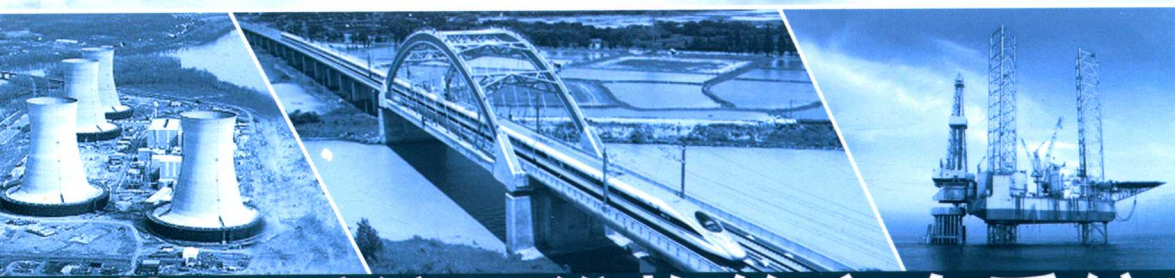
装备科技译著出版基金

# Engineering a Safer World

## Systems Thinking Applied to Safety



# 基于系统思维构筑安全系统

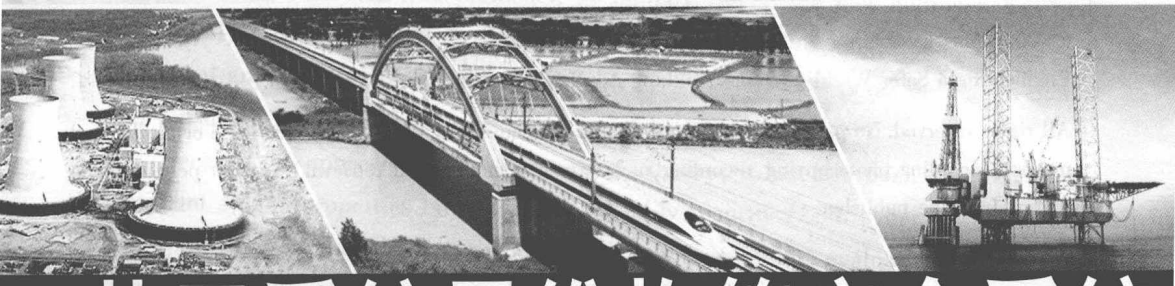
[美] 南希·莱文森 著
唐涛 牛儒 译

国防工业出版社
National Defense Industry Press

装备科技译著出版基金

# Engineering a Safer World

## Systems Thinking Applied to Safety



# 基于系统思维构筑安全系统

[美] 南希·莱文森 著
唐涛 牛儒 译

國防工業出版社
National Defense Industry Press

著作权合同登记　图字:军-2013-004号

图书在版编目(CIP)数据

基于系统思维构筑安全系统/(美)莱文森(Leveson,N. G.)著;唐涛,牛儒译. —北京:国防工业出版社,2015.3

书名原文:Engineering a safer world:systems thinking applied to safety

ISBN 978-7-118-09781-8

Ⅰ.①基… Ⅱ.①莱… ②唐… ③牛… Ⅲ.①安全系统工程 Ⅳ.①X913.4

中国版本图书馆 CIP 数据核字(2015)第049400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 710×1000　1/16　印张 25 ¼　字数 481 千字

2015年3月第1版第1次印刷　印数 1—2000 册　定价 128.00 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

# Forward to Chinese Edition

Too many losses occur that in retrospect appear to be preventable. They do not involve unknown factors but simply unrecognized ones. One of the problems is the techniques used to perform hazard analyses are all over 50 years old. At the time they were created, the complex, software – intensive systems common today did not exist. To improve safety in these systems, we need to update our assumptions about accident causation and our tools and methods based on these assumptions. This book describes a new approach to system safety engineering.

Since this book was first published in January 2012, the new approach has been successfully used in almost every industry around the world. Careful comparisons with traditional approaches have all shown this new systems approach is not only more powerful, but much less expensive to use.

Because the approach is based on systems theory, it has also been found to handle important system properties beyond safety, notably security (both cyber and physical). The application of the ideas to security are more recent, but evaluations in industrial and military applications have found them to effective and they are starting to be adopted.

The major difference between the STAMP approach and the more traditional approaches is that it is a top – down, system engineering approach to problem solving rather than a bottom – up reliability approach. It allows integrating safety and security into the system design during concept formation, which reduces the costs of making changes later in development.

