

后浪出版公司

崩溃

MELT DOWN

Why Our Systems Fail and What We Can Do About It

Chris CLEARFIELD
and
András TILCSIK

[美] 克里斯·克利尔菲尔德
安德拉什·蒂尔克斯 著

李永学 译

四川人民出版社

后浪出版公司

Why Our Systems Fail
and What We Can Do About It

Chris CLEARFIELD
and Andrius TILCSIK

〔美〕 克里斯·克利尔菲尔德
安德拉什·蒂尔克斯 著

李永学 译

崩

潰

崩

潰

MELT DOWN



四川人民出版社

图书在版编目 (CIP) 数据

崩溃 / (美) 克里斯·克利尔菲尔德, (美) 安德拉什·蒂尔克斯著; 李永学译. -- 成都: 四川人民出版社, 2019.5

ISBN 978-7-220-11182-2

I. ①崩… II. ①克… ②安… ③李… III. ①决策学
IV. ①C934

中国版本图书馆 CIP 数据核字 (2018) 第 300312 号

Meltdown: Why Our Systems Fail and What We Can Do About It
Copyright © 2018, Christopher Clearfield and András Tilcsik, 2018

本书中文简体版权归属于银杏树下 (北京) 图书有限责任公司。

四川省版权局
著作权合同登记号
图字: 21-2018-622

BENGKUI

崩溃

著 者
译 者
选题策划
出版统筹
特约编辑
责任编辑
装帧制造
营销推广

[美] 克里斯·克利尔菲尔德 [美] 安德拉什·蒂尔克斯
李永学
后浪出版公司
吴兴元
方 丽
林袁媛
墨白空间·曾艺豪
ONEBOOK

出版发行
网 址
E - mail
印 刷
成品尺寸
印 张
字 数
版 次
印 次
书 号
定 价

四川人民出版社 (成都槐树街 2 号)
<http://www.scpph.com>
scrmcbs@sina.com
北京盛通印刷股份有限公司
143mm × 210mm
10.75
250 千
2019 年 5 月第 1 版
2019 年 5 月第 1 次
978-7-220-11182-2
68.00 元

后浪出版咨询 (北京) 有限责任公司常年法律顾问: 北京大成律师事务所 周天晖 copyright@hinabook.com
未经许可, 不得以任何方式复制或抄袭本书部分或全部内容
版权所有, 侵权必究

本书若有质量问题, 请与本公司图书销售中心联系调换。电话: 010-64010019

本书献给愿意倾听我们的呼吁者、陌生人和领袖们。

我们需要更多你们这样的人。

献给琳妮娅、托瓦尔德和苏林。

——克里斯·克利尔菲尔德

献给我的父母和马文。

——安德拉什·蒂尔克斯克

meltdown / 'melt · daʊn / 名词

1. 核反应堆中的事故，燃料过热，导致反应堆芯熔化；起因或为地震、海啸、鲁莽测试、寻常的错误，也可能只是阀门堵塞。
2. 系统崩溃或失灵。

目 录

引言 普通的一天	1
----------	---

第一部分 我们周围的种种故障

第 1 章 危险区	15
第 2 章 深水,新地平线	37
第 3 章 黑客、欺诈以及不便刊载的新闻	61

第二部分 征服复杂性

第 4 章 走出危险区	89
第 5 章 复杂的系统,简单的工具	109
第 6 章 审视不祥之兆	135
第 7 章 解剖异端	167
第 8 章 减速效应	197
第 9 章 异乡异客	221
第 10 章 意 外	247

结语 大崩溃的黄金时代	271
-------------	-----

致 谢	277
-----	-----

注 释	283
-----	-----

引言 普通的一天

“‘空’这个字上打了引号，这一点吸引了我的注意。”

