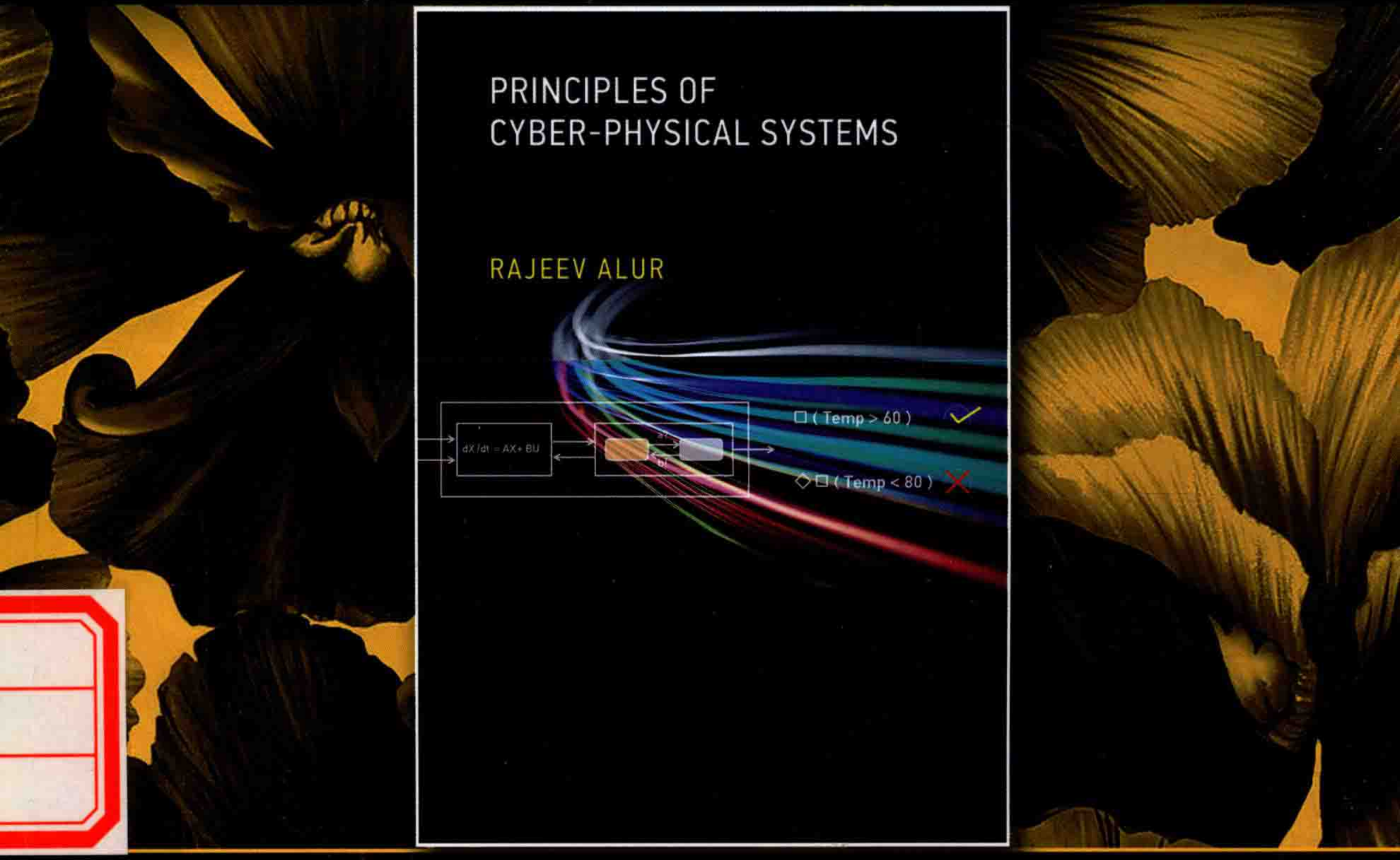
HZ BOOKS
华章教育

计　算　机　科　学　丛　书

信息物理融合系统（CPS）原理

[美]　拉吉夫·阿卢尔（Rajeev Alur）　著
董云卫 张雨　译

Principles of Cyber-Physical Systems



机械工业出版社
China Machine Press

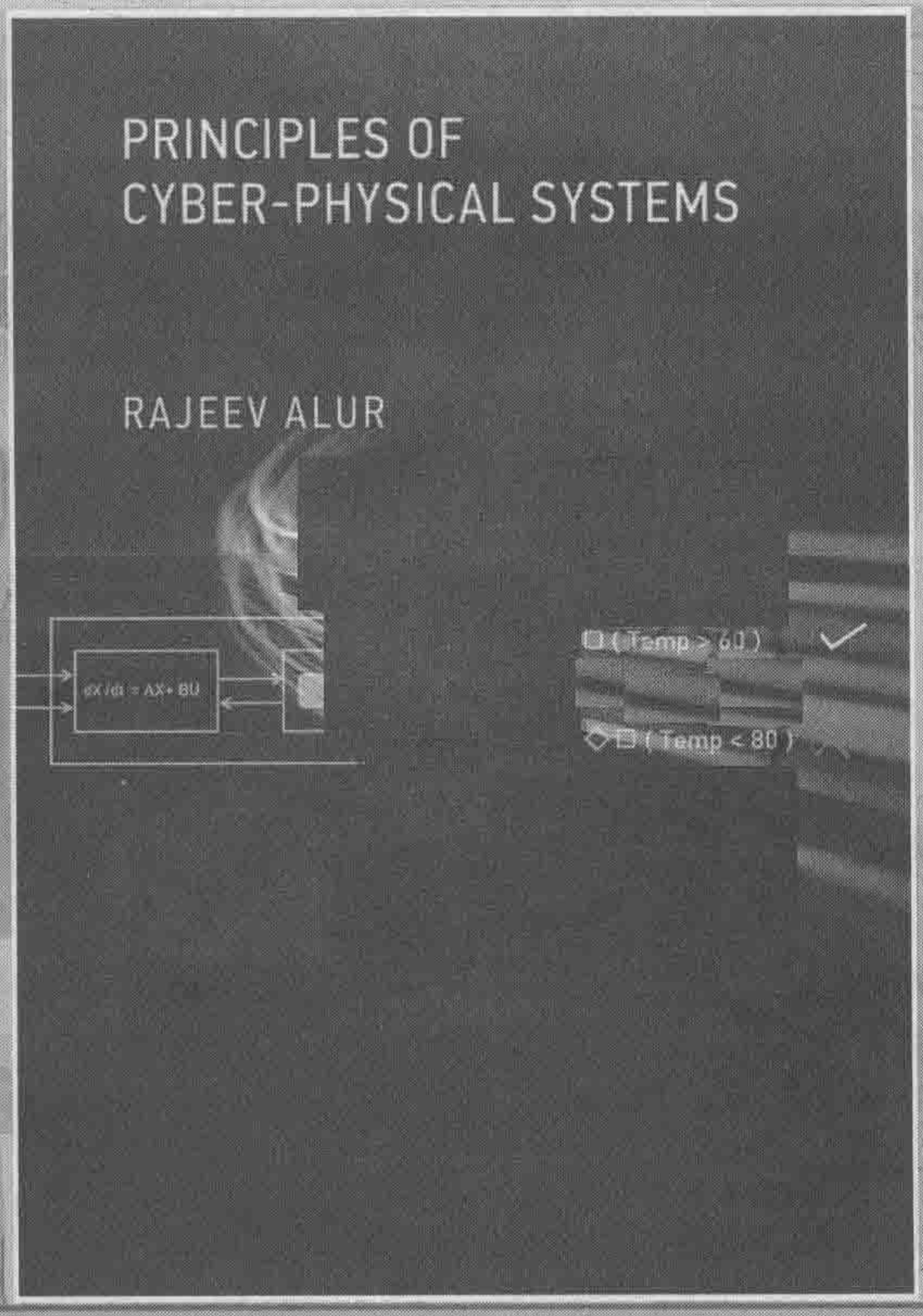
机 科 学 丛 书

信息物理融合系统（CPS）原理

[美] 拉吉夫·阿卢尔（Rajeev Alur）著

董云卫 张雨 译

Principles of Cyber-Physical Systems



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

信息物理融合系统（CPS）原理 /（美）拉吉夫·阿卢尔（Rajeev Alur）著；董云卫，张雨译．
—北京：机械工业出版社，2017.1
（计算机科学丛书）
书名原文：Principles of Cyber-Physical Systems

ISBN 978-7-111-55904-7

I. 信… II. ①拉… ②董… ③张… III. 异构网络－研究 IV. TP393.02

中国版本图书馆 CIP 数据核字（2017）第 020302 号

本书版权登记号：图字：01-2016-2387

本书主要介绍信息物理融合系统的基本理论，包括系统设计、规约、建模和分析方法。针对基于模型的设计、并发理论、分布式算法、形式化的规约和验证方法、控制理论、实时系统和混成系统等分支学科，从不同侧面对信息物理融合系统进行描述。本书采用数学化的建模、规约与分析等概念，并配以案例阐述信息物理系统所涉及的分布式算法、网络协议、控制设计和机器人等理论。

本书适合作为计算科学、计算机工程和电子工程相关学科的高年级本科生或一年级研究生的教材。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：盛思源　　责任校对：殷　虹
印　　刷：中国电影出版社印刷厂　　版　　次：2017 年 6 月第 1 版第 1 次印刷
开　　本：185mm×260mm　1/16　　印　　张：18.25
书　　号：ISBN 978-7-111-55904-7　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

文艺复兴以来，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的优势，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭示了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下，美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章公司较早意识到“出版要为教育服务”。自 1998 年开始，我们就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力，我们与 Pearson，McGraw-Hill，Elsevier，MIT，John Wiley & Sons，Cengage 等世界著名出版公司建立了良好的合作关系，从他们现有的数百种教材中甄选出 Andrew S. Tanenbaum，Bjarne Stroustrup，Brian W. Kernighan，Dennis Ritchie，Jim Gray，Afred V. Aho，John E. Hopcroft，Jeffrey D. Ullman，Abraham Silberschatz，William Stallings，Donald E. Knuth，John L. Hennessy，Larry L. Peterson 等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力相助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专门为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近两百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都将步入一个新的阶段，我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

华章网站：www. hzbook. com
电子邮件：hzjsj@hzbook. com
联系电话：(010)88379604
联系地址：北京市西城区百万庄南街 1 号
邮政编码：100037

