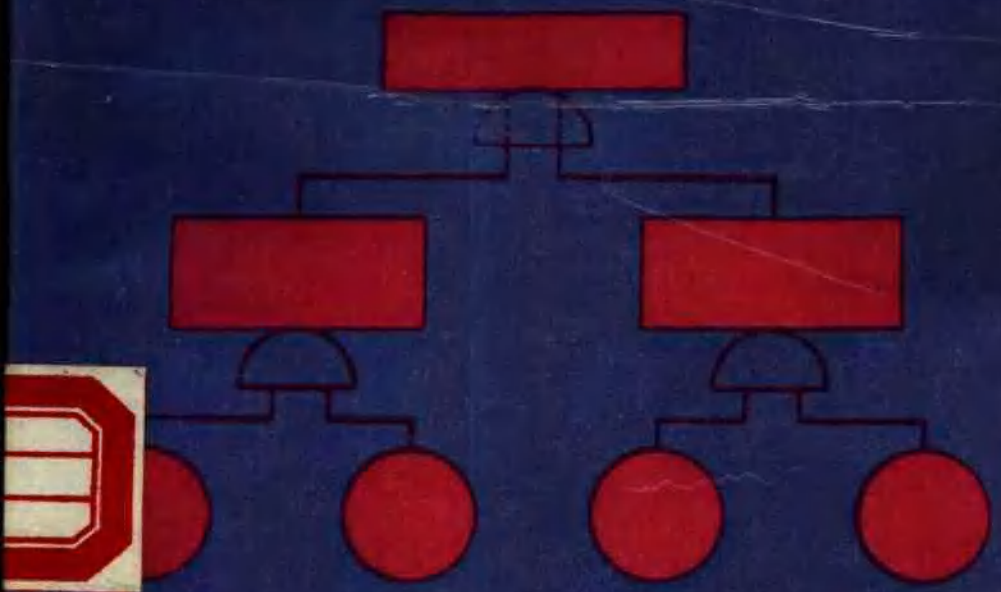
故障树分析

（FTA）

安全工程学

〔日〕综合安全工程学研究所 编著



机械工业出版社

故障树分析(FTA)安全工程学

〔日〕综合安全工程学研究所　编著

主编：井上威恭

姚　普　译　王逸文　校

机械工业出版

故障树分析，是美国于60年代开发的安全分析方法。最初应用于宇宙技术，以后作为机械装备危险性的评价方法，广泛应用于产业界的各个领域。日本引进了这一方法，并结合日本的实际，对各个领域的安全事故问题，作了广泛而实际的研究分析和运用。

本书系统地介绍了：系统安全工程学的涵义和发展；故障树分析的理论方法步骤；安全水平的评价；并列举了很多分析应用案例，包括，石油化工、机械设备、粉尘爆炸等方面。

本书可供企业领导，技术、管理人员，特别是安技人员，可靠性、质量管理人员阅读，也可供管理机关和有关教育部门师生参考。

FTA安全工学

监　修　井上威恭
编　者　综合安全工学研究所
发行所　日刊工業新聞社
昭和54年4月27日　初版发行

* * *

故障树分析(FTA)安全工程学

〔日〕综合安全工程学研究所　编著
主编　井上威恭
姚　菁　译　王通文　校

责任编辑：武　江　责任校对：宁秀娥
封面设计：刘　代　版式设计：张伟行
责任印制：卢子祥

*

机械工业出版社出版（北京阜成门外百万庄南里一号）
（北京市书刊出版业营业许可证出字第117号）
人民交通出版社印刷厂印刷
新华书店北京发行所发行　新华书店经售

* * *

开本850×1168 1/32　印张9 1/4　字数232千字
1989年4月北京第一版·1989年4月北京第一次印刷
印数　0.001—1.595·定价：8.00元

*

ISBN 7-111-00414-0/F·32

序

日本的综合安全工程学研究所（Research Institute of Safety Engineering 简称 RISE）（财团法人），以综合研究、开发日本国的安全工程学为宗旨，于昭和48年（1973）开始了工作。作为其事业的一环，规划有图书的编著发行业务。《FTA（Fault Tree Analysis）安全工程学》就是其开始发行的第二本书。

