防事故也需要成本，安全也有投入和产出的问题。为了科学、经济合理地预防事故，人们已经不满足于对事故发生可能性的定性预测，还希望能够定量地预测事故的发生及其后果，评价系统的安全状况是否符合人们期望的标准。这就需要新的事故预测和安全评价的理论和方法。

20 世纪 60 年代出现的系统安全工程为我们提供了系统的、定量的事故预测和安全评价的理论和方法。在系统安全工程中，事故预测与系统安全评价紧密地联系在一起，相辅相成：根据系统内存在危险源的情况预测可能发生的事故；通过对系统内危险源的危险性评价，以及对危险源控制措施的评价，定量地预测事故发生可能性以及一旦发生事故时其后果的严重程度。

1.1.1　系统安全评价与预测的产生

系统安全评价与预测是系统安全工程的基本内容之一，与系统安全工程同时产生和发展。

20 世纪 50 年代以后，科学技术进步的一个显著特征是设备、工艺和产品越来越复杂。战略武器研制、宇宙开发和核电站建设等使得作为现代先进科学技术标志的大规模复杂系统相继问世。这些复杂的系统往往由数以千万计的元件、部件组成，元件、部件之间以非常复杂的关系相连接；在它们被研制及使用的过程中常常涉及高能量。系统中的微小差错就会引起大量能量的意外释放，导致灾难性的事故，“蝼蚁之穴”可毁千里长堤。这些大规模复杂系统的安全性问题受到了人们的关注。

在开发研制、使用和维护这些大规模复杂系统的过程中，逐渐萌发了系统安全的基本思想。作为一种现代安全工程理论和方法体系的系统安全，起源于 20 世纪 50～60 年代美国研制 Atlas 和 Titan 洲际导弹的过程中。

20 世纪 50～60 年代，导弹推进剂是由气体加压到 41.2MPa，温度低达 -196℃ 的低温液体。这种推进剂的化学性质非常活泼且有剧毒，其毒性远远超过战争中使用的毒气，其破坏性比烈性炸药更猛烈，其腐蚀性超过工业生产中使用的腐蚀性化学物质。负责该研制项目的美国空军官员们开始并没有认识到他们着手建造的导弹系统潜伏着巨大的危险性。在洲际导弹试验的头一年半里就发生了四次爆炸，造成了惨重的损失。在此之前，美国空军曾发生许多飞行事故。一般地，空军官员们都把事故的原因归于飞行员的操作失误。但是由于导弹上没有飞行员，爆炸完全是由于导弹自身的问题造成的，而不能再把导弹爆炸的责任推到驾驶员身上。很明显，分析爆炸原因应该追究导弹投入试验之前的构思、设计、制造和维护等方面的问题。以此为契机，美国开始了系统安全方面的研究。

此前，没有可以用来解决这些复杂系统的安全性的方法。为此，人们做了许多工作来开发防止系统发生事故的方法。新方法被一个一个地开发出来了，新概念逐渐产生了；安全工程原有的概念和方法中正确的部分被保留和改进了，其他领域许多有用的科学技术和工作方法被吸收进来，形成了系统安全的理论、原则和方法体系。其中，系统安全工程则是实现系统安全的手段。

系统安全工程首先在美国空军内应用之后，又被推广到美国陆军和海军。1969 年美国国防部颁发《系统安全大纲要求》，即 MIL-STD-882 标准，详细规定了武器系统开发研究、生产制造和使用、维护的系统安全标准。1984 年颁发了修订版 MIL-STD-882B，1993 年和 2000 年又相继颁布了 MIL-STD-882C 和 MIL-STD-882D。该标准对系统安全的实施和要求做了全面的规定，建立了系统安全的完整概念，给出了系统安全分析、设计、评价的基本原则、内容及要求，提出了定性的系统安全评价方法，是系统安全产生和发展的一个重要标志。

在这一阶段，人们研究开发了许多以系统可靠性分析为基础的系统安全分析方法，可以定性或定量地预测系统故障或事故。

此后，系统安全工程进入航空航天及核工业等领域，系统安全评价与预测进入了一个新的发展阶段。

1.1.2 概率危险性评价

自工业革命以来，长期困扰工业界的一个问题是“How safe is safe enough”，系统安全工程的概率危险性评价使得这个问题的定量解决成为可能。

在核电站系统安全工程的研究和应用方面，美国麻省理工学院的拉氏姆逊（N. C. Rasmussen）教授从 1972 年起，由美国原子能委员会出资 300 万美元，花费 50 人·年的工作量，完成了萨里（Sarrey）核电站和桃花谷（Peach bottom）核电站的概率危险性评价。该研究在没有核电站事故先例的情况下预测了核电站事故，应用事件树分析和故障树分析等系统

