



工业互联网产业联盟
Alliance of Industrial Internet



工业互联网 体系架构

(版本1.0)



工业互联网产业联盟 (AII)

2016年8月

编写说明

近年来，随着以互联网、物联网、云计算、大数据、人工智能等为代表的新一代信息技术与传统产业的加速融合，全球新一轮科技革命和产业变革正蓬勃兴起，一系列新的生产方式、组织方式和商业模式不断涌现，工业互联网应运而生，国内外的探索也全面展开，正推动全球工业体系的智能化变革。

工业互联网涉及工业和互联网等信息通信技术领域的各个环节和各个主体，正形成复杂和全新的生态系统。对工业互联网认识 and 理解的差异，有可能导致技术选择、标准路线上的分化，影响互操作性和部署成本。为此，在工业和信息化部指导下，工业互联网产业联盟（以下简称 AII）启动了工业互联网体系架构研究，在总结国内外发展实践的基础上，撰写了工业互联网体系架构报告（1.0 版），提出了工业互联网的内涵、目标、体系架构、关键要素和发展方向。报告旨在推动业界对工业互联网达成广泛共识，以体系架构为牵引，为联盟各项工作以及我国工业互联网的技术创新、标准制定、试验验证、应用实践等提供参考和引导，共同推动工业互联网的健康快速发展。

工业互联网是一个长期发展和演进的过程，毫无疑问，目前我们对工业互联网的认识还是初步和阶段性的。联盟将根据国内外工业互联网的发展情况以及产业界的反馈意见，在持续深入研究的基础上适时修订和发布报告新版。

指 导 单 位：工业和信息化部

牵头编写单位：中国信息通信研究院

参与编写单位：中国电信集团公司、华为技术有限公司、中国科学院沈阳自动化研究所、
中国航天科工集团公司、海尔集团公司、三一集团有限公司、阿里云计算有限公司、
北京奇虎 360 科技有限公司、中国移动通信集团公司、中兴通讯股份有限公司、
清华大学、网神信息技术（北京）股份有限公司、北京中数创新科技股份有限公司

编写组成员：

中国信息通信研究院：余晓晖、李海花、田洪川、高巍、刘默、田慧蓉、魏凯、刘阳、杜加懂、
肖荣美、李强、张恒升、蒋昕昊、李铮、谢玮、王峰、张雪丽、秦业、
黄颖、王欣怡、王晓玲、刘丽辉、刘钊、刘荣朵、刘贺贺、刘棣斐、关欣、
杨希、杨思维、宋菲、张田、赵峰、段世惠、徐贵宝

中国电信集团公司：孙健、张东、夏艳

华为技术有限公司：蒋旺成、彭炎

中国科学院沈阳自动化研究所：于海斌、曾鹏

中国航天科工集团公司：柴旭东、李润强

海尔集团公司：陈录城、张维杰
三一集团有限公司：贺东东、王锦霞
阿里云计算有限公司：刘 松、马铁宝、李俊平
北京奇虎 360 科技有限公司：谭晓生
中国移动通信集团公司：林 琳、吴淑燕
中兴通讯股份有限公司：高 峰
清华大学：王建民、王 成
网神信息技术（北京）股份有限公司：陶耀东
北京中数创新科技股份有限公司：镇锡惠、王 昆

工业互联网产业联盟理事长、中国信息通信研究院院长曹淑敏亲自领导工业互联网体系架构及相关研究，组织成立工业互联网参考架构、需求、网络、数据、安全、标识、产业、政策等专题研究小组，多次安排专题会议听取汇报并给出指示，推动了工业互联网体系架构和关键方向深入研究和成果提炼。刘多副院长、张延川副院长、科技委蒋林涛主任等领导及技术标准研究所王志勤所长、石友康副所长、续合元总工程师，信息化与工业化融合研究所朱敏副所长，安全研究所魏亮所长，政策与经济研究所辛勇飞副所长等也在工业互联网体系架构和报告编制过程中积极给与了指导。

报告编制中，为充分了解产业发展现状和需求，编写组对国内外上百家典型企业和机构开展了大量调研，包括通用电气、航天科工、海尔、三一重工、博世、富士康、智能云科、潍柴动力、九江石化、沈阳自动化研究所、中联重科、和利时、浙大中控、中国商飞、上海仪电、沈阳机床等工业企业，华为、英特尔、中国电信、中兴通讯、思科、思爱普、中国移动、数码大方、石化盈科等家信息通信企业，阿里巴巴、腾讯、百度、京东、苏宁云商、找钢网、欧冶云商等互联网企业，美国工业互联网联盟（IIC）、美国国家标准与技术研究院（NIST）、美国信息产业机构（USITO）、德国联邦教育和研究部、德国电气电子行业总会（ZVEI）、德国工业 4.0 科学顾问委员会、德国弗劳恩霍夫协会等机构。通过调研，深入了解产业界和政府等对工业互联网的认识和探索，为工业互联网体系架构研究和本报告的撰写提供了重要参考。

报告编制中，编写组就体系架构设计中的关键问题先后征询了邬贺铨、胡启恒、朱高峰、李国杰、吴澄、沈昌祥、刘玠、李伯虎、李培根、刘韵洁、谭建荣、桂卫华、王恩东、柴洪峰、陈纯、吴建平、余少华、高新民、朱森第、董景晨、于海斌、钱华林、毛伟等 30 多位院士及专家意见，并结合意见对报告进行了多次修改和完善。中国互联网协会高新民副理事长还对报告的编制提供了很多详细的指导意见。

在此一并感谢所有参与本报告编写，以及为本报告提供指导和建议的专家、企业和机构。



编写说明	1
目 录	3
图 目 录	4
一、工业互联网的内涵及与智能制造的关系	5
(一) 工业互联网的内涵	5
(二) 工业互联网和智能制造的关系	5
二、工业互联网体系架构	7
(一) 工业互联网业务需求	7
(二) 工业互联网体系架构	7
三、工业互联网的网络体系	9
(一) 工业互联网网络体系框架	9
(二) 工业互联网网络互联体系	10
(三) 工业互联网地址与标识解析体系	14
(四) 工业互联网应用支撑体系	16
四、工业互联网的数据体系	19
(一) 工业大数据内涵特征	19
(二) 工业互联网大数据功能架构	19
(三) 工业互联网大数据应用场景	20
(四) 存在的问题	22
(五) 发展趋势	22
五、工业互联网的安全体系	24
(一) 工业互联网安全体系框架	24
(二) 现状分析	25
(三) 存在的问题	25
(四) 发展趋势	26
六、工业互联网的实施	27
(一) 工业系统现状及实施目标	27
(二) 工业互联网网络的实施	28
(三) 工业互联网数据的实施	33
(四) 工业互联网安全的实施	34
附件 1: 术语与定义	36
附件 2: 缩略语	39

图 目 录

图 1 工业互联网业务视图	7
图 2 工业互联网体系架构	8
图 3 工业互联网互联示意	9
图 4 工业互联网整体网络体系目标框架	9
图 5 工厂网络连接现状	10
图 6 工厂内部网络目标架构	12
图 7 工厂外部网络目标架构	14
图 8 工业互联网应用支撑体系	18
图 9 工业互联网数据体系参考架构	19
图 10 工业互联网大数据技术应用示意	20
图 11 工业互联网安全体系	24
图 12 现阶段工业系统实现架构	27
图 13 工业互联网目标实现架构	28
图 14 网络互联的实施	29
图 15 标识解析的实施	30
图 16 方式一：工厂云平台的实施	31
图 17 方式二：工业云平台的实施	31
图 18 方式三：混合云的实施	32
图 19 工业互联网数据的实施	33
图 20 工业互联网安全的实施	34

一、工业互联网的内涵及与智能制造的关系

（一）工业互联网的内涵

工业互联网的内涵用于界定工业互联网的范畴和特征，明确工业互联网总体目标，是研究工业互联网的基础和出发点，我们认为，工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施。其本质是以机器、原材料、控制系统、信息系统、产品以及人之间的网络互联为基础，通过对工业数据的全面深度感知、实时传输交换、快速计算处理和高级建模分析，实现智能控制、运营优化和生产组织方式变革。工业互联网可以重点从“网络”、“数据”和“安全”三个方面来理解。其中，网络是基础，即通过物联网、互联网等技术实现工业全系统的互联互通，促进工业数据的充分流动和无缝集成；数据是核心，即通过工业数据全周期的感知、采集和集成应用，形成基于数据的系统性智能，实现机器弹性生产、运营管理优化、生产协同组织与商业模式创新，推动工业智能化发展；安全是保障，即通过构建涵盖工业全系统的安全防护体系，保障工业智能化的实现。工业互联网的发展体现了多个产业生态系统的融合，是构建工业生态系统、实现工业智能化发展的必由之路。

工业互联网与制造业的融合将带来四方面的智能化提升。一是智能化生产，即实现从单个机器到产线、车间乃至整个工厂的智能决策和动态优化，显著提升全流程生产效率、提高质量、降低成本。二是网络化协同，即形成众包众创、协同设计、协同制造、垂直电商等一系列新模式，大幅降低新产品开发制造成本、缩短产品上市周期。三是个性化定制，即基于互联网获取用户个性化需求，通过灵活柔性组织设计、制造资源和生产流程，实现低成本大规模定制。四是服务化转型，即通过对产品运行的实时监测，提供远程维护、故障预测、性能优化等一系列服务，并反馈优化产品设计，实现企业服务化转型。

工业互联网驱动的制造业变革将是一个长期过程，构建新的工业生产模式、资源组织方式也并非一蹴而就，将由局部到整体、由浅入深，最终实现信息通信技术在工业全要素、全领域、全产业链、全价值链的深度融合与集成应用。

（二）工业互联网和智能制造的关系

作为当前新一轮产业变革的核心驱动和战略焦点，智能制造是基于物联网、互联网、大数据、云计算等新一代信息技术，贯穿于设计、生产、管理、服务等制造活动的各个环节，具有信息深度自感知、智慧优化自决策、精准控制自执行等功能的先进制造过程、系统与模式的总称。具有以智能工厂为载体、以生产关键制造环节智能化为核心，以端到端数据流为基础、以全面深度互

联为支撑四大特征。

智能制造与工业互联网有着紧密的联系，智能制造的实现主要依托两方面基础能力，一是工业制造技术，包括先进装备、先进材料和先进工艺等，是决定制造边界与制造能力的根本；二是工业互联网，包括智能传感控制软硬件、新型工业网络、工业大数据平台等综合信息技术要素，是充分发挥工业装备、工艺和材料潜能，提高生产效率、优化资源配置效率、创造差异化产品和实现服务增值的关键。因此我们认为，工业互联网是智能制造的关键基础，为其变革提供了必须的共性基础设施和能力，同时也可以用于支撑其他产业的智能化发展。



二、工业互联网体系架构

（一）工业互联网业务需求

工业互联网的业务需求可从工业和互联网两个视角分析，如图 1 所示。

从工业视角看，工业互联网主要表现为从生产系统到商业系统的智能化，由内及外，生产系统自身通过采用信息通信技术，实现机器之间、机器与系统、企业上下游之间实时连接与智能交互，并带动商业活动优化。其业务需求包括面向工业体系各个层级的优化，如泛在感知、实时监测、精准控制、数据集成、运营优化、供应链协同、需求匹配、服务增值等业务需求。

从互联网视角看，工业互联网主要表现为商业系统变革牵引生产系统的智能化，由外及内，从营销、服务、设计环节的互联网新模式新业态带动生产组织和制造模式的智能化变革。其业务需求包括基于互联网平台实现的精准营销、个性定制、智能服务、众包众创、协同设计、协同制造、柔性制造等。

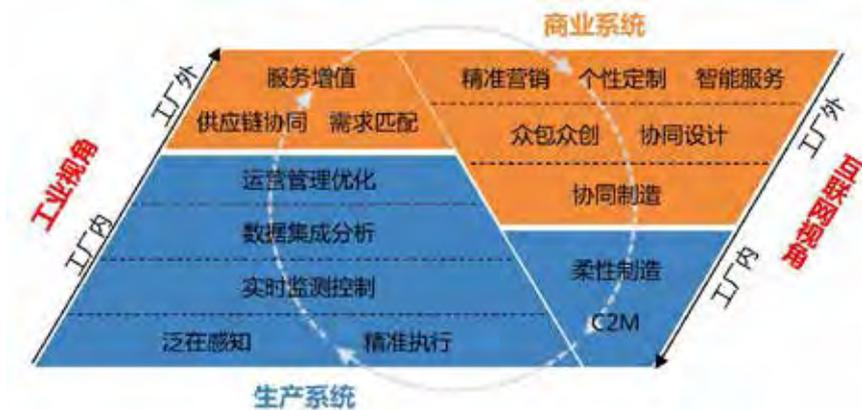


图 1 工业互联网业务视图

（二）工业互联网体系架构

工业互联网的核心是基于全面互联而形成数据驱动的智能，网络、数据、安全是工业和互联网两个视角的共性基础和支撑。

其中，“网络”是工业系统互联和工业数据传输交换的支撑基础，包括网络互联体系、标识解析体系和应用支撑体系，表现为通过泛在互联的网络基础设施、健全适用的标识解析体系、集中通用的应用支撑体系，实现信息数据在生产系统各单元之间、生产系统与商业系统各主体之间的无缝传递，从而构建新型的机器通信、设备有线与无线连接方式，支撑形成实时感知、协同交互的生产模式。

