模块 3

工业互联网基础技术

工业互联网的基础技术主要包括支撑工业互联网系统搭建与应用实施相关的各类技术，覆盖工业技术与互联网技术，基本可从网络、数据、安全三个维度划分。

在网络维度方面，网络技术作为工业互联网的基础核心，是异构、分布的大量工业要素互联的基本使能技术，主要包括实现物物互联的物联网及实现互联互通的网络通信技术。网络通信技术门类众多，受篇幅所限，本模块将重点介绍工业互联网中重要的网络通信技术，即移动互联网技术、天地一体化网络技术及高性能计算技术。

在数据维度方面，工业大数据无疑会成为工业互联网实现工业要素互联后的核心价值创造者，而云计算技术、建模仿真技术则是支撑泛在、异构、海量的工业大数据采集、聚合、处理、分析的关键技术，因此本模块将重点展开介绍云计算、建模仿真与工业大数据的相关内容。

在安全维度方面，工业互联网对于国计民生的战略意义，决定了其安全保障的至关重要性。信息安全技术无疑会成为工业互联网实现工业要素安全、互联互通与协同协作可靠的核心技术基础。

本模块主要介绍工业互联网的基础技术，包括物联网技术、网络通信技术、云计算技术、工业控制技术、工业大数据技术、建模仿真技术及信息安全技术。本模块知识图谱如图 3-1 所示。

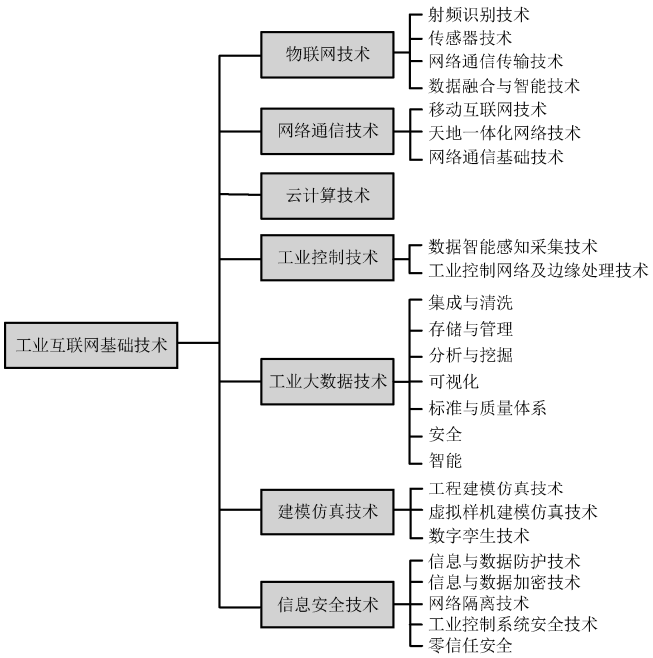


图 3-1　模块 3 知识图谱

电子工业出版社有限公司 版权所有

3.1 物联网技术

3.1.1 物联网的内涵


物联网技术

比尔·盖茨在 1995 年提出了“物物互联”的概念；1999 年美国 Auto-ID 中心率先提出建立在物品编码、射频识别技术和互联网基础上的物联网概念。目前，人们对物联网还没有一个可接受的明确定义，但从一般意义上讲，物联网是一个网络，它可以将任何具有独立地址并基于信息媒介（如互联网或传统通信网络）的普通物理物体连接起来，如图 3-2 所示。换句话说，在物联网世界中，每一个物体都在被寻址，每一个物体都在通信，每一个物体都在被管理。这种情形下的“物”，如工厂内的制造设备、家用电器、汽车和街角的自动售卖机，它们将信息上传到网络，无须通过人工，就能以机器对机器的方式自动报告运转情况、启动报警功能，或发出信号要求补充材料、下订单等。也就是说，在物联网世界中，每个物体均可被寻址、通信、被管理，因此，物联网被视为继计算机、互联网和移动通信后引领信息产业革命的新浪潮。

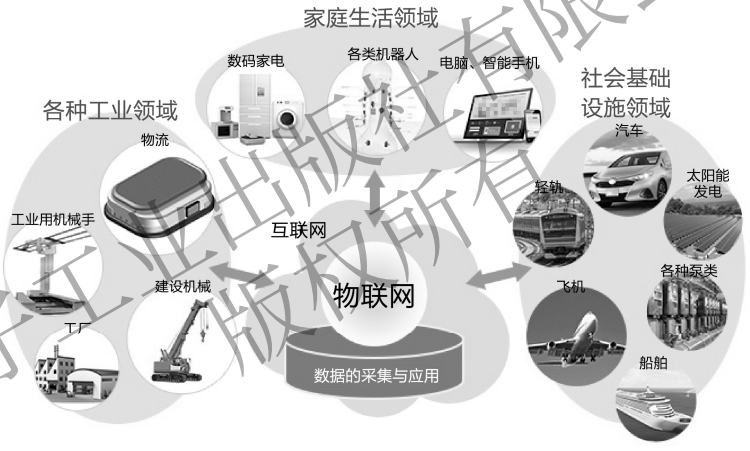


图 3-2 物联网

3.1.2 物联网的特性

物联网（IoT）不同于我们通常所说的传统意义上的互联网，它的特点体现在事物的存在形态、运行状态和被动行为等特征上。

1. 传感器技术的综合应用

在现实社会中，各行各业均存在大量不同类型的传感器，这些传感器已经、正在或将被连接部署到物联网上。部署后的传感器成为信息源，根据各自类型特性捕获不同格式和内容的信息。这些信息动态变化，传感器通过特定频率循环采集，实现数据持续更新。

2. 基于互联网的泛在网络

互联网是物联网的核心要素与重要基础。融合不同有线和无线网络后，互联网可将获取的数据信息精确传递至任何所需的数据中心、运算平台和应用终端。鉴于信息源数据繁多，为确保数据传输快速无误，在传输过程中数据需要与各种异构网络、协议相适应和匹配。基于互联

电子工业出版社有限公司 版权所有

网的泛在网络（Ubiquitous Network）是不同类型的有线和无线网络的综合体，其基本特征是无所不在、无所不包、无所不能，旨在实现任何时间、任何地点、任何人、任何物都能顺畅地通信。泛在网络包括物联网、互联网、电信网、传感网等。移动通信技术（如 Wi-Fi、5G 等）的进步，以及射频识别（RFID）和云计算技术的支撑，是实现泛在网络的关键因素。由此产生的数据可以精确地分布到任何连接到网络的数据中心、运算平台或应用终端。

3．智能处理与智能控制能力

物联网利用云计算、模式识别等智能技术，拓展了其应用范围和应用领域。通过结合传感器与智能处理，物联网可获取和捕捉庞大数据源，并对其进行加工处理和高级分析，从而获取所需信息数据，将大规模数据高效、可靠地组织起来，为上层应用提供智能的支撑平台。

3.1.3　物联网的关键技术

1．射频识别技术

射频识别（Radio Frequency Identification，RFID）技术是利用射频信号，通过空间耦合（交变磁场或电磁场）来实现无接触信息传递，并通过所传递的信息达到自动识别目的的技术。应用射频识别技术可开发出 RFID 系统，典型的 RFID 系统由询问器（阅读器）和多个应答器（智能标签或电子标签）组成，如图 3-3 所示。其中电子标签也被称为 RFID 标签或 RFID 卡，是物联网中信息采集的主要源头之一。将电子标签附着在目标物品上，可对物品进行全球范围内的追踪和识别。例如，装有电子标签的汽车通过高速公路收费站时能被自动识别，实现不停车缴费。

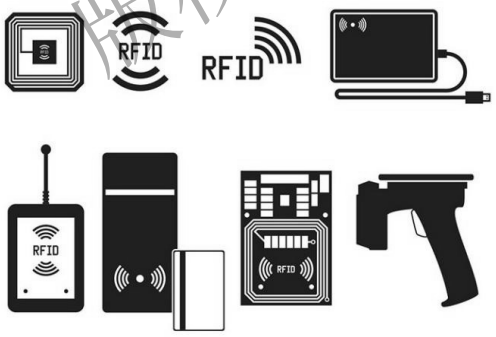


图 3-3　RFID

近年来，RFID 得到了逐步完善，具备了许多独特的优势，如耐水性高、磁稳定性高、读取快速、内存容量大、识别距离远等，RFID 在许多应用场景中能够提供远超条形码的功能，且效率更高，是条形码技术的有力补充和升级。特别是，当具有通信功能的 RFID 与可以给任何物体提供 IP 地址的 IPv6 技术相结合时，这两种技术的优势可以被充分发挥出来，实现物联网所倡导的人与人、人与物、物与物的互联。

2．传感器技术

传感器可通过声、光、电、热、力、位移、湿度等信号来感知现实世界，为物联网提供最原始的信息。例如，通过温度传感器可感知鱼塘水温，通过压力传感器可感知桥梁受力情况。

电子工业出版社有限公司 版权所有

传感器增强了人类对环境的感知能力，是现代生活中人们获取信息的重要手段，无线传感器就是传感器的一个典型代表。与通常所说的传感器不同，无线传感器不仅可以包含传感器部分，还可以包含一个微处理器和一个无线通信芯片。因此，无线传感器节点不仅可以接收来自外部世界的信息，还可以分析和传输这些信息，如图 3-4 所示。

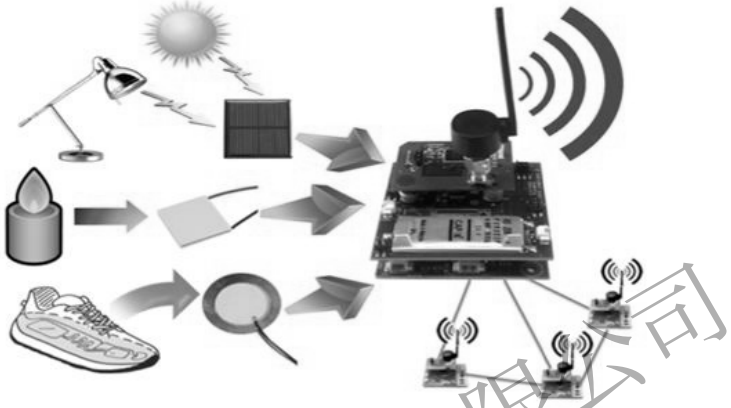


图 3-4　无线传感器

3．网络通信传输技术

使用网络通信传输技术可实现物联网中物与物、人与物之间信息的交流。例如，可以通过互联网、移动通信网、卫星通信等传输物联网感知到的信息。

无线传感器网络是由大量小型、低成本、低功率的传感器节点组成的多跳无线网络。无线传感器网络的应用范围很广，但主要应用于环境监测场景，特别是在满足长期和大规模的监测需求方面。它们还可以根据用户需求和网络带宽，按计划自动和动态地进行数据收集和传输。

4．数据融合与智能技术

使用数据融合与智能技术对收集到的各种感知信息进行综合分析和处理，可以实现实时监控、信息管理、实时预警、智能决策等功能。例如，通过对感知到的鱼塘水温、pH、溶解氧及氨氮等进行融合处理，可实时对鱼塘水质状况进行综合评价。