Finally, concentrating on engineering development is not enough to achieve high levels of safety. This book describes how to operate and manage safety – critical systems. I hope it will help you to engineer a safer world.

Nancy G. Leveson

# 中译版序

有很多事故看起来似乎可以避免，因为基于传统事故致因模型的分析结果显示，这些事故仅仅是由一些简单但未被发现的因素引起的，并未涉及任何未知因素。出现这种情况的原因之一是我们的危险分析技术已使用了50多年，在这些分析技术形成之时，今天普遍使用的复杂软件密集系统还不存在。为了改进系统的安全性，需要更新我们关于事故致因的假设。这本书介绍了一种系统安全工程的新方法。

自2012年1月本书首次出版以来，STAMP方法已成功应用于世界上几乎所有领域，与传统的方法相比较，该方法不仅强大，而且经济高效。

由于该方法是以系统理论为基础的，它还能用于分析安全性之外的其它重要的系统特性，如保密性（网络和物理的）。虽然保密性分析方面的应用是近些年才提出的，但它在工业和军事领域的应用已经取得了较好的效果，并已逐渐被大家接受。

STAMP与传统方法的主要区别在于它是一个致力于解决问题的自顶向下的系统工程方法，而不是一个自底向上的可靠性方法。该方法从概念构建开始就将安全性和保密性融入系统设计，从而减少了系统开发后期更改设计带来的损失。

仅关注系统开发仍无法完全保障系统的运行安全，因此本书还描述了如何操作和管理安全苛求系统的新方法。我希望本书能帮助您设计一个更加安全的系统。

南希·莱文森

# 译者序

随着人们了解世界、征服世界的愿望越来越大，科学技术进步的一个显著特征是装备的功能越来越强、自动化程度越来越高、规模体积越来越庞大、系统越来越复杂，计算机技术的发展更使装备如虎添翼，战略武器的研制、宇宙开发和核电站建设等一批标志现代科学技术水平的复杂巨系统相继问世。这些复杂巨系统往往由数以万计的元件、部件以及大量的软件组成，元件、部件之间以非常复杂的关系相连接，系统设计、研发、运营及维护等过程需要庞大的团队，并且与政府部门、企业组织管理机构密切相关，构成了一个庞大的社会技术系统。这类系统的研制和使用过程中常常涉及高能量，微小的差错就可能引起大量的能量意外释放，导致灾难性的事故，复杂巨系统的安全性问题受到了人们的关注。这类系统的安全性呈现出涌现性特性，传统的安全方法有很大局限性和不足。在这些复杂巨系统开发研制、使用和维护的过程中，系统安全的基本思想逐渐形成。

本书作者美国工程院院士南希·莱文森（Nancy G. Leveson）教授是系统安全领域国际权威专家。她 30 多年来一直从事系统安全，尤其是软件密集型系统安全的研究和教学工作，完成过多项美国航天局及美国军方系统安全方面的研究项目和咨询项目，参加过“哥伦比亚”号航天飞机等重大事故调查，具有深厚的理论基础和丰富的工程实践经验。莱文森教授的研究涉及设计、开发、运营、管理及文化等系统安全的所有方面，研究成果已广泛应用于军事、航空、航天、铁路、化工、核电、石油天然气及医药卫生等行业。莱文森教授教授十分注重将系统思维及系统工程应用于复杂社会技术系统，强调不应只专注影响系统安全的技术问题，还应重视影响系统安全的社会、管理，甚至政治等其他因素。本书首先对传统的事故致因假设及其过度简化提出质疑，深入分析了传统的事故致因模型的局限性和不足。在此基础上，针对复杂社会技术系统特点运用系统理论思想提出了一个新的事故致因模型——STAMP（Systems – Theoretic Accident Model and Process）。STAMP 模型将组件交互列为事故致因因素之一，把安全问题转换为控制问题，将系统安全重点由防止失效转到实施行为的安全约束。最后一部分介绍使用新模型形成的事故调查和分析、危险分析、安全设计、运行和管理系统安全新技术，包括 STPA（System Theoretic Process Analysis）和 CAST（Causal Analysis Based on STAMP）。书中还列举了许多军事、航空、航天、化工、核电及医药等行业的事故分析案例及构建更加安全系统的成功范例。本书适合从事复杂系统设计与分析工作的人员参阅，也适合

