万物相联万物生

专题组稿人：刘云浩
清华大学

关键词：物联网　嵌入式系统

我第一次看到Internet of Things（IoT）这个词的时候，根本没想到后来会使用物联网这样一个精致的词来对应它。2007年在一个并非学术圈的人面前说起物联网的时候，我直接被作为口齿不清、当作是互联网的口误而忽略了。2010年收到的关于作物联网报告的邀请超过我此前收到的所有邀请的总和。今年春节前我去一个三星级酒店，在大堂的咖啡厅听到一桌几个中年人兴致勃勃地交流投资方向，忽然其中一位站起来大声说：“物联网谁不知道啊，既无新意也无卖点！”

网络嵌入式系统和物联网，我们真的透彻理解了么？物联网概念中强调的更广泛而全面的互联互通，更透彻的感知和更深入的智能，到底是什么？或者说，如何深刻理解这三个“更”字呢？

首先，是不是没有物联网就没有互联互通？显然不是。100多年前发明的电话早就把人们的通信和联系定义在世界范围内了，20世纪90年代移动电话的普及更是把人们和远在天边的朋友随时随地的联系起来进行交流。1995年之后出现的互联网革命则进一步丰富了交流的手段：从单纯的语音已发展到多媒体数据。而物联网要带来的是更广泛和更全面地互联互通。怎么广泛而全面？

其一，是互联互通的对象从人延展到物体，不仅人与人要交流，物和物也要互通。从技术角度来说，这意味着联网终端的多样性大大增加了。原先的网络设备，通常都是智能化程度较高的如移动电话、PDA、iPad，甚至就是一台计算机；而物联网中物体所附带的网络设备（或设备化的普通物理对象），其智能往往比较低，比如一个传感网节点，其计算能力和存储量远远不能和前述设备相比。未来更多的上网设备，其智能可能仅仅体现在具备一个能被识别的标记（ID）。万不可小看这个“被识别”的能力！在物联网时代，能主动认知和控制自己之外的对象的，可以称作是具有主动智能，而有能力使得自身被智能主体所认知和控制的，可以称作是拥有被动智能。被动智能也是智能！其二，是互联互通方式，也就是网络通信模式的扩展，亦即更深层次的广泛与全面的物联网的互联互通，有可能仅仅是一天当中只有一分钟甚至一秒钟接入了网络，比如容迟网（DTN）的模式，也可能只是逻辑上被连进了网上，比如一个节点A和另一个移动节点B每小时都有一次固定数据交换，而A自身从未直接上网，但是由于移动节点B每天都移动到一个基站把它所有获取来的数据上传，这种情况下A和B都算物联网上的节点。这些都体现了物联网通信模式的广泛性。

在物联网之前，互联网主要以有线方式提供服务，而眼下处于初级阶段的物联网虽然融合了无线方式，但通信模式主要以Client/Server为主，也就是节点之间的数据交换通过基站完成，就像我们所熟悉的移动通信网络、射频识别标识（RFID）系统等。确切地说这还不能算严格的物物相连，而是物站相连：物体与基站之间通过主从式的、单跳的方式进行数据通信。真正自组织网络（Ad Hoc Network），也就是以对等网（P2P）的模式实现物与物的多跳连接，必然是物联网下一阶段的主要特点。也许物联网80%的功能用客户端/服务器（Client/Server）方式就可以完成，但另外的20%却因画龙点睛而不可或缺。物联网互联互通广泛而全面的另一个

方面，体现在联网节点数量上。当今上网的用户有多少？10亿人肯定是有的。但如果没有物联网，即使所有地球人都上网，平均每人几台上网设备，百亿或者千亿量级也就是极限了。但物联网的时代，每一个物件都可以上网，每一个物件都可控制，这个数量肯定不是千亿甚至万亿可以限制住的。这样大的数量激增，对于网络技术所带来的冲击肯定是天翻地覆的，但这还远远比不上对人们心灵上的冲击：试想，有一天你身边所有的物件都拥有或多或少的智能，那岂是仅仅对隐私泄漏的担忧？

正是有了更广泛更全面的互联互通，物联网的感知才更透彻更具洞察力。我们已经知道传感器是一百多年前就有的设备，但通信功能却是近十来年才附加的。通信功能对于传感器产生的影响，几乎可以类比于文字和语言对于人类！当人类可以使用语言交流并使用文字记载的时候，文明时代就来临了。传感器也是这样，单独工作的传感器，完全依仗人们预先布设的工作，既没有协同，也做不到自适应。我们来重温一下大家所熟悉的瞎子摸象的故事，之所以每个人摸完了大象给出了截然不同的描述，就是因为他们没有（用通信的方式）相互协同。如果每个人在摸完了大象的一部分之后，和其他伙伴交换自己的位置以及观测角度，显然可以更透彻地完成对大象的感知。

再举一个小例子，比如需要知道今天的室外温度，你拿着一个温度计（你也可以称作温度传感器）出门了，找到一个合适的地方放上温度计，过了10分钟给出一个读数。这个读数在多大的程度上可以代表这个地区的温度呢？先抛开气象的专业测量与定义不去深究，至少大家都明白这个温度计放在树阴下和放在日光下很可能测出不同的结果来。也就是说在测量过程中需要人的辅助才能有效定义这个测量的真实含义。假如不是人拿着而是随机的摆放这个温度传感器呢？显然如果你不知道它摆在哪里了，这个节点送回来的数据所代表的意义就大打折扣了。这还是我们假设设备本身并没有出现工作异常的情况。为了减小误差我们可以做这样一件事，就是在一个很小的物理范围内放很多节点，比如10个，然后通过取平均值或者干脆去除异常点的方法来校正测量结果，更复杂一些的是近来学术界很火的不确定数据处理（uncertain data processing），如果上升到理论高度就是考量数据质量（data quality）问题。但是这是测量一个日常所熟悉的环境，也就是说我们实际已经使用了先验知识。假如测量的是一个完全未知的环境，当随机布设了10个传感器的时候，这些传感器尽管相距非常近，但恰好有8个在水里，2个在水外，那么无论上述哪种方法都不可能获得我们真正想要测量的结果。

有了更透彻的感知，自然就有了更综合更深入的智能。最早提出的传感网经典应用当中就有将温度传感器应用于森林防火。如何从传感器连续不断的枯燥乏味的温度测量值中发现潜在的火灾危险呢？我们当然可以定义温度大于某个阈值是发生火灾的标志，这可以算是最简单的事件检测算法。进一步，我们可以利用多个传感器协同感知，避免由于单个传感器故障造成的误警或漏警，提高火灾检测的可靠性，这是“人多力量大”的智能。更进一步，我们可以利用湿度、风速、风向等多维度感知数据，判断森林火灾发生的条件，提供森林火灾预警信息供相关部门参考，将灾害消除在萌芽状态，这是“防患于未然”的智能。如果能从长期的温度数据中挖掘模式，从看似不相关的气象事件中挖掘联系，探索“厄尔尼诺现象”对全球气候带来的影响，这是“审堂下之阴而知日月之行”的智能。从温度感知数据上升到火灾事件，再从短时间离散的事件上升到长期大规模的气候现象，体现了智能的不断深入。这个例子还可以引申到日常生活中。你明天上午从北京去天津开会，预计10点左右从北京出发， 12点左右抵达。上网查阅之后知道可以坐火车，坐长途汽车，也可以自己开车，相比之下似乎开车最便捷，随后你把路线也查了，GPS也带上了。但有了物联网，它可能建议你乘火车去，为什么呢？你身上的体域物联网（body area network）检测到你最近工作压力大，心肺功能不大稳定需要保护，而道路物联网发现明天你去的地方将路过一个修路段，为了绕行你将不得不穿过一个海鲜市场，

拥堵的人群加上你对海鲜的过敏可能引发身体某项功能的紊乱，因此建议你还是乘火车过去。

物联网真正的成功，不靠各种论坛、讲座和宣传，至少不仅仅是，而是实际的系统。但我们还是要边干边想、边讨论边交流。借助中国计算机学会（CCF）和ACM联合提供的学科前沿讲习班（ADL）这个平台，图灵奖获得者斯法克斯（Joseph Sifakis）教授和我一起，请了10位这个领域非常活跃的国际国内的著名学者，准备在无锡开一个研讨会。本专题我们邀请国外的5位讲者根据他们要讲的内容写了4个短文，算是会前热身吧。看了Sifakis教授的文章，我们得知平均一天当中为每个人服务的嵌入式芯片有230块之多。当年Mark Weiser提出普适计算时，曾用过Invisible Computing（不可见计算）这个词。曾几何时，他预见的场景已出现在我们身边。他回顾了计算机科学发展的历史以及嵌入式系统迅猛发展的现状，提出了物联网必然成为计算机科学发展史上一座新里程碑的观点，也因此将计算机科学中“系统”（尤其是嵌入式系统）层面的研究推向了一个新的高度。通过深入分析嵌入式系统设计发展的趋势，详细刻画并描述了目前严谨系统设计给研究人员提出的三个严峻挑战，对计算机科学的发展从作为科学本身、包含的研究以及教学等三个方面一一进行了展望。

美国工程院院士、加州大学伯克莱分校的阿尔博托(Alberto Sangiovanni Vincentelli)教授更是用了Frankstein这个世界上第一篇科幻小说的人物来展开讨论。他告诉我们信息物理系统（CPS，就是美国人对物联网概念的理解）将在不远的未来支持不可想象的社会大规模应用，因此在系统设计上将面临一系列严峻挑战。与Sifakis教授相呼应的，他指出最有前景的一种解决方法是使用结构化与形式化的设计方法，并讨论了“契约式设计（contract-based design）”，为满足系统工业的迫切需求指出了一个方向。

葡萄牙波尔图大学路易斯阿尔梅达教授认为物联网基础设施的建设需要全新的通信抽象模型，在保证开放性和实时性的同时，具有高度的自适应性，这样才能够更有效地利用网络带宽。更重要的是，阿尔梅达教授还提出了基于资源预留模式的改进方法，为未来信息物理系统的构建指出了一个合理的发展方向。瑞士联邦理工大学计算机工程系洛萨·蒂勒（Lothar Thiele）教授和詹·布泰尔（Jan Beutel）教授协作完成的文章简要介绍了网络嵌入式系统发展的背景和基础，并从能量受限等角度详细分析了网络嵌入式系统的发展瓶颈。通过对FlockLab实验平台架构进行详尽的解析，从无线传感器网络系统设计和跨学科合作应用两个方面对极端环境下物理环境监测等研究进行了探讨。

我们在国内也请了本领域的几位名人。首先我的老师倪明选教授将要来会上给我们介绍他最近在医疗物联网上的进展，我们还邀请千人计划归国工作的胡斌教授和基金委杰青基金获得者陈贵海教授，分别在生物计算和数据中心与物联网的联合运用上给我们带来惊喜。基金委信息学部的肖人毅博士也要来介绍一下这几年基金委在物联网和CPS方向上支持的项目进展情况。由于篇幅有限，这次的专辑就没有给他们留出空间，我们期待他们的演讲吧。

在史元春老师的反复催促下，今天终于能够把几个文章整理完毕了。忽然想起当年把作业放在一旁，迫不及待地打开千辛万苦借来的《机器猫》，一边深深地鄙视一事无成的野比一边无限憧憬着他形影不离的机器猫。小叮当神奇口袋里的宝贝是那么的不可思议。英国作家布莱克说：“今天在实践中证明的东西，就是过去在想象中存在的东西。”希望我们的每一次探索，都能为我们曾经的想象加上一双可以踏在陆地上的脚。

