装备科技译著出版基金

可靠性维修性保障性
学术专著译丛

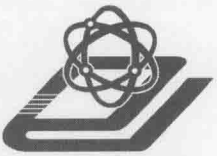
丛书主编 康锐

脆弱系统

Vulnerable Systems

【瑞士】Wolfgang Kröger
【意】Enrico Zio 著
林元晟 主译
李大庆 主审

國防工業出版社
National Defense Industry Press



可靠性维修性保障性学术专著译丛

脆弱系统

Vulnerable Systems

[瑞士] Wolfgang Kröger, [意] Enrico Zio 著
林元晟 主译
李大庆 主审

国防工业出版社
·北京·

著作权合同登记　图字:军-2013-132号

图书在版编目(CIP)数据

脆弱系统/(瑞士)克隆格,(意)齐奥(Zio,E.)著;
林元晟主译.—北京:国防工业出版社,2014.9
(可靠性维修性保障性学术专著译丛)
书名原文:Vulnerable systems
ISBN 978-7-118-09723-8

Ⅰ.①脆...　Ⅱ.①克...②齐...③林...　Ⅲ.①系统可靠性-研究　Ⅳ.①N94

中国版本图书馆 CIP 数据核字(2014)第 209189 号

※

國防工業出版社出版发行
(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** 11¾　**字数** 214 千字
2014 年 9 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 48.00 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

《可靠性维修性保障性学术专著译丛》
编 审 委 员 会

《可靠性维修性保障性学术专著译丛》

总　序

可靠性理论自20世纪50年代发源以来，得到了世界各地研究者的广泛关注，并在众多行业内得到了成功的应用。然而，随着工程系统复杂程度的不断增加，可靠性理论与方法也受到了日益严峻的挑战。近年来，许多国际知名学者对相关问题进行了深入研究，取得了一系列显著的成果，极大地丰富和充实了可靠性理论与方法。2012年，国际知名出版社Springer出版了一套“可靠性工程丛书”，共计61种，总结了近年来可靠性维修性保障性相关领域内取得的绝大部分研究成果，具有很强的系统性、很高的理论与实用价值。

经过国内最近30年的普及和发展，可靠性的重要性已经得到业界的普遍认可，即使在民用领域，可靠性的研究与应用也发展迅猛。他山之石，可以攻玉，系统地了解国际上可靠性相关领域近年来的最新研究成果，对于国内的可靠性研究者与实践者们都会大有裨益。为此，国防工业出版社邀请北京航空航天大学可靠性与系统工程学院以Springer出版的可靠性工程丛书中的10种，外加Wiley、World Scientific、Cambridge、CRC、Prentice Hall出版机构各一种，共15种专著，策划组织了《可靠性维修性保障性学术专著译丛》的翻译出版工作。我具体承担了这套丛书的翻译组织工作。我们挑选这15种专著的基本原则是原著内容是当前国内学术界缺乏的或工业界急需的，主题涵盖了相关领域的科研前沿、热点问题以及最新研究成果，丛书中各专著原作者均为相关领域国际知名的专家、学者。

组织如此规模的学术专著翻译出版工作，我们是没有现成经验的。为了保证翻译质量和进度，在组织翻译这套丛书的过程中，我们做了以下几方面的工作：一是认真遴选主译者。我们邀请了国内高校可靠性

工程专业方向的在校博士生作为主译者，这些既有专业知识又有工作激情的青年学者对翻译工作的投入是保证质量与进度的第一道屏障。二是真诚邀请主审专家。我们邀请的主审专家要么是这些博士生的导师，要么是这些博士生的科研合作者，他们均是国内可靠性领域的知名专家，他们对可靠性专业知识把握的深度和广度是保证质量与进度的第二道屏障。三是建立编审委员会加强过程指导。我们邀请了国内知名专家与主审专家一起共同组成了丛书编审委员会，从丛书选择、翻译指导、主审主译等多个方面开展了细致的工作，同时为了及时沟通信息、交流经验，我们还定期编辑丛书翻译工作简报，在主译者、主审者和编审委员中印发。可以说经过以上工作，我们坚信这批专著的翻译质量是有保证的。