华章科技图书出版中心

译者序

Principles of Cyber-Physical Systems

进入21世纪，以计算机科学为代表的信息技术发展迅猛，一些代表新技术发展的计算技术名词泉涌而出，如物联网、互联网+ 、云计算、大数据、工业4.0等，而信息物理融合系统(Cyber-Physical System，CPS)是其中最为引人关注的技术热词之一。CPS作为一个正式的概念于2006年由美国国家自然基金委员会科学家Helen Gates提出后，就被美国、欧盟和中国等各国政府定位为影响未来科技研究、国家信息技术与产业融合发展的国家战略目标，并制定了一系列的CPS技术研究和产业发展计划。

从技术上讲，CPS是为解决信息技术对传统产品数字化后所带来的问题进行的一次系统性思考。这些问题包括：数值计算误差积累、跨平台的计算时序性、开环控制的不确定性、分布式计算的网络时延、多核计算的调度性以及长生命周期产品的运维等。这些问题逐步成为一道阻碍新一代智能计算技术发展必须跨越的鸿沟。这就要求计算技术专家必须另辟计算科学的方法论和实践工程技术，指导工程技术人员在产品的策划和设计之初就用系统工程的观点，考虑贯穿于产品全生命周期的两类因素——物理过程和计算过程，以及它们之间的相互影响。

CPS技术的发展不仅要继承嵌入式系统、网络通信和控制论的技术和方法，同时还要对现有理论、技术框架进行突破和创新。CPS系统集成了计算过程和物理过程，并且物理过程与计算过程相互影响、深度融合。CPS的概念也指出了CPS的两条发展路径：物理系统的信息化和计算系统的物理化。这两条道路是将导致CPS的研究、开发和应用的多样化发展，还是将殊途同归、形成一套统一的理论和方法，还有待于广大的CPS技术研究开发人员通过进一步的努力来验证，我们将拭目以待。

本书从计算理论的角度总结了CPS技术必须考虑的理论方法，并综合了分布式控制和网络通信等相关技术，是一本系统介绍信息物理融合系统理论基础的教材或者工具书，不仅适合初学者，还适用于有相关经验的研究人员和工程技术人员。本书不但概述了信息物理融合系统的基本原理，而且详细介绍了对此类系统的规约、设计、建模和分析等一套理论，包括基于模型的设计方法、并发理论、分布式算法、形式化规约和验证方法、控制理论、实时系统和混成系统等，并配以案例分析来阐述信息物理系统所涉及的分布式算法、网络协议、控制设计和机器人等多学科分支理论。本书的选材和作为教材的特点在前言和第1章中已有详述，被世界名校采纳作为教材也充分说明了其价值，此处不再赘述。

本书的翻译主要由董云卫博士和张雨博士共同完成，西北工业大学嵌入式系统实验室的葛永琪、吴婷婷、魏晓敏、孙鹏鹏、贺媛媛、姜臻颖、魏昕和李峰等研究生也参与了本书的部分翻译和校对，他们为本书的出版付出了辛勤劳动。

由于中西方文化背景上的差异以及我们的学术和语言水平的限制，译文中难免有不妥甚至错误之处，欢迎读者及专家批评指正。

译者

2016年10月1日于西安

信息物理融合系统由能够相互通信的计算设备组成，这些计算设备借助传感器和作动器实现与物理世界的交互。现实生活中，这样的系统越来越多，从智能建筑到医疗设备再到汽车都可以看作信息物理融合系统。在过去的十多年中，开发确保信息物理融合系统可靠性的设计和分析工具是一项具有挑战性的工作，它吸引了众多学术界和工业界的研究人员开展卓有成效的跨学科研究。

本书的目标是为信息物理融合系统的设计、规约、建模和分析提供一套基本理论，这些理论勾画了开发信息物理融合系统所涉及的众多分支学科，包括基于模型的设计方法、并发理论、分布式算法、规约和验证的形式化方法、控制理论、实时系统和混成系统。我试图为信息物理融合系统设计和分析方法相关的研究主题提供一套脉络清晰的理论思想。全书采用数学化的建模、规约与分析等概念，并配以案例研究图解来阐述信息物理系统所涉及的分布式算法、网络协议、控制设计和机器人等多学科分支理论。

本教材自成体系，适合作为计算科学、计算机工程和电子工程相关学科的高年级本科生或一年级研究生一学期课程的教材。第 1 章讨论了几种可供选择的课程组合。

我对信息物理融合系统的研究兴趣萌生于 20 世纪 90 年代和 Tom Henzinger 合作研究混成系统协同性。另外，本教材的结构基于我与 Tom 合作撰写但未出版的课堂讲义《Computer-Aided Verification》(计算机辅助验证)，其中，第 2 章和第 3 章中的一些例子和图例也来自该讲义，并得到 Tom 的同意。因此，Tom 对本教材的贡献是不可估量的，我对他表达崇高的敬意。

我对信息物理融合系统的理解和本书的内容深受宾夕法尼亚大学工程学院 RECISE 信息物理融合系统研究中心的学生和同事的影响。在此，我对我的同事 Vijay Kumar、Insup Lee、Rahul Mangharam、George Pappas、Linh Phan、Oleg Sokolsky 和 Ufuk Topcu 给予的合作与支持表示敬意。同时，我还要感谢 DARPA 和 NSF 在信息物理融合系统研究项目上对我的持续资助。

在过去的 5 年中，我已经勾画出了本教材的草稿，取名《Principles of Embedded Computation》(嵌入式计算的基本原理)，最初目标是在宾夕法尼亚大学开设一门嵌入式系统硕士研究生课程。定期教授这门课程是促使我完成本书的关键动因，学生的反馈也极大地促进了本教材内容的完善。感谢所有的学生和勤勉的助教，他们是 Sanjian Chen、Zhihao Jiang、Salar Moarref、Truong Nghiem、Nimit Singhania 和 Rahul Vasist。

