Modeling and Simulation 建模与仿真, 2020, 9(3), 345-356
Published Online August 2020 in Hans. http://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2020.93035

Hans汉斯

Review on Cyber-Physical System Research and Development

Jie Jiang[1], Xiaodong Wang[2,3], Pei He[2], Huan Yang[2], Pengpeng Liu[1], Yangming Guo[2,3]

[1]Troops 92942 PLA, Beijing
[2]School of Computer Science, Northwestern Polytechnical University, Xi'an Shaanxi
[3]Research and Development Institute of Northwestern Polytechnical University in Shenzhen, Shenzhen Guangdong
Email: 105537429@qq.com

Received: Aug. 4th, 2020; accepted: Aug. 18th, 2020; published: Aug. 25th, 2020

Abstract

Cyber physical system (CPS) is a complex system including computing, network and physical entities, known as the next generation network technology. This paper introduces the definition and characteristics of CPS in detail, and reviews the origin and development of CPS at home and abroad. Starting from the existing embedded system, network control system, Internet of things, and industrial control system, the paper discusses the existing theory and technology that can be used in CPS, and focuses on the analysis of the safety, reliability and credibility in the design of CPS. Based on the typical application of CPS such as intelligent transportation, intelligent power grid and intelligent medical treatment, and on the basis of summarizing the existing research results, this paper analyzes the key technologies of application-oriented CPS, points out the problems and challenges existing in the typical application, and looks forward to the research trend of CPS system.

Keywords

Cyber Physical System (CPS), Physical Space, Cyberspace, Security, Reliability, Credibility

赛博物理系统研究与发展综述

江　杰[1]，王晓东[2,3]，何　佩[2]，杨　欢[2]，刘鹏鹏[1]，郭阳明[2,3]

[1]中国人民解放军92942部队，北京
[2]西北工业大学计算机学院，陕西　西安
[3]西北工业大学深圳研究院，广东　深圳
Email: 105537429@qq.com

收稿日期：2020年8月4日；录用日期：2020年8月18日；发布日期：2020年8月25日

文章引用: 江杰, 王晓东, 何佩, 杨欢, 刘鹏鹏, 郭阳明. 赛博物理系统研究与发展综述[J]. 建模与仿真, 2020, 9(3): 345-356. DOI: 10.12677/mos.2020.93035

摘　要

赛博物理系统(CPS, Cyber-Physical System)是一个包含计算、网络和物理实体的复杂系统，被誉为下一代网络技术。本文详细介绍了CPS的定义与特点，回顾了CPS的起源及国内外发展历程。通过与现有的嵌入式系统、网络控制系统、物联网、工业控制系统等技术的对比，讨论可用于CPS的现有理论和技术，重点分析了CPS设计中的安全性、可靠性和可信性。立足于智慧交通、智能电网、智慧医疗等CPS典型应用，在总结已有研究成果的基础上，指出现有典型应用所存在的问题与挑战，展望了CPS系统的研究动向。

关键词

赛博物理系统，物理空间，赛博空间，安全性，可靠性，可信性

1. 引言

1992 年，NASA 率先提出并定义了 CPS (Cyber-Physical Systems)的概念。美国政府于 2006 年 2 月发布了《美国竞争力计划》，将 Cyber-Physical Systems (CPS)列为重要的研究项目；同年，美国国家科学基金会(National Science Foundation, NSF)把 CPS 技术列为其关键的研究领域之一，并与美国其他联邦机构合作举办了一系列关于 CPS 的研讨会。2007 年 7 月，美国总统科学技术顾问委员会(PCAST)在《挑战下的领先——竞争世界中的信息技术研发》报告中列出了八大关键信息技术，其中 CPS 就位列首位[1]。与此同时，很多著名院校和研究机构全力配合政府的 CPS 发展规划，开展的一系列针对 CPS 研究也取得了创新性的代表成果。如麻省理工学院的分布式智能机器人花园、宾夕法尼亚工程学院的汽车导航软件 GrooveNet，卡内基梅隆大学的智能电网等[2]。

2009 年，我国的四位院士向国务院提交了一份“有质量的 GDP”报告，提出将 CPS 作为我国未来信息技术发展方向的提议，该提议得到了国务院相关领导的充分肯定。国家自然科学基金、973 计划和 863 计划近年来已经把 CPS 的相关研究作为重要支持方向。2010 年 1 月 15 日，国家 863 计划信息技术领域办公室和专家组在上海举办了“信息－物理融合系统发展战略”论坛，重点讨论了国民经济领域的 CPS 应用系统范例，研究了国家急需的 CPS 应用系统战略布局。2012 年 4 月在北京举办的 CPS Week 上，来自国内外的专家学者均对 CPS 的发展和研究给予了高度关注和热烈讨论。另外，中国香港、中国台湾、日本、印度、巴西等国家与地区也相继把 CPS 作为未来 5~10 年信息技术领域的关键技术而展开研究。

2. CPS 的核心概念

2.1. CPS 的定义

目前，学术界对 CPS 还没有一个统一的定论，国内绝大多数文献将 Cyber-Physical System 简单翻译为信息物理系统。中航工业集团信息中心首席顾问专家宁振波则认为，Cyber 并不能简单翻译为信息，用赛博物理系统来表示 CPS 更加确切。这是因为 CPS 因控制而兴起，由于计算而发展壮大，借助互联网而

