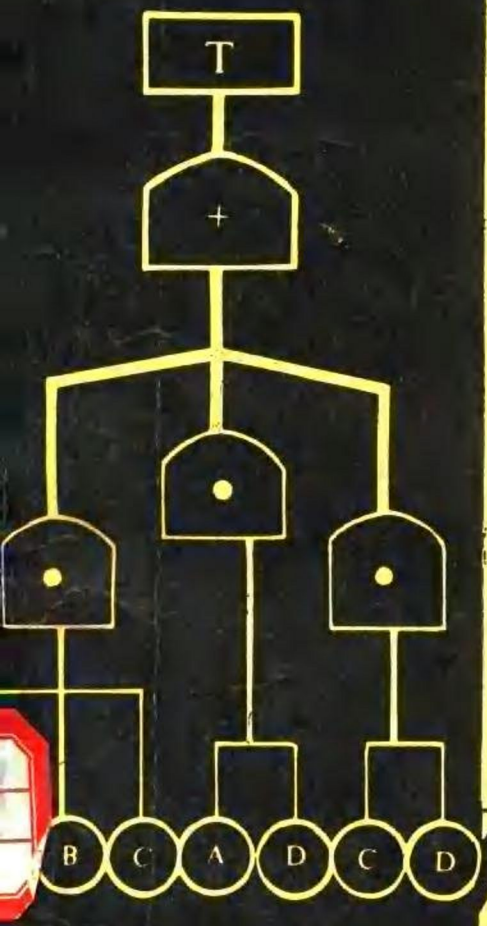
安全系统工程

冯肇瑞 崔国璋 编



冶金工业出版社

安 全 系 统 工 程

冯肇瑞　　崔国璋　　编

冶 金 工 业 出 版 社

内 容 提 要

本书介绍了安全系统工程这一新兴学科。

全书共分十章。书中着重阐述了安全系统工程的由来和发展，介绍了各种分析方法及其在安全工作中的应用，还就安全评价作了论述。主要内容包括：安全检查表，危险性预先分析，故障类型和影响分析，事故树分析，事件树分析，因果分析和可操作性研究等。书后附有安全系统工程常用名词术语解释。

本书适合安全技术干部、劳动保护干部、设计和生产人员阅读，也可供大专院校安全工程专业师生参考。

安 全 系 统 工 程

冯肇瑞 崔国璋 编

*

冶金工业出版社出版
（北京北河沿大街嵩祝院北巷39号）
新华书店北京发行所发行
冶金测绘印刷厂印刷

*

850×1168 1/32 印张 $9\frac{3}{8}$ 字数 246 千字

1987年6月第一版 1987年6月第一次印刷

印数00，001～25，200册

统一书号：15062·4546 定价1.75元

序

安全系统工程是近年来发展起来的新学科，它采用系统工程的方法、分析、评价生产过程中的不安全因素，预先采取措施防止重大灾害和人身伤亡事故的发生。事实证明，这种方法问世以来，事故本身变成了一个可以进行研究、预测和分析的带有规律性的事物，打破了事故不可知论的老概念，从而使控制事故成为可能，给传统安全的改革开辟了新途径，也给安全和劳动保护工作带来了很大的活力。

我国推广安全系统工程已经有好几年了，不少企业结合本厂实际，在传统安全管理工作的基础上，采用安全系统工程方法，取得了可喜的成绩，使企业的安全面貌有了改善，管理水平有了较大幅度的提高。大家认为，安全系统工程确实是搞好安全和劳动保护工作，降低伤亡事故和生产资料损失的有力武器之一。

几年来全国各地纷纷举办安全系统工程训练班，将近上万个企业进行了或正在进行试点。本书是在几年讲课的基础上，结合现场试点经验，比较系统地介绍了安全系统工程中的各种方法，特别偏重实际的应用方面，以供各地推广此项技术之用。

