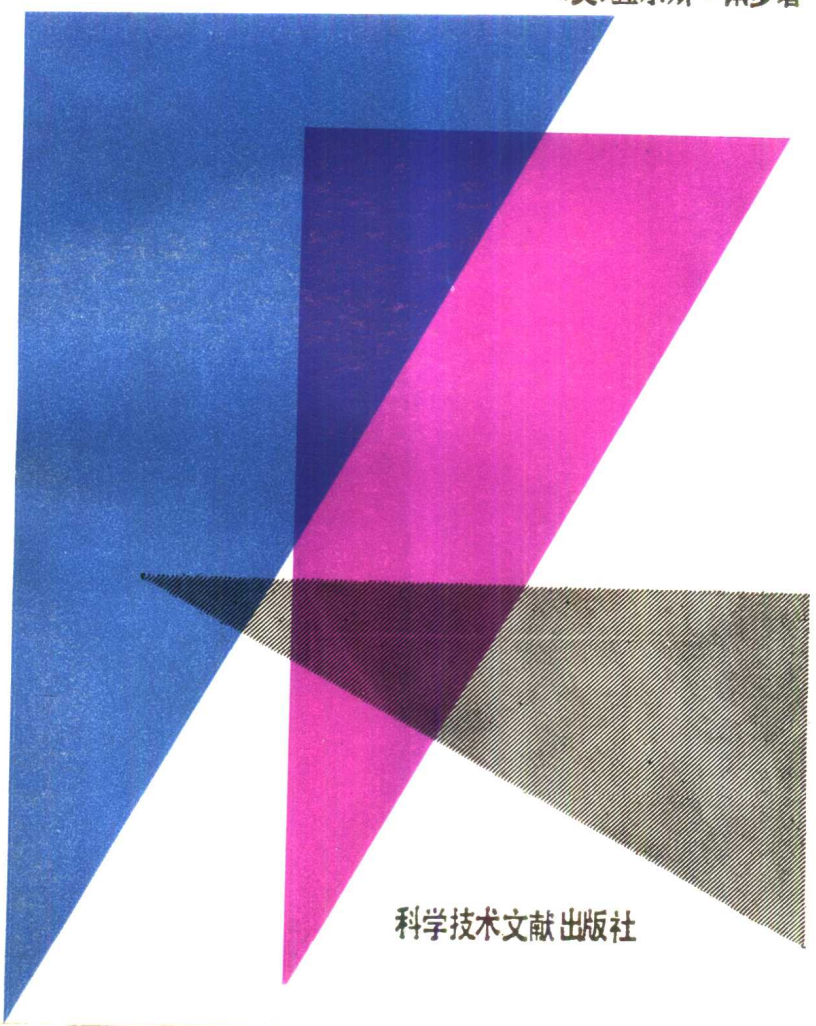
高风险技术与“正常”事故

〔美〕查尔斯·佩罗著



科学技术文献出版社

高风险技术与"正常"事故

〔美〕查尔斯·佩罗著

寒　窗译　柯洛斯校

科学技术文献出版社

1988

内 容 简 介

现代社会的生存与繁荣离不开技术，但许多技术系统又难免发生事故，给人类造成巨大的灾难。为什么有些技术系统几乎不可避免地要发生事故？是否只要提高警惕，就一定能做到防患于未然？人们应当怎样对待高风险技术？美国耶鲁大学社会学教授查尔斯·佩罗提出了许多发人深省的问题并试图给以回答。

本书深入浅出，案例丰富，适于决策人员、管理人员、工程设计人员和广大理工科学生阅读。

Charles Perrow

Normal Accidents

Living with High-Risk Technologies

Basic Books, Inc., Publishers

1984

高风险技术与“正常”事故

〔美〕查尔斯·佩罗著

寒 军译 何洛斯校

科学技术文献出版社出版

中国科学技术情报研究所印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

787×1092毫米 32开本 10.25印张 220千字

1988年5月 北京第一版第一次印刷

印数：1—3000册

社科新书目：198—011

统一书号：17176·483 定价：2.65元

ISBN 7-5023-0560-2/C·5

译者的话

继美国三里岛核电站事故之后，1984年底在印度博帕尔发生的毒气泄漏事故再次向世人敲响警钟：许多技术系统在为人类造福的同时，也对人类构成了威胁。怎样认识和解决这个矛盾？这是本书作者提出的问题。

