

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。

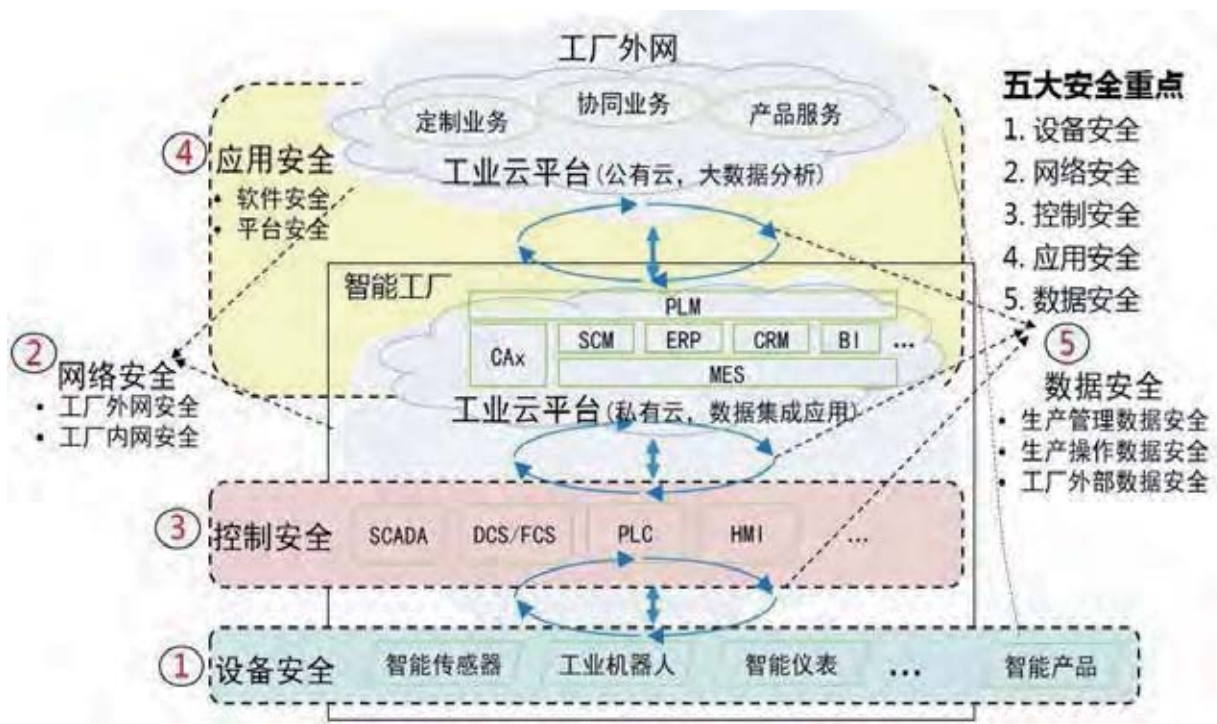


图 11 工业互联网安全体系

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 and 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 and 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 and 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。