不是安全工程师甚至不是工程师的读者，书中介绍的方法可以用于任何复杂的社会技术系统。

由于包含军事、航空、航天、化工、核电及医药等行业实例，涉及大量专业术语和知识，本书的翻译也是一项庞大的“系统工程”。为使读者理解原著的精髓，从实例中吸取更多经验和教训，掌握更多生命周期全过程中使系统保持安全的方法和技术设计，译者以原貌呈现为原则，力求易于阅读、忠实原著。同时，为便于广大读者阅读，书中的人名也都进行了翻译。

本书由唐涛、牛儒等负责翻译，其中第 1 章～第 10 章及第 12 章～第 14 章由唐涛翻译，第 11 章由牛儒翻译，附录 A、B、C、D 由李辰岭、何晖、韩笑翻译。此外，刘超、刘金涛、陈黎洁、唐武梅、宿帅等参与了本书的翻译工作。全书由唐涛负责全面技术审译，李辰岭、何晖、韩笑、莫小凡参与了全书的审译。英国约克大学的葛晓程博士对本书翻译也提供了帮助，特此表示感谢。

由于译者水平有限，书中疏漏和差错之处敬请广大读者批评和指正。

我们声称技术是生命的力量、是美好的愿景和其自身的推动力，但又将所有过错都归咎于技术。用技术来解释一切，并最终为自己辩解。

—— T. 凯勒·扬(T. Cuyler Young)，《自然界中的人》

献给传授过我系统安全工程知识的所有杰出工程师，特别是对我非常信任的格雷迪·李(Grady Lee)，同时也献给将系统思维运用于安全的早期奠基人，包括 C. O. 米勒(C. O. Miller)以及在美国提出系统安全的航空航天工程师。还要献给在欧洲做出开创性工作的赞斯·拉斯穆森(Jens Rasmussen)。

# 前　言

由计算机科学专业研究生毕业并成为计算机科学系教师之后，我开始了系统安全领域的探索。工作的第一周，我接到休斯飞机制造公司地面系统部系统安全工程师马里恩·穆(Marion Moon)的一个电话。显然，在我之前他已经找过若干老师，而我也许是他最后的希望。他告诉我，在水雷项目中遇到一个新问题，他称其为“软件安全”。我告诉他我对这个问题一点都不了解，而且之前也在不相关的领域工作，但我愿意试一试。此后的30年，我一直致力于研究软件安全问题及构筑更安全系统的方法。

2000年左右，我感到非常沮丧。尽管许多聪明的学者长期致力于安全问题的研究，但却进展缓慢。工程师们很认真地进行似乎对事故没有很大影响的安全分析。我认为进展缓慢的原因是因为传统安全工程方法的技术基础和假设已经不再适用于今天我们正在构建的复杂系统。

工程领域经历了一场技术革命，而应用于安全和可靠性工程的故障树(FTA)和失效模式与后果分析(FMEA)却变化很小。大多数系统都用数字组件来构建，此类系统的工作方式与其所取代的纯模拟系统有很大区别，而且系统及其工作所处环境的复杂性也大大增加。随着事故致因的变化，建立在简单模拟系统基础之上的旧的安全设计技术的有效性逐渐降低。

20多年来，我注意到工业领域的工程师们费力地将旧的技术应用到新的软件密集型系统中——耗费大量精力却收效甚微。同时，如果我们想有效地减少损失，工程师们就不应还是只专注于技术问题，而忽视影响系统安全的社会、管理，甚至政治等其他因素，我决定寻找新的技术和方法。这本书介绍了新的事故模型以及相应的系统安全技术的研究成果。

我认为出路在于提出基于现代系统思维和系统理论的安全方法。虽然这些方法看似是新的或者形式上有所改变，但都植根于第二次世界大战后发展起来的系统工程思想，并仍以安全设计的独特方法即系统安全为基础。系统安全是由以C. O. 米勒(C. O. Miller)、杰罗姆·莱德勒(Jerome Lederer)、威利·哈姆(Willie Hammer)等为代表的航空领域工程师于20世纪50年代创造性提出的，最初是为解决航空系统，特别是军用飞机和弹道导弹系统日益增加的复杂性问题。随着时间的推移，许多系统工程思想受主流工程方法，特别是可靠性工程的影响，已经丢弃或被替代。

本书回归到这些早期的思想并加以充实，使之适应于今天的技术，同时也借鉴了欧洲赞斯·拉斯穆森(Jens Rasmussen)等在安全及人因工程中应用系统思维的开创性成果。