安全分析方法建立了核反应堆事故模型，并输入各种故障率数据进行了概率危险性评价。1975年美国原子能委员会发表了题为《美国商用核电站事故危险性评价》的安全研究报告，即WASH 1400（NUREG 701014）。

拉氏姆逊的研究报告曾在美国国内引起核电站支持者和反对者之间的激烈争论。但是，不久后发生的三哩岛核电站事故证明，该研究采用的系统安全分析方法和概率危险性评价方法是正确的。美国原子能委员会于1980年发表了《核电站安全目标》，于1981年出版了《概率危险性评价指南》。之后，系统安全工程以及概率危险性评价受到世界各国的重视。

继核工业领域应用之后，概率危险性评价被成功地应用于化学工业和石油化学工业领域。1976～1978年间，英国原子能机构就坎维岛（Can Vey）化学和石油化学工业安全性问题进行了概率危险性评价。此次评价由于是概率危险性评价在非核领域的首次应用，引起了科技界人士的极大兴趣，也受到工业界一些人士的怀疑。1981年，英国健康与安全委员会（HSE）进行了复评，肯定了评价结果，认为概率危险性评价是一种有效的决策辅助工具。

目前，航空航天以及海上石油等领域已经广泛地应用概率危险性评价。

1.1.3 重大工业事故预防

随着化学工业、石油化学工业的发展，大量易燃易爆、有毒有害的物质相继问世。它们作为工业生产的产品或原料在被生产、加工处理、储存运输过程中一旦发生事故，其后果非常严重。特别是20世纪70年代以后，世界范围内发生了许多震惊世界的重大火灾、爆炸、有毒有害物质泄漏事故。这些事故的共同特点是，事故造成的人员伤亡、物质损失、环境污染非常严重，其影响范围往往超出工厂的围墙，威胁公众安全，甚至威胁邻国居民安全。因此，防止重大工业事故问题受到世界各国的广泛关注。

可能引起重大工业事故的危险源被称为重大危险源，一些欧洲国家较早地提出了重大危险源控制的问题。

1974年，英国的弗利克斯保罗（Flixborough）工厂发生了环已烷蒸气云爆炸事故，使28人丧生、89人受伤、2450幢房屋损坏，直接经济损失达700万美元。以此次事故为契机，英国健康与安全委员会（HSE）建立了重大危险源咨询委员会，进行重大危险源控制和立法方面的咨询。

1976年，意大利的塞维索（Seveso）工厂和曼福莱多尼亚（Manfredonia）工厂发生大量毒物泄漏事故。塞韦索工厂的环已烷泄漏使30人受伤、22万人疏散。面对频繁发生的重大工业事故，原欧共体于1982年颁布了《关于工业活动中重大事故危险源的指令》，简称《塞韦索指令》，要求各加盟国、行政监督部门和企业等承担在重大工业事故控制方面的责任和义务。例如，要求企业必须提出安全报告，让企业自己了解自身的危险性。最初，该指令把重点放在掌握化工企业危险物质的储存量和识别设备、工艺异常上，后来扩展到核电站安全、环境污染控制等方面问题。1996年欧盟颁布了新版的《Seveso指令Ⅱ》。

世界其他地区也相继发生了一些重大工业事故。例如，1984年墨西哥城发生石油液化气爆炸事故，使650人丧生、数千人受伤；1984年印度的博帕尔农药厂发生甲基异氰酸盐泄漏，导致2000人死亡、2万人受伤。我国曾发生了黄岛油库火灾、南京炼油厂火灾和吉林双苯厂爆炸等重大工业事故。

1988年国际劳工局（ILO）颁发了《重大工业事故控制指南》，指导各国的重大危险源控制工作。

到1991年，原欧共体各加盟国都已经把塞韦索指令移植到国内法律中。例如，英国首先

颁布了《重大工业事故防止法》，要求企业提出包括定量分析在内的内部报告和外部报告；意大利规定，如果安全报告有不实之处，企业负责人将被处以包括监禁在内的重罚。

1993 年国际劳工局通过了《预防重大工业事故公约》。该公约要求各成员国必须采取措施控制重大危险源。

在重大工业事故危险源控制实践中，系统安全评价与预测又有了许多新发展。例如，适用于化工生产那样工艺过程危险源辨识的危险性与可操作性研究，适用于重大危险源评价的火灾爆炸指数法、事故后果分析等。

系统安全工程作为现代安全工程的标志，越来越广泛地应用于安全工程的各个领域，并在实践中不断发展、完善。

1.1.4 中国的系统安全评价与预测

中国自 20 世纪 70 年代末、80 年代初开始了系统安全评价与预测的研究和应用，并将其与工业安全的理论、方法紧密结合，使得原本为解决大规模复杂系统安全性问题的系统安全工程迅速在工业安全领域推广和普及。

