HZ BOOKS 华章教育

Pearson

经 典 原 版 书 库

信息物理系统
应用与原理

[印度] 拉杰·拉杰库马尔（Raj Rajkumar）
卡内基-梅隆大学

[美] 迪奥尼西奥·德·尼茨（Dionisio de Niz）
卡内基-梅隆大学
马克·克莱恩（Mark Klein）
美国软件工程研究所（SEI）
著

（英文版）

SEI SERIES IN SOFTWARE ENGINEERING

Cyber-Physical Systems

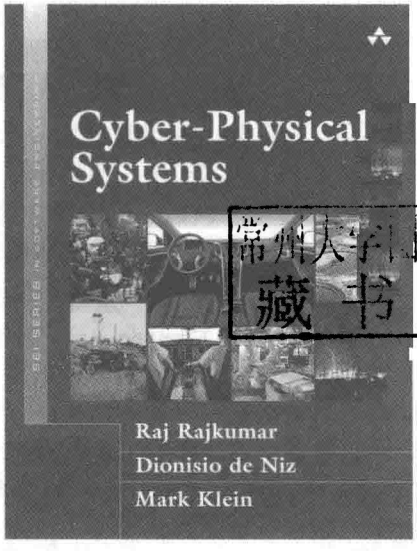
Raj Rajkumar
Dionisio de Niz
Mark Klein

机械工业出版社
China Machine Press

经 典 原 版 书 库

信息物理系统
应用与原理
（英文版）

Cyber-Physical Systems



常州大学图书馆
藏书章

[印度] 拉杰·拉杰库马尔（Raj Rajkumar）
卡内基-梅隆大学

[美] 迪奥尼西奥·德·尼茨（Dionisio de Niz）
卡内基-梅隆大学

马克·克莱恩（Mark Klein）
美国软件工程研究所（SEI）

著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

信息物理系统应用与原理（英文版）/（印）拉杰·拉杰库马尔（Raj Rajkumar）等著．—北京：机械工业出版社，2018.4
（经典原版书库）
书名原文：Cyber-Physical Systems

ISBN 978-7-111-59598-4

Ⅰ．信… Ⅱ．拉… Ⅲ．异构网络－高等学校－教材－英文 Ⅳ．TP393.02

中国版本图书馆 CIP 数据核字（2018）第 060139 号

本书版权登记号：图字 01-2017-0729

Authorized Reprint from the English language edition, entitled *Cyber-Physical Systems*, ISBN 9780321926968, Raj Rajkumar; Dionisio De Niz; Mark Klein, published by Pearson Education, Inc., Copyright © 2017 by Pearson Education, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

English language edition published by China Machine Press, Copyright © 2018.

本书英文影印版由 Pearson Education Inc. 授权机械工业出版社独家出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

此影印版仅限于中华人民共和国境内（不包括香港、澳门特别行政区及台湾地区）销售发行。

本书封面贴有 Pearson Education（培生教育出版集团）激光防伪标签，无标签者不得销售。

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：张梦玲 责任校对：殷 虹
印 刷：中国电影出版社印刷厂 版 次：2018 年 4 月第 1 版第 1 次印刷
开 本：186mm×240mm 1/16 印 张：24.25
书 号：ISBN 978-7-111-59598-4 定 价：89.00 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

版权所有·侵权必究
封底无防伪标均为盗版
本书法律顾问：北京大成律师事务所 韩光/邹晓东

出版者的话

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

前 言

美国国家科学基金会（National Science Foundation, NSF）将信息物理系统（Cyber-Physical System, CPS）定义为构建并依赖于计算算法与物理组件（即信息组件和物理组件）的无缝连接的工程系统。这种整合意味着，要理解 CPS 的行为，我们不仅要关注信息部分或物理部分，还要考虑两部分的相互协作。例如，当系统检测到撞车事故将要发生时就需要确定汽车安全气囊的行为。只保证充气指令是否被安全气囊执行是不够的，还需要验证这些指令的执行与物理过程是否是同步完成的。具体而言，20 毫秒之内执行可以确保司机撞上方向盘之前安全气囊完全充气。CPS 中信息、物理部分之间的无缝整合涉及多个方面。这个简单例子就涉及软件逻辑、软件执行时间和物理过程。

虽然充气气囊这个例子包含了 CPS 的重要部分，但它并未涉及 CPS 最具挑战的部分。充气气囊的信息组件和物理组件都十分简单，它们之间的交互可以简化到仅区分软件完成时间和事故中司机撞上方向盘的时间这种情况。但是，随着软件和物理过程复杂度的增加，它们之间整合的复杂度也将显著提高。在大型 CPS 中（如商用飞机），多个物理和信息组件的整合以及各部分之间的权衡就变得十分具有挑战性。例如，在波音 787 梦幻客机上添加额外锂电池就必须要先满足一系列限制条件。这不仅需要满足在不同操作模式下特定电池配置（在特定处理速度和电压下与软件进行交互）的功耗需求，还需要明确为维持所需电压系统应何时以及如何对电池充放电，同时也需要检测充放电配置以确保电池不会过热（在 787 航行经历中电池过热曾导致起火），并且这种检测要与系统散热部分的设计衔接。更重要的是，所有这些方面都需要经过联邦安全管理局（Federal Aviation Administration, FAA）严格标准的认证。