我们迄今为止的经验是，本书所描述的新方法比现有的技术更有效、花费少、易于使用，希望读者从中获益。

## 与《安全体(Safeware)》的联系

我的第一本书《安全体》全面概述了目前系统安全的理论和方法，为了解最新发展现状提供了参考。为了避免重复，一般不再赘述《安全体》中出现过的安全工程的基本概念，但为使本书自身前后连贯仍有一些重复话题，其中也包含了在撰写《安全体》之后我对系统安全的进一步理解。

## 读者

本书主要是写给富有经验的专业人员，而不是纯理论的学术研究人员或一般民众。因此，尽管提供了参考文献，本书并不打算引用或描述该专题已有的所有成果，或提供该领域研究状态的学术分析。本书的目的是为工程师以及其他关心安全的人员提供一些试图减少事故并使系统和复杂产品更加安全时可以使用的工具。

本书也是写给那些不是安全工程师或甚至不是工程师的读者，书中的方法可以用于任何复杂的社会技术系统，如医疗卫生和金融行业。本书向您展示了如何“重新设计”系统，以便提高安全性并更好地管理风险。本书内容有助于读者在自己的专业领域中预防事故发生或减少事故带来的损失。

## 内容

这种安全新方法的基本前提是需要扩展传统的致因模型以便处理今天的工程系统。常见的事故致因模型假设事故是由组件失效引起的，提高系统组件的可靠性或制定处置系统组件失效的预案可防止事故。虽然对过去相对简单的机电系统而言，这个假设是正确的，但对今天我们所要构建的复杂社会技术系统来说，这个假设就不再适用了。我们需要新的事故致因扩展模型、支撑更加有效的工程方法，以便提高安全性并更好地管理风险。

本书分为三个部分。第Ⅰ部分解释为什么需要一种新的方法，包括传统的事故模型的局限性、新模型的目标以及新模型所基于的系统理论基本思想。第Ⅱ部分提出了新的事故致因扩展模型。第Ⅲ部分介绍如何使用新模型形成系统安全新技术，包括事故调查和分析、危险分析、安全设计、运行和管理。

为了确定新技术的有效性，我将其试用到多种实际系统中。本书的编写也因此耗时甚长。为了不再进一步推迟出版时间，我将编写练习、更多的例子和其他辅

助教学和学习的资料，放在网站上供下载。

第6章～第10章有关系统安全工程和危险分析。刻意独立成章撰写，可以用做本科生和研究生的系统工程教材。在系统工程课程中，安全只是课程内容的一部分，这一部分主要关注安全性设计。

## 致谢

本书所阐述的理论研究一部分得到了美国国家科学基金会和美国国家航空航天局多年来的资助，特别是美国国家航空航天局兰利研究中心的大卫·埃克哈特（David Eckhardt）提供了初期资金，使本项工作得以开始。

同时，在此也衷心感谢帮助我发展这些想法的所有学生和同事，需要感谢的人员太多以至无法一一列出，但我想在书中介绍他们提出或者我们共同提出的想法时提到他们以表感激之情。由于疏忽本应该感谢但没有感谢的人员敬请谅解。我的学生、同事和我经常讨论并分享各自的观点，有时很难确定想法源于何处。创新通常包含一个过程，在此过程中我们每个人都从别人所做的工作中获得灵感，很难确定哪个人具体负责了哪个部分的内容。毫无疑问，他们做出了无价的贡献，对我的思想产生了重要的影响。

特别感谢在我写这本书时在麻省理工学院就读并为发展这些想法发挥重要作用的学生们：尼古拉斯·杜拉克（Nicolas Dulac）、玛格利特·斯特林费洛（Margaret Stringfellow）、布兰登·欧文斯（Brandon Owens）、马蒂厄·库蒂里耶（Matthieu Couturier）和约翰·托马斯（John Thomas），他们协助完成了书中所使用的例子。

对本书中的想法做出重要贡献的其他以前的学生有：马特·杰夫（Matt Jaffe）、埃尔温·翁（Elwin Ong）、娜塔莎·尼奥吉（Natasha Neogi）、凯伦·马莱（Karen Marais）、凯瑟琳·韦斯（Kathryn Weiss）、大卫·斯普肯（David Zipkin）、斯蒂芬·弗雷德里希（Stephen Friedenthal）、迈克尔·摩尔（Michael Moore）、米尔娜·戴柳克（Mirna Daouk）、约翰·斯蒂利（John Stealey）、斯蒂芬妮·凯西（Stephanie Chiesi）、布莱恩·王（Brian Wong）、马尔·阿瑟顿（Mal Atherton）、丹尼尔·奥塔（Shuichiro Daniel Ota）和波莉·艾伦（Polly Allen）。

