

# 信息物理系统研究

专 业 就 是 实 力

2015年06月 第 1 期 总第 2 期

内部资料 注意保存

## 本期主题

信息物理系统的发展现状、质量风险及  
应对策略建议

赛迪信息物理系统测评实验室 主办

北京赛迪信息物理系统测评实验室有限公司（中国软件评测中心），隶属于工业和信息化部中国电子信息产业发展研究院，现有员工 120 人，其中博士和硕士人数达到 88 人。公司紧跟产业发展和市场需求，历经 25 年发展，在技术发展与融合、发展与对抗的背景下，在国家重点项目的支撑下，以及在院“软硬结合、转型提升”的方针指导下，测评业务经历了软件产品与系统测试、电子系统可靠性测评到信息物理系统全生命周期的质量保障测评。公司专注于测试标准、测试技术、测试工具和测试公共服务平台等专业测评技术研究，面向移动终端、云计算、物联网、工业控制、数控机床、汽车电子、智能传感器、光伏等不同领域，为基于信息物理系统的国家基础设施提供第三方测评服务。

2014年11月3日，北京赛迪信息物理系统测评实验室有限公司（中国软件评测中心）所申报的“信息物理系统测评北京市工程实验室”，在北京市发改委2014年市级工程研究中心和工程实验室评审中脱颖而出，通过认定。该工程实验室的申报工作受到了赛迪研究院罗文院长、黄子河副院长，以及中心骆俊瑞总工、刘法旺常务副主任的高度关注和大力支持。

在我国“信息化和工业化深度融合”的战略发展背景下，工业和信息化部部长苗圩指出，两化深度融合是我国工业的4.0，而信息物理系统是实现工业4.0的基础。信息物理系统是在感知基础上，融合了计算、通信和控制能力的可控、可信、可扩展的网络化系统，广泛应用于工业控制系统、智能电网、智能交通系统、智慧城市等国家基础设施建设中，其安全可靠运营涉及国计民生和国家安全。

中国软件评测中心经过25年发展，服务范围已经从软件拓展到电子系统，进一步提升到融合了“感、联、知、控”特征的信息物理系统，不断践行将传统离线的测试转变为连续的、实时的、在线的、自动化的全生命周期的系统测评。信息物理系统测评北京市工程实验室的成功认定，中心将重点通过加强理论研究、搭建基础环境、研制标准体系、研发测评工具，以及建设公共服务平台向甲乙双方提供客观、科学、公平、公正的第三方测评服务和共性技术支持，保障涉及国家安全和国计民生的关键基础设施的安全可靠运行。

## 『刊首语』

信息物理系统（Cyber-Physical System，简称 CPS）是一个在环境感知的基础上，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，它通过计算进程与物理进程相互影响的实时反馈循环实现信息世界与物理世界的深度融合和交互。CPS 的概念一经提出就受到了全世界范围内的广泛关注。占据 CPS 技术的国际领先地位被认为是国家未来科技竞争力和振兴工业制造业的关键所在。无论是美国的“先进制造业”战略、德国的“工业 4.0”战略、英国的“高价值制造”战略、欧盟的“第八框架计划——2020 地平线计划”，还是中国的“两化深度融合”战略与“中国制造 2025”，都以新一代信息技术与传统产业的深度结合作为突破点，而 CPS 理论与技术则是其实现的基础。

当前广泛使用的电力网络、交通网络、通信网络、能源网络、空管网络、制造网络等关键基础设施均具备信息物理系统的特征。CPS 的广泛应用使其可靠性与安全性越发重要，一旦系统发生故障或遭到攻击，由于系统的互联互通互操作，故障的传播将会产生巨大的连锁影响。目前由于对 CPS 故障规律认识不够、未能进行有效测评与验证，导致故障、事故频发，甚至造成重大损失和人员伤亡的例子时有发生。实践表明，只有通过在系统全寿命周期开展有效的质量保障工作，充分利用测评理论与技术，及时发现系统缺陷或漏洞并采取补偿措施和风险管理手段，扼制故障和事故的发生，才能保障这些涉及国计民生和国家安全的系统安全可靠运行。

本期以“信息物理系统的发展现状、质量风险及应对策略建议”为主题，介绍了 CPS 的典型相关系统、主要特征和应用领域；概述了 CPS 的质量特性与质量风险因素，分析了典型事故案例和存在质量风险因素的原因；提出了应对策略和建议措施。



# 目 录

## CONTENTS

### 本期主题：信息物理系统的发展现状、质量风险及应对策略建议

#### 一、信息物理系统的发展现状

|                      |    |
|----------------------|----|
| 1.1 CPS的典型相关系统 ..... | 1  |
| 1.2 CPS的主要特征 .....   | 8  |
| 1.3 CPS的应用领域 .....   | 11 |

#### 二、信息物理系统的质量风险

|                        |    |
|------------------------|----|
| 2.1 CPS的质量特性 .....     | 12 |
| 2.2 CPS的质量风险因素 .....   | 13 |
| 2.3 CPS的典型事故案例分析 ..... | 17 |
| 2.4 CPS存在质量风险的原因 ..... | 20 |

#### 三、应对策略建议

|                |    |
|----------------|----|
| 3.1 政策导向 ..... | 22 |
| 3.2 建议措施 ..... | 24 |

## 本期主题：

# 信息物理系统的发展现状、质量风险及应对策略建议

## 一、信息物理系统的发展现状

信息物理系统（Cyber-Physical System，简称CPS）可定义为一个在环境感知的基础上，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，它通过计算进程与物理进程相互影响的实时反馈循环实现信息世界与物理世界的深度融合和交互。因此，除传统的物理系统工程技术外，CPS还包含了将来无处不在的智能感知、网络通信、大数据、云计算、智能控制等ICT技术，并通过两种技术的融合，涌现出新的功能。不同于物联网的物-物相连，CPS还通过计算、通信等信息系统实现对物理系统或物理过程的控制，改变并重新调整了我们与物理世界的交互方式。

### 1.1 CPS的典型相关系统

通过《信息物理系统研究》第一期对CPS的概念、发展历程和技

术挑战的分析可知，CPS的产生是科技与经济发展共同驱动的产物，并不是凭空出现，一蹴而就的。近年来，随着ICT（Information Communication Technology，信息通信技术）技术的飞速发展，尤其是微电子技术 with 互联网技术的广泛应用，出现了诸如软件密集系统、嵌入式系统、过程控制系统、无线传感器网络、物联网、云计算等新型开放式的、大规模的、复杂的现代工程系统。这些系统都是新一代信息技术与传统物理工程系统相融合的产物，是CPS发展的初级阶段。下面将分别介绍一下这些系统，可加深我们对信息物理系统发展现状的认识。

#### 1.1.1 软件密集系统

根据IEEE Std 1471-2000对软件密集系统的定义，所谓软件密集系统即系统中的软件在系统研制费用、研制时间或系统功能特性等一

个或多个方面占主导地位的系统。随着科学技术的发展，越来越多的设备从电子机械密集型逐渐向软件密集型发展。引起软件规模增长有三个原因：第一是系统功能的扩大，由此要求软件完成更多更复杂的功能；第二是硬件\软件功能分配有很大转移，软件在系统功能中所占比例从10%上升到35%；第三是系统希望通过软件改善人机接口，以获得更好的交互方式。

现有电子系统中软件的主要功能是数据的采集、传输、计算和显示，其特征是“面向数据”。区别于这类系统，软件密集系统具有“面向信息”和“面向知识”的特点。数据是一串数字或字母。当合适的数据在合适的时候放在合适的地方，才可称之为信息。比信息层次更高的是知识，它不仅包含反映客观对象特征的事实，而且包含从事实之间的关系中提取新事实的推理规则。软件密集系统将帮助使用者根据不同使用场景做出相应决策，而不是仅仅提供数据。以新一代的航空电子系统为例，在飞行中根据即时情况重新规划航路，在作战时鉴别目标的优先级顺序，建议

