[美] Clifton A.Ericson Ⅱ 著
赵廷弟 焦健 赵远 田瑾 朱国振 译

危险分析技术

Hazard Analysis Techniques for System Safety

國防工業出版社
National Defense Industry Press
WILEY

装备科技译著出版工程资助出版

危险分析技术

Hazard Analysis Techniques for System Safety

[美]Clifton A. Ericson Ⅱ 著

赵廷弟　焦健　赵远　田瑾　朱国振　译

国防工业出版社

·北京·

著作权合同登记　图字:军-2011-018号

图书在版编目(CIP)数据

危险分析技术/(美)埃里克森(Ericson,C. A)著;
赵廷弟等译. —北京:国防工业出版社,2012.7
书名原文:Hazard Analysis Techniques for System Safety
ISBN 978-7-118-08205-0

Ⅰ. ①危...　Ⅱ. ①埃...　②赵...　Ⅲ. ①风险分析　Ⅳ. ①C934

中国版本图书馆CIP数据核字(2012)第160006号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路23号　邮政编码100048)
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本710×960　1/16　印张29　字数532千字
2012年7月第1版第1次印刷　印数1—3000册　定价98.00元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776
发行传真:(010)88540755　　发行业务:(010)88540717

译者序

安全性是产品的固有属性，安全是产品使用中不出现危险而导致事故的实时状态或条件。没有绝对的安全，只有是否可接受的事故风险。系统安全工程是系统工程的一部分，是在产品全寿命周期内，运用科学原理、工程和管理技术，及时识别危险并且采取一些必要措施，消除危险或降低风险，使事故风险达到可接受水平。系统安全工程中的关键是识别危险，随着系统的构成、行为逻辑及使用环境复杂性及事故损失的增长，在系统的研制过程中就需要投入更多的精力去识别和控制危险。

本书的作者在多个领域从事了40多年系统安全工程工作，具有深厚的理论基础和丰富的工程经验，本书是一本难得的、较为全面而体系化地描述危险、系统安全原理，特别是危险分析技术的系统安全专著，有益于我们更好地理解危险、系统安全原理，掌握危险分析的技术与工具，以便在实践中更好地应用。该书很值得从事系统安全工作的人员参阅。

本书的翻译也是一项较为艰辛的工作，译者以原貌呈现为原则，为读者提供一本易于阅读理解、忠实原著的危险分析译著。由于“safety”在国内有安全与安全性两种概念，在本译著中，译者根据前后文的含义及国内的习惯用法，分别译作安全或安全性，同时原书中的某些观点，译者不尽认同，但译著中忠实原著，在此说明。

本书由赵廷弟、焦健、赵远、田瑾、朱国振翻译，其中第1章～第3章由赵廷弟、赵远翻译；第14、16、20、22、25和26章由赵远翻译；第4章～第11章和第17章由田瑾翻译；第12、13、15、18、19、21、23、24章和附录A、B、C由焦健翻译；全书由赵廷弟负责全面技术审译，由朱国振负责英文审译。此外，戴瀛、李晓磊、彭照光、王晓云、王薇、吴洋、吴居宜、赵诺和张兆国等参与了本书的翻译工作。全书由屠庆慈和曾天翔主审。

由于译者水平有限，书中疏漏和差错之处在所难免，敬请广大读者批评和指正。

译者

2012年4月

前　言

在我40年的系统安全职业生涯中，有两个关于危险分析的问题一直困扰着我。第一，没有用于定义危险的组成和危险到事故的驱动过程的危险理论的形式化描述。第二，缺少好的参考资料来详细地描述怎样开展大数相关的危险分析技术和方法。我写这本书是为系统安全工程师和从业人员解决这些问题。本书的内容适合于有经验的专家和刚接触该领域的分析人员。

本书的一个主要特点是详细地描述了危险理论，阐明了危险—风险—事故之间的联系，并给出了图解和示例。另外，提出了危险的三个必要要素，以及危险三角模型。

本书的另一个主要特点是描述了在系统安全领域中最常用的22种危险分析方法。本书中的每种分析方法都有完整的一章对其进行描述。另外，各种描述方法的章节组织结构相似，从而给分析者可能遇到的许多常见问题提供一致性的解答。书中给出了详细的示例，帮助分析人员学习和理解分析方法。