我也很幸运地收到了其他大学的研究者对本教材手稿的反馈建议。特别是根据 Sriram Sankaranarayanan 和 Paulo Tabuada 的建议，对第 6 章和第 9 章的内容进行了很多修改。特别感谢 Christos Stergiou 对最新版本进行了仔细的推敲，并对第 9 章的例子用 Matlab 工具进行模拟。

借此机会感谢出版商(MIT 出版社)对本项目的支持，特别是 Virginia Crossman、Marie Lufkin Lee 和 Marc Lowenthal 在本书出版过程中提供了大量的帮助和鼓励。本书的写作耗时多年，如果没有家人的支持也是不可能完成的，我要特别感谢我妻子 Mona 的友善、爱和耐心。

Rajeev Alur
美国费城宾夕法尼亚大学
2015 年 1 月

目 录

Principles of Cyber-Physical Systems

第1章 简介

Principles of Cyber-Physical Systems

1.1 什么是信息物理融合系统

最早的计算机是专门用来进行数值计算和信息处理的单机系统。时至今日，我们也用计算机处理类似的任务，但是随着嵌入式系统的出现，计算机系统的作用已今非昔比，计算机无所不在。嵌入式系统是指集成了计算机硬件和计算机软件，为完成特定目的而设计的机电或电子系统。从手表到照相机，再到电冰箱，今天我们所能看到的工业产品几乎都属于嵌入式系统，因为在这些设备中集成了一个微控制器和相应的软件系统。信息物理融合系统是对嵌入式系统最一般意义的扩展。信息物理融合系统由一些能够相互通信的计算设备组成，这些计算设备能够通过传感器和作动器与物理世界实现反馈闭环式交互。这样的系统无所不在，并且发展越来越迅猛，从智能建筑到医疗设备再到汽车，都是信息物理融合系统的应用。

自主移动机器人团队就是信息物理融合系统的一个典型例子。给这个能够自主移动的机器人团队分配特定的任务：它们要从未知的建筑平面图所示的某一间屋子内识别和检索某一目标。为了完成该目标，每一个机器人都需要安装多种传感器，用来收集关于物理世界的相关信息。例如，安装 GPS 接收器用于跟踪机器人的位置，安装照相机用于获取周围环境的快照，安装红外温度传感器用于检测人的存在。该系统主要的计算问题是如何利用上述传感器所收集的信息来构造建筑物的完整地图，这就要求机器人团队中的每个机器人都能够通过无线链路以协调方式进行信息交换。机器人、障碍物和目标物的当前位置信息知识决定了每一个机器人移动的规划。机器人移动规划包括对每一个机器人发出的高级命令，诸如“以时速 5 英里向西北方向匀速移动”。这样的指令需要转换为控制机器人移动的电机的低级控制输入。设计目标包括安全操作(如机器人不能被障碍物或其他机器人绊倒)、任务完成(如目标物能够被机器人找到)和物理稳定性(如每一个机器人都应该是一个稳定的动态系统)。要构造这样一个多机器人协同系统来完成上述设计目标，就需要从控制、计算和通信相互协同的方式来考虑设计策略。

尽管从 20 世纪 80 年代起一些特定形态的信息物理融合系统就在工业领域得到应用，然而直到最近，嵌入式系统产品的部件才随着处理器、无线通信和传感器等技术的成熟以较低的成本就能具备较强的性能。人们逐渐认识到构造可靠的信息物理融合系统需要功能强大的计算平台作为支撑，而强大的计算平台的开发则需要先进的工具和开发方法。在 21 世纪初，为了迎接这个挑战，人们开始研究集成控制、计算和通信的系统方法论，这就成为一个催化剂，并形成了一个不同寻常的学科——信息物理融合系统。设计信息物理融合系统的相关理论已经被美国政府部门列为主要优先研究的科学技术，这在汽车、航空电子、制造业和医疗设备等工业界也一样被重视。

1.2 信息物理融合系统的主要特征

从计算机科学学科创建开始，对辅助开发人员构建计算机硬件和软件系统的理论、方

法和工具开展系统化研究就一直是计算机科学的研究主题。在经典的计算机理论中，软件理论研究只关注计算复杂性和基于结构化编程的开发方法这两个方面，这样的技术手段对于今天我们所面临的复杂软件基础平台系统开发是很有帮助的。然而，这些传统的软件系统设计理论却不能直接用来设计信息物理融合系统，这是因为二者在系统设计阶段的关注存在巨大的差异。下面我们将讨论信息物理融合系统的主要特征。

反应式计算

在经典的计算模型中，当我们给计算设备提供一个输入时，它就会产生一个输出。例如排序程序就是这样的一种计算，给程序输入一列数据，程序经过计算后输出一列经过排序的数据。我们把计算程序由输入到输出的正确性用数学方法抽象为一个函数。程序的计算性和复杂性理论可以帮助我们理解一个函数是否是可计算的，以及计算的效率如何。传统的软件程序是对函数或过程的抽象，这种抽象可以很方便地把简单函数进行组合，形成复杂的函数，进而完成软件程序的开发。