由于单一系统复杂度的增加，CPS 面临着更多的挑战。尤其是人们正在研究无人干预情况下的 CPS 间交互。这与互联网的开始十分类似。互联网开始时是两台电脑之间简单地连接。但当全世界的电脑无缝地连接起来，在网络上开发出大量的服务时，真正的革命出现了。这种连接不仅允许将大量的服务交付到世界各地，而且使收集和处理大量的信息（“大数据”）成为可能。我们可以利用大数据探索人群的趋势，当大数据与社交网络（如 Facebook 和 Twitter）相结合时，甚至可以探索人群的实时趋势。在 CPS 中，这场革命才刚刚开始。通过智能手机上的 GPS 应用收集的行驶信息，我们可以去选一条低拥堵线路。虽然这种技术仍然需要人为调节，但是在某种程度上这符合智能公路的发展方向。这方面的成果近期层出不穷，例如在多个涉及自动汽车的项目中，汽车不仅知道如何自动驾驶，并且可以和同一路线上的其他非自动汽车进行交互。

此为试读，需要完整PDF请访问：www.ertongbook.com

CPS 的出现

在 CPS 作为一个特定的学科领域出现之前，包含信息组件和物理组件的系统就已经存在。但这两个组件之间的交互十分简单，理论支撑基础也分散于计算机科学和物理科学之中。它们独立发展，没有交集。例如，在热弹力、空气动力学和机械应力学等学科中，验证性能的技术是独立于计算机技术（如逻辑时钟、模型检测、类型系统等）的进步而发展的。实际上，这些进步是从一些行为中抽象出来的，这些行为对某一学科领域很重要，但与其他学科领域相关性不大。例如，编程语言和逻辑验证模型的本质是只考虑指令的顺序，不受时间本身的影响。这种本质与车辆运动和房间温度控制这类物理变化过程中时间的重要性形成鲜明对比。

早期计算和物理科学之间交互的具体实现大多是成对的简单交互模型。例如实时调度理论和控制理论。调度理论加入了计算元素的时间，这样可以验证与物理过程交互的响应时间，从而确保整个过程不超过计算部分的预期并且可以进行修正。另一方面，控制理论将控制算法和物理过程结合起来，并且分析算法是否可以使系统保持在期望区域内。然而控制理论采用连续时间模型，在这一模型下计算瞬间发生，它使用附加延迟来考虑包含调度时间在内的计算时间，这使确定计算周期和提供调度接口成为可能。

随着领域之间交互复杂度的增加，人们研究了新的技术去模拟这种交互。例如，混合系统是一种状态机，在这个状态机中，状态用于模拟计算和物理状态，转换用于模拟计算动作和物理变化。虽然这种技术提高了描述复杂交互的能力，但分析往往是比较棘手的。通常情况下，模型复杂度阻碍了系统实际维度的分析。此外，随着相关学科数量的增长（如泛函、热力学、空气动力学、机械、容错），为了确保任意学科的假设和它的模型不因其他学科的模型而失效，我们需要分析它们之间的交互。例如，为了防止过热而降低处理器速度的动态散热管理（Dynamic Thermal Management, DTM）系统，会因实时调度算法设定的处理器速度而失效。

CPS 的发展动力

在 CPS 蓬勃发展的今天，我们面临的挑战是能否深入理解 CPS 的行为和发展技术，从而评估 CPS 的可靠性、保密性和安全性。这实际上是 CPS 科学界的核心动力。因此，CPS 是由两个相辅相成的因素驱动的：应用和理论基础。

应用

CPS 的应用可以让研究者与从业者相互协作，以便更好地理解问题和挑战，提供能经受住实践检验的方案。如医疗设备，CPS 研究人员与医生合作了解造成医疗设备失误的来

源与挑战。人体如何处理不同药物，如何实施安全措施以避免药物过量注射，如何确保护士输入正确信息，这些都需要一定的假设，错误假设会引起输液泵的错误。此外，现今的医疗设备仅作为独立的设备，不允许互相连接。因此，医疗从业者需要在使用过程中协调这些设备，确保设备间的相互作用不引发安全性问题。例如，手术过程中需要胸部 X 射线机，就必须确保呼吸机被禁用；另一方面，一旦用完 X 射线机，呼吸机需要在一个安全的时间间隔内重新启动，这可以防止患者窒息。尽管这种不变性可以在软件中实现，但目前的认证技术和策略会阻止这种整合的出现。研究人员在此领域的工作就是开发技术以使这种相互作用的认证成为可能。这个问题在第 1 章中会详尽地讨论。

