国际信息工程先进技术译丛

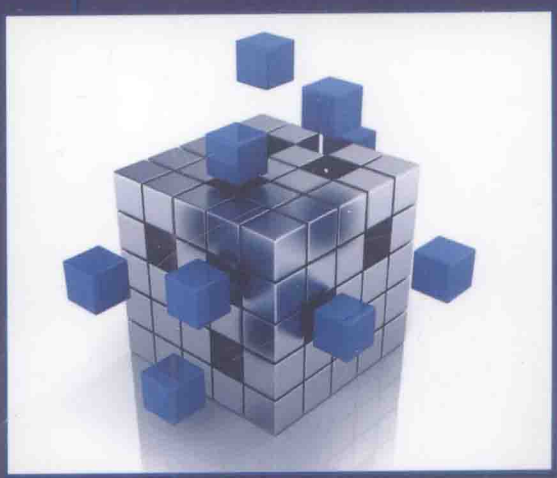
WILEY

工业关键系统的形式化方法：应用综述

Formal Methods for Industrial Critical Systems: A Survey of Applications

[意] Stefania Gnesi
Tiziana Margaria 著

靳添絮 连晓峰 等译



机械工业出版社
CHINA MACHINE PRESS

国际信息工程先进技术译丛

工业关键系统的形式化方法：应用综述

[意] Stefania Gnesi
Tiziana Margaria 著
靳添絮　连晓峰　等译

机械工业出版社

图书在版编目（CIP）数据

工业关键系统的形式化方法：应用综述/（意）格涅斯（Gnesi，S.），（意）玛格丽特（Margaria，T.）著；靳添絮等译．—北京：机械工业出版社，2014.12

（国际信息工程先进技术译丛）

书名原文：Formal methods for industrial critical systems：a survey of applications

ISBN 978-7-111-48521-6

Ⅰ.①工… Ⅱ.①格…②玛…③靳… Ⅲ.①计算机技术－应用－工业－自动控制系统－研究 Ⅳ.①TP273

中国版本图书馆 CIP 数据核字（2014）第 266002 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：顾 谦 责任编辑：顾 谦

版式设计：霍永明 责任校对：樊钟英

封面设计：马精明 责任印制：李 洋

北京市四季青双青印刷厂印刷

2015 年 1 月第 1 版第 1 次印刷

169mm×239mm · 15.25 印张 · 280 千字

0 001－2 600 册

标准书号：ISBN 978-7-111-48521-6

定价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务 网络服务

服务咨询热线：(010)88361066 机 工 官 网：www.cmpbook.com

读者购书热线：(010)68326294 机 工 官 博：weibo.com/cmp1952

(010)88379203 教育服务网：www.cmpedu.com

封面无防伪标均为盗版 金 书 网：www.golden-book.com

形式化方法以数学为基础，其目标是建立精确的、无二义性的语义，对系统开发的各个阶段进行有效的描述，使系统的结构具有先天的合理性、正确性和良好的维护性，能较好地满足用户需求。本书记录和展示了作者关于形式化方法如何在工业关键系统中进行应用的研究成果。

本书分为6部分：第1部分是概述；第2部分致力于介绍建模范例；第3部分介绍了包括形式化方法和相关工具的使用以及应用程序在实际系统领域的发展；第4部分则向读者展示了形式化方法在通信系统中的发展和成果；第5部分则介绍了形式化方法在互联网和在线服务方面的应用；而在第6部分则介绍了实时应用程序的形式化方法。

本书可用作高等院校计算机科学、自动化相关专业本科生、研究生以及教师的参考用书，也可作为业内专业人士的参考书。

译 者 序

形式化方法以数学为基础，对系统开发的各个阶段进行有效的描述，是有效验证系统设计和开发正确性的重要手段之一。让已经被普遍应用于测试方法复杂且对安全性有很高要求的控制系统的形式化方法更好地融入工业中，并使得它们在那里可以发挥最大的作用，这也是译者翻译本书的初衷。

本书作者是 Stefania Gnesi 和 Tiziana Margaria。其中，Stefania Gnesi 之前在佛罗伦萨大学任教，主讲针对软件系统分析和规范的方法和工具，现在是意大利比萨 ISTI-CNR 的一位形式化方法和工具实验室的领导。而 Tiziana Margaria 则是波茨坦大学数学和自然科学学院的一位教授，在那里她负责信息学院的服务和软件工程学科，也曾在德国哥廷根（Göttingen）大学、多特蒙德工业大学、帕绍大学，以及瑞典和意大利的大学游历过。应该说，作者在形式化方法在工业关键系统应用方面是有很深研究的。