对此书的撰写提供协助和录入的同事包括：西德·尼德克（Sidney Dekker）、约翰卡·罗尔（John Carroll）、格尔圣菲尔德（Joel Cutcher－Gershenfeld）、约瑟夫·萨斯曼（Joseph Sussman）、贝蒂·巴雷特（Betty Barrett）、艾德·巴舍尔德（Ed Bachelder）、玛格丽特－安妮·斯道瑞（Margaret－Anne Storey）、梅根·迪尔克斯（Meghan Dierks）和斯坦·芬克尔施泰因（Stan Finkelstein），在此谨向他们表示衷心的感谢。

# 目　录

## Ⅰ　基　础


**第 1 章　为什么需要不同的方法** …… 2

**第 2 章　对传统安全工程基础的质疑** …… 5

2.1　混淆安全性和可靠性 …… 5
2.2　将事故致因描述为事件链 …… 10
2.2.1　直接致因 …… 14
2.2.2　选择事件的主观性 …… 14
2.2.3　选择事件链条件的主观性 …… 16
2.2.4　忽视系统因素 …… 17
2.2.5　在事故模型中包括系统因素 …… 21
2.3　概率风险评估的局限性 …… 24
2.4　事故中操作员的作用 …… 27
2.4.1　操作员导致了绝大多数的事故吗? …… 27
2.4.2　事后诸葛亮 …… 28
2.4.3　系统设计对人为错误的影响 …… 28
2.4.4　心智模型的作用 …… 30
2.4.5　另一种人为错误的观点 …… 33
2.5　事故中软件的作用 …… 34
2.6　系统的静态观和动态观 …… 36
2.7　关注追究责任 …… 38
2.8　新事故模型的目的 …… 41

**第 3 章　系统论及其与安全性的关系** …… 44

3.1　系统论概述 …… 44
3.2　涌现性和层次性 …… 45
3.3　通信和控制 …… 46
3.4　用系统论解读事故 …… 48

3.5 系统工程与安全 …… 49
3.6 将安全融入系统设计 …… 51

## Ⅱ STAMP:基于系统理论的事故模型

**第4章 致因的系统理论观** …… 54

4.1 安全约束 …… 55
4.2 分层安全控制结构 …… 58
4.3 过程模型 …… 63
4.4 STAMP 模型 …… 64
4.5 事故原因的通用分类 …… 66
4.5.1 控制器操作 …… 67
4.5.2 执行器和被控过程 …… 70
4.5.3 控制器和决策者间的协调和沟通 …… 70
4.5.4 背景和环境 …… 72
4.6 新模型的应用 …… 72

**第5章 友军误击事故** …… 75

5.1 背景 …… 75
5.2 防止误击事故的分层安全控制结构 …… 77
5.3 使用 STAMP 的事故分析 …… 86
5.3.1 近因事件 …… 87
5.3.2 物理过程故障与异常交互 …… 90
5.3.3 飞机与武器的控制器 …… 91
5.3.4 ACE 与任务指导 …… 102
5.3.5 预警机操作员 …… 105
5.3.6 更高层控制 …… 112
5.4 误击事故结论 …… 120

## Ⅲ STAMP 使用

**第6章 使用 STAMP 构建和运行更安全的系统** …… 123

6.1 为何有时安全工作不经济—有效 …… 123
6.2 系统工程在安全中的作用 …… 126
6.3 系统安全工程化过程 …… 127
6.3.1 管理 …… 127

6.3.2 工程开发 …… 128
6.3.3 运营 …… 129

**第7章 基础** …… 130

7.1 定义事故和不可接受的损失 …… 130
7.2 系统危险 …… 132
7.2.1 划分系统边界 …… 133
7.2.2 识别高层系统危险 …… 134
7.3 系统安全需求和约束 …… 137
7.4 安全控制结构 …… 139
7.4.1 技术系统的安全控制结构 …… 140
7.4.2 社会系统中的安全控制结构 …… 144