普及应用。溯本求源，Cyber 的实质是一种实现控制的特殊结构，是藉由信息，来控制物质、能量和信息，而“信息”只是被控制载体，并不是控制结构和控制机制，因而赛博物理系统则更能反映 CPS 的内涵[2]。

CPS 的概念最早由美国提出，2006 年美国国家自然科学基金会(NSF—The US National Science Foundation)的海伦、吉尔把 CPS (赛博物理系统)定义为[3]：“赛博物理系统是在物理、生物和工程系统中，其操作是相互协调的、互相监控的和由计算核心控制着每一个联网的组件，计算被深深嵌入每一个物理成分，甚至可能进入材料，这个计算的核心是一个嵌入式系统，通常需要实时响应，并且一般是分布的。”CPS 自提出以来就引起了学术界的广泛关注，各研究者及研究单位就自己的研究领域，给出了 CPS 的定义。

Lee 指出，CPS 是一系列计算进程和物理进程组件的紧密集成，通过计算核心来监控物理实体的运行，而物理实体又借助于网络和计算组件实现对环境的感知和控制[4] [5]。

Branichy 认为 CPS 是智能系统，从嵌入式系统出发，CPS 就是在物理进程上集成了生物特性的计算(computation)、通讯(communication)、控制(control)技术；从实现形式来看，CPS 就是具备安全可靠的“3C”能力的智能机器人系统[6] [7]。

何积丰院士在文献[8]中提出：“CPS，从广义上理解，就是在一个环境感知的基础上，深度融合了计算、通信和控制能力的可控可信可扩展的网络化物理设备系统，它通过计算进程和物理进程相互影响的反馈循环实现深度融合和实时交互来增加或扩展新的功能，以安全、可靠、高效和实时的方式监测或者控制一个物理实体。CPS 的最终目标是实现信息世界和物理世界的完全融合，构建一个可控、可信、可扩展并且安全高效的 CPS 网络，并最终从根本上改变人类构建工程物理系统的方式。”

以上的各种概念虽在出发点和定义形式上有所差异，但其核心离不开计算、通信、控制，其思想在于利用信息技术监测并控制物理世界，从而提供智能化的服务，是具有自感知、自记忆、自认知、自决策、自重构的一个新型智能的复杂系统[9]。CPS 的关键在于“Cyber”与“Physical”之间的交互与协同，即在感知的基础上深度融合 3C 技术，实现计算进程与物理进程之间的循环反馈，如图 1 所示[10]。

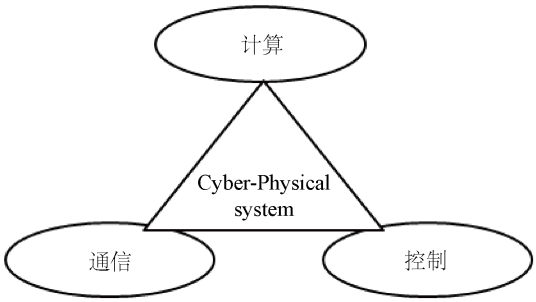

Figure 1. Curve: system result of standard experiment
图 1. CPS 的核心概念

2.2. CPS 的体系结构

体系结构是系统的灵魂，目前，绝大多数的研究都是基于层次结构的 CPS 体系架构。从功能角度出发，文献[11]给出了 CPS 的三层体系架构，如图 2 所示。

图 2 中，感知单元、决策单元、执行单元是 CPS 系统的基本功能模块，这三大功能模块结合反馈循环控制原理实现了 CPS 系统对物理空间与信息空间的协作与融合。底层的感知模块和控制模块构成物理实体层，提供感知信息并执行控制指令，赛博网络层是跨空间、跨系统的复杂动态网络，实现数据的传输和资源的共享，决策控制层结合用户需求，通过云计算、大数据等技术实现对数据的分析与处理，给

出执行单元控制指令。从技术层面看，CPS 系统由分布在不同位置的智能实体组成，任一实体都具有自感知、自记忆、自认知、自决策、自重构能力，其技术架构如图 3 所示。