本书分为 6 部分：第 1 部分是概述；第 2 部分致力于介绍建模范例；第 3 部分介绍了包括形式化方法和相关工具的使用以及应用程序在实际系统领域的发展；第 4 部分则向读者展示了形式化方法在通信系统的发展和成果；第 5 部分则介绍了形式化方法在互联网和在线服务方面的应用；而在第 6 部分则介绍了实时应用程序的形式化方法。

本书第 1 ~3 章由靳添絮翻译，第 4 ~7 章由连晓峰翻译，第 8 章由董美华、胡冰川、班岚和金成学翻译，第 9 章由胡波、周锐、王佩荣和潘媛翻译，第 10 章由苑昆、郑舒阳、贾琦和毋冬翻译，第 11 章由陆亚灵、郭晓钰和王炜伊翻译。全书由靳添絮审校整理，并对原书中的错误进行修正。

限于译者的经验和水平，书中难免存在缺点和错误，敬请广大读者批评指正。

译 者

原 书 序

——Mike Hinchey

正如我们所知，作为许多信用先驱动机的第一台计算机是整个19世纪航运业的一个重大问题。在此期间出现的对数表对该行业至关重要，通常包含造成船只、货物和生命损失的简单但显著的错误。一般认为Babbage差动机可体现计算机系统许多概念标准（包括存储、程序甚至类似于现代激光打印机工作原理的打印机设计）。目的是实现自动打印航运业常用的表格并降低不准确性。

取决于计算位置的数据*正确性*对航运业尤为关键。“正确性”的概念自从计算机科学真正成立以来就一直受到困惑。在第一台实用计算机（正如现在所知）出现之前，图灵（Turing）就一直关注着20世纪30年代出现的问题。计算机先驱，如Zuse和Wilkes早就意识到，正确性将是需要解决的重要问题。

20世纪60年以来或自从具有现代电子计算机以来，可靠性和可信性等相关问题就一直受到安全、保护、性能以及许多其他问题的高度关注。提出形式化方法（Formal methods）（先于现代计算机本身的一个术语）来解决软件系统和硬件系统中的正确性问题以及涉及的其他相关问题。

对于确认“形式方法学”的学者，这是一个极大的进步，并欣慰地看到在该领域取得显著进展以及形式化方法对关键应用领域的极大贡献。然而，在现实中，形式化方法仍没有在实践中得到所期望的广泛应用，许多人认为该方法并未形成规模，成本高，且难以理解和应用。

形式化方法研究人员认为主要关注于教学、开发更多有用符号以及更好（集成）的支持工具，强调系统的某一方面而不是整个系统（即所谓的形式化方法作用），建立用户社区，并鼓励在现实生活中应用形式化方法。在关键的工业领域，形式化方法已得到广泛应用。值得注意的是，“关键”的定义已发生变化，意味着不仅仅是生命或财产损失，或违反安全以及故障所产生的后果，而且在商业意义上，还意味着金融损失、丧失竞争力或声誉受损。

从事工业关键系统中的形式化方法（FMICS）研究的是从1992年运行至今的运行时间最长的欧洲信息与数学研究联盟工作组（ERCIM）。该工作组由超过12个ERCIM合作伙伴以及欧洲其他几十个相关研究组组成，致力于提高基于形式化方法的技术，并鼓励通过技术转让激励形式化方法在关键工业中的应用。

本书汇集了该工作组优秀研究成果以及在关键工业中的应用实例，如航空、

航天、铁路信号（已成为形式化方法技术的一个主要驱动行业）等领域。尽管本书从规范到实现和校验等各个方面讨论了形式化方法，但重点在于模型校验，反映过去10年左右时间内在工业应用中的显著进步与成功应用。

应用结果表明形式化方法在工业关键系统中的正确性。各位作者都是各自领域的专家，但不应该低估在将形式化方法引入行业中的极大困难，这种信息非常简单：对于特定应用领域和特定关键工业，形式化方法将会继续存在。