FTA是美国在1961年为了分析宇宙火箭的安全性而开发的一种分析方法。其后作为机械装置设备危险性的评价方法而广泛应用于产业界的各个领域。

FTA介绍到日本虽已几年，但广泛地为一般的产业方面所采用却是最近的事情。特别是劳动省（部）劳动基准局把它采用为化工成套设备的安全性评价方法，通商产业省（部）立地公害局（管理产业布局和公害问题的局）把它作为石油联合企业的防灾害评估方法，使得人们对 FTA 的关心迅速高涨起来。

综合安全工程学研究所为适应这一迫切的要求，也于昭和52年（1977年）2月邀请了日本国内 FTA 方面的先驱者为讲师，举办了 FTA 讲习会，盛况空前。

本书是以当时的各位讲师为核心，请他们执笔著述了，由入门到基础理论和定量的分析方法，由单机到系统的应用等FTA的各个方面。

有的人认为 FTA 在日本只是刚刚就绪，还没有齐全的反馈数据，开展定量的分析为时尚早；也有的人认为如果现在不去实践，那就是等待“百年河清”无所作为。

因此，本书采取由简单的事物到复杂系统的应用，由定性的评价到定量的评价。以使读者根据其所需，有选择的可能。

本书如果能成为日本发展 FTA 的基石，并对促进安全工程

学有所贡献，则将深感荣幸。

井上威恭

1979年2月

执笔人：

井上就一　京都大学工学部（第2章）

井上威恭　埼玉工业大学（第7章）

近藤太二　劳动省产业安全研究所（第1章）

佐山华敏　冈山大学工学部（第5章）

樋口敬一　三菱油化株式会社（第6章）

山崎博　日挥株式会社（第4章）

行待武生　庆应义塾大学工学部（第3章）

目　录

1. FTA入门

1.1 系统安全工程学

1.1.1 什么是系统安全

近年来，随着灾害趋向大型化，灾害原因复杂化，系统安全这一语汇已被各个方面所使用。本书的主题FTA（Fault Tree Analysis）实际上就是为了达到系统的安全所采用的一种系统分析方法。为此，在论述FTA之前，需先讲明系统安全的要领。