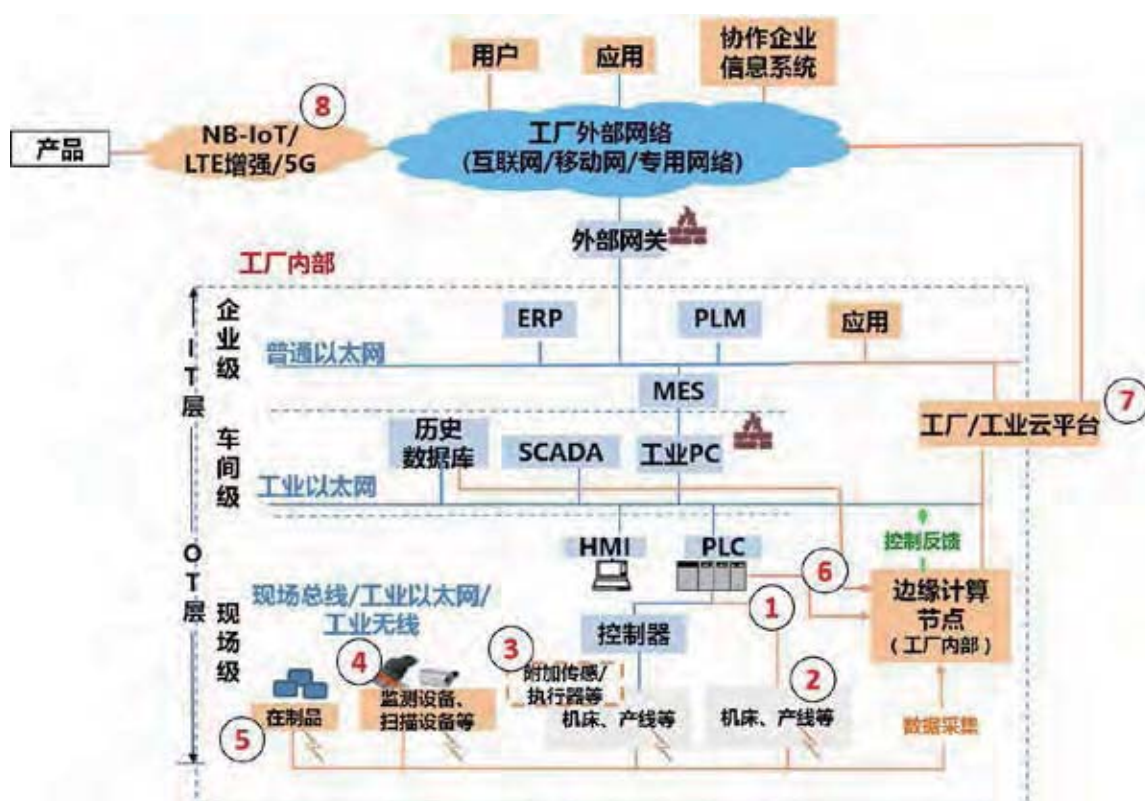


图 14 网络互联的实施

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 and 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，可能需要考虑建立安全、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。