万物相联，万物生。1969年，因特网尝试搭建。1999年，“IOT”的概念提出。2012年，因特网43年，物联网13年，都处在未知大于已知、未来多于过去的时刻。■

刘云浩

CCF国际合作部主任。ACM China副主席。清华大学教授。主要研究方向为传感器网络等。yunhao@greenorbs.com

计算机科学的愿景——系统发展观

作者：约瑟夫·斯法科思（Joseph Sifakis）
译者：GreenOrbs绿野千传项目组

关键词：计算机系统

计算机科学的演变

计算机科学是一门年轻的学科，它的出现可追溯至1936年，图灵（A.M. Turing）和哥德尔（K. Gödel）二位科学家的初期工作奠定了学科发展的基础。在过去的70年里，计算机科学的研究领域和关注重心经过了多次变迁。最早期的计算机主要应用于军事防卫领域中的数值计算。20世纪70年代，大型机的出现将计算机引入到了商用领域。与此同时，大规模集成电路的发展也促进了计算能力的指数级增长（摩尔定律）。80年代，信息科学和电子通讯技术的融合开辟了新的天地，网络服务、互联网以及信息化社会应运而生。到了90年代，一场对整个学科前景影响举足轻重的变革悄然展开，那就是嵌入式系统的广泛应用。时至今日，全球生产的芯片中有超过95%的部分为嵌入式应用。这些集成了必需的软件和硬件的电子元件专门针对发挥着关键作用的特定功能而设计。它们藏身于各种各样的仪器设备之中：如移动电话、照相机、家用电器、汽车、飞机、火车、医疗设备等。据统计，在2008年，平均每人每天用到将近230块嵌入式芯片，其中家用电器80块，工作40块，汽车70块，移动设备40块。

可以预见，在不远的将来，作为嵌入式技术和互联网融合的结果，“物联网”将在计算机科学发展史上树立起一座新的里程碑。数以亿计的嵌入式系统提供了数以亿计的零散服务，而物联网旨在使用互联技术来整合这些服务。为了达成这一目标，当前互联网的底层架构必须通过升级等手段，使之变得更安全，更可靠，反应更加敏锐。举例来讲，一个交换媒体文件的简单服务，将来可能要包含实时监控的功能。“系统”变得无处不在：万物的状态皆可感知、测量、监控；人与物可以以一种全新的方式交流互动；智能系统使得各种事件的预测更加容易，各种资源的分配更加优化。

现在可能很难想象，计算机科学在20年后将有怎样的发展。相较于其他学科，计算机科学的发展更有赖于两股力量的共同驱动：实际应用和成指数级增长的技术进步。而伴随着研究重心由“算法”和“程序”向“系统”层面的转移，计算机科学涵盖的范围亦将不断扩大。

从程序到系统

我认为在计算机科学的发展史上有两大里程碑：计算机的发明以及计算理论的发展。前者完成了计算设备从机械化到电子化的转变，使计算变得更加快速和可靠；而后者发展了一系列的便于人们研究算法、程序以及性质的计算模型。这无疑开启了机械化计算的道路，处理的中心问题是“函数是否以及何时能通过计算模型得到计算”。更为重要

的是，这些模型忽略了物理时间和物理资源，将计算看作一系列基本操作构成的有限长序列，而是复杂度理论也成为基于时间与内存的抽象表达。程序与算法本质上是“关联”的抽象表达，而这种“关联”与物理资源是完全独立的。在这个意义上，程序与算法的行为有着共同的特点：有终结、确定和与运行平台无关。

与程序和算法不同，系统会对外界进行反馈，换言之，系统总是不断地与外部环境进行交互。系统的输入是触发状态改变的激励，而计算输出结果的过程又可能改变环境的状态。系统的行为可以抽象成历史输入和历史输出的“关联”。一般而言，系统没有终结，也并不确定。此外，系统的行为是与平台相关的，其正确性取决于运行平台的动态特性（比如运行次数）。从这点上说，计算理论的本质决定了它在对系统的研究上派不上太大的用场。即便我们充分掌握了某个程序和某个硬件平台的全部特性，也未必合适的理论来预测该程序在这个平台上运行时的行为。因此，计算的理论亟需进一步扩展，从而适应研究重心从程序到系统的转变。我们必须把物理资源和系统与环境间的相互作用考虑到计算模型中来，进而不断丰富和完善计算模型。

系统设计趋势

与传统的计算机系统，例如台式计算机和服务器等不同，嵌入式系统必须同时满足下列几项技术需求：

反应性（reactivity） 响应延迟必须是已知并且有限的。这一点对于实时应用程序和有效的服务质量控制都是必不可少的；

自主性（autonomy） 在无人介入的情况下，提供连续的服务。尤其是对于移动设备来说，系统应当不需要手动重启，并且具备最优的能耗管理策略；

可靠性（dependability） 具有抵抗攻击、硬件故障、软件运行错误等威胁的能力；

扩展性（scalability） 性能提升与资源消耗的匹配性。

由于嵌入式系统往往集成在大规模商业产品中，使得嵌入式系统必须有最优的性价比。可是，在系统的设计中，实现最佳的经济效益比不计成本地实现高品质往往要困难得多。总之，嵌入式技术对开发系统的能力提出了新的挑战：必须兼顾功能性和质量，同时要把成本控制在可接受的范围内。

我们付出了很高的代价，终于得以掌握，但仍然不能有效整合以下两类系统：一类是低复杂度，但确保极高安全性与可靠性（safety and security critical）的系统，例如航空控制器和智能卡；第二类是复杂度非常高但是仅保证尽量好的服务质量（best-effort）的系统，例如电信系统和互联网上的万维网（web）应用等。前者强调可靠性，而后者则更倾向在保证一定服务质量的同时，寻求最优的资源利用率。因此，对于未来的系统，我们亟需实现下列目标的技术：

核心关键系统成本的有效控制 在运输、医疗和能源等应用领域中，嵌入式技术通过提供全新的服务，在极大改善人们生活质量的同时，也进行有效的资源管理。例如，将汽车的油门和刹车从传统的钢缆机械控制改为用电子信号控制，可以降低生产和操作的成本，用“主动安全”取代“被动安全”。

异构“系统级系统”（systems-of-systems）的可靠集成 通过开发整体化的服务系统，将分布于不同地理位置、拥有不同技术特性、使用不同通信媒介的系统整合起来，为此我们必须掌控关键特性和非关键特性间的交互，并确保系统的容错性。举例而言，当非关键服务发生错误的时候，如何避免这种错误祸及关键性服务的正常运行？因为缺乏指导性理论，这是当前一个开放性的难题。在“系统级系统”设想之中，通过连接日常物件来提供整体化服务的物联网最具代表性。我们可以举出很多例子，一个经典实例就是提供高效可靠能源管理的“智能电网”；再比如“智能运输系统”，其宗旨是增进交通安全，同时减少车辆损耗、运输时间和燃料消耗。

想在上述几个方向上取得长足进展，必须在系统设计的基础性研究方面花大力气。虽然在过去几十年中，在理论、方法和工具上都取得了一定的进步，结果却是喜忧参半。一方面，大规模集成电路和电子通信技术的发展带来了多核处理器和传感网络，给我们提供了越来越多的可能性；另一方面，系统设计与集成的发展不仅没有与时俱进，差距反而越来越大。实际上，今日的计算机科学研究已经远远滞后于日益增长的需求。除了少量的工作[1, 2, 12, 13]之外，在广大计算机科学研究人员的研究日程和计划上，系统设计并未得到足够的重视。

三大挑战

追求严谨的系统设计（rigorous system design）也同时给我们提出了三大挑战：（1）物理世界与计算世界联姻；（2）基于组件的设计；（3）自适应性。

物理世界与计算世界联姻

我们需要一整套理论和模型来涵盖连续和离散的动态性，这样就可以从整体上预测系统和外界物理环境的交互行为[1~2]。通常，在应用软件的开发和实现过程中往往受到以下两点限制：

硬件运行平台的物理资源限制 用户需要在充分了解平台的基础上才能更好的优化使用系统资源。这就需要掌握好上层软件和底层硬件的交互，特别是掌握硬件电路的实时动态性对软件设计带来的影响。

系统的物理环境限制 这通常和用户的使用习惯和系统的实时性有关，例如任务的截止时间和实时的外界扰动等。

我们仍然缺少理论、方法和工具来应对这些由于物理世界和计算世界分离所造成的问题，因此，需要重新审视和修订计算模型，把电子工程和控制论模型整合进来，并进一步把计算模型和物理系统工程中使用的分析模型结合起来。困难在于，物理分析模型中使用大量的微分方程和线性近似来描述电子机械系统的行为，系统中组件之间的交互是通过数据流网络来完成的，不断地将并发的输入数据流转换成输出数据流；与此不同的是，计算模型往往是过程化和顺序化的，组件之间的交互通过控制流完成（比如方法调用）。我们并没有切实可行的理论来整合这两种模型。虽然存在一些理论，如混合动力系统论[3]，已经在语义层（转换系统层面）建立了两种模型的关联，但语义转换的过程破坏了两种模型原有的结构。因此，系统工程师仍旧需要诸如能将Maltab/Simulink（http://www.mathworks.com/products/simulink/）和过程化的编程语言结合的，将不同系统相结合的技术。

基于组件的设计

与其他工学学科一样，计算机科学也需要理论、方法和工具来降低成本，高效率地将异构组件整合成复杂的系统，从而保证系统的生产能力和正确性。

系统设计师往往需要从不同的视角入手，处理结构迥异的组件，进而反映系统的各个方面。目前通常使用一些语义无关的形式方法，例如软件编程、硬件描述和模拟。这实际上破坏了设计流程的连续性和统一性，并使得系统的开发和验证评估完全脱节。

我认为，设计流程中使用的系统描述应该基于一个统一的语义模型。这个模型需要保持总体的一致性，保证每一步的描述都与前一步的关键性质相吻合。语义模型应当具有足够的表现能力来包容组件的异构性。总体而言，目前有三种异构性的分类[1]：

计算异构性 语义模型应该同时包含同步和异步的计算，特别是能够对软硬件混合的系统进行建模；

交互异构性 语义模型应该能够自然而且直接地描述多种执行调度机制，包括信号量、会合、广播和方法调用等；

抽象异构性 语义模型应该支持从应用软件到其实现方法不同层次的抽象。

现有的整合理论框架都是基于单一的运算：如自动机的乘积（product of automata）、函数调用等。这些框架可能由于表达能力不够丰富从而导致设计的复杂化。例如,我们往往需要添加额外的组件来协调某个给定组件集合中组件之间的交互[4]。又比如，通过一些强同步方法整合组件时，广播模型往往需要在若干方法中选择同步度最高的。因此，需要一些提供组合操作的框架，使得我们能自然而且直接的描述协议、调度和总线等协调机制，并且这些框架应该包括一个统一的组合范式，通过明确的、完备的、有组织的概念来描述和分析组件之间的协调关系。另外，这些框架还应该具有可行的方法来确保构造的正确性，从而避免单一验证的局限性。这些方法主要利用了下述两个原理[5]：

复合性原理（compositionality） 是指复合组件的属性能够根据子组件的属性来推测。例如，如果各个子组件都是防死锁的，那么（在某种条件下）它们组成的整个组件也应该是防死锁的。需要强调的是，复合性原理应该考虑组件复合而带来的新属性。比如，若子组件的操作都是符合原子性的，则复合之后的组件应该可以为资源共享提供互斥访问的机制。一种特殊而且有效的复合性是，在组件之间能够达成一致的行为等价性[6]。在这种情况下，在行为等价的组件之间进行替换，仍旧能够得到一个等价的系统模型。但如今，我们仍然缺少复合性理论来探究组件的过程属性和组成系统以后可能出现的新属性。

