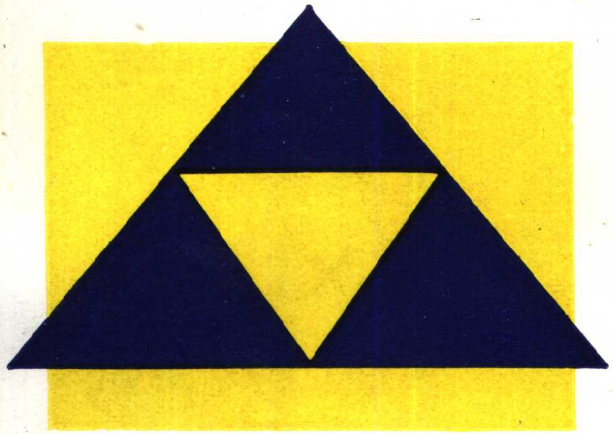
〔美〕威廉P·罗杰斯



XI TONG AN QUAN GONG CHENG DAO LUN

系统安全工程导论

轩 王志民 译
柴本良 张连超 校

劳动人事出版社

系统安全工程导论

[美]威廉P.罗杰斯

译者：吕武轩　王志民

校对：柴本良　张连超

劳动人事出版社

Introduction to
System Safety Engineering
William P. Rodgers
1971, by John Wiley & Sons, Inc

系统安全工程导论

〔美〕威廉 P. 罗杰斯

吕武轩　王志民　译　　柴本良　张连超　校

劳动人事出版社出版

（北京市和平里中街12号）

新华书店北京发行所发行

787×1092　32开本　4印张　97千字

1984年8月第1版　1984年8月北京第1次印刷

书号：15238·0057　　书价：0.73 元

序　言

本书内容，顾名思义，就是向读者介绍“系统安全工程”。正如任何一门新的专业学科一样，人们对于什么是系统安全，它到底能解决什么问题，以及怎样应用这门科学，目前尚缺乏了解。而这三个问题正是本书着墨的重点。为便于读者接受，在写法上较少使用专业术语。本书的内容，有助于读者了解在产品和装置设计与试制中系统安全工程的作用，读者还将了解到保障系统安全工作实施所必须的情报的类型；有保留价值的安全工作经验；有助于法律工作者进行产品责任诉讼的有效决策文件，以及系统安全与其它工程规划学科诸如可靠性、系统工程、试验工程之间的关系。

作者首次将促使系统安全工程产生与发展的历次重大安全事故汇入一本书中；介绍这一新学科的历史背景，目的是为讨论系统安全实际应用问题奠定基础。本书第四章通过实例讨论了系统安全工程的各种分析方法。

作者提出的关于系统安全工程基本理论与实用方法，各种教科书和管理参考手册皆可使用。只要应用本书中所阐述的一般原理，并遵循第三章中所示的基本系统安全产品开发规划的经验，即可有效而经济地完成系统安全工程项目。

威廉 P·罗杰斯

1971年8月于加利福尼亚州　雷东多比奇

目　录

第一章

产品开发中的安全

在解释一个题目时，最难办的就是确保所用术语定义能够被人理解。这一点对于“安全”一词尤其如此。每个人在要他写出安全的确切定义之前，几乎都说他理解安全的含义。人们不难看出，“安全”一词虽然常用，但是由于使用者主观上的评价不同，其含义也就会有许许多多的变化。例如，让一名训练有素的飞行员来驾驶一架民用飞机，一般认为是比较“安全”的；但是若让一个从未受过飞行训练的人来驾驶，这却是非常危险、甚至是拿生命冒险的事。再以驾驶汽车而论，一个人每天上、下班时往来于洛杉矶高速干道上，认为这样的生活方式是“安全”的，否则就不会每周五、六天、每天两次在那上面频繁行驶；然而，让一个只在人口稀少的美国农村双车道公路上开车的司机驱车到洛杉矶高速干道上去，尤其是在高峰期间，那将是非常苦脑而危险的事。