物联网将大量的传感器节点构成无线传感器网络，通过各种传感器采集信息。在信息感知的过程中，网络存在大量冗余信息，采用各个节点单独传输数据到汇聚节点的方法会浪费大量的通信带宽和宝贵的能量资源，降低信息的收集效率，影响信息采集的及时性。在这种情况下，可采用数据融合与智能技术进行处理。数据融合是指对多种数据或信息进行处理，组合出高效且符合用户需求的数据的过程。智能技术是为有效达到某种预期目的，利用知识进行分析后所采用的各种方法和手段。在物体中植入智能系统，可使其具备一定的智能性，实现与用户的主动或被动沟通。

3.2　网络通信技术

网络通信技术（Network Communication Technology，NCT）是一种通过使用计算机和网络通信设备来收集、存储、处理和传输信息（如图像和文本），从而实现高速传输和完整交换信

电子工业出版社有限公司 版权所有

息的技术。从通信对象的角度而言，NCT 大致可分为互联网技术、连接手机等移动终端的移动互联网技术，以及连接机器等物理物体的物联网技术。

3.2.1　移动互联网技术


移动互联网技术

1．移动互联网的内涵

移动互联网结合了移动通信设备和互联网的优点，是两者相互融合而成的通信网络。运营商可以为无线网络提供支持，互联网公司可以提供一系列的应用。移动互联网不仅具有“随时使用”的便捷性，还具备“随身携带”的便携性，并且可以分享和互动，如图 3-5 所示。


图 3-5　移动互联网

无线移动宽带技术的逐步发展，促进了移动互联网业务的发展，使移动互联网的使用更加便捷、普及，并以极快的速度推广应用。移动通信和互联网的优势相结合，为移动通信网络带来了很大的应用空间，创造了可持续的商业模式，为传统的互联网类业务开辟了新的天地，反过来又促进了移动通信网络宽带化的发展。移动宽带业务已逐渐成为移动运营商的主要业务之一。

2．移动互联网的特点

与传统互联网相比，移动互联网有其突出的特点。

（1）灵活性和移动性：移动互联网是一个基本网络，由覆盖整个地区的三维网络组成，并可以使移动设备非常容易地连接到网络。这种连接可以通过各种形式实现，如 GPRS、3G、4G、5G、WLAN 和 Wi-Fi，其中移动终端是主要载体。

（2）准确性和实时性：上述的灵活性和移动性使信息可以在任何时候都能被接收和处理，只要网络在可及范围内。它保证了信息交流的准确性和实时性。

（3）定位性和感应性：基于位置的服务（Location Based Services，LBS）功能不仅可以确定移动设备的位置，还可以分析它们的运动趋势，以确定它们的未来方向，所以移动互联网具有非常强大的定位和预测能力。

（4）保密性和安全性：由于移动互联网和移动终端可以限制移动互联网服务的使用，因此为了保证信息的安全和隐私，需要根据各自网络和终端类型的技术特点，采用不同的安全类型，并进行分类管理。由于移动通信的电磁特性是全方位的，对空间是开放的，因此在网络上传输的信息很容易被截获和窃听，信息内容的保密性和安全性同时受到严重质疑。

电子工业出版社有限公司 版权所有

（5）网络的局域限制：虽然移动互联网易于搬迁，但它在基站覆盖区域、网络性能和终端容量方面存在局限性。

3．移动互联网的关键技术

移动互联网的关键技术主要包括移动终端、网络服务平台、应用服务平台、5G 和网络安全控制。

（1）移动终端技术：移动终端技术大致分为先进终端制造技术、终端硬件平台技术和终端软件平台技术。终端制造技术是整合机械工程、自动化技术、信息技术和电子技术而形成的技术、装置和系统的一个总称。终端硬件平台技术是实现移动互联网信息输入、输出、存储和处理的技术的总称，通常又被细分为处理器芯片技术和人机交互技术。终端软件平台技术是指在移动终端上通过用户和硬件接口进行数据和信息交换的技术，通常又被细分为移动操作系统、移动中间件和移动应用技术。

（2）网络服务平台技术：网络服务平台技术是指将两个或多个移动互联网终端设备连接到互联网的计算机信息技术的总称，其核心技术是将各种移动互联网终端设备连接到互联网，形成一个互联网络。

移动通信网络技术：移动通信网络从 1G 时代开始，经过不断地发展和研究，经历了 2G、3G 和 4G 时代，5G 网络时代也已经到来，移动互联网技术的性能在每个阶段不断升级、完善，实际使用量不断增加，应用领域不断扩大。

无线局域网技术：得益于 IEEE 802.11ad 标准，无线局域网基于接入点（AP）安全监控、管理和控制以及无线控制器（AC）访问控制，实现了 AC-PC 架构和 WLAN 解决方案技术的使用。

无线 MESH 网络技术：无线 MESH 网络（WLAN mesh network，WMN）是由 mesh 路由器和客户端组成的多跳无线网络，其通过节点自组织形成网状拓扑结构，支持动态路由选择和数据多跳中继传输，解决了传统单跳网络覆盖盲区问题。冗余路径机制可避免单点故障，通过短跳传输提升带宽利用率。其骨干网络可通过无线多跳互连降低发射功率需求，部署时仅需供电即可扩展覆盖范围。WMN 技术采用多跳无线技术的示意图如图 3-6 所示。

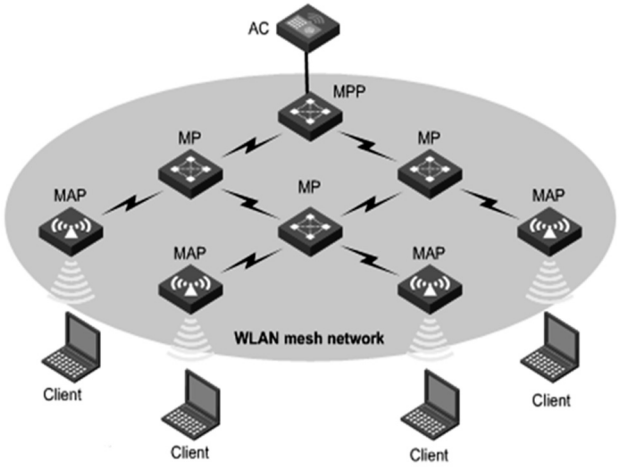


图 3-6　WMN 技术采用多跳无线技术的示意图

其他接入网络：实现小区域无线局域网的运行，可采用 NFC、IrDA、Zigbee、UWB 和蓝

电子工业出版社有限公司 版权所有

牙等技术。

异构无线网络架构的主要形式是紧耦合和松耦合。紧耦合的无线电接入系统是主从关系，而松耦合的无线电接入系统则没有这种主从关系。

移动网络管理技术有两种类型：IP 移动管理技术和独立媒体切换协议。IP 移动管理技术是一种网络层的移动性管理技术，允许移动终端在异构的无线电网络中移动。IPv6 技术是一种快速发展的技术，用于管理具有高度安全性和足够地址空间的移动网络。基于 IPv6 技术，用户可以实现自动地址配置，有效解决三角路由问题。IEEE 802.21 是一个独立媒体切换协议，可用于实现异构网络之间的互操作和自由切换。

（3）应用服务平台技术：基于各种协议，形成应用服务平台技术，其可以将相关应用提供给移动互联网终端，具体可采纳的技术包括云计算、HTML5、Widget、Mashup、RSS 和 P2P 等。

云计算技术：云计算采用一种服务交付和利用模式，能够通过按需网络使用所需的信息处理和计算服务，如图 3-7 所示。这些服务可以是信息技术、软件、互联网相关服务或任何其他服务。基于云计算技术，软件和硬件资源可以被有效地共享，计算机和其他设备可以获得有关服务要求的信息。云计算的本质是利用计算技术对连接到网络的数据资源进行统一和标准化管理和调度，作为用户不断需求的计算资源池，提供支持良好用户体验的服务。云计算技术是基于分布式计算模式，即大规模计算的，而不是基于由远程服务器和本地计算机实现的传统计算模式的。



图 3-7　云计算

HTML5 技术：HTML5 是 Hyper Text Markup Language 5 的缩写，以传统的 HTML 为基础，增加了创新的属性和元素，如嵌入互动文件、客户端存储、音频、视频和图形功能。此外，它还纳入了 Web GL 技术标准，该标准加速了网页 3D 界面的创建，为搜索引擎的功能拓展和用户索引操作提供了技术支撑，并支持在小屏幕设备上使用。HTML5 将 Web 带入一个成熟的

电子工业出版社版权所有

应用平台，在这个平台上，视频、音频、图像、动画以及与设备的交互都进行了规范。

Widget 技术：Widget（中文音译为微件）是一种基于代码重用概念的技术，可以理解为“应用小插件”，即一种可供用户制作和自由下载的小工具。它包含了娱乐、工作、学习等领域的多种实用功能。目前的 Widget 应用大体可分为三种：Desktop Widget、Web Widget 及 Mobile Widget。天气插件如图 3-8 所示。



图 3-8　天气插件

Mashup 技术：Mashup 是一种基于网络的内容集成技术，将两种以上使用公共或者私有数据库的 Web 应用合并在一起，形成一个整合应用。其一般使用源应用的 API，或者一些 RSS 输出（含 atom）作为内容源，被合并的 Web 应用所使用的技术，则没有限制。Mashup 不需要很高的编程技能，用户只需要熟悉 API 和网络服务工作方式即可使用该技术，因此其很快成为一种流行的网络技术，被广泛应用于地图 Mashup、新闻 Mashup、微博 Mashup、搜索和购物等领域，以支持丰富而愉悦的用户体验。

RSS 技术：RSS（Really Simple Syndication）也被称为聚合内容，是一种简单的基于 XML 的技术，是在互联网上被广泛采用的内容包装和投递协议，广泛应用于网上新闻频道、网络博客和电子商务领域。该技术允许用户从一个网站访问选定的和聚合的内容。聚合、实时、低成本和个性化的 RSS 技术使得不同格式和需求的内容能够被聚合、分类并高速传递给用户或读者，同时能够被存储、分类和管理。RSS 图标如图 3-9 所示。



图 3-9　RSS 图标

P2P 技术：P2P 被称为点对点技术，又被称为对等互联网络技术，如图 3-10 所示。该技术采用分布式网络结构模型，依赖网络中参与者的计算

电子工业出版社有限公司 版权所有

能力和带宽，而不是依赖于较少的几台服务器。通过文件、语音和流媒体，P2P 技术可以实现计算机系统之间的直接通信，以提高计算机资源和网络带宽的共享访问效率和利用率。在 P2P 网络的基础上，每台计算机都扮演着客户端和服务器的角色。P2P 技术是相当方便和高效的，因为它实现了系统之间的直接数据交换，充分利用了有限的网络资源，消除了服务器瓶颈的技术限制。基于 P2P 的互联网是非常动态的，网络服务的带宽受到每个用户共享空间的连接时间、频率和容量的影响。目前，P2P 技术已被广泛应用于网络游戏、文件共享、搜索引擎、点对点计算和协作等领域，并具有广阔的商业和市场应用前景。