为了阐明系统安全的概念，首先有必要明确其定义。

一般地，所谓系统（System）是指：

（1）由多数元素或元素的集合所构成；

（2）它们具有相互的关联；

（3）在一定的条件下；

（4）为达到某种目的而作用的集合体。

在通常的产业系统中，系统的构成要素有材料、零件、机器、设备等，以及在那里工作的人。作为系统的功能则是：信息的传递，物件或能源的生产，人、物件、能量的转移等等。

至于所谓安全，词典中是这样注释的：人不受伤害，物不受损伤、损害（或不给予），而且人无受伤害，物无受损伤、损害（或不给予）的顾虑。

那么，对系统安全就可以做出这样的定义："对某一系统，在一定的功能、时间、成本等制约条件下，使人员和设备蒙受的伤害和损伤为最少"。

为了达到系统安全的目的，就有必要在系统的计划、设计、制造、运用等全过程中，准确地运用系统的安全管理和系统安全工程学（参阅图1.1）。

这里，所谓系统安全管理[1]，是指为了实行系统的安全业务，所必要的程序管理中的一个领域。包括：

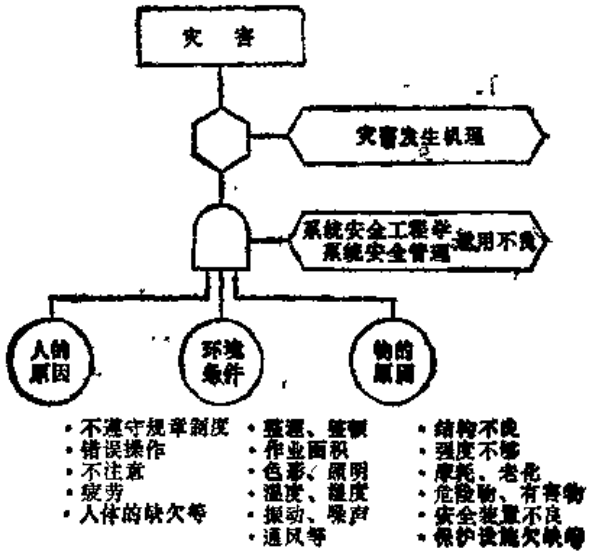


图1.1 系统灾害

（1）系统安全必要事项的同一性鉴定㊀

（2）安全活动的计划、组织、以及其管理

（3）与其它系统程序领域间的协调

（4）为使系统安全的目标能有效而及时地实现，所进行的程序分析、检查研究，以及评价等工作。

至于系统安全工程学[1]，它是运用科学的工程学原理，及时地鉴别系统内的危险性，以便采取必要的预防或控制措施的系统工程学的分枝之一。系统安全工程学是在阐明、预测以及评价系统安全性的工程技术设计、安全分析原理及方法的基础上，进而又基于数学、物理学、以及有关科学领域的专业知识和特殊技术所构成的一门学科。

1.1.2 系统安全的由来[2]

以下我们将对系统安全的起源及其进展情况加以瞻顾。50年代末期，由于国际局势的紧张和应付苏联导弹技术的进步，美国

㊀ 作为同一性的事物，加以鉴别的工作。

迫于形势要加速开发导弹武器。为了缩短开发时间，强力实行了构思、设计、制造、应用等各个阶段的工作并行的平行开发方式。事前曾预想到由于平行作业所带来的修改和走弯路，将使费用增大，但那时系统安全工程学还未被承认为独立的部门，因而关于安全性问题，只能完全依靠设计人员或技术人员的判断。

在某导弹地下储存库和发射基地，从最初的动作试验开始，仅在一年半的期间内，就相继发生了四次重大事故。每次都要遭受几百万美元的损失。经过事故发生后调查的结果，弄清楚了是由于需要从根本上加以改正的安全方面的重大缺陷造成的。对这些缺陷要加以修正，实际上需要庞大的经费和时间，结果导致这种导弹系统不得不全面地予以废弃。这样，开发后不到2年的昂贵系统，由于安全上的缺陷，终于报废了。

由于这些教训，开始认识到了系统安全性的重要性。由此促进了以系统安全计划为基础的民兵导弹系统的开发。1962年4月公布了有关系统安全的最早的美国军用设计规范——《空军弹道导弹开发用系统安全工程学 (System Safety Engineering for the Development of AF Ballistic Missile)》。同年9月根据民兵武器系统计划，把系统安全作为单独的合同项目，制订了《武器系统安全标准 WS133B》。

此后，对于系统安全的认识进一步加深，随之，设计规范的适用范围也逐步扩大。1963年9月美国空军制定了军用标准MIL-S-38130，“规定了系统、相关于系统及装备的安全工程学的通用必要事项 (General Requirements for Safety Engineering of Systems and Associated Subsystem and Equipment)”。1966年6月将此标准加以修订成为 MIL-S-38130A，规定为全美军事装备所有一切合同上的必要条件。

1969年7月，MIL-S-38130A又加以修订而成为MIL-Std-882“关于系统、相关系统及装备的系统安全程序必要事项 (System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for dated 15 July, 1969)”。这

一标准既定为军事装备有关合同上的必要条件，同时也成为一般产业的系统安全程序的有力指针。

另一方面，与美国军用装备系统安全同时发展的核武器和原子能工业，对安全性也提出了极为重要的问题。如果我们想到那种意料不到的核爆炸所引起悲惨情况，即使是爆炸一次，也是不能允许的。而且即便不是爆炸，而是由于某种事故导致射线泄漏，也将对很多人产生长期的重大影响。因此，美国原子能委员会和美国国防部关于核物质和核武器的处理实行了极为严格的管制。而这种管制反过来对作为独立的系统安全工程学学术领域的发展，却起了推进的作用。事实上以后面将要谈到的关于原子能成套设备危险性评价的拉斯姆逊报告（Rasmussen Study）[3]为开端，最近有关系统安全的研究，多数是有关原子能产业方面的。

与武器的开发和原子能产业的出现相并行，促进系统安全工程学发展的，还有一个原因是产品安全问题。60年代以来，由于美国技术的迅速进步和环境的急剧变化，对开发新产品必然要求缩短开发期限。如象从前那种按计划、设计、试制、改进等步骤去做，需要很长岁月才能开发出新产品，而这种费很大气力得到的新技术有可能在还没有商品化之前，就已陈旧老化。于是，有很多新产品在其安全性还未得到充分确证之前就投放到市场上了。这也是60年代在美国发生很多灾害的原因之一。于是，为了在短期内能开发出无损于安全性的新产品，系统安全工程学就成为必不可少的一门学科了。