安全一词是按主观和相对的方式定义的。韦伯斯特*把安全定义为“安全存在的条件；保证自身或他人的安全，免除各种危险或危害，特别是偶然事故或疾病的危险。”遗憾的

---

*. Webster 系美国著名韦氏大字典的编纂者（译注）。

是，如果一个词要用这个词本身来定义它自己时，这样的定义充其量也只是个模糊的定义。这再次说明“安全”一词是相对的和主观的这一事实。国防部在其1969年7月15日颁发的系统安全军用标准（Mil-Std-882）中，把安全定义为“免除人员伤亡、设备损坏的条件”。这一定义在关于“设备损坏”问题上引起了很大争论，从字面上讲，这包括了由磨损导致的故障和由违章引起的事故。一个比较具体的阐述安全的定义是：“保证免除可能伤害人员或毁坏装备的偶然或意外事件的环境”。这就是本书各章都将使用的定义。

只是在近六十年来，雇主们才对安全给予较多的重视。不久之前，个人防护仍由本人自己负责，雇主们只不过发放一些防护器具。在二十世纪初期之前，雇人的主要因素就是生产。工作服及手工工具的配备，均由后人自己负责。雇工的自身安全是每个人自己的责任；雇员由于受伤而失业，就很难领到工资。实际上，如果受伤使生产受到影响，雇员还常常受罚。

在过去六十年中，安全的责任已由雇员转到雇主方面了。现在，提供安全的工作环境及维持安全环境所必须的工具与设备则是雇主的责任。事实上，因为法庭的判决往往有利于受伤的雇员，所以雇主如不为雇员的安全提供一切可能的预防措施，那就会铸成大错而付出很大代价。安全责任的转移是工会、雇员组织和广大公众共同努力的结果，他们要求通过立法和监察迫使工业管理者承担这一义务。例如，几年前，为了保护公众和运输工人的安全，特制订了《州际商务委员会关于铁路、货车、机动车辆及通过集装箱陆路和水路运输易爆和其它危险物品的规定》。如果一个公司不遵守这

一规章，就是违反86届国会通过的86-710号公法。违者可被处以10000美元的罚款和长达10年的监禁。

以往，安全方案是在事后确立的，具有亡羊补牢的味道，也就是说，事故发生之后，接着进行调查，看采取什么必要措施，以防止类似事故重复出现。简短回顾一下产品开发的指导思想，将有助于理解这种事后安全补救法的起源。

在五十年或更久以前，一个新就业的青年徒工，要在车间里从头学习如何用自己的双手制造产品，他这样做的结果是，学会了掌握机械员、装配工、试验员及操作或使用人员的工作要领。这种徒工培训需要若干年头，雇员对此是早已预料到的，并在他一生工作中作了这样的安排。本世纪初叶，一个人毕生只渴望从事一、两种产品的制造，然而，这种情况已不复存在了。在为国家技术、自动化与经济发展委员会准备的研究报告中，即在1966年2月该委员会报告《技术与美国经济》附卷二《技术变革对职业的冲击》33页“现代工业社会技术发展与普及速度的调查”(作者福兰克·林恩，伊利诺斯州芝加哥市INTEC公司）一文中，有如下一段叙述：

> 一项新技术从开始发明到商业上承认有用，其平均时间间隔从本世纪初（1880～1919）的30年减少到第二次世界大战后的16年；而把一项基本的技术发明转到商品生产所需的时间，在1960～1970年调查期间，则从了平减至5年。