作者的基本观点是，许多技术系统都具有子系统之间配合紧密、相互作用复杂的特点。系统的这种固有性质就是高风险技术系统易于发生事故的原因。求助于越来越多的安全装置不仅不一定能使技术系统免于事故，有时它们反而成了事故之源。从这个意义上说，技术系统的事故是不可避免的、是“正常”的。他批驳了动辄将事故归咎于操作者失误、归咎于系统设计的缺陷等一些传统的错误认识。显而易见，我们将与许多业已存在的高风险技术长期共存，还有一些具有潜在危险的新技术很快就要问世。如何控制和调节前者？如何评价与发展（或摒弃）后者？作者提出了一个新颖的半定量的分析框架，对社会中各种系统（包括技术系统与组织系统）的配合松紧程度与相互作用的强弱程度进行了分析，接着，就应当改进哪些技术系统、限制哪些技术系统的问题提出了建议。

科学技术现代化是实现四个现代化的关键，我们正在大力发展科学技术，因此，佩罗教授提出的问题也同样严峻地摆在我们面前。我们相信，本书阐述的思想对于理工科的广大研究生和大学生具有相当程度的启发意义，而对于工程设计人员、科学技术管理人员和负责安全工作的领导干部则更

具有直接的参考价值。读者通过本书提供的大量生动的技术系统事故案例以及对这些案例的分析可以学到许多东西。

作者用深入浅出的语言讲清了复杂深奥的问题，叙述生动，见解独到，例证丰富。对于书中行文过于累赘之处，我们在翻译时作了必要的删节。

本书的导言、第一章与第二章由武夷山同志翻译，第三章与第四章由金炬同志翻译，第五章与第八章由彭强同志翻译，第六章与第七章由李保炬同志翻译，第九章由李耕耕同志翻译。柯洛斯同志总校。

一九八五年六月

导　言

欢迎您光临高风险技术的世界。您也许已经注意到，高风险技术似乎正在迅速增加。一点儿不错。在技术不断扩张、战争此伏彼起、人类日益侵入自然的同时，人类创造的系统——即组织，以及组织的组织——使操作者、车船机的乘客、无辜的在场者和后代面临的危险与日俱增。本书将要评价这样一些系统——核电厂、化工厂，飞机和空中交通控制，船舶，水坝，核武器，太空行动和遗传工程。这些危险的系统大部分都具有酿灾潜势，能一举夺去千百人的性命，缩短成千上万人的寿命，或使几百万人变成残废。这样的系统正在逐年增多。这真是坏消息一桩。

本书给您带来的好消息是，如果我们能够较深刻地理解风险系统的性质，也许就能减轻甚至消除这些危险。为了实现这点，我在这里就必须提供许多坏消息。但是，我们之所以进行这番研究，是因为看到了有可能将高风险技术管理得更好。我们可以在许多方面做出改进，这些我不详论，因为它们都是明显不过的——改善操作人员的培训，加大设计的安全系数，加强质量控制，进行更有效的管制，等等。政府部门和工业界的专家们正在上述方面努力工作。我对这些努力的成效并不过分乐观，因为，风险增大的速度似乎比降低风险的势头来得快。不过，这已不属本书的讨论范围了。

我将详论高风险技术的特征。这些特征表明，不管常规的安全措施是多么有效，仍有一种事故是不可避免的。对于酿灾潜势很大的系统（如核电厂，核武器系统，重组

DNA*的生产，或载有剧毒物或易爆物的船舶），这可不是好消息。举例来说，这意味着核电厂熔融造成放射物质扩散到大气中的概率不是百万年一次，而更可能是今后十年内就将发生一次。

大部分高风险系统都具有某些特征（不是指剧毒、易爆、造成遗传缺陷这样一些性质），使得事故是不可避免的，甚至是“正常”的。这与故障的相互作用方式，与系统各部分的相互关联方式有关。我们可以分析一下这些特征，以便更好地懂得，为什么这些系统会发生事故，为什么事故的发生几乎是必然的。懂得了这些，我们就能较为理直气壮地提出，某些技术应当放弃，而对于另外一些不能放弃的技术（因为我们这个社会的一大部分就是围绕这些技术建立的），则应当加以改造。高风险系统的风险不可能完全消除。能消除其风险的系统顶多不过那么几个。然而，我们至少可以做到不再瞎责备人，不再乱找原因，不再把系统修补得更容易出事故。