I

6月的一个温暖的周一¹，刚好在下班交通高峰期之前，安·惠雷（Ann Wherley）和戴维·惠雷（David Wherley）搭上了开往华盛顿的112号地铁列车的第一节车厢。他们参加了医院对志愿者的培训，正要回家。车厢靠前端的一位青年女子起身让座，惠雷夫妇一起坐下。他们从中学时代起就像这样形影不离。戴维62岁，最近刚退休，他们正期待着自己的40周年结婚纪念日，届时他们会去欧洲旅游。

戴维曾经是屡立功勋的战斗机飞行员、空军军官。事实上，在“9·11”事件中，他正是那位下令战机紧急起飞，在华盛顿上空盘旋巡航的上将。²在他的严令之下，战机驾驶员酌情处理，击落任何威胁这座城市的客机。尽管他是一位空军上将，他却不肯乘坐由司机驾驶的豪车。他喜欢乘坐地铁。

下午4时58分，列车驾驶员拉动了紧急制动闸，刺耳的金属摩擦声打断了车轮有节奏的咣当声。然后，112号列车撞上了什么东西：那是一辆不知为何停在轨道上的列车。碎玻璃和弯曲的金属件四下横飞，夹杂着乘客的尖叫。冲击之下，大堆破碎的座位、车顶碎块和金属棒形成了一堵13英尺（1英尺=0.3048米）厚的碎片墙。这堵墙冲进112号列车，造成安·戴维和另外7人丧生。

这样一次相撞本来是可以避免的。整个华盛顿地铁系统由100多英里（1英里=1609.344米）的铁轨组成，全部联网，列车运行也受到监控。当列车相互靠得过近时，它们会自动减速。但那天，当112号列车转过一个弯道时，另一辆列车出现在它前面的铁轨上。这是真实世界中的事件，而轨道传感器居然没有发现。112号列车自动加速，因为根据传感器检测，前方道路畅通无阻。等到驾驶员看到停在那里的列车并紧急制动时，相撞已经不可避免。

就在救援人员从残骸中抢救受伤人员时，地铁工程师也投入了紧张工作。他们必须保证其他列车不会发生危险。为了做到这一点，他们必须解决这个不解之谜：一列两个足球场那么长的列车是怎样消失的？

II

像112号列车遭遇的这类警报器失灵的故障时有发生。不妨让我们看看下面的一份清单，这是一周内发生的新闻事件标题：

- 巴西发生矿难
- 新的一天，又一次黑客行为：盗用信用卡的恶意软件袭击连锁旅店
- 韩国现代汽车公司因制动开关失灵召回汽车
- 弗林特水危机正在发酵，华盛顿的“政府失误”
- “情报机构大规模失误”导致巴黎多次恐袭
- 温哥华蒙冤入狱近 30 年的男子诉讼案最终尘埃落定
- 应对埃博拉病毒：科学家抨击“极端脆弱的全球系统”
- 7 岁孩童被谋杀一案的调查，系统失误，未能提供保护
- 印度尼西亚用火烧清理土地却导致大规模野火，造成生态灾难
- 美国食品和药物管理局调查在华盛顿和俄勒冈墨西哥餐厅发生的大肠杆菌爆发事件

看上去这一周似乎特别糟糕，但这其实完全没有什么特殊之处。很少有哪一周没有几件灾难性的崩溃事件。这一周是工厂事故，下一周则是哪家大公司破产，再过一周又会出现一件可怕的医疗失误。即使是小问题也会导致大破坏。例如，近年来就有几家航空公司因为技术系统故障而导致所有航班停飞，旅客滞留多日³。这些问题自然会让我们生气，但我们对此已经司空见惯。生活在 21 世纪，我们依赖着数不清的复杂系统，它们深刻地影响着我们的生活——从输电网到净水处理工厂，从交通系统和交流网络到医疗保健，一直