不光是基本的技术发明转化到商品生产所需时间减少到几年，而且新产品与新工艺的数量也在按指数速率增长。这一增长速率与图1所示的人口增长速率成正比例。今天现有

的人口占人类诞生以来人口总数的三分之二。了解到这一点，就不难理解新产品数量的巨大增长了。

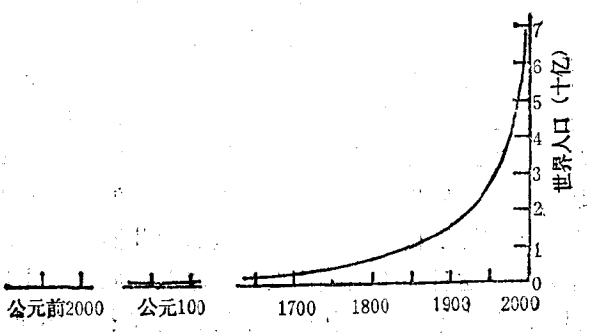


图1　世界人口增长

注：资料引自1963年世界百科全书年鉴，188～189页

表示新产品增长的另外两个例子是美国的研究与发展（即科研）总经费和科学家与工程师数量的增长情况，如图2所示。

消费品数量与复杂性的增加及开发周期的缩短，迫使新产品的管理工作发生变化。在产品寿命周期内，在提出生产计划之前，过去往往有充裕的时间制造一、两个成品，进行试验，改进，再试验……。只有到这时，才可以妥善地确定每一产品的制造步骤及费用，以及准确地制订生产计划。可是，现在再也不会如此了。今天，我们生活在变化的环境中。技术发展是大量的和显著的，人们的思想也必须是敏感的、发展的，并须适应于下列一些事物给我们带来的不断变化着的生活方式：瞬时通信，高速运输，大量的计算机分

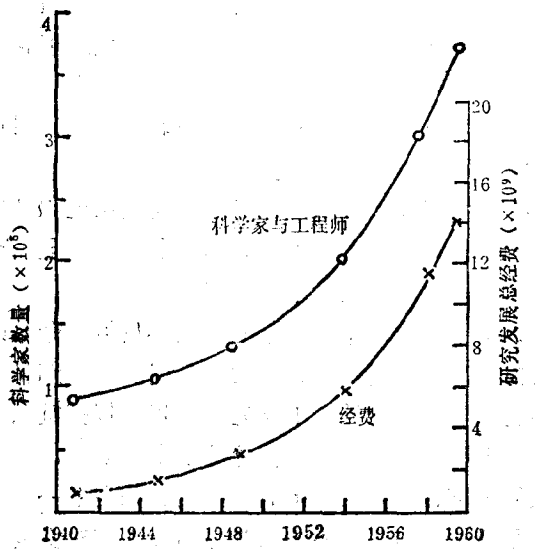


图 2　美国的科研经费与科学家数量

析，情报储存与检索能力，高能能源（如原子裂变、激光射束）的控制与利用，等等。这种环境变化的结果之一，就是产品开发的专业化。

今天，一个雇员通常只专长于成品生产中的一个很窄的领域，例如，一个汽车工程师可能对汽化器很专，而对发动机或汽车的其余部分则可能知道得很少；一个机械师可能非常精通六角车床，但可能完全不懂得钻床或铣床。

这一切与安全联系起来表明了什么？

1. 专业化的生活方式，对雇员个人来说，经常隐藏着

普遍的潜在危险，因此，雇员的安全工作完全由雇主负责。

2．新产品更加复杂、昂贵，亡羊补牢式的事故补救做法既不经济，又不保险。

3．法律责任的转变，导致了消费者和（或）用户以及雇员对有关产品安全计划的关注。

4．高能能源（如高能火箭燃料、高压系统及原子裂变）的发现，使事故的灾难程度大为增加。事实上，对于原子爆炸，即使一次事故也是不能容许的。

表1列举了近几十年来发生的一些事故给生命与财产造成的重大损失。表2列出1958～1964年间美国联邦雇员和全国雇员年度职业事故统计。难怪近年来越来越把重点放在未雨绸缪式的识别、分析、预防事故的安全计划上，而不是亡羊补牢式的出事、调查、补救的做法上。如在下一章将看到的那样，系统数量与复杂性的增加也迫使人们对安全的看法发生变化。

表1　涉及燃料和(或)炸药的一些事故(矿井爆炸事故除外)