合适的攻击方式和武器发射程序。可以按任务类型和飞行员的意愿随时重新编排显示内容和格式。任何信息可迭加在全视场上或选择的某一部分上。

软件密集系统属于大规模复杂系统，以美国宇航局的软件系统为例，1963年水星计划系统200万条指令，1967年双子座计划系统400万条指令，1973年阿波罗计划系统1000万条指令，1979年哥伦比亚航天飞机系统4000万条指令。但是一万条指令的复杂度却不仅仅是100条指令复杂度的100倍。随着软件密集系统规模的增长，软件密集系统的可靠性问题逐渐凸显，成为限制其发展的难点。

### 1.1.2 嵌入式系统

根据英国电气工程师协会(U.K. Institution of Electrical Engineer)的定义，嵌入式系统为控制、监视或辅助设备、机器或用于工厂运作的设备。嵌入式系统(Embedded System)实际上是嵌入式计算机系统(Embedded Computer System)的简称，目前被广泛理解为是一种“完全嵌入受控器件内部，为特定应用而设计的专用计算

机系统”。它以应用为中心、以计算机技术为基础，软硬件可以裁剪，可适应系统对功能、可靠性、成本、体积、功耗等严格要求。一般来说，嵌入式技术的应用与发展使我们能够将计算和通信功能按照特定的方式添加到物理系统之上，认为是CPS的重要基础之一。汽车电子系统与机械系统的成功结合就是早期成功的案例。计算机控制的汽车引擎的出现对低油耗与低排放汽车的出现都起到了关键作用。嵌入式系统是一种典型的软硬件综合系统，例如现代的机器人、航空器的飞行控制系统，通讯网络的智能化控制器、电网系统的智能化控制装置、汽车的自动挡传动装置、微型计算机控制的家电产品等。

嵌入式系统的软硬件均是面向特定应用对象和任务设计的，具有很强的专用性。需要嵌入式系统提供的功能以及面对的应用和过程都是预知的、相对固定的，所以嵌入式系统在不同的使用场景下，通常会从不同的使用需求出发，采取不同的实现方案，即使逻辑上的系统结构相同，在物理组成上也会有所不同。一般来说，嵌入式系统包括

机电装置，对实时性要求很高。有些系统，如MEMS（微机电系统）反馈环相对封闭，还可能面临在资源有限的情况下的优化问题。

嵌入式系统的失效通常是软件失效与硬件失效耦合作用的结果。硬件操作环境的改变引起软件失效，如内存模块局部故障是一种操作环境的异常配置，可能会使软件在这种异常环境下造成失效。反过来说，嵌入式系统中软件失效也会影响到硬件。这主要是由于一个实际的具备容错特性的系统多数要借助于软件来实现，即软件的故障检测、重组等也将影响硬件的可靠性。

### 1.1.3 过程控制系统

以表征生产过程的参量为被控制量使之接近给定值或保持在给定范围内的自动控制系统称之为过程控制系统。这里“过程”是指在生产装置或设备中进行的物质和能量的相互作用和转换过程。表征过程的主要参量有温度、压力、流量、液位、成分、浓度、位置、尺寸等。通过对过程参量的控制，可使生产过程中产品的产量增加、质量提高和能耗减少。一般的过程控制

系统通常采用反馈控制的形式，这是过程控制的主要方式。

过程控制系统一般由以下几部分组成：被控制的过程（或对象）；用于过程参数检测的检测与变送仪表；控制器；执行机构；报警、保护和连锁等其他部件。过程控制系统的基本结构如图1所示。控制器根据系统输出量检测值 $Y(t)$ 与设定值 $R(t)$ 的偏差，按照一定的控制算法输出控制量 $u$ ，对被控过程进行控制。执行机构接受控制器送来的控制信息调节被控量，从而达到预期的控制目标。过程的输出信号通过过程检测与变送仪表，反馈到控制器的输入端，构成闭环控制系统。

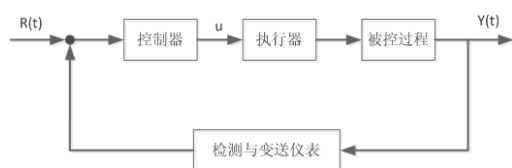


图1 过程控制系统的基本结构

过程控制系统中的被控过程、被控对象、被控量是多样的，明显地区别于运动控制系统。如：石油化工过程、冶金工业中的冶炼过程、核工业中的动力核反应过程等等，这些过程的机理不同，甚至执

行机构也不同。当然，由于被控过程、被控对象的多样性也决定了过程控制系统的控制方案必然是多样的。这种多样性包含系统硬件组成和控制算法以及软件设计。随着现代工业生产的发展，工业过程越来越复杂，对过程控制的要求也越来越高。传统的模拟式过程检测控制仪表已经不能满足控制要求，因而采用计算机作为控制器组成计算机过程控制系统。从控制方法的角度看，有单变量过程控制系统，也有多变量过程控制系统。同时，控制算法多种多样，有PID控制、复杂控制，也有包括智能控制的先进控制方法等等。

#### 1.1.4 无线传感器网络

无线传感器网络(Wireless sensor network, WSN) 主要由部署在监测区域内大量的微型传感器节点构成，是通过无线通信方式形成的一个多跳自组织网络。无线传感器网络中的传感器节点以协作的方式感知、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。

WSN的发展得益于微机电系

统(Micro-Electro-Mechanism System, MEMS)、片上系统(System on Chip, SoC)、无线通信和低功耗嵌入式技术的飞速发展,其概念的产生与物联网几乎在同一时期。即1998年,美国在先进国防研究项目局(ARPA)的一个研究项目中第一次提出无线自组织传感器网络的概念。无线传感器网络所具有的众多类型的传感器,可探测包括地震、电磁、温度、湿度、噪声、光强度、压力、土壤成分、移动物体大小、速度和方向等周边环境多种多样的现象。潜在的应用领域可以归纳为:军事、航空、防爆、救灾、环境、医疗、保健、家居、工业、商业等领域。

相对于静态传感器网络来说,通信可以使用有线通路实现,有固定、可靠的电源。而移动的无线传感器网络要在节点的供电、通信、计算和存储等资源受限的情况下、实现高能效、可靠的无线通信通道。因此,它具有网络节点多(根据需求可能包含多达上千个甚至上万个节点)、高冗余、网络自组织、拓扑结构动态性强、空间位置寻址(IEEE802.15.4/ZigBee协议)

和以数据为中心的特点。无线传感器网络的节点分布相对稠密,从而导致节点更容易出现故障,节点故障和环境干扰造成网络的拓扑结构经常改变。

#### 1.1.5 物联网

物联网的英文名称为“Internet of Things (IoT)”,是指通过射频识别(Radio Frequency Identification, RFID)、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“物物相连”的网络。物联网是互联网的延伸,它包括互联网及互联网上所有的资源,兼容互联网所有的应用,但物联网中所有的元素(所有的设备、资源及通信等)都是个性化和私有化的。物联网主要解决物品与物品(Thing to Thing, T2T),人与物品(Human to Thing, H2T),人与人(Human to Human, H2H)之间的互连。但是与传统互联网不同的是,H2T是指人利用通用装置与物品之间的连接,从而使得物

品连接更加的简化，而H2H是指人之间不依赖于PC而进行的互连。因为互联网并没有考虑到对于任何物品连接的问题，故我们使用物联网来解决这个传统意义上的问题。

物联网是新一代信息技术的重要组成部分，也是21世纪信息化时代的重要发展阶段，近年来受到中国、美国、日本、韩国、德国、欧盟等国家的高度重视和得到了快速发展。目前的物联网通信大都发生在物品与服务器、物品与人之间，而物品之间的通信应用还较少。随着对传感器技术和智能嵌入式技术的应用，未来的物联网不仅仅提供传感器的连接，其本身也具有智能处理的能力，能够对物体实施智能控制。一般认为，物联网具有感知

层、网络层和应用层三层架构。也有学者认为还应在网络层和应用层之间包含处理层，即通过云计算等技术对海量信息进行处理，如图2。应用层是物联网与行业专业技术结合，满足行业需求，使“物物相连”的能力获得应用。因此，应用创新是物联网发展的核心。物联网的精神实质是提供不拘泥于任何场合，任何时间的应用场景与用户的自由互动，依托云计算、互联网和模式识别等技术，其应用领域将更加广泛，必将成为CPS的重要发展助力之一。