系统安全是一个已证实的工程领域，在系统研发阶段，被用于识别和减轻危险，从而消除或降低潜在事故或意外事件的风险。系统安全的最终目的是挽救生命。我最大的希望是本书的读者能够使用这些知识，更好的理解危险识别和分析。这将帮助设计和构建安全的系统，进而挽救更多的生命。

致　谢

本书此部分很自然地要感谢许多人。本书反映了我在系统安全领域40年的工作历程。许多人感动和影响着我的人生，有太多人要列出和感谢。对那些被我遗忘的人，我很抱歉。但是由此看来有少数人将永远在我的记忆中。

首先，也是最重要的，我要感谢我的妻子 Debbie。她给我默默地支持和鼓励使我在系统安全领域很出色，这使得世界更加安全。她无私地让我全身心投入到系统安全协会和这本书的编写上。

我想致谢并将这本书献给开展民兵武器系统研制项目的波音系统安全组织。这个项目是一个严峻的考验，系统安全的实践正是从这里真正地开展起来的，我也是从这里开始系统安全工程的职业生涯的。在工作上，该组织给了我深刻的回忆，并对我的人生可能有很大的影响。Niel Classon 是系统安全领域早期有远见的领军人物，在他的带领下，该组织中的 Dave Haasl、Gordon Willard、Dwight Leffingwell、Brad Wolfe、Joe Muldoon、Kaz Kanda、Harvery Moon 和 Bob Schroder 在我的发展过程中给了很大的帮助。另外波音的管理者 Hal Trettin 在我职业生涯的早期给予我系统安全方面的指导。

在我职业生涯的后期，桑迪亚国家实验室的 Perry D'Antonio 帮助我在系统安全协会中取得卓越的成绩并成为该国际组织的主席。应用军械技术（Applied Ordnance Technology）公司的 Paige Ripani 帮我将事业转移到海军顾问这个新方向。最后，海军军械安全和安保活动（the Naval Ordnance Safety and Security Activity（NOSSA））的 Ed Kratovil 给我在特殊海军系统和软件安全项目中提供了工作机会。

此外，我也想肯定并感谢我的朋友 Jim Gerber、Sidney Andrews、Dave Shampine、Mary Ellen Caro、Tony Dunay、Chuck Dorney、John Leipper、Kurt Erthner、Ed Nicholson、William Hammer 和 Jerry Barnette 的工作，他们审阅了早期的手稿并为此书提供了很有价值的意见和建议。

目　录

第1章 系统安全

1.1 简 介

我们生活在一个由系统和风险构成的世界里。从工程学的角度来看，生活中的许多方面都涉及到系统。例如，房子是一种系统，汽车是一种系统，输电网络也是一种系统。商用飞机是在经济运输系统和全球空管（空中控制）系统内运行的系统。系统已经成为现代生活必不可少的组成部分。

系统和技术也使我们面临事故，因为系统会发生故障或非正常工作从而导致财物损坏和人员伤亡。系统发生故障并导致伤亡、损失或类似不良后果的可能性就是事故风险。例如，交通信号灯失效是一种危险，由此可能导致汽车相撞的事故。汽车、交通和交通信号灯组成一个日常使用的特定系统，因为它风险小，所以我们接受这个潜在的事故风险。房间里的瓦斯炉可能发生故障并爆炸也是一种危险，它能造成房屋起火燃烧或更严重的事故。这是另一种特定系统，我们知道它会带来不利的后果，却选择容忍，因为瓦斯炉事故风险很小，而益处很大。

我们生活在由不同系统错综复杂相互交织的环境里，这些系统都会影响我们的安全。每个系统都有特定的设计和组成部分，而且每个系统都含有能带来特定事故风险的固有危险。我们总是在接受系统的益处和它所带来的事故风险之间进行权衡。在研制和制造系统时，就应该考虑消除和减少事故风险。有些风险很小，很容易就能接受，然而有些风险很大，必须马上对其进行处理。当系统在研制过程中采取了系统设计控制措施（即系统安全）时，事故风险一般都比较小，而且是可接受的。