1917.12.6 ——加拿大，新斯科金，哈利法克斯作战物资爆炸起火，死1500人以上，伤4000人，2000人无家可归，损失财产3500万美元。

1921.9.21 ——德国，奥珀
硝铵爆炸，死亡约600人。

1937.3.18 ——得克萨斯州，新伦敦
天然气爆炸，摧毁校舍，413名儿童和14名教师死亡。

1939．3．1——日本，大阪
大型弹药库爆炸，村庄被夷为平地，500人死亡和受伤，300

家房屋被毁坏，8313人无家可归。

1939. 7.10——西班牙，Penandara de Bracamonte
弹药制造厂爆炸，毁坏了市区，近100人死亡，1500人受伤。

1941. 6. 8——南斯拉夫，斯梅德雷沃
弹药厂爆炸，死亡1000人，城市的大部分被毁坏。

1942. 5. 1——比利时，Tessenderlo
化工厂爆炸，死250名工人，伤1000人。

1944. 4.14——印度，孟买
船上火灾引起弹药爆炸，128人死亡，1000人受伤。

1944. 7.17——加利福尼亚州，芝加哥港
两个弹药库爆炸，死亡300多人。

1947. 4.16——得克萨斯州，得克萨斯城
法国军舰 GRANDCHAMP 号爆炸，城市大部分被毁，伤亡或失踪人数超过500。

1947. 8.20——西班牙，加的斯
造船厂爆炸，死亡300～500人。

1948. 3.9——中国，青岛
弹药库爆炸，死亡至少200人，炸伤几百人。

1948. 7.28——德国，路德维希港
I. G. Farben 公司的化工厂因爆炸起火被毁，死亡近200人，受伤几千人，损失1500万美元。

1948. 9.22——中国，香港
仓库失火，化学物品爆炸，死亡135人，伤57人。

1953.10.16——马萨诸塞州，波士顿
美国LEYTE号航空母舰爆炸起火，死37人，伤40人。

1956. 8. 7——哥伦比亚州，Cali
七辆装有黄色炸药的卡车爆炸，估计死1100人。

1958. 6.23——巴西，圣阿马罗
焰火爆炸，约100人死亡。

1960. 3. 4——古巴，哈瓦那
法国军火船爆炸，死亡75～100人，伤200人。

注：以上资料取自美国百科全书。

表 2　职业事故统计

(1958～1964年，每年损失)

	联　邦　的	全　国　的
死　亡	1,200	13,800
受伤丧失劳力	300,000	1,960,000
损失劳动日	18,500,000	235,000,000*

* 相当于990,000人一年的工作量。

第二章

关于系统安全学科的发展

随着第二次世界大战而来的工业技术飞速发展，美国工业界开始从“系统”的角度考虑问题。韦伯斯特把“系统”定义为某些有规律的相互作用或相互关联的事物的集合。按韦氏的描述，哲学是对现实世界及人类本性与行为的事实与规律进行研究的科学，它包括逻辑学、伦理学、美学、形而上学及认识论。把这两个定义与第一章中“安全”的定义结合起来，我们可以得到对“系统安全学科”的定义，即：“用逻辑方法和已有认识调查研究各种事实，以保证人员和设备在一定环境中和谐工作，免受意外或偶然事故损害或伤害的科学。”

系统安全学科的这一定义，包含着事前对事故进行定义、分析、预防的概念。在用这个定义对系统安全基本原理加以表述时，人们很可能会问，这岂不是系统工程的任务吗？对，是这样的。然而，如果我们认为系统安全只是设计师和（或）工程师的任务，那么，经验业已证明，那将会形成无人负责从而事故丛生的局面。让我们考察一个典型的例子，即一个早已从美国空军库存清册中撤销的井下发射的弹道导弹计划。这个重要武器系统设计于五十年代末期，那时国际上政治压力极大，亟需研制能用运载工具发射的核弹

头，作为一种主要威慑手段，以遏止世界爆发全面核战争。在该系统研制过程中，大力应用图 3 所示的同时并进的研制原则。提出这个原则是试图缩短武器系统从方案选定到具有初步作战能力所需的时间。诚然，许多改进与改型工作要花更多金钱。但是，面对着世界核威胁，自然会得出这样的结论：通过追加费用去赢得时间，这是合算的，因而竭力采用同时并进的研究方法。