1.1.6 云计算

ISO/IEC17788 《云计算词汇与概述》（Information technology - Cloud Computing -

|     |          |          |          |          |          |          |
|-----|----------|----------|----------|----------|----------|----------|
| 应用层 | 远程<br>监控 | 异地<br>医疗 | 环境<br>监测 | 智能<br>家居 | 资源<br>探索 | 信息<br>检索 |
| 处理层 | 云计算      |          | 网格计算     |          | 并行计算     |          |
| 网络层 | 无线传感网    | 互联网      | 移动网络     | 局域网      | 广电网络     |          |
| 传感层 | 智能终端     | RFID设备   | 传感器节点    | 网关设备     | 移动设备     |          |

图2 物联网的层次架构

Overview and vocabulary) 对云计算的定义为：云计算是一种将可伸缩、弹性、共享的物理和虚拟资源池以按需自服务的方式供应和管理，并提供网络访问的模式。云计算模式由关键特征、云计算角色和活动、云能力类型和云服务分类、云部署模型、云计算共同关注点组成。云计算的关键特征为：广泛的网络接入、可测量的服务、多租户、按需自服务、快速的弹性和可扩展性、资源池化。云能力类型是根据资源的使用情况，对为云服务客户提供的云服务的功能进行的分类。有三类不同的云能力类型：应用能力类型、基础设施能力类型和平台能力类型。云服务类别是拥有相同质量集的一组云服务。一种云服务类别可对应一种或多种云能力类型。典型的云服务类别包括：基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。云计算角色和活动一般分为云服务客户、提供者和协作者。

自SaaS在20世纪90年代末出现以来，云计算服务已经经历了十多年的发展历程。云计算服务真正受

到整个IT产业的重视是始于2005年亚马逊推出的AWS服务，产业界认识到亚马逊建立了一种新的IT服务模式。在此之后，谷歌、IBM、微软等互联网和IT企业分别从不同的角度开始提供不同层面的云计算服务，云服务进入了快速发展的阶段。云服务正在逐步突破互联网市场的范畴。政府、公共管理部门、各行业企业也开始接受云服务的理念，并开始将传统的自建IT方式转为使用公共云服务方式，云服务将真正进入其产业的成熟期。

云计算有四类典型的部署模式：“公有云”、“私有云”、“社区云”和“混合云”。云服务一般来说包括IaaS、PaaS、SaaS三类服务。IaaS 是基础设施类的服务，将成为未来互联网和信息产业发展的重要基石。互联网乃至其他云计算服务的部署和应用将会带来对IaaS 需求的增长，进而促进IaaS的发展；同时，大数据对海量数据存储和计算的需求，也会带动IaaS的迅速发展。PaaS服务被誉为未来互联网的“操作系统”，也是当前云计算技术和应用创新最活跃的领域，与IaaS 服务相比，PaaS 服务

对应用开发者来说将形成更强的业务粘性，因此PaaS服务的重点并不在于直接的经济效益，而更着重于构建和形成紧密的产业生态。SaaS服务是发展最为成熟的一类云服

务。传统软件产业以售卖拷贝为主要商业模式，SaaS服务采用Web技术和SOA架构，通过网络向用户提供多租户、可定制的应用能力，大大缩短了软件产业的渠道链条，使软件

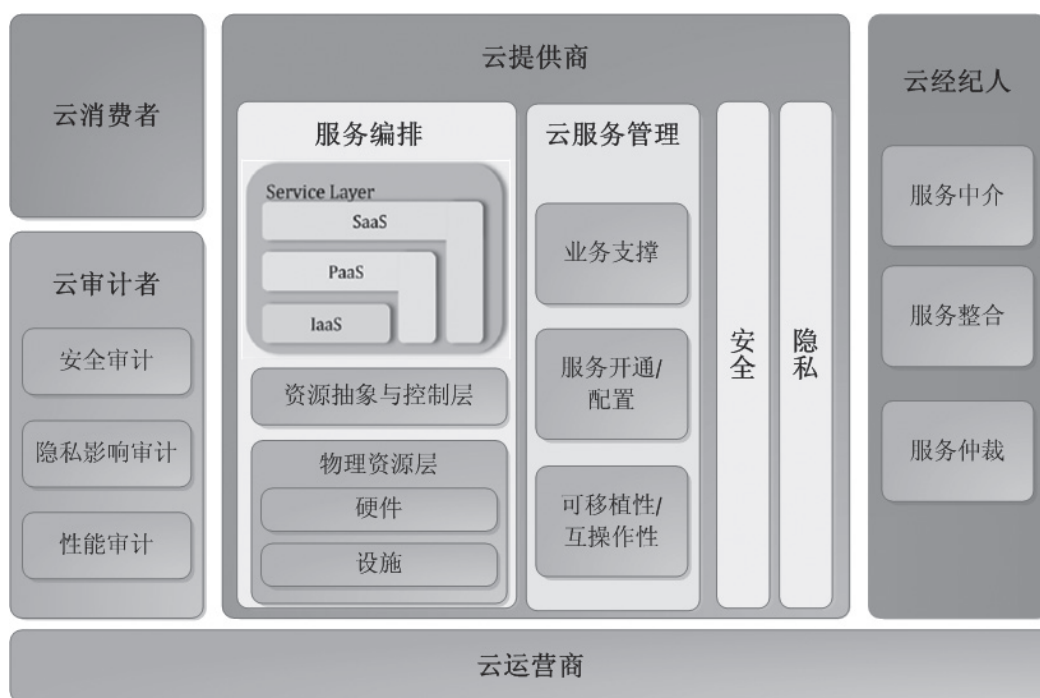


图3 云计算参考架构

提供商从软件产品的生产者转变为应用服务的运营者。

## 1.2 CPS的主要特征

CPS及其子系统，其结构在空间与时间维度上具有分布式、异构性、可扩展性、自组织性和自治性等特征，所处环境复杂多变，并可通过鲁棒控制实现具有实时性的综

合协调。CPS属于复杂系统，具有复杂系统的开放性、巨量性、进化涌现性、自组织性、层次性、非线性和脆性的共性特点。同时，CPS具有很多独特的特点，体现在信息物理高度融合、系统功能交互涌现、动态结构自主演化、内外状态深度感知、网络实时控制等方面。

### 1.2.1 信息物理高度融合

CPS的信息物理高度融合主要体现在两个方面，宏观上的“虚实结合”与微观上的“软硬不分”。虚实结合是指虚拟的信息世界和现实物理世界的结合，物理世界的特征和状态，可以跨越整个网络空间被实时、可靠、安全地传输至信息世界，使信息世界能够正确、全面的认知和分析物理世界的状态，并及时做出基于网络的控制决策。软硬不分是指，CPS中硬件与软件高度集成，软件被嵌入到硬件中，使其具有计算和通信的能力。在这一点上，CPS与嵌入式系统颇有神似，但仍有不同。两者的软硬件融合虽然都是为了增强物理设备的功能，但是CPS可实现将计算与通信单元嵌入并连接在物理系统或过程之上，通过网络通信与控制实现物理系统的协调同步，解决资源的有效利用等问题，以更好地适应周围不确定的、动态发展和变化的环境。

### 1.2.2 系统功能交互涌现

系统科学把整体才具有，孤立的部分及其总和不具有的特性称为涌现性。就系统自身而言、涌现性主要是由它的组成单元按照系统的

组织、连接方式相互作用、相互补充、相互制约而激发出来的，是一种组分之间的相干效应。CPS作为一类在时间和空间等维度上具有多重复杂性的复杂系统，系统功能交互涌现。以基于CPS的智能交通系统为例，城市交通系统是由道路系统、流量系统和管理系统组成的典型的、开放的复杂系统。不论是以交叉路口或区域对应于节点，还是以车辆作为节点，网络都具有非规则的结构和动态变化的拓扑结构。因道路状况、网络结构、信号灯控制、驾驶员的行为特征、甚至因基建施工和临时社会活动产生的交通拥堵等等复杂性因素交互作用，往往导致交通系统某种功能、行为的涌现。