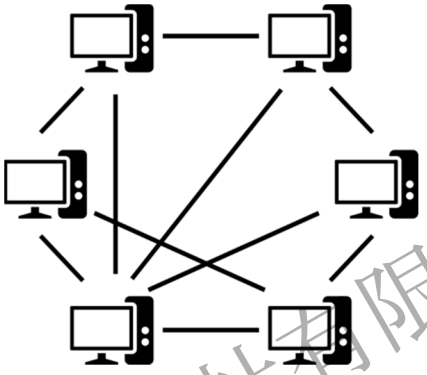


图 3-10　P2P 技术

（4）5G 技术：第五代移动通信技术（5th Generation Mobile Communication Technology，5G）是一种具有高速率、低延迟和大带宽特点的新一代宽带移动通信技术，如图 3-11 所示。5G 通信设施是实现人、机、物互联的网络基础设施。5G 是一种构建高性能移动互联网络的技术，能提供峰值为 10Gb/s 及以上的宽带，具有毫秒级的延迟和超高的连接密度。5G 技术有以下特点。



图 3-11　5G 技术

高速率：5G 基站的峰值需求至少为 20Gb/s。基于这种高速网络，5G 可以支持云机器人、云无人车和工业设施管理系统的互联互通，实现通用移动网络标准和基于该概念的工业网络技术的整合。

电子工业出版社有限公司 版权所有

大带宽：5G 的宽带性质使其下载速度达到 1Gb/s，远高于 4G 的 100Mb/s。5G Wi-Fi 在 5GHz 无线电频段工作，是传统 Wi-Fi 速度的三倍，一些高性能的 5G Wi-Fi 可以达到 1Gb/s 的下载速度。

泛在网：5G 时代使用的微型基站（即小型基站）可以跨越终端通信，并连接到工业生产监控的各个角落的网络信号，在常见的应用场景中提供广泛的覆盖。

低延迟：3G 网络的延迟约为 100 毫秒，4G 网络的延迟为 20 ~ 80 毫秒，而 5G 网络的延迟则降至 1 ~ 10 毫秒。5G 通过优化帧结构和减少时域中的每个子帧来优化物理层的延迟。

5G 的关键技术包括网络功能虚拟化（Network Functions Virtualization，NFV）、软件定义网络（Software Defined Network，SDN）和网络切片。NFV 是一种针对网络架构（Network Architecture）的概念，其利用虚拟化技术，将网络节点阶层的功能，分割成几个功能区块，分别以软件方式实现。该技术不局限于硬件架构，是一种用信息技术虚拟化技术取代传统的专用网络硬件的技术，通过软件使网络功能在通用硬件之上运行。SDN 是网络虚拟化的一种实现方式。其核心技术 OpenFlow 通过将网络设备的控制面与数据面分离开来，实现了网络流量的灵活控制，使网络变得更加智能，为核心网络及应用的创新提供了良好的平台。网络切片是一种按需组网的方式，可以让运营商在统一的基础设施上分离出多个虚拟的端到端网络，每个网络切片从无线接入网到承载网再到核心网进行逻辑隔离，以适配各种类型的应用。在一个网络切片中，至少可分为无线网子切片、承载网子切片和核心网子切片三部分，物理网络按需在多个独立网络（SA）架构中被虚拟化，每个网络切片与接入网、传输网和核心网在逻辑上是分开的，可以灵活地适应不同的服务要求和兼容同一网络中的多种用途，不需要为每种服务多次建立专用网络，从而大大降低成本。

（5）网络安全控制技术：网络安全控制技术包括防火墙、入侵检测系统、虚拟专用网络、超文本传输安全协议、访问控制列表、数据加密、交换式局域网、数据安全存储、安全扫描和漏洞检测等技术。

防火墙（Firewall）通常位于网络边界处，用于监视进出网络的数据流量，验证网络通信，控制通信阈值，在内网和外网之间形成隔离和封锁机制，根据预定义的规则来允许或阻止特定的网络连接，从而保护计算机免受恶意病毒的侵害。防火墙技术能够对 IP 地址进行有效审计，并自动转发到受保护的网络地址，阻止潜在的恶意流量，如恶意软件攻击、网络钓鱼等。

入侵检测系统（Intrusion Detection System，IDS）是一种监测网络流量和系统活动的技术。它可以检测并报告可能存在的入侵行为，如端口扫描、恶意软件传播等。IDS 可以帮助用户发现和响应潜在的安全威胁。

虚拟专用网络（Virtual Private Network，VPN）通过加密和隧道技术在公共网络上建立安全的连接。它可以保护用户数据在传输过程中的机密性，并提供远程访问网络资源的安全通道。

超文本传输安全协议（Hypertext Transfer Protocol Secure，HTTPS）是一种基于 SSL/TLS 协议的加密通信协议，用于在客户端和服务器之间进行数据的加密传输。HTTPS 可以防止数据在传输过程中被窃听或篡改。

访问控制列表（Access Control List，ACL）是一种基于规则的访问控制机制，用于限制用户对网络资源的访问权限。ACL 可以根据用户身份、IP 地址、时间等条件来控制网络的访问权限，从而保证网络资源的安全性。

数据加密技术可以将敏感数据转换为密文，并通过加密算法保护数据的机密性。只有掌握正确密钥的人才能解密数据，从而保证数据在存储和传输过程中的安全性。

电子工业出版社版权所有

交换式局域网技术使用逻辑拓扑结构，在互联网上实现面向交换的网络安全技术。

数据安全存储技术在数据恢复和存储技术的基础上，为系统资源提供整体的、多层次的备份。其使用大容量的服务器，在用户和服务器端安装软件，数据备份在服务器上集中管理。如果数据文件丢失或破坏，系统硬件和软件可以对其进行统一恢复。

安全扫描和漏洞检测技术可以收集网络信息，检测安全漏洞，分析和预先评估潜在攻击，了解系统的安全性和可靠性。

3.2.2　天地一体化网络技术


天地一体化网络技术

1．天地一体化网络的内涵

天地一体化信息网络（简称天地一体化网络）是借助卫星、飞机、空中平台及地面站间链路，将地面、海上、天空和太空中的用户、飞行器及各类通信平台相互连接，运用智能高速处理、交换和路由技术，实现信息准确获取、快速处理与高效传输的一体化高速宽带信息网络，也就是天基、空基和陆基一体化的综合信息网络，如图 3-12 所示。目前，很多国家均高度重视天地一体化网络的发展。我国天地一体化网络由天基骨干网、天基接入网、地基节点网组成，并与地面互联网和移动通信网互联互通，建成“全球覆盖、随遇接入、按需服务、安全可信”的天地一体化网络体系。

电子工业出版社有限公司
版权所有

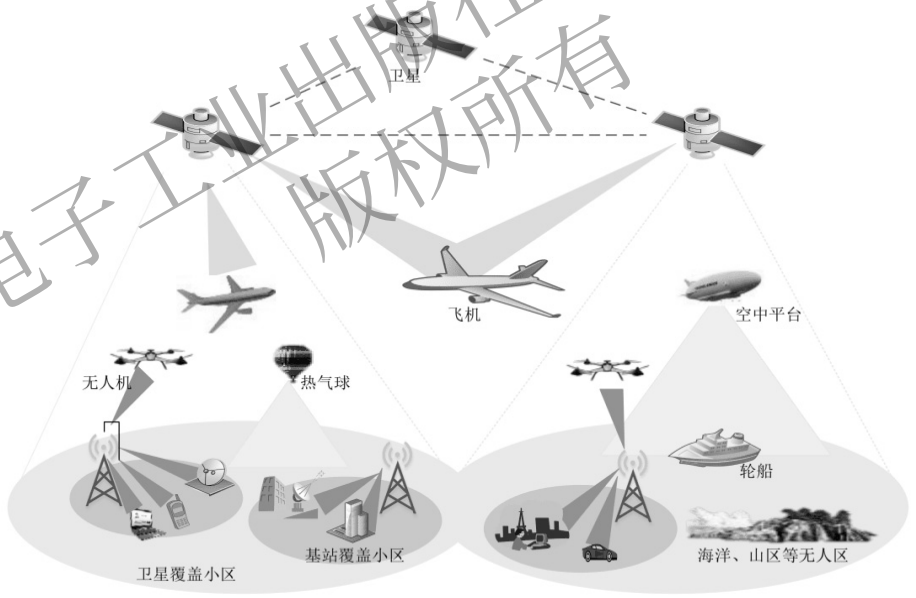


图 3-12　天地一体化网络

天地一体化网络涵盖技术体制与网络系统设施两大层面。技术体制方面包含网络体系架构、功能指标体系、星座及组网设计、频谱及轨位协同、信息传输体制、多维度路由交换、业务服务体制设计、多层面安全防护及一体化运维管控等；网络系统设施方面则包括天基骨干网、天基接入网、地基节点网、用户终端网、天基信息港和地面信息中心等。

2．天地一体化网络的特点

与地面通信网络相比，因应用环境的不同，天地一体化网络具备其自身的技术特点：一是

网络规模庞大、广域无缝覆盖，特别是对地观测网络和空中交通管制网络，更要求在全球各区域实现全天时、全天候对无缝通信、导航、观测和监视的覆盖，区域广泛，节点种类和数量繁多，网络结构复杂；二是网络拓扑时变、灵活机动，需要具有应对突发事件的应急组网能力，组网结构动态可变、运行状态复杂；三是多功能融合、信息协同能力强，可面向不同的应用服务对各种信息资源进行管理、协调及优化，实现信息交换处理一体化，最大限度地开发、利用各种信息资源。

3．天地一体化网络的关键技术

天地一体化网络作为国家重大信息基础设施，可将人类活动范围拓展至太空、远海乃至深空。它凭借先进的网络通信技术，将太空、临空、天空和地面等基本平台无缝连接成一体化信息网络，不仅能够处理可见光、紫外线、红外线、太赫兹波、雷达信号、高光谱等多谱段信息，还支持高速、宽带、大容量信息传输，能为各类用户提供安全可靠、不间断、实时、按需的信息服务。其涉及的关键技术众多，主要包括天网地网体系结构构建技术、天地一体化网络协议体系构建技术、天地信息融合移动接入技术、天地一体化多层面网络安全保密技术及天地一体化多层级网络运维管理技术等。

3.2.3　网络通信基础技术


网络通信基础技术

1．通信网络技术

通信网络是将一定数量的节点和连接这些节点的传输系统有机地组织在一起，按约定的信令或协议完成任意用户间信息交换的通信体系。从硬件结构看，通信网络由终端节点、交换节点、业务节点和传输系统构成，其硬件功能是实现接入交换网的控制、管理、运营和维护；从软件结构看，通信网络包括信令、协议、控制、管理、计费等要素，其功能是通过通信协议及网络管理来实现用户间的协调通信。整个系统的有效运行，还依赖于底层物理链路上稳定的位同步与帧同步，并遵循统一的传输体制。