本套丛书适合于从事可靠性维修性保障性相关研究的学者和在校博士、硕士研究生借鉴与学习，也可供工程技术人员在具体的工程实践中参考。我们相信，本套丛书的出版能够对国内可靠性系统工程的发展起到推动作用。

北京航空航天大学可靠性与系统工程学院

康　锐

2013 年 11 月 8 日

PREFACE

Today's modern systems have become increasingly complex to design and build, while the demand for reliability and cost effective development continues. Thus, reliability has become one of the most important attributes in these systems. Growing international competition has increased the need for all designers, managers, practitioners, scientists and engineers to ensure a level of reliability of their product before release at the lowest cost. This is the reason why interests in reliability have been continually growing in recent years and I believe this trend will continue during the next decade and beyond.

It is these growing interests from both industries and academia that motivate Springer to publish the Springer Series in Reliability Engineering, for which I serve as the series editor. This series consists of books, monographs and edited volumes in important subjects of current theoretical research development in reliability and in areas that attempt to bridge the gap between theory and application in fields of interest to practitioners in industry, laboratories, business and government.

I am very delighted to learn that the National Defense Industry Press from China is planning to translate selected books from the Springer Series as well as some other distinguished monographs from other presses into Chinese. The books in the collections to be translated cover most of the timely and important topics in reliability research areas and are of great values for both theoretical researchers and engineering practitioners.

The translations are organized and managed by Professor Rui Kang from Beihang University, who is a world-wide leading expert in reliability related areas. With his expertise and dedication, the quality of the translations is guaranteed. I'm sure that the translations of these outstanding books will be a great impetus to the research and application of reliability engineering in China.

Personally, I will treat the translation collection as an attempt to exchange ideas of reliability researchers in the international community with their Chinese counterparts. I really hope that these kinds of idea interchanges will be more common and frequently in the future. Specifically, I am really looking forward to hearing more from our Chinese colleagues. Wish the research and application of reliability in China a bright future!

Hoang Pham

Dr. Hoang Pham, IEEE Fellow
Distinguished Professor
Rutgers University
Series Editor, Springer Series in Reliability Engineering

序

不断发展的科技和日趋激烈的市场竞争对产品提出了日趋强烈的可靠性需求，希望能够以尽可能低的成本高效保证产品可靠性。可靠性业已成为现代工程系统最重要的属性之一。面向这种需求，Springer 出版社组织出版了《Springer 可靠性工程丛书》。这套丛书由 61 种专著组成（截止到 2013 年 11 月），涵盖了近年来可靠性相关领域内取得的最新理论成果，介绍了可靠性工程在实际工程上的应用，具有很强的理论和实践价值。

作为《Springer 可靠性工程丛书》的主编，我很高兴中国的国防工业出版社计划将这套丛书中的部分专著以及其他一些近年出版的可靠性优秀英文专著翻译出版，推出《可靠性维修性保障性学术专著译丛》。《可靠性维修性保障性学术专著译丛》中的专著选题覆盖了可靠性领域近期的大部分研究热点和重要成果，具有重要的理论价值和实践指导意义。

这套丛书的翻译工作由北京航空航天大学的康锐教授负责组织。康锐教授是国际知名的可靠性专家，我相信，康锐教授的专业知识和奉献精神，能够有效保证译著的质量。我确信，这些优秀专著的翻译出版将极大地推动中国的可靠性研究和应用工作。

就我个人而言，我更愿意将《可靠性维修性保障性学术专著译丛》看作是可靠性领域内的国际学者与中国同行们进行的一次思想交流。我期待这样的交流在未来更加频繁。特别地，希望中国优秀学者们能够更多地以英文出版学术专著，介绍他们的学术成果，从而向可靠性领域的国际同行们发出来自中国的声音。衷心祝愿中国的可靠性事业更上一个台阶！