另一方面，由于人们安全意识的提高和保护消费利益风潮的兴起，在美国，让产品制造者负担由于产品的缺陷而发生事故的“产品赔偿责任（product liability）”事例多起来了；而且在法理方面所谓严格责任的理论也逐渐成为主流；那就是，受害者对制造者的过失或是否违反合同，即使没有得到证据，只要能提出产品有某种缺陷，就可以要求制造者承担责任。

在这种形势下，要开发具有高度安全性的产品，就必须从计划开始直到使用的各个阶段，都要应用系统安全工程学，这就对

其发展寄予了很大的期望。

1.1.3 系统安全与产业安全

(1)产业灾害动向

日本的产业灾害以1961年为顶峰。以后有所减少，直到最近，灾害件数和灾害率两方面才呈现稳步下降的趋势。图1.2[4]示

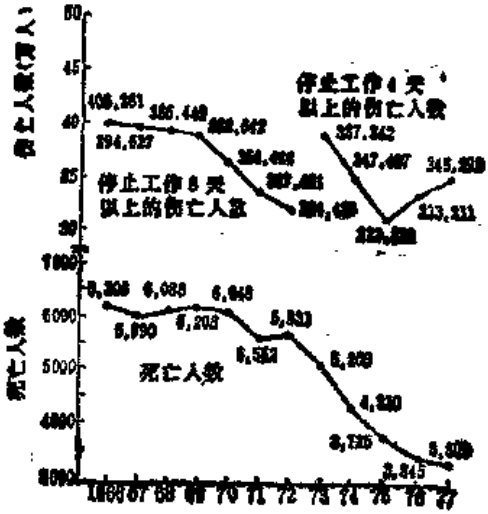


图1.2 全产业部门死伤人数的变迁
(1978年产业安全年鉴)

出从1966年到1977年全产业部门死伤人数的演变情况。1977年死亡人数为3302人，与前一年相比减少了1.3%，但停止工作4天以上的伤亡人数为345293人，反而增加3.6%。而且把停止工作不足4天的受害人数包括在内，则年受伤害人数达到114万人。此外，一次事故导致死伤人数超过8人的重大灾害，如图1.3[4]所示，1968年㊀达到480件的最高数字，其后有减少的趋势，但到1974年以后处于几乎停滞状态。

关于这些灾害的背景情况可以举出以下几点：

㊀ 原文昭和43年误为84年——译者

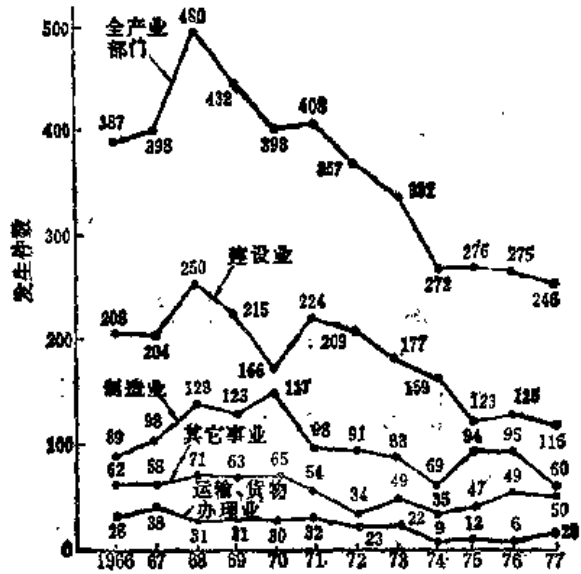


图1.3 按产业区分重大灾害发生件数的变迁
（1978年产业安全年鉴）

1)灾害的内涵包括：坠落、滑倒、被机器挤轧等原始形式即所谓初级灾害占多数；

2)中小企业发生的灾害约达总数的80%，灾害率也由企业规模的大小而有显著的差异；

3)反之，随着机械设备的大型化、高速化，建设工程的大规模化，新技术引进以及有害物质的使用等情况，而增大危险性；

4)近年来灾害之所以减少，可以认为是受石油危机生产萎缩的影响，但由于严峻的经济形势而产生忽视安全的倾向，使灾害有可能重新抬头。

总之，问题还是很多的，今后的动向未必容许乐观。

（2）不安全状态与不安全行为

一般地来说，产生灾害的原因也不一定是单纯的。即便是所

调初级灾害，如果加以调查分析，也多数是由于几种原因互相联系影响而导致灾害的发生。

仅从导致灾害直接原因的不安全状态（物的因素）和不安全行为（人的因素）来看，仅属于单方面的情况是很少的。虽然因统计方法的不同会有些差异，但一般来看，灾害的70～90%是由物的客观原因和人的主观原因二者相重叠造成的。