一个完整的通信网络主要包括业务网、传送网和支撑网。其中，业务网负责向用户提供各种通信业务，其技术要素主要包括网络拓扑结构、交换节点技术、编号计划、信令技术、路由选择、业务类型、计费方式、服务性能保证机制；传送网独立于具体业务网，负责按需为交换节点/业务节点之间的互联分配电路，提供信息的透明传输通道，包含相应的管理功能，其技术要素包括传输介质、复用体制、传送网节点技术等；支撑网负责提供业务网正常运行所必需的信令、同步、网络管理、业务管理、运营管理等功能，以提供令用户满意的服务，其技术要素包括信令网、同步网、管理网等。

通信网络的分类方式多样，按业务类型可分为电话通信网、数据通信网和广播电视网；按空间距离可分为广域网、城域网和局域网；按信号传输方式可分为模拟通信网和数字通信网；按运营方式可分为公共电信网和专用电信网。

计算机网络是通信网络的一种特殊形式。它是由分布在不同地理位置、功能独立的若干计算机系统通过通信设备和通信线路连接而成的网络，借助功能各异的网络软件（如网络通信协议和网络操作系统），以不同长度的分组方式传输和处理数据，以此实现网络中资源的有效共享与信息的可靠传输。计算机网络的主要目的在于实现软件和硬件资源的共享、数据的可靠传输，提高计算机系统的可靠性，并提供全面的信息服务。

电子工业出版社有限公司 版权所有

2．高性能计算技术

高性能计算技术作为一种综合技术与研究方法，致力于通过多种途径（如改进算法、优化软件及革新架构等）提升计算机的计算性能。它从更深层次上挖掘并增强了单台计算机的计算能力，具体而言，其采用先进的半导体技术、电路设计、新型材料及创新工艺来打造性能更为强劲的处理器。单纯提升单台计算机的计算能力，可能会促使超级计算机技术的投入应用，然而这类技术往往成本高昂且难以实现盈利。此外，使用多核处理器虽能在一定程度上加快计算速度，但可添加的处理器数量存在上限。

高性能计算技术的主流方式与未来发展趋势，在于从广度上提升多台计算机联网的计算能力。其主要架构涵盖星群（Constellation）、并行向量机系统（Parallel Vector Processors，PVP）、对称式多处理机（Symmetric Multiple Processor，SMP）、分布式共享存储器/非均匀存储器访问（DSM/NUMA）、大规模并行处理机（Massively Parallel Processor，MPP）、工作站机群（Cluster of Workstations，COW），以及网格计算、云计算、边缘计算和 GPGPU 技术等。当前，高性能计算技术已广泛应用于虚拟仿真、天气预报、汽车制造等众多领域，成为支撑国家产业发展的关键技术。

（1）网格计算技术：网格计算是分布式计算的一种，通过共享网络将不同地点的大量计算机相连，从而形成虚拟的超级计算机，也就是将各处计算机的空闲处理器能力整合在一起，通过任务分解，形成比单台计算机功能更强大的虚拟计算机，并整合和集中数据以产生更强大的计算能力，如图 3-13 所示。为了应对日益增长的带宽需求，信息世界被有机地统一结构化。一个由网格计算技术组成的网络的图像有无限的可扩展性，计算能力不受 CPU 数量的限制。

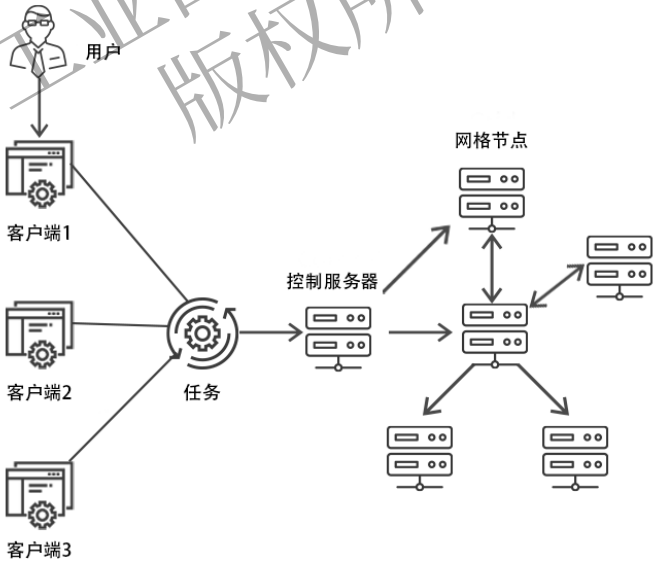


图 3-13　网格计算

（2）云计算技术：云计算（Cloud Computing）是分布式计算的一种，是指通过网络“云”将巨大的数据计算处理程序分解成无数个小程序，然后通过多台服务器组成的系统处理和分析这些小程序，得到结果并返回用户。云计算技术使数以亿计的计算机的虚拟化、控制和调度联系在一起，形成动态和生态友好的资源池，向用户提供个性化的服务。汇集和提供资源的网络被称为“云”。云计算与网格计算类似，提供了一个可无限扩展的网络平台。云计算形成的

电子工业出版社有限公司 版权所有

网络比网格计算支持的网络更加动态，资源分配可以根据用户的需求随时调整。

（3）边缘计算技术：边缘计算是指在靠近物或数据源头的一侧，采用集网络、计算、存储、应用核心能力为一体的开放平台，就近提供最近端服务。其应用程序在边缘侧发起，可以产生更快的网络服务响应，满足了行业在实时业务、应用智能、安全与隐私保护等方面的基本需求。边缘计算处于物理实体和工业连接之间，或处于物理实体的顶端，但云计算仍然可以访问边缘计算的历史数据。边缘计算技术是一种新的计算模式，充分利用网络边缘的网络资源、存储资源和计算资源，在网络边缘接收、分析和处理数据，为附近的用户提供实时服务，如图 3-14 所示。它可以有效补充和协调云计算，为用户提供更好的服务。边缘计算所处理和分析的数据包括来自云服务的下游数据和来自万物互联服务的上游数据。

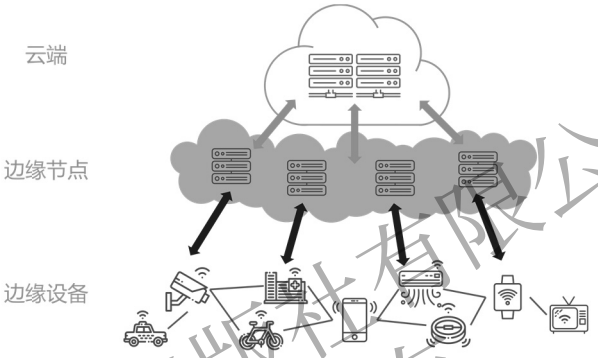


图 3-14　边缘计算

边缘计算包括一些关键技术，如新的分布式存储系统、可靠的低延迟网络、异构计算和计算迁移。在工业制造领域，边缘计算支持传统接口和协议设备之间的实时水平通信，实现了 OT 和企业 IT 之间的可靠数据连接。边缘计算还提供了实时计算、存储和通信机制、边缘侧建模工具、智能实时数据清理和预处理工具，并可为数字孪生系统提供基本的建模和数据融合支持。

（4）GPGPU 技术：通用图形处理器（General Purpose Graphic Processing Unit，GPGPU）是一种利用处理图形任务的图形处理器来计算原本由中央处理器处理的通用计算任务的图形处理器。这些通用计算常常与图形处理没有任何关系。现代图形处理器具有强大的并行处理能力和可编程流水线，使得流处理器可以处理非图形数据。特别是在面对单指令流多数据流（SIMD），且数据处理的运算量远大于数据调度和传输的需要时，通用图形处理器在性能上大大超越了传统的中央处理器应用程序。利用 GPU 进行大规模的并行计算，可以将 PC 的计算性能提高几倍到十几倍，达到高性能计算机的水平，如图 3-15 所示。目前 CUDA 和 Stream 技术已被普遍使用。

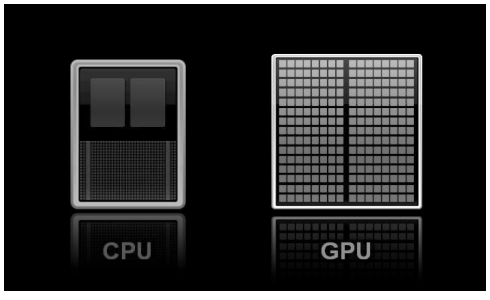


图 3-15　GPGPU 技术

电子工业出版社有限公司 版权所有

未来，高性能计算技术发展的重点方向大概率是云计算和 GPGPU 技术。

3.3　云计算技术


云计算技术

云计算是指通过计算机网络（多指因特网）形成的计算能力极强的系统，可存储、集合相关资源并按需配置，向用户提供个性化服务。

早期，云计算就是简单的分布式计算，用于解决任务分发问题，并进行计算结果的合并。因而，云计算又被称为网格计算。通过这项技术，可以在很短的时间（几秒钟）内完成对数以万计的数据的处理，从而实现强大的网络服务。现阶段所说的云计算已经不单单是一种分布式计算，而是分布式计算、效用计算、负载均衡、并行计算、网络存储、热备份冗杂和虚拟化等计算机技术混合演进并跃升的结果。

2006 年，谷歌首次正式提出了“云计算”的概念。目前，全球主要发达国家制定了多项发展云计算技术的国家计划，国内外众多知名 ICT 企业也纷纷推出云计算相关系统和产品，同时学术界也在积极研究云计算技术，并继续深化其发展。

3.3.1　概念与特点

云计算技术的概念自诞生以来，就有许多不同的观点，但总的来说，有以下几个方面。

（1）云计算技术包括两个概念，即云计算服务和云计算平台，其分别对应商业模式及技术机制。云计算服务是一种新的商业模式，为大量用户提供永远连接和永远可用的服务，支持多个用户按需访问服务资源并提供可靠的服务。云计算平台是实现“云服务”概念的技术机制，它就像一个控制“可扩展网络超级计算机”的操作系统。对于不同的应用需求，云计算平台可以快速调动和协调各种软硬件资源，完成计算、存储和通信服务，用户不需要关注实施细节。

（2）云计算技术是网格计算、分布式计算和并行计算的延伸和发展。

（3）根据组成云的不同网络，云计算有四种部署模式：私有云、公共云、社区云和混合云。云计算的可贵之处在于高灵活性、可扩展性和高性价比等，与传统的网络应用模式相比，其具有如下优势与特点。

一是高层次虚拟化：所有资源（如计算、存储、应用和网络设备）都由云计算平台链接、管理和分配。虚拟化突破了时间、空间的界限，是云计算最为显著的特点。具体而言，它使得物理平台与应用部署环境在空间上完全分离、彼此无关，因此用户能通过统一的虚拟平台，完成数据的备份、迁移和扩展等操作。

二是动态可扩展性：云计算具有高效的运算能力，在原有服务器基础上增加云计算能力，可大幅提升计算速度，最终通过动态扩展虚拟化层级，实现应用层面的弹性扩展。用户可以利用应用软件的快速部署条件来简单快捷地将所需的已有业务及新业务进行扩展。例如，当计算机云计算系统中的设备出现故障时，对用户来说，无论是在计算机层面上，还是在具体运用上均不会受到阻碍，其可以利用计算机云计算具有的动态扩展功能来对其他服务器开展有效扩展。

