铁路安全系统工程简明教程

曹 琦 编

西南交通大学出版社

铁路
安全系统工程

简明教程

曹琦编

西南交通大学出版社

内 容 简 介

本书对安全系统工程中较为成熟，生产中得到广泛应用的安全检查表、事故树分析、故障类型及影响分析、系统安全评价四种方法作了深入具体的阐述；对必要的数学知识从实用的角度作了扼要易懂的处理；对有关的事故原理、安全心理学、人机工程学及安全生产目标管理知识也作了必要的介绍。本书各章还穿插了铁路各部门的事故实例，并专题编写了铁路事故预测实例一章。

本书特点简明实用，适于铁路的中、基层生产管理干部、安全技术干部及工程技术干部作为继续教育培训用书，也可作为大专院校的教学用书，对路外厂矿有关人员也有较高的参考价值。

铁路安全系统工程简明教程
TIELU ANQUAN XITONG GONGCHENG JIANMING JIAOCHENG
曹 琦 编
*
西南交通大学出版社出版发行
（四川 峨眉）
西南交通大学出版社印刷厂印刷
*
开本：787×1092 1/16 印张：13.75
字数：347千字 印数：1—5000册
1988年11月第一版 1988年11月第一次印刷
ISBN 7-81022-085-3/TB 006
定价：3.65元

前　言

安全系统工程学是本世纪60年代才发展起来的一门新兴学科，它是现代安全工程中最主要的学科之一。

安全系统工程与传统安全管理的主要区别就在于：它摆脱了安全工作单纯依靠个人的生产经验，工作中头痛医头、盲目被动的状态；以信息论、控制论、系统论为依据建立了科学的安全管理方法；以计算机为工具可以对庞大的工业系统进行相当准确的事故预测。安全系统工程已经成为现代巨大规模工业生产和高速度、高密集度交通运输工程发展中风险决策的技术之一；成为系统运行中必须依靠的安全管理技术；成为事故发生后的主要分析手段。

安全系统工程内容十分丰富，它是以系统科学、安全心理学、安全人机工程学、形式逻辑学、可靠性工程、布尔代数、概率论与数理统计等学科作为基础的一门综合性学科。为了适应在职管理干部及现场安全技术干部的需要，使读者在没有上述基础的情况下可以直接阅读，并能付之应用，本书力求贯彻实用原则，编成一本“简明教程”。本书没有采取大学安全工程专业教科书的框架，而是选择了安全系统工程中最成熟、最有效、最常用的安全检查、事故树分析、故障类型影响分析及安全评价四种方法作为全书骨干，并围绕骨干内容的需要补充了事故原理，人一机系统、人的操纵可靠性分析等属于安全理论、安全人机工程学及安全心理学方面的内容，最后还简要地介绍了安全生产目标管理的方法。对于必要的数学知识，从通俗实用的角度作了扼要易懂的处理。各章的后面还附有练习题，使之全书构成一个简明实用的体系。

本书的另一特点是尽量结合铁路安全技术和安全管理的实际进行选材，除在各章适当穿插铁路的机、辆、工、电、运各部门实例外，还在最后编写了铁路事故预测实例一章，并对铁路安全进行系统管理的问题进行了专门的讨论。

本书是铁道部干部部组织编写的，为全路中、基层干部的继续教育试用系列教材之一。适于铁路的中、基层生产管理干部，安全技术干部及工程技术干部作安全技术培训，也可作为大专院校教学或自学用书，并可供路外厂矿的有关人员参考。

本书在编写过程中参考和引用了国内外许多文献资料以及个别实例，在此特向文献作者表示谢意。书中有不妥之处，敬望读者批评指正，以便不断改进。

曹　琦

1988年8月 峨眉

目　录

第一章　导　论

第二章 人 — 机 系 统

第三章　人的操作可靠性分析

第四章　事故原理

第五章 安全检查表

第六章 事故树分析（一）——事故树结构

第七章 事故树分析（二）——定性分析

第八章 事故树分析（三）——定量分析

第九章 铁路事故预测实例

第十章 设计阶段系统故障预测

第十一章 安 全 评 价

第十二章 安全生产目标管理

第一章 导 论

1.1 系统的概念

1.1.1 系统的定义

在一定的环境中，由若干个可以互相区别的要素构成的、各要素之间存在着一定联系的、并能适应环境的变化而保持其功能的集合体称之为系统。在系统中，人、设备与过程有秩序地组合起来去实现统一的目标，其功能是接受信息、能量和物质，并根据时间程序处理和产生新的信息、能量和物质，这就是系统的输入和输出过程。