相比之下，一个反应式系统可以与环境持续不断地进行从输入到输出的交互。例如，在汽车的巡航控制器程序这样一个典型的反应式计算的例子中，当我们希望改变汽车的行驶速度时，我们就向控制程序输入一个高级输入命令：打开或关闭巡航控制器。控制程序就需要对我们的输入做出反应：产生一个输出，这个输出就是作用到汽车发动机油门的受力反应。同样，巡航控制系统的行为自然地可用一个能够被观察到的输入和输出序列来描述，这种详细说明输入/输出序列的正确描述对应着控制系统可接受的运行行为。信息物理融合系统就是一个反应式系统，因此本书所关注的设计对象就是反应式计算类型的系统。

并发性

在传统的顺序计算模型中，计算是由一个可顺序执行的指令序列组成，并且在同一时刻只能有一条指令执行。在并发计算过程中，如多线程(通常又称为构件或进程)计算，计算构件是可并发执行的，并且计算在执行过程中，并发执行的构件之间相互交换信息以完成最终的计算目标。并发性是信息物理融合系统的基本特征。我们给出一个能够自主移动机器人团队的例子。在这个例子中，机器人团队中的每一个成员都是一个具有可分离属性的个体，并且可以并发执行。每一个机器人都有多个传感器和处理器，计算任务由一组与环境相关的指令蓝图组成，这些指令包含了机器人对环境感知的视觉数据和运动路径规划信息，并且对这些信息的处理可以分解到不同的处理器中并行运算。运动路径规划任务可以分解为有逻辑关系的可并发执行子任务，例如，基于局部规划的避障子任务和基于全局规划的向目标前进的行走路径子任务。

理解分布式并发计算系统模型和设计的基本原理对信息物理融合系统开发是至关重要的。对于顺序计算来说，图灵机模型被认为是最经典计算模型，然而，对于并发计算来说，还没有一种现成的形式化模型被广泛认可。广义地讲，当前的计算模型可以分为两类：1）同步模型：构件依据锁步协调运行，并且计算以同步循环逻辑顺序推进；2）异步模型：构件以独立的速度运行，它们之间通过发送和接收消息来交换运行所需的信息。这两种计算模型对信息物理融合系统的设计是非常有用的。在我们的例子中，机器人系统可以看作由多个能够交换信息的机器人个体组成的一种异步系统。为了便于机器人个体计算过程设计的简单化，一个机器人的计算过程可以分解为依据某种同步逻辑方式而并发执行的许多活动。

物理世界的反馈控制

控制系统与物理世界以反馈回路方式进行交互，这种交互过程是通过传感器来测量环

境信息变化，并通过作动器来对环境施加影响。例如，轿车的巡航控制器不停地监视轿车的行驶速度，并适时调整油门，以确保轿车的行驶速度接近期望的巡航速度。轿车控制器就是一种信息物理融合系统的构件，它们与传统的计算机不同，信息物理融合系统中的计算设备与物理装置集成在一起。

对于控制器的设计来说，物理装置要求对物理量进行动态建模：为了调整油门的受力，巡航控制器需要建立轿车行驶的速度模型，该模型把速度看作油门随时间而变化的函数。动态控制系统的设计和分析有一套完整的理论，这些基本原理包含了丰富的数学工具，理解这些基本原理对信息物理融合系统的设计者来说是最基本的要求，也是非常有价值的。传统的控制理论只关注连续时间系统。在信息物理融合系统中，组成控制器的软件是离散的，软件由可并发执行的构件组成，它们可能有多种运行模式，并且能够与连续演化的物理世界进行交互。这样的系统又称为混成系统，它是由离散的计算过程和连续动态过程混合而成。这种系统的控制器设计和分析所需的基本理论正是本书所讨论的主题。

实时计算

编程语言、支持操作系统和处理器体系结构的基础设施，通常都不支持实时的具体表示方式。它们对传统的计算应用，如文件处理，提供了较为方便的抽象，但是实时性能对于信息物理融合系统来说是非常重要的。例如，巡航控制器为了满足控制轿车速度的需要，设计控制器时，需要把组成控制器的子构件的计算执行和通信消耗时间考虑进去。

通过对时间延迟建模、理解时间延迟对需求正确性、系统性能、时间依赖的协调协议和资源分配策略等属性的影响，能确保实时系统相关属性的可预测性，这也是实时系统的一个分支的研究主题。研究信息物理融合系统的设计和实现理论方法的目的就是要基于这些技术来构造信息物理融合系统。

安全攸关应用

当设计和实现一套巡航控制器时，系统中的一些错误可能会导致系统产生一些不可接受的后果(如导致死亡)，因此，我们希望在较高的层次上保证系统操作的正确性。一些应用系统在设计时，把系统安全性设计提高到优先于其他属性(如系统性能、开发成本等)的级别，这类的应用称为安全攸关应用。例如，航空电子、汽车电子和医疗设备等信息物理融合系统中的计算设备就是安全攸关应用。基于此观点，我们需要建立这样的概念：在设计阶段就需要确保系统可正确地工作是至关重要的，并且，有的时候也是政府对这类系统认证的相关法规的强制性要求。

传统的系统开发流程是设计、实现、广泛的测试和对检测到的错误逐一验证。此外，还有更多理论方法用于系统开发，包括数学计算误差精度需求的实现、支持系统操作环境的系统构件的模型设计、利用分析工具对系统模型满足需求进行检查等。与传统的开发方法相比，这些方法能够在系统开发早期检测到系统设计中存在的错误，确保系统具有较高的可靠性。这些基于形式化模型和验证方法的安全攸关应用开发方法日益被行业采用，这也是本书集中讨论的主题。