三是按需部署自助服务：计算机包含了许多应用、程序软件等，不同的应用对应的数据资源库不同，所以用户运行不同的应用需要具备较强的计算能力以对资源进行部署，而云计算平台能够根据用户的需求快速配备计算能力及资源。用户可以根据自己的应用需求，随时随地动

电子工业出版社有限公司 版权所有

态、灵活地访问云计算资源，并且可以按量缴费。

四是高灵活性和高通用性：目前市场上大多数信息技术资源、软件、硬件都支持虚拟化，比如存储网络、操作系统，以及开发软件、硬件等。虚拟化要素统一存放在云系统资源虚拟池当中进行管理，云计算的兼容性非常强，不仅可以兼容低配置机器、不同厂商的硬件产品，还能够外设获得更高性能计算。云计算平台采用“面向服务的架构”的概念，提供模块化、可灵活扩展的处理能力和自由互联的各种服务，以及底层硬件资源和高层应用模块的自由调度。企业可以通过重组资源和模块来满足不同的业务需求，快速完成整个业务系统的功能转型。

五是高可靠性架构：即使服务器发生故障，也不会影响计算与应用的正常运行。这是因为若单点服务器出现故障，则可以通过虚拟化技术将分布在不同物理服务器上的应用进行恢复或利用动态扩展功能部署新的服务器进行计算。平台云计算服务对高层应用是透明的，并具有高度安全的信息技术架构。服务提供方对底层架构的所有安全性、可用性和可靠性问题负责。云计算的基础软件技术使企业能够从传统结构无缝过渡到新的信息技术架构，将计算机集群作为独立机器，以极低的管理成本获得巨大的存储空间和计算能力。

六是商业实用性：将资源放在资源虚拟池中统一管理，在一定程度上优化了物理资源，用户不再需要购买昂贵、存储空间大的主机，可以选择相对廉价的 PC 组成云，这不仅减少了用户开销，而且计算性能不逊于大型主机。云计算技术采用无共享架构，每个节点都是独立自主的，因此系统中不存在资源竞争，可扩展性得到了保证。同时，它支持计算资源的充分共享，考虑到技术应用的投入和产出，这显然在商业上是可行的。

3.3.2 服务模式

通常，云计算的服务模式分为三类：软件即服务（Software as a Service，SaaS）、平台即服务（Platform as a Service，PaaS）和基础设施即服务（Infrastructure as a Service，IaaS）。这三种云计算服务有时被称为“云计算堆栈”，因为它们构成了一个层次分明的服务架构：IaaS 位于底层，PaaS 构建于 IaaS 之上，而 SaaS 则位于顶层，直接面向最终用户。

（1）软件即服务（SaaS）：各种互联网和应用程序的软件是一种被称为“软件即服务”的服务，它是通过互联网提供软件和相关数据的一种形式。通过互联网提供按需付费的软件应用程序，是软件即服务模式的典型形态：云计算提供商负责托管和管理软件应用程序，同时支持用户通过全球互联网连接并访问应用程序。用户可以远程访问和使用某些软件，通常是通过互联网使用浏览器访问，而不必在终端计算机上购买和安装软件，只需要根据使用量支付费用。

（2）平台即服务（PaaS）：作为服务，为开发人员提供通过全球互联网构建应用程序和服务的平台。PaaS 为开发、测试和管理软件应用程序提供按需开发环境，用户只需要提供基础软硬件并具备设备管理功能。

（3）基础设施即服务（IaaS）：基础设施即服务是云计算主要的服务类别之一，负责向云计算提供商的个人或组织提供计算能力、存储、网络和其他基础计算资源，他们可以在这些资源上部署和运行任何软件，包括操作系统和应用程序。

3.3.3 技术体系

随着云计算的逐步发展和产业的不断演进，总体、感知、虚拟化、构建、运行、评估、应用及运营等技术正逐步形成一个相对完整的技术体系，围绕着实现云计算模式全生命周期活动。

电子工业出版社有限公司 版权所有

云计算总体技术一般主要从系统的角度研究云计算系统的架构和服务模式、支持云计算实施的系统集成技术，以及相关的标准和规范。

Youseff 等提出了一个基于云计算三种服务模式的分层云堆栈架构，Lenk 等改进了分层云堆栈架构。结合最近的研究和实践，这里介绍一种面向服务的层次化云计算系统体系架构，如图 3-16 所示。

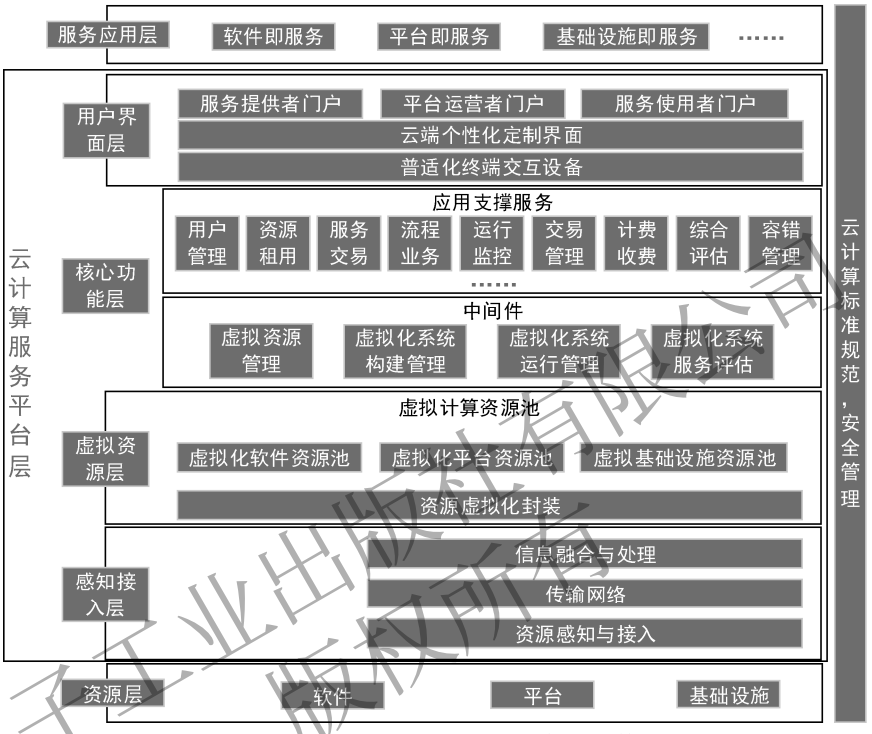


图 3-16　一种面向服务的层次化云计算系统体系架构

在系统集成方面，针对不同异构云系统的集成技术是目前研究的主要内容，主要出现了两种方法：一种是“总线”集成，如 CloudSwitch，它抽象了不同云平台的应用和接口，为异构云系统提供总线集成服务；另一种是正在开发中的技术，为使各类云系统通过标准化的 API（应用程序接口）进行交互和集成，其建立了各类集成接口标准。此外，还值得研究的是基于服务计算的集成技术。

云计算技术还包括云计算资源感知技术、资源的虚拟化/服务化技术、云服务环境的管理与构建技术、虚拟化云服务运行技术、云服务评估技术、可信云服务技术、普适人机交互技术等。

3.4　工业控制技术

工业控制技术主要利用电子电气、机械、软件组合实现。其主要使用计算机技术、微电子技术、电气手段，使工厂的生产和制造过程更加自动化、效率化、精确化，并具有可控性及可视性。

随着物联网技术的快速发展，工业控制技术对数据采集质量、数据传输速度、数据分析计

电子工业出版社有限公司 版权所有

算能力提出了更高的要求，工业互联网的应用为工业控制技术带来了新的发展动力。基于工业互联网的新型工业控制系统，利用智能传感器和新型网络等基础设施，依托工业互联网、人工智能和大数据等集成技术，实现了工厂的自动化控制。

新型工业控制系统主要包括工业资源层、智能控制感知层、工业网络及边缘处理层、工业互联网平台（INDICS 平台）和工业应用层，如图 3-17 所示。工业资源层中的工业生产制造过程的设备及过程数据由智能控制感知层采集，数据经工业网络及边缘处理层处理后，传输到工业互联网平台和工业应用层；通过利用人工智能技术和大数据分析技术等新一代信息技术进行数据的处理，并将处理结果反馈给工业资源层的终端工业设备或控制端，从而实现工业系统中的自动化控制应用。

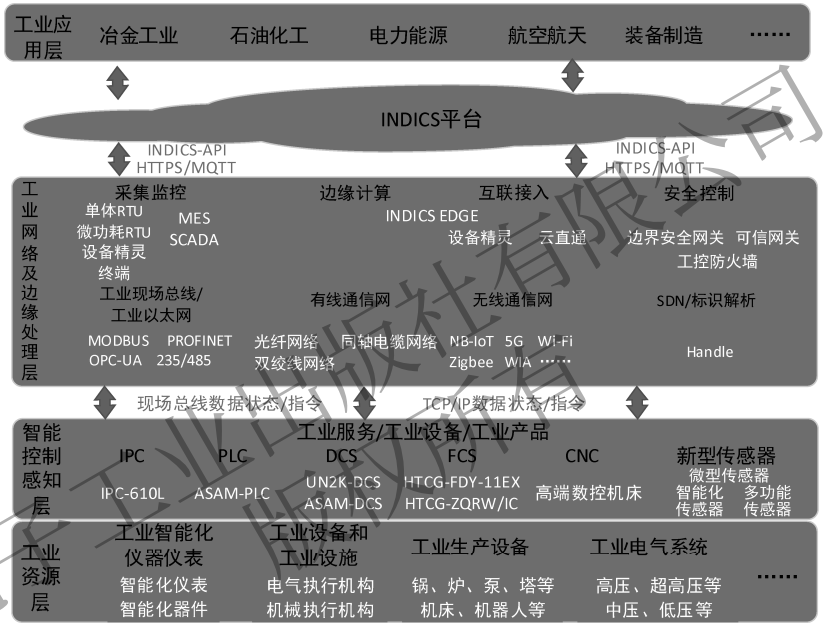


图 3-17　新型工业控制系统的组成

其中，工业资源层包括工业智能化仪器仪表、工业电气系统和工业生产设备等硬件资源，并提供基于工业互联网的工业设备和工业设施。智能控制感知层提供数据采集和控制设备，如 PLC、DCS 和 FCS 等，以及基于新网络的新型传感器，用于实现工业控制和基于工业互联网的工业数据大规模采集。工业网络及边缘处理层为基于工业互联网的多源异构工业数据提供智能连接、互操作性和处理技术，支持大规模数据传输和基于新网络协议的边缘计算。工业应用层作为一个新的工业控制系统，为各种工业应用场景提供控制应用，如冶金工业、石油化工、电力能源、航空航天和装备制造等。

3.4.1　数据智能感知采集技术


数据智能感知采集技术

随着工业互联网、人工智能和大数据技术的发展，基于工业互联网的工业控制技术对数据感知提出了更高要求。工业互联网环境下的数据智能感知采集技术是一种新的数据采集技术。作为智能时代工业控制过程中的主要数据采集技术，它已经成为基于工业互联网的新型工业控制系统发展的关键技术。