系统往往是多级递阶结构组成的，一个系统可以分为若干个子系统，子系统还可以再分。同时一个系统也可以属于另一个更大的系统，作为大系统的子系统。

系统可以有物质形态的，也可以有观念（思维）形态的。

1.1.2 系统方法

系统方法是指按照事物的系统性把对象放在系统形式中加以考察的方法。

系统方法的基本原则如下：

(1) **整体性原则** 整体性原则是把对象作为由各个组成部分构成的整体，研究整体的构成及其发展规律，即把系统当作整体来对待，从整体与部分相互依赖、相互结合、相互制约的关系中揭示系统的特征和运动规律。

整体功能不等于部分功能的总合，整体将产生部分所没有的功能。

(2) **综合性原则** 要求对系统从时间上、空间上进行综合考察，在综合的基础上进行分析，再回到综合，每一层次分析的结果都要反馈到上一层次的综合中去，与整体进行比较，并进行修正，使之部分与整体达到统一。

(3) **联系性原则** 构成系统的元素之间，元素与环境之间，有着特定的联系，物质与能量之间的相互转换及不同物质形态之间的信息交换，都体现着联系性。

(4) **有序性原则** 系统都是有序的，因此系统必然是有层次的，系统的发展一般是由较低级的有序状态走向较高级的有序状态的定向演化，在这一发展的过程中，系统必然是开放的，从外界环境中耗散物质、能量和信息，系统内部各子系统将按照一定的目标协同运动，以达到系统总的目的。

(5) **动态性原则** 任何系统内部都存在着矛盾运动，推动着系统的发展，因此研究系统时，应在动态中协调各部分的关系，才能准确地掌握系统的规律，取得综合的动态平衡，使系统不断得以优化。

(6) **结构性原则** 系统的整体性功能是由系统的结构决定的，同样的元素，组成不同的结构，将会产生不同的功能。系统优化的一个重要方面就是取得最优的结构。

(7) **模型化原则** 模型化是使系统方法从定性到定量的重要途径，通过对真实模型的实验，可以具体分析系统的运行状况，也可以建立数学模型对系统进行定量描述。

1.1.3 系统分析

系统分析就是将所要研究的对象从环境中划分出来，确定其边界、划分子系统、确定子系统之间联系、确定系统与环境之间的联系；用数学方法、模拟方法对系统进行综合与分析，作出系统的动态预测；采取控制措施，使系统达到最佳化。

系统分析的一般步骤如下：

(1) 提出问题，确定功能，明确边界条件及各种指标；

(2) 搜集并分析资料；

(3) 建立模型；

(4) 系统最佳化；

(5) 系统评价。

安全系统分析即按这一程序进行。

1.2 安全系统工程概述

1.2.1 安全系统工程的内容

安全系统工程就是用系统科学的方法，对事故进行定性和定量分析预测及安全评价的工程学。其主要内容简述如下：

(1) **建立安全系统功能模型** 安全系统功能模型一般是用一组规定的符号按事故因果的层次，绘制出事故发生的树状结构图，来描述事件的组合方式及其事件发生的时间、空间结构。

功能模型是建立在对原系统或相近系统的分析、研究及大量事故统计资料的基础之上的。

(2) **建立事故结构的数学模型** 目前主要是用布尔代数方法建立事故结构函数，用概率论的方法建立事故发生的定量分析模型。

(3) **对事故进行定性分析** 目前用作定性分析的数学方法主要有三种：① 事故等级评定法，如故障类型及影响分析；② 布尔代数分析法；③ 模糊集合综合评判方法作基本事件结构重要度分析*。

(4) **对事故进行定量分析** 事故在系统运行的过程是否发生，何时发生，事先不能准确的预计。事故的发生是个随机事件，但用概率统计的方法可以分析出随机事件的发生规律，并作出定量的描述。所以对事故定量分析时，概率论是主要的数学工具。

(5) **安全评价** 安全评价分为定性评价与定量评价两种。定性评价建立在事故定性分析的基础上，定量评价建立在对事故定量分析的基础上。

定量评价又分为两种：

① 可靠性定量评价 在评价之前，首先定义安全函数，目前常用的安全函数有安全

---

* 这种方法尚不成熟，本书不作介绍。

度、危险率、事件重要度、事故严重度、风险率等。然后作评价计算，将所求得的值与评价标准相比较，作出判断。

② 指数法 这种方法是用每种事件的危险值和各种物质潜在危险的物质系数计算失火爆炸指数，再与规定的安全指数相比较，作出判断，此法主要用于化工系统。

安全评价是安全技术和安全管理的主要依据。生产是个不断变化发展的过程，安全管理也必然是个不断变化发展的过程，因此上述五个方面，在生产中并不是一次性工作，而是不断循环的过程，所以安全管理与生产管理之间，必然形成既有纵向联系又有横向交叉的网络状态。这两个方面就构成了企业全面目标管理的内容。

1.2.2 安全系统工程的特点

系统工程是实现系统最优化的一门工程学，安全系统工程，是把安全作为一个系统，对安全进行系统分析，并使之达到最优化的工程学，其目的在于确保人一机系统具有很高的可靠性和安全性。