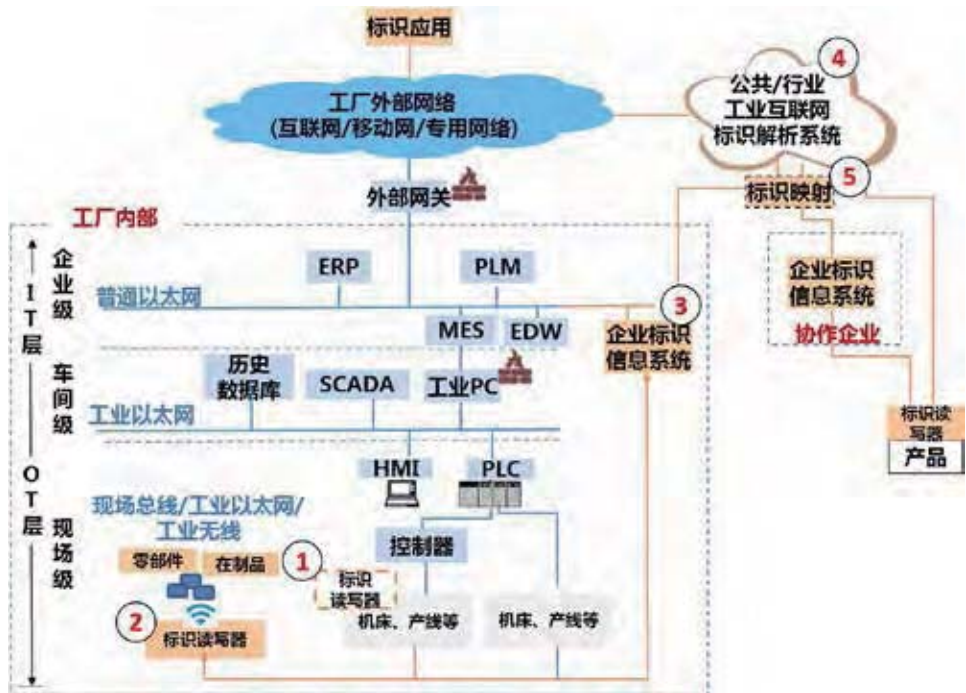


图 15 标识解析的实施

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。

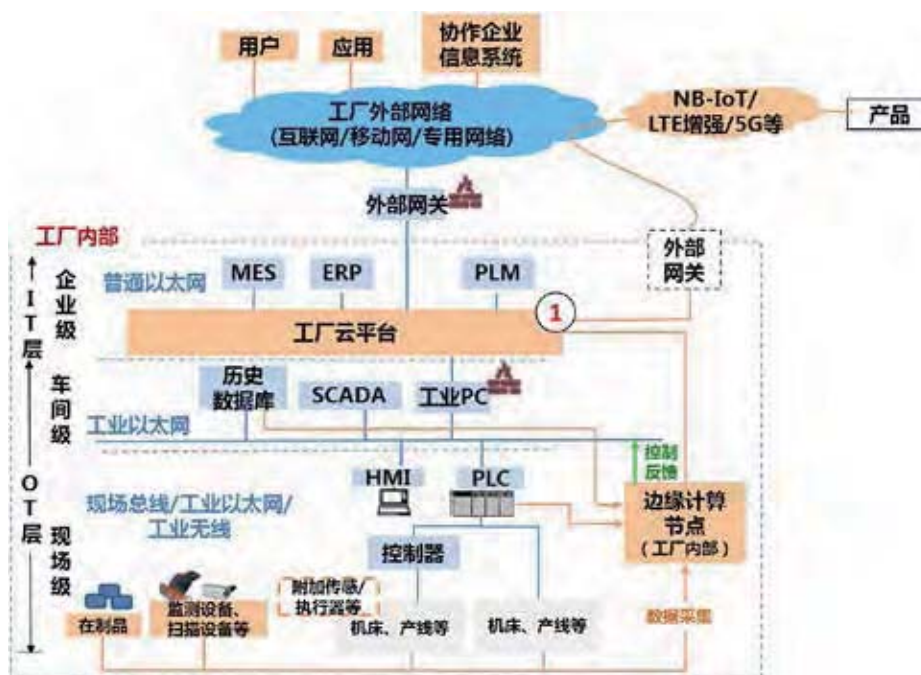


图 16 方式一：工厂云平台的实施

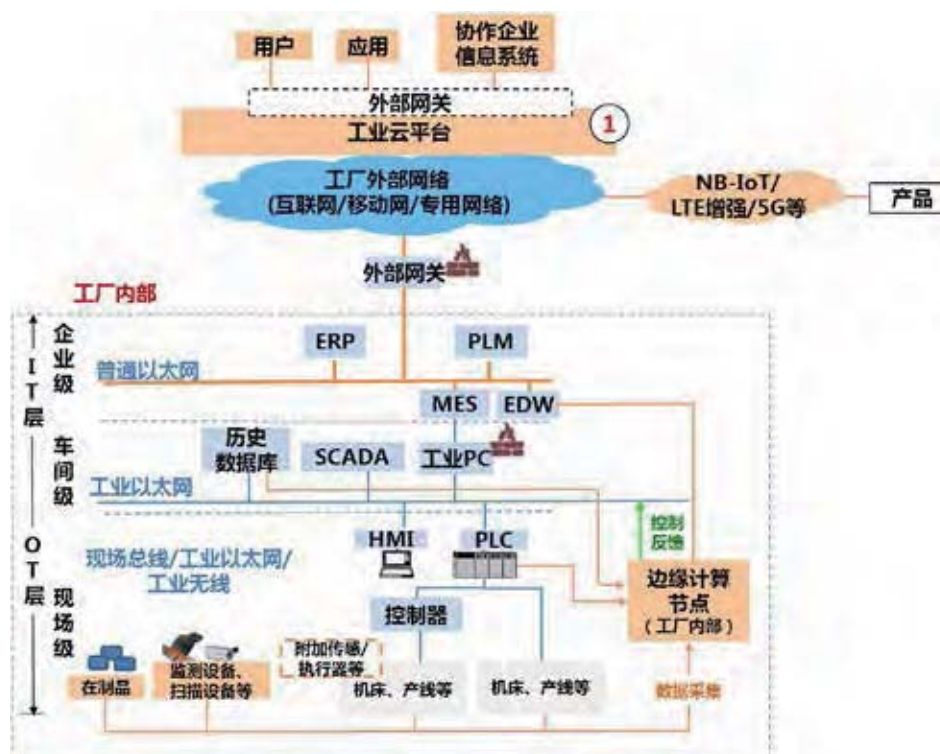


图 17 方式二：工业云平台的实施

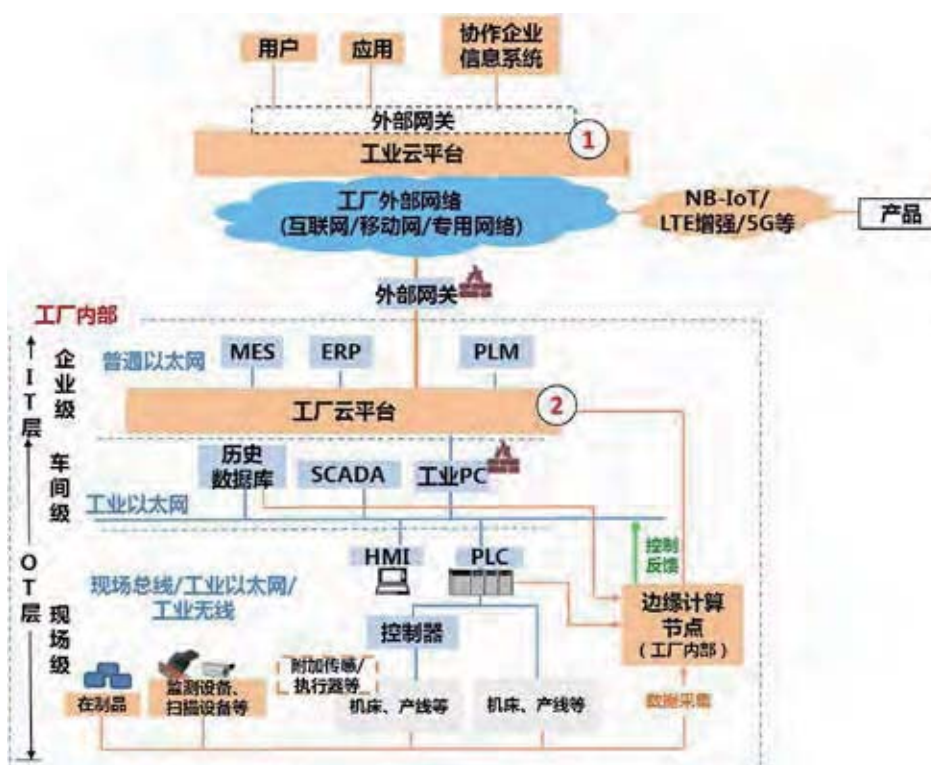


图 18 方式三：混合云的实施