工业互联网环境下的数据智能感知采集技术，采用 PLC、DCS、FCS、新型传感器等智能

电子工业出版社有限公司版权所有

感知采集系统和设备，采集工业生产中的诸如智能化仪器仪表、数字电动执行机构等工业设备执行过程中产生的运行数据。通过机器学习、神经网络、智能化判断推理等过程进行数据的分析与处理，达到智能化控制目标。下面介绍几个典型的数据智能感知采集技术。

1．PLC 技术

可编程逻辑控制器（Programmable Logic Controller，PLC）是一种专门为工业环境应用设计的电子控制设备。它采用一种可编程的存储器，在其内部存储执行逻辑运算、顺序控制、定时、计数和算术运算等操作的指令，通过数字式或模拟式的输入/输出来控制各种类型的机械设备或生产过程。西门子 PLC 如图 3-18 所示。



图 3-18　西门子 PLC

它的特点是高度灵活、易于使用、适应性广、可靠性高、抗干扰性强、编程简单。其目前被广泛应用于工业控制系统中。

2．DCS 技术

集散控制系统（Distributed Control System，DCS）是以微处理器为基础，采用控制功能分散、操作和管理集中、兼顾分而自治和综合协调设计原则的新一代仪表控制系统，也可直译为“分散控制系统”或“分布式计算机控制系统”。

它遵循控制功能分散、操作和管理集中的基本设计思想，采用多层分级、合作自治的结构形式。其主要特征是集中管理和分散控制。DCS 在电力能源、冶金工业、石油化工等各行各业得到了极其广泛的应用。

DCS 是一种分散的综合控制系统，通过分解系统结构，采用分层控制和分级管理的方法，在难以集中控制的大规模复杂过程控制系统中，减少对过程监测和控制的人为干预。它增加了过程控制的可用性、安全性和可靠性，提高了产品质量和效率，实现了数据交换和信息管理的目标，是目前工业控制系统中广泛使用的控制结构。随着设备间信号传输逐渐从模拟信号转向数字信号，动态的现场实时过程控制可由独立设备在过程控制层面直接完成，这不仅大幅降低了集中式数据处理与传输的压力，还使系统具备安全可靠、灵活性强、控制特性优及综合控制能力突出的显著优势。

3．FCS 技术

现场总线控制系统（Fieldbus Control System，FCS）是集散控制系统（DCS）的更新换代产品，是由 DCS 和 PLC 演变而来的控制系统技术，其核心技术是现场总线技术。FCS 和 DCS 的结构对比如图 3-19 所示。FCS 将多点、多站、分布式、参数化的数字控制器和仪器设备结合在一起，形成一个具有分布式结构、互操作性和协调性的控制系统。凭借较高的通信效率、稳定性、可靠性、可扩展性以及较低的设置和维护成本，FCS 在工业控制领域获得了广泛认可，并逐渐成为工业控制系统的主流技术。从本质上说，它是一种数字通信协议，是基于智能现场设备和自动化系统的数字式、全分散、双向传输、多分支结构的通信网络。它是控制技术、仪表工业技术和计算机网络技术三者的结合，具有现场通信网络、现场设备互连、互操作性、分散的功能块、通信线供电和开放式互联网络等技术特点。

电子工业出版社有限公司 版权所有

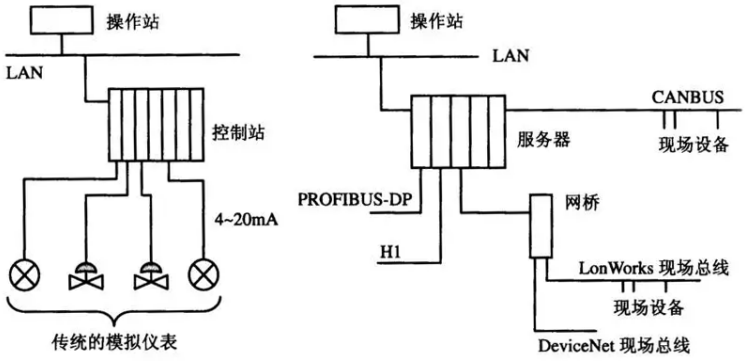


图 3-19　FCS 与 DCS 的结构对比

FCS 系统的核心是总线协议（总线标准）。总线协议确定了相关的关键技术与设备，确保了现场总线系统的互操作性。为了实现互操作，每个现场总线装置都用装置描述（DD）来描述，DD 包括所有必要的参数描述和主站所需要的操作步骤，确保了装置通信过程中所有信息的完整性。现场总线标准经历了多年的纷争，形成了一个由 8 个类型组成的 IEC61158 现场总线国际标准，分别是 TS61158、ControlNet、PROFIBUS、P-Net、FF-HSE、SWIFTNet、WorldFIP 和 Interbus，每个标准都是独立的，每个总线协议都有一套相应的软件和硬件支持。

FCS 有 5 种基本类型：数字控制、机器人控制、物料经营控制、批量过程控制和连续过程控制。这 5 种类型目前正在几个典型应用中积极实施，包括制造业、过程控制领域、建筑自动化以及发电厂、发电站和能源系统的自动化。这种分散的现场控制、多系统动态控制和逻辑过程控制的典型组合是先进 FCS 技术发展的强大动力。上述典型应用可与通信网络和工业互联网信息平台相结合，通过数据采集、大数据分析和系统监测，实现工业系统的现场控制、优化生产节奏和监测系统安全的目标。FCS 与企业的 ERP、MES 等信息化系统相结合可以获得仓储管理、物料优化、物流配送自动化等数据，成为支撑企业管理水平提升的基础。

电子工业出版社有限公司 版权所有

4．新型传感技术

工业互联网与互联网的不同之处在于，它在传感器层面连接物理世界和信息世界，基于传感器的数据收集为工业互联网应用层面可靠和准确的数据检索提供了技术基础。随着人工智能、大数据技术，以及新材料和网络的发展，传感技术也在经历转型。与传统的传感技术相比，新型传感技术更加紧凑、数字化、智能化和网络化，适合在工业控制系统中集成和应用。基于工业互联网控制系统，新型传感器主要包括微型传感器、智能传感器和多功能智能传感器。

微型传感器也被称为微型敏感元件，通常利用先进的微电子制造技术和微机械加工制造技术来制造，其内部结构尺寸一般在微米甚至纳米量级。这种微小的尺寸使得微型传感器具有许多优点，如小体积、低成本、集成化、智能化等。其特点是体积小、重量轻、耗电量低。在工业互联网时代，微型传感器由于其出色的灵敏度特性，经常被用作工业控制领域的信号检测和测量装置。例如，其能够在航空、医学和工业自动化等领域结合新的网络技术进行接触测量、非接触接近测量和远距离信号检测。图 3-20 所示为博世 BHI 160BP 集成惯性 MEMS 传感器。MEMS 传感器，即微机电系统传感器，是一种基于微电子机械系统（Micro-Electro-Mechanical System）技术制造的微型传感器。其结合了微机械加工技术和微电子处理能力，能够在微观尺度上感知和响应物理量。

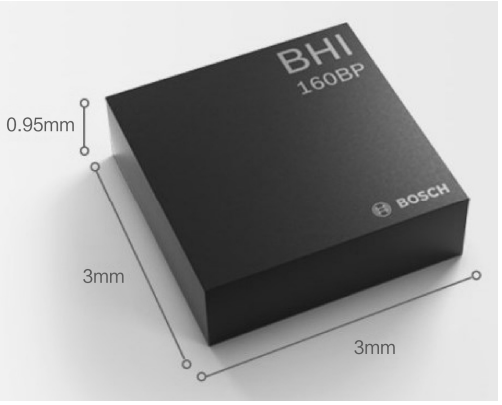


图 3-20　博世 BHI 160BP 集成惯性 MEMS 传感器

智能传感器是具有信息处理功能的传感器，带有微处理器，具有采集、处理、交换信息的能力，如基于光学感应采集信息的条形码，利用射频信号自动识别目标对象的 RFID 技术等新型智能化数据采集装置。其优点包括纠错、自我诊断和自我校准、多参数混合测量、实时处理大数据以及具备与计算机系统的标准化接口。基于新的网络和智能技术的新型智能传感器被广泛用于系统前端的远程监控和数据检测。

多功能智能传感器是一种能同时感受两种或两种以上被测量并转换成可以接收和处理的信号的装置，且集成了传感器、信号处理单元、通信接口与智能算法。其特点是采集各种物理量、实时信息处理、数据分析和存储及高速数据传输。例如，将 PVDF 材料、无触点皮肤敏感系统、压力传感元件、微处理器、信号处理和传输结合在一起的人造皮肤触觉传感器，可以实现触觉、刺激和其他仿生功能。

电子工业出版社有限公司
版权所有

3.4.2　工业控制网络及边缘处理技术



工业控制网络及边缘处理技术

1. 工业控制网络

随着工业互联网的发展，工业控制网络正在整合新一代的信息、数字和智能技术，其以工业以太网、工业有线通信网络、工业无线通信网络和 DN/标识解析为基础网络，符合多协议和信息化层次模型，可以实时处理来自工业设施的测量和控制信息。工业控制网络是数据和信息处理的通道。

基于工业互联网的新型工业控制网络，弥补了传统工业控制系统基于网络传输方式的缺点，将控制端网络采集和监控、边缘计算和工业控制信息安全控制等技术与工业控制数据整合在一起，实现了边缘计算和数据预处理，并通过网络管理层将数据传输到云基础设施进行分析和处理。

（1）工业以太网：工业以太网是一个强大的区域和蜂窝网络，与 IEEE 802.3/802.3u 兼容。主要的工业以太网技术有 MODBUS TCP/IP、Ethernet/IP、PROFINET、EtherCAT 等。自适应的 10/100Mb/s 工业以太网使得形成星型、总线型和环型网络拓扑结构非常方便，如图 3-21 所示。与传统的以太网技术相比，工业以太网的特点是抗干扰能力强、数据传输速率高、软硬件产品种类多、应用范围广。

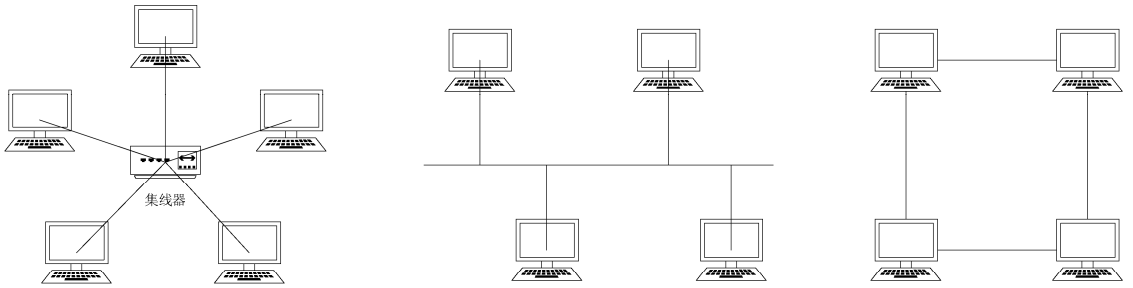


图 3-21　网络拓扑结构

（2）工业有线通信网络：工业有线通信网络是指用同轴电缆、双绞线和光纤等传输介质连接工业设备和控制系统的通信网络，用于数据和信息传输，是使用十分广泛的工业网络连接形式之一。然而，它也有一些缺点，如数据传输速率低和抗噪声能力弱，以及容易受到传输距离的限制。