由于电网作为国家基础设施的战略重要性，电网是 CPS 的另一个重要应用领域。由于电能消费者和生产者各自独立，电能生产和消费具有不协调的特性，这是此领域的主要挑战。尤其是，每个家庭按一下电源开关就可以改变电能消费，这些按开关的动作会对电网产生聚合效应，因此电网需要平衡电能供应。类似地，风能、太阳能等可再生能源的电能生产不稳定、不可预知，这使平衡电能的供需成为一大挑战。这些元素之间的相互影响本质上是信息和物理之间的相互影响。一方面，电力供应者之间存在以计算机为中介的协调，另一方面，供应者与消费者之间的相互影响主要存在于电能的物理消耗过程中。目前一系列的技术已经应用于电网的控制与发展，这可以保护电网基础设施免受损坏，同时提升可靠性。然而，新一轮的挑战需要信息与物理元素结合起来，支持高效的市场、可再生能源、更便宜的能源价格。第 2 章讨论了电网领域的挑战和进展。

最有趣的、有技术创新的 CPS 应用领域之一也许就是传感器网络。传感器的发展和部署面临空间、时间、能量、可靠性方面的挑战，这是这一领域独具的。第 3 章讨论了传感器网络面临的挑战和这一领域的主要技术创新。

虽然一些应用领域有自己的趋势，新兴的应用领域也可能很快浮出水面。但是本书只讨论被 CPS 学科界定为最有影响力的领域。

基础理论

CPS 的理论发展集中在多学科领域间的相互作用所带来的挑战。有关实时调度的一些趋势很值得一提。第一个趋势是为适应过载执行而出现的新调度模型。这些模型将多个执行预算与基于关键性的任务分类结合起来，确保在正常操作期间所有任务都可以满足时限要求。当过载发生时，高关键性的任务从低关键性的任务中窃取处理器周期来满足其时限要求。第二个趋势来自于周期性上的变化。间歇任务模型（rhythmic task model）允许任务的周期随着物理任务的变化频率而持续变化。例如，在这种情况下，某个任务由汽车发动机的曲轴角位置触发，新的调度分析技术就需要验证这种系统的时序性。在第 9 章中，我们将讨论实时调度的基础和创新。

模型检验和控制综合理论之间的交叉创新是待研究的发展方向。在这个方向上，混合状态机模型用于描述物理对象的行为和计算算法的要求。该模型用于自动合成控制器算法来增强所需的规范。第 4 章将讨论这个案例。学术界已经开发了许多新技术来分析控制算法中调度规则的时序效应。这些问题将在第 5 章中讨论。

学术界已经探索的另一个交互领域是模型检测和调度之间的关系。有团队开发了一种称为 REK 的新模型检查器，它将任务交错的约束加到单调速率调度器和周期性任务模型中，减少了验证工作。这些新交互将在第 6 章中讨论。

安全性是另一个受物理过程显著影响的领域。特别是软件和物理过程之间的交互给潜在的攻击者提供了新的攻击机会，这使 CPS 安全与纯软件安全之间有很大的差异。于是产生了这种由于攻击导致的差异，即传感器的错误数据很难与物理过程中真正的数据相区分。这些防止中间人攻击的创新点与其他重要技术将在第 7 章中介绍。

在分布式实时系统中，实现分布式代理之间的同步通信新技术是非常有用的，这能够减少对功能正确性进行形式证明所需的工作。第 8 章将详细讨论此问题。

CPS 分析技术依赖于模型，而模型的形式语义是一个必须解决的关键挑战。第 10 章介绍了模型集成语言中模型形式语义的最新发展。

本书讨论了大量的理论进展以及每个领域的挑战。一些进展源于应用领域的具体挑战，另一些进展带来了新的发展机会。

读者对象

本书面向实践人员和研究人员。对于实践人员，本书描述了当前受益于 CPS 的应用领域，以及有利于 CPS 发展的技术。对于研究者，本书提供了一份应用领域的调查报告，并突出了当前的成就和有待解决的挑战，以及当前学科的进步和挑战。

本书分为两部分。第一部分介绍了当前 CPS 的 3 个典型领域，这些应用领域推动了 CPS 的技术革命。第二部分介绍了 CPS 发展中使用的多学科理论基础。

目 录

第一部分 CPS 应用领域

此为试读，需要完整PDF请访问：www.ertongbook.com

Contents

Part I

Cyber-Physical System Application Domains

此为试读,需要完整PDF请访问: www.ertongbook.com