全书由冯肇瑞、崔国璋编写。第一章至第五章、第九章至第十章由冯肇瑞编写；第六章至第八章由崔国璋编写。

由于编者水平有限，错误之处在所难免，希读者不吝指教为幸。

编者

1986年7月

目　录

第一章　安全系统工程概论…… 1
第一节　安全系统工程的定义…… 3
第二节　安全系统工程的发展过程…… 6
第三节　安全系统工程的内容…… 7
第四节　安全系统工程在安全工作中的应用…… 9
第五节　安全系统工程的优点…… 10
第六节　我国推广安全系统工程的现状…… 11
第二章　系统安全分析方法…… 13
第一节　关系比较密切的分析方法…… 14
第二节　有许多共同点的分析方法…… 17
第三节　根据逻辑方法进行分析的方法…… 19
第四节　如果……怎么办的分析方法…… 23
第五节　其他的分析方法…… 25
第六节　如何选用分析方法…… 27
第三章　安全检查表…… 28
第一节　安全检查表的定义…… 28
第二节　安全检查表的内容要求…… 29
第三节　安全检查表的编制…… 31
第四节　安全检查表示例…… 31
第四章　危险性预先分析…… 54
第一节　危险性预先分析的分析步骤和分级…… 54
第二节　辨识危险性…… 56
第三节　危险性控制…… 59
第四节　分析实例…… 62
第五章　故障类型和影响分析…… 65
第一节　基本原理…… 65
第二节　分析步骤…… 75

第三节　致命度分析…… 76
第四节　应用实例…… 77
第六章　事故树分析…… 88
第一节　概念和定义…… 88
第二节　事故树的分析步骤…… 89
第三节　事故树的符号及其意义…… 92
第四节　事故树作图…… 99
第五节　布尔代数及运算定律简介……108
第六节　概率及计算公式……114
第七节　利用布尔代数化简事故树……118
第八节　最小割集及其求法……122
第九节　最小径集及其求法……126
第十节　最小割集和最小径集在事故树分析中的作用……129
第十一节　结构重要度分析……132
第十二节　基本事件的发生概率……139
第十三节　利用事故树结构函数计算顶上事件发生概率……146
第十四节　利用最小割集计算顶上事件发生概率……147
第十五节　利用最小径集计算顶上事件发生概率……150
第十六节　化相交集合为不交集合理论在事故树分析中的应用……153
第十七节　顶上事件发生概率的近似算法……157
第十八节　概率重要度分析……162
第十九节　临界重要度分析……165
第二十节　事故树分析应用示例……167
第七章　事件树分析……174
第一节　事件树分析的依据和在可靠性工程中的应用…174
第二节　事件树分析方法及应用……177
第八章　因果分析……183

第一节 因果图……183
第二节 分析与评价……183
第九章 可操作性研究……190
第一节 基本原理……191
第二节 分析步骤……194
第三节 应用实例……197
第十章 安全评价……202
第一节 安全评价的内容……204
第二节 安全评价的现实意义……267
附录 1 安全系统工程名词术语……274
附录 2 危险化学品的物质系数［MF］表……280
参考文献……291

第一章　安全系统工程概论

安全系统工程，是以系统工程的方法研究、解决生产过程中的安全问题，预防伤亡事故和经济损失发生的一个新技术学科。

众所周知，安全问题是随着生产的产生而产生，随着生产的发展而发展的。十八世纪工业革命以来，由于使用了蒸汽机，每年锅炉爆炸带来成千人的死亡。二十世纪上半叶，资本主义迅速发展，工业规模不断扩大，煤矿、水运、堤坝、土建、化工等工程往往一次发生数百人甚至上千人的重大伤亡事故。生产条件的恶化，工伤事故和职业病日益严重，引起了人们的广泛关注。国际劳工局（ＩＬＯ）于1919年成立，开始组织国际范围内预防事故的情报交流和制订工业安全卫生法规，从而安全技术逐步形成了一个综合性学科。

二次世界大战以后，工业的技术水平和生产规模又有了提高，核能、航天等尖端工业，大型石油、化工、冶金等重工业，事故越来越频繁，公害越来越严重。事故和公害发生后，企业损失巨大，舆论强烈不满，从而成为很大的社会问题。