在工业控制网络中，数据和信息的传输，以及工业设备之间通过有线网络连接提供服务必须遵循某些控制数据传输的协议，如 USB 协议、RS-232 协议、RS-485 协议和 M-Bus 协议等。这些协议统一了通信的各项规则，具体定义了通信双方需要共同遵守的执行功能、数据传输的步骤与速度、同步数据的方式和格式，以及设备间的协同关系等。

（3）工业无线通信网络：随着计算机、通信和无线传感器网络技术的快速发展，满足低成本、低能耗、高灵敏度的数据传输要求的无线网络正成为复杂工业现场环境和高可靠性工业应用的关键网络传输通道。特别是随着 5G 技术的发展和应用，无线网络正在从传统的 Wi-Fi 和蓝牙数据传输方式向多协议和多标准的工业应用发展。

工业无线通信网络在工业生产中发挥着重要作用，扩大了原有工业有线通信网络的覆盖范围，弥补了现有工业总线和有线网络的不足。高效的工业无线通信网络通过连接人和机器，大大加快了工业生产的决策过程，减少了设备停机时间，增加了工业工厂的网络冗余，从而提高生产力，有效降低生产成本，使企业实现实时运营。

2．边缘处理技术

边缘处理技术主要指的是边缘计算（Edge Computing）技术，它是一种新型的分布式计算方式，将计算、存储和数据处理能力从遥远的云端转移到数据源附近的“边缘”节点。其核心思想是在靠近数据源的边缘节点上处理数据，以减少数据传输的需求，加快响应速度并节省带宽。它特别适用于需要进行实时数据处理或对延迟敏感的场景。

其核心技术主要包括边缘节点（分布式设备，用于数据采集、存储与处理。这些设备包括智能传感器、工业控制器、路由器和网关等，其能够在本地进行数据处理，减少了对中心化云服务器的依赖）、边缘 AI（部署于边缘节点的机器学习模型，可以实现实时预测和决策。边缘 AI 对计算性能有很高的要求，需要使用高效的硬件加速器来支持复杂的人工智能推理任务，如 ASIC 芯片、FPGA 芯片、GPU 芯片和 DSP 芯片等）、容器与微服务（提供灵活的应用部署与扩展能力，有助于优化边缘计算的性能）、通信协议（支持边缘设备之间的数据传输和通信）

电子工业出版社有限公司

等。工业控制系统边缘的数据采集、存储、处理和传输越来越多地借助边缘计算网关和边缘数据处理技术来实现。如图 3-22 所示，在边缘进行预处理后，数据可以被发送到云端进行开发和使用，从而使工业数据的价值实现最大化。跨越边缘/云的综合协作商业模式扩展了工业生产规模，提高了工业管理的效率。

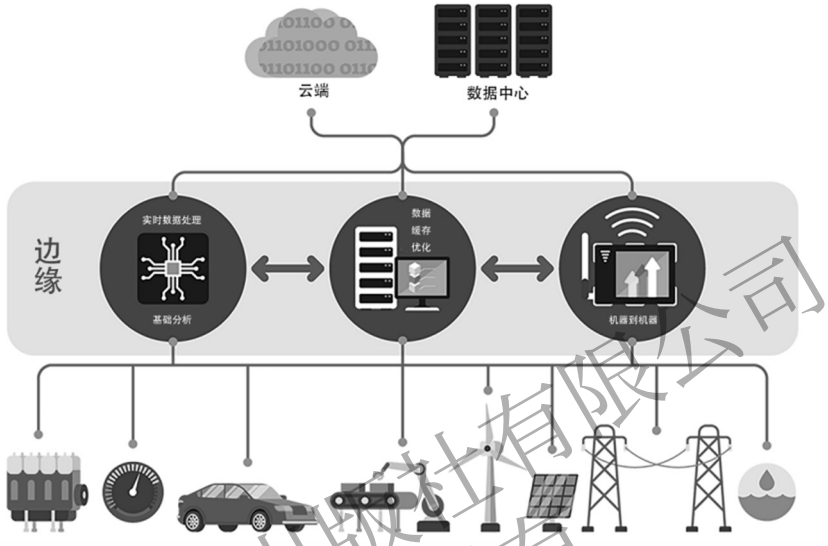


图 3-22　边缘处理

3.5　工业大数据技术

工业大数据技术

信息技术的加速发展不仅改变了世界市场本身，还改变了人们的工作和生活方式。特别是在工业生产中，低成本、耐用的微型传感器的引入和以物联网为代表的新一代网络技术的发展，赋予了许多物理物体感知和传输表达的能力，大量工业数据的收集和传输已经超越了时间和地点的限制。云计算等新的数据技术可以大大降低工业数据处理的技术门槛和成本，工业大数据时代已经到来。工业大数据是工业互联网真正意义上的企业应用价值的关键。

3.5.1　工业大数据的来源

工业大数据（Industrial Big Data）是指在工业领域，围绕典型智能制造模式，从客户需求到销售、下单、计划、研发、设计、工艺、制造、采购、供应、库存、发货和交付、售后服务、运维、报废或回收再制造等整个产品全生命周期各个环节所产生的各类数据及相关技术和应用的总称。随着传感器的普及，智能芯片被嵌入设备和产品中，就像飞机的黑匣子一样，自动记录所有生产和销售过程中的数据。工业大数据以产品数据为核心，极大延展了传统工业数据范围，同时包括工业大数据相关技术和应用。其主要来源可分为以下三类：企业经营管理数据、制造全生命周期数据、技术/产品/设备数据，如图 3-23 所示。

电子工业出版社有限公司 版权所有

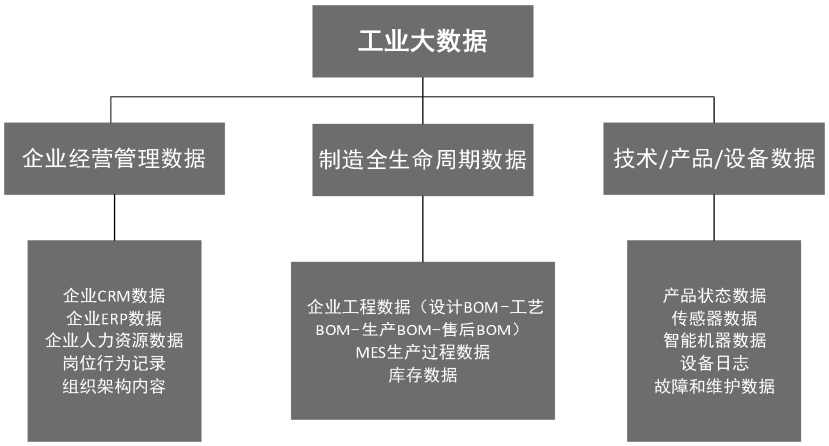


图 3-23　工业大数据的主要来源

3.5.2　工业大数据的特征和分类

工业大数据除了具有一般大数据的 4V 特征（数据量大、多样、快速和价值密度低），还具有时序性、强关联性、准确性、闭环性等特征。

（1）数据量大（Volume）：工业数据体量比较大，随着大量机器设备产生的高频数据和互联网数据的持续涌入，大型工业企业的数据集将达到 PB 级甚至 EB 级别。庞大的工业数据对数据存储、并发处理的要求极高。

（2）多样（Variety）：第一体现在数据类型多样性和来源广泛；第二体现在工业数据分布广泛，其分布于机器设备、工业产品、管理系统、互联网等各个环节；第三体现在数据结构复杂，既有结构化和半结构化的传感数据，也有非结构化数据。

（3）快速（Velocity）：快速是指获得和处理数据的速度快。工业数据处理对速度的需求呈现多样性：生产现场级要求时效性分析达到毫秒级，管理与决策应用需要支持交互式或批量数据分析。

（4）价值密度低（Value）：价值密度是有价值的数据量与数据总量的比率。建设大数据基础设施的关键是如何从智能制造云产生的大量数据中提取有价值的信息。以设备的远程操作和维护为例，在不间断的监测过程中，被认为有用的数据非常少。

（5）时序性（Sequence）：工业大数据具有较强的时序性，如订单、设备状态数据等。

（6）强关联性（Strong-Relevance）：一方面，产品生命周期同一阶段的数据具有强关联性，如产品零部件组成、工况、设备状态、维修情况、零部件补充采购等；另一方面，产品生命周期的研发设计、生产、服务等不同环节的数据之间需要进行关联。

（7）准确性（Accuracy）：准确性主要是指数据的真实性、完整性和可靠性，更加关注数据质量，以及处理、分析技术和方法的可靠性。工业大数据对数据分析的置信度要求较高，仅依靠统计相关性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相结合，挖掘其中的因果关系。

（8）闭环性（Closed-loop）：包括产品全生命周期横向过程中数据链条的封闭和关联，以及智能制造纵向数据采集和处理过程中，需要支撑状态感知、分析、反馈、控制等闭环场景下的动态持续调整和优化。

从数据产生的频率来看，工业大数据可以分为三类：第一，静态数据，如企业信息、资料

电子工业出版社有限公司 版权所有

数据、经验公式及专家知识等不变化或者极少变化的数据；第二，低频率生成的动态数据，如设计模型数据、库存管理数据、用户反馈数据等由个人或群体维护的数据；第三，高频率产生的实时数据，如从产品、设备、传感器等实时获得的模拟和数字信息。

在企业生产和运营方面，工业大数据可以按照不同环节和不同用途分为三类：第一，业务数据，主要反映企业资源和管理成果，包括企业的人力、财力和物力的基本信息，以及供应商、客户和其他深度参与企业业务活动的合作伙伴的基本信息；第二，生产数据，主要反映企业的生产能力，也涵盖整个产品生命周期，即产品开发和设计、原材料准备、工艺制造、产品制造和售后服务等各个方面的基本数据；第三，环境数据，主要反映生产保障、质量控制和遵守生产标准的情况，包括设备运行环境、温度和湿度、噪声、空气、废水和废气排放、能源消耗等数据。生产环境会影响产品质量，对环境数据的动态监测可以反映出生产过程是否符合国家和行业标准以及是否合理。

目前的数据使用情况表明，业务数据比生产和环境数据使用得更频繁。然而，随着工业互联网的发展，合作设计、共同生产和供应链联系所创造的利益将越来越受到重视，产品生命周期和质量控制，以及产品能源效率等方面数据的使用将变得更加频繁。

3.5.3　工业大数据的关键技术

工业大数据的关键技术包括大数据集成与清洗、存储与管理、分析与挖掘、可视化、标准与质量体系、安全、智能等方面的技术，如图 3-24 所示。这些关键技术的应用推动了工业互联网由以服务个人用户消费为主向服务生产性应用为主转变，重塑了产业模式、制造模式和商业模式，促进了柔性制造、智能制造和网络制造的发展。