### 1.2.3 系统结构动态演化

系统的结构、状态、特性、行为、功能等随着时间的推移而发生的变化称为系统的演化。一般来说，系统演化的动力有的来自系统内部，组分关联方式的改变，引起系统功能及其他特性的改变。系统演化的动力也来自外部环境。环境的变化以及环境与系统相互联系和作用方式的变化，都会导致系统整

体特性和功能的变化。

CPS是动态开放的，这体现在CPS可以动态地接受各类组件的接入和退出，自主获得每个接入单元的信息并能够随时控制该组件，从而有利于系统自身的动态调整和构建大规模复杂系统。同时，CPS能够自动排除或修复各种故障组件，以保证系统正常工作的能力，实现系统的全局性能优化。

CPS的演化是在内部动力和外部动力共同作用的结果。不同于其他系统的是，CPS是自主演化的，这主要体现在其具有高度的自组织性，能够在不影响整体系统结构功能的基础上实现系统结构的动态重组和重新配置，以满足不同的任务需求或适应外界环境的动态变化。其组件与子系统也都具有自适应、自配置、自维护、自优化和自保护能力，支持CPS完成自感知、自决策和自控制。

#### 1.2.4 内外状态深度感知

由于对智能感知技术的应用，CPS中蕴含着大量设备的运行数据，如基于CPS的智能电网系统中线温度、弧垂、振动、舞动等数据。这些数据是CPS得以监测、观

察、认知、控制自身状态的关键依据。由于SCADA系统（Supervisory Control And Data Acquisition，数据采集与监控系统）等自身监控系统的存在，CPS可以实时获取这些数据。通过对这些数据的采集、存储、传输、挖掘和处理能够实现对自身状态的深度感知。相对于传统系统，CPS不再需要人工干预和调整，节省资源消耗的同时提高了运行效率。同时，这也使得CPS能对自身运行过程中出现的或可能出现的问题作出迅速的反映，具有自我故障监测和前瞻性的预测能力。同时，CPS也能够从环境中获取数据，提取有效信息，如基于CPS的智能电网系统中输电线周围微气象数据等。

CPS以数据为中心，各个层级的组件与子系统都围绕数据融合向上提供服务，内外部数据沿着从物理世界接口到用户的路径上不断提升抽象级，用户最终得到全面、精确的信息，实现对内外部状态的深度感知。

#### 1.2.5 网络实时适时控制

大多数CPS的建立为了支持实时应用，如智能交通、智能电网、

石油管网等，以便及时了解物理设备的现状，通过网络化控制手段对物理设备和环境进行必要和高效的控制和干预。可以说，CPS连接着信息世界和物理世界，信息获取、传输、处理的实时性会影响到用户判断与决策精度，控制指令传输、执行的实时性会影响到任务能否正确执行、设备能够正确运行等各个方面，尤其体现在关键基础设施领域。因此，CPS对时间要求严格，传感模块能够实时感知环境变化，决策控制模块能够根据实时数据进行判决，实现对物理过程的实时控制，感知数据和控制指令能够在网络中实时传输。当然，CPS的实时性不仅体现在信号感知、计算以及控制等方面上。还体现在大量分布式异构设备在跨平台、跨空间范围上的实时响应，以及人机交互上。

除了实时性，适时性也是CPS区别于其他系统的特征。适时性指的是在CPS中，每个应用任务均具有其执行期限，在此执行期限内，任务必须完成，如果超过此期限，任务便是无意义的。

### 1.3 CPS的应用领域

CPS技术是新一代信息技术与传

统物理工程技术的多学科综合。它的应用范围十分广阔，涉及航空航天、石油石化、电力、水资源调度与污水处理、公路与轨道交通、先进制造、环境监测与灾害控制、远程医疗与辅助生活、城市管理、节能建筑和国防系统等重要基础设施的建设与管理，如现有的民航空中交通管理、业务运行及其广域信息管理系统，智能电网及其广域监测系统，石油油气管网及其SCADA系统，核电站仪控系统，轨道交通及其通信与监控系统，集散式工业控制系统，汽车电子与智能交通系统，工业机器人与智能制造系统，远程医疗系统与物联网、智慧城市等，如图4所示。

新一代科学与工程研究利用CPS将计算与物理单元进行更好的连接与融合，增强系统的自适应性、子系统或组成单元的自治性、系统的整体效能、可靠性、安全性；网络的广泛应用可以极大地降低建筑、制造等系统的运维成本。因此，这也极大地拓宽了CPS的应用维度，扩充人类行为能力与范围，例如：在事故、冲突或碰撞发生前的及时干预；提高机器人手术和纳米级制造

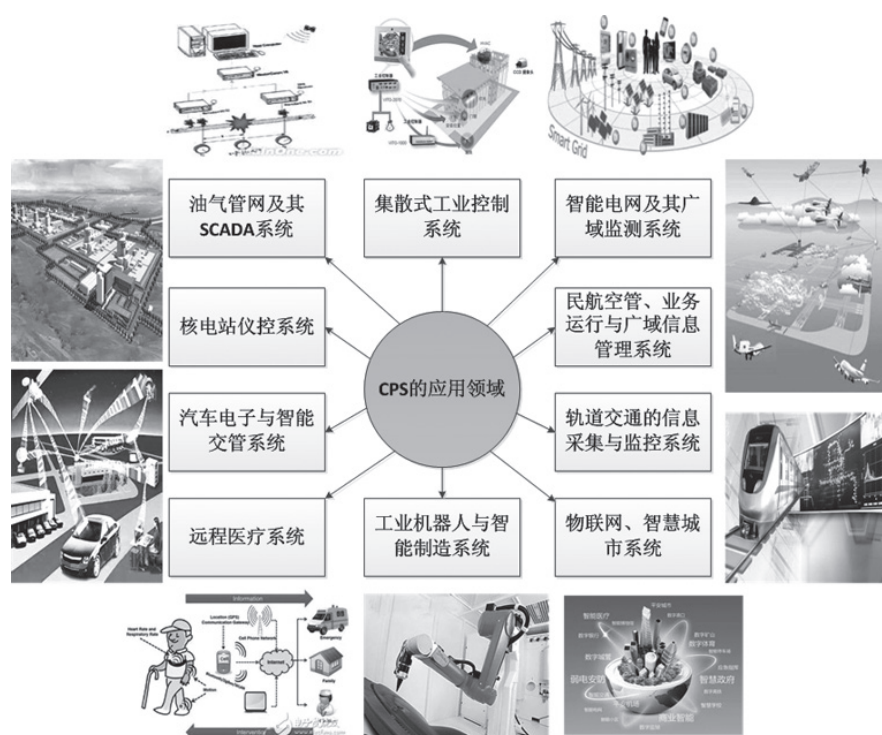


图4 CPS的应用领域示例

领域的操作精度；在危险的或人类难以到达的环境中的作业，如地球外太空探测、救援、灭火、深海勘探；空中交通管理或空战中的协调与调度；净零能耗的建筑的效能管理等。可以预见的是，随着移动互联技术更加广泛的应用，CPS技术将在智能制造、智慧城市等面向未来的工业信息化变革中发挥更加重要的作用。

## 二、信息物理系统的质量风险

### 2.1 CPS的质量特性

通常，产品质量是指反映产品

满足明确的和隐含需要的能力的特性总和。产品的质量是由过程形成的，过程是由一系列子过程（活动）组成的，包括产品生命周期各个过程，如规划过程、设计过程、制造过程、使用过程、报废处理过程等。QoS（Quality of Service，服务质量）最早源于网络流量工程领域，指的是网络满足给定业务合同的概率。网络QoS通常可以量化为带宽、延迟、抖动、丢失率、吞吐量等具体的性能指标。产品是用来提供一定的服务或业务的，因此用

服务质量衡量产品的服务满足要求的能力。

产品的质量特性可以划分为专用质量特性和通用质量特性两个方面。专用质量特性反映了不同产品类别和自身特点的特性特征。例如，对于飞机而言，其专用质量特性一般包含飞行速度、飞行高度、加速度、最大航程、载重等。通用质量特性可以反映不同类别产品均应具有的共性特征，一般包括可靠性、耐久性、安全性、环境适应性、维修性、测试性、保障性、可用性、经济可承受性、需求适应性、标准符合性、易用性、电磁兼容性、可信性、脆性与弹性等。通用质量特性与专用质量特性之间具有协调统一、相互促进和不断发展的关系。