“数据”是工业智能化的核心驱动，包括数据采集交换、集成处理、建模分析、决策优化和

反馈控制等功能模块，表现为通过海量数据的采集交换、异构数据的集成处理、机器数据的边缘计算、经验模型的固化迭代、基于云的大数据计算分析，实现对生产现场状况、协作企业信息、市场用户需求的精确计算和复杂分析，从而形成企业运营的管理决策以及机器运转的控制指令，驱动从机器设备、运营管理到商业活动的智能和优化。

“安全”是网络与数据在工业中应用的安全保障，包括设备安全、网络安全、控制安全、数据安全、应用安全和综合安全管理，表现为通过涵盖整个工业系统的安全管理体系，避免网络设施和系统软件受到内部和外部攻击，降低企业数据被未经授权访问的风险，确保数据传输与存储的安全性，实现对工业生产系统和商业系统的全方位保护。工业互联网体系架构如图 2 所示。



图 2 工业互联网体系架构

基于工业互联网的网络、数据与安全，工业互联网将构建面向工业智能化发展的三大优化闭环。一是面向机器设备运行优化的闭环，核心是基于对机器操作数据、生产环境数据的实时感知和边缘计算，实现机器设备的动态优化调整，构建智能机器人和柔性产线；二是面向生产运营优化的闭环，核心是基于信息系统数据、制造执行系统数据、控制系统数据的集成处理和大数据建模分析，实现生产运营管理的动态优化调整，形成各种场景下的智能生产模式；三是面向企业协同、用户交互与产品服务优化的闭环，核心是基于供应链数据、用户需求数据、产品服务数据的综合集成与分析，实现企业资源组织和商业活动的创新，形成网络化协同、个性化定制、服务化延伸等新模式。

三、工业互联网的网络体系

(一) 工业互联网网络体系框架

随着智能制造的发展，工厂内部数字化、网络化、智能化及其与外部数据交换需求逐步增加，工业互联网呈现以三类企业主体、七类互联主体、八种互联类型为特点的互联体系，如图 3 所示。

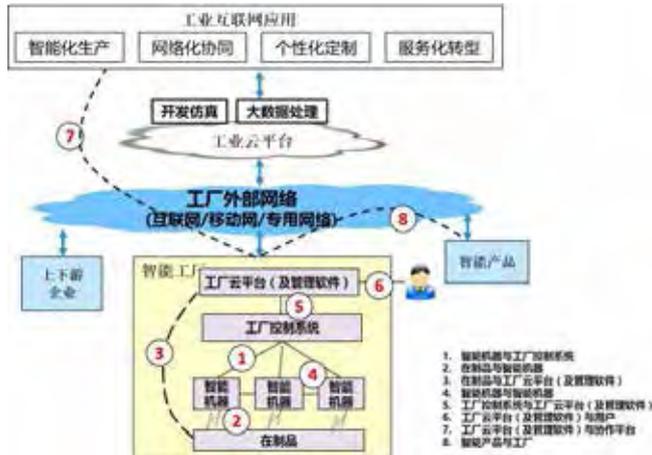


图 3 工业互联网互联示意

三类企业主体包括工业制造企业、工业服务企业（围绕设计、制造、供应、服务等环节提供服务的各类企业）和互联网企业，这三类企业的角色在不断渗透、相互转换。七类互联主体包括在制品、智能机器、工厂控制系统、工厂云平台（及管理软件）、智能产品、工业互联网应用，工业互联网将互联主体从传统的自动化控制进一步扩展为产品全生命周期的各个环节。八种互联类型包括了七类互联主体之间复杂多样的互联关系，成为连接设计能力、生产能力、商业能力以及用户服务的复杂网络系统。

以上互联需求的发展，促使工厂网络发生新的变革，形成工业互联网整体网络架构，如图 4 所示。

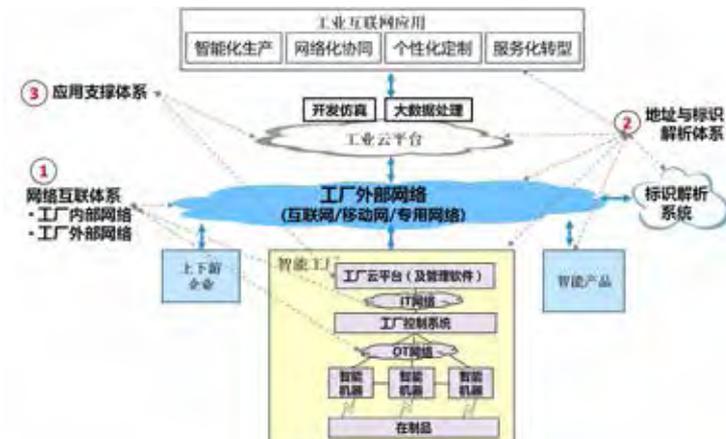


图 4 工业互联网整体网络体系目标框架

与现有互联网包含互联体系、DNS 体系、应用服务体系三个体系相类似，工业互联网也包含三个重要体系。一是网络互联体系，即以工厂网络 IP 化改造为基础的工业网络体系。包括工厂内部网络和工厂外部网络“两大网络”。工厂内部网络用于连接在制品、智能机器、工业控制系统、人等主体，包含工厂 IT 网络和工厂 OT（工业生产与控制）网络。工厂外部网络用于连接企业上下游、企业与智能产品、企业与用户等主体。二是地址与标识体系，即由网络地址资源、标识、解析系统构成的关键基础资源体系。工业互联网标识，类似于互联网域名，用于识别产品、设备、原材料等物体。工业互联网标识解析系统，用于实现对上述物体的解析，即通过将工业互联网标识翻译为该物体的地址或其对应信息服务器的地址，从而找到该物体或其相关信息。三是应用支撑体系，即工业互联网业务应用交互和支撑能力，包含工业云平台和工厂云平台，及其提供的各种资源的服务化表述、应用协议。

（二）工业互联网网络互联体系

1、工厂内部网络

（1）现状分析

工厂内部网络是在工厂内部用于生产要素以及 IT 系统之间互联的网络。总体来看，工厂内部网络呈现“两层三级”的结构，如图 5 所示。“两层”是指“工厂 OT 网络”和“工厂 IT 网络”；“三级”是根据目前工厂管理层级的划分，网络也被分为“现场级”、“车间级”、“工厂级/企业级”三个层次，每层之间的网络配置和管理策略相互独立。

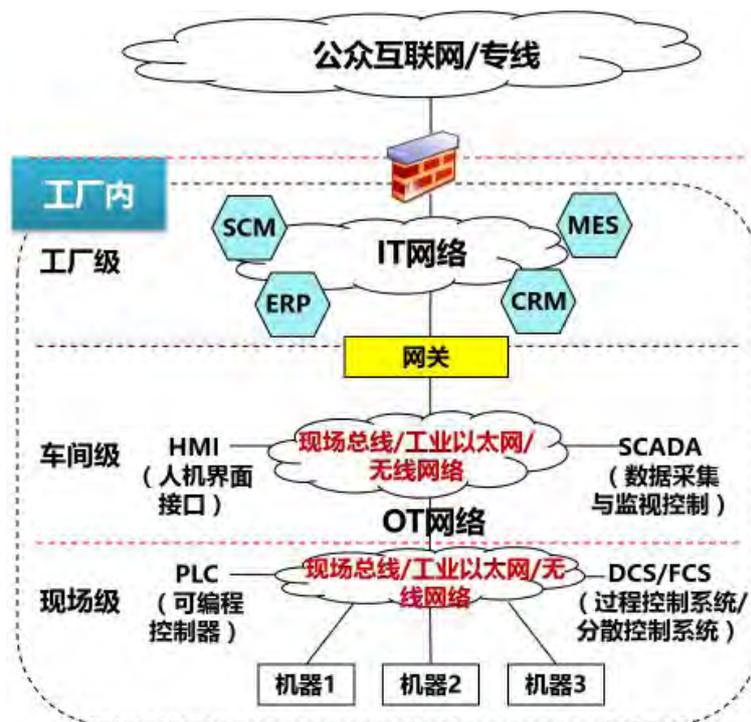


图 5 工厂网络连接现状

其中，工厂 OT 网络主要用于连接生产现场的控制器（如 PLC、DCS、FCS）、传感器、伺服器、监控设备等部件。工厂 OT 网络的主要实现技术分为现场总线和工业以太网两大类。工厂 IT 网络主要由 IP 网络构成，并通过网关设备实现与互联网和工厂 OT 网络的互联和安全隔离。

（2）存在的问题

目前工厂内部网络“两层三级”这种技术体系和网络结构相互隔离的状况使 IT 系统与生产现场之间的通信存在较多障碍。一是工业控制网络与工厂信息网络的技术标准各异，难以融合互通。二是工业生产全流程存在大量“信息死角”，亟需实现网络全覆盖。三是工厂网络静态配置、刚性组织的方式难以满足未来用户定制、柔性生产的需要。

（3）发展趋势

为适应智能制造发展，工厂内部网络呈现扁平化、IP 化、无线化及灵活组网的发展趋势。

工厂内网络扁平化。一是随着智能机器发展和智能分析的集中，工厂 OT 系统将逐渐打破车间级、现场级分层次组网模式，智能机器之间将逐渐实现直接的横向互联。二是整个工厂管理控制系统扁平化，包括 IT 系统和 OT 系统部分功能融合（如 HMI），或通过工业云平台方式实现，实时控制功能下沉到智能机器，促使 IT 与 OT 网络逐步融合为同一张全互连网络。

工厂内网络以太网/IP 化趋势。随着工业网络技术的发展演进，现场总线正在逐步被工业以太网替代。未来，工业内有线连接将被具有以太网物理接口的网络主导，同时基于通用标准的工业以太网逐步取代各种私有的工业以太网，并实现控制数据与信息数据同口传输。随着以太网的广泛使用，工业网络的 IP 化趋势将更为凸显，IP 技术将由 IP 网络向 OT 网络延伸，实现信息网络的 IP 到底，从而使得 IT 与 OT 节点（机器）直接可达。而为解决大量支持 IP 的装备接入问题，IPv6 技术将在工厂内广泛应用。

工厂内无线网络成为有线网络的重要补充。无线技术逐步向工业领域渗透，呈现从信息采集到生产控制，从局部方案到全网方案的发展趋势。目前无线技术主要用于信息的采集、非实时控制和工厂内部信息化等，Wi-Fi、Zigbee、2G/3G/LTE、面向工业过程自动化的无线网络 WIA-PA、WirelessHART 及 ISA100.11a 等技术已在工厂内获得部分使用。对于低功耗、广覆盖、大连接等工业信息采集和控制场景，NB-IoT 将会成为较好的技术选择。同时无线技术正逐步向工业实时控制领域渗透，成为现有工业有线控制网络有力的补充或替代，如 5G 已明确将工业控制作为其低时延、高可靠的重要应用场景，3GPP 也已开展相关的研究工作，对应用场景、需求、关键技术等进行全面的梳理，此外 IEC 正在制定工厂自动化无线网络 WIA-FA 技术标准。

工厂内网络灵活化组网。未来基于智能机器柔性生产将实现生产域根据需求进行灵活重构，智能机器可在不同生产域间迁移和转换，并在生产域内实现即插即用。这需要工厂网络的灵活组网，实现网络层资源可编排能力，软件定义网络（SDN）是其中实现方式之一。

(4) 目标架构

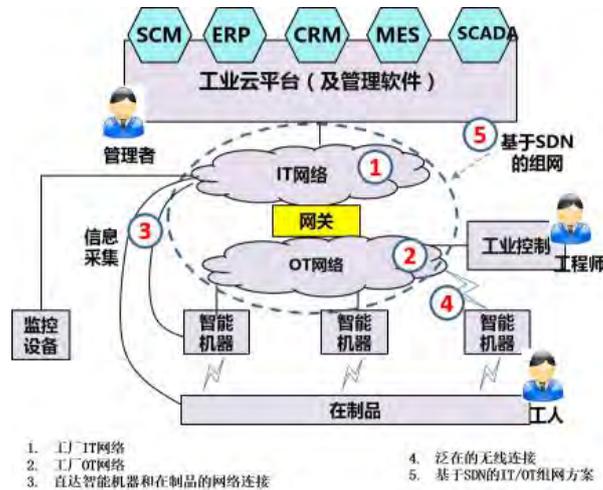


图6 工厂内部网络目标架构

工业互联网场景下工厂内部网络方案将包括五个主要环节，如图6所示，一是工厂IT网络。为适应互联网的发展趋势，同时也为了工厂内庞大数量的生产、监控终端接入，IT网络应该基于IPv6或支持IPv4/IPv6双栈。二是工厂OT网络。工业以太网将逐步替代现场总线，实现“e网到底”，同时在以太网向下延伸基础上实现智能机器、传感器、执行器等的IP化或IPv6化。三是直达智能机器和在制品的连接。智能机器、传感器、在制品等生产现场设备、物品将实现到IT网络的直达连接以实现生产现场的实时数据采集等功能。四是泛在的无线连接。生产现场的智能机器、在制品、传感器、运送设备等将通过各类无线技术实现连接，根据设备能耗、传送距离等可采用Zigbee等短距离通信技术或Wi-Fi、LTE增强、NB-IoT、5G等无线技术。五是基于SDN的IT/OT组网方案。IT网络和OT网络采用SDN技术，实现控制平面与转发平面的分离，通过SDN控制器与制造控制系统（如MES等）协同进行网络资源调度，支撑柔性制造和生产自组织。