安全系统工程有以下三个特点：

(1) 用系统分析的方法，按系统可分割的属性，可以深入地全面地揭示出造成某种事故的全部基本事件（原因），不论是多大的系统都可以按所要求的水平作出分析。

(2) 生产要素（人、机器、材料等）如果都各自处于静止、隔离的状态，并不具有造成人员伤亡和财产损失的危险性，一旦他们之间进行有机的结合构成动态系统时，在他们相互作用的交接部分（界面）上便潜伏着由于故障或失误造成人机事故的危险。用系统分析的方法能全面地找出控制事故发生的基本事件组合状态，为安全设计及安全管理提供依据。

(3) 运用数学方法对事故的发生作出定性和定量分析，为系统设计和运行之前提供事故预测；为运行中的系统提供最有效、最经济的安全措施方案；为事故发生后提供科学的分析总结方法。

1.3 系统安全管理的任务

1.3.1 系统安全管理的一般要求

(1) 系统安全管理以解决一系列问题来保证其目标的实现。在既定的任务下，系统的设计应满足适时、成本低、效果好而且安全性高的要求。

(2) 在整个系统寿命周期内，对所有的危害都应进行分析、鉴别、评价，并消除或控制在可以接受的安全水平上。

(3) 应尽量采用在其他系统上证明是行之有效的安全数据、新设计、新材料、新的生产工艺和测试技术等，以提高系统的可靠性。

(4) 随系统运行所产生的各种有危险性的物质，均应考虑易于安全处理。

系统安全的流程，大致如图 1.1 所示，系统安全分析和评价是系统安全的核心，只有严谨准确地分析和符合客观规律的评价，才能作出最优化的决策。

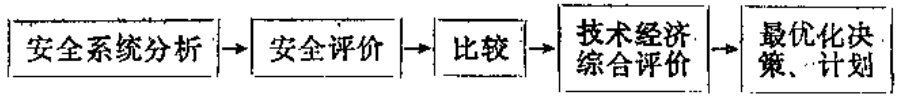

图 1.1 系统安全流程

1.3.2 开发初期的系统安全管理任务

(1) 合同招标时，由发标者提出安全评价和保障安全的必要条件，投标者则应提出工程阶段需要实行的系统安全工程方案。这一阶段要求制订出符合既定任务需要和系统寿命周期要求的系统安全设计，对可供选择的系统方案作出评价。

(2) 评价在整个寿命周期中影响安全的有关原材料、设计要点、手段、操作原理和环境。

(3) 进行预期危害分析，即拟设的危害分析（PHA），用以判别系统的固有危险，确定预测事故的危险等级，调查不安全因素存在于哪个子系统之中，继而识别危害因素转变成危险状态的触发条件，并进一步研究消除隐患的措施及其效果。

(4) 对于特殊部分，须研究类似系统成功的安全设计，根据类似系统的经验来确定本系统的安全要求。

(5) 鉴别在整个系统寿命周期中，需要合同保证的安全要求是否明确，以及在合同中确定安全设计、分析测试、试车及验收要求。

(6) 对每一方案的系统安全分析、结论及建议要编成文件，为便于决策，要写出开发阶段所有安全任务结论的总结报告。

1.3.3 试运行阶段的系统安全管理任务

在对样机测试、试车、验收等进行广泛的分析的基础上确定下列要求，

(1) 制订合乎现代要求的系统安全计划，说明综合的系统安全效果，鉴别出设计、生产、操作及后勤任务中的危害。

(2) 建立系统安全所要求的项目，并使所制订的试车和验收安全要求规范化。

(3) 搜集有关的系统安全要求和危害生产方面的情报，据此提出改进设计的建议，在满足试车和验收任务的前提下，保证达到最优的安全程度。

(4) 在定性和定量分析检验的说明书内容中，应满足系统安全的要求（包括承包方提供的设备、支援设备、连接设备和辅助设备等），并进行子系统、系统、操作和后勤支援的危害分析。

(5) 审查所有的测试计划，以保证测试任务的安全实施，保证通过分析和测试检查发现的不安全因素能够被消除或控制住，并审查为安全而计划的训练项目。

(6) 评价试车及验收阶段记载下来的事故树分析（FTA）和伤亡事故调查的结论，提出重新设计或其他改进的措施。系统安全的研究、分析和试验所取得的系统安全要求，应列入系统计划书中。

(7) 将试车及验收阶段进行的上述系统安全任务写出总结报告，并应积极着手准备在全面工程开发阶段和生产开始阶段，将要用到的系统安全程序计划。

1.3.4 工程全面开发阶段的系统安全管理任务

(1) 审查初步设计是否已将安全设计要求编入，确保在试车及验收阶段所判明的不安全因素得以避免或控制到允许限度。

(2) 在使子系统、系统、操作和后勤支援先进化的同时，一方面核定其设计和试验效