改革开放以来，国家十分重视安全工作，在贯彻“安全第一，预防为主”安全生产方针、加强安全管理的同时，注重采用先进安全科学技术，“安全是科学”逐渐深入人心。改革开放政策也为学习国外先进安全科学技术打开了方便之门，国内一些院校、研究所开始介绍、研究系统安全工程，并把系统安全工程用于一般工业安全领域。

最初的研究主要集中在作为危险源辨识方法的各种系统安全分析方法方面，预测可能发生的事故，应用故障树分析、事件树分析等方法分析事故发生原因，进行定性的安全评价，指导事故预防工作。一些行业、部门、地区有组织地推广，使得系统安全分析方法迅速普及。许多企业的安全专业人员都能够应用故障树分析等方法进行事故原因分析。一些企业，如鞍山钢铁公司等，结合中国企业安全工作的实际情况，开展了群众性的危险源辨识、评价和控制工作。

20 世纪 80 年代中期，一些行业，如机械、化工等行业，开展了群众性的安全评价工作，其中包含了系统安全性评价；一些化工、石化、医药企业应用火灾爆炸指数法进行了系统安全评价；核工业、海上石油等工业领域开展了概率危险性评价。

我国群众性的系统安全工程实践推动了系统安全工程研究的不断深入，使故障树分析与合成，危险源辨识、评价理论和方法等方面的研究取得很大进展。特别是，在国家“八五”计划期间，国内进行了题为“重大危险源宏观控制技术研究”的科技攻关，开始了重大事故后果分析以及针对重大危险源的系统安全评价与预测，推动了我国的重大危险源辨识、评价和控制研究工作。2002 年颁布的《中华人民共和国安全生产法》，对控制重大危险源做了明确规定。

目前，系统安全评价与预测在我国核工业、航空航天、海上石油、矿业、冶金、化工、机械、电力、建筑等各工业领域都得到了广泛应用。

我国正在企业中推广建立职业健康管理体系工作，现代职业健康管理体系的核心就是危险源辨识、评价和控制。

近年来，根据政府法令的要求，我国广泛开展了建设项目的劳动安全预评价、验收评价，以及各种专项安全评价，如危险化学品专项安全评价、矿山专项安全评价等，使系统安全评价走上了法制的轨道。

1.2 系统安全与系统安全工程

1.2.1 系统的基本概念

系统是由相互作用、相互依存的若干元素组成的具有特定功能的有机整体。

一部机器是由若干零部件组成的可以实现一定生产目的的有机整体，可以被看做是一个系统。由机器、工具、材料和人员组成的生产作业单元可以被看做是一个系统。由若干生产作业单元组成的班组，由若干班组组成的车间，由若干车间组成的工厂也可以分别被看做系统。

系统的基本特征是具有整体性、层次性、目的性和适应性等。

（1）整体性。系统是由若干不同元素组成的、具有特定功能的有机整体。系统的功能不是各元素功能的简单叠加，而是由元素之间相互作用产生的一种新的整体功能。元素在系统中的作用是由系统整体规定的，为实现系统的整体功能服务的。元素一旦离开了系统就失去了它在系统中的作用，也就不再是系统的元素了。

（2）层次性。一个系统是一个有机的整体，具有一定的功能。一个系统可以分割成若干较小的部分，这些较小的部分也是一个有机的整体，具有一定的功能，也是一个系统，它是原系统的子系统。依次，子系统又可分割成更小的子系统，一直分割到元素为止。例如，工厂可以划分为车间，车间是工厂这个系统的子系统；车间可以划分为班组，班组是车间的子系统等。由于系统具有层次性，在进行系统安全分析时可以把系统分割为若干子系统再分析。

（3）目的性。系统具有特定的功能和特定的目的，为了实现其特定的目的而把元素组织起来形成系统。

（4）适应性。任何系统都存在于一定的环境之中，与环境间进行能量、物质和信息的交换。系统的适应性是指系统通过自我调节适应环境变化的性质。

研究系统需要利用系统论方法。系统论方法的显著特征是强调整体性、综合性和最优化。

（1）整体性。系统是具有特定功能的有机整体，系统的构成应该保证其整体功能的发挥，实现系统的整体目标，各个子系统、元素都应该为系统的整体目标服务，服从整体目标。

（2）综合性。从系统元素、系统构造、元素间联结方式等多方面进行综合研究。

（3）最优化。根据需要和可能，定量地确定系统性能的最优目标，然后动态地协调系统与子系统、元素间的关系，使子系统、元素的性能和目标服从系统的最优目标，实现系统的最优。