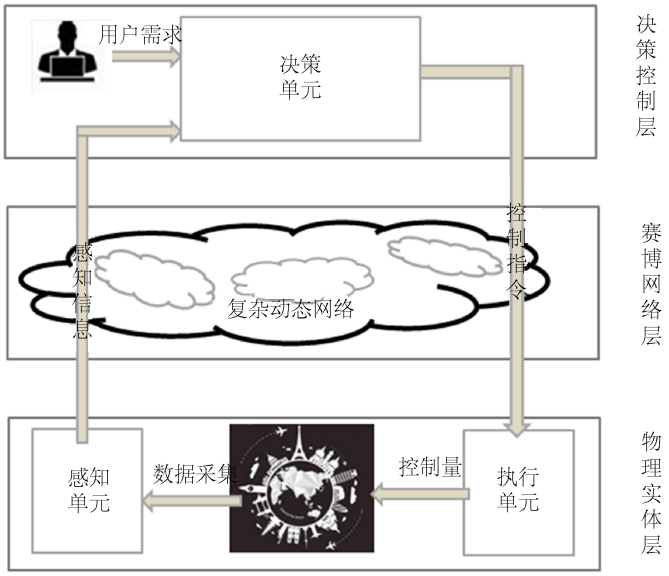

Figure 2. Curve: system result of standard experiment
图 2. CPS 的体系结构

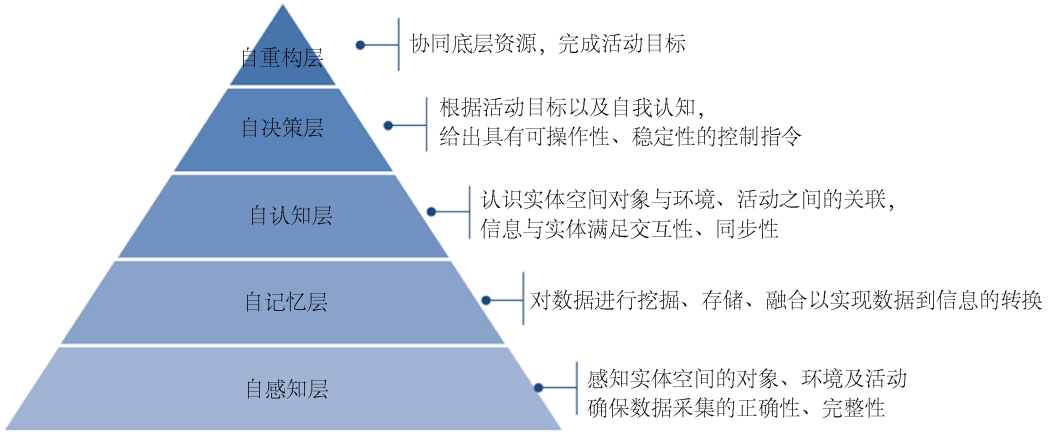

Figure 3. Curve: system result of standard experiment
图 3. CPS 的技术架构

由此可以得出，CPS 具有以下的特点：

1) 数据多样性：CPS 中蕴藏着大量物理世界的感知数据，这些数据来自各种各样的传感器，其数据类型及表现形式各不相同。感知数据是系统监测、认知、控制物理世界的关键依据。因此，CPS 需要对多样的感知数据具备获取、存储、认知、挖掘、分析的能力。

2) 网络开放性：CPS 构建了能够指导物理实体空间的网络环境，其网络是根据系统活动目标及所处环境动态变化的，结构具有不确定性。CPS 是复杂的大规模或超大规模系统，由多个子系统及功能模块组成，由于实时任务的不同，系统会自动根据目标进行优化配置，各子系统及功能模块会频繁地接入接出网络。

3) 异构异质：CPS 是一个异构的分布式系统，由异构的通信网络、异构的计算网络、异构的控制系统和异质的物理设备构成。

4) 时空约束性：CPS 具有严格实时性和空间约束，并且不同的构件可能具有不同的时间和空间粒度。CPS 的最终目标是实现物理空间与信息空间的协调统一，系统的计算进程和物理进程之间是双向的关系，计算进程控制物理进程，物理进程反馈数据给计算进程，物理实体空间与赛博网络空间在时间、空间上是相互约束的。

5) 自我认知能力：能够对数据进行筛选、特征提取，实现从数据到信息的转化，将机理模型和数据驱动模型相结合，保证数据的解读符合客观的物理规律，并从机理上反映对象的状态变化。同时结合数据可视化工具和决策优化算法工具为用户提供面向其活动目标的决策支持。

6) 学科间的融合：CPS 系统涉及多领域、多学科，不同学科之间处理问题的方式是不同的。例如控制领域是通过微分方程和连续的边界条件来处理问题，而计算则是建立在离散数学的基础上；控制对时间和空间都十分敏感，而计算则只关心功能的实现。CPS 须实现学科间的深度融合，提供统一的描述方式。

3. CPS 的属性与关键技术

安全性、可靠性、可信性是保障 CPS 有效、持续运转的三大关键属性，受到了 CPS 研究人员的高度关注[12]，在一些学术文章上，常常将这三者的概念混淆。Sean 认为，这只是一个人们对语义解释的问题，如果一个系统是不安全的，那么相应地，这个系统必然也是不可靠、不可信的[13]。常识告诉我们安全性、可靠性、可信性在某种程度上是相互重叠的。本节从技术层面出发，剖析它们之间的重叠与区别，并给出 CPS 在这三大关键属性上应重点关注的研究点。

3.1. 安全性

国际标准化组织(ISO)将安全性定义为设备或系统在正常状况或故障发生时或发生后能够避免造成物理环境中的危害，保持必要的整体性能稳定的能力。CPS 因应用领域的特殊性(如军事作战系统、医疗系统、电力系统、交通系统以及其他重大基础设施建设等)对系统的安全性要求很高，任何一个 CPS 系统均是实时的安全系统，必须在系统投入使用之前确保其安全性[14]。CPS 是复杂的新型的智能网络系统，其安全性不同于传统的互联网安全，要想确保 CPS 系统的安全，必须清楚系统面临的所有潜在威胁。基于层次化的 CPS 体系结构，本文分别从物理实体空间、赛博网络空间以及决策控制空间这三个方面各自的对象及功能展开对 CPS 的安全性讨论。