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系统和管理系统的数据，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。

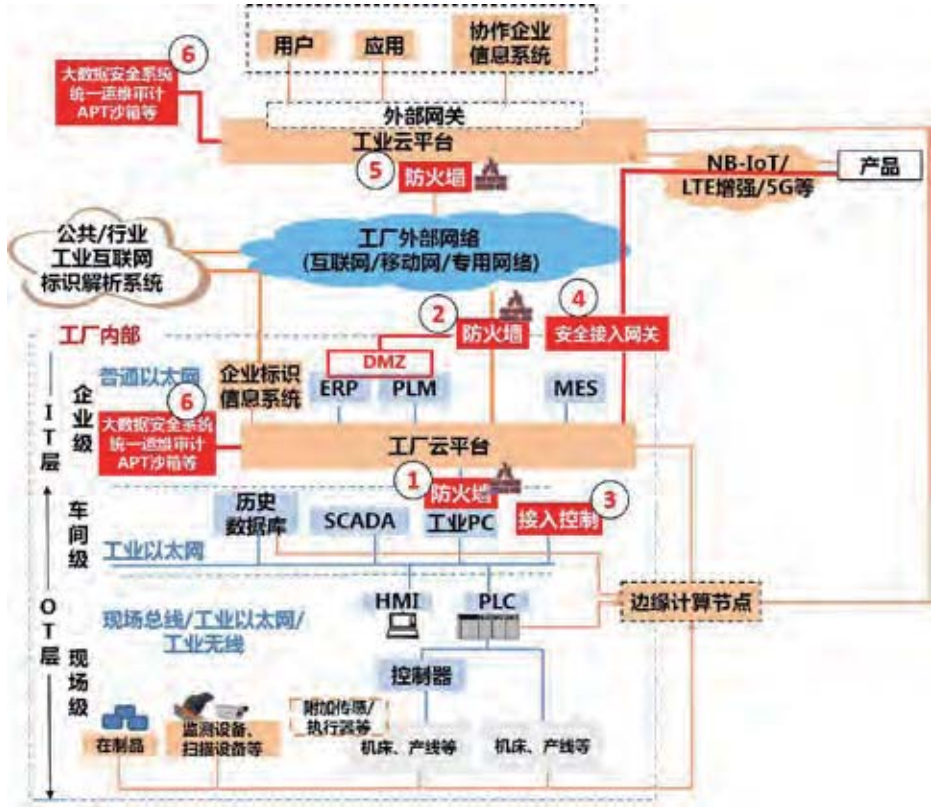


图 20 工业互联网安全的实施

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 zone 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：aai@caict.ac.cn

网 址：<http://www.aai-alliance.org/>



扫描二维码，关注工业互联网产业联盟