基本论证过程很简单。分析的起点是一座工厂、一架飞机、一只船、一个生物实验室或其他包含许多组元（零件、程序、操作者）的系统。然后，组元之中有两个以上出了故障，这些故障以预料不到的方式相互作用。没人会想到甲出故障时乙也出毛病，两个故障相互作用的结果，既引起了火灾，又使火灾报警器失灵。再者，当时没人能弄懂这种相互作用，因而不知所措。这些问题总归是设计者们从来没想到过的。下一次，他们会再增添一个报警系统和一个灭火器，但是天晓得，也许这回不可避免的故障之间又发生了三种预

*DNA即脱氧核糖核酸，后文同，——译注

料外的相互作用。这种发生相互作用的倾向是系统的特征，而不是系统零件或操作者的特征。我们称此为系统的“相互作用的复杂性”。

对于某些具有这种复杂性的系统（如大学，研究和发展实验室），事故不会蔓延开去，不会太严重，因为这些系统中总存在着许多松弛环节，总有处理事故的时间，总可能用其他方式解决问题。但是，假设系统又是“紧配合”的，那会怎么样呢？所谓紧配合，是指过程发生得很快，无法止住，或无法将出故障的零件与其他零件隔离开，或不存在能够维持安全生产的第二种方法。此时，就不可能从最初的扰动状态复原；这一故障将迅速地、势不可当地蔓延开来（至少得蔓延一段时间）。安全系统和操作者采取的行动也许使局面更糟，因为一时还不清楚问题到底出在哪里。

或许，许多生产过程在最初的时候都是这样的——相互作用方式复杂，配合紧密。但是，随着经验的积累，出现了更好的设计、设备和工艺程序，于是避免了预料外的相互作用，降低了系统的配合程度。但是，对于本书将考察的大部分系统，似乎无论是组织改善还是技术创新都不能使它们发生系统事故的趋势有所减弱。这些系统所要求的组织结构有着很大的内在矛盾；这些系统求助于一些技术药方，但技术药方进一步增大了相互作用的复杂性，进一步加强了配合程度。于是，系统变得更容易发生某些事故了。

如果说，相互作用的复杂性与紧配合——这是系统的特征——将不可避免地导致事故，那么我相信，称这种事故为**正常事故**或**系统事故**是无可非议的。采用**正常事故**这一古怪的用语是想表明，由于系统的上述特征，故障之间的预料外

的多重相互作用是不可避免的。这一概念反映了系统的总体特征，而不反映发生事故的频率。人总是要死的，死亡是正常的，但是人只会死一次。系统事故并不常见，甚至可以说是罕见的，但是这些事故会造成大灾难。罕见并不能使人宽心。

介绍正常事故或系统事故这一概念的最好办法，是假想一个以日常生活经历为基础的例子。这应该是我们大家都熟悉的经历：某一天里，似乎一切都乱了套。

百事不顺的日子

这天上午你打算进城去进行谋职面试，这是好不容易才争取到的机会。当你做早餐时，爱人已经出门半天了。倒霉的是，她临走前忘了关火，煮咖啡的玻璃壶也没拿下来。咖啡煮干了，玻璃壶烧裂了。你喝咖啡成瘾，于是就在壁橱里大翻一通，终于找出一只内分三层的旧式咖啡壶。你一边望着钟，一边等水开。煮好后，你急匆匆地喝了一杯就冲出门去。跑到汽车跟前，你才发现忙乱间把汽车钥匙（和房门钥匙）忘在屋里了。没关系，为了对付这种意外事件，你平时在过道里藏着一把备用房门钥匙。但是你突然想起，备用钥匙已在几天前的一个晚上交给一位朋友了，因为他打算来取几本书，而你知道他来取书时你会不在（备用钥匙好比是一条工程师所说的冗余通道，现在给堵上了）。

时候已经不早了，只好赶快向邻居借车，邻居是一位和蔼的老绅士。他每月大概只用一次车，平素车保养得很好。你敲敲他的门，借车的话头已经准备好。但是他告诉你，事

不凑巧，上星期他汽车的加速器坏了，这天下午就要来人将加速器取走修理。又一个“备用”系统失效了。这一次与你的行为根本没有关系（在本例中，钥匙与加速器几乎没有关联，忘带钥匙与加速器出故障二者是**无配合事件**，或叫独立事件）。那么，公共汽车总没问题吧。且慢，并非总没问题。在你敲门前，那位和蔼的老绅士一直在听广播，他告诉你刚听见的消息：公共汽车公司停业了，以对付司机们拒绝驾驶他们认为不安全的一些汽车并要求提高工资的举动（你瞧，别的不说，你认为不会出问题的安全系统——公共汽车，照样跟你作对）。你到邻居家打电话要一辆出租车。但是由于公共汽车停驶，此刻你一辆出租汽车也要不到（公共汽车停驶与出租汽车缺乏这两个事件是密切联系着的，因为是一个事件触发了另一事件，它们是相关事件，或者叫**紧配合事件**）。