2、工厂外部网络

(1) 现状分析

工厂外部网络主要是指以支撑工业全生命周期各项活动为目的，用于连接企业上下游之间、企业与智能产品、企业与用户之间的网络。目前，大量工业企业已经与公众互联网之间实现互联，但互联网为工业生产带来的价值仍比较有限。从互联形式上来看，工厂的生产流程和企业管理流程仍封闭在工厂内部，从公众互联网的角度来看，工厂内部仍是一个“黑盒”。从应用形式上看，工厂与互联网的结合主要是在产品销售和供应链管理等环节，互联网在工业生产全生命周期中的资源优化配置作用仍未充分体现。

(2) 存在的问题

目前以IPv4公众互联网为主体的工厂外部网络承载未来工业互联网应用存在四个方面主要问题，一是网络性能难以满足。公众互联网没有服务质量的保证，难以满足工业生产与互联网融合

后对网络提出的低时延、高可靠、服务质量保证的需求。二是网络承载能力难以满足。目前的公众互联网业务承载和隔离能力较弱，在 VPN 专网上能够承载的 VPN 数量也有限，难以满足大量工业企业专线互连的要求。三是网络安全威胁。工业互联网应用对网络安全的要求进一步提升，目前互联网的安全能力有待提高。四是网络地址空间有限。目前以 IPv4 为基础的公众互联网自身面临地址枯竭的局面，难以承载工业互联网数以百亿终端接入的要求。

(3) 发展趋势

随着网络和信息化技术、服务模式的发展，原来局限在工厂内的工业生产过程逐步扩展到外部网络，工业生产信息系统与互联网正在走向深度协同与融合，包括 IT 系统与互联网的融合、OT 系统与互联网的协同、企业专网与互联网的融合、产品服务与互联网的融合。

企业 IT 系统与互联网融合从网络层面来看是工厂内部 IT 网络向外网的延伸。企业将其 IT 系统（如 ERP、CRM 等）托管在互联网的云服务平台中，或利用 SaaS 服务商提供的企业 IT 软件服务。

OT 系统与互联网协同从网络层面看是部分 OT 系统网络向外网的延伸。在一些人力较难达到，且又需要实现生产过程调整和维护的场景下，需要通过可靠的互联网连接，实现远程的 OT 系统控制。目前互联网的质量对于时延、抖动、可靠性有极高要求的实时控制还无法承载。

企业专网与互联网融合是将在公众网络中为企业生成独立的网络平面，并可对带宽、服务质量等进行灵活快速定制。这类业务场景需要提供独立的网络资源控制能力，开放的网络可编程能力，以及定制化的网络资源（如带宽、服务质量等）。目前的互联网尚不支持此类业务场景，需要网络虚拟化及软件定义网络技术的进一步发展及部署。

产品服务与互联网融合将通过智能工业产品的信息采集和联网能力为工业企业提供新的产品服务模式。工业企业基于这些平台可以为用户提供产品监测、预测性维护等延伸服务，从而延长了工业生产的价值链。这类业务的基础是对海量产品的数据采集与监测，需要通过无线等技术实现工业产品的泛在接入。

工厂与公众网络的互联需求不断增强和扩展，新型互联的出现对现有公众网络不断提出新的需求，一是支持百亿终端接入，联网的工业装备及产品数量将达到百亿级水平。二是支持百级业务平面，考虑工业现场 OT、IT 各类应用以及未来业务发展，不同质量要求的业务平面应达到数百级别。三是支持百万用户隔离，全国规模以上工业企业数量在 50 到 60 万家左右，每个企业按照 3 到 5 个 VPN 需求计，网络的承载能力需达到百万级 VPN 水平。四是提供全程服务质量保证，满足不同工业互联网应用端到端的网络质量可靠性要求。五是提供网络编排能力，网络应通过开放接口支持工业和其他行业用户对网络功能和协议进行自定义。六是提供内嵌安全能力，实现内生安全与网络可溯源以便保障关键应用安全。

工业与外部网络的进一步融合，将推动个性化定制、远程监控、智能产品服务等新制造和服务模式。为此，工厂外部网络需要具备更高速率、更高质量、更低时延、安全可靠、灵活组网等能力，这些需求在目前的互联网上还无法满足，需采用 5G、软件定义网络（SDN）、网络功能虚拟化（NFV）等一系列新的网络技术和部署来支撑工业互联网发展。

(4) 目标架构

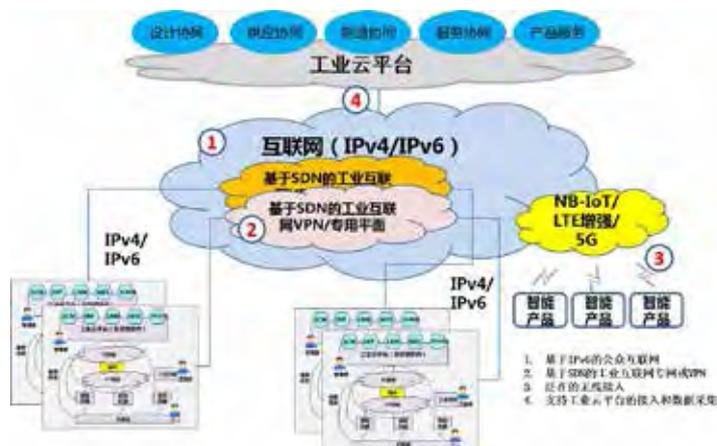


图7 工厂外部网络目标架构

工业互联网场景下工厂外部网络方案将包括四个主要环节，如图7所示，一是基于IPv6的公众互联网。工业互联网的终端数量将达到数百亿量级，IPv6在公众互联网中的部署势在必行，同时还需要考虑IPv4到IPv6的过渡网络方案。二是基于SDN的工业互联网专网或VPN。对一些网络质量要求较高，或比较关键的业务，需要用专网或VPN的方式来承载。专网中需要利用SDN、NFV等技术实现业务、流量的隔离，并实现网络的开放可编程。三是泛在无线接入。利用NB-IoT、LTE增强、5G等技术，实现对各类为满足各类海量的智能产品的无线接入。四是支持工业云平台的接入和数据采集。工厂外部网络支持企业信息化系统、生产控制系统，以及各类智能产品向工业云平台的数据传送和服务质量保证。

(三) 工业互联网地址与标识解析体系

1、标识及标识解析体系

(1) 现状分析

如同域名系统（DNS）在互联网中的作用一样，标识解析体系是工业互联网的关键神经系统。工业互联网中的标识，就类似于互联网中的域名，是识别和管理物品、信息、机器的关键基础资源。工业互联网中的标识解析系统，就类似互联网中的域名解析系统，是整个网络实现互联互通的关键基础设施。

目前国内外存在多种标识编码及标识解析方案。标识编码方面尚未统一，中小型企业内部大量使用自定义的私有标识，而涉及流通环节的供应链管理、产品溯源等应用模式正在逐步尝试跨企业的公有标识。标识解析方面总体可分成两大发展路径。以是否基于DNS区分，标识解析体系发展存在两条路径（改良路径和变革路径）。改良路径仍基于互联网DNS系统，对现有互联网DNS系统进行适当改进来实现标识解析，其中以美国GS1/EPCglobal组织针对EPC编码

提出的 ONS 解析系统相对成熟。国际上主要的标识解析体系在中国都授权设立了分支机构，如电子标准化院组建的 OID 注册中心，物品编码中心负责国内的 EPC 编码分配。同时我国相关单位也在基于 DNS 系统积极探索其它改良方案，如中科院计算机网络信息中心的物联网异构标识解析 NIOT 方案，中国信息通信研究院 CID 编码体系。国内单位通过在我国家顶级域 .CN 下注册二级域名，形成境内标识解析系统。同时为改变域名解析系统长期受制于美国的局面，国内互联网企业（天地互连公司）开展了根节点拓展实验“雪人计划”。变革路径采用区别于 DNS 的标识解析技术，目前主要是数字对象名称管理机构（DONA 基金会）提出的 Handle 方案，未来还可能出现新的技术方案。Handle 方案采用平行根技术，实现各国共同管理和维护根区文件，现已在 ITU、美、德及我国设置了 4 个根服务器，既可以独立于 DNS 又能够与现有 DNS 兼容。电子一所负责运营中国根。

目前各方案在国内均已启动并形成一定规模布局，且不同方案之间已具备互通能力，可以互相兼容、互通和共存。

（2）存在的问题

为支撑工业互联网发展，标识解析体系面临一些新的需求和挑战，现有标识解析体系尚难以完全满足这些需求。一是功能方面，由于工业互联网中的主体对象来源复杂、标识形式多样、难以统一，需要支持异构兼容性和有效扩展性。二是性能方面，工业互联网的标识数据将大大超过现有的互联网标识数据，需要工业互联网标识解析系统具有高效性和可靠性，针对工厂内柔性制造等特定场景还需要保障较低的解析时延。三是安全方面，由于工业互联网标识解析系统中存储了更多涉及到国计民生敏感数据，所以需要提供隐私保护、真实认证、抗攻击能力，攻击溯源能力。四是管控方面，标识是工业互联网重要的基础资源，可以反映和统计分析工业运行状态，需要更加公正平等的治理体系。目前主要标识解析系统是否能够满足工业互联网在功能、性能、安全、管控等方面的需求还需要检验。

（3）发展趋势

闭环的私有标识及解析系统正在逐步向开环的公共标识及解析系统演进。目前标识技术在资产管理、物流管理等部分环节得到应用和推广，并正在向生产环节渗透，如产线可以通过自动读取在制品标签标识来匹配相应的处理。随着面向产品全生命周期管理及跨企业产品信息交互需求的增加，将推动企业标识系统与公共标识解析的对接。标识对象也将随着自动化标识技术的应用逐步扩展，初期可能侧重产品标识，逐步覆盖原材料、软件系统等各种管理对象和要素。

多种标识解析体系在一定时期内共存。基于改良路径的方案和基于变革路径的方案在国内外均已启动并形成一定规模布局。从目前看，已有的标识类应用现状难以打破，短期内难以实现标识解析体系的统一。且目前多种方案已具备互通能力，可以相互兼容、互通和共存。

公平对等是标识解析的重要发展方向。传统互联网的治理格局长期不变，DNS 域名系统的最高管理权掌握在少数国家手中，这种集中化的单边管理机制既容易受到黑客攻击，又存在控制

权争议问题。目前，国内外已经提出并开始布局多种新型标识解析体系方案，如 ONS 在 2.0 版本已经支持并连根，Handle 采用平行根设计，其共同特征是倾向于分布式的多边管理机制，更加强调公平、对等。

2、工业互联网地址

工业互联网发展需要大量的 IP 地址。工业互联网需要支撑海量智能机器、智能产品的接入，而目前已趋于枯竭的 IPv4 地址难以满足未来工业互联网发展的海量地址空间需求。因此 IPv6 是工业互联网发展的必然选择。IPv6 在解决工业互联网地址需求的同时，也能为工厂内网各设备提供全球唯一地址，为更好的进行数据交互和信息整合提供了条件。

IPv6 在工业互联网应用的技术和管理将成为研究热点。IPv6 虽然已经研究了多年，但工业应用有其特殊性，尤其是工厂内网在安全性、可靠性、网络性能等方面都有较高的要求，因此 IPv6 与工业互联网结合的技术需要进一步深入研究。同时，工业生产关系国计民生，提前开展 IPv6 地址在工业互联网中分配和管理的研究，将有利于提高主管部门的互联网监管水平。

（四）工业互联网应用支撑体系

（1）现状分析

工业互联网应用支撑体系包括三个层面，一是实现工业互联网应用、系统与设备之间数据集成的应用使能技术，二是工业互联网应用服务平台，三是服务化封装与集成。

工业互联网应用、系统与设备集成的应用使能技术是支撑工业企业内部或工业企业与互联网数据分析平台之间实现数据集成和互操作的基础协议。与互联网中的 HTML 等协议类似，工业互联网中的应用使能技术的主要作用是在异构系统（不同的操作系统、不同的硬件架构等）之间实现数据层面的相互“理解”，实现信息集成与互操作。OPC 是目前应用较广泛的工厂内应用使能技术，其定义了一套通用的数据描述和语法表达方法（信息模型），每个系统可以将各自的数据信息以 OPC 的格式进行组织，从而可以被其他系统所获取和集成。