CPS的质量是一项综合指标，是对硬件可靠、软件可信、信息安全、网络可靠、控制规则完备的水平，以及故障诊断、定位、恢复的水平的综合衡量，对各单独指标的测试与评价也是CPS运行质量测评的基础。

## 2.2 CPS的质量风险因素

CPS任何一个组成部分存在缺陷

和漏洞，都可能引起故障的发生，继而引发风险事件，导致严重的后果。“风险”是带来损失或伤害的一种情况，对风险的度量则是指对意外事件的可能性和对损害的严重程度度量。因此，CPS的风险是系统导致人身伤亡、财产受损及其他经济损失的自然灾害、意外事故和其他不测事件的可能性和严重程度。风险导致的事故危害等级可以从高到低分为人员伤亡、环境破坏、功能丧失、功能降级和安全隐患等级别。鉴于风险事件后果的严重性，我们应该在系统的论证、设计、研制、运维等全寿命周期各个阶段预防风险事件发生，并能实现制定有效措施减缓事件发生带来的影响。对风险源进行辨识、分析、度量、测试和评估是开展此项工作的重要手段。

我们将影响CPS质量的风险因素分为内因和外因两类。同时，还应考虑系统结构的因素，即系统组成单元之间的关系带来的某个或某些单元故障（包括缺陷、漏洞引起的失效或有效攻击事件）在系统内引起的故障的传播。而且，随着系统复杂性的增加，System of

Systems/Network of Networks这样的多子系统综合与协同作用的大规模复杂系统的出现,故障传播以“级联失效”方式出现。总之,CPS的系统缺陷、漏洞和环境条件等内外因素及其耦合是导致风险事件发生的主要原因。

### (一) 内因

内因是指引起CPS出现风险事件的系统内部因素。CPS的组成要素可以分为硬件、软件、网络结构、控制规则和人员五个方面,因此,系统的风险内因主要来自硬件故障、软件缺陷、网络漏洞或配置性能不足、运行规则不合理、系统架构不合理和人因失误等。

### (二) 外因

外因是指引起CPS出现风险事件的系统外部因素,可以分为环境因素、使用模式变化和外部攻击三类。

#### (1) 环境因素

环境是指围绕着某一事物(通常称其为主体)并对该事物会产生某些影响的所有外界事物(通常称其为客体),可分为自然环境和社会环境。

自然环境条件对于产品来说是

一个无法回避的、必须加以考虑的因素,是指系统在使用时的物理、化学和生物等条件,例如气候环境条件、生物环境条件、化学污染物、力学作用等,每一种环境条件由各种环境因素的不同等级参数值表示,如气候环境条件通常是由温度、湿度、气压、太阳辐射强度、沙尘、雨量等参数值组成。环境从各方面使产品性能劣化,如温度、生物和污染物破坏表面保护层;风沙、尘埃和生物剥蚀产品表面;机械振动冲击造成应力疲劳;大气中的盐和其他污染物引起或促进化学腐蚀;温度、湿度使电子元器件受损,产生绝缘击穿,接触器不导电、电阻值改变和电性能变坏等。

社会环境是指人类生存及活动范围内的社会物质、精神条件的总和,广义包括整个社会经济文化体系,狭义仅指人类生活的直接环境,按包含要素的性质和功能分为不同种类。具体而言,社会环境就是我们所处的社会政治环境、经济环境、法制环境、科技环境、文化环境等宏观因素。社会环境通过影响与CPS相关的人员,进而对CPS本身产生影响。社会环境的变化,如

政治经济形势的变化会影响人的生活，进而影响人的情绪和行为，导致人因失误的发生。另一方面，政治环境、经济环境和法制环境的变化，会影响CPS的功能、结构等，科技环境的变化，会对CPS相关的理论和技术产生影响，这些都会引起系统的演化，进而导致风险事件的发生。

### (2) 运行模式

CPS为完成不同任务，或使系统安全、经济、合理运行，需要经常变更系统的运行方式，由此相应地会引起系统结构或参数的变化。如，电力系统具有最大运行方式和最小运行方式等不同的运行方式。最大运行方式，是系统在该方式下运行时，具有最小的短路阻抗值，发生短路后产生的短路电流最大的一种运行方式。最小运行方式，是系统在该方式下运行时，具有最大的短路阻抗值，发生短路后产生的短路电流最小的一种运行方式。在设计变、配电站选择开关电器和确定继电保护装置整定值时，往往需要根据电力系统不同运行方式下的短路电流值来计算和校验所选用电器的稳定性和继电保护装置的灵敏

度。运行方式的变化，会改变CPS的运行环境、运行参数等，对CPS的硬件、软件、网络结构产生影响，引起风险事件的发生。

### (3) 外部攻击

外部攻击是指来自系统外部的人或物对系统内硬件、软件等的破坏，可分为物理攻击和非物理攻击，非物理攻击一般指网络攻击。

物理攻击一般指人为的恶意破坏，指外部对系统组成元素的直接破坏。对硬件的攻击是通过改变环境参数或直接改变硬件参数对硬件设备进行干扰。对软件的攻击是通过在软件级注入故障。

CPS对网络的依赖性强，所产生的风险也很高，网络系统所面临的入侵、事故、失效等威胁不但影响网络系统的本身，还将形成一种链式反应，产生严重的后果。CPS面临分布式拒绝服务攻击、蠕虫病毒、对Internet域名系统(DNS)的攻击和对路由器攻击或利用路由器的攻击威胁。例如对空地协同的空中交通管理系统的攻击如图6所示。入侵者通过对系统的飞行计划数据、航行情报数据、空管飞行监视数据、空域流量和需求数据、气象数据等重

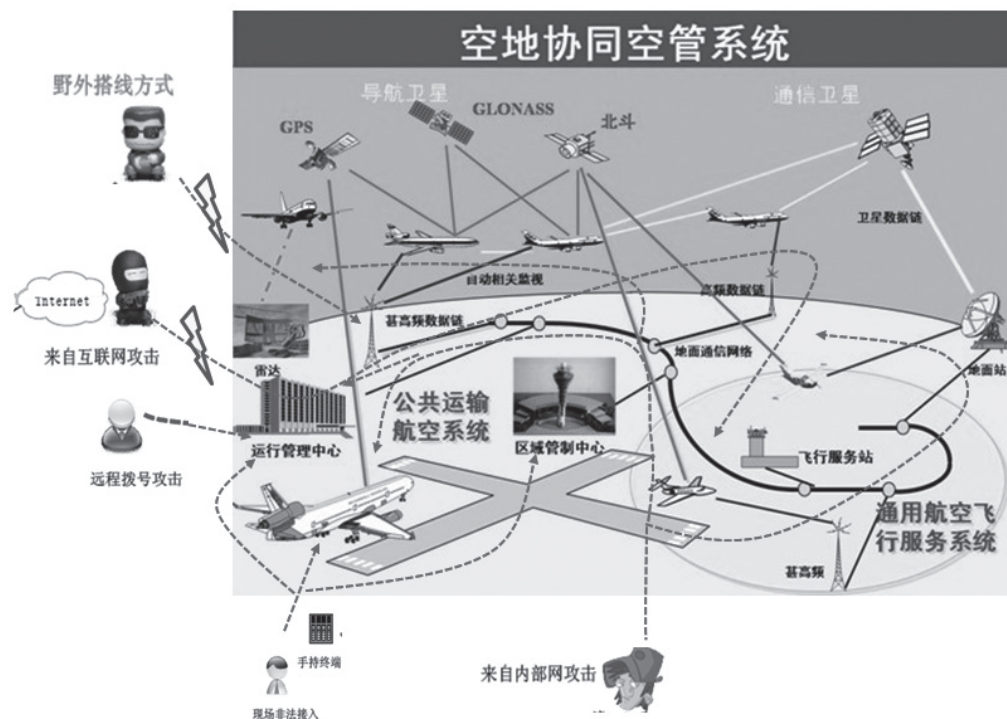


图5 CPS的应用领域示例

要信息，通过窃取、篡改、删除、伪装等方式，带有破坏意图地引发事故，制造安全威胁，达到他们目的。

### (三) 故障传播行为

故障传播指的是故障所引起的错误在不同实体之间的传播情况，所涉及的实体可以是物理器件、数据对象、语句、函数、进程等等。CPS是一个时变、高维、非线性、时空大范围跨越的巨大系统，各层次、子系统、设备之间具有高度复杂化的相互连接和相互依赖关系，