组合性原理（composability） 是指当各个组件复合时，各自重要的属性能够被完整地保留。比如有两个组件，它们由同样的组件集复合而成，其中一个通过互斥访问机制来共享某个资源，而另一个通过调度器来优化对该共享资源的访问。在这二者组合得到的复合体中，互斥访问机制和调度器之间会不会产生矛盾呢？系统工程师每天都在被类似的问题困扰。虽然针对某些具体问题，他们可以利用现有的解决方案，但仍然需要能够灵活地整合不同解决方案且不丢失重要特性的一些方法。电信系统的特征交互、网页服务的相互干扰、面向方面编程中的干扰都是系统组合性缺失的佐证。

自适应性

与不确定的环境交互时，系统必须提供可以满足既定要求的服务。系统的不确定性可以通过系统在正常和极端情况下的行为差异来刻画。不可确知的物理环境加剧了系统的不确定性。此外，分层模型、缓存、预测执行、工艺缺陷和老化带来的平台差异性均会导致运行时间的差异。

这种不确定性直接影响了分析技术的可预测性。对于某一个属性，可预测性是指我们能以何种正确程度来对其进行定性或定量的预测。由于不确定性的存在，系统模型一般用来表示实际系统行为的可靠抽象,但即使如此，还是可能包含附加的难以实施的执行序列。再者，在一个给定的系统模型中，由于不是所有的重要属性都是可计算的，也导致了准确的分析技术无法实现。例如，一条指令的执行时间依赖于数据存储的位置(高速缓存或主存)以及数据的大小[7]，因而同一条指令的最好情况执行时间（BCET）和最坏情况执行时间（WCET）可能相差100倍。遗憾的是，这两种时间不可能被完全正确地计算出来，时间分析工具又只能提供各自的上界和下界，使得依赖于分析工具的近似计算的表现可能会很糟糕。

不确定性和可预测性的缺失对于系统设计方法有着重要的影响并且会增加开发成本。当前，主要存在两种不同的设计范式。

关键工程范式 是基于对所有潜在危险形势的最坏情况分析。设计者们通过静态分析，预留了安全操作需要的所有资源（内存、时间），通常得到的是一个资源过度使用的系统。系统占用的物理资源可能比实际需要的大几个数量级，经常导致很高的生产成本和能量损耗。例如，实时系统中的任务反应时间必须有一个确定的上界和一个通过近似计算最坏情况执行时间得到的下界。这会导致严格实时系统硬件平台的资源被浪费掉。关键工程范式的另一个原则是使用大量冗余来提高可靠性。但冗余技术（例如TMR）也会导致资源过度使用。如果我

们用智能的轻型监测和错误恢复技术取而代之，则会带来很多好处。

最佳工程范式 用于复杂的非关键系统中。它基于的是平均情况分析和动态的资源管理。设计者使用服务质量管理技术来优化速度、内存、带宽和能量。通常各类服务正常运行所需要的物理资源看起来已经分配好，服务质量也是可以保证的，但在极端情况下（比如服务请求被阻止），系统服务质量就可能下降甚至根本提供不了服务。

通常，通过强调每个系统分类的关键属性，进而保持关键工程范式与最佳工程范式的分离是我们克服系统的不可预测性的一种手段。但是，大多数应用还是结合了这两种范式。正如同过去十年当中汽车制造业所经历的那些磨难一样，两种范式的结合带来了许多难以解决的问题。

有两种预期的途径可以解决当前技术的局限性：

途径之一是通过确定性来提高可预测性。其核心思想是简化硬件构架或者强制产生一些时间确定并可被观察到的行为[8]（如使用时间触发构架[9]），进而减少固有的以及由于预估而带来的不确定性。但是，这将带来严重的性能下降并要求在应用程序编写方面有重大改变[14]，因此我并不认为这是一个切实可行的方法。

途径之二是通过自适应协调关键和最佳工程范式组件间可预测的共享资源，来满足系统的关键性质，从而消除关键和最佳工程范式之间的鸿沟。主要思想是使用自适应控制器进行动态资源管理，为关键性质分配更高的优先级使其得到保障，而剩下的资源可以被最佳工程范式组件使用，这就避免了不必要的资源保留并且不需要非常精准的工具来分析最坏情况。

自适应控制器监视着系统状态并且控制着系统行为来满足一些既定的要求。这些要求往往是一个目标集合，如对截止时间等的严格约束和对资源最优利用的约束等。它将学习函数、目标管理函数和计划函数以层次化和结构化的形式整合在一起。根据系统状态，目标管理函数把一个已满足资源要求的目标传递给计划函数，后者计算出一个可执行的计划并以此来驱动系统。学习函数则对目标管理函数内的约束条件参数做出良好的估计，如执行时间的最坏情况和吞吐量均值等。

对自适应控制器的研究起源于控制论的研究[10]。研究人员发现在计算系统中使用自适应技术的应用日益增多，如多媒体系统中的性能控制、网络中的吞吐量控制和分布式系统中的自我维护和恢复等。这使得针对自适应控制器的研究浮出水面。

自适应系统设计并非完美无暇，其中一个重要的问题就是如何减少由监测和控制带来的额外开销。所以，为了有效的管理资源，我们需要将控制权交给应用程序的执行平台。

自适应性系统设计对未来智能系统的愿景完全不同于以往的人工智能。后者认为人类智慧可以逐渐被极为精准地描述，从而最终被机器来运行。而自适应性系统设计是使用基于控制的方法来处理不确定性，进而逐步实现系统的正确性。

计算机科学展望

作为科学本身

计算机科学具有自身独特的概念和范式，它主要用来处理关于信息的表达、转化和传播等问题。以此而论，它是研究从计算模型到软件和计算装置设计等与计算息息相关的各个方面的一门科学。

信息作为一种区别于物质和能量的客观存在，它可以被存储、转化、传播和使用。虽然信息是无形的，但可以通过语言中的语法、语义等要素来进行表达。它与物理“信息”的不同之处在于，后者存在于物理系统中，在信息论和物理学科中采用熵进行描述。诚然，与任何科学一样，计算机科学需要通过数学来进行理论验证，但我们不应该把它理解为数学的一个分支。重要的是，它繁衍了能够对计算特性进行解释和预测的理论，同时能通过实验的方法来验证。

计算机科学对比物理学

虽然嵌入式系统使得计算机科学与物理学结合

更为紧密，但是要想将计算机科学与物理学进行联姻，我们还必须对两者的差异和联系有更深入的了解。既然两种学科在方法论和范式上有许多重要的区别，那么我们能否像定义时间、实体存储器或能量一样来定义计算模型?

物理学基于连续数学，而计算机科学却植根于离散数学。物理学的研究对象是给定的“现实”，目的是发现支配物理现象的客观规律，计算机科学的研究对象是计算系统——只不过是人类的发明而已，它的运行规律已经事先被人为定义。

物理系统可以通过不同物理量之间的微分方程来描述，在很大程度上，物理现象的本质都是线性的，或者更进一步说，是确定的和可预测的。在对物理系统的研究中，综合法（synthesis）是构建物理系统工程的主导范式。一些物理系统工程，如桥梁或者集成电路的搭建，均能够通过行为描述微分方程的求解来解决。然而，即使是最简单的计算系统如RS翻转，也很难用任何基于有限集上的微分方程来描述。因而，计算系统通常通过程序和计算装置等可执行的形式来描述。计算系统的行为从本质上来说常常是不确定和不可预测的，难以用综合法解决，这就使得计算系统工程在很大程度上不得不依赖于校验和测试。

总体说来，计算机科学通过理论和模型使得我们对于离散动态系统有了更深层次的理解。面对客观世界，它提出了一种构建性和操作性的视角，弥补了物理学中传统的陈述性方法。

人工智能对比自然智能

生物组织能够紧密融合影响它们发展和演化并相互作用的物理和计算现象。一方面，生物组织与计算系统具有一些共同的特性，比如说对记忆和语言的使用，具有软硬件的划分等；另一方面，它们之间也有一些本质区别。生物组织中的“计算”是鲁棒的，其内在的机制具有很强的环境适应性。更重要的是，它具有抽象能力以及对常识认知的能力。

这些区别使生物组织和计算系统之间形成了一条不可逾越的鸿沟。简单的说，鲁棒性意味着对系统微小变化的响应也是微乎其微的。然而，离散性特征意味着现有的计算模型实际上很难具有这种鲁棒性。

尽管有这些不同，在计算机科学和生物学中仍然存在很多交叉甚至“杂交”的机会。比如说，神经科学和认知科学的结果能够激发新的非冯·诺依曼体系，反过来，合成生物学也能从计算机科学中的计算机辅助设计（CAD）和系统工程技术中找到灵感。

计算机科学的研究

不幸的是，当前计算科学领域的研究范围和焦点并不能解决系统设计和工程中产生的基本问题。以下三种典型的问题左右着研究团体的决策。

因循守旧（The business as usual syndrom）

依循惯例而不冒险去探索新的思路是在所有科研团体的研究者中普遍存在的态度。可惜的是，这种态度同样也盛行于计算机科学的研究中。

夸大其词（The hype syndrom）

与其他学科相比，计算机科学领域内的专家们似乎过分乐观地估计了解决困难问题和克服障碍的可能性。这种情况或许可以被解释为因投资方对创新的强烈需求和激励以及因应用和市场的广泛需求带来的强大推动力所导致的结果。

通常一些科学研究的路线图和陈述见解的论文会为我们提出所谓的“挑战”和对现实的希望。然而，这些挑战往往只是描述了一种愿景，真正的科学挑战是需要被明确指出的，是阻碍着知识的发展及其在一定领域的有效使用的重要障碍[11]。区别于增量式的科学进步，在科学挑战实现之前和之后一定存在一个明确的突变。此外，科学挑战还暗含一些“正面”的内涵，比如它必须遵守既定的道德和公共利益准则。最后，不同于那些描绘了一个长期而宽泛目标的愿景，科学挑战至少需要满足以下准则中的一条：

明确定义（well-defined） 科学挑战要么是明确定义的一个单独的问题（例如：费马大定理（Fermat's Last Theorem）），或者是明确定义的，需要一个框架作为解决手段的一组强关联的问题（例如：相对论）。

合乎情理（plausibile） 科学挑战需要兼顾现存的知识体系，包括广为接受的理论限制，如复杂性，可计算性，并且不能否认和忽略实验证据。

有意义（relevant） 完成科学挑战所需的资源应该与其目标的重要性和实现的风险相对称。尽管如此，科学挑战能够（并且应该）在不考虑完成所需资源的情况下进行系统的阐述和规划。

人工智能、第五代计算机、程序综合和并行处理等问题都曾经被夸大为重大的科学突破。但是，这些问题中的每一个都不能至少满足上述准则中的任何一条。它们基本上没有明确的定义、受到理论上的限制而显得不合乎情理。

理论与实际的失衡（The nice theory syndrom)