工业互联网应用服务平台目前主要体现为可集成部署各类工业云服务能力和资源的平台，以实现在线设计研发、协同开发等工业云计算服务。这类服务主要面向中小工业企业。一是通过在线的集成设计云服务可以为工业企业提供设计资源和工具服务。二是开展基于云平台的多方协作、设计众包等新型开发方式，实现制造资源高效整合。目前也逐步出现一些工业云服务平台，通过利用应用使能技术，实现对生产现场数据的有效采集与分析，并将结果应用于企业管理与决策。

目前工业企业服务化集成主要集中在工厂运营层信息系统中，大型企业通过企业服务总线（ESB）将 ERP、CRM、MES 等信息系统通过 SOA 化的形式进行资源组织，为企业运营提供基础管理支撑。在此基础上，向工厂 / 车间下沉的 MES 或者 SCADA 系统基本停留在业务逻辑预

置开发、数据库为中心的交互模式，而底层设备、物料等生产资源仍无法实现 SOA 化的服务资源调度。

（2）存在的问题

目前工业互联网应用支撑体系仍在发展的初期，存在三个主要问题：一是工业云平台的标准化和规范化问题。目前面向工业云平台缺乏标准与规范，企业可能会针对云服务业务绑定、数据迁移、数据安全等问题有所顾虑。二是应用使能技术通用性问题。目前 OPC 在工厂内部获得了较广泛的应用，在一定程度上解决了设备与系统信息交互与集成问题，但是 OPC 仅规范了读写格式，对于设备与系统缺乏结构化、模型化的规范化表示，因此对上层应用系统来说仍然是独立的 I/O 变量或功能，系统集成和业务逻辑复杂。三是服务化有待发展与探索。目前企业级各个信息系统已可以实现基于 SOA 的集成，但生产控制层面主要还是基于定制协议和定制逻辑，难以快速进行服务组合与设计。此外如何实现生产企业内部业务及数据的互联网服务化，还需探索。

（3）发展趋势

云计算逐步引入到工厂内部和工厂外部。一是以 IaaS 模式为基础开展工厂私有云和公共云建设。云计算为工业企业 IT 建设提供了更加高效率、低成本、可扩展的方式，通过 IaaS 可以在不对现有企业 IT 架构进行较大改变的情况下，实现系统到云端的平滑迁移。一些大企业可以自建私有云平台，或采用混合云模式充分利用公共云的能力，而中小企业则更多利用公共云服务，提升其 IT 建设能力。二是以 PaaS 平台构建工业应用新模式。PaaS 平台既有后端强大计算、存储能力的支撑，同时前端又可以以简单易用的 REST 接口实现应用的快速构建，可以满足工业企业对预测维护等创新应用的快速开发、部署需求。对于传统 PaaS 平台来说，面对工业互联网应用需求，需要实现对设计、生产、供应等各个环节的数据采集能力，并在云端构建面向工业各领域的特有分析模型和通用应用支撑能力。三是以 SaaS 平台向企业直接提供 IT 应用服务。目前已经有厂商针对企业管理、协同研发等领域提供 SaaS 服务，随着工业互联网的发展，面向工业领域的 SaaS 服务将逐步丰富，形成覆盖研发设计、协同制造、企业管理、产品服务全流程的应用产品。中小企业利用 SaaS 服务可以快速构建覆盖全生命周期的多样化应用。

应用使能技术工厂内外呈现不同趋势。一是工厂内不同系统间的数据集成协议。工厂内部以 OPC-UA 为代表的系统集成协议将得到更加广泛的应用，成为连接生产设备和 IT 系统的“数据总线”，以解决由于制造控制系统、IT 系统类型众多、厂商各异，数据格式、模型不同，无法被其他系统所“理解”和处理的问题。二是工业设备、产品到云平台之间的系统集成协议。工业设备、产品到云平台之间的系统集成协议则会形成以开放标准为主的协议集，为实现对产品制造、使用、维护等过程中数据的充分分析与利用，发挥生产、产品数据的最大价值，需要将来自生产现场和智能产品的异构数据通过网关或消息中间件的转换形成统一模型的数据信息发送到云端，实现集中分析处理。目前实现从生产现场到云端的应用系统集成协议类型很多，如 OASIS 的 MQTT 和 AMQP，IETF 的 CoAP 和 XMPP 等。

服务化封装与集成成为解决异构应用、系统与设备协同的重要手段。随着工业互联网的发展，各种智能设备、控制系统、信息系统、智能产品等将在工厂内部及整个互联网中实现互联与协作，通过对这些设备与系统的功能进行服务化封装，如通过服务化将生产设备由传统的数据源变为可重组的服务单元，从而可以简化各类业务与应用系统开发，并正在成为重要的发展方向。其中，基于语义的服务化封装，可以有效解决异构设备与系统的抽象与可认知问题，而受到产业的积极推进。

4) 目标架构

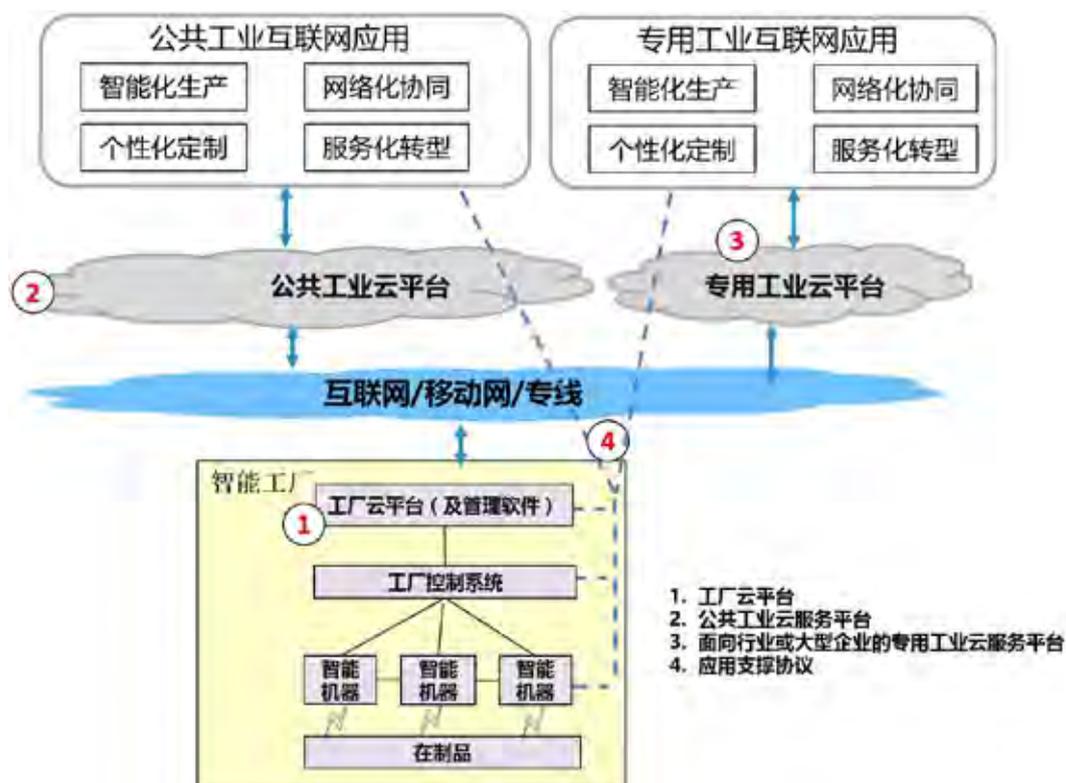


图 8 工业互联网应用支撑体系

工业互联网场景下应用支撑体系方案将包括四个主要环节，如图 8 所示，一是工厂云平台。在大型企业内部建设专有云平台，实现企业 / 工厂内的 IT 系统集中化建设，并通过标准化的数据集成，对内开展数据分析和运营优化。还可以考虑混合云模式，将部分数据能力及信息系统移植到公共云平台上，便于实现基于互联网的信息共享与服务协作。二是公共工业云服务平台。面向中小工业企业开展设计协同、供应链协同、制造协同、服务协同等新型工业互联网应用模式，及提供 SaaS 类服务。三是面向行业或大型企业的专用工业云服务平台。面向大型企业或特定行业，提供以工业数据分析为基础的专用云计算服务。四是工厂内各生产设备、控制系统和 IT 系统间的数据集成协议，以及生产设备、IT 系统到工厂外云平台间的数据集成和传送协议。

四、工业互联网的数据体系

（一）工业大数据内涵特征

工业大数据是指在工业领域信息化应用中所产生的数据，是工业互联网的核心，是工业智能化发展的关键。工业大数据是基于网络互联和大数据技术，贯穿于工业的设计、工艺、生产、管理、服务等各个环节，使工业系统具备描述、诊断、预测、决策、控制等智能化功能的模式和结果。工业大数据从类型上主要分为现场设备数据、生产管理数据和外部数据。现场设备数据是来源于工业生产线设备、机器、产品等方面的数据，多由传感器、设备仪器仪表、工业控制系统进行采集产生，包括设备的运行数据、生产环境数据等。生产管理数据是指传统信息管理系统中产生的数据，如 SCM、CRM、ERP、MES 等。外部数据是指来源于工厂外部的数据，主要包括来自互联网的市场、环境、客户、政府、供应链等外部环境的信息和数据。

工业大数据具有五大特征。一是数据体量巨大，大量机器设备的高频数据和互联网数据持续涌入，大型工业企业的数据集将达到 PB 级甚至 EB 级别。二是数据分布广泛，分布于机器设备、工业产品、管理系统、互联网等各个环节。三是结构复杂，既有结构化和半结构化的传感数据，也有非结构化数据。四是数据处理速度需求多样，生产现场级要求实现实时时间分析达到毫秒级，管理与决策应用需要支持交互式或批量数据分析。五是对数据分析的置信度要求较高，相关关系分析不足以支撑故障诊断、预测预警等工业应用，需要将物理模型与数据模型结合，追踪挖掘因果关系。

（二）工业互联网大数据功能架构

工业互联网数据架构，从功能视角看，主要由数据采集与交换、数据预处理与存储、数据建模、数据分析和数据驱动下的决策与控制应用四个层次五大部分组成，如图 9 所示。

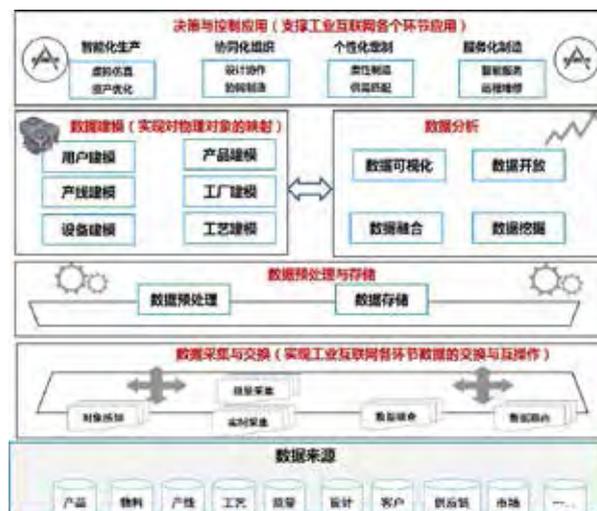


图 9 工业互联网数据体系参考架构

数据采集与交换层主要实现工业各环节数据的采集与交换，数据源既包含来自传感器、SCADA、MES、ERP 等内部系统的数据，也包含来自企业外部的数据，主要包含对象感知、实时采集与批量采集、数据核查、数据路由等功能。

数据预处理与存储层的关键目标是实现工业互联网数据的初步清洗、集成，并将工业系统与数据对象进行关联，主要包含数据预处理、数据存储等功能。

数据建模层根据工业实际元素与业务流程，在数据基础上构建用户、设备、产品、产线、工厂、工艺等数字化模型，并结合数据分析层提供数据报表、可视化、知识库、数据分析工具及数据开放功能，为各类决策的产生提供支持。

决策与控制应用层主要是基于数据分析结果，生成描述、诊断、预测、决策、控制等不同应用，形成优化决策建议或产生直接控制指令，从而实现个性化定制、智能化生产、协同化组织和服务化制造等创新模式，并将结果以数据化形式存储下来，最终构成从数据采集到设备、生产现场及企业运营管理持续优化闭环。

（三）工业互联网大数据应用场景

工业大数据的应用覆盖工业生产的全流程和产品的全生命周期。工业大数据的作用主要表现为状态描述、诊断分析、预测预警、辅助决策等方面，在智能化生产、网络化协同、个性化定制和服务化延伸四类场景下发挥着核心的驱动作用。工业大数据技术应用示意如图 10 所示。