1.3　研究主题概述

本书的目标是介绍信息物理融合系统的基本原理方法，包括系统设计、规约、建模和分析方法。为了突显信息物理融合系统的重要特征，本书主要针对基于模型的设计、并发理论、分布式算法、规约和验证的形式化方法、控制理论、实时系统和混成系统等分支学科，从不同侧面对信息物理融合系统进行描述。现有的研究资料和教材力求对这些技术原

理进行阐述，并着重解释信息物理融合系统在设计和分析过程中需要用到的上述理论方法中的有关核心概念，这也是本书致力实现的目标。本书主要讨论形式化模型、基于模型的设计，以及规约与分析三个方面，并把这三个方面交织起来讲述，下面就这三个方面的主题进行具体阐述。

形式化模型

系统设计过程中对系统进行建模的目的是为复杂系统设计的管理提供一种数学抽象手段。在反应式系统模型中，构件是模型的基本单元，它通过输入和输出与环境进行交互。不同的交互方式可以设计成不同类的模型。我们从第2章开始关注同步建模，所有同步模型中的构件都将遵循锁步依次执行。在第4章中，我们将关注异步模型，在这类模型中不同活动可以以不同的速度独立执行。在第6章中，我们将研究动态系统的连续时间模型，这种模型适合于刻画物理世界动态演化的属性。第7章介绍时间模型，该类模型通过具体的时间延迟边界为描述构件之间交互的时间属性提供便利。最后，第9章通过集成离散交互和动态系统来研究混成系统。

为了描述模型，我们综合应用方框图、代码段、状态机和微分方程等方法来对系统进行建模。我们采用一种精确的数学描述方法来形式化地定义模型，利用该模型的形式语义可帮助我们回答诸如此类的棘手问题："系统构件可能包含的行为有哪些?"和"构件组合后导致的结果是什么?"等。本书介绍的建模概念的例子包括：非确定性行为、构件的输入/输出接口、时间触发和时间触发的通信、同步组合的等待依赖、共享内存通信、同步原语的原子性、异步系统的公平性、动态系统的均衡性、时间与混成系统的奇诺(Zeno)行为等。

规约与分析

为了验证系统设计(或系统实现)是否满足如预期设想的正确性，系统设计者首先需用数学精确方式来正确地刻画所捕获的系统需求。然后，设计者可以用分析工具对系统需求进行验证。本书讨论需求的形式化规约方法，以及与形式化验证相关的技术。

第3章介绍安全性需求。安全性需求可以表述为：任何坏的状态(或事件)都不会发生，并且可以用不变量或监视器来形式化地描述。我们首先选择归纳不变量的通用技术来证明一个系统是否满足安全性规约，并且利用状态空间搜索算法来自动构建安全性属性。这类算法包括枚举和符号搜索算法，包括使用有序二叉判定图(BDD)的数据结构的符号搜索算法，该算法通常用于硬件验证。由于信息物理融合系统中存在时间相关的动态连续变量，所以这给信息物理融合系统的安全性验证提出了新的挑战。为了验证系统的混成动态属性，我们研究基于栅栏函数(barrier certificate)和符号搜索算法的系统证明方法，这两类特殊的验证方法称为时间自动机和线性混成自动机。

第5章介绍活性需求：这种规约可以描述为"好的事件最终会发生"。我们介绍时序逻辑线性时序逻辑(LTL)来形式化地表示这样的正确活性需求，并说明为了便于捕获LTL需求，监控器如何生成Büchi自动机。模型检验是一种对系统模型的LTL需求进行自动化验证的常用方法。不管是枚举还是状态空间搜索技术，最终都可归类为求解模型检验问题，并且活性需求也可以用一种称为排名函数的通用证明理论来证明。

对于动态系统来说，最基本的设计需求在于系统是否具有稳定性，它的非形式化表式是指系统的一个微小的输入扰动不会导致系统可观察行为的不对称变化。该属性是控制论的经典话题，将在第6章中讨论，本书也会特别介绍线性系统。在此类系统建模中，使用线性代数是非常有效的设计系统稳定性模型的数学工具。

在实现嵌入式系统时，一个主要的问题是如何建立时间延迟分析模型，该模型需要能够刻画系统模型中不同任务在给定的计算平台上运行时，关于时间延迟与模型级别假设的一致性。实时调度理论的目标就是对此类问题进行形式化描述，并提供相应的解决方法，该内容将在第 8 章中讨论。我们主要着重理解两种基本调度算法：最早截止期优先(EDF)算法和单调速率算法。

6

基于模型的设计和案例研究

建模、规约和分析的理论可通过系统设计问题的构造方法进行阐述，如分布式算法、网络协议、控制设计和机器人技术。我们将阐述建模与编程的区别，例如，能够对非确定性行为进行规约，也可以包括环境行为的显式模型。在设计基于模型的解决方案时，需要强调两个原则：

1) 结构化设计：简单的构件可以组装在一起来执行多个复杂的任务，相反地，一个设计问题可以分解为多个简单的子任务。

2) 基于需求的设计：在前面准确说明正确性需求，而且在早期阶段还可用来指导设计的选择和调试。

我们研究互斥、一致性和首项选择等的经典分布式协调问题。这些问题在本教材中会反复介绍，并且还会强调介绍协同原语对系统设计的影响。另外，还将重点讲述消息通信的问题，包括：在有损网络中如何可靠地传递信息；在通信过程中由于时钟缺陷导致时间不确定性时，如何同步信息的发送者和接受者。我们通过巡航控制器设计的例子来说明如何用低层级 PID 控制器设计框图来开展集成化同步设计。教材内容还包括信息物理融合系统的案例研究：设计心脏起搏器监视器和心脏起搏器的时间模式反应器；设计机器人团队协调避障系统和多跳网络通信稳定控制器。