且它们通过物理连接和信息通信方式相互影响，是一个以网络为基础的系统。在CPS运行过程中，系统的某个设备或子系统局部在外因或内因的作用下出现功能失效或产生故障后，由于系统内部的耦合作用，可能会引起其它设备或子系统功能失效或故障，进而引发连锁反应，最终导致整个系统的功能失效与故障。其故障传播具有复杂性的特点：从长程时间上看，既表现出无序的非稳定性，又存在着有序的周期性和节律性；从短程时间

看，多时间尺度上的动态行为相互交织，运行模式和故障变化复杂。CPS的故障在空间上既存在区域性，又具有普遍性，故障波及的范围既具有可预测性又存在随机性和突变性。

当前，很多学者等从复杂系统的角度提出“复杂系统脆性”的概念，复杂系统是指组成系统的所有个体之间均存在非线性的相互作用，整个系统具有敏感性和不可逆性；系统具有层次性，个体或子系统在低层次所发生的相互作用可在高层次上涌现出全新的特征。组成复杂系统的所有子系统间存在强耦合作用。不可以将整个系统分成几个小部分来单独进行研究，然后简单地汇集各部分知识以达成对总体的理解。复杂系统脆性概念是指：对一个复杂系统 $S$ ，其存在一个子系统或一个部分 $S_i$ ，对外界环境相当敏感，当 $S_i$ 受到内外环境因素的影响或者攻击而发生崩溃时，可能会使其它部分或子系统也发生崩溃，进而致使整个系统全部崩溃。CPS是典型的复杂系统，不同的组件之间存在物理、信息或功能耦合的关系。在外因和内因同时作用下，

其结构更复杂、功能更强大的同时也变得更为脆弱。

## 2.3 CPS的典型事故案例分析

随着系统建设规模的不断增加，系统呈现出大型化、一体化、协同化、开放化和硬件的通用化等复杂系统的特点；系统的使用环境和使用模式也更加复杂；同时，系统内人员、软件、硬件、网络的交互影响也不不断深化，使其对信息的完整性和实时性要求越来越高。这些都给系统建设方、使用方和管理方带来了很大的挑战，稍有不慎就可能導致系统的故障，甚至导致重大事故的发生。

### 2.3.1 轨道交通系统事故案例

2011年7月1日，全国铁路调图。全国铁路将开行旅客列车2128.5对，增加了195对；全面实施了“三种混合运行”的列车开行新模式：①在时速300公里的高速铁路上，同时开行时速300公里和时速200-250公里两种动车组列车；②在时速200-250公里的线路上，同时开行时速200—250公里动车组列车和时速120-160公里普通客车；③在时速200公里及以下线路上，开行普通客车和货物列车。在此背景下，京

沪高铁通车。2011年7月10日，京沪高铁G151次往上海方向列车在山东省境内发生停车断电事故，造成当天19趟列车晚点。2011年7月12日，京沪高铁安徽省境内“供电设备发生故障”，造成多趟列车停车和晚点。2011年7月13日，由上海虹桥开往北京南的G114次列车，运行至常州北站突发故障，列车无法正常运行。经及时换车处置，未影响京沪高铁其他列车正常运行。但受故障影响，G114次列车预计17时到达北京南站，晚点2小时30分。

2011年7月23日晚8:30左右，甬温线永嘉站至温州南站间，北京南至福州D301次列车与杭州至福州南D3115次列车发生追尾事故，导致D301次1、2、3列车厢侧翻，从高架桥上坠落，毁坏严重，4车厢悬挂桥上，D3115次15、16车厢损毁严重。事故造成40人死亡，200多人受伤，D301次列车司机当场死亡，直接经济损失19371.65万元。经调查和事故认定结果得知，该事故原因首先是列车控制中心设备具有严重设计缺陷，因雷击导致的轨道电路设备故障未能察觉，导致后续时段轨道实际有车占用时，列控中心设备仍

按照无车占用状态进行控制输出；同时轨道电路发送器与列控中心通信故障，导致占用轨道列车无法通过人工控制按时驶离事故路段，最终酿成重大事故。

轨道交通系统是典型的CPS，尤其是列车运行的信息采集与监控系统负责严密监视整个系统的运行状态，在发生问题时能及时根据状态信息进行应急响应、制定故障控

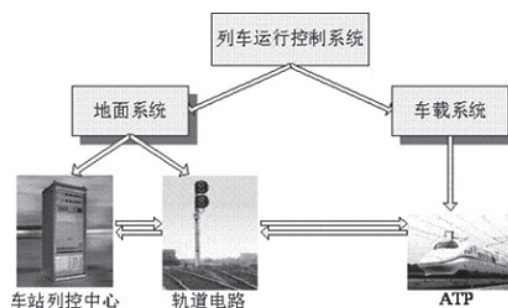


图6 列控系统示意图

制策略、避免事故发生起到决定性的作用，其故障小则导致带来经济损失，重则酿成事故、带来人员伤亡，对国家和城市的可靠与安全生产运营影响巨大。全国调图这些行为本身就是复杂系统的突变，原有的运行机制是否能够平稳过渡起到至关重要的作用。然而由于缺乏有效的预先评估，未能及时预测负载突然增加和变更后的调度机制是否

安全可靠，以“正点到达”和“经济利益为优先”的目标与原则，以及应急预案的不完备增加了上述事故后果的严重程度。

### 2.3.2 工业控制系统事故案例

以网络 and 智能控制技术为核心的工业控制系统，如核电站仪控系统、石油管网的信息采集与监控系统（简称为SCADA系统）也是目前已部署的典型CPS之一。工业控制系统已经成为涉及民生和国家安全的重大、关键基础设施的“心脏和大脑”，其安全问题在西方发达国家受到了越来越高度的重视。从克林顿1998年签发《关键基础设施保护》总统令（PDD-63），到奥巴马2009年5月29日公布的《网络空间政策评估——保障可信和强健的信息和通信基础设施》报告，美国将关键基础设施的安全与网络安全紧密联系在一起，在国家安全战略高度上进行了周密部署。欧洲对控制系统安全问题也高度重视，欧盟成立了专门的机构ENISA，于2011年12月发布了针对其成员国的《工业控制系统安全保护建议》。随着“网络战”和“制网权”概念的提出，西方发达国家将控制系统的安全技术

作为新的干预和制衡的手段。第一次海湾战争中，美国特工利用伊拉克购买的一批打印机途径安曼的机会植入病毒芯片，在“沙漠风暴”行动中通过无线网络唤醒这些“潜伏”的打印机，使伊拉克的防空体系陷于瘫痪，多国部队如入无人之境。在2008年8月俄格冲突中，俄罗斯同时发动网络攻击与传统战争，对格鲁吉亚的指挥通讯、电力供应系统、武装力量进行并行打击，在最短的时间内结束战斗，干净利索地取得战争胜利。2010年，一种名为“震网”的蠕虫病毒入侵了伊朗布什尔核电站，20%的离心机报废，伊朗大约3万个网络终端感染。“震网”蠕虫病毒侵入西门子为核电站设计的SCADA系统，意在夺取核电设备的控制权，意图就是发达国家利用工业控制系统的安全漏洞遏制伊朗核技术发展。

### 2.3.3 电力系统事故案例

2003年8月14日美国东北部和加拿大东部互联电网发生大面积停电事故，在停电29小时候恢复供电。这场事故共损失6180万KW负荷，263座电厂531台发电机停运（包括10座核电站19台核电机组），约5000万

人受到影响，造成超过300亿美元的经济损失。这一世界电力史上规模最大、影响范围最广的一次停电。2006年11月4日欧洲大陆互联电网发生大面积停电事故，共造成11个国家的1500万用户停电。2011年9月8日，美国西南部发生大停电事故，包括美国、墨西哥部分地区在内超过500万用户受到影响，由于正值“9.11”恐怖事件10周年前夕，这不仅给居民生活和企业生产带来了严重影响，也给社会民众造成了一定的恐慌情绪。