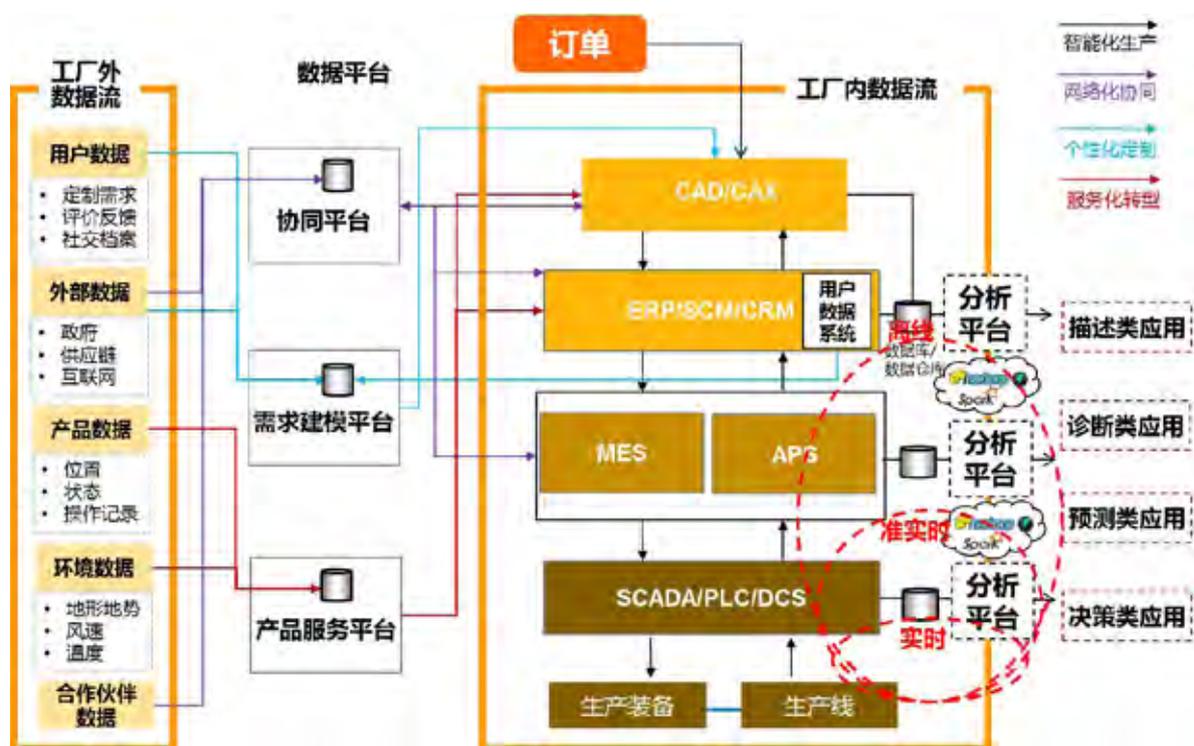


图 10 工业互联网大数据技术应用示意

(1) 智能化生产中的工业大数据应用

虚拟设计与虚拟制造。虚拟设计与虚拟制造是指将大数据技术与 CAD、CAE、CAM 等设计工具相结合，深入了解历史工艺流程数据，找出产品方案、工艺流程、工厂布局与投入之间的模式和关系，对过去彼此孤立的各类数据进行汇总和分析，建立设计资源模型库、历史经验模型库，优化产品设计、工艺规划、工厂布局规划方案，并缩短产品研发周期。

生产工艺与流程优化。生产工艺与流程优化是指应用大数据分析功能，评估和改进当前操作工艺流程，对偏离标准工艺流程的情况进行报警，快速地发现错误或者瓶颈所在，实现生产过程中工艺流程的快速优化与调整。

设备预测维护。设备预测性维护是指建立大数据平台，从现场设备状态监测系统和实时数据库系统中获取设备振动、温度、压力、流量等数据，在大数据平台对数据进行存储管理，进一步通过构建基于规则的故障诊断、基于案例的故障诊断、设备状态劣化趋势预测、部件剩余寿命预测等模型，通过数据分析进行设备故障预测与诊断。

智能生产排程。智能生产排成是指收集客户订单、生产线、人员等数据，通过大数据技术发现历史预测与实际的偏差概率，考虑产能约束、人员技能约束、物料可用约束、工装模具约束，通过智能的优化算法，制定预计划排产，并监控计划与现场实际的偏差，动态的调整计划排产。

产品质量优化。产品质量优化是指通过收集生产线、产品等实时数据和历史数据，根据以往经验建立大数据模型，对质量缺陷产品的生产全过程进行回溯，快速甄别原因，改进生产问题，优化提升产品质量。

能源消耗管控。能源消耗管控是指对企业生产线各环节能耗排放和辅助传动输配环节的实时监控，收集生产线、关键环节能耗等相关数据，建立能耗仿真模型，进行多维度能耗模型仿真预测分析，获得生产线各环节的节能空间数据，协同操作智能优化负荷与能耗平衡，从而实现整体生产线柔性节能降耗减排，及时发现能耗的异常或峰值情况，实现生产过程中的能源消耗实时优化。

(2) 网络化协同中的工业大数据应用

协同研发与制造。协同研发与制造主要是基于统一的设计平台和制造资源信息平台，集成设计工具库、模型库、知识库及制造企业生产能力信息，不同地域的企业或分支机构可以通过工业互联网网络访问设计平台获取相同的设计数据，也可获得同类制造企业闲置生产能力，实现多站点协同、多任务并行、多企业合作的异地协同设计与制造要求。

供应链配送体系优化。供应链配送体系优化主要是通过 RFID 等产品电子标识技术、物联网技术以及移动互联网技术获得供应商、库存、物流、生产、销售等完整产品供应链的大数据，利用这些数据进行分析，确定采购物料数量、运送时间等，实现供应链优化。

(3) 个性化定制中的工业大数据应用

用户需求挖掘。用户需求挖掘主要指建立用户对商品需求的分析体系，挖掘用户深层次

的需求，并建立科学的商品生产方案分析系统，结合用户需求与产品生产，形成满足消费者预期的各品类生产方案等，实现对市场的预知性判断。

个性化定制生产。个性化定制生产主要指采集客户个性化需求数据、工业企业生产数据、外部环境数据等信息，建立个性化产品模型，将产品方案、物料清单、工艺方案通过制造执行系统快速传递给生产现场，进行产线调整和物料准备，快速生产出符合个性化需求的定制化产品。

（4）服务化延伸中的工业大数据应用

产品远程服务。产品远程服务是指通过搭建企业产品数据平台，围绕智能装备、智能家居、可穿戴设备、智能联网汽车等多类智能产品，采集产品数据，建立产品性能预测分析模型，提供智能产品的远程监测、诊断与运维服务，创造产品新的价值，实现制造企业的服务化转型。

（四）存在的问题

工业大数据应用的主要障碍在于以下几点：一是企业数据源较差，尤其是对于机器设备、生产线等实时生产数据采集数量、类型、精度以及频率方面存在较大提升空间。二是企业间和企业内部部门间信息孤岛普遍存在，数据的交互、共享和集成存在很大障碍，数据融合应用价值难以有效挖掘利用。三是缺乏工业大数据应用成熟模式和灯塔式项目，尽管一些先进企业正在进行工业大数据应用的尝试，但仍处于初级阶段，应用经验积累不多，尚未形成行业应用推广模式。四是工业大数据核心技术、软件平台产品，以及系统集成和应用开发能力仍然有待加强，安全可控能力不足。

（五）发展趋势

随着工业互联网建设和应用不断深入，数据的价值与作用将越来越凸显，数据分析将向工业各环节渗透，预测、决策、控制等更智能的应用成为发展方向，最终构成从数据采集到设备、生产现场及企业运营管理优化的闭环。工业数据未来将呈现出以下几个发展方向：一是跨层次跨环节的数据整合。当前工业数据水平来看分散在研发设计、生产管理、企业经营等各个环节，垂直来看分散在生产现场、企业管理（MES、ERP）等不同层次，下一步数据在垂直和水平两个方向都需要整合，为全局视图分析奠定数据基础。其中语义技术将发挥重要作用，利用语义可以对工业互联网数据的含义进行标注，使数据在异构系统之间能够被正确理解和处理。二是数据在边缘的智能处理。在靠近数据源头的网络边缘节点上，通过融合计算、存储与控制等功能，实现数据的边缘处理、分析与过滤，以满足工业生产现场实时连接、实时控制、实时分析、安全隐私等需求，并可以与云平台实现互补。三是基于云平台数据集成管理。将数据汇聚起来，

上传到云计算平台进行分析处理，是未来的主流方向，基于成熟的、经验证的技术以及大数据平台来支撑工业数据的数据建模、数据抽取 ETL、查询与计算，与传统实时数据库、关系数据库和 MPP 数据混搭应用，是云化的工业大数据平台构建的主流方向。四是深度数据分析挖掘。知识驱动的分析方法，建立在工业系统的物理化学原理、工艺及管理经验等知识之上。数据驱动的分析方法，完全在数据空间中通过算法寻找规律和知识。未来的发展趋势是更多的将基于知识的方法与数据驱动方法融合，满足工业数据分析对高置信度的要求。五是数据可视化。建立机器、生产流程、全生产周期等拟真数字化模型，并进行可视化呈现，使生产管理者、系统开发者和用户能够更加直观全面地了解相关信息，支撑设计、生产、产品流通与交易、产品服务等环节的决策水平。



五、工业互联网的安全体系

(一) 工业互联网安全体系框架

工业互联网的安全需求可从工业和互联网两个视角分析。从工业视角看，安全的重点是保障智能化生产的连续性、可靠性，关注智能装备、工业控制设备及系统的安全；从互联网视角看，安全主要保障个性化定制、网络化协同以及服务化延伸等工业互联网应用的安全运行以提供持续的服务能力，防止重要数据的泄露，重点关注工业应用安全、网络安全、工业数据安全以及智能产品的服务安全。因此，从构建工业互联网安全保障体系考虑，工业互联网安全体系框架主要包括五大重点，设备安全、网络安全、控制安全、应用安全和数据安全，如图 11 所示。

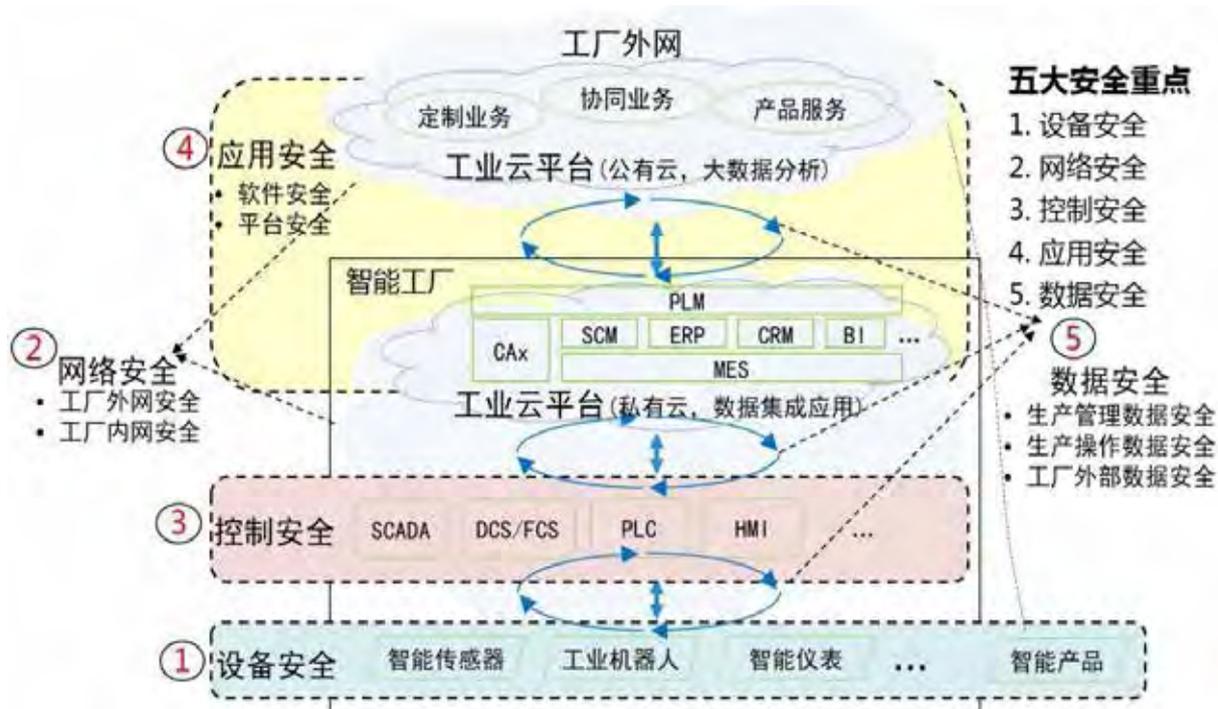


图 11 工业互联网安全体系

其中，设备安全是指工业智能装备和智能产品的安全，包括芯片安全、嵌入式操作系统安全、相关应用软件安全以及功能安全等；网络安全是指工厂内有线网络、无线网络的安全，以及工厂外与用户、协作企业等实现互联的公共网络安全；控制安全是指生产控制安全，包括控制协议安全、控制平台安全、控制软件安全等；应用安全是指支撑工业互联网业务运行的应用软件及平台的安全；数据安全是指工厂内部重要的生产管理数据、生产操作数据以及工厂外部数据（如用户数据）