物理实体空间对应智能实体的自感知层，该层包含许多的基础设施：传感器、路由器、服务器等，为 CPS 的正常运行提供了最基本的保障。物理实体空间主要存在以下安全威胁：物理破坏、设备故障、线路损坏、外界干扰等威胁，这些实体的安全需要在物理过程中采用状态监测、健康状态评估、故障诊断、安全预警等技术来确保。同时，自感知层的传感器构成了无线传感器网络来获取物理空间的相关信息，因此在物理实体空间，不仅要考虑实体设备的安全，还需要考虑传感器网络的安全，要防止节点被控制、窃取、篡改、干扰、攻击等，需要使用必要的消息加密、密钥管理、入侵检测、安全路由、信任管理等机制进行节点的身份认证和数据的完整性验证。

赛博网络空间包含 CPS 的自记忆层、自认知层、自决策层，实现数据到信息的筛选、存储和融合，通过对数据和信息的挖掘与分析，认识物理实体以及物理实体与环境、活动之间的关联，并根据活动目标结合实时的环境状况给出可能的解决方案，可通过神经网络、机器学习、深度学习等人工智能的相关技术进行数据的特征提取、聚类分析，进而实现物理实体的自认知。赛博网络由大量的异构网络组成，

面临的威胁主要有拒绝服务攻击、路由攻击、恶意代码、用户隐私泄露、错误路径选择等[15]，不同的网络抵御安全威胁的方法不同，因而在设计赛博网络空间的安全结构时需要考虑各个子网络的兼容性与一致性，其安全任务主要包括节点间的身份认证、网络资源的访问控制、数据传输的保密性与完整性、远程接入的安全、路由系统的安全等。

决策控制空间对 CPS 进行管理与控制，其目标是达成整个系统的自重构能力[16]。当物理实体空间的实体健康状态出现衰退，造成输出出现偏差时，控制系统根据健康的偏差及自决策层提供的解决方案来调节实体的操作或者用系统当前可用的其它设备来替代故障实体，使得设备的输出维持在目标区间内。决策控制层面向用户应用，因 CPS 应用领域的不同相应的安全需求也不同，因此需要根据具体的应用提供具体的针对性的安全措施。例如，在医疗系统中需要保护病人的个人隐私，在交通系统中需要用户身份认证等。决策控制空间的安全对策主要有差异化的数据库安全服务、访问控制、用户隐私保护机制、安全软件等。

3.2. 可靠性

可靠性表示系统在规定的条件下和规定的时间内完成规定功能的能力，是 CPS 的重要特性之一，它表示系统所提供的服务完全可以被信赖的能力。在系统的整个生命周期内，任何的威胁都有可能影响到系统，从而导致系统的可靠性下降。按照层次化的管理方式，CPS 系统可从上到下依次划分为系统、任务、功能、资源四级对象。从对系统的影响程度来看，依据系统中对象有效性发展过程中的异常现象，可将对系统可靠性影响的因素分为缺陷、错误、故障、失效[17]。

资源缺陷是系统某种特性上的不足，缺陷有激活和休眠两种状态，当缺陷被激活时就会引起一个功能错误，缺陷的发现以及处理直接影响到错误的发生与否。功能错误是系统实际的操作结果与期望意图出现了一定程度的偏差，若错误的结果对系统功能产生影响，则会进一步导致任务故障，错误的发现与处理影响到故障的呈现与否。故障则是在系统界面上提交服务不成功的表现，即系统任务的失败，而故障的累积规模直接关系到系统失效发生的可能性。系统失效也就是系统进入了不能动作的瘫痪状态。

系统失效由资源缺陷一步步演化而来，如何提高系统资源保证能力，提高系统资源利用效率，提高系统资源协同能力是保障 CPS 可靠性的基础问题。预测与健康管理技术(PHM)为 CPS 的实现提供了基础性支撑，通过对资源进行测试诊断，结合资源共享、功能复用、系统重构等技术支撑系统的决策，从而达到系统能力的实现，保障系统任务的完成。

3.3. 可信性

ISO/IEC 15408 标准关于可信性的描述：一个可信的组件、操作或过程的行为，在任意操作条件下是可以预测的，并能很好地抵抗应用软件、病毒以及一定的物理干扰造成的破坏。Laprie 认为可信性是系统在任务开始时可用性给定的情况下，在规定的时间和环境内能够使用且完成规定功能的能力，即系统动则成功的能力[18]。CPS 在国家关键的基础设施中承担着十分重要的职能，系统的一个暂时的微小的故障都有可能给国家的公共安全、经济效益带来致命的影响，因而其可信性研究十分有必要。

CPS 所面临的可信性威胁主要来源于数据、网络以及人为因素三大方面。CPS 中的物理实体是带有人的智慧的，它能够通过对数据的学习，自主形成知识。一个面向具体应用的 CPS 系统的可信性主要问题就是系统所得到的数据的可信性分析。数据的可信性首先面临的是数据获取媒介(即传感器的可信性)，CPS 允许一定程度的传感器冗余，一旦某个传感器不能准确地工作，其他的传感器或传感器组仍然可以提供准确的数据信息，但问题是系统并不能预先知道哪些传感器是可信的，这就需要系统能够从所获得的冲突数据中推测出实际的情况。其次，一个 CPS 所拥有的传感器个数可能是成千上万的，产生的数据