经过分析可以发现，三起大停电事故均是由于单一故障触发（无论是设备故障、软件运行错误还是外界环境影响），引起潮流瞬时转移、电压大幅波动、设备负载越限，逐步导致一系列保护和自动装置动作，先后造成变压器、输电线路、发电机和负荷的自动切除，最终使得至受电区域的主通道严重过载并自动解列造成的。这是由一系列互为因果的事件形成的故障发展过程，属于典型的“级联失效故障”。同时，在事故过程中，由于监测系统的不完善，无法向工作人员提供可靠的、足够的和及时

的系统状态信息，以至于丧失了一个又一个挽救的机会。

## 2.4 CPS存在质量风险的原因

虽然CPS在众多涉及国计民生和国家安全的工业生产和人民生活领域得到了广泛的应用，但是由于对CPS故障规律认识不够、未能建立有效测试、评价与验证机制保证其可靠、安全运行，导致故障、事故或遭受攻击事件频发，缺乏及时应对措施，甚至造成重大损失和人员伤亡的例子已在现有部署的CPS上多次发生。在发展和对抗的背景之下，CPS的安全可靠运行事关重大，其测试、评价理论与技术的研究刻不容缓。

### 2.4.1 对CPS故障规律认识不足

以往对的物理系统的设计分析与测试评估，一般假设物理故障相互独立。CPS系统中应用在物理系统之上的计算机与网络则考虑相反的原则，即大量网络攻击可能同时来袭或者多个故障协同发生。例如，分布式的服务攻击会使大量的僵尸电脑出现，以某种方式攻击同一个目标，遭受攻击的系统则很难恢复。甚至有时故障是不易察觉的，如软件的大量复制会导致系统

级故障或失效。这在物理系统中是极不常见的现象。CPS实现信息系统与物理系统的全面深度融合，但是现在计算机系统的部署很少考虑基于计算机控制的可靠性。这就导致系统面临着新的威胁——物理系统将会通过信息空间受到攻击。同样的，信息系统也会遭受到来自物理器件、设备和系统级的故障与安全威胁。试想如果汽车发动机引擎控制器的硬件突然故障，导致汽车无法制动；这样的问题可能会导致灾难性的事故。系统所处环境的多样性、多变性和严酷性也是不可避免的。同时，随着CPS中相对独立的子系统的建设规模和复杂性不断增加，导致系统间风险相互依赖性增强，系统脆性也将成为新的挑战，极易发生级联失效，引发连锁反应，使故障或事故变成不可控状态。因此，CPS的故障呈现了新的复杂特性、特殊机理以及复杂的故障行为。目前人们对CPS中可能发生的故障类型的了解是非常不全面的。

#### 2.4.2 缺乏CPS质量测评体系

CPS系统是对多种高新技术的有机融合，具备复杂系统的各类特点，对系统的建模和测评成为突破

的重点领域。目前国外的爱达荷国家实验室、橡树岭国家实验室、西北太平洋国家实验室等均已开展研究，而我国在CPS领域起步较晚，尚未开展体系化研究，缺少测评技术规范、测评工具及测评环境。测评体系的缺失阻碍了创新步伐，制约了发展后劲。

在此背景下，CPS测评技术的发展刻不容缓。能够在CPS设计、研发过程中通过测评技术识别系统风险并采取相应措施，系统的效费比将得到很大提升；在其运行、维护过程中通过测评技术，监测其运行状态，基于实时监测数据的基础上得到当前风险量化指标甚至预测下一时刻风险值，从而帮助用户对可能出现的风险及时响应，选取和实施高效、全面的安全措施，避免危险和损失的发生。CPS的测评将为CPS的安全运行提供了保障，为科学合理的安全决策奠定了理论基础，更为安全策略与防御措施的制定提供了指导，从而真正实现变“被动响应”为“主动防御”。可以说CPS测评技术将极大的体现复杂系统科学与风险管理的根本思想，实现风险的控制、预测/预防，是未来CPS科

学的基础理论与技术发展中不可或缺的部分。

### 三、应对策略建议

#### 3.1 政策导向

##### 3.1.1 工业4.0

“工业4.0”在德国被认为是第四次工业革命，是德国政府2011年11月公布的《高技术战略2020》中的一项战略，旨在支持工业领域新一代革命性技术的研发与创新，保持德国的国际竞争力。前三次工业革命被认为分别是机械化、电气化和信息化。而第四次工业革命被认为应当是将物联网及服务全面引入制造业。德国制造业一直处于世界领先地位，尤其是装备制造业。其历史悠久，经验积淀深厚，在研发、生产和复杂工艺的流程管理方面，都具有其他国家不可匹敌的优势。“工业4.0”提出的信息物理系统（CPS）将全面嵌入制造、工程、材料使用和供应链管理，即建造可以全球定位联动的“智能工厂”。它所展现的未来工业前景是强大的智能网络和进一步的去人工化。在一个“智能、网络化的世界”里，物联网和务联网（服务互联网技术）将渗透到所有的关键领域，创

造新价值的过程逐步发生改变，产业链分工将重组，传统的行业界限将消失，并会产生各种新的活动领域和合作形式。

2014年10月，在第三轮中德政府磋商期间，工业和信息化部部长苗圩与德国工业4.0平台相关机构就加强中德制造业创新合作进行了座谈。德国工业4.0的发起机构德国信息通信与新媒体协会（BITKOM）、机械设备制造业联合会（VDMA）、弗劳恩霍夫协会的负责人以及德国大众汽车公司、蒂森克虏伯公司、博世集团、SAP公司、西门子公司等德国工业企业的专业技术负责人和专家代表结合各自的实践，从不同角度阐述了通过供应链横向协同、研发生产纵向信息集成以及全生命周期管理，实现个性化定制、服务型制造和产业价值链提升的基于信息物理系统（CPS）的智能制造新模式，就其内涵、意义、前景和挑战等议题进行精辟的论证和广泛的交流，表达了与中国工业界开展有关合作的积极态度。中德政府磋商后发表《中德合作行动纲要》宣布，两国将开展“工业4.0”合作，该领域合作有望成为中德未来产业合作

的新方向。

以此，“工业4.0”作为我国工业化和信息化“两化深度融合”战略，列入我国工业发展进程。对促进全面实施推进《两化深度融合专项行动计划（2013—2018）》，加快完善制造业国家创新体系和综合标准化体系，打造智能化生产体系和发展模式具有重要的意义。作为工业发展的新基础，发展CPS有关理论和技术至关重要。

### 3.1.2 中国制造2025

2015年3月25日，李克强总理主持召开国务院常务会议，部署加快推进实施“中国制造2025”，实现制造业升级。经历了近3年时间制定而成的这份规划，被视为“用三个10年完成中国从制造业大国向制造业强国转变”的第一个10年路线图。国务院常务会强调，“中国制造2025”要顺应“互联网+”的发展趋势，以信息化与工业化深度融合为主线。

“互联网+”概念早在“两会”

不难发现，这10大重点发展领域均与CPS技术密切相关，作为基础理论与技术，CPS技术的发展亦至关重要。

期间就和“中国制造2025”同时提出。此次国务院常务会议再度明确了顺应“互联网+”概念，意味着“中国制造2025”将有望引入“互联网+”作为重要发展思路。换句话说，以互联网为标志的信息技术，将在中国制造业升级过程中，扮演至关重要的角色。

有了主线，此次国务院常务会还透露了“中国制造2025”的两个制造：强化工业基础能力，提高工艺水平和产品质量，推进智能制造、绿色制造。创造二字离不开技术提升，智能牵引。工信部部长苗圩说，我们还不是制造业强国，没有一大批具有国际竞争力的骨干企业，产业发展重大技术、装备亟待突破。完成从制造业大国向强国的转变，智能制造将是主攻方向。而在中国经济发展过程中，考虑环境影响和资源效率的现代制造模式的“绿色制造”也是首次出现在国务院常务会的议题中。这也意味着制造业将改变传统制造模式，推行绿色制造技术，发展相关的绿色材料、绿色能源和绿色设计数据库、知识库等基础技术，生产出保护环境、提高资源效率的绿色产品。