Mike Hinchey
勒罗（Lero），利默里克（Limerick）

——Alessandro Fantechi 和 Pedro Merino

本书具有很长历史，这是ERCIM中FMICS研究组的部分历史，这是该联盟中时间最久的活跃工作组。

FMICS工作组致力于形式化校验技术的发展，并开发如国际联合项目、校验相关和形式化方面的软件，并从1996年开始，举办FMICS年度研讨会。

这些活动大大促进了关于目前进行的确定最有效的形式化开发和校验技术的科学研讨，并在工业应用方面有着敏锐观察。FMICS社会成员大多与行业联系紧密，由此直接对过去10年内在工业关键系统中发展缓慢但不断引入的形式化方法作出巨大贡献。

本书的出版来源于2004年在Aix Les Bain举行的研讨会。形式化方法的不断发展，特别是由于工具性能不断完善的越来越多模型校验技术，以及近年来出现的基于模型的设计等日益增长的重要性，使之在一本书中难以全部展现当前工业应用中的发展现状。因此，本书的内容在过去几年内不断变化。

作为FMICS工作组的总负责人，为此特别感谢本书编辑，他们成功收集了该研究领域不断发展，以及在工业生产中日益增长的软件和计算机控制系统应用的文献资料。因此，我们相信这是形式化方法在大量不同领域得到应用的见证。

Alessandro Fantechi 和 Pedro Merino
FMICS 工作组主席

原书前言

目前，形式化方法的必要性已作为设计过程中不可缺少的环节，在工业安全关键系统中得到广泛认可。在更通用的定义中，“形式化方法”一词包括了所有具有精确数学语义以及以形式化方式描述系统行为的相关分析方法的符号。

在过去十几年内，出现了许多形式化方法：声明法、并发和移动系统的过程演算法以及相关语言等其他方法。尽管这些形式化方法的优点不可否认，但实践经验表明，每个方法都特别适用于处理系统某些方面。因此，设计一个理想的复杂工业系统需要多个形式化方法的专家从不同角度来描述和分析系统。

本书的目的主要是提供一种目前工业关键系统设计中主流形式化方法的全面介绍。本书有3个目标：减轻形式化方法的学习负担，这也是在工业应用中的一个主要缺点；帮助设计人员选择采用最适合其系统的形式化方法；介绍关键系统分析的先进技术和工具。

本书分为6部分。第1部分为概述和发展现状。第2部分专门介绍建模范例。其中第2章是关于同步数据流语言LUSTRE及其在SCADE工具集中的产业转移；第3章介绍了群智能的基本概念，这在各种不同应用领域如医疗、生物信息学、军事/防御、监控，甚至互联网电视广播中得到广泛应用。讨论了适用于基于群智能的系统中形式化方法的具体要求。

第3部分包括有关在实际系统中形式化方法的应用及其相关工具的开发应用。其中第4章主要是关于交通运输系统，介绍了在当前工业应用中铁路信号形式化方法的综述；第5章介绍了模型校验技术在航空电子领域中的应用。

第4部分介绍了形式化方法在通信系统中的应用。其中在第6章中阐述了如何应用形式化方法来提高主动服务的可靠性，尤其是重点关注代码移植、路由信息、高度重配置、服务间交互或安全策略等方面，包括互联网和在线服务；第7章介绍了概率模型校验的应用，特别是利用概率定时自动机进行通信协议，并重点进行了工业相关的IEEE 802.3（CSMA/CD）案例分析。

第5部分涵盖了互联网与在线服务。其中第8章介绍了如何利用模型首先描述和验证在线分布式决策系统中的单变量，设计为一个大型协作模型的集合及自动机学习用于确定实现后实际系统的集体应急行为；第9章描述了利用模型校验来验证具有发布/订阅通知服务的群件系统中的用户意识。

第6部分介绍了运行时形式化方法的应用。其中第10章中，介绍了测试和测试控制表示版本3（TTCN-3），并应用于Web服务测试；第11章对实际中自

动机学习以及其面临的主要挑战、改进以及可能的解决方案进行综述，并进行案例分析，以表明理论研究主动学习技术可得到强大应用，从而成为实际系统开发中的重要工具。

尽管意识到本书不能详尽、全面地介绍形式化方法在工业中的应用，但相信并希望读者能从中体会到该方法可能在实践应用中不断提高和促进。

Stefania Gnesi
Tiziana Margaria

目　　录

第3部分　交通运输系统

第4部分 通信系统

第5部分　互联网与在线服务

第6部分 运行时：测试和模型学习

第 1 部分

概述和发展现状