量更是惊人，受到技术限制和环境的影响，CPS 数据难免会携带大量的噪声，如何从大量噪声数据中筛选出可信并且有意义的数据并进行传输、集成和存储是亟待解决的问题。

网络是 CPS 实现的基础，CPS 通过网络将各类传感器连接起来实现数据的感知与传送，并且完成对物理实体的远程控制。CPS 的网络需要满足极高的可信性，要能够迅速将数据、指令等信息发送到指定模块，要能够做到行为状态、行为结果可评估，行为异常可控制。一般来说，CPS 网络的可信性应首先满足安全性，保证网络牢不可摧，不能够随意被入侵、窃取甚至是破坏。同时，网络要满足可扩展性，CPS 是开放的系统，其工作环境具有高动态性，不同模块的接入与断开很频繁，必须使 CPS 网络满足动态的工作方式，在模块增加或减少后网络继续保持稳定安全，在少数攻击或模块连接失败的情况下，网络能够继续完成应有的功能。

CPS 的最终目标是为人提供更加高效、智能的服务。人是 CPS 系统的一个重要节点，不仅具有感知数据的能力，还能够进行分析、决策，从而控制物理实体。有研究表明，大约 50%以上系统的失效或崩溃是由人引起的。与以往的系统相比，CPS 的开放性更强，使用者与系统之间有着更加灵活的交互与控制，人对系统的干预和操作更是无处不在。因此，在 CPS 系统中必须给人一个具有唯一性、可区分的特征，系统在接受人的操作时必须验证其特性，并根据其知识水平、个人能力、操作熟练程度、相关经验等给予不同的权限，系统在收到指令时也必须验证操作者的身份，再决定是否响应操作。

4. CPS 技术与现有系统技术的关联

CPS 所涉及的领域很广，研究内容之间联系紧密，不可避免地成为一门多学科融合的新兴研究领域。CPS 技术吸收了嵌入式系统、无线传感网络、物联网、工业控制系统等技术的特点，但又不等同于这些系统。CPS 可以理解为基于现有的这些信息系统的高效能网络化智能信息系统，其与现有系统技术的主要区别与联系如图 4 所示。

Figure 4. Curve: system result of standard experiment
图 4. CPS 与现有系统技术的对比

4.1. CPS 与嵌入式系统

嵌入式系统(embedded system)是软件和硬件的高度结合体[19]。一般认为嵌入式是以应用为中心，以计算技术为基础，并且软硬件可裁剪，适用于系统对功能、可靠性、成本、体积、功耗有严格要求的专用计算机系统。传统的物理设备通过嵌入式系统来扩展和增加新功能，形成的系统基本上是封闭的系统；

而 CPS 则是开放的系统，它可以智能地根据所处的物理环境及相应的服务需求，通过网络连接随时随地动态添加相关的节点到系统之中。从控制角度来看，嵌入式系统侧重于静态控制，通常执行的是带有特定要求的预先定义的任务，难以实现随时间动态变化的问题的有效监控[20]；CPS 则侧重的是动态控制，系统实时感知物理环境的变化，通过自主的学习、计算、分析给出相应的决策，通过控制单元反向作用于物理实体。在嵌入式系统中，重点往往是更多的计算单元，极少关注计算单元和物理单元之间的交互；然而，CPS 对物理和计算单元之间的交互提出较高的结合与协同[21]。不同于传统的嵌入式系统，一个完整的 CPS 通常设计为一个个相互作用的元素的物理输入和输出，而不是作为独立的网络设备，CPS 是计算与物理成分的集成，相当于嵌入式系统 + 网络 + 控制，是嵌入式系统的发展方向和研究热点。

4.2. CPS 与无线传感网络

无线传感器网络(Wireless Sensor Networks, WSN)是一种分布式传感网络，由大量的静止或移动的传感器以自组织和多跳方式构成的无线网络，协作感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息，并最终把这些信息发送给网络的所有者。CPS 与无线传感网络都是动态的网络，没有严格的控制中心，节点可以随时移动、加入或者离开网络，任何节点的故障都不会影响整个网络的运行，具有很强的抗毁性。传感器网络实现了数据的采集、处理和传输三种功能，是一种开环的监测系统，可以简单看成是实现了 CPS 的感知器节点。相比之下，CPS 是一种闭环的监控系统，它的实现不仅需要感知器，还需要控制器，二者缺一不可[22]，无线传感网络技术的发展能够促进 CPS 的实现，然而，无线传感网络的节点并不直接适用于 CPS，这是因为 CPS 的节点不但具备具数据的采集、处理和传输功能，它还具备一定的智能化，能够根据当前任务与环境进行一定的分析计算，节点之间进行通信交互和协调，得出可行的解决方案[23]。

4.3. CPS 与物联网

物联网是通过射频识别(RFID) (RFID + 互联网)、红外感应器、全球定位系统、激光扫描器、气体感应器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络[24]。物联网的关键环节可以归纳为全面感知、可靠传送、智能处理。全面感知是指利用射频识别(RFID)、GPS、摄像头、传感器、传感器网络等感知、捕获、测量的技术手段，随时随地对物体进行信息采集和获取；可靠传送是指通过各种通信网络、互联网随时随地进行可靠的信息传输和共享；智能处理是指对海量的跨部门、跨行业、跨地域的数据和信息进行分析处理，提升对物理世界、经济社会各种活动的洞察力，实现智能化的决策和控制。