表1.1 日本制造业按原因区分灾害发生状况

（1977年，停止工作4天以上）

不安全状态				不安全行为			
区分		次数（人）	比率（%）	区分		次数（人）	比率（%）
调查总件数		104638	100.0	调查总件数		104638	100.0
由于不安全状态		87377	83.5	由于不安全行为		98910	94.5
不安全状态的内涵	物体自身的缺陷	4783	4.6	不安全行为的内涵	使安全装置无效	2748	2.6
	防护措施的缺陷	14464	13.8		不执行安全措施	5636	5.4
	物体放置方法，作业场所的缺陷	16015	15.3		不安全的摆放	3078	3.0
	保护器具、服装等的缺陷	2817	2.7		造成危险状态	2060	2.0
	作业环境的缺陷	687	0.7		不按规定使用装置	3071	2.9
	外部的、自然的不安全状态	3695	3.5		机器等运转中的扫除、加油、修理，检查	7604	7.3
	作业方法（指定，认可的）的缺陷	38654	36.9		保护器具、服装的欠陷	3153	3.0
					接近其它危险场所	17614	16.8
					其它不安全行为	11754	11.2
	其它及不可分类的	6262	6.0		驾驶失误（驾驶者）	1792	1.7
					操作错误	30856	29.5
					其它，及不可分类的	9544	9.1
无不安全状态者		17261	16.5	无不安全行为者		5728	5.5

特别是，由多因素组成的复杂系统，由于某种细小的机械故障或作业的失误，发展扩大而酿成巨大灾害的事例也不少。

针对这些情况，就有必要分析各种原因相互之间的关系，查明发生灾害的症结所在，查出与灾害关联较深的原因，重点地采取对策和措施。就是说，在产业安全方面也有必要引进系统安全。

(3)系统安全与产业安全的关系

系统安全与产业安全的关系，主要通过以下四个过程或阶段相紧密联系。

(i)产业安全要配合系统安全

从系统安全开发初期就有这种考虑，让系统安全技术人员和产业安全技术人员明确各自分担的责任：前者对产品安全负责；后者对工作人员安全负责，通过双方的配合协作以分别达到各自的目的。因为如果由于产业安全工作做得不够而发生事故，不仅要伤害作业人员，而且对装置、研制中和制造中的产品也要有所损害，以致给预定的系统安全程序的完成带来障碍。即使不发生事故，在不安全的环境下工作，也可能受到影响，制造出不良的零部件，从而难以实现系统安全设计的目标。另一方面，产品或系统如果缺乏安全性，在制造过程中导致事故发生的危险性就要增高，作业人员的安全就难以维持。

(ii)产业安全引进系统安全方法

系统安全开发以后不久，就有人提出建议，认为这种方法特别是系统安全分析方法也可以适用于产业安全领域。1965年卡洛涅（Kolodner）[5]在其关于安全性定量化的论文中介绍了FTA和Block Diagram Analysis〔框图分析法〕；同年里克特(Recht)[6]在其系统安全分析（System Safety Analysis）一文中介绍了FM&E（Failure Mode and Effect）〔故障（失效）模型和效应〕，FTA、THERP（Technique for Human Error Rate Prediction）〔人的失误率预测技术〕以及Cost Effectiveness Analysis〔费用效果分析〕等等系统安全分析方法。暗示了这些方法也可以适用于产业安全领域。其后，在原子能成套设备或化工成套设备等复杂而且危险性高的系统安全分析中，利用了以上述方法为主的很多的系统安全分析方法。

(iii)系统安全程序应用于产业安全

系统安全分析在系统安全程序中占据重要的地位，但却不是其全部。系统安全必须考虑，包括产品合同、开发、设计、制