通过多年的实践，人们总结出对付事故的两种办法。

其一是事故发生后吸取经验，进行预防的方法，有人也叫作“问题出发型”方法。例如从事故后果查找原因，采取措施防止事故重复发生。通常我们所采取的各种组织和技术措施，如设立专职机构，制定立法标准，进行监督检查和宣传教育等，以及防尘排毒、防火防爆、安全防护设备、个人防护用具等，都属此类。这就是我们所说的传统安全工作方法。

另一个是用系统工程控制事故的方法，有人也叫作“问题发现型”方法。这种方法是从系统内部出发，研究各构成部分存在的安全联系，检查可能发生事故的危险性及其发生途径，通过重新设计或变更操作来减少或消除危险性，把发生事故的可能降低到最小限度。这就是近二十年来发展起来的安全系统工程方法。

传统安全工作法虽然为防止伤亡事故做出了并正在做出重大的贡献，但也存在一些问题。如安全工作总是跟在生产后面跑，说是防患于未然，实际上很难做到。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？主要原因在于：

一是安全的属性问题，由于安全是依附于生产而存在的，生产中如果不发生事故，则往往引不起人们的注意，看不到安全工作的作用，觉得搞不搞安全也没有什么了不起，不仅企业领导人甚至工人本身也有这种思想。

二是由于工业技术不断地进步和发展，人们对新技术中许多潜在性的危险因素还认识不清，没有意识到发生事故后的严重后果。

三是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才感觉出它的存在，这就减少了人们对它进行深入研究的兴趣。

这些因素导致了安全工作方法的局限性，主要表现在：

（1）凭经验和直感处理生产中的安全问题多，而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。

（2）定性的即“安全”或“不安全”的概念多，而定量的概念少。如生产的安全性多大？事故发生的可能性有多少？有多大的严重后果？都无法回答，不能给人以实质性的概念。

（3）由于没有系统性，所以解决安全问题时总是片断地和零碎地进行，头痛医头、脚痛医脚，而系统地、全面地解决问题少。

（4）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？才能控制重大事故？心中无数，有很大的盲目性。

总之，传统安全工作方法越来越不能适应生产的发展，有必要改进，很多有识之士已经注意到了这一点。

我国在解放前，由于“三座大山”的压迫，加上工业技术落后，根本无劳动保护和安全工作可言。只是在解放后，这项工作才真正开始。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；1956年，国务院相继颁布了三大规程（工厂安全卫生规程，建筑安装工程安全技术规程和工人职员伤亡事故报告规程）和劳动保护有关法令，健全了安全机构，加强了安全工作，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，安全工作虽然取得了巨大的成绩，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生产发展要求的问题。

多少年来，人们特别是安全工作者总想找到一个办法，能够事先预测到事故发生的可能性，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、管理中对发生事故的危险性加以辨识，并且能够根据对危险性的评价结果，提出相应的安全措施，达到控制事故的目的。安全系统工程学就是为了达到这个目标而发展起来的。

第一节　安全系统工程的定义

什么是安全系统工程？安全系统工程的定义是：采用系统工程方法，识别、分析、评价系统中的危险性，根据其结果调整工艺、设备、操作、管理、生产周期和投资等因素，使系统可能发生的事故得到控制，并使系统安全性达到最好的状态。

为什么要用系统工程方法来研究和处理安全问题呢？这就要先解释一下什么是系统和系统工程。

什么是系统，钱学森教授描述系统的概念时说，极其复杂的研制对象称为系统，即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，而且这个"系统"本身又是它所从属的一个更大系统的组成部分。日本的斋藤嘉博给系统下的定义是："由若干部件或子系统相互间有机地组合起来可完成某一功能的综合体"。

一般来讲，系统具有四个属性。

一、整体性

系统是由至少两个和两个以上的要素（元件或子系统）所组成，

它们构成了一个具有统一性的整体——即系统。要素间不是简单的组合，而是组合后构成了一个具有特定功能的整体，换句话说，即使每个要素并不都很完善，但它们可以综合、统一成为具有良好功能的系统。反之，即使每个要素是良好的，而构成整体后并不具备某种良好的功能，也不能称之为完善的系统。