物联网是以物或者物理世界为中心，主要解决物品与物品，人与物品，人与人之间的互连，而 CPS 则是以服务为中心，主要解决的是物理实体与信息之间的有效融合，从而为人提供更智能化的服务。物联网所擅长的是无线连接，主要实现的是感知；CPS 实现的则是感控，CPS 不仅要具有感知功能，还需要实现控制，它对设备计算能力的要求远远超过了物联网的要求。物联网可以看作是 CPS 的一种简约应用，因为物联网中的物品不具备控制和自治能力，通信也大都发生在物品与服务器之间，因此物品之间无法进行协同。

4.4. CPS 与工业控制系统

如今工业控制系统遍地开花，但是这些控制系统基本是封闭的系统。工业控制网络大都采用工业控制总线进行通信，网络内部各个独立的子系统或者说设备很难通过开放总线或互联网进行互联，而且设备之间的通信功能比较弱[25]。CPS 则把通信放在与计算和控制同等的地位上，这是因为 CPS 强调的分

布式应用系统中物理设备之间的协调是离不开通信的。CPS 对网络内部设备的远程协调能力、自治能力、控制对象的种类和数量，特别是网络规模上远远超过现有的工业控制网络。

5. CPS 的典型应用及挑战

从 CPS 的提出发展到今天，理论和技术方面都取得了一系列的研究成果，在实际应用方面，目前 CPS 已在航空航电、交通、电力、医疗、农业等人类生活的方方面面展开了其应用研究。本节将详细分析 CPS 在智慧交通、智能电网、智慧医疗上的典型应用，在分析研究现状的基础上指出 CPS 在面向不同的实际应用时的技术难点与面临的挑战。

5.1. 智慧交通

借助 CPS 技术，交通系统围绕交通运输基础设施网络、运载工具和客货运输的对象三要素，构建全面感知、泛在互联的智慧交通基础感知与控制网络系统，实现以数据为中心的交通系统的协调管控与创新服务[26] [27]。Chellappan S 深入分析了面向车辆管理监测的 CPS，认为车辆管理是一个社区内的基于 P2P 模式的车辆的自主协作通信[28]。文献[29]结合 CPS 的特点，提出了基于感知层、计算层、控制层、网络层、应用层的层次架构模型。龚奏等人在中针对综合交通的各种问题，理论性探究了 CPS 在综合交通上应用的可行性[30]。虽然现在的交通系统已经初具一定程度的智能化，但离智慧交通还有相当长的距离，主要存在下列的挑战与限制，CPS 关键在于物理(离散)与信息(连续)的深度融合，目前仍然没有相应的描述语言和软件工具来正确有效地建立这种 CPS 模型。智慧交通包含基础设施建设、环境监测、信息服务、运输组织、行业管理、支撑保障等多各系统，各系统有独立的管理运行模式，交通 CPS 应以智慧出行、智慧物流、智慧关机为目标，深度融合各个子系统，实现资源优化配置，进一步提高交通的智能化。

5.2. 智能电网

传统的电网是按照模拟技术设计的，适应不了数字化社会的需求，在配电方面缺乏实时的监测和资产管理，难以达到持续的供需平衡，电网利用系数低下，不能满足节能减排和可持续发展的要求。将 CPS 技术应用于电网建设能够实时监测发电、配电、输电、供电、用电等每一个节点，对电网信息进行整合分析，保证从供电设备到用电设备之间每一点上电流和信息的双向流动，实现电力系统运行的优化管理[31] [32]。电力系统是现代社会的关键性基础设施，一旦受到网络攻击，后果不堪设想，电力 CPS 中电网的生产管理和调度控制高度依赖信息系统，网络攻击和信息系统的不正常工作状态均会威胁电网安全。Proceedings of the IEEE 以此为主题，深入讨论了 CPS 中网络攻击的实现模式与安全防护体系[33] [34]。同时，电网的自愈性[35]也是至关重要的，智能电网要实现在很少或者无人工干预的情况下，满足几乎不中断对用户供电服务的前提下，隔离系统中有问题的元件，进行电力资源的整合与配置[36]，使系统迅速恢复到正常运行状态。

5.3. 智慧医疗

IBM 最先提出智慧医疗的概念，设想通过打造健康档案区域医疗信息平台，充分利用先进的 CPS 技术，实现医疗患者与医疗人员、医疗机构、医疗设备之间的信息互联、共享协作、科学诊断以及公共卫生的预防，推动医疗服务的智能化发展[37] [38] [39]。目前，智慧医疗的基础架构已经初具规模，大多数医院都建有完善的 HIS (医院信息系统，包括医院管理信息系统(HMIS)和临床信息系统(CIS)、LIMS (实验室信息管理系统)、PACS/RIS (影像归档和通信系统) [40]，配合医生工作站、电子病历和处方、网上传输和查询系统实现医疗信息的共享。但这只是实现了信息层面的共享，未来，与人体传感器网络[41]相关