等各类数据的安全。

（二）现状分析

随着互联网与工业融合创新的不断推动，电力、交通、市政等大量关系国计民生的关键信息基础设施日益依赖于网络，并逐步与公共互联网连接，一旦受到网络攻击，不仅会造成巨大经济损失，更可能带来环境灾难和人员伤亡，危及公众生活和国家安全，安全保障能力已成为影响工业互联网创新发展的关键因素。总的来看，由于信息化和自动化程度的不同，工业细分行业的安全保障体系建设情况也各不相同，信息化、自动化程度越高的行业，开放程度也相对较高，面临的安全风险随之增大，对安全也更加重视，安全保障体系建设相对更完善。

目前，工业领域安全防护采用分层分域的隔离和边界防护思路。工厂内网与工厂外网之间通常部署隔离和边界防护措施，采用防火墙、VPN、访问控制等边界防护措施保障工厂内网安全。从工厂内网来看，可进一步分为企业管理层和生产控制层。企业管理层主要包括企业管理相关的ERP、CRM等系统，与传统IT系统类似，主要关注信息安全的内容，采用权限管理、访问控制等传统信息系统安全防护措施，与生产控制层之间较多的采用工业防火墙、网闸等隔离设备，一般通过白名单方式对工业协议如OPC等进行过滤，防止来自互联网的威胁渗透到生产过程。生产控制层包括工程师站、操作员站等工作站，以及PLC、DCS等控制设备，与生产过程密切相关，对可靠性和实时性要求高，主要关注功能安全的问题。因此，尽管工程师站、操作员站等目前仍多采用win2000/XP等操作系统，但考虑到系统稳定性以及对功能安全的影响，极少升级补丁，一般也不安装病毒防护软件等。同时，传统生产控制层以物理隔离为主，信息安全隐患低，工业私有协议应用较多，工业防火墙等隔离设备需针对专门协议设计，企业更关注生产过程的正常进行，一般较少在工作站和控制设备之间部署隔离设备以避免带来功能安全问题。此外，控制协议、控制软件在设计之初也缺少诸如认证、授权、加密等安全功能，生产控制层安全保障措施的缺失成为工业互联网演进过程中的重要安全问题。

总体来看，业界在积极推动工业防火墙、工业安全监测审计、安全管理等安全产品的应用，但整体对工业互联网安全的研究及产业支持还处于起步阶段，现有措施难以有效应对工业互联网发展过程中日益复杂的安全问题。从工业互联网未来演进看，工业网络基础设施、控制体系、工业数据和个人隐私、智能设备以及工业应用的安全保障是未来发展的重点。

（三）存在的问题

随着工业融合创新以及工业互联网的不断演进，工厂环境更加开放，未来工业互联网安全主要面临以下几方面的问题，一是设备安全问题。传统生产设备以机械装备为主，重点关注物理和功能安全，未来生产装备和产品将越来越多的集成通用嵌入式操作系统及应用软件，海量设备将直接暴露在网络攻击之下，木马病毒在设备之间的传播扩散速度将呈指数级增长。二是

网络安全问题。工厂网络向“三化（IP化、扁平化、无线化）+灵活组网”方向发展，面临更多安全挑战。现有针对TCP/IP协议的攻击方法和手段成熟，可被直接利用攻击工厂网络。网络灵活组网需求使网络拓扑的变化更加复杂，传统静态防护策略和安全域划分方法面临动态化、灵活化挑战。无线技术的应用需要满足工厂实时性可靠性要求，难以实现复杂的安全机制，极易受到非法入侵、信息泄露、拒绝服务等攻击。三是控制安全问题。当前工厂控制安全主要关注控制过程的功能安全，信息安全防护能力不足。现有控制协议、控制软件等在设计之初主要基于IT和OT相对隔离以及OT环境相对可信这两个前提，同时由于工厂控制的实时性和可靠性要求高，诸如认证、授权和加密等需要附加开销的信息安全功能被舍弃。IT和OT的融合打破了传统安全可信的控制环境，网络攻击从IT层渗透到OT层，从工厂外渗透到工厂内，但目前有效的APT攻击检测和防护手段缺乏。四是应用安全问题。网络化协同、服务化延伸、个性化定制等新模式新业态的出现对传统公共互联网的安全能力提出了更高要求。工业应用复杂，安全需求多样，因此对网络安全隔离能力、网络安全保障能力要求都将提高。五是数据安全问题。工业数据由少量、单一、单向正在向大量、多维、双向转变，具体表现为工业互联网数据体量大、种类多、结构复杂，并在IT和OT层、工厂内外双向流动共享。工业领域业务应用复杂，数据种类和保护需求多样，数据流动方向和路径复杂，重要工业数据以及用户数据保护难度增大。

（四）发展趋势

随着工业互联网的发展演进，以下将成为业界主要关注和推进的重点内容。一是设备内嵌安全机制。生产装备由机械化向高度智能化转变，内嵌安全机制将成为未来设备安全保障的突破点，通过安全芯片、安全固件、可信计算等技术，提供内嵌的安全能力，防止设备被非授权控制或功能安全失效。二是动态网络安全防御机制。针对工厂内灵活组网的安全防护需求，实现安全策略和安全域的动态调整，同时通过增加轻量级的认证、加密等安全机制保障无线网络的传输安全。三是信息安全和功能安全融合机制。工厂控制环境由封闭到开放，信息安全威胁可能直接导致功能安全失效，功能安全和信息安全关联交织，未来工厂控制安全需综合考虑功能安全和信息安全的需求，形成综合安全保障能力。四是面向工业应用的灵活安全保障能力。业务应用呈现多样化，未来需要针对不同业务的安全需求提供灵活的安全服务能力，提供统一灵活的认证、授权、审计等安全服务能力，同时支持百万级VPN隔离及用户量增长；五是工业数据以及用户数据分类分级保护机制。对重要工业数据以及用户数据进行分类分级，并采用不同的技术进行分级保护，通过数据标签、签名等技术实现对数据流动过程的监控审计，实现工业数据全生命周期的保护。

六、工业互联网的实施

(一) 工业系统现状及实施目标

现阶段工业系统的数字化、网络化已具备一定基础，但与工业互联网泛在互联、全生命周期数字链等愿景相比，在网络、数据、安全等方面还存在很大改造和提升的空间。现阶段工业系统实现架构如图 12 所示，在网络互联方面，工业网络层级复杂、现场总线、工业以太网、普通以太网等多种联网技术并存但以有线为主，工厂与外部互联有限；在数据智能方面，不同层级之间的数据相对隔离，底层设备采集有限，系统间数据集成困难，云、大数据等技术还未有效开展；在安全保障方面，以满足现有工业系统的安全保障需求为主，且更多侧重功能安全。



图 12 现阶段工业系统实现架构

在工业互联网背景下，工业系统在网络互联、数据智能、安全保障等方面将进行快速的迭代演进，云和大数据技术逐步引入，扁平化的软硬件部署架构成为重要发展趋势，从而引发工业系统各层级网络、数据和安全的深刻变化。结合工业互联网网络、数据、安全发展趋势，本报告给出的工业互联网目标实现架构如图 13 所示。



图 13 工业互联网目标实现架构

工业互联网目标实现架构主要呈现四个方面关键特征：一是体系架构方面，实现层级打通、内外融合，传统工业系统多层结构逐渐演变为应用层、平台层和边缘层三层，整体架构呈现扁平化发展趋势；二是网络互联方面，各种智能装备实现充分网络化，无线成为有线的重要补充，新型网关推动异构互联和协议转换，工厂与产品、外部信息系统和用户充分互联；三是在数据智能方面，工业云平台成为关键核心，实现工厂内外部数据的充分汇聚，支撑数据的存储、挖掘和分析，有效支撑工业信息控制系统和各种创新应用；四是在安全保障方面，各种安全机制与工业互联网各个层次深度融合，实现纵深防御，立体防护，通过多种安全措施保障网络互联和数据集成安全。工业互联网目标架构的实现将是一个长期过程，需要网络、数据、安全等方面逐步协同推进。

（二）工业互联网网络的实施

（1）网络互联的实施

网络互联的实施主要是解决工业互联网各种设备、系统之间互联互通的问题，涉及现场级、车间级、企业级设备和系统之间的互联，以及企业信息系统、产品、用户与云平台之间不同互联场景，针对现有工业系统既包含现有设备与系统的网络化改造，还包含新型网络连接的建设。网络互联的实施涉及的主要环节如图 14 所示。

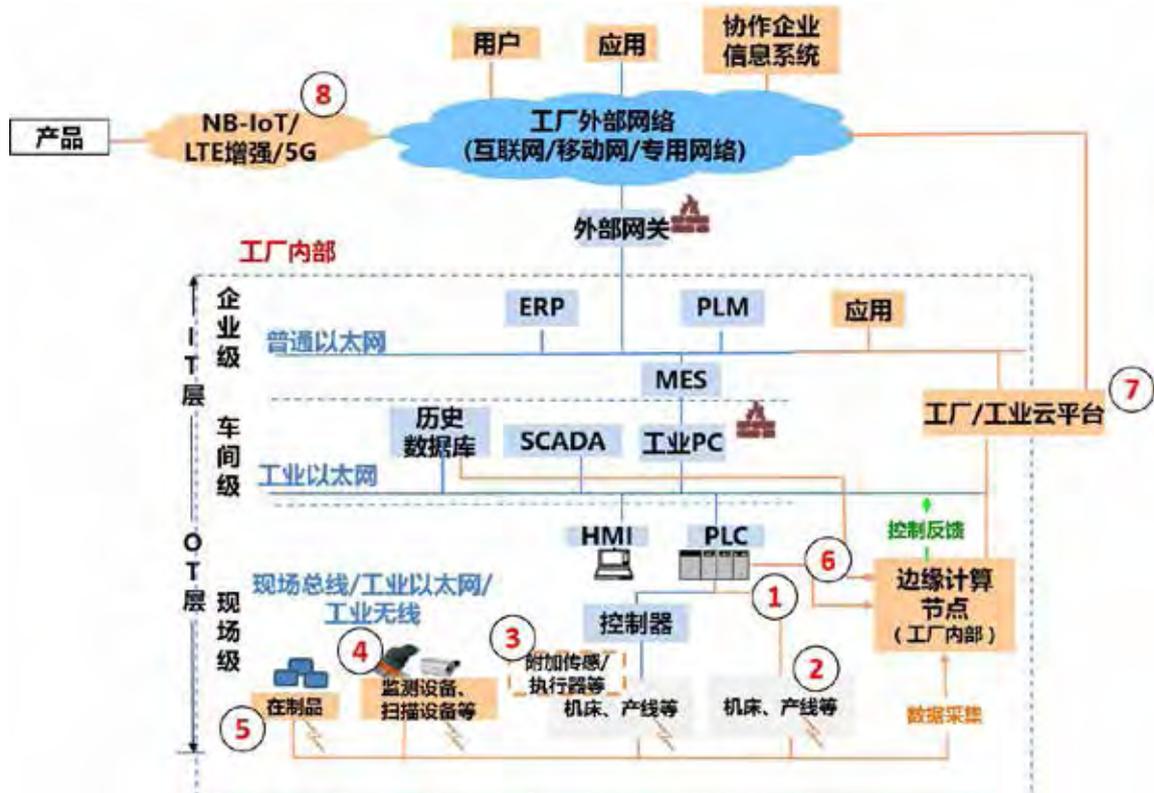


图 14 网络互联的实施

在现场级和车间级，主要实现底层设备横向互联以及与上层系统纵向互通的连接。一是对控制器与机床、产线等装备装置的通信方式进行改造，如以工业以太网代替现场总线。二是现有工业装备或装置，如机床、产线等，增加网络接口，三是对现有工业装置或装备附加传感器、执行器等增加与外部的信息交互。四是为了采集生产现场信息或执行反馈控制，部署新的监测设备、扫描设备、执行器等。五是对在制品通过内嵌通信模块或附加标签等方式，增加与工业系统的信息交互功能。六是部署边缘计算节点，汇聚生产现场数据及来自工业控制系统如 PLC、历史数据库的数据，并进行数据的边缘处理。具体采用的联网方式需要结合通信需求、布线情况、电源供应等，并充分结合 IP 化、无线化等趋势，如针对在制品，可以采用短距离通信和标识技术，如蓝牙、二维码、RFID 等；针对生产装备或装置，可以直接利用现有的联网方式，也可以考虑利用工业以太网、工业无线等增加联网接口；针对监测设备，如果实时性要求不高，可以采用有线宽带通信、无线宽带、LTE 增强、NB-IoT、5G 等技术。

在工厂企业级或工厂外部，应注重引入云平台和大数据技术，并通过云平台实现与生产设备或装置、工业控制系统、工业信息系统、工业互联网应用之间的信息交互，以及与协作企业信息系统、智能产品、用户之间的信息交互，以便为制造企业提供提供不同地域、不同功能的各类系统的横向互联，以及与上层应用、跨企业 / 跨行业各类主体之间的互联，为价值链协作提供支持。具体联网方式也依赖于互联场景，如针对工厂 / 工业云平台与生产设备或装置、工业控制系统、