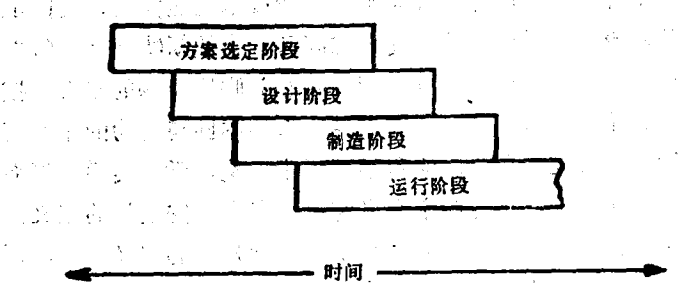


图 3　同时并进原则——系统寿命周期各阶段的划分

遗憾的是，系统安全没有被当作专门的职责加以确定，而被认为只是所有设计师和工程师的事。另一方面，技术发展与系统复杂性的问题又带来了迟迟未被注意的大量接口问题。在达到初步作战能力后不到18个月内，上述武器系统就出现了四次较大的事故，每次都使导弹和（或）发射井系统损失几百万美元。事后调查结果表明，安全措施缺陷严重，需要制订彻底改进计划加以弥补。事实上，这种改进费用极其高昂，以致决定弃置整个武器系统而加速布署现存的“民兵”导弹系统。这样，原设计服役期至少为十年的主要武器系统，实际使用还不到二年，主要原因在于安全上具有缺

陷。一些较严重的缺陷包括以下几点：

1. 燃料和氧化剂（JP-4和液氧）的储存与输送管道并排安装，理论上可以断定这不会有问题，但是经验表明，在大量输送推进剂的过程中，泄漏在所难免。垫片会从法兰盘挤出，填料会从泵或阀门中跑出，膨胀和收缩会引起疲劳破裂，或者，锈蚀与腐蚀可导致管道破裂。而管道使用期越长，就越有可能发生上述事故，从而出现泄漏，并可能带来不幸后果。

2. 柴油发电机废气也是从地下井总排气管排放的，而废气中可能含有丰富的氧气。事实上，这就开始孕育一场重大事故，因为含有丰富燃料的发电机废气一旦与氧混合起火，就会引起一系列火灾与爆炸。

3. 在远距离发射控制室中，没有任何直观监视系统供发射操作人员判断井下出现的问题是大是小。由于可能有严重的危险，维修人员不能在情况不明时贸然进入井下，小问题得不到及时识别、解决，结果演变成重大事故。

4. 作为主供电电源的柴油发电机要求在远距离发射控制中心连续操作，而又没有操作人员用直观检漏及监听将会发生故障的信号，理论上这是可能的，然而，经验再次证明，为了防止事故，操作人员必须始终亲自在场看管发电机，别人绝不能代替。

5. 实际上，在发射井中没有自动消防设备，只是在井的周边装有集水系统，然而这对电火、对液氧燃料或金属材料的起火是无济于事的。

且不论忽视安全要求给经济带来什么损失，只说原子裂变的出现带来了一个什么独特的问题，一次偶然的原子爆炸

的灾难性后果如此严重，以致一次事故也不能容许。由于安全的缘故，美国原子能委员会对使用和搬运核材料已规定了极为严格的控制要求。此外，国防部通过国际原子支援局对所有核武器的设计与使用都保持严密的控制。为适应这些部门的要求而采取的控制措施，对于五十年代末确认系统安全为一门独立的学科具有重大影响。然而，直到1962年4月，才出版了《空军弹道导弹研制工作的系统安全工程》这第一个军用规范（弹道系统部文件62—41）。同年（1962年）秋，根据1962年9月15日发布的弹道系统部文件62—82号《武器系统安全规范WS113B》"民兵武器系统计划"把系统安全作为合同中的单独条款。

从此，系统安全受到越来越多的注意。在空军导弹计划中尤其如此，这是因为导弹试验次数有限，而且如本章前面的例子指出的那样，事故的后果严重。1963年6月，第53届空军工业界联合会议全力讨论系统安全问题。这一年9月，美国空军出版了MIL-S-38130号军用标准《军用规范——对于系统、有关子系统以及设备的安全工程的一般要求》。1966年6月，国防部修订这一规范（MIL-S-38130A），并要求在所有国防合同中加以应用。

1969年7月，这个规范又被修订为Mil-Std-882号军用标准《关于系统、子系统及设备的系统安全计划的要求》。为了便于了解这个军用标准的范围，下面摘录其4.1节"系统安全计划的一般要求"的内容：

> 承包商应制订和维护有效的系统安全计划，通过统一安排，使之贯穿于系统研制、生产及作战使用的所有阶段之中。系统安全计划应规定严格的途径，运用方法