举例来说，美国喷气推进实验室早就研究喷气发动机。后来美国陆军想搞一个“下士”导弹系统，它涉及弹头、弹体、发动机、制导等子系统。最初他们想用该实验室研制的发动机作推进器，但没有从系统的整体性来考虑，只是把现有的子系统拼拼凑凑，虽然导弹可以起飞，但很不成功，造价既高又不便维修。后来又搞“中士”导弹系统，该实验室提出要有权参与整个导弹设计，亦即对全系统“特定功能”有所了解，而且要求参加从设计、生产到使用的全过程。从整体性出发的结果，制造成功了功能有显著改进的“中士”导弹系统。

二、相关性

系统内各要素之间是有机联系和相互作用的，要素之间具有相互依赖的特定关系。例如，对于电子计算机系统来说，各种运算、贮存、控制、输入输出装置等各个硬件和操作系统、软件包等都是子系统，它们之间通过特定的关系，有机地结合在一起，就形成了一个具有特定功能的计算机系统。

三、目的性

所有系统都为了实现一定的目标，没有目标就不能称之为系统。不仅如此，设计、制造和使用系统，最后是希望完成特定的功能，而且要效果最好。这就是所谓最优计划、最优设计、最优控制和最优管理和使用等。

四、环境适应性

任何一个系统都处于一定的物质环境之中，系统必须适应外部环境条件的变化，而且在研究系统的时候，必须重视环境对系统的作用。

那么什么是系统工程呢？所谓工程，就是服务于特定目的的各

项工作的总体，如水利工程、机械工程、土木工程、电力工程、冶金工程、化学工程等等。如果这个特定的目标是系统的组织建立或者是系统的经营管理，就可以看成是系统工程。

日本工业标准（J I S）对系统工程的定义为："系统工程是为了更好地达到系统目标，而对系统的构成要素、组织结构、信息流动和控制机构等进行分析与设计的技术"。

至此，我们就可以归纳出一个中心问题，那就是为什么要用系统工程的方法来解决安全问题，才能有效地防患于未然呢？其理由如下：

第一，使用系统工程方法，可以识别出存在于各个要素本身、要素之间的危险性。

我们知道，危险性存在于生产过程的各个环节，例如原材料、设备、工艺、操作、管理之中。这些危险性是产生事故的根源。安全工作的目的就是要识别、分析、控制和消除这些危险性。使之不致发展成为事故。利用系统可分割的属性，可以充分地、不遗漏地揭示存在于系统各要素（元件和子系统）中存在的所有危险性。然后就可以对危险性加以消除，对不协调的部分加以调整，这就有可能消除事故的根源并使安全状态达到优化。

第二，使用系统工程方法，可以了解各要素间的相互关系，消除各要素由于互相依存、互相接合而产生的危险性。

要素本身可能并不具有危险性。但当进行有机的结合构成系统时，便产生了危险性。这个情况往往发生在子系统的交接面或相互作用时。

人机交接面是多发事故的场所，最突出的例子如人和压力机、传送设备等的交接面。对交接面的控制，在很大程度上可以减少伤亡事故。

危险物的质量，能量贮积都是构成重大恶性事故的物质根源。适当地调整加工量和处理速度，可以大量降低事故的严重性。例如，炸药研磨由吨位级改为公斤级，加工速度相应增大，这样做虽然并不能减少处理事故，但能使事故严重性大大降低。现代化的大型石油

化工生产，也存在着能量贮积和加工速度之间的安全优化问题。

第三，系统工程所采用的一些手段都能用于解决安全问题。

系统工程几乎使用了各种学科的知识，但其中最重要的有运筹学、数学、控制论。系统工程方法所解决的问题，几乎都适用于解决安全问题。例如，使用决策论，在安全方面可以预测发生事故可能性的大小；利用排队论，可以减少能量的贮积危险；使用线性规划和动态规划，可以采取合理的防止事故的手段。至于数理统计、概率论和可靠性，则更可广泛地用于预测风险、分析事故。因此可以说使用系统工程方法可以使系统的安全达到最佳状态。