Hoang Pham
博士，IEEE 会士
罗格斯大学特聘教授
Springer 可靠性工程丛书主编

译者序

关键基础设施遍布于广大地区，大部分是人造的大型物理工程系统，如电力系统、城市供水系统、信息与通信系统和交通系统等，它们协同运作共同为人们提供生活必需的各项基本功能和服务，是国家安全运行和持续发展的必备基础。随着科技的现代化发展，关键基础设施的组件之间和不同关键基础设施之间都存在（相互）依赖关系。例如，电力系统和计算机系统存在相互依赖关系，电力系统能为计算机系统提供能源动力，而计算机系统用于电力调度等相关的控制。这些关键基础设施一旦遭受内外部的干扰，由于（相互）依赖关系的存在，系统易表现出极端脆弱性，发生难以预料的系统故障涌现，表现为大规模的级联失效。

系统的动态级联失效行为会对国家安全、经济卫生、自然与社会环境产生重大的危险和威胁。如，2003 年美加大停电就是级联故障导致的大停电事故，其影响范围多达 5000 多万人，总经济损失高达 100 亿美元；2011 年日本福岛核电站泄漏事件事后被评估为 7 级国际核事件，日本以东及东南方向的西太平洋海域已受到福岛核泄漏事故的显著影响，它还造成多位民众和医护人员遭到核辐射，导致日本多个地区电力轮流发生短缺，且造成目前无法估计的经济损失。然而，这些危害巨大的重大事故的隐含原因却很难完全用传统的可靠性理论发现。对这些关键基础设施进行脆弱性分析，可以帮助我们发现系统中隐藏的故障相关关系及其可能造成的级联失效，进而成为保证关键基础设施等复杂系统可靠性的重要理论指导和技术支持。

针对国内关于基础设施脆弱性分析的资料书籍较少、工程应用经验匮乏的现状，国防工业出版社和北京航空航天大学可靠性与系统工程学院共同策划，启动了本书的翻译工作，旨在向国内相关领域的人员介绍系统脆弱性分析的概念框架和基本分析方法，从而推动国内相关的理论研究和工程应用的发展。系统脆弱性分析的相关知识的普及和应用，在一定程度上能抑制大规模级联失效的发生，提高关键基础设施的可靠性，避免造成不必要的人员伤亡和财产损失。

本书根据 Springer 出版社 2011 年出版的 *Vulnerable Systems* 一书翻译而成，是一本全面介绍系统脆弱性分析的相关理论和工程应用的学术专著。原书作者均为关键基础设施脆弱性分析领域内世界知名的专家学者。原书作者 Wolfgang Kröger 是系统风险分析的专家，担任苏黎世联邦理工大学（ETH）的教授，目前是 ETH 风险中心执行董事。原书另一位作者 Enrico Zio 教授是可靠性领域专家，担任欧洲安全与可靠性协会（ESRA）主席，任职于巴黎中央理工大学和意大利米兰理工大

学。目前，Enrico Zio 教授担任可靠性领域顶级期刊 Reliability Engineering and Systems Saftey（RESS）的编委和 IEEE Transactions on Reliability 的副主编。该书内容汇聚了脆弱性分析领域专家多年的研究、教学的知识，融合了相关领域专家的最新成果，包含了关键基础设施脆弱性分析的具体知识与实用技术，内容丰富充实，具有显著的前瞻性和指导意义。因此，译者认为，本书的翻译出版，对于国内关键基础设施等复杂系统的可靠性理论研究和工程应用工作都具有重要的指导意义和参考价值。

全书共分为 7 章，第 1 章介绍了重要术语和定义；第 2 章介绍了关键基础设施的属性；第 3 章讨论了关键基础设施脆弱性分析方法面临的挑战；第 4 章主要介绍进行脆弱性分析的基本方法；第 5 章重点介绍了脆弱性评估的概念框架；第 6 章详细介绍了脆弱性分析的方法；第 7 章对全书内容进行概括性总结。