风险就像无形的无线电信号一样充斥在我们周围，有些是明显和清晰的，有些是很弱的，另外还有一些则是失真且不清晰的。安全和生活一样，是一个探索、理解和选择可接受风险的过程。系统安全是识别和控制事故风险的形式化、规范的过程。随着系统越来越复杂和危险，就需要投入更多的精力去理解和管理系统的事故风险。

系统安全和有效的风险管理的关键是识别和降低危险。要成功地控制危险，就必须理解危险并且知道如何识别它们。本书的目的就是让读者更好地理

解危险和掌握识别危险的工具和技术，以便在系统研制过程中有效地控制这些危险。

1.2 系统安全背景

系统安全的理想目标是研制没有危险的系统。然而，绝对的安全是不可能的，因为完全消除全部危险状态往往是不可能的，特别是当处理那些带有固有危险的复杂系统，例如武器系统、核能发电厂、商用飞机。

既然通常不可能消除所有的危险，现实的目标就变成了研制具有可接受事故风险的系统。这个目标的实现，就要通过识别潜在危险、评估其风险和采取正确的措施，来消除或降低已识别的危险，包括需要事故风险管理的系统化方法。安全是风险管理过程的最基本部分。

危险总是存在的，但是它们的风险必须而且能够控制在可接受的范围。因此，安全是一个相对概念，意味着一种可度量和可接受的风险水平。系统安全并非一个绝对的量值，而是一个事故风险管理的优化水平，受到费用、时间、使用效能(效果)的制约。系统安全需要评价风险，并由适当的决策机构来决定接受或者拒绝风险水平。事故风险管理是系统安全工程和管理职能的基本工作。系统安全是从最初的系统方案设计，贯穿详细设计和试验、直至报废处置，整个系统寿命周期进行约束和控制的过程(也就是，“从摇篮到坟墓”或“从孕育到埋葬”)。

系统安全的基本目标是识别、消除或者控制、记录系统危险。系统安全包含了事故风险管理和安全性设计的所有理念，是一门识别和控制危险并使其风险水平达到可接受程度的学科。安全性是一种必须有意识地设计到产品中的系统属性。从历史角度来看，在系统研制阶段对安全性采取主动的预防措施要比事故发生之后再去尝试增加安全特性更为有效。系统安全工作是一种先期投资，以避免潜在的事故导致的未来损失。

1.3 系统安全描述

系统安全是对系统、子系统、设备、材料和设施的研制、测试、生产、使用和处置过程中面临的系统、人员、环境及健康事故风险的管理过程。

作为一种规范化的方法，系统安全大纲(SSP)是通过工程、设计、教育、管理策略以及对实施和条件监督控制等措施来消除危险，能确保完成恰当的系统安全管理和工程任务。规范化的系统安全过程最初是由美国国防部及其军

事分支机构建立的，并作为美军标 MIL－STD－882 颁布的。在民营企业的商业化产品研制过程中也采用相同的过程，比如：商用飞机、铁路运输、核电和汽车等。

系统安全的目的是保护生命、系统、设备和环境，其基本目标是消除导致人员伤亡、系统损失、环境破坏的危险。如果危险不能被消除，那么接下来的目标就是通过设计控制手段以降低事故风险。通过降低事故的可能性或事故的严重程度可达到降低事故风险的目的。

当系统安全大纲应用于初期的方案设计阶段并贯穿于系统研制和采办的整个周期时，就能以较小的费用达到上述目标。现代系统，特别是武器系统，已非常复杂，要有意地防止事故发生就需要系统安全过程。能源材料自身的危险、环境的影响以及操作要求的复杂都增加了系统的复杂性。另外，还必须考虑硬件故障、人为差错、软件接口（包括程序错误）和环境的多样性。