1.4　课程组织指南

本书适合作为计算机科学、计算机工程和电子工程等专业高年级本科生或一年级研究生一个学期课时的教材。本节将对课程组织给出一些建议。

先修课程

本教材重点讲述了信息物理融合系统的建模、设计、规约和分析的基本原理。这些原理涉及许多数学知识，如微积分、离散数学、线性代数和逻辑学等。教材中的许多概念来源于微积分，因此这些题目中的课程不是先修课程。然而，学习本教材并不要求完全掌握这些基本知识。当然，要正确理解本教材的内容，也需要掌握一些必要的数学理论知识。本教材适用对象是完成了先修理论知识、计算机科学课程(如离散数学和计算理论)或电子工程课程(信号和系统、动态系统)的学生。

7

在本教材中，我们讨论应用系统的设计问题，这些应用包括控制系统、分布式协调系统、网络通信协议和机器人。在每一个案例研究中，需要具备相关数学理论基础来阐述应用领域的基本约束条件，而不需要明确的背景知识。然而，要很好地理解教材中的案例，具有软件或系统设计与实现相关的一些经验是需要的。这些经验可以从面向本科生开设的一些课程中获得，例如，操作系统和程序开发等计算机科学课程、机械或控制系统等电子工程课程。

章节选择

课时量为一学期的课程不需要讲解课本的全部内容。图 1-1 显示了各章之间的依赖关系，它可以作为组织本课程教学各章节内容的指导。即便要把标有星号的可选内容略过，

但每章中的基本概念是必须讲解的。下面介绍三种可选的课程组织方式。

图 1-1 各章之间的依赖关系

快节奏课程组织方式，其目的是涵盖建模、设计、规约和验证的所有内容，这种组织方式在宾夕福尼亚大学讲授了多年，证明是可行的。如果选择这种课程组织方式，我们推荐跳过 3.3 节、5.3 节、6.4 节、7.2 节和 9.3 节等。

基本课程组织方式，只关注与建模和设计相关的内容，忽略分析和验证技术。在组织此方式下，3.3 节、3.4 节、5.2 节、5.3 节、6.4 节、7.3 节和 9.3 节可以跳过不讲。然而，我们还是推荐有些内容需要要重点讲解，如原则性设计中的形式化规约需求，因此应该包括规约的形式化方法。

第三种课程组织方式是通过删除第 6、8 和 9 章来缩小教学范围。这种教学方式只关注反应式系统的建模、设计、规约和验证技术，不包括计算系统与物理世界交互的建模。

作业和项目

在每一章内容之后都设计了大量的作业，希望学生能够用严格的数学方法来解答作业中提出的问题。一些具有挑战性的作业已用星号进行了标识。

除了设计了一些解决方法理论性强的作业外，教材还提供了一些应用项目来训练软件的建模和分析方法。本教材仅限于讨论一般义上的建模概念，不与特定软件设计工具的具体含义的概念表述相关联。下面给出一些设计项目的例子：

1) 同步建模与符号安全性验证(第 2 章和第 3 章)：其中一个项目就是关注同步硬件设计，如仲裁者和片上通信协议的设计与验证。该项目帮助读者理解子构件的层次组成。建模项目可使用行业标准硬件描述语言，如 VHDL 和 Verilog(参见 vhdl.org)等。作为完成该项目设计的备选方案，也可采用学术建模工具 NuSmv(参见 nusmv.fbk.eu)来设计系统，该工具采用基于 BDD 的符号状态空间搜索方法来实现系统建模和需求验证。

2) 异步建模和模型检查(第 4 章和第 5 章)：关于分布式协议的设计(例如，实现现代多处理器系统之间协调访问的全局共享内存的高速缓存一致性协议)，可采用建模工具 Spin(参见 spinroot.com)来对多处理器之间的异步通信进行建模。该工具允许用户使用时态逻辑方法对系统的安全性和活性需求进行详细说明，并采用模型检测方法对协议的正确性进行调试。

3) 动态系统的控制设计(第 6 章)：关于控制系统的课程中有一个传统的项目，该项目涉及的控制器模型包含了物理系统的建模。然后采用线性代数的工具实现组合系统的稳定性。动态系统建模这类的项目比较适合于教学活动。Mathworks 公司开发的软件工具 Matlab(参见 mathworks.com)通常用于动态系统建模，此类问题的典型例子是设计一个摆钟控制器的模型，该控制器的钟摆移动到最高点垂直位之后就会向反方向回摆。

4）时间系统的建模与验证(第 7 章)：建模工具 Uppaal(参见 uppaal.org)支持交互时间自动机建模和基于符号状态空间搜索的安全性属性的验证。医疗设备中的控制算法就是此类案例研究，该算法采用基于需求的设计与分析方法对心脏起搏器自动注入泵模型来进行设计与验证，也可以对心脏起搏器模型进行精化。