本书由北京航空航天大学博士研究生林元晟主译，李大庆副教授主审。北京航空航天大学故障学基础理论实验室的研究生协助译者进行了本书初稿的翻译，并完成了全书公式的录入，对他们的辛勤工作，译者谨在此表示衷心的感谢（以参与翻译的章节顺序为序）：邵英华（第 1 章、第 2 章部分）、武文博（第 2 章部分、第 3 章和第 4 章）、井海龙（第 5 章和第 6 章部分）、刘王佳、叶翠、高蕾、蒋旭和林元晟（共同完成第 6 章）、林元晟（第 7 章）。本书的翻译、出版过程中，北京航空航天大学康锐教授、国防工业出版社白天明编辑给予了悉心的指导与帮助，在此向他们致以由衷的谢意。

由于时间仓促和译者水平有限，本书的翻译难免有不妥之处，敬请广大读者批评指正。

北京航空航天大学可靠性与系统工程学院

林元晟

2014 年 4 月

前　言

20世纪80年代，人们对国家关键基础设施的担忧主要是公共工程耗损老化问题；由于国际恐怖主义增多（特别是“9·11”事件之后）以及基础设施易遭自然灾害破坏的问题出现，人们的关注点转变为对国家安全的重新定义；2000年以来，史无前例的不同失效类型的组合故障和蓄意网络攻击（包括网络攻击）开始引起人们的重视。其结果是，人们的关注点不再是局域范围内的基础设施而是逐步扩展至整个国家/地区，甚至全世界。同时，对单一失效机理的担忧发展为考虑由潜在故障、灾难和威胁的组合发生的危害。因而，减少和管理关键基础设施脆弱性的最新策略和提供的相关分析仪器必须要符合“全风险方法”。

社会一直依赖于基础设施提供的服务，随着现代信息通信技术（ICT）的广泛运用，现代基础设施中的系统不断相互集成，使得系统的操作环境发生变化。例如：市场不断自由化和市场间的相互依赖关系不断增强。同时，社会民众已经非常依赖于基础设施提供的持续服务（如互联网和电力供应持续为人们提供的服务）。而现在，我们一直在防止这些系统损坏或崩溃，因为系统损坏或崩溃会带来人们难以承受的巨大的不便和严重后果，如重大经济损失。例如，2003年8月14日的北美大停电事故，影响到5千万人的生活，并导致了30亿美元的保险索赔。

从分析的角度来看，人们普遍认同当今的基础设施结构变得愈加复杂，其行为也变得更加难以被认知和预测。在对复杂网络的研究过程中发现，网络中的某些元素（节点）会变得更加重要，同时一些（拓扑）结构对于随机失效或蓄意攻击相当敏感。为了降低工程和社会中基础设施的脆弱性，我们需要对系统脆弱性进行更深入地理解，并且对其进行预防分析。已有的脆弱性分析的框架与方法技术还未得到合理利用，且新的方法技术的发展仍不能满足需求。

存在不同类型、不同维度的基础设施，它们对于社会有着不同的重要作用，即不同程度的关键性。本书主要讨论分布在不同地域的大规模物理工程网络，尤其是对于高度工业化国家具有不容置疑的重要意义的网络，如：

——能源供应（电力，天然气）

——城市淡水供应与废水处理

——信息与通信

——交通（铁路，公路）

——控制系统（数据采集与监控系统，SCADA）

这些系统之间大多存在不同程度和不同阶次的耦合及相互依赖作用，难以被轻易认知和仿真。通常，这些系统包括被控部分和控制部分，一般是使用与公共信息通信系统相同的运行技术，还可能采取更直接的技术，如互联网能够为交通网络提供数据和控制指令。本书将详述这些系统的结构条件。同时，我们也会介绍这些脆弱性评估方法的质量、适合性和不足。