工业信息系统之间的互联，可以直接利用现有的互联网或企业级信息网络；针对工厂 / 工业云平台与协作企业信息系统，可能要考虑建立安全、可靠的 VPN 专线来实现信息交互；针对工厂 / 工业云平台与产品，可以采用 NB-IoT、LTE 增强以及未来的 5G 等广域移动通信网络及各种有线通信。

(2) 标识解析的实施

标识解析的实施主要通过标识技术的应用，实现对零原材料、在制品、产品等信息的自动读写，并借助标识解析系统，实现对产品全生命周期管理以及各级异构系统之间的信息交互。标识解析的实施涉及的主要环节如图 15 所示。

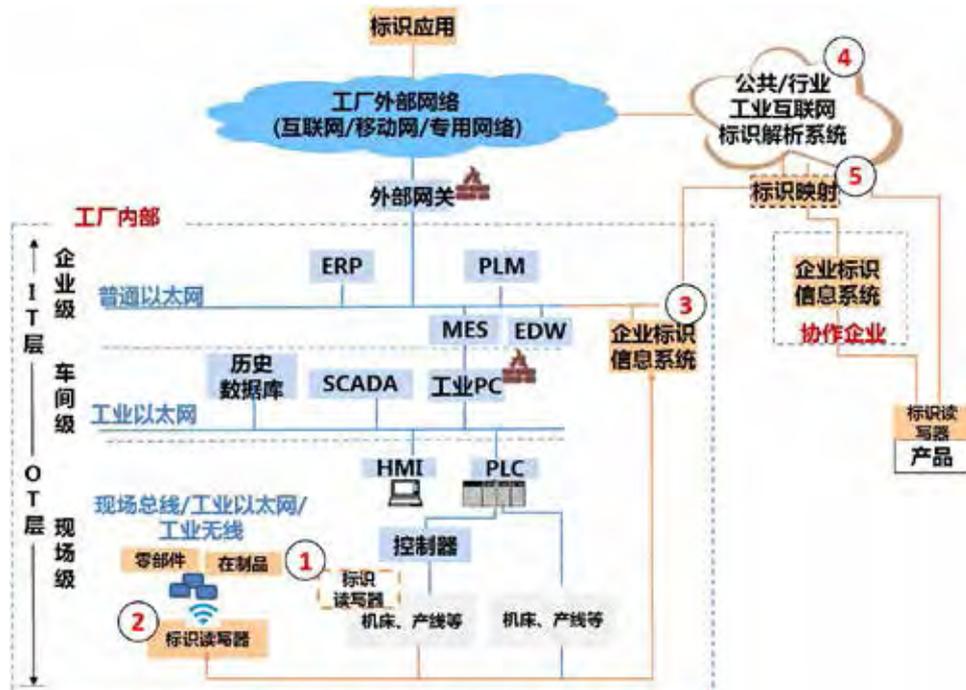


图 15 标识解析的实施

在工厂内部，为推动标识解析技术应用，一是根据需求对拟跟踪对象进行标识，可以标识设备、原材料、在制品、产品，另外也可以为部门机构、订单、工艺、人等赋予标识；二是部署标识读写器，可以嵌入在机床等装备上，也可以单独部署，通过标识读写器实现对标识的自动识读，或同时进行信息的写入；三是建设标识信息系统，实现对企业内部标识及相关信息管理，同时支持与公共 / 行业工业互联网标识解析系统的对接。

在工厂外部，核心是围绕产品标识实现跨企业、跨行业、跨地区的产品信息管理。一是需要根据工业互联网标识解析和应用需求，建设公共标识解析系统、行业级标识解析系统，并与企业标识信息系统、标识读写设备对接，以支撑各种基于标识的应用；二是考虑到现在一些企业或行业已经应用标识解析，但以私有解决方案为主，同时考虑到目前多种标识解析方案共存，为实现跨企业、跨行业的标识及信息交互，需要提供标识映射和信息对接机制。

(3) 应用支撑的实施

应用支撑的实施主要是解决工业互联网各种数据、服务的集成分析和利用，并为上层工业互联网应用提供支撑，其中关键是推动工厂 / 工业云平台建设，提供数据存储分析处理、应用支撑、开放接口等。工厂 / 工业云平台的实施包含三种方式，具体如图 16、图 17、图 18 所示。

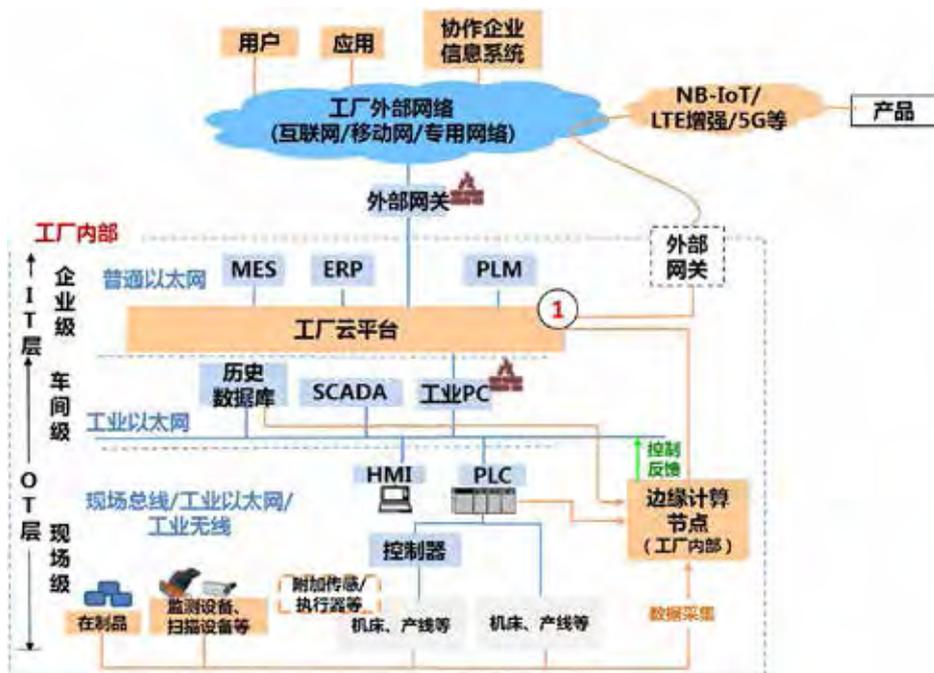


图 16 方式一：工厂云平台的实施

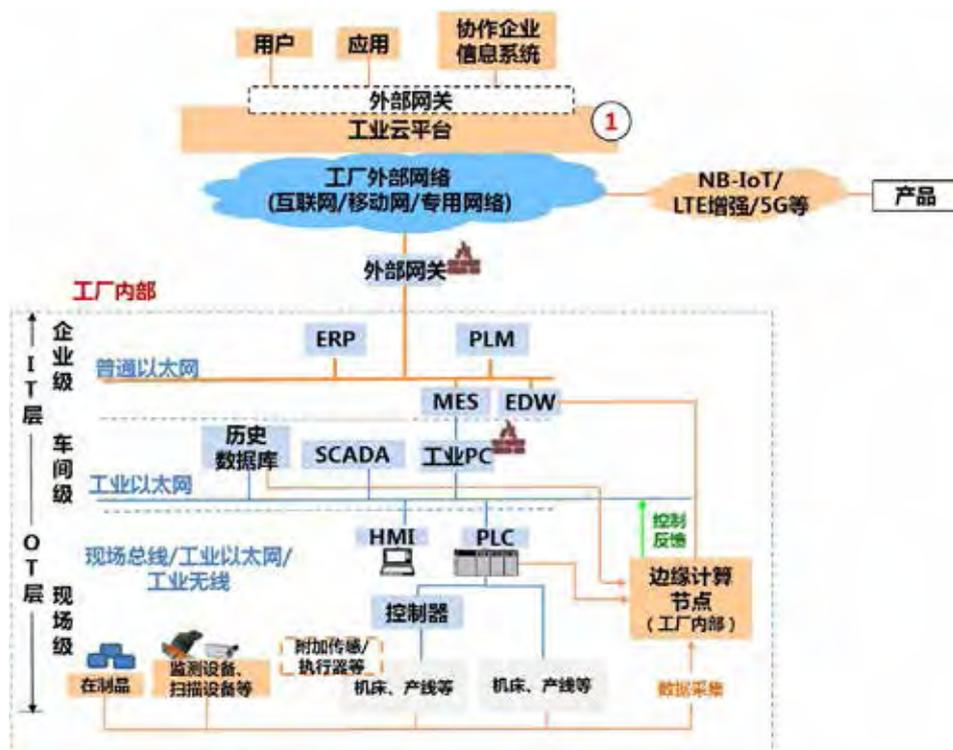


图 17 方式二：工业云平台的实施



图 18 方式三：混合云的实施

方式一是工厂云平台的实施，即在工厂内部部署云平台，汇聚工厂内部的各种数据，包括来自产线上传各类机器、仪表等采集数据以及来自工厂信息和管理系统的数据，根据需要还可以对外互联汇聚来自用户、产品、协作企业的信息，最终目标是实现对设备、产线、工厂等物理对象以及工艺、加工流程等的无损数字化映射与描述，在此基础上还可以是实现对这些软硬件的服务化组合与调用，同时还可以为 MES、ERP 等工业信息系统提供运行平台环境。

方式二是工业云平台的实施，工业云平台部署在互联网等公共网络上，可以汇聚来自设计、生产、物流、市场、产品、用户等工业互联网价值链上的数据，目标是实现围绕生产全生命周期、全价值链的全局数据分析和优化。同时工业云平台可以与工厂信息系统交互，使工业云平台可以调用工厂内部数据，工厂内部信息系统也可以调用外部数据。

方式三是混合云的实施，即工厂云平台与工业云平台协同部署的方式。企业内部耦合紧密的信息或系统运行在工厂云平台上，而将适宜对外提供的数据、服务或对外交互的系统运行在工业云平台上。

同时工厂 / 工业云平台与边缘计算节点之间应相互相互，边缘计算节点根据实时性、安全性隐私等要求，对数据进行本地化处理，同时对过滤后的数据传送到工厂 / 工业云平台，形成“基于云计算的全局优化 + 基于边缘计算的局部优化”的趋势。

应用使能技术实施方面，在工厂内部，对于新上线的设备和系统（包括工厂云平台），应考虑其对 OPC-UA 的支持；在工厂外部，工业云平台应考虑对 OPC-UA、MQTT XMPP 等多种的应用使能技术的支持，以及协议适配和转换的功能，以支持采用不同应用使能技术的设备和系统接入。

服务化封装与集成实施方面，在对设备和系统进行改造过程中，应考虑对设备和系统功能进行服务化抽象和封装，并提供服务调用接口。如果对设备和系统直接改造困难，可以考虑部署服务适配器（可以是独立的硬件，也可以是软件中间件），由服务适配器对这些设备和系统的功能进行服务化抽象和封装，并提供服务调用接口。同时在云平台上应提供服务适配、注册、发现、组合以及管理等功能，以支持服务的灵活编排和调用。在服务化封装与集成的实施和推进过程中，应逐步引入语义技术。

（三）工业互联网数据的实施

工业互联网数据的实施涉及数据全面的采集与流动、工业数据云平台建设，以及多层次数据处理和分析能力构建，在此基础上支撑各种智能应用，同时应注意构建数据反馈闭环，以实现信息系统之间以及信息系统与物理系统之间的相互作用。工业互联网数据的实施涉及的主要环节如图 19 所示。



图 19 工业互联网数据的实施

一是推动工厂管理软件之间的信息交互，目前很多企业在工厂内部已经部署了一些管理软件，如研发设计类软件（CAD、CAE、CAPP、CAM等）、生产管理软件、客户管理软件CRM、供应链管理软件SCM等，但有些企业的这些管理软件之间缺乏有效的信息交互与集成，应推动这些管理软件之间的数据流动；二是推进全面数据感知采集，包括采集机器、在制品等运行状态信息，采集生产环境信息，并可以考虑从工业控制系统采集必要的信息；三是可以考虑部署边缘计算节点，实现边缘数据分析处理智能，同时构建边缘数据控制闭环，满足边缘实时控制、数据安全等要求；四是利用云和大数据技术，推动工厂内部数据集成分析，同时构建决策反馈闭环，实现对工业生产的控制以及各种智能管理决策应用；五是通过工厂外部的工业云平台，汇聚产品数据、用户数据、环境数据、协作企业数据等等，并利用大数据技术，实现海量、复杂数据的综合存储、分析和处理；六是构建综合反馈闭环，在工业云平台大数据集成与分析基础上，建立从工业云平台到企业级信息系统的综合性分析反馈闭环，提升工厂内外的联动。

（四）工业互联网安全的实施

随着工业互联网的创新发展，现有相对封闭的工业系统更加开放，将面临更新新的安全问题和挑战，工业互联网需要通过综合性的安全防护措施，保证设备、网络、控制、数据和应用安全。工业互联网安全实施涉及的主要环节如图 20 所示。