的产品及设备，例如智能药瓶、胶囊型检测机器人、机器人手术辅助系统、远程手术设备的研发将成为CPS在智慧医疗上的发展方向。

6. CPS的研究热点

CPS的最终目标是实现服务的智能化，其核心在于使任意一个物理实体具有人的智慧，能够自主获取数据，通过分析、学习而形成知识，并通过网络实现与其他节点的通讯交互，结合外界信息与自身的知识，各节点之间相互协作共同达到服务目标。CPS实现的基础是数据的获取，现有的数据都是通过传感器直接采集然后传送给数据处理中心，这给数据处理带来了极大的不便。智能传感器将成为未来CPS研究的热点问题，它不同于传统的传感器。智能传感器由传感器与微处理器相结合而成，充分利用计算机的计算和存储能力，结合神经网络、人工智能、深度学习等技术，使传感器具有分析、判断、学习的能力，能够对传感器的原始数据进行处理并对传感器的内部行为进行调节，使采集的数据更加有效。

另外，CPS的测试验证是系统投入使用的必要前提，也是制约CPS发展的主要因素。目前，一些小型的简单CPS系统已经投入使用。如何保证复杂的大规模CPS应用的成功建设和实施是一个新的挑战，CPS设计实践中的测试与验证将扮演极为重要的角色。不同于以往的系统，CPS本身具有随机性，这无疑增加了CPS系统测试与验证的难度。通过测试与验证确保系统的安全性、可靠性、可行性，应从以下两个方面着手：

1) 针对CPS构建过程中的技术难点，确保技术上的可行性，如从多元数据到信息的转化、网络节点的接入与接出、物理空间与赛博空间的时空统一、网络安全保障等技术问题进行建模和评估；

2) 针对已有的简单CPS应用，对系统中的物理设备假定各种可能出现的环境状况，进行测试与验证，进一步构建不同系统之间相互系统作用的混合系统模型，实现跨平台、跨地域、跨范围的大规模的CPS系统。

致　谢

国家某重点科研项目(MJ-2016-S-42, MJ-2018-S-34)，国防基础科研计划项目，国网浙江省电力有限公司科技项目(2020年)，陕西省创新能力支撑计划项目(2019PT-03)以及全军共用信息系统装备预研专用技术项目、装备预先研究项目(共用技术)。

参考文献

[1] 王军. 换个角度理解信息物理系统[J]. 智慧工厂, 2019(8): 20.

[2] 宁振波. CPS的精义. 工业4.0100术语 [Z].

[3] 郭楠, 贾超. 《信息物理系统白皮书(2017)》解读(上) [J]. 信息技术与标准化, 2017(4): 36-40.

[4] 郭楠, 贾超. 《信息物理系统白皮书(2017)》解读(下) [J]. 信息技术与标准化, 2017(5): 42-47.

[5] Lee, E.A. and Seshia, S.A. (2010) An Introductory Textbook on Cyber-Physical Systems. *Proceedings of the* 2010 *Workshop on Embedded Systems Education*, Scottsdale, October 2010, 1-6. https://doi.org/10.1145/1930277.1930278

[6] Branicky, M. (2008) CPS Initiative Overview. IEEE, Washington DC.

[7] Baheti, R. and Gill, H. (2011) Cyber-Physical Systems. IEEE, Washington DC.

[8] 何积丰. Cyber-Physical Systems [J]. 中国计算机学会通, 2010, 6(1): 25-29.

[9] Lee, J. (2015) Industrial Big Data. The Revolutionary Transformation and Value Creation in Industry 4.0 Era. China Machine Press, Beijing.

[10] Wang, Z.J. and Xie, L.L. (2011) Cyber-Physical System: A Survey. *Acta Automatic Sinica*, **37**, 1157-1156.

[11] Tan, Y., Goddard, S. and Perez, L.C. (2008) A Prototype Architecture for Cyber-Physical Systems. *ACM SIGBED Re-*

view, **5**, Article: 26.

[12] Banerjee, A., Venkatasubramanian, K.K., Mukherjee, T. and Gupta, S.K.S. (2012) Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber-Physical Systems. *Proceedings of the IEEE*, **100**, 283-299. https://doi.org/10.1109/JPROC.2011.2165689

[13] 惠战伟, 黄松, 谈利群. 任务关键软件可信性评测及影响因素的研究综述[C]//中国计算机学会. 2008 年中国计算机学会体系结构专委会学术年会(ACA'08)论文集, 2008: 116-120.

[14] Tang, H., Tan, F., Song, B., *et al*. (2011) Cyber-Physical System Security Studies and Research. *Multimedia Technology* (*ICMT*), Beijing, July 2011, 4883-4886.

[15] Fletcher, K.K. and Liu, X.F. (2011) Security Requirements Analysis, Specification, Prioritization and Policy Development in Cyber-Physical Systems. 2011 *5th International Conference on Secure Software Integration and Reliability Improvement-Companion*, Jeju Island, 27-29 June 2011, 106-113. https://doi.org/10.1109/SSIRI-C.2011.25

[16] Govindarasu, M., Hann, A. and Sauer, P. (2012) Cyber-Physical System Security for Smart Grid. PSERC Publication, New York.