到法律诉讼。但有时候，这些系统让我们陷入困境。

灾难有时是大规模的，如英国石油公司（BP）在墨西哥湾的石油泄漏、日本福岛的核灾难，以及全球金融危机，它们似乎源于各自不同的问题。但从本质上来说，这些灾难的根源惊人地相似。这些事件有着共同的 DNA，而研究人员对此才刚刚有所认识。有共同的 DNA 意味着，某个行业中发生的事故可以为其他领域的人提供经验教训：牙医可以从飞行员那里学到东西，营销团队可以从特警队身上吸取教训。理解深水探测和高海拔登山这类高风险新奇领域中发生灾难的深层原因，也能使我们获得经验教训，理解日常系统中的灾难。事实证明，日常生活中的崩溃事件，如项目失误、招工对象不当，甚至是聚餐不欢而散这类事件，跟石油泄漏和登山死难这类事故有许多共同之处。幸运的是，全球的研究人员在过去几十年间已经找出了一些解决方法，它们可以为我们提供借鉴，告诉我们应该如何做决定、建立团队、设计系统、防止越来越普遍的各种崩溃事故。

本书分为两部分。第一部分探讨系统为什么会失灵，揭示看上去风马牛不相及的事件背后隐藏的共同原因，这些事件包括星巴克的社交媒体灾难、三里岛核事故、华尔街大崩盘，以及英国偏远小城镇邮局中发生的离奇丑闻。第一部分也探讨了进步的悖论：我们的系统能力更强了，但同时它们也变得更复杂，要求更高，结果造成了那种小失误便可酿成大错的局面。曾经无关痛痒的系统现在可以偶尔损伤人命、让公司破产、让人蒙冤入狱。第一部分也告诉人

们，那些使我们的系统面对偶然发生的崩溃无能为力的变化，也为黑客行为与欺诈这类有意识的犯罪提供了沃土。

第二部分是本书的主体，我们会在这部分探讨可行的解决办法。它告诉我们，人们如何从小失误出发，找到重大威胁发源之所：接待员如何通过向上司汇报情况而挽救一条鲜活的生命；开始时被飞行员讥为“魅力学校”的训练计划如何让他们的飞行变得前所未有的安全。这一部分我们将考察多样化如何帮助我们避免大错误，以及从珠穆朗玛峰的登山家和波音公司的工程师那里我们能了解到简洁的力量。我们将学习电影团队和急诊室工作人员处理危机的方法，这些方法又如何拯救了操作失误的脸谱网（Facebook）首次公开募股，挽回了塔吉特百货公司（Target）失败的加拿大扩张。我们也将重新思考地铁列车未被感应到这一谜题，并看看工程师对这一悲剧的分析结果。

我们写作本书时使用了两个不同的途径。克里斯的职业生涯始于证券与金融衍生品交易员，他在自己的交易桌前目睹了雷曼兄弟银行（Lehman Brothers）的倒闭和全球股市的动荡。大约就在那时，他开始了飞行员训练，并对避免灾难性错误这一问题产生了浓厚的兴趣。安德拉什一直在学术领域，研究为什么企业组织机构会因为复杂化而举步维艰。几年前，他首创了一种叫作“组织机构灾难性失灵”（Catastrophic Failure in Organizations）的课程，让来自不同背景的经理人聚在一起，研究各种重大的灾难事件，在日常崩溃事件上分享他们的经验。

这本书的写作素材来自事故报告、学术研究资料和对各种人物（从首席执行官到第一次购置房产的人士）的广泛访谈。我们从中发现的设想可以解释各种崩溃事件，并给所有人提供能够使用的实际洞见。在一个灾难频仍的年代，这些设想有助于人们在工作与个人生活中，在管理组织机构时，以及在应对某些最重大的全球挑战时，做出正确的决定。

III

在本书写作过程中，我们采访的第一批人中就有本·伯曼（Ben Berman），他是美国国家航空航天局（NASA）的研究人员、机长，曾担任事故调查员，并拥有哈佛大学经济学学位。按照他的解释，要理解微小改变如何防止重大崩溃，航空业从各方面来说都是理想实验室。⁴