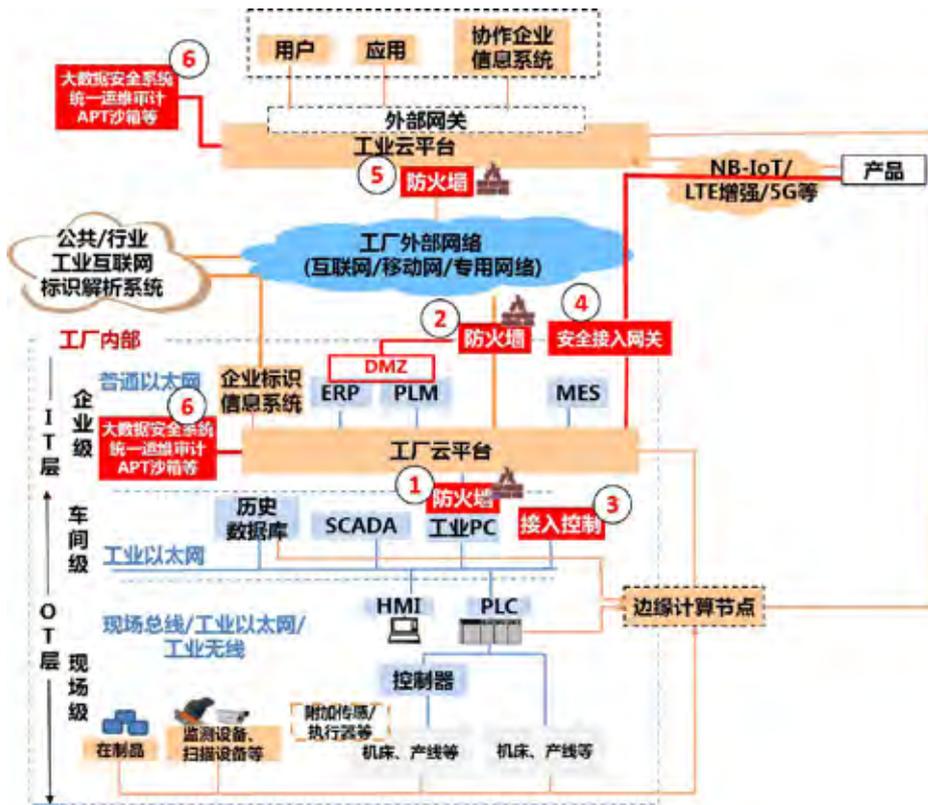


图 20 工业互联网安全的实施

工厂互联网各互联单元之间应该进行有效可靠的安全隔离和控制。一是工业控制系统与工业信息系统之间，应部署防火墙；二是工厂外部对工厂内部云平台的访问应经过防火墙，并提供 DDoS 防御等功能，ERP、PLM 等与外部进行交互的服务和接口应部署在 DMZ 区域，同时部署网络入侵防护系统，可对主流的应用层协议及内容进行识别，高速高效的自动检测和定位各种业务层的攻击和威胁；三是工厂内部所有接入工厂内部云平台、工厂信息系统、工业控制系统的设备，都必须实现接入控制，进行接入认证和访问授权；四是工厂外部接入工厂内部云平台的智能产品、移动办公终端、信息系统等，应经过运行有远端防护软件的安全接入网关；五是对部署在公共互联网上的工业云平台的各种访问应经过防火墙，并提供 DDoS 防御等功能；六是采用基于大数据的安全防护技术，在工厂云平台、工业云平台上部署大数据安全系统，基于外部威胁情报、日志分析、流量分析和沙箱联动，对已知和未知威胁进行综合防御，并准确展示安全全貌，实现安全态势智能感知。

此外，工业互联网安全实施应当强化智能产品和网络传输数据的安全防护。一是智能产品的安全加固。智能产品的部署位置分散，容易被破坏、伪造、假冒和替换，导致敏感泄露。因此应当对智能产品进行专门的安全加固，如采用安全软件开发工具包（SDK）、安全操作系统、安全芯片等技术手段，实现防劫持、防仿冒、防攻击和防泄密。二是外部公共网络数据传输的安全防护。通过外部网络传输的数据，应采用 IPsec VPN 或者 SSL VPN 等加密隧道传输机制或 MPLS VPN 等专网，防止数据泄漏、被侦听或篡改。



附件 1：术语与定义

序号	词汇	英文	定义	备注
1	工业互联网	industrial internet	工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施	
2	智能制造	intelligent manufacturing	基于物联网、大数据、云计算等新一代信息技术，贯穿于设计、生产、管理、服务等制造活动的各个环节，具有信息深度自感知、智慧优化自决策、精准控制自执行等功能的先进制造过程、系统与模式的总称	
3	众包众创	crowdsourcing	借助互联网等手段，将传统由特定企业和机构完成的任务向自愿参与的所有企业和个人进行分工，最大限度利用大众力量，以更高的效率、更低的成本满足生产及生活服务需求，促进生产方式变革。	参考国发〔2015〕53号
4	个性定制	customization	通过互联网平台，将用户需求和企业产品设计、生产计划精确匹配，并借助模块化产线和新型制造工艺，实现的产品多样化、定制化生产制造模式	
5	协同设计	collaborative design	企业与企业之间，通过网络化的设计平台，分工并行开展的产品设计模式，可有效缩短产品设计周期。	
6	协同制造	collaborative manufacturing	基于网络协同平台，将制造任务、订单信息分配给不同地域、不同规模的制造企业，将社会分散的制造资源、制造能力在网络平台进行集聚共享，形成网络化协同的生产组织模式。	
7	柔性制造	flexible Manufacturing	由统一的信息控制系统、物料储运系统和一组数字控制加工设备组成，能适应加工对象变换的自动化机械制造系统。	参考 MBA 智库
8	精准营销	precision marketing	在充分了解顾客信息的基础上，针对客户喜好，有针对性地进行产品营销，在掌握一定的顾客信息，市场信息后，将直复营销与数据库营销结合起来的营销新趋势。	参考 MBA 智库
9	供应链协同	supply chain Collaboration	指两个或两个以上的企业为了实现某种战略目的，通过公司协议或联合组织等方式而结成的一种网络式联合体。	参考 MBA 智库

10	垂直电商	vertical e-business	在某一个行业或细分市场深化运营的电子商务模式。	参 考 MBA 智库
15	智能机器	smart machine	通过添加传感、通信、计算、控制模块，使机器具备自决策、自组织、自适应等能力。	
16	边缘计算	edge computing	将计算能力延伸到生产现场，实现数据的分布式计算分析，形成本地的实时优化决策。	
17	标识	identifier	在一定范围内唯一识别身份的编码或者符号	
18	解析	resolve	根据标识查询地址以及其它信息的映射过程。	
19	根服务器	root server	标识解析体系中最高层级的服务器。	
20	根区文件	root zoon file	存储标识解析体系中最高层级映射信息的数据文件。	
21	工厂内部网络	enterprise internal network	在工厂内部，用于生产要素互联以及企业 IT 管理系统之间连接的网络。	
22	工厂外部网络	enterprise external network	以支撑工业全生命周期各项活动为目的，用于连接企业上下游之间、企业与智能产品、企业与用户之间的网络。	
23	OT 网络	operation technology network	用于连接生产现场设备与系统，实现自动控制的工业通讯网络	
24	IT 网络	IT technology network	用于连接信息系统与终端的数据通信网络	
25	现场总线	field bus	连接智能现场设备和自动化系统的数字式、双向传输、多分支结构的通信网络	参考 IEC
26	工业以太网	Industrial ethernet	基于标准以太网协议，用于工业自动化或过程控制中连接现场设备和系统的通信网络	
27	软件定义网络	software defined network	一种网络控制和转发分离的网络架构，上层应用和服务可以通过网络控制层的可编程接口实现对底层网络设备的控制	参考 ONF
28	网络虚拟化	network virtualization	能够实现网络资源动态调配、动态管理的技术	
30	现场级	work cell	由企业确定的一个物质的、地理的或逻辑的生产群组，完成某项工序活动，或称为工段。	参 考 GBT 20720.1-2006

31	车间级	work center	多个工段组成的生产车间，完成产品某个部分的生产制造。	
32	工厂级 / 企业级	enterprise	多个车间组成的生产场所，负责产品由原型到实物的生产，以及运营管理决策的制定。	
33	SCADA 系统	supervisory control and data acquisition	有监控程序及数据收集能力的电脑控制系统，用于工业程序、基础设施或是设备中。	参考维基百科
34	客户关系管理	customer relationship management	企业管理中信息技术、软硬件系统集成的管理方法和应用解决方案的总和，目的是改善与销售、市场营销、客户服务和支持等领域的客户关系有关的商业流程。	参考 MBA 智库
35	制造执行系统	manufacturing execution system	位于上层的计划管理系统与底层的工业控制之间的面向车间层的管理信息系统，为操作人员 / 管理人员提供计划的执行、跟踪以及所有资源（人、设备、物料、客户需求等）的当前状态	

附件 2：缩略语

序号	缩略语	中 文	英 文
1.	5G	第五代移动通信技术	the 5th Generation of communication technology
2.	AII	工业互联网产业联盟	Alliance of Industrial Internet
3.	AMQP	高级消息队列协议	Advanced Message Queuing Protocol
4.	APT	高级持续性威胁	Advanced Persistent Threat
5.	CID	通信标识	Communication IDentifier
6.	COAP	受限应用协议	Constrained Application Protocol
7.	CRM	客户资源管理	Customer Relationship Management
8.	DCS	分布式控制系统	Distributed Control System
9.	DDoS	分布式拒绝服务	Distributed Denial of Service
10.	DDS	数据分布服务	Data Distribution Service
11.	DMZ	隔离区	DeMilitarized Zone
12.	DNS	域名系统	Domain Name System
13.	DONA	数字对象名称管理机构	Digital Object Numbering Authority
14.	Ecode	物联网统一标识	Entity Code
15.	EPC	电子产品代码	Electronic Product Code
16.	ERP	企业资源计划	Enterprise Resource Planning
17.	ESB	企业服务总线	Enterprise Service Bus
18.	ETL	抽取 - 转换 - 加在	Extract-Transform-Load
19.	FCS	现场总线控制系统	Field Bus Control System
20.	GS1	全球物品编码协会	Globe Standard 1
21.	HMI	人机界面接口	Human Machine Interface
22.	HTML	超文本标记语言	HyperText Markup Language
23.	IaaS	基础设施即服务	Infrastructure as a Service
24.	IETF	国际互联网工程任务组	Internet Engineering Task Force
25.	ISA	国际自动化学会	International Society of Automation
26.	LTE	长期演进	Long Term Evolution
27.	MPLS	多协议标签交换	Multi-Protocol Label Switching
28.	MES	制造执行系统	Manufacturing Execution System
29.	MPP	大规模并行处理	Massive Parallel Processing
30.	MQTT	消息队列遥测传输	Message Queuing Telemetry Transport

31.	NB-IoT	基于蜂窝的窄带物联网	Narrow Band Internet of Things
32.	NIOT	国家物联网标识平台	National Internet of Things Name Service Platform
33.	OASIS	结构化信息标准促进组织	Organization for the Advancement of Structured Information Standards
34.	OID	对象标识符	Object Identifier
35.	OMG	对象管理组织	Object Management Group
36.	ONS	对象名称服务	Object Name Service
37.	OPC	用于过程控制的 OLE	OLE for Process Control
38.	OPC-UA	OPC 统一架构	OPC Unified Architecture
39.	ORS	对象标识解析系统	Object Identifier Resolution System
40.	OS	操作系统	Operating System
41.	OT	操作技术	Operation Technology
42.	PaaS	平台即服务	Platform as a Service
43.	PLC	可编程控制器	Programmable Logic Controller
44.	PLM	产品生命周期管理	Product Lifecycle Management
45.	REST	表述性状态传递	Representational State Transfer
46.	RFID	射频识别	Radio Frequency Identification
47.	SaaS	软件即服务	Software as a Service
48.	SCADA	数据采集与监控系统	Supervisory Control And Data Acquisition
49.	SCM	供应链管理	Supply chain management
50.	SDK	软件开发工具包	Software Development Kit
51.	SDN	软件定义网络	Software Defined Network
52.	SOA	面向服务的体系结构	Service-Oriented Architecture
53.	SOAP	简单对象访问协议	Simple Object Access Protocol
54.	SSL	安全套接层	Secure Sockets Layer
55.	VPN	虚拟专用网	Virtual Private Network
56.	WIA-FA	面向工厂自动化的无线网络	Wireless Network for Industrial Automation - Factory Automation
57.	WIA-PA	面向工业过程自动化的无线网络	Wireless Networks for Industrial Automation Process Automation
58.	HART	可寻址远程传感器高速 通道	Highway Addressable Remote Transducer
59.	XMPP	可扩展消息和表示协议	Extensible Messaging and Presence Protocol



工业互联网产业联盟
Alliance of Industrial Internet

工业互联网产业联盟

地 址：北京市海淀区花园北路52号，100191

电 话：010-62305887

邮 箱：aia@caict.ac.cn

网 址：<http://www.aia-alliance.org/>



扫描二维码，关注工业互联网产业联盟