本书通过领域内的重要文献报告的深入调研，充分结合作者正在开展的科研工作，旨在收集和获取复杂物理工程网络的脆弱性研究领域的知识。本书的读者包括自然与工程科学的硕士或博士研究生，相关领域的研究员，产业和机构中的非日常从业人员，以及负责关键基础设施设计和保护的主管人员。

本书按照一个虚拟的脆弱性分析过程进行编排。首先，本书采取自上而下的方式介绍了关键基础设施，定义了脆弱性等关键术语的概念；其次，阐述了关键基础设施相互依赖的复杂性和维度等重要特征，以及在探知基础设施性质方法中存在的挑战。本书用更加普遍的术语对脆弱性的评估方法进行分类和概述。之后，在重要章节中详细介绍了用于筛选分析和深入分析的一些方法。在方法选择时，主要取决于选择的方法能否应对由于基础设施类型和基本特点不同带来的挑战和是否能达到事先定义的分析目标。复杂网络理论、概率方法和多个体仿真等方法将被作为重点，还借助算例分析来介绍它们的基本方法、算法规则和运用方式。其优缺点将被分开讨论，最后进行比较。一些著名的方法，例如 Petri 网络，会在后面提到但不会做详细说明；参考书籍也会给出。

缩略词

ABM	Agent – based modeling　多个体仿真
ALMs	Accelerated lifetime models　加速寿命模型
ALSP	Aggregate level simulation protocol　聚合级仿真协议
ATHEANA	A technique for human error analysis　人因失误分析技术
BNs	Bayesian networks　贝叶斯网络
CARA	Controller action reliability assessment　控制器动作可靠性评估
CCDF	Complementary – cumulative distribution function　互补累积分布函数
CDM	Communication data and management　通信数据和管理
CFP	Cognitive failure probability　认知失效概率
CIs	Critical infrastructures　关键基础设施
CREAM	Cognitive reliability and error analysis method　认知可靠性和误差分析方法
CTMC	Continuous – time Markov chain　连续时间的马尔可夫链
DAWG	Data analysis working group　数据分析工作小组
DISD	Distributed interactive simulation　分布式交互仿真
DMSO	U. S. Defense modeling and simulation office 美国国防部建模与仿真办公室
DOE	U. S. Department of energy　美国能源部
EHV	Extra – high voltage　超高压
ENTSO – E	European network of transmission system operators for electricity 欧洲电力传输网络系统运营商
EPOCHS	Electric power and communication synchronizing simulator 电力和通信同步模拟器
EPS	Electric power system　电力系统
EPSS	Electric power supply system　电力供电系统
ET	Event tree　事件树

FLSC	Swedish air force air combat simulation center 瑞典空军作战模拟中心
FOM	Federate object model　联邦对象模型
FSM	Finite state machine　有限状态机
FMEA	Failure modes and effects analysis　故障模式和影响分析
FT	Fault tree　故障树
GLMs	Generalized linear models　广义线性模型
GVW	Geographic valued worth　地理权衡的价值
HAZOP	Hazard and operability　危险与可操作性
HEART	Human error assessment and reduction technique 人因失误评估和降低技术
HLA	High level architecture　高层体系结构
HRA	Human reliability analysis　人因可靠性分析
ICT	Information communication technology　信息通信技术
IEEE	Institute of Electrical and Electronic Engineers 电气与电子工程师协会
IEs	Initiating events　触发事件
IRRIS	Integrated risk reduction of information – based infrastructure systems 基于信息的基础设施系统的综合风险降低
ISS	Interactive simulation systems　交互式仿真系统
LAN	Local area network　局域网
LTI	Linear time invariant　线性时不变
MCs	Markov chains　马尔可夫链
MAUT	Multi – attitude utility theory　多态效用理论
MCS	Minimal cut set　最小割集
MLDs	Master logic diagrams　主逻辑图
MPNs	Markov/Petri nets　马尔可夫/Petri 网
MTTF	Mean – time – to – failure　平均故障间隔时间
NERC	North American electricity reliability council 北美电力可靠性委员会
NET	Network event tree　网络事件树