**第8章 STPA:一种新的危险分析技术** …… 150

8.1 危险分析新技术的目标 …… 150
8.2 STPA 过程 …… 151
8.3 识别潜在的危险控制(步骤1) …… 154
8.4 确定不安全的控制如何发生(步骤2) …… 156
8.4.1 识别致因场景 …… 158
8.4.2 考虑随着时间推移控制的退化 …… 161
8.5 人工控制器 …… 161
8.6 STPA 用于安全控制结构中的组织层 …… 164
8.6.1 流程和组织方面的风险分析 …… 164
8.6.2 缺陷分析 …… 165
8.6.3 识别组织和流程风险的危险分析 …… 167
8.6.4 分析和潜在扩展的使用 …… 168
8.6.5 与传统的流程风险分析技术的比较 …… 169
8.7 重建社会技术系统:药品安全和万络悲剧 …… 169
8.7.1 围绕批准和召回万络的事件 …… 170
8.7.2 万络案例分析 …… 172
8.8 STPA 与传统危险分析技术的比较 …… 176
8.9 小结 …… 177

**第9章 安全指导下的设计** …… 178

9.1 安全指导下的设计 …… 178
9.2 工业机器人的安全指导下设计案例 …… 179

9.3 安全设计 …… 186
9.3.1 受控过程和物理组件设计 …… 187
9.3.2 控制算法的功能设计 …… 187
9.4 设计人工控制器的特殊考虑 …… 194
9.4.1 容易但无效率的方法 …… 194
9.4.2 控制系统中人的作用 …… 195
9.4.3 人因错误的基本原理 …… 197
9.4.4 提供控制选择 …… 199
9.4.5 匹配任务与人的特征 …… 201
9.4.6 减少人因错误的设计 …… 202
9.4.7 支持产生和维护准确的过程模型 …… 203
9.4.8 提供信息和反馈 …… 210
9.5 小结 …… 217

**第 10 章 将安全整合到系统工程中 …… 218**

10.1 规范的作用及安全信息系统 …… 218
10.2 意图规范 …… 219
10.3 整合系统和安全设计的过程 …… 222
10.3.1 建立系统的目标 …… 223
10.3.2 定义事故 …… 225
10.3.3 确定系统危险 …… 225
10.3.4 将安全整合到架构选择和系统折中研究中 …… 226
10.3.5 记录环境假设 …… 233
10.3.6 生成系统级需求 …… 234
10.3.7 识别高层设计和安全约束 …… 235
10.3.8 系统设计和分析 …… 240
10.3.9 记录系统的局限性 …… 246
10.3.10 系统验证、维护和演进 …… 247

**第 11 章 事故与未遂事故分析 …… 248**

11.1 事故分析中应用 STAMP 的一般过程 …… 249
11.2 建立相关事件链 …… 250
11.3 定义与事故相关的系统和危险 …… 251
11.4 编写安全控制结构文档 …… 253
11.5 分析物理过程 …… 254
11.6 分析安全控制结构的更高层 …… 256

11.7 有关事后诸葛亮的讨论及举例 …… 265
11.8 协调与沟通 …… 269
11.9 动态特性和向高风险状态的迁移 …… 271
11.10 CAST 分析得出的建议 …… 273
11.11 CAST 与传统事故分析的比较 …… 276
11.12 小结 …… 277

**第 12 章 控制运行中的安全** …… 279

12.1 基于 STAMP 的运行 …… 279
12.2 在运行中检测开发过程缺陷 …… 281
12.3 对变更进行管理或控制 …… 283
12.3.1 计划中的变更 …… 283
12.3.2 计划外的变更 …… 284
12.4 反馈通道 …… 285
12.4.1 审核和性能评估 …… 286
12.4.2 异常、未遂事故和事故的调查 …… 288
12.4.3 报告系统 …… 289
12.5 使用反馈 …… 293
12.6 教育与培训 …… 293
12.7 创建运行安全管理计划 …… 295
12.8 将 STAMP 应用到职业安全 …… 296

**第 13 章 管理安全与安全文化** …… 298

13.1 为什么管理者应重视安全并在此方面投入 …… 298
13.2 实现安全目标的总体安全需求 …… 302
13.2.1 管理承诺与领导 …… 302
13.2.2 公司的安全方针 …… 303
13.2.3 沟通与风险意识 …… 304
13.2.4 控制系统向高风险迁移 …… 305
13.2.5 安全、文化与处罚 …… 306
13.2.6 建立有效的安全控制架构 …… 311
13.2.7 安全信息系统 …… 316
13.2.8 持续的改进和学习 …… 317
13.2.9 教育、训练和能力拓展 …… 317
13.2.10 小结 …… 318