1.2.2 系统安全的定义

系统安全是人们为解决复杂系统的安全性问题而开发、研究出来的安全理论、原则、方法体系。所谓系统安全，是在系统寿命期间内应用系统安全工程和管理方法，辨识系统中的危险源，并采取控制措施使其危险性最小，从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。

系统安全主张在系统的早期阶段预测、控制危险源。系统安全的一个基本原则是安全工作贯穿于系统的整个寿命期间，即早在一个新系统的构思阶段就必须考虑其安全性问题，制定并开始执行安全工作规划，进行系统安全工作，并把系统安全工作贯穿于整个系统寿命期间，直到系统报废为止。

该项原则充分体现了系统安全的重要特征：安全工作不仅仅是在系统运行阶段进行，而是

贯穿于整个系统寿命期间。也就是说，在新系统的构思、可行性论证、设计、建造、试运转、运转、维修直到废弃的各个阶段都要辨识、评价、控制系统中的危险源。特别是在新系统的构思、可行性论证和设计阶段进行的系统安全工作，包括预测新系统中可能出现的危险源及其危害，通过良好的工程设计消除或控制它们，更能体现预防为主的安全工作方针。

从安全科学理论的角度，系统安全包含许多创新的安全观念。

（1）没有绝对安全。长时间以来，人们一直把安全和危险看做截然不同的、相互对立的事情，认为某一事物或者安全或者危险，没有中间状态。许多词典里把安全一词解释为“没有危险的状态”；在日常安全工作中把安全理解为“不会发生事故，不会导致人员伤害或财物损失的状态”。系统安全与以往的安全观念不同，认为世界上没有绝对安全的事物，任何事物中都包含不安全的因素，具有一定的危险性，安全只是一个相对的概念。

一个工厂、一个生产过程在一段时间内可能没有发生事故，但是却不能保证永远不发生事故。事故是一种出乎人们意料之外的事件，其发生与否并不取决于人的主观愿望。“事故为零”只能是安全工作的奋斗目标，通过安全工作的艰苦努力使事故发生间隔时间尽可能延长，使事故发生率逐渐减少而趋近于零，却永远不能真正达到事故为零。平时人们说某工厂、某生产过程安全时，是把它与本厂某阶段或其他不安全的工厂、生产过程相比较而言的。“安全的”工厂、生产过程并不意味着已经杜绝了事故和事故损失，只不过相对地事故发生率较低，事故损失较少并在允许限度内而已。

既然没有绝对的安全，系统安全所追求的目标也就不是“事故为零”那样的极端理想的情况，而是达到“最佳的安全程度”，一种实际可能的、相对的安全目标。

安全是相对的，危险是绝对的。所谓安全，就是没有超过允许限度的危险，也就是发生事故、造成人员伤亡或财物损失的危险没有超过允许的限度。这里的“允许的限度”是人们用来判别安全与危险的基准。

（2）危险源是事故发生原因。系统安全认为，系统中存在的危险源（hazard）是事故发生的根本原因。按定义，危险源是可能导致事故的潜在的不安全因素。系统中不可避免地会存在着某些种类的危险源。系统安全的基本内容就是辨识系统中的危险源，采取措施消除和控制系统中的危险源，使系统安全。

危险性（risk）是指某种危险源导致事故、造成人员伤亡或财物损失的可能性。一般地，危险性包括危险源导致事故的可能性和一旦发生事故造成人员伤亡或财物损失的后果严重程度两个方面。在定量地描述危险源的危险性时，采用危险度作为指标；在概率地评价危险源的危险性时，一般认为危险度等于危险源导致事故的概率和事故后果严重度的乘积。

在控制系统中的危险源方面，道格拉斯曾经提出了有名的系统安全三命题：

1）不可能彻底消除一切危险源和危险性；

2）可以采取措施控制危险源，减少现有危险源的危险性；

3）宁可降低系统整体的危险性，而不是只彻底地消除几种选定的危险源及其危险性。

由于人的认识能力有限，有时不能完全认识系统中的危险源及其危险性；即使认识了现有的危险源，随着科学技术的发展，新技术、新工艺、新能源、新材料和新产品的出现，又会产生新的危险源。对于已经认识了的危险源，受技术、资金、劳动力等诸多因素的限制，完全根除也是办不到的。因此，系统安全的目标是努力控制危险源，把后果严重的事故的发生可能性降到最低，或者万一发生事故时，造成的人员伤亡和财产损失最少。

（3）本质安全。系统安全强调通过良好的工程设计实现本质安全（inherent safety），即系统固有的（building in）安全而不是附加的（adding to）安全。