在任何领域，理论的目的是构建出能准确描述真实系统的模型，进而能够用于解释现象和预测系统的行为。它们应能帮助系统创建者更好地完成工作。

一种常见的态度是研究数学上较为简洁的理论框架，而不管它们与实际有多少相关性。诺贝尔经济学奖得主保罗·克鲁格曼说：“……在学术界，有一类理论能让聪明但缺乏创造性的年轻人尽可能地展现他的聪明，而这类理论往往更能吸引到忠诚的跟随者。”在计算机科学领域，简单的数学框架常常吸引了最才华横溢的研究者，产生出枯燥的和真正的计算毫无关联的“低水平理论”。这样的方式导致了理论和实践的分离，进而伤害到整个学科。爱因斯坦曾经说过：“让一切尽可能简单，但不是为了简单而简单”。但是在计算机科学研究中，有人持相反的态度，认为存在一些以特定方式构建的框架可以描述真实的系统，如UML和AADL。其实，它们包含了大量和语义无关的结构和元素，因此在实际使用中无法得到严格的形式化描述，进而也不能在这些框架上建立有用的理论。

我们需要的理论框架应该是有足够的表达能力来直接包含描述系统的高等概念和元素的极小集，同时也能经得起形式化和分析的检验。正如圣埃克苏佩里曾说：“最终达到完美,不在于无可增添,而在于无可删减。”

那么，有可能为计算系统找到一个数学上优雅并且实用的理论框架吗？我们知道，由于存在本质差异，无法期待拥有像物理系统那样美好和强大的理论体系。此外，还有一个更为深刻的原因：计算系统由人工构造，而物理系统却经历了漫长的演化。当你扔出一块石头时，它可以通过一条抛物线来描述。但是却不存在这样清晰的定律来控制程序的执行。

爱因斯坦曾说：“这个世界上最难理解的事情是所有的事情都是能理解的。”

计算机科学需要处理人工系统的构造问题。其中的关键是可构造性，即能有效地构造正确系统的能力[1]。根据需求合成复杂系统是一个难以驾驭的过程，这就要求我们去研究从组件构造正确系统的原理。这样做的目的是尽可能避免对复杂系统进行庞大的后期验证工作。目前在计算机科学领域已经存在大量有关可构造性的算法、架构和协议。它们的应用（几乎）能无代价地确保简单系统的正确性。而针对一个复合系统，怎样才能从其组件的特性有效地推断出全局特性？这仍然是一个古老却亟待解决的开放性问题，目前还没有令人满意的答案。这将成为系统集成的一个限制性因素，同时或许也意味着计算机科学已经明确降低到二流学科的地位。

计算机科学教学

计算机科学课程设置很少意识到系统的重要性，并且忽略了对学科的宏观描绘。对计算机科学的教学，我有以下一些建议：

教学生怎样从系统的层面上思考（设计过程、工具、用户和物理环境的交互）。通过引入控制理论和电子工程领域的原理、范例和技术使计算机科

学课程得到扩展和丰富。

讲透原理（基本原则、架构、协议、编译以及仿真等等），少讲具体实现。通常课程都为学生讲述专业所需知识的细节，而这些知识是可以从今后的职业生涯中获得的。一方面，学生应该有能力去应对这些由科技和应用而带来的不断变化；另一方面，他们也应该能认识到现存计算理论的局限，即，理论通常都会做出一些将现实过分简单化的假设。

重视信息和计算，并将它们作为不仅仅可以适用于计算机的普遍性的概念；激发学生的辩证思考能力，帮助他们理解和掌控数字世界。■

作者：约瑟夫 斯法科思（Joseph Sifakis）

2007年ACM图灵奖获得者，法国Verimag实验室创始人和研究总监。
Joseph.Sifakis@imag.fr

译者：GreenOrbs绿野千传项目组

GreenOrbs绿野千传科研团队，率先发起面向长期大规模无线传感网系统开展研究、实验、部署和应用。项目组的工作始于2008年，在林业碳汇、城市碳排放和空气质量监测等领域展开跨学科研究实践，迄今为止，在浙江临安天目山自然保护区和江苏无锡高新技术开发区部署了数千个节点的多跳自组织无线传感网系统。

项目组成员主要由来自清华大学、香港科技大学、西安交通大学、浙江农林大学、北京邮电大学、杭州电子科技大学、哈尔滨工业大学以及美国伊利诺伊理工学院等。

参考文献

[1] Henzinger T.A., Sifakis J., The Discipline of Embedded Systems Design, COMPUTER, 2007, 40, 36 ~ 44

[2] Lee E.A., Cyber Physical Systems: Design Challenges, 11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC 2008) (5-7 May 2008, Orlando, Florida, USA) IEEE Computer Society, 2008, 363 ~ 369

[3] Alur R., Courcoubetis C., Halbwachs N., Henzinger T.A., Ho P.-H., Nicollin X., Olivero A., Sifakis J., Yovine S., The Algorithmic Analysis of Hybrid Systems, THEOR COMPUT SCI, 1995, 138, 3 ~ 34

[4] Sifakis J., A Framework for Component-based Construction, Aichernig B.K., Beckert B. (Eds.), 3rd IEEE International Conference on Software Engineering and Formal Methods (SEFM05) (7-9 September 2005, Koblenz, Germany) IEEE Computer Society, 2005, 293 ~ 300

[5] Bliudze S., Sifakis J., A Notion of Glue Expressiveness for Component-Based Systems, LECT NOTES COMP SCI, 2008, 5201, 508 ~ 522

[6] Milner R., A Calculus of Communication Systems, Springer-Verlag, Secaucus, NJ, USA, 1982

[7] Wilhelm R., Engblom J., Ermedahl A., Holsti N., Thesing S., Whalley D., Bernat G., Ferdinand C., Heckmann R., Mitra T., Mueller F., Puaut I., Puschner P., Staschulat J., Stenström P., The Worst-case Execution Time Problem Overview of Methods and Survey of Tools, ACM T EMBED COMPUT S, 2008, 7, 1,45

[8] Henzinger T.A., Kirsch C.M., The Embedded Machine: Predictable, Portable Real-Time Code, ACM T PROGR LANG SYS, 2007, 29

[9] Kopetz H., The Rationale for Time-Triggered Ethernet, Proceedings of the 29th IEEE Real-Time Systems Symposium (30 November - 3 December 2008, Barcelona, Spain) IEEE Computer Society, 2008, 3 ~ 11

[10]Astrom K.J., Wittenmark B., Adaptive Control, 2nd edition, Addison-Wesley Longman Publishing Co., Boston, MA, USA, 1994

[11]Gray J., What Next? A Dozen Information-Technology Research Goals, J ACM, 2003, 50, 41 ~ 57

[12]Sangiovanni-Vincentelli A., Quo Vadis, SLD? Reasoning About the Trends and Challenges of System Level Design, P IEEE, 2007, 95, 467-506

[13]Caspi P. et al., Guidelines for a graduate curriculum on embedded software and systems, ACM T EMBED COMPUT S, 2005, 4, 587 ~ 611

[14]Lee E., Absolutely positively on time: what would it take?, COMPUTER, 2005, 38, 85 ~ 87

网络嵌入式系统可靠架构搭建

作者：詹·布泰尔（Jan Beutel） 洛萨·蒂勒（Lothar Thiele）
译者：毛续飞

关键词：网络嵌入式系统 可靠架构

基础

近年来，由于受到网络化持续增长的显著影响，各种规模和类型的计算机系统设计和搭建已经不再局限于一个处理器加上内存的独立配置，而是通过大量的此类设备的组合和集成来实现。这些设备一般都采用分布式分层的组织方式并且能够互联互通，通常支持全球范围的连通性，即接入互联网。虽然使用高性能服务器和工作站的商业计算机系统在一定程度上充分发挥了先进的并行计算技术在性能更好的硬件（摩尔定律）上应用的优势，而嵌入式系统仍然面临着特殊的挑战，并且这些挑战在网络环境下变得更为严峻：首先，大规模的分布式操作往往基于不可靠网络（无线）的链路连接，伴随的不稳定性往往对系统的可预测性和可靠性有很大影响；其次，资源的匮乏、应用的复杂性和多种多样的定制需求也产生了不合适及不充分的系统架构。而且这一事实往往在设计阶段无法避免，直到实际应用中才逐渐显现。目前大量由电池供电的便携式设备引发了一种将能量作为系统层面上主要优化目标的趋势，已经成为新的研究焦点，为新的模式和设计方法带来了巨大的机会。

在应对网络化嵌入式系统设计的特殊挑战下，特别是在考虑可靠性的背景下，我们认为同时强化基础性研究和实践与应用性研究是不稳妥的。主要是因为后者聚焦于实践方面的研究，必然使得跨学科领域的专家学者利用更长的时间在小范围内（最小临界数量上）进行协作。

再看无线传感网络领域，目前的应用正处于一个日臻完善的阶段。这些应用包括工业过程监测控制、环境监控、后勤保障、医疗应用和交通流量监控等。对其中很多应用来说，测量数据非常珍贵、不能丢失，而且必须实时送达。由于传感器价格昂贵，传感器网络部署和维护更新都需要耗费大量人力成本，因此，为了进一步推进无线传感器网络的发展，必须创建具备已知和可预测属性的高质量系统工具。接下来我们将给出关于新模型和方法的概述。这些模型和方法能够协助实现可预测的、高效的网络化嵌入式系统。例如形式测试和测试基础架构、太阳能优化使用、数据去噪方法、网络拓扑发现和传感器校准等。此外，我们将提出一种新的设计方案把感知数据从采集、本地存储、传输到基站、传输到主机、数据库存储，到最终的数据包过滤和校准等一系列工作设计成稳定的端到端系统。我们将通过一些大规模、长期部署、工作在恶劣环境下的无线传感器网应用（例如城市空气质量监测和永久冻结地带的环境感知应用等）论证我们的设计方案。

能量

设计高度自治和可靠的网络系统要考虑很多因素，其中一个主要的因素是如何持续有效地供能以及在保障性能条件下的低能耗工作。尽管对于软件开发来说，测试是保证系统正确运行的主要手段，但是基于能耗跟踪可视化或者基于测量的方法已经不适用于分析不同硬件平台和不同测试环境中具有

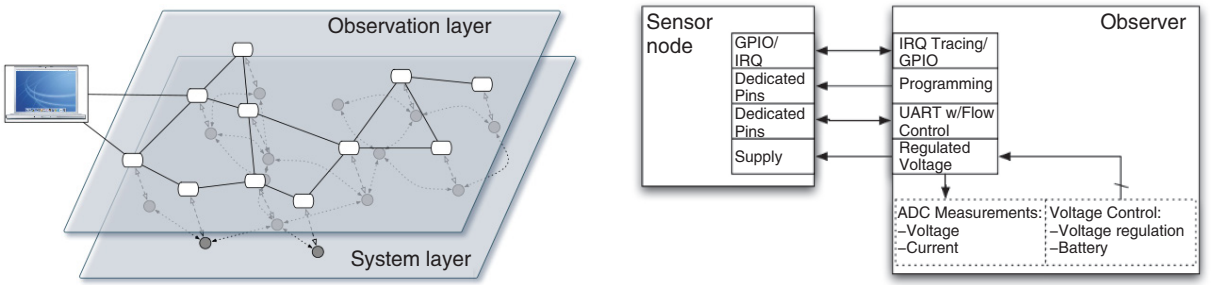


图 1 FlockLab系统和软件架构

众多属性的软件产品。所以，有必要利用能量监测来无干扰地探测运行系统的软硬件错误。例如形式化一致性测试，即检测在实际硬件上运行的一个无线传感网应用的能耗轨迹和该系统期望状态之间的一致性[1]。例如FlockLab实验平台架构[5]也可以用于观察研究[3]。