每一架航班出事的概率可以忽略不计，但是每天有 10 万多架商业航班起航，许多故障都在脱离掌控酿成大祸之前，就被检误测试和警告系统这类监测系统发现了。⁵

尽管如此，事故仍会发生。而发生事故时，我们会获得大量的数据资料，以便查明事故的发生原因。比如驾驶舱语音记录器和黑匣子记录的机组人员的行为和有关飞机本身行为的信息，通常从旅程开始一直到事故发生。对伯曼这样的研究人员来说，这些记录至关重要。他们会细致地发掘空难现场的一切资料，以防止将来发生

类似事故。

1996年5月，一个晴朗的下午，伯曼正在纽约市和家人在一起。这时他的传呼机响了。伯曼当时正在美国国家交通安全委员会下属的“现场行动队”（Go Team）中任职，这支团队要随时待命，应对重大事故。他很快就了解了这次事故的惨状：搭载了100多名旅客的瓦卢杰航空公司（ValuJet）592号航班，从迈阿密机场起飞10分钟后消失在雷达上，接着坠毁在佛罗里达大沼泽地中。⁶ 飞行员的无线电通信记录显示当时机舱失火，但火灾因何而起却是一个谜团。

伯曼第二天抵达坠毁现场时，喷气机燃油的气味仍然在空中萦绕未去。厚稠的沼泽地上到处散落着飞机碎片，已经无法辨认出这是一架飞机。破碎的残骸掩埋在齐腰深的水下，散布在茂密的锯齿草与沼泽腐泥中。沼泽上漂浮着运动鞋和拖鞋。

搜寻队忙着清除黑色的沼泽水，伯曼则在迈阿密机场集合了他的团队，开始与负责这架航班起飞的地勤人员谈话。机坪操作员一个接一个地走进瓦卢杰地面站站长的办公室，调查人员当天在那里扎下了大营。大部分交谈类似这样：

伯曼：你注意到这家航班有什么问题吗？

机坪操作员：没什么啊，真的没有……

伯曼：你在检修飞机、进行拖机作业或其他任何时候，有没有发现什么不同寻常的事？

机坪操作员：没有，一切正常。

伯曼：有什么引起你注意的事情吗？

机坪操作员：没有，什么都没有，完全没有。

谁都没有注意到任何特殊的事情。

然而，在面谈茶歇期间，伯曼在站长办公桌上的一摞纸中注意到了一件有趣的事情。那摞纸的下面压了一张纸，纸头露了出来，上面有一个签名。签名是失事航班机长坎达琳·库贝克（Candelyn Kubeck）的。伯曼把那沓纸从文件托盘中取了出来，一张张地翻检。这些纸没什么特殊之处，只不过是瓦卢杰 592 号机的标准航班信纸。

佩剑科技公司™

运货单

No. 01041

目的地：亚特兰大，哈茨菲尔德机场，C 大厅，28 号门，瓦卢杰航空公司，GA，30320

日期：1996 年 5 月 10 日

经由：瓦卢杰航空公司（COMAT）

品种	数量	计量单位	零件号码	序号	状况	说明
1	5	件	“5 箱”			氧气罐
						“空”

但他注意到了其中一页纸：

这是一份来自航空公司维修分包商佩剑科技公司（SabreTech）的运货单⁷，其中罗列了瓦卢杰航空公司在机上的“公司材料”（COMAT），即公司所有的物资。伯曼对此很感兴趣。飞机上曾经起火，而这份文件称飞机上载有氧气罐。而且伯曼还告诉我们另外一点：“‘空’这个字上打了引号，这一点吸引了我的注意。”

调查组人员驱车前往佩剑科技公司在机场的办公室，找到了签署这份运货单的职员。他们得知，在运货单上描述为氧气罐的这些物品其实是化学氧气发生器，用来给应急氧气面罩充氧。

“那么它们是空的吗？”伯曼问。

“它们失效了，不能用了，过期了。”