你打电话给约你面谈的那位女士的秘书，说：“一时半会儿我真讲不清，总之今天上午什么倒霉事都让我碰上了，我不能如约见汤普森女士了。请重新安排一个时间好吗？”你对自己说，下星期我要安排好两辆小汽车和一辆出租汽车，要亲自煮早餐咖啡。接电话的秘书回答说“没问题”，但他心里面却说，“这个人显然办事不稳重。催了几个星期要与汤普森会面，最后说来不了。”他在备忘录上写下了大意相同的几句话，然后有意识地安排了一个下周最不方便的时间，汤普森女士恐怕不得不取消排在这个时间的活动。

现在我请你就此事件填写一个简短的调查表。问题：这一“事故”或故障的主要原因是以下的哪一项？

1．人的过错（如没关咖啡壶下面的电热器，匆忙间忘

了带钥匙）？是___不是___拿不准___

2．机械故障（邻居汽车的加速器）？是___不是___拿不准___

3．环境（公共汽车停驶，出租汽车供不应求）？是___不是___拿不准___

4．系统设计（现在的设计造成了把自己锁在房门外的可能性。如果不用门钥匙就锁不上门，情况就不同了。出租车队缺乏应付意外情况的能力）？是___不是___拿不准___

5．办事程序不当（如用玻璃壶煮咖啡；出发时间太晚，未留余地）？是___不是___拿不准___

最合适的回答不是“以上各条都对”或其中的任何一条对，而是“以上各条一条也不对”。（当然，我没有将这一条列出供你们选择）事故的原因在于系统的复杂性。也就是说，每一故障（设计、设备、操作者、程序、环境）本身都算不上什么太严重的问题。既然不存在完美的事物，就应当估计到会发生这些故障。通常我们不太注意这些故障。如果你的汽车钥匙在身上，或邻居的汽车能用，那公共汽车停驶影响不了你。如果能叫到出租汽车，邻居汽车的加速器坏了也于事无妨。若不是这次面试很重要，没小汽车、没公共汽车、没出租汽车都无所谓。换上其它任何一天的早晨，即便咖啡壶坏了令人扫兴，但也不至于增添你的焦虑，使你出门忘了带钥匙。

虽然这些故障本身没什么了不起，而且每样东西都有备用系统（或者说，若主要通道堵塞了，还有冗余通道可走），但是当它们相互作用起来的时候，问题就严重了。对

这个事故，只能用多重故障的相互作用来解释。我们能估计到，公共汽车有时会停驶；我们也能估计到，使用那种撞锁，会出现忘带钥匙的情况（否则为什么要藏一把备用钥匙呢？）。我们想不到的是，所有这些事件一起发生。所以你才会在电话上对汤普森的秘书说，“讲不清楚”。墨菲定律（即，任何事物，只要有可能出毛病，就迟早会出毛病）在我们身上应验了。

那一事故的原因在于那天早晨我们面临的情景是相互作用的、与紧配合的，而不在于个别的故障，因为那些故障应当是可以估计到的，并且每一故障都有备用系统来对付。大部分时候，我们注意不到生活中存在的固有的配合现象，因为大部分时候没出故障，或虽然出了故障，但故障之间并没发生相互作用。可是突然之间，我们过去没想到会发生相互联系的事物（公共汽车与加速器，咖啡和借给别人的钥匙）之间发生了联系。突然之间，系统的配合变得比我们原先认识到的更紧了。如果相互作用的系统同时又是紧配合的，那么这些系统发生此类事故就是“正常”的，尽管不是经常的。说它正常，并不是指系统事故经常发生和能预料得到——事实上它既不经常发生，又预料不到，正因为如此才使我们不知所措。这里的“正常”是说，系统不时地经受这种相互作用，这是系统的内在性质。三里岛事故便是这样一种正常事故或系统事故。本书将考察的其他许多事故也是正常事故。我们之所以有这种事故，是因为我们建成了这样一个工业社会，该社会的某些部分（如大型工厂企业或军事活动）包含着高度相互作用、紧配合的单元。不幸的是，有些高相互作用、紧配合系统的酿灾潜势很大。