5）混成系统建模与模拟(第 9 章)：建模工具 Stateflow 和 Simulink(参见 mathworks.com)、Modelica(参见 modelica.org)和 Ptolemy(参见 ptolemy.org)支持混成系统的结构化建模。多机器人协调项目提供了丰富的问题域，可利用这些建模工具对信息物理融合系统进行设计与分析。该项目的分析目标是帮助学生理解如何利用数值模拟方法对不同设计变量进行折中。

补充阅读

对于要求高可信的嵌入式及信息物理融合系统设计的新科学案例，在过去的十多年中已开展了许多研究(参见[Lee00，SLMR05，KSLB03，HS06，SV07])。现在，这个分支学科又有了一个生机勃勃的学术研究社区，每年举行一次的学术会议“Embedded Systems Week”(参见 esweek.org)和“Cyber-Physical Systems Week”(参见 cpsweek.org)，展现信息物理融合系统的研究现状和发展趋势。

《Introduction to Embedded Systems》[LS11]是一本与我们选题和内容最为接近的教材，也是本书最有价值的参考书。相比之下，《Introduction to Embedded Systems》[LS11]的选题范围更为宽泛，例如，它还讨论了嵌入式应用的处理器体系结构，而本书则对分析与验证技术的开发进行了更加深入的讨论，并提供了相应的案例研究。

还有一些参考书与本书讲解的主题相关，可对深入学习相关内容提供帮助。参考书[Hal93]关注于同步模型，讨论了基于模型设计的理论基础。参考书[Mar03]重点介绍嵌入式系统设计方法，参考书[Pto14]重点介绍采用集成异构模型的建模方法来设计系统。在内容丰富的分布式系统参考资料中，参考书[Lyn96]和[CM88]介绍了范围广泛的分布式算法，强调了形式化建模、正确性需求和验证等内容。为了介绍形式化逻辑及其应用的软件验证方法，我们推荐参考书[HR04]和[BM07]。参考书[CGP00]和[BK08]着重介绍了自动化验证和模型检测方法。参考书[Lam02]阐述了反应式系统使用的规约和开发的逻辑方法。动态系统讲解的内容与线性系统控制器设计方法相关，有许多经典的参考书可以借鉴，包括[AM06]和[FPE02]。实时系统介绍的内容强调系统的可调度性，可参见[But97]和[Liu00]。最后，还有一些研究专著，如[Tab09]、[Pla10]和[LA14]，它们关注于混成系统的形式化建模、控制和验证方法。

第2章

Principles of Cyber-Physical Systems

同步模型

当我们给一个功能构件提供一个输入时，它就会产生输出，并且可以用数学方法把系统的这种行为依据输入与输出的关系描述为一种映射关系。相应地，反应式构件能够通过这种持续的输入与输出的映射关系来维持系统内部状态，以及与其他构件之间的交互。我们首先重点讨论反应式计算的离散和同步模型，这类系统中的所有构件都循环依次执行。在每次循环中，反应式构件读取输入，基于它的当前状态和输入，它计算输出，并更新自己的内部状态。

2.1 反应式构件

作为第一个示例，我们考虑图2-1所示的Delay构件。该构件有一个布尔值输入变量in，一个布尔值输出变量out，以及由一个布尔变量x表示的内部状态。为了描述构件的行为，我们首先需要描述状态变量的初始值。对于Delay构件而言，假设x的初始值为0。在每次循环中，该构件根据起始时刻状态变量x的值设置输出变量out，同时将该状态x作为当前循环的输入变量进行更新。因此，第一次循环的输出为0，在随后的每次循环中，其输出都等于上一次循环的输入。

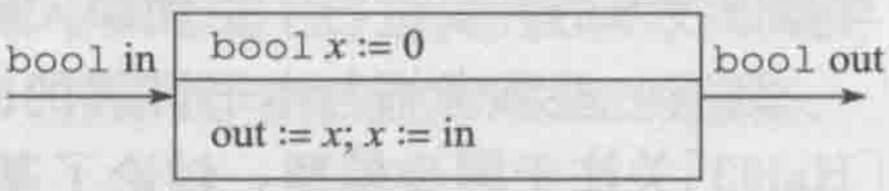


图2-1 反应式构件Delay

2.1.1 变量、值和表达式

为准确表达构件定义的各个方面，我们需要介绍一些数学概念，诸如，变量、变量表达式，以及变量的赋值。我们利用型参(Typed variable)描述构件。常用的型参类型有：

- nat——表示自然数集。
- int——表示整数集。
- real——表示实数集。
- bool——表示布尔值{0，1}的集合。
- 枚举类型——是包含有限数量符号常量的集合。例如，一个二值集合的枚举型参可以表示为{on，off}。

给定一个型参集合V，V上的一个赋值是对V中所有变量的类型一致的赋值。也就是说，V上的一个赋值是一个定义域为V的函数q，使得对任意变量$v \in V$，$q(v)$是一个属于类型v的值。我们用Q_V表示V上的所有值的集合。例如，若V包含两个变量，变量x为bool类型，变量y为nat类型，那么赋值q将给x赋予一个布尔值，给y赋予一个自然数。集合Q_V包含上述所有可能的赋值。

型参集合V上的型参表达式e是由V中的变量、常量，以及与这些变量相对应的这些类型上的原始运算构成的。对于数字类型，如nat、int和real等，我们将利用算术运算，如加法、乘法和比较运算(如=、≤)。为建立布尔表达式，我们利用如下的逻辑算子：

- 非(¬)：当e的值为0时，表达式$\neg e$的值为1。