NSF	National science foundation 美国国家科学基金会
OMT	Object model template 对象模型模板
OPF	Optimal power flow 最优潮流
PHMs	Proportional hazard models 比例风险模型
PI	Performance index 性能指标
PRA	Probabilistic risk assessment 概率风险评估
QRA	Quantitative risk assessment 定量风险评估
RTI	Run time infrastructure 运行支撑系统
RTU	Remote terminal unit 远程测控终端
SCADA	Supervisory control and data acquisition 监测控制和数据采集
SHERPA	Systematic human error reduction and prediction approach 系统的人因失误降低和预测方法
SLIM/MAUD	Success likelihood index method/multi – attribute utility decomposition 成功可能性指数法/多态效用分解
SOC	Self – organized criticality 自组织临界性
SOM	Simulate object model 模拟对象模型
SUB	Substation 变电站
THERP	Technique for human error rate prediction 人因失误率预测技术
TSO	Transmission systems operator 传输系统运营商
UCTE	Union for the coordination of transmission of electricity 电力协调传输联盟
UML	Unified modeling language 统一建模语言
WAN	Wide area network 广域网

目　录

缩略词 …… XVI

第 1 章　重要术语的介绍和定义 …… 1

参考文献 …… 6

第 2 章　关键基础设施的属性 …… 8

2.1　复杂性 …… 8
2.2　经验知识 …… 9
2.3　依赖的维度 …… 17
2.4　关键基础设施(相互)依赖关系的实证研究 …… 21
2.5　关键程度 …… 23
参考文献 …… 26

第 3 章　关键基础设施脆弱性分析方法面临的挑战 …… 27

3.1　涌现行为 …… 27
3.2　相互作用的复杂规则 …… 28
3.3　单系统的特点和“体系” …… 28
3.3.1　多层系统 …… 28
3.3.2　状态更改 …… 28
3.3.3　演化系统 …… 29
3.3.4　体系 …… 30
3.4　多样的危害和威胁 …… 30
参考文献 …… 32

第 4 章　基本方法 …… 33

4.1　统计分析 …… 33
4.2　概率模型 …… 37

4.3 风险分析 …… 38
4.4 复杂网络理论 …… 40
4.5 多个体的建模与仿真 …… 41
4.6 动态控制系统理论 …… 42
参考文献 …… 43

第5章 脆弱性评估的概念框架 …… 47

5.1 概要 …… 47
5.2 逐步评估方法的框架概要 …… 48
5.2.1 事前定义意外事件的评估方法框架 …… 48
5.2.2 包含情景生成的评估方法框架 …… 48
参考文献 …… 54

第6章 分析方法 …… 55

6.1 统计数据的评价 …… 55
6.2 复杂网络理论 …… 59
6.2.1 概念大纲 …… 59
6.2.2 建模技术 …… 60
6.2.3 级联失效建模 …… 69
6.2.4 期望的结果 …… 71
6.2.5 应用案例 …… 72
6.2.6 结论 …… 79
6.3 关键基础设施的风险分析 …… 80
6.3.1 概念大纲 …… 80
6.3.2 建模方法 …… 81
6.3.3 应用案例:针对恐怖袭击的电网脆弱性评估 …… 87
6.3.4 结论 …… 93
6.4 级联失效动力学的概率模型 …… 94
6.4.1 介绍 …… 94
6.4.2 概念框架 …… 94
6.4.3 电力系统中的级联失效机制 …… 94
6.4.4 应用案例:对于单个基础设施的级联失效动力学建模 …… 99
6.4.5 相互依赖的基础设施的概率动态建模 …… 101
6.4.6 结论 …… 107