我们通过“百事不顺的日子”的例子介绍了一些有用的术语。事故可由**多重故障**引起。上例分析了产生故障的五个组元：设计、设备、程序、操作者和环境。将此概念应用于一般的事故，则必须加入第六种组元——供应品和材料。这六种组元缩略为DEPOSE*组元。上例说明，系统的不同部分可能发生很强的相互依存关系（如公共汽车停驶造成出租车不足），这种依存关系称为**紧配合**。从另一方面说，系统中的各事件亦可独立发生（如加速器出故障与忘记带钥匙），这些是**松配合**事件。它们虽然都属于同一个事件发生序列，但一个事件并不是由另一事件引起的。

还有一点是上例无法说明的。该例并不是正常事故或系统事故的最好例证。在该例中，事件的相互依存关系是人即“操作者”能够理解的。虽然他既影响不了单个的事件，又影响不了这些事件的相互依存关系，但毕竟能理解这种相互作用。在复杂的工业系统、空间系统和军事系统中，当我们说到正常事故时，一般（但并不总是）含有这样的意思：相互作用不仅是预料外的，而且在紧急关头是**不可理解**的。部分原因在于，这种人机系统中的相互作用确实是看不见的（这里，“看不见的”取其本义）；另一部分原因在于，即使能看见这种相互作用，人们也不相信。以后我们将会明白，人们不一定以“眼见”“为实”。有时候，我们必须首先相信“为实”，然后“眼”才能“见”到。

---

*DEPOSE是设计（Design）、设备（Equipment）、程序（Procedures）、操作者（Operators）、供应品和材料（Supplies and materials）、环境（Environment）这六个组元的英文字头拼成的。——译注

提　要

第一章考察三里岛事故。该事故由四个独立的小故障引起，操作者有可能发现不了其中任一故障。不是操作者，而是系统引起了这一事故。第二章提出的问题是，如果这些核电厂那么复杂，配合那么紧，可为什么没出现更多的“三里岛”事故呢？对核电业及该行业中的一些大小事故的分析表明，三里岛核电厂这种大规模的核电厂尚未得到充分的时间显现其酿灾潜势。

有了关于复杂性、配合、灾难这样一些概念的粗糙的定义，我们就能讨论许多问题。但是，为了更深入地探索高风险系统的世界，我们还需要更准确的定义，需要系统、事故及其后果的更好的模型。这便是第三章的内容。第四章是将关于复杂性、配合与灾难的理论应用于化学工业。关于故障之间的预料外的相互作用，该章给出了一些最有趣、最离奇的实例。

第五章中，我们要进入周围环境，考察飞机和飞行、空中交通控制、机场、空中航线等等内容。总体说来，飞行系统是很复杂的、配合很紧的。飞行是冒险的，现在如此，将来永远如此。另一方面，我们将考察，人们如何通过组织变革与技术发展真正降低了航线系统的复杂性与配合程度。就具有内在危险性的系统的安全标准来看，航线系统已发展得很安全了。第六章论述关于水运的风险，它所揭示的情形正好相反。人们既未能降低系统的复杂性，也未能减弱其配合程度。

第七章似乎有些离题，因为水坝、湖泊、矿井并不容易发生系统事故。不过，水坝之类的事故之所以可以预见和可以避免，正因为它们是线性系统而不是复杂系统。这就支持了本书的观点而不是离题。另外，若将眼光从个别的水坝或矿井再放远些，考察一下它们存在于其间的更大的系统，我们就会发现存在着一种“生态-系统事故”。

第八章讨论的系统要深奥得多。空间行动虽然是紧配合的复杂系统，但是它的酿灾潜势从来就很小，现在就更小了。更重要的是，这种系统有助于我们考察操作者的作用。核武器方面的事故表明，该系统是如此复杂，如此易于出错，以致我们这个地球更可能毁于某人的漫不经心而不是某人的勃然大怒。这种前景是很可怖的。该章中讨论基因分裂或重组DNA的一节同样是可怖的。

最后一章专门谈论新型巫师——风险评估专家和无形之中成了他们的同盟者的认知心理学家。最后，我们将总结考察过的各种系统的优点与缺点，并提出几条小小的建议。

目　录