[17] 赵宁社, 王国庆, 王恒. 一种面向需求的综合化系统健康度量方法[J]. 计算机工程, 2011, 37(21): 267-269, 272.

[18] Ma, L., Yuan, T., Xia, F., *et al*. (2010) A High-Confidence Cyber-Physical Alarm System: Design and Implementation. 2010 *IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber*, *Physical and Social Computing*, Hangzhou, 18-20 December 2010, 516-520. https://doi.org/10.1109/GreenCom-CPSCom.2010.75

[19] 张晶, 增闲云. 嵌入式系统概述[J]. 电测与仪表, 2002, 39(4): 42-44.

[20] Rammig, F.J. (2008) Cyber Biosphere for Future Embedded Systems. In: Brinkschulte, U., Givargis, T. and Russo, S., Eds., *Software Technologies for Embedded and Ubiquitous Systems*, *SEUS* 2008, *Lecture Notes in Computer Science*, Springer, Berlin, 245-255. https://doi.org/10.1007/978-3-540-87785-1_22

[21] Shi, J., Wan, J., Yan, H., *et al*. (2011) A Survey of Cyber-Physical Systems. 2011 *International Conference on Wireless Communications and Signal Processing* (*WCSP*), Nanjing, 9-11 November 2011, 1-6. https://doi.org/10.1109/WCSP.2011.6096958

[22] Tricaud, C. and Chen, Y.Q. (2009) Optimal Mobile Actuator/Sensor Network Motion Strategy for Parameter Estimation in a Class of Cyber Physical Systems. 2009 *American Control Conference*, St. Louis, 10-12 June 2009, 367-372. https://doi.org/10.1109/ACC.2009.5160289

[23] Tang, L.A., Yu, X., Kim, S., Han, J.W., Hung, C.-C. and Peng, W.-C. (2010) Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems. 2010 *IEEE International Conference on Data Mining*, Sydney, 13-17 December 2010, 1079-1084. https://doi.org/10.1109/ICDM.2010.63

[24] Oleshchuk, V. (2009) Internet of Things and Privacy Preserving Technologies. 2009 1*st International Conference on Wireless Communication*, *Vehicular Technology*, *Information Theory and Aerospace & Electronic Systems Technology*, *Aalborg*, 17-20 May 2009, 336-340. https://doi.org/10.1109/WIRELESSVITAE.2009.5172470

[25] 任磊, 任明仑. 基于社会信息物理系统的智慧制造资源组织模式[J]. 中国科技论坛, 2017(7): 118-125.

[26] 雷志鹏. 论发展智慧交通的任务和措施[J]. 新丝路, 2016(1): 38-39.

[27] 邓玉勇, 李璨, 刘洋. 我国城市智慧交通体系发展研究[J]. 城市, 2015(11): 68-73.

[28] Chellappan, S. and Madria, S.K. (2008) Networked Automotive Cyber Physical Systems: Applications, Challenges and Research Directions. *National Workshop on High-Confidence Automotive Cyber-Physical Systems*, Troy, 3-4 April 2008, 55-58.

[29] 汪治华, 张亚杰, 杜凯. 交通 CPS 体系结构设计[J]. 公路交通科技, 2012, 29(S1): 142-146.

[30] 龚奏, 李苏剑, 邢恩辉. 综合交通信息物理系统研究[J]. 计算机科学, 2014, 41(z2): 43-50.

[31] 陈恩黔, 楼书氢, 陈奔. 国外智能电网的研究概况及在我国的发展前景[J]. 中国电力教育, 2011(18): 90-91.

[32] 梁云, 黄莉, 胡紫巍, 李沛. 面向未来智能配用电的信息物理系统: 技术、展望与挑战[J]. 供用电, 2018(3): 1-8.

[33] Mo, Y.L., Kim, H.-J.T., Brancik, K., *et al*. (2012) Cyber-Physical Security of a Smart Grid Infrastructure. *Proceeding of the IEEE*, **100**, 195-209. https://doi.org/10.1109/JPROC.2011.2161428

[34] Siddharth, S., Adam, H. and Manimaran, G. (2012) Cyber-Physical Security for the Electric Power Grid. *Proceedings of the IEEE*, **100**, 210-224. https://doi.org/10.1109/JPROC.2011.2165269

[35] 郭文花, 张学军. 一种基于 CPS 的多源配电网故障定位与隔离方案[J]. 自动化技术与应用, 2016, 35(1): 82-86.

[36] 庄伟, 牟龙华. 智能配电网信息物理融合保护系统的研究[J]. 电力系统保护与控制, 2012, 40(4): 113-118.

[37] Earth Application. National Space Biomedical Research Institute.

[38] National Space Biomedical Research Institute (NSBRI). Earth Application. https://ntrs.nasa.gov/search.jsp?R=20140010662

[39] 方媛, 林德南. 智慧医疗研究综述[J]. 新经济, 2014(19): 70-72.

[40] 邱扬. 智慧医疗平台设计和应用[J]. 医学信息学杂志, 2015, 36(11): 16-19.

[41] 黄辰, 潘永才, 李可维, 等. 基于传感器聚类数据挖掘的物联网智慧医疗模型设计[J]. 传感器与微系统, 2014, 33(4): 76-79.