在 MIL－STD－882D 中，系统安全的定义如下：

贯穿系统寿命周期各阶段，在系统使用效能以及适应性、时间和费用约束下，应用工程和管理的原理、准则和技术，使系统达到可接受的事故风险。

系统安全的目的是通过危险识别和缓解技术进行事故风险管理。系统安全工程是系统工程的一部分，运用科学和工程原理及时识别危险并且采取一些必要措施，以预防或控制系统中的危险。利用数学以及其他学科领域中的专业知识和专门技术，结合工程设计与分析的原理和方法，来确定、预测、评价、记录系统的安全性。

系统安全管理是项目管理的一部分，能确保各种系统安全任务得以完成。这包括识别系统安全要求；规划、组织和控制为达到安全目标而开展的各种工作；协调其他项目要素；分析、审核和评价项目以保证及时有效地实现系统安全目标。

系统安全的基本思想是一种规范化的过程，通过消除危险或降低危险的事故风险而有意识地将安全性设计到系统中，是在系统寿命周期内，通过有意识地把事故的可能性降低到可忽略的水平，以达到挽救生命和财产损失的过程。系统寿命周期一般定义为方案设计、初步设计、详细设计、试验、制造、使用和处置等阶段。为了采取主动，在系统研制最初的方案设计阶段就要开展安全性工作。

系统安全的目的是确保在尽可能大的范围内发现危险，并在系统研制过程中尽早采取防护措施以避免在项目后期再进行设计修改。安全性设计是安全使用的先决条件。系统出故障的情况是可预测的，而能预测通常意味着能避免。就像墨菲（Murphy）规律说的："任何可能出错的地方都将会出错。"系统安全的

目的就是发现什么会出错(在其发生之前)并制定控制措施阻止其发生或者降低发生的可能性,这是通过识别和减少危险得以实现的。

1.4 系统安全过程

如图 1.1 所示,MIL - STD - 882D 建立了一个包含八个主要步骤的系统安全核心过程(core system safety process)。系统安全核心过程包括制定一个系统安全大纲(SSP),以落实事故风险管理过程。系统安全大纲应正式记录在系统安全大纲计划(system safety program plan ,SSPP)中,详细说明将要开展的安全性工作项目,包括特定的危险分析、报告等。危险识别后,应评价其风险,并制定危险减少方法以降低确需处理的风险。可通过系统安全要求(System Safety Requirements,SSR)将危险消减方法落实到系统设计中。所有被识别出的危险将汇集成为危险措施记录(hazard action records,HAR)并保存在危险跟踪系统(hazard tracking system ,HTS)中。利用 HTS,危险被持续跟踪直至实现闭环管理。

从系统安全核心过程可以看出安全一直围绕着危险。该过程的关键是危险识别和消除或降低。因此,系统安全分析人员对于危险的理解、识别和降低至关重要。

系统安全核心过程可以简化为如图 1.2 所示的过程。这是一个事故风险管理过程,其中通过危险识别、危险事故风险评价以及对风险不可接受的危险进行控制而获得安全。这是一个闭环过程,在这个过程中,分析和跟踪危险直至采取可接受的闭环措施并得以验证。为了在系统设计过程中就影响系统设计方案,而非在系统研制完成后再试图强迫更改设计,该过程应与系统实际研制过程相结合。

系统安全包含了一个寿命周期整体技术途径,它基于事故的预防措施必须尽可能早的开展,并持续到系统使用寿命终止的思想。通常将安全性设计到装备中的费用,要比在装备已制造完成或投入使用时再加入安全性的费用少得多且更为有效。此外,经验表明不管系统安全大纲多么有效,在一个新设计的系统中总有一些危险无法检测出来。因此,在系统的整个寿命周期中,必须有效地实施系统安全大纲,以确保一旦出现安全问题就能被识别,并采取适当的措施。

系统安全的关键是对危险的管理。为了有效地控制危险,人们必须理解危险原理和危险识别。本书的目的是让读者更好地理解危险并掌握用于识别危险的工具和技术。当危险被识别和理解后,才能被正确地消除或降低。