高度自治需要连续不断地供能。除了在满足性能要求的情况下研究最小化能耗的方法，我们还需要考虑如何利用有限、时变的能源优化应用程序的性能。例如，根据预测未来可用的能量，程序可以调整其参数和工作模式，从而最大化地利用资源[2]。如果有些程序需要实时响应，那么这个节点上的任务调度则需要考虑能源属性、能源容量以及这一任务的期限。在这种情况下，调度程序需要综合考虑能耗和时间的限制[3]。

但在嵌入式网络系统中，这种以单个节点为中心的分析手段已经无法满足需求了。相反，通信和网内处理是达到能耗高效利用需要考虑的因素：即基于计算的能耗比通信的能耗少几个数量级的假设下，如何尽量减少需要传输的信息量。同时，网络范围内的分析也需要考虑端到端的时间限制[4]。

无线传感器网络系统设计

通过系统建模和精准分析来预测未来的系统行为通常是前期设计的选择，通过测量来刻画实际运行的系统则是不可或缺的。在这一方面，FlockLab实验平台架构[5]扩展了传统的无线传感网（MoteLab，TWIST）的反向通道模型。它基于一套功能强大的观察者和目标的平台，具有全同步的分布式观察能力，不受单个数据收集节点带宽限制。在测试中，类似于无线传感器节点这样的设备可以被观察者平台局部增强，并可以被远程重新编程，详细地记录日志、激励、能量控制和能耗分析（图1）。FlockLab平台中的观察者可以适应四种不同的硬件平台，以此满足不同用户的要求。苏黎世联邦理工学院目前使用的实验平台配备30个节点，分布在校园建筑内外，与人工气候箱相连。在这种实验条件设置下，可以将环境对无线通信的影响与强大的逻辑数据获取能力结合起来。

要实现远程观测真实情景下的环境和系统，首先需要安装部署功能丰富的节点。有了这样能充分满足需要的测试性部署，我们就能进行在线观察、实验和学习[6]。这不仅让我们有机会从实际部署中获取经验，并清晰彻底地定义在应用需求规格限定下设计的可能性，也使得我们能够在构建第一个具体的应用原型之前就有可能对系统的性能进行概要分析。因此，这在很大程度上省略了在传统方法中必须不断进行的精制硬件的过程。

为了推进这种研究方法，我们对核心站点进行充分的实验和测试，使其具有很高的灵活性并充分满足需求（图1）。通过这个平台和可由用户配置的软件框架，我们可以不断地对低功率节点、专用的高速率传感器（如GPS、摄像头等）和满足应用需要的工作站进行新的探索。

使用TDMA（time division multiple access，时分多址）调度和同步的方法可以很好地达到可预测的高效通信。从这个意义上，我们正在开展同步的

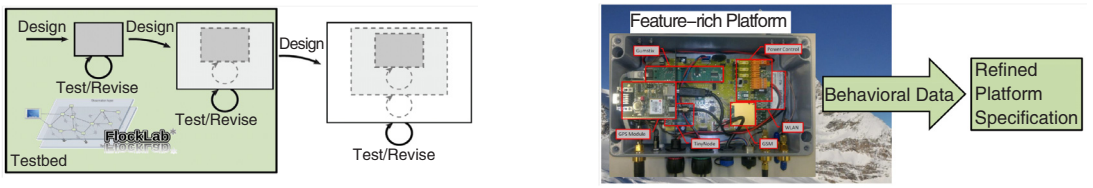


图2 传统的瀑布模型（左侧）采用不断细化的方式。利用功能丰富的核心站点从开发优化的X-Sense无线GPS传感器的现场实验来得出详细的行为需求

系统架构和协议的研究。PermaDAQ[7]传感器节点架构使用非常粗粒度的局部同步过程实现关注点拆分来处理这个问题。相反，格罗斯（Glossy）[8]则采用更彻底的方法对系统架构的所有层进行全局的同步。底层网络同步机制相当的高效和快速，并且能智能地利用编码机制和相长干涉这些底层无线电的特殊属性为自己服务。

让人不易察觉的是，过去无线网络嵌入式系统产生的原始数据并不是像设计和期望的一样正确，这意味着采集的数据不仅存在由中断导致的空白，还存在严重的序列顺序问题和数据重复[9]。只有对原始数据进行全面的去噪、转化和映射操作之后，领域专家才能对这些数据进行分析。举例来讲，其中一种数据去噪方法就是利用时间间隔来提供安全界限，最终生成没有重复的、按照数据获取时间正确排序的数据流。此外，不符合系统规格的数据也会被除去（图3）。

跨学科合作应用

为了进一步获得专业知识，了解实际应用背景，我们一直与环境科学研究领域的合作伙伴进行项目合作，以加深彼此的了解。除了促进交叉学科的研究，我们还获得了环境科学研究领域相关的许多研究成果，而如果没有使用最先进的无线传感器环境科学技术，这一切是不可能实现的。

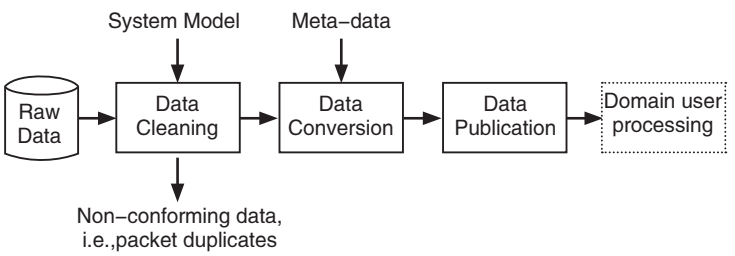


图3 收集到的元数据首先需要结合数据生成和传递系统的形式化模型进行去噪

PermaSense财团关注多种工程及科学长期研究项目，主要从事极端环境下（特别是在气候变化和自然灾害条件下）开创性的基础研究[10~11]，其中许多研究都是在长年冻土的环境下进行的。在过去的四年中，我们一直在设计并且在马特/采尔马特和瑞士少女峰/格林德瓦等极端环境中部署无线传感器网络，一边监测岩石冰川的群体运动，一边观察无线传感器网络在高山冻土中运行的稳定性[12~13]。该系统需要适应恶劣的天气环境，能够提供可靠的服务并确保数据的质量和数量。

除了增强系统部署能力以提高整体性能架构，这项研究活动还将极大地提升环境科学研究的水平。如果没有超低能耗无线传感器网络在海拔3500米高山冰川的长期部署，这些研究工作在从前都是无法想象的。

我们最近的一个研究项目OpenSense（http://www.opensense.ethz.ch）是为车队中的车辆安装诸如监控空气质量传感器，利用车辆的移动性以获得更好的监控覆盖范围。通过充分利用车队的运动，只需利用很少的传感器就可以在空间和时间上对城市进行很好地覆盖[14]。这里的挑战在于移动数据处理和如何更好地理解这些数据的组成。校准行为不仅仅只是定期进行，还可以通过两个或两个以上的移动传感器交叉数据检查的方式完成。

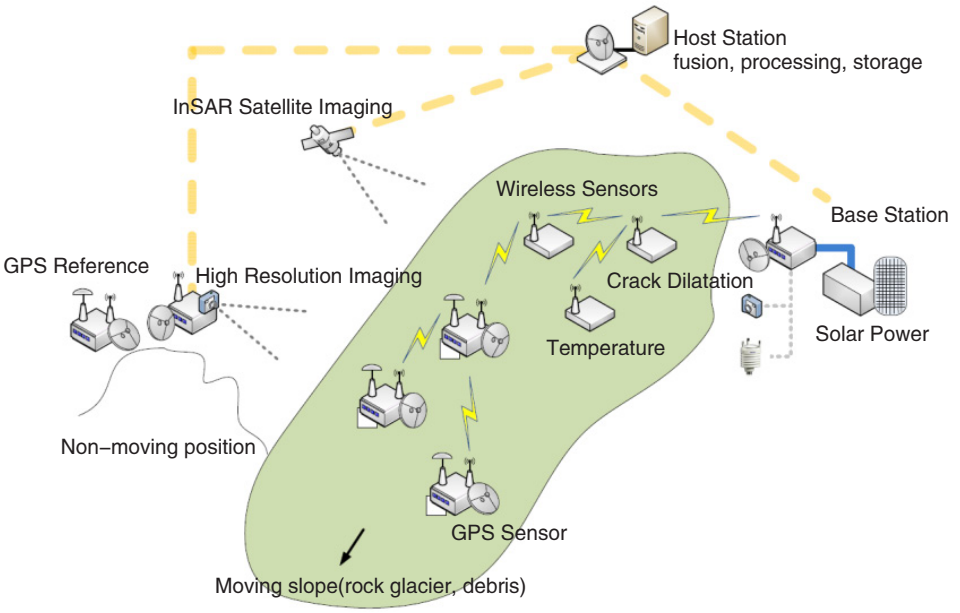


图4 岩石地形走势的详细分析及使用的多种类型的传感器，从不同的时间和空间尺度看信息融合

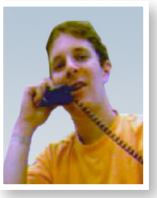
再比如，当车辆通过参考空气质量监测站的时候也可以完成数据校准[10]。

小结

综上所述，我们依次描述了系统的设计原则，适用于嵌入式网络系统开发，需要尽可能高质高量数据的应用场景以及以低成本来保持系统可控性和可见性的准则。我们所获得的经验主要源于极端条件下的研发环境监测的无线传感器网络（见http://www.permasense.ch和http://www.opensense.ethz.ch）以应用于建筑等安全性至关重要领域的传感器网络。

致谢

以上研究成果与研究小组的许多成员的努力密不可分，特别是马蒂亚斯·凯勒（Matthias Keller）、伯恩哈德·布什利（Bernhard Buchli）、费德里科·法拉利（Federico Ferrari）、马尔科·泽姆林（Marco Zimmerling）、奥尔加·索科（Olga Saukh）、大卫·哈森弗拉泽（David Hasenfratz）、克莱门斯·莫泽（Clemens Moser）、托尼奥·赛尔（Tonio Gsell）、罗马·林姆（Roman Lim）和克里斯托夫·瓦尔泽（Christoph Walser）等。我们的工作还得到了Nano-Tera项目的X-感知项目，OpenSense项目以及瑞士自然科学基金资助项目MICS-PermaSense的支持。■



作者：詹·布泰尔（Jan Beutel）
苏黎世u-blox AG。研究兴趣包括设计、测试和验证无线嵌入式网络系统及其应用。

作者：洛萨·蒂勒（Lothar Thiele）
瑞士联邦理工大学计算机工程系全职教授。研究兴趣包括嵌入式系统设计的模型、方法及软件工具，嵌入式软件以及生物计算优化方法。

译者：毛续飞
清华大学软件学院博士后。主要研究方向为无线网络的算法设计与分析及大规模无线传感器网络的应用研究等。xufei.mao@gmail.com

参考文献

[1] M. Woehrle, K. Lampka and L. Thiele: Exploiting timed automata for conformance testing of power measurements. Proc. Formal Modeling and Analysis of Timed Systems 2009, Springer, pages 275-290, September, 2009

更多参考文献：www.ccf.org.cn/cccf

驯服弗兰肯斯坦博士*：设计网络嵌入式系统

作者：阿尔博托·西欧凡尼·维埃洛爱
（Alberto Sangiovanni Vincentelli）
译者：董　玮

关键词：网络嵌入式系统

通过与物理世界进行丰富的连接（物联网），信息技术已经迅速地向分布式和协作化的环境（云）发展。特别需要指出的是，预计到2020年每人将拥有数千台设备。这些设备会使计算无处不在并支持超乎想象的社会大规模的应用。庞大的计算会给我们带来很多困难，即使在计算设备没那么多的今天，我们在设计安全的应用程序时，仍面临着一系列严峻的挑战。