第二节　安全系统工程的发展过程

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，从头做起。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“武器安全系统标准”。这对以后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—38130，1967年7月又发表了安全系统工程计划标准MIL—STD-882。在这项标准中，首次奠定了安全系统工程的概念，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故，受到一次惨痛的教训。

另外，英国以原子能公司为中心，从六十年代中期开始收集有关核电站故障的数据，对系统的安全性和可靠性问题，采用了概率评价方法，后来进一步推动了定量评价的工作，并设立了系统可靠性服务所和可靠性数据库。它们的任务是收集核电站的设备和装置的故障数据，提供给有关单位。

1974年，美国原子能委员会发表了有关核电站事故评价报告。这项报告是该委员会委托麻省理工学院的拉斯姆逊教授,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”即WASH—1400。报告收集了核电站各个部位历年发生的故障及其概率，采用了事件树和事故树的分析方法，作出了核电站的安全性评价。这个报告发表后，引起了世界各国同行的关注。后来，美国原子能委员会又撤消了这个报告，但在1979年美国发生三浬岛核电站放射性物质泄漏事故后，总统组织的调查委员会重新认定WASH—1400的分析方法是正确的。

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，十几年来在电子、宇航、航空、铁路、公路、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年公布的化工联合企业六步骤安全评价方法，就贯穿了安全系统工程的内容。

当前，安全系统工程已普遍引起了各国的重视，国际安全系统工程学会每两年举办一次年会，1983年在美国休斯敦召开的第六次会议，参加国有四十多个，从讨论议题涉及面的广泛，可以看出这门学科越来越引起了人们的兴趣。

第三节　安全系统工程的内容

安全系统工程主要包括三个方面。

一、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，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。根据需要可以把分

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。每种深度都可以得出相应的答案，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，看看哪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。

当前已经发表的系统安全分析方法有数十种之多，从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缘故。

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）、既能定性又能定量的故障类型和影响分析法、事件树分析法和事故树分析法等四种较为实用。我国应用系统安全分析法起步较晚，近两年来刚开始在企业推行安全检查表法和事故树定性分析法，已广为人们所接受。

二、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的潜在危险和薄弱环节所在，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。但这比起用传统安全方法来，已经系统和准确得多了。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进安全状况。

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。

三、安全措施

安全系统工程内容的最后一项是采取安全措施，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。

第四节　安全系统工程在安全工作中的应用

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。军事装备零部件对可靠性、安全性的要求十分严格，否则不仅完不成武器的设计，而且制造过程中的各个环节也不安全。后来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安全技术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。

一、安全技术工作和系统安全分工合作时期

安全系统工程发展的初期阶段，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，两者分工协作共同完成生产任务。如果安全工作做得不好，发生了事故，不仅工人受到伤亡，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污染和质量问题。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性不良，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，二者有着极为密切的关系。

二、安全技术工作引进系统安全分析方法阶段

安全系统工程发展不久，安全技术工作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，根据其本身的特点和环境条件进行安全性的定性和定量分析，作出科学的评价，并据此采取针对性的安全措施，所以，这种方法对安全工作十分有用，自然也就很快被安全工作所采用。

三、安全管理引用了安全系统工程方法阶段

由于安全系统工程不仅可以评价系统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、以及对工人教育、训练等阶段，都可以使用这种方法提高系统性和准确性。

四、以安全系统工程方法改革传统安全工作阶段

在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。

第五节　安全系统工程的优点

从以上几节所述，可以明显地看出在传统安全工作的基础上，采用安全系统工程的方法有很多优越性，它可以使预防为主的安全工作从过去凭直观、经验的传统方法，发展成为能预测事故的定性及定量方法，其优点有：

（1）通过分析可以了解系统的薄弱环节所在及危险性可能导致事故的条件。从定量分析可以预测事故发生的概率，从而可以采取相应的措施，控制事故的发生。不仅如此，通过分析还能够找到发生事故的真正原因，并查到未想到的原因。

（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，大幅度地减少伤亡事故。

（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）不断地采取改善措施。

（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）可以迅速提高劳动保护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