这是一个很重要的示警信号。化学氧气发生器在激活时会产生大量热能，而且在错误的场合下，本来用于救人的氧气可以造成人间炼狱。如果箱子里存放的是过期的氧气发生器，也就是说，是达到了使用期限的氧气发生器，而不是空罐子，那么就相当于在飞机上装上了一颗威力强大的定时炸弹。怎么会发生这种事情？这样一件致命的货物是怎样进入一架客机的呢？

调查的结果显示，一大堆乱糟糟的错误、巧合和日常混乱凑到了一起。瓦卢杰航空公司曾购置了三架飞机，并雇用佩剑科技公司在迈阿密机场的一间机库进行修理。这些飞机上的许多氧气发生器都过期了，需要替换。瓦卢杰公司告诉佩剑科技公司，如果其中哪个氧气发生器没有耗尽（也就是说它还能造氧），就必须给它装上一

个保护盖。

但过期的氧气罐和未耗尽的氧气罐之间的区别很混乱。许多发生器过期了，但并没有耗尽。还有一些氧气罐过期了，也耗尽了。而且还有一些替换的新氧气罐，它们既没有过期，也没有耗尽。“如果很混乱，就别浪费时间去区分清楚了，于是佩剑科技公司的机械师没有去浪费这个时间，也没人认为他们应该将这些氧气罐区分清楚。”⁸ 记者兼飞行员威廉·朗格维舍（William Langewiesche）在《大西洋》（*The Atlantic*）杂志上写道：

是的，一位机械师或许可以使用瓦卢杰航空公司的工作证查阅庞大的 MD-80 维修说明书，找到 35-22-01 章，在其中的“h”行找到“保存或者处理氧气发生器”的指示。如果他孜孜不倦地在各种选项中摸索，这位机械师可以在说明书的另一个部分找到如下指示：“所有可供使用或者不可使用（未耗尽）的氧气发生器（氧气罐）都应该存放在一个专门区域，以保证每套设备不会暴露在高温或可能损坏的状况下。”如果他再绞尽脑汁地思考这些话括号内文字的含义，他或许会推导出，“未耗尽的”氧气罐也就是“不可使用”的氧气罐，而且因为他没有装运保护盖，他或许就应该按照 2. D. 部分中描述的方式，把这样的氧气罐送进某个安全区并把它们“初始化”。

而这还没有完，还有更多的细节、更多的区别、更多的术语、

更多的警示以及更多的工程用语。

总之结果就是这些氧气发生器没有装上保护盖，甚至就这么装在硬纸板箱子里。过了几周，它们被送到了佩剑科技公司的运送与接收部门。它们就这样存放在那里，一直到运送职员接到清理场地的指示。他理所当然地认为，应该把这些纸板箱送往亚特兰大的瓦卢杰航空公司总部。

这些罐子上带有绿色标签。从工艺上说，绿色标签意味着“可以修理”，但贴上绿色标签的机械师是怎么想的，我们就不清楚了。这位职员认为这个标签的意思是“无法使用”或“报废”。因此他做出了结论，认为这些氧气罐是空的。另外一位职员填写了运货单，在“空”这个词上加了引号，并标注数量为“5 箱”。而给词语加上引号只不过是他的习惯而已。

这些箱子一步步通过系统，从机械师到办事员，在机坪操作员手里进了货舱。机组人员没有发现这个问题，库贝克机长签署了航班文件。“于是，旅客们的最后一道安全防线也失效了，”朗格维舍写道，“他们很不走运，是系统杀了他们。”

对华盛顿地铁 112 号列车和瓦卢杰 592 号航班的调查揭示，这些事故都源于同一个原因：我们的系统越来越复杂了。当 112 号列车撞击事故发生时，全国公共广播电台（National Public Radio）节目制作人贾丝明·加斯德（Jasmine Garsd）刚好在靠后几节的车厢里。⁹“火车的撞击就像一部快进的电影戛然而止，”她回忆道，“在这样的瞬间，你会意识到两件事，在我们构建的这样一个庞大的机器世界