设计复杂分布式系统的本质是连接：连接概念、连接物理对象、连接团体人员。未来的产品将会把物理世界和虚拟世界连接在一起。连接可能使系统提供比单纯的组件叠加更多的功能，但也可能提供更少的功能，甚至可能由于组件之间不恰当地交互，使得整个系统根本无法工作。而且这种情况的发生几率是存在的，就像一场恶梦将要发生！要高效地管理一个大系统各组件间的关系，需要那些尖端设计方法的共性原则。我们来探讨一下设计原则和多尺度系统的演变过程，指明一些振奋人心和不断精进的分布式系统设计领域，如能源效率、合成生物学、飞机和汽车。

系统行业，包括汽车、航空和消费电子企业正面临着重大困难。这是因为，一方面产品本身的复杂性正成倍上升，另一方面，用户对产品功能、正确性以及上市时间的要求越来越紧迫。由上市时间推迟或产品缺陷带来的成本是惊人的，因为企业必须承受产品召回和交货延误带来的开销。由于设计问题导致破坏性影响的例子不胜枚举。这些问题的具体根源是复杂的，涉及到设计过程、与不同开发部门以及供应商的关系、不完备的需求分析和测试验证等。此外，在工业界中有一个广泛的共识：目前我们只在整个设计空间中考虑了一个很小的集合，如果能优化整个实现过程，将对我们大有裨益。虽然一些在更高效的设计空间探索方面的尝试已经开始，但是仍有必要对问题进行更好的形式化描述，并且有效融合供应链上的不同参与者。子系统在设计期间传递给系统组装器的信息，例如时间、功耗、尺寸、重量以及其他物理特征，对于设计空间的探索还有很大的提升空间。在这种情况下，一个系统设计方面的错误会造成巨大的社会经济损失，并危及到整个公司的存亡。难怪人们热衷

* 弗兰肯斯坦博士，是英国诗人雪莱的妻子玛丽·雪莱在1818年创作的小说《弗兰肯斯坦》中的主人公。《弗兰肯斯坦》被认为是世界第一部真正意义上的科幻小说。《弗兰肯斯坦》的全名是《弗兰肯斯坦——现代普罗米修斯的故事》，中译本也翻译成《人造人的故事》。小说将弗兰肯斯坦刻画成一位从事人的生命科学研究的学者，他力图用人工创造出生命。美国工程院院士、加州大学伯克利分校阿尔博托·西欧凡尼·维埃洛爱教授用此作标题来比喻物联网这个人造的事物带来了巨大的机会，同时也给我们科学工作者带来了要解决的难题。

于利用风险管理手段来评估由于设计失误、发布延迟、产品召回以及负债带来的风险。寻找合适的应对策略来降低风险并且制定应急方案是如今大型项目采用的主要方法。目前的首要问题是，当今系统公司使用的设计方法需要根本性的变革。要解决的问题是理解系统设计的原则，理解设计方法的必要改进，理解供应链的动态性。加深这些理解对一个系统公司是必须的，这样公司才能更好地服务客户，更好地加快产品开发速度，更好地提高产品质量。

本文的关注点是网络嵌入式系统，也称为信息物理系统（cyber-physical system，CPS）。信息物理系统集成了计算和物理过程。由嵌入式计算机及其组成的网络对物理过程进行监控，物理过程对计算产生反馈回路，反之亦然。新兴的信息物理系统应用注定要以分布式的形式在一个平台上运行。这个平台将高性能的计算机簇（基础设施核心）和大量的移动通信设备协调在一起，而这些移动通信设备又被更大群的传感器包围（从宏观的到微观的）。大部分这样的新兴应用可以被划分为“分布式传感控制系统”，这类系统从本质上已经远远超出了传统意义上的“计算”或者“通信”范畴。这些应用将有可能从根本上影响到我们如何处理当今社会面临的重大问题：比如国家机密及安全、监视、能源管理和分配、环境监控、高效可靠的交通、有效的医疗保健。这些应用的一个共同属性是它们同时牵涉到大量的功能部件——从云计算提供的数据和计算服务，传感器上的数据收集，到移动终端上的数据访问；另一个属性是系统跨越了多种尺度——有空间尺度上的（从非常大的到非常小的），有时间尺度上的（从非常快的到非常慢的），有功能尺度上的（包括由异构功能构成的多层复杂架构），有技术尺度上的（整合了多个领域的技术）。这个分布式平台的每个组件（计算和数据簇、移动便携设备以及传感器系统）本身就是一个多尺度系统，并带来一些独特的设计挑战。

如今的工程师们在多个不同的行业成功地设计了信息物理系统。但不幸的是，这种系统的研发成本非常大，并且也很难严格执行研发计划。信息物理系统的复杂性，尤其是为了提升性能，合并了不同的子系统，增加了整体设计和验证的难度。随着这些系统复杂性不断增加，我们可能会无法对这些物理和网络方面间的交互进行严格建模，从而造成严重的不稳定性。系统将变得不安全，并可能产生不可预测的灾难性后果。

实现和运行这些多尺度系统面临很多复杂的挑战，并且覆盖了很多尚未解决的设计与运行时问题，包括建模与抽象化、验证、检验与测试、可靠性与弹性、多尺度技术整合和映射、能耗、安全及诊断和运行时管理等。如果不能以一种恰当全面的方法解决这些问题，即使不会导致这些新技术不被采用，也一定会推迟这些新技术的广泛应用。我们相信在信息物理系统的工程中，最有前景的一种解决方法就是使用结构化与形式化的设计方法。这种方法能够无缝地整合多尺度设计空间的不同维度（如行为、空间、时间）。正因如此，它能够提供恰当的抽象来应对固有的复杂性，并能够提供正确的实现。

当开发新的系统设计方法时，必须解决以下技术问题：

1.异构系统的整体设计流程，包括技术上和组织上的设计。我们认为跨越传统界限的模型整合使用并没有被很好的研究和开发。

2.复杂系统的验证，尤其是在任何交互都是很困难的且解决代价极其昂贵的系统整合阶段的复杂系统验证，在国防和自动化以及其他工业中都是很常见的一种需求。

3.对于如何处理可变性、不确定性以及生命周期问题（比如一个产品系列的可扩展性），使用现有的系统工程方法论和工具并不能很好地解决。

4.在启发式的过程中，系统需求的采集和分析占了很大比重。目前使用的非正式文本和基于自然语言的技术在启发式的过程中面临很严重的问题。形式化的需求工程还处于起步阶段，必须开发相应的数学模型、形式化分析技术和与之相联系的系统实现。

5.由于很少充分地考虑设计空间的探索，导致一些没有达到最优的设计。这些设计在体系结构选择阶段没有考虑到为了减少成本、故障率和投入市场的时间所需要的可扩展性、重用性以及容错性。

针对设计工艺的挑战，我们需要考虑的不是仅针对方法论、工具或者模型这些设计的简单部分中某一点问题的解决方案，而是处理整个设计的全过程。解决这样的挑战需要一个能够整合不同物理系统、控制逻辑以及体系结构的新的建模方法。在这个过程中，必须保证现有的方法、模型和工具都能得到兼容而不是完全被摒弃，这样才能保证设计人员不会反对设计改革，从而平稳地过渡到新的设计方法。另外，必须开发一个设计平台来承载新的技术，并整合一系列现有交互性不强的工具。研究计划中提出的“契约式设计（contract-based design）”在欧美是一个比较普遍的观点，它形成了广泛而积极的范围来应对系统工业的迫切需求。当原始设备制造商必须和他的提供商就需要交付的子系统或者零件达成一致时，就会使用契约。

契约包含一个约束各方的法律部分和一个作为参考的技术附件，由供应商提供完整的参考。当为同一家公司开发不同的子系统或者一个系统的不同方面时，此契约同时会被作为并行工程的技术附件使用。从我们的观点来看，契约可以应用在任何地方以及系统设计的所有阶段，从需求的获取到嵌入式计算基础设施以及具体设计（电路和硬件）。尤其是契约明确地处理了合作内容，分别表述为对环境的假设以及承诺建立在这些假设上的系统。一个契约还可以形式化地描述为$\boldsymbol{C}=(\boldsymbol{A},G)$，其中$\boldsymbol{A}$=假设，$\boldsymbol{G}$=承诺。这里的A和G是所有满足属性的输入和输出的集合。虽然假设和保证的推理已经被发现了相当长的一段时间，但是几乎只被用作设计软件时的验证。我们的目标更为远大：基于明确假设的契约设计是一个设计哲学问题，必须遵循所有的设计规范使用各种各样的模型。这里所说的模型内容非常丰富，不仅包含配置、类型和数据分类，而且可以描述各种时间和能量的功能及性能和安全性。

为了给系统工程师一个基于契约设计技术的选择，我们必须开发：

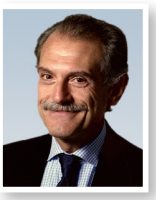
1.用于契约描述的数学基础和用于设计的工程学需求（架构和工具）；

2.一个系统工程架构以及与之关联的方法论和工具集，这些事物关注于物联网系统的多抽象层的系统需求模型、契约规格和验证；

3.一个针对交叉边界设计流的系统工程架构，主要解决契约设计的组织上影响和随时间演化系统的配置和管理。

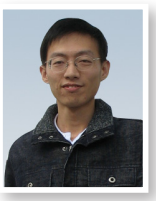
在这次表述中，本文的目标是描述上下文系统层设计里基于契约的设计。

我们先回顾了需要应对的挑战。契约的概念是一个统一的视角，就是怎样把出现在每一步设计流程中的需求和规则形式化；然后提供一个简洁的形式化的契约概念；带着这个想法，展示了怎样去结合契约和基于平台的设计来囊括其他的方法，并提出了一个简单的控制问题来展示上述方法论的使用；最后，提出了一个可以使契约广泛应用于工业的潜在发展方向。■



作者：阿尔博托·西欧凡尼·维埃洛爱（Alberto Sangiovanni-Vincentelli）

美国工程院院士、加州大学伯克利分校电气工程和计算机科学系教授。



译者：董　玮

CCF会员。浙江大学讲师。主要研究方向为嵌入式软件与传感器网络。

weidong@ieee.org

信息物理系统的网络挑战

作者：路易斯·阿尔梅达（Luis Almeda）
译者：杨盘隆

关键词：信息物理系统 CPS

简介

信息物理系统（Cyber Physical Systems，CPS）的概念从产生到现在还不到十年。它的诞生是颇具争议的。它和目前现有的研究领域都有部分重叠，如嵌入式系统、实时系统、控制和模型驱动工程。尽管由于缺乏准确的定义，又与其它研究领域有着严格的区分而颇受非议，但是迄今为止，信息物理系统似乎已经被认定是上述各个领域的交叉，同时又是上述领域的推广与泛化。信息物理系统与嵌入式系统和实时系统并不一定要有本质的不同，但是已经超越上述研究领域，同时又把控制系统、模型驱动工程和其他学科融合进来。通过建立模型的物理过程和计算平台，可以促进互操作过程，更好地了解系统状态，并实现更好地控制。出于这种原因，在一些场况下，人们也把信息物理系统称为网络监测和控制系统（network monitoring and control，NMC）。