此次会议还透露了“中国制造2025”重点发展的十大领域，促进生产性服务业与制造业融合发展，提升制造业层次和核心竞争力。它们分别是：新一代信息技术、高档数控机床和机器人、航空航天装备、海洋工程装备及高技术船舶、先进轨道交通装备、节能与新能源汽车、电力装备、新材料、生物医药及高性能医疗器械、农业机械装备。



图7 中国制造2025重点发展10大领域

### 3.2 建议措施

安全可靠测评作为系统工程技术，伴随着工程领域的发展已经实践多年，是能够将故障/事故解决在“事前”，降低系统质量风险的有效解决途径。CPS的基础理论与技

术研究方兴未艾，那么CPS测评技术的发展也不可能是一蹴而就的。研究CPS测评基础理论与技术，研发测评工具，建设测评公共服务平台将是一个逐步推进的过程。在此过程中，在对传统系统硬件、软件（含复杂分布式软件系统和嵌入式软件）、嵌入式系统（软硬件综合系统）、通信网络、无线传感器网络的功能、性能、可靠性、安全性以及风险评估等测评技术的研究基础上，面向物联网、电网及其广域监控系统、石油管网及其信息采集与监控（SCADA）系统、轨道交通信号网络、汽车电子系统、交通网络、光伏发电及其监控系统等工程系统领域开展测评理论与技术的应用实践经验与创新是降低CPS质量风险的可行之路。同时，对各类CPS构成的关键基础设施及其具有风险依赖性的基础设施网络开展基于系统复杂性特征的安全可靠性测评也将成为未来缓解CPS质量风险的发展方向之一。

总体来说，稳步推进CPS测评研究需要做好以下几点关键技术：

（1）集中优势资源、加快公共服务平台建设。公共技术服务平台

实现对政府、企业和行业应用的全面支撑，构建产学研用的产业链环境面向整个产业链，打造CPS领域服务团队，产学研用相结合，支撑政府工作，协助政府进行政策的落实，协助企业进行产品和技术的提升，协助用户保证系统可靠设计、安全运行。

（2）加大培训力度、提高安全可靠意识。在已有的理论、技术与工具平台基础上，积极引进国内外最新可靠性与安全性测评技术和工具，并进行消化与再创新，不断促进自主创新能力的提升；加强CPS测评工程技术人才和测试工程师的培养；积极与科研机构、产业部门沟通，推广CPS测评的重要理念，提高从业人员的可靠性与安全性设计、研发与运维的意识。

（3）加快落实CPS测评工程实践。在充分认识CPS测评重要性与紧迫性的前提下，明确重点工程实践领域，开展实际测评工作，积极主动发现问题，可帮助优化在研系统的设计、已有系统的运维安全。

（4）开展CPS在线监测。我国有一部分大型基础设施（如大型跨度桥梁、大型体育场馆、超高层建

筑、大型水利工程、电网电站、核电站、城市防洪系统等）都是在20世纪五六十年代或者更早的时期建造的，后建的与已有的新型基础设施的能力建设也面临巨大的负载压力与资源限制。对这些已有关键基础设施、工业生产系统或关键设备的运行状态与健康状态进行监测，实现预警机制，对其稳定、有效运行至关重要。

（5）加强CPS对抗威胁与攻击能力。通过对CPS安全性测评的研究，在物理系统与信息系统的安全漏洞检查的基础上，通过攻防对抗模拟，对其对抗安全威胁与攻击的能力进行评估，根据评估结果进行改进与完善，可以极大增强系统的安全防护能力；同时，根据上述能力建设，在CPS测评技术体系下搭建相应的安全性测评子体系，构建自主可控的安全防护体系。

（6）加强数据融合分析、故障预测、安全事故预警等技术的研究。通过对分析结果数据、测试数据、状态监测数据、专家知识等数据进行数据融合分析，对多源信息进行优化组合与科学处理，建立故障预测、安全事故预警与故障诊断

模型，提高状态监测与故障诊断与预测的智能化程度，这对涉及CPS的城市规划、资源管理、环境监测与分析，构建系统专用与通用质量特性的闭环控制是必不可少的基础技术。

（7）推动建立自主的安全完整性等级测评认证标准和体系。我国近些年可以说处于安全事故多发状态。功能安全和安全完整性等级只是作为一个名词概念，在国内工业领域业内流传。SIL（Safety Integrity Level）-安全完整性等级认证是基于IEC 61508，IEC 61511，IEC 61513，IEC 13849-1，IEC 62061，IEC 61800-5-2等标准，对安全设备的安全完整性等级（SIL）或者性能等级（PL）进行评估和确认的一种第三方评估、验证和认证。功能安全认证主要涉及针对安全设备开发流程的文档管理（FSM）评估，硬件可靠性计算和评估、软件评估、环境试验、EMC电磁兼容性测试等内容。目前国内还没有具备综合型完整的SIL认证能力的机构。在国际市场份额方面与国外

认证机构在我国的分支机构相比，更是有名无实。国内大型研发企业为了打入国际市场，纷纷将自己的产品送到国外SIL认证机构进行安全完整性认证，这一举动，无疑将自主研发的产品部分或全部知识产权公之于发达国家。因此，我国亟需完善我国自主的功能认证标准和认证机构，同时以此为依据，为国外产品准入我国市场设立，反制竞争对手，从而保护目前我国安全可靠相对薄弱的工业产业。

（8）建立CPS测评服务体系。CPS测评服务体系包括：重点研究测评指标体系与关键技术等CPS测评基础理论与技术；建立测评的公共技术服务平台，搭建测评实验环境，研发与采购测评工具；进行行业的测评应用验证示范，参与制定相关行业测评标准，切实通过积极参与系统开发与集成过程、验收过程、运维过程中的CPS的定性与定量评估和质量等级评定，有效做到事前、事中与事后的质量与可靠安全控制，全面建设与提升各个工业领域中CPS的可靠性与安全性保障能力。

工业和信息化部计算机与微电子发展研究中心（中国软件评测中心），简称：中国软件评测中心，作为国内权威的第三方软、硬件产品及信息系统工程质量安全与可靠性检测机构，是直属于国家工业和信息化部的一类科研事业单位。自成立二十余年来，中国评测秉承“专业就是实力”的宗旨，共承担了10万余款软硬件产品和1万余项信息系统的测试任务，业务网络覆盖全国500多个大中型城市，所出具的测试报告在61个国家和地区实现互认。中国软件评测中心通过测试、设计（规划、工程规划）、监理、认证、评估、培训等主营业务，构建基于第三方服务的科技产业链。旗下的赛迪测评、赛迪设计、赛迪监理、赛迪认证、赛迪评估、赛迪培训等业务在业内拥有权威地位。

中国软件评测中心先后申请了30余个国家科研项目，先后建立了包括国家云计算公共技术服务平台、国家物联网公共技术服务平台、中国移动互联网应用软件检测平台等在内的6个国家级技术平台，开发了具有自主知识产权的30余种专业测试工具，获得了50余项软件著作权，拥有16个国家级质量体系认证证书，并主持了7项质量领域国家标准和行业标准的制定。

中国软件评测中心先后成立了深圳、广州、山东、无锡四个分中心，大连、安徽、青岛三个办事处，服务范围涵盖了全国31个省及直辖市。

详情请浏览网站：[www.cstc.org.cn](http://www.cstc.org.cn)



唯有實力出眾，



才能贏得客戶尊重

测试 · 监理 · 认证 · 评估 · 培训

—— 致力于电子系统安全可靠：云计算 · 物联网 · 智能终端 · 集成电路 · 工业控制系统 · 信息系统工程

中国软件评测中心

地址：北京市海淀区紫竹院路66号赛迪大厦4/6/12/13/14层  
电话：010-88559238/9239 010-88559372/9373

邮编：100048 网址：www.cstc.org.cn  
邮箱：service@cstc.org.cn



中国评测  
新浪官方微博



中国评测  
微信公众平台

您的关注是我们成长的动力,如需获取更多前沿科技  
研究信息,请关注我们!