通常，信息物理系统包含了嵌入式、实时控制系统，特别是模型驱动的相关的设计技术。从体积小的系统，比如具有主动安全控制能力的个人交通系统segway，到规模庞大的系统，如智能楼宇或与用来控制能源效率的绿色工厂[1]，信息物理系统几乎无处不在。

然而，由于普及程度日益提高，信息物理系统越来越依赖于分布式平台，特别是更广泛地使用网络（图1），从传感器到控制系统、自动化或企业网络，网络能够将无数不同类型和用途的节点有效互连，为整个系统的目标共同协作。

与分布式系统一样，网络在支撑信息物理系统的主要功能方面扮演了不可替代的角色，为保证系统实时响应外部物理过程的动态变化，起到了至关重要的作用。因为建立可靠的数据分发机制是建立分布式应用的基础。

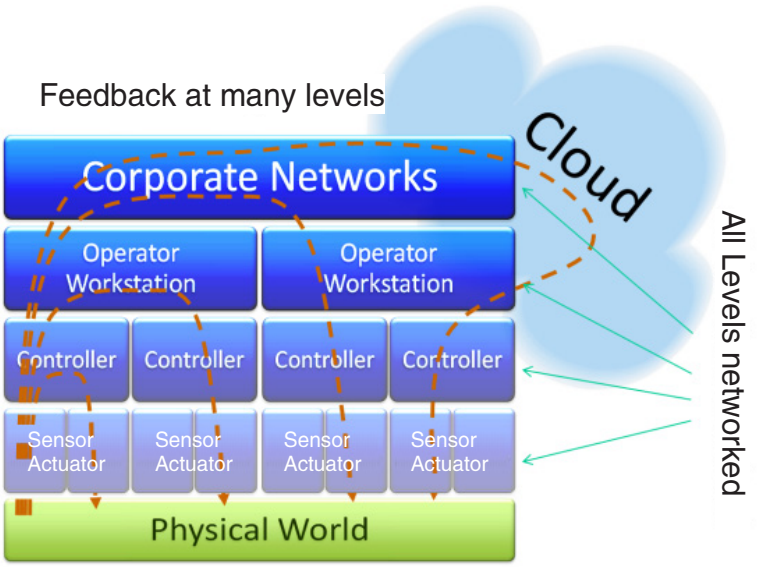


图1 信息物理系统的体系结构

信息物理系统的网络要求

信息物理系统多数是建立在分布式计算平台基础之上，依靠网络的数据传输能力来实现协同的。由于信息物理系统具有独特的物理特性，系统的计算和通信行为都需要满足实时性的约束。不仅如此，信息物理系统经常应用于资源配置有限的动态场景中，因此需要自适应技术，以避免资源紧张和利用率不足。例如，一组自主监测的机器人，可以根据处于活跃状态的机器人数量，以及在监视区域内是否有感兴趣的跟踪对象等实际情况，来自适应地调整通信频率。此外，一些信息物理系统是由数量众多的元件组成的，且分布广泛，例如工厂管理和商用飞机。还有一些系统是在不同地点工作，并通过互联网实现组件之间的协作，例如智能电网和远程交互。因此，必须考虑系统的可扩展性。许多信息物理系统是开放的，例如在工厂车间里增加机器人，灵活地进行任务调度；或者是一些并非信息物理系统的应用，但是却与之共享相同的网络基础设施。对于信息物理系统，除了时效性、适应性、可扩展性和开放性等基本要求，其他方面如可靠性、可用性和安全性也是同等重要的。网络系统对于通信计算平台的影响是巨大的，因为它同时决定了系统对物理世界的控制程度，以及对物理世界状态表示的精确程度。平台的核心作用如图2所示。

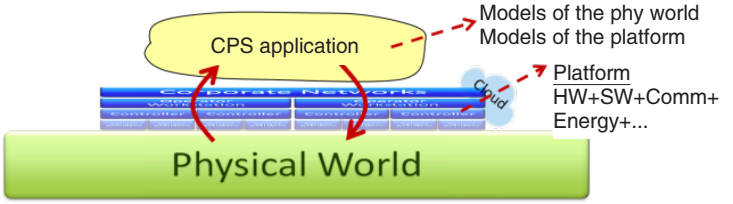


图2 平台的作用是协调信息物理系统应用程序和实际物理过程

图2同时还说明了信息物理系统应用程序的一个基本特征，是使物理过程和平台相结合的模型，可以提高系统的状态控制和获取知识的准确性。网络控制领域提供了一个很好的例子来说明融合模型的重要性，通过在分布式系统中实现控制器，结合平台和物理过程的融合模型，能够有效地提高系统的控制精度。

何种网络适合信息物理系统

一个很自然的问题是：“现有的网络技术是否足以支持我们刚才提到的各种要求？” 答案是否定的！绝大多数现有的实时通信技术是基于固定部署的嵌入式系统。这些系统都是基于开发成熟的技术，系统形态和通信需求都需要事先确定，提供时效性保证与可计算的网络时延和时延抖动上限。像TTEthernet和AFDX的技术就是很好的例子。然而，它们并不是开放系统，也不能有效地适应环境变化。在某些情况下甚至连可扩展性都可能会受到限制。相反，一些技术能够无缝支持动态的通信需求，能够支持开放性和适应性，但通常没有时序分析和准入控制，无法提供及时的保障。这在基于普通以太网或CAN（controller area network）总线的系统中是常见的，因为在这样的网络中运行时无法附加任何额外的通信需求。

反观大型网络，如互联网，尽管在过去十年中，具有扩展性的服务质量控制已经取得了长足的进步，但通信的基本能力还是以提供“尽力而为”的服务为主。事实上，有许多技术可以在互联网的核心层提供带宽、延迟和抖动保障，如采用第3层的以太网交换技术或采用2.5层交换技术的资源预留，或是采用多协议标签交换技术。这些技术允许创建满足带宽和时延要求的虚电路（也称隧道）。然而，由于网络提供商的多样性和网络终端普遍缺乏QoS控制能力，目前还难以充分发挥这些技术的优势，提供可控的、可计算的端到端延迟和延迟抖动能力。上述技术提供了相当程度的系统自适应性，但基本上都只是关注路由和队列管理功能，而没有考虑信道容量或时间需求。

此外，互联网研究关注的是可扩展性或吞吐量，而嵌入式网络研究领域则往往关注时延，却没

有太多考虑吞吐量和可扩展性方面的要求。这些不同的研究领域各自为战，几乎没有交叉。直到最近，由于信息物理系统的出现，这种状况才有所改变。目前，特别需要根据可扩展性和实时通信的需求，建立统一的网络体系，以满足信息物理系统和交互式访问所带来的可扩展性和时延的要求。

信息物理系统所面临的网络挑战

由于系统的形态各异，覆盖了网络研究中非常广泛的领域，使提供一个满足信息物理系统要求的通用网络变得异常困难。然而，我们还是能够找到一些满足所需的功能，为将来的设计产生积极影响，同时提高网络接口的适应程度。更重要的是，网络功能应独立于特定的底层网络协议支持，从而有利于标准化和部署，这有点类似于多协议标签交换（multiprotocol label switching，MPLS）网络或是互联网服务提供商。但在系统适应性和对终端系统的改造方面要远远优于他们的表现。

因此，我们认为一个通信抽象应该具有如下特点：

· 首先要易于与更高层协议工作，这意味着它非常适合用一个简单而准确的方法集成到现有信息物理系统应用中，例如采用虚拟信道与指定的带宽、延迟和抖动保障；

· 提供QoS，保证使用最低的要求，例如，与虚电路交换（隧道）的资源预留协议（resource reservation protocol，RSVP）和多协议标签交换的基本要求一致；

· 采用分层组合的方式扩展到更大规模的网络，支持信道级的整合；

· 在动态环境下，考虑高效利用带宽的适应性，例如，利用时序约束和松弛管理技术；

· 对系统过载、连续失败和拒绝服务攻击具有容忍能力，同时避免系统崩溃。

这种抽象依赖于面向时间的服务水平协议，并直接利用2层交换技术支持资源预留和自适应队列管理（数据链路层）。此外，也可以使用面向时间

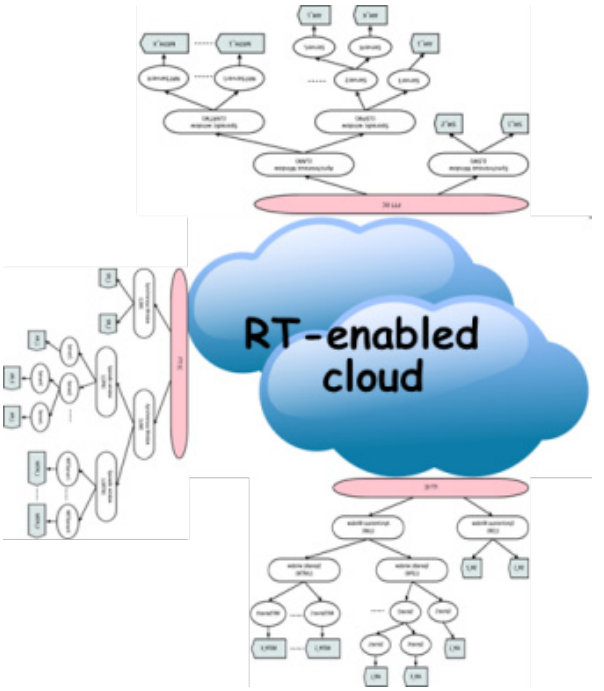


图3 具有实时功能的网络为分布式信息物理系统提供无缝融合支持

的流量调度，以数据截止日期为基础，考虑系统可扩展性，提供基于截止日期和负载感知的分布式资源预留机制。其结果将是一个全局的实时网络，可以无缝提供远程服务和实时保证，即具有实时处理能力的云（如图3所示）。

一种可能的路径

随着互联网的进化，支持延迟敏感型服务成为一种趋势。可以预见，互联网服务提供商会提供服务水平协议和商业发展模式，包括明确的时钟参数，而不是仅仅提供带宽和比特率信息。

然而，在互联网边缘之外，终端网络（也被称为接入网络）必须支持所需的实时性属性，为系统提供端到端业务的支持。事实上，目前大多数的信息物理系统除了在远程监控和系统维护时会使用互联网进行系统的控制操作，大多数情况下是不使用互联网的。

因此，我们集中考虑终端网络的能力，采用自

下面上的方法解决网络的挑战。我们从一般嵌入式系统解决方案出发，增加开放性和适应性，根据需要扩展到所需的范围。我们研究的网络模型如图4所示，展示了一个具有虚拟电路或虚拟通信能力的网络，通常根据虚链路容量、延迟、业务周期和抖动的要求而建立，可以灵活地建立、拆除或在线调整。同时，多个虚电路可以通过捆绑复用，以实现调整相关参数，并达到应用所要求范围，保证业务服务质量。

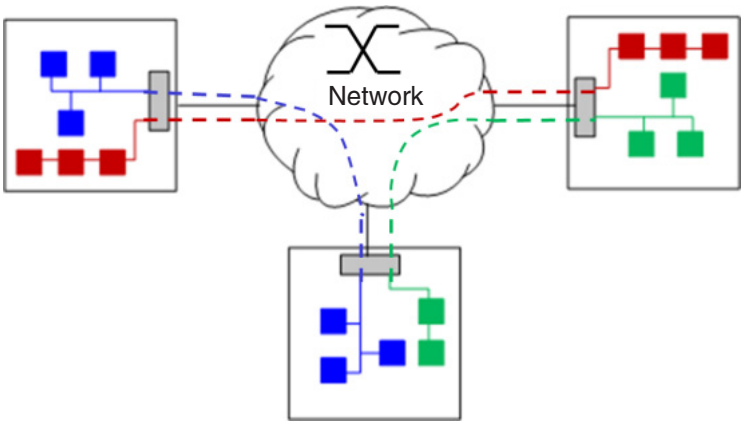


图4 动态虚拟电路交换网络模型

为了实现图4中的网络模型，我们一般采用两种方法，主要取决于对网络行为控制水平的要求。对于控制要求非常高的场景，特别是复用有线网络实现接入的情形，我们建议采用灵活的时间触发（flexible time-triggered，FTT）模式，结合时间触发（time-triggered，TT）中的在线流量调度方法[2]。这种方案可以在不同的DLL协议之上实现，但目前绝大多数都依靠CAN（FTT - CAN）和灵活时间触发式以太网（FTT - SE）来实现。我们可以按照图4中的设计模型，利用现有的商用以太网交换机实现灵活时间触发式以太网。图5显示了一个用灵活时间触发式以太网支持时间上独立的虚拟通道的层次化模型。在这种设计下，系统能够支持多种类型的业务流，从快速数据流形态下的短小的控制数据包，到实时视频流、文件传输和通用的互联网接入业务。这些通道可以创建、管理和撤销，并由相应的应用程序或第三方实体，如操作员执行。后一种选择可以支持传统的或通用的应用，可以提供所需基本功能的虚拟网络。独立的虚拟通道能够有效地切分网络容量，也使得灵活时间触发的协议，特别适合支持所谓的混合优先级的应用中，因为在这样的应用背景下，不同优先级的业务共享相同的通信链路。

灵活时间触发式以太网使用一个独立的节点，即主控节点，通过分组调度实现周期性的流量控制。每一个周期被称为一个基本循环，每个节点将只发送周期调度允许的流量。在每一个基本循环内，每个节点只发送流量调度所允许的流量，从而

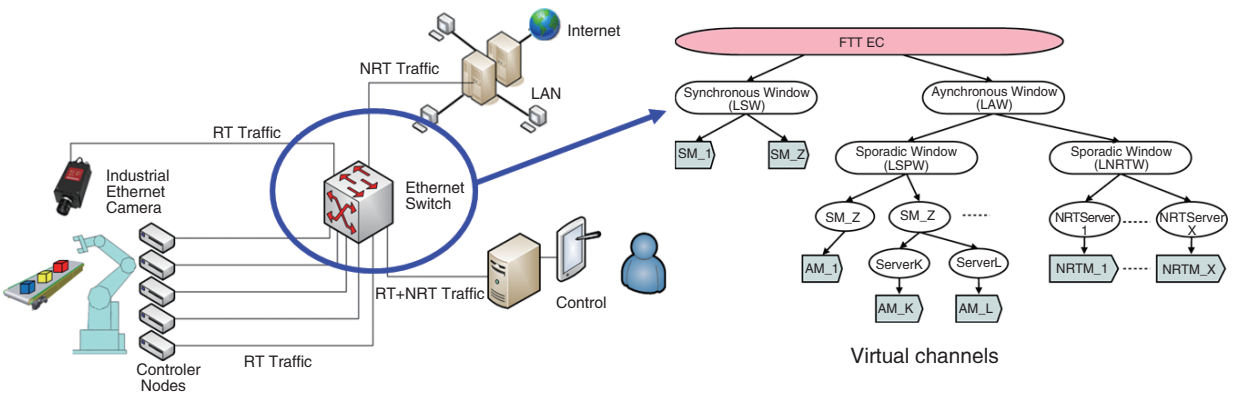


图5 使用灵活时间触发的范例，设置时序上独立的层次化通道以支持多种流量需求

保证交换机的队列将在每个循环结束时是空的。因此，流量在经过基本循环的调度后，将按照主节点的要求发送数据。典型的时间周期可以设置成1到20毫秒。通过集中的流量调度策略，所有现有的策略都可以执行，无论是以截止日期为目标的，以优先级驱动的，或是基于服务器响应的，还是基于业务等级的，均可以很好地支持。特别是部署流量调度策略，与现有实时分析的工具和框架一致，利用阈值和响应时间作为控制准则，进行有效的网络计算。

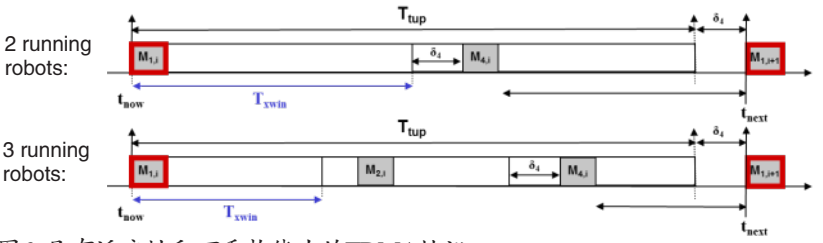


图6 具有适应性和可重构能力的TDMA协议

灵活时间触发对网络的处理方式与实时操作系统管理处理器的方式十分相似，均支持周期性的同步任务，也支持非周期下的异步或突发任务或数据流。特别需要指出的是，与所有的时间触发方法类似，灵活时间触发的协议本身通过相对相位控制支持同步流，可实现较高的带宽利用率和较低的时延抖动。

然而，灵活时间触发以太网要求终端节点的网络设备驱动程序上执行各自的适配程序。但是以HaRTES[3]为基础的交换模式却并不需要这样的条件，它是由一个普通嵌入式以太网交换机和一个快速时间的主节点组成。旧版本节点或通用节点可以直接连接，并通过交换机实现自适应调整，极大地提高了系统互操作水平。

灵活时间触发的协议采用循环的同步框架，以此实现全网同步，并支持相对相位控制。然而，这种级别的控制，有时却过犹不及。因为对于网络容量和突发的控制是足够用的，但在相对相位控制方面却无能为力，只能将突发行为的控制功能放到终端节点上。为此，我们最近提出了在终端节点使用Linux的流量控制方法，与刚刚描述的灵活时间触发的协议类似，建立一个中心主控终端节点，完成在终端节点[4]建立，撤销或更新虚拟通道的任务，从而满足系统的时间要求。我们创建了一个建立在灵活时间触发以太网和Linux的系统之上的特定发布-订阅中间件，使得两个系统之间应用程序移植更加透明。

对于高可靠性的应用，使用主节点备份机制是强制性的。这一点已经在灵活时间触发的CAN总线系统中实现，用于保持更新过程中的主副本同步。然而，这一点必须在基于以太网的环境下做出改变。可扩展性也是一个非常重要的问题。最近的一些研究工作，分析了不同的方法实现灵活时间触发网络系统的可扩展性。主要做法包括使用多个（不限数量）的网络，每个都有其自己的主控节点和网关，并且在多跳情况下将本地流量有效分离。但是跨越多个网络的资源预留和同步机制仍然悬而未决的问题。

传统方法无法在同一网络上为不同类型的应用提供服务保障，特别是在控制质量较差的网络条件下保证系统的性能。例如，在无线网络上，由于处于开放环境，会受到信号干扰和衰减的影响，网络质量较差。在这样的网络中，在有线网络中使用的流量控制方法会由于较长的延迟和更高的丢包导致无法执行。我们研究的重点是为自主机器人提供基本的通信手段，这项研究属于移动信息物理系统的范畴。

为此，我们为多机器人协同提供了一套定制解决方案，机器人能够定期分享他们的状态，并保存在每个机器人在实时数据库中[5]。这种结构使本地进程访问远程变量，就像本地访问一样方便。采用本地存储的图像，将网络中的通信延迟考虑进来，将有助于机器人对合作行为做出有效的判断和分析。

在基于TDMA模式的WiFi无线通信背景下，允许每个移动单元，在专用时隙内按顺序广播剩余的实时数据库副本数目。节点同步监听网络状态，而

无须全局时钟同步，时隙数量是动态变化的，根据目前网络中活跃单元的数目而定（图6）。因此，需要进行配置的参数只有TDMA时隙的周期和各个单元的惟一标识。节点单元能够发起初始化进程，从崩溃中恢复，或在任何时候离开网络。在实践中，该协议已被证明是有效的，它不仅能够减少队列丢包，同时提高了协同行为的效率。我们也已在简单的周期模式下对协议进行了理论分析。由于进行了一些近似处理，性能表现略有保守。这个协议已经成功用于验证一个小规模的，包含10~15个机器人成员的群组。如果应用于一个较大的机器人群组，需要一个合适的聚类方法。目前此问题尚无法解决。需要注意的是群组的概念需要，这能够使保证群组成员之间配置的一致性。我们可以把一个接入点[5]范围内的所有成员定义成一个群组。最近，协议扩展到ad-hoc模式，支持动态拓扑结构，同时支持ZigBee在相对定位中的应用[6]。

结论

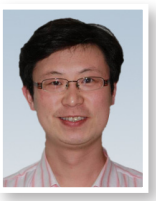
本文介绍了网络对于各种类型信息物理系统的支撑情况，分析讨论了网络研究对信息物理系统的作用，为有效地支持分布式信息物理系统提出了一系列设计要求。同时认为现有技术无法满足上述设计要求，特别强调必须考虑从终端系统到互联网，都要具备及时性、开放性和适应性的特点。除了互联网之外，我们采用自底向上的方法，从嵌入式系统角度出发建立信道抽象模型。如灵活时钟触发协议和Linux流量控制网络，还包括为无线状态共享所提出的具有适应性和可重构TDMA时隙分配技术。同时，我们也提出了目前亟需解决的问题。我们认为，所提到的方法都会为建立分布式信息物理系统提供一定程度的支持，包括在互联网边缘运行的，具有实时控制能力的协议，也包括那些运行于大范围部署的专用网络协议，如智能电网和远程交互网络。

致谢

本文的思想和内容与强大的团队协作密不可分。我在这里要特别向下列同事表示感谢，他们是圣保罗·佩特雷亚斯、里卡多·马劳、瑞·桑托斯、弗雷德里科·桑托斯和路易斯·奥利维拉。■

作者：路易斯·阿尔梅达（Luis Almeda）

葡萄牙波尔图大学教授。



译者：杨盘隆

CCF会员。中国人民解放军理工大学副教授。主要研究方向为无线传感网技术，认知无线电技术和嵌入式网络系统设计。panlongyang@gmail.com

参考文献

[1] Giese, H. etal. (Eds.) (2011) “Science and Engineering of Cyber-Physical Systems”. Dagstuhl Reports 1(11):1 ~ 22, http://drops.dagstuhl.de/opus/ volltexte/2012/3375/pdf/dagrep_v001_i011_p001_s11441.pdf

[2] The Flexible Time-Triggered paradigm, available online at: http://www.fe.up.pt/ftt

[3] The HaRTES Ethernet (FTT-enabled) switch, available online at: http://www.ieeta.pt/lse/hartes

[4] Mario Sousa, Luis Silva, Ricardo Marau, Luis Almeida. A Real-Time Resource Manager for Linux-based Distributed Systems. Work-in-Progress session of RTSS 2011, Vienna, Austria, November 30, 2011

[5] A Real-Time Database (RTDB) middleware for collaborative robotics, available online at: http://code.google.com/p/rtdb/

[6] Luis Oliveira, Luis Almeida, and Frederico Santos. A Loose Synchronisation Protocol for Managing RF Ranging in Mobile Ad-Hoc Networks. RoboCup Symposium 2011, Istanbul, Turkey. July 11, 2011