图 3-24　工业大数据的关键技术

工业大数据技术基于工业云计算服务平台进行海量数据的存储、挖掘和可视化呈现。这包括使用 Hadoop、Spark、Storm 等大数据框架进行批处理和流处理，以及利用决策树、贝叶斯、支持向量机等机器学习算法进行深度挖掘，利用数字孪生技术从测试、开发、工艺及运维等角度实现产品全生命周期内生产、管理、连接的高度数字化及模块化，并通过更广泛的互联互通，实现对物理世界的安全、可靠、高效、实时、协同的感知和控制。

1．大数据集成与清洗技术

大数据集成是指把不同来源、不同格式、不同特点性质的数据进行有机集中，这种集中包

电子工业出版社有限公司 版权所有

括逻辑与物理两种形式。大数据清洗是指对在平台上集中的数据进行重新审查和校验，发现和纠正可识别的错误，并处理无效值和缺失值，从而得到干净、一致的数据。

大数据集成与清洗技术的特点包括能够清洗海量实时数据；能够实现异构数据类型集成，包括传感数据等轻量结构化数据，以及监控视频、图片等非结构化数据。

2．大数据存储与管理技术

大数据存储与管理是指采用分布式存储、云存储等技术对数据进行经济、安全、可靠的存储与管理，确定数据优先级，并采用高吞吐量数据库技术和非结构化访问技术支持云系统中数据的高效、快速访问。

大数据存储与管理技术的特点包括能够实现海量数据的分布式存储；为保证实时制造决策与工控指令反馈，需要对各类存储数据进行快速访问。

3．大数据分析与挖掘技术

大数据分析与挖掘是指从海量、不完全、模糊及随机的大型数据库中发现隐含在其中有价值的、潜在有用的信息和知识。

大数据分析与挖掘技术的特点包括以应用目标为导向，即工业大数据应用目标广泛，需要深度结合应用目标进行特征算法设计；需要建立云制造应用的定量解析模型或人工智能分析模型。

4．大数据可视化技术

大数据可视化是指利用二维综合报表、VR/AR、数字孪生等计算机图形图像处理技术和可视化展示技术，通过传感器以及数据分析、建模仿真等手段，将数据转换成图形、图像并显示在屏幕上，实现工业运行过程的监控、预测和优化，如图 3-25 所示。大数据可视化技术使得枯燥、抽象的数据变得直观且易于理解，并通过交互处理实现了基于可视化数据的分析、交流和决策支持。

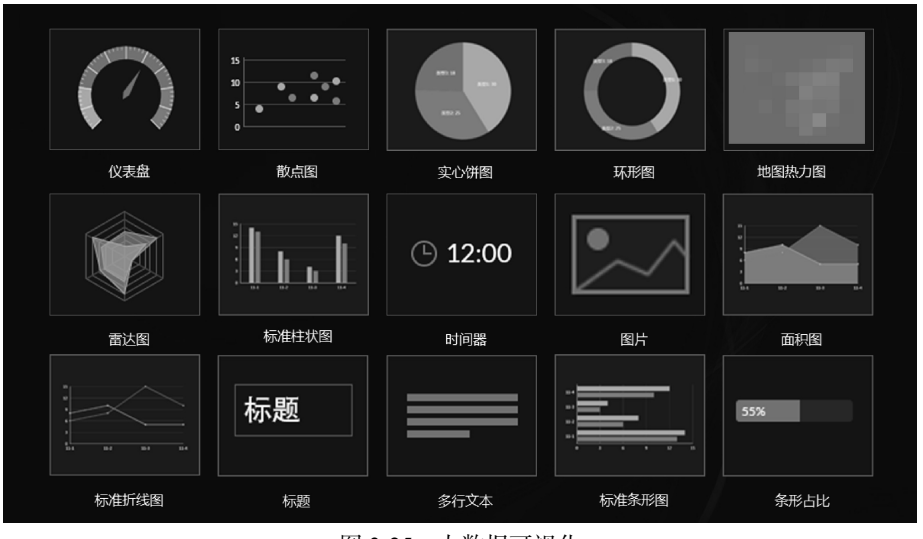


图 3-25　大数据可视化

大数据可视化技术的特点包括能够综合处理并显示多维度数据；能够在生产制造和企业

电子工业出版社有限公司 版权所有

经营管理等场景中，为决策者提供强大的视觉化交互支持。

5．大数据标准与质量体系技术

大数据标准与质量体系包括工业互联网中大数据通用技术、平台、产品、行业、安全等方面的标准与规范，涉及数据规范、标准、控制、监督等技术。

大数据标准与质量体系技术的特点包括多类型标准需求迫切；以交换和交易过程为导向，即标准与质量体系聚焦于跨领域数据交换集成和应用数据交易。

6．大数据安全技术

大数据安全技术涉及大数据采集、传输、存储、挖掘、发布及应用等技术，以及用户管控、数据溯源、隐私数据保护及安全态势感知等技术。

大数据安全技术的特点包括隐私保护要求高、难度大、关联性强；能够进行数据产生及应用过程的追溯与保护。

7．大数据智能技术

大数据智能技术包括数据平台技术、数据管理技术、数据分析技术、数据交互技术和数据可视化技术等。

大数据智能技术的特点包括海量数据的处理分析和挖掘，大规模机器学习和深度学习等技术的跨学科融合，以及通过建立模型解决现有问题和实现预测。

3.5.4　工业大数据价值的实现方式

1．实现量的积累

工业大数据价值的实现，始于数据量的积累。已经安装在中国的生产线上并开始有效运行的机器数量庞大，且装机量的年增长速度迅猛，远远高于全球平均水平。此外，中国自主研究、开发和生产机器的潜力越来越大，机器的应用范围也从高科技产业扩大到传统产业。在基础设施建设方面，中国的高速铁路技术和其他基建能力已稳步走向全球。随着制造业的转型升级，以及工业生产规模的不断扩大、国内技术的自主研发和智能生产的推广，中国将出现“工业 2.0”“工业 3.0”“工业 4.0”并行发展的局面。在这一过程中，生产规模的不断扩大、国产机器的自主研发推广及智能化生产的应用，将产生海量的产品数据、运营数据和价值链数据。这些数据的记录、传输、加工和存储，不仅规模庞大、增长速度惊人，而且为工业大数据的深度挖掘和价值发现提供了丰富的素材和对象。

2．通过深入的数据分析创造商业价值

工业大数据的真正价值，不仅在于其规模的庞大，更在于通过深入分析创造实质性的商业价值。虽然大数据能为企业提供对用户需求的洞察、提升生产效率、革新生产营销模式等，但面对来源多样、类型复杂、表现不一的数据，数据的存储、清洗、挖掘和提取工作充满挑战。

要充分挖掘这些数据的潜力，必须综合运用计算机科学、统计模型、机器学习、专家系统等先进分析技术，快速解析数据、提取关键信息、建立数据间的联系，从而获得对企业决策有价值的洞察。经过精心分析和价值挖掘的数据，甚至可以转化为数据产品，实现其商业价值。

出于工业出版社有限公司
版权所有

3．通过提高数据质量、优化数据管理来加强数据治理

要想进一步发挥工业大数据的潜力，除需要积累大量数据和进行深入的数据分析外，数据治理同样重要。数据质量的高低和数据管理的优劣直接影响大数据价值的实现。我国工业数据规模庞大，但在数据质量和管理上与发达国家相比仍有不小差距。

造成这一现象的原因包括我国生产工艺和流程与国际先进水平相比仍有较大差距。此外，在“工业 4.0”和工业互联网概念普及之前，我国制造业主要依靠低成本劳动力获得竞争优势，对先进机械设备的依赖相对较弱。同时，制造企业内部的现代化管理水平不高，产业链协同效应较差，数据孤岛现象普遍，数据应用基础薄弱。产业链低端环节、生产流程的简单性、对人工的依赖以及生产流程和产业链的孤立性，都导致了数据质量差、管理不善、数据关联度低和管理意识薄弱。这些问题在很大程度上限制了大数据价值的有效发挥。

3.5.5　工业大数据实施的关键问题

1．数据质量控制问题

原始数据质量决定了分析结果的质量。大数据的使用价值将是企业在未来获得竞争优势的关键因素之一，而企业的数据资产也越来越受到关注。然而，即使采用相同的数据收集和处理技术，如果要处理的原始数据的质量不同，则得到的结果和数值也会有很大差异。低质量的数据不仅增加了处理的复杂性，还可能导致解释上的严重错误。目前，中国的工业数据在一致性、完整性、准确性和及时性方面存在很多问题，如材料管理中的多编码和生产过程中的混合时间线，这是因为在数据源头上缺乏对数据管理的认识和能力。

2．多源数据关联问题

在大数据时代，工业数据的积累具有高噪声、异质性和来源多元、体量巨大的特点，这使得数据分析和应用成为一个重大挑战。通过建立数据关联模型来检测来自多个异质数据源的数据的相关性，作为大数据综合应用的下一步，具有重要意义。例如，层次化的物料清单（Bill of Material，BOM）定义了企业信息系统数据的核心语义结构。针对跨生命周期的研制 BOM 和实例 BOM 间结构失配问题，业界提出了中性 BOM 模型，并以此为核心，向前关联设计制造 BOM，向后关联服务保障 BOM，形成星型结构，极大地降低了数据关联的复杂度。同时，针对装备物联网数据和外部互联网数据，可以根据其绑定的物理对象（零部件或产品）与相应的 BOM 节点相关联，以解决生命周期管理过程中 BOM 结构不匹配的问题。

3．大数据系统集成问题

工业大数据的来源更加广泛，并且装备物联网数据（半结构化数据）和外部互联网数据（非结构化数据）都要与企业信息系统（结构化数据）进行集成，因此要重构数据支持平台，甚至替换“旧”系统。通过重构数据支持平台，可以打通企业不同部门和生产流程的数据路径，收集内部和外部互联网数据、半结构化和结构化数据，实现不同来源的数据整合，降低数据收集成本，展现数据的真正价值。

电子工业出版社有限公司 版权所有

3.6　建模仿真技术


建模仿真技术

建模仿真技术是以系统技术、相似原理、信息技术、模型理论、建模与仿真应用领域有关技术为基础，在计算机系统、仿真工具、物理设备等的支撑下，构建仿真目标模型，对产品全生命周期活动进行设想或者模拟的一门多学科综合性、交叉性技术。

建模是仿真的基础。它是指针对需要研究的对象，应用相关学科知识，进行近似表达的过程。通过建模，可以创建出具有三维立体感的虚拟模型，为后续的分析和仿真提供基础。

仿真则是在建模完成后，结合计算机科学手段，对模型进行图像化、数值化、程序化等的表达，以模拟和预测真实世界的物体和现象。仿真技术能够实现对真实情况的还原和测试，通过模拟极端环境，可以在短时间内获得更加准确的数据。

建模仿真技术的核心在于，其能够提供强大的数据处理和可视化功能，使用户更直观地了解和分析研究对象。它被广泛应用于能源、电力、石油化工、信息、材料、交通、医学、航空航天、国防军事等领域的系统论证、试验、分析、维护、辅助决策及人员训练场景，不仅可以支撑科研院所的科学研究，还可以服务于制造业生产优化、工程项目管理、产品测试改进等场景。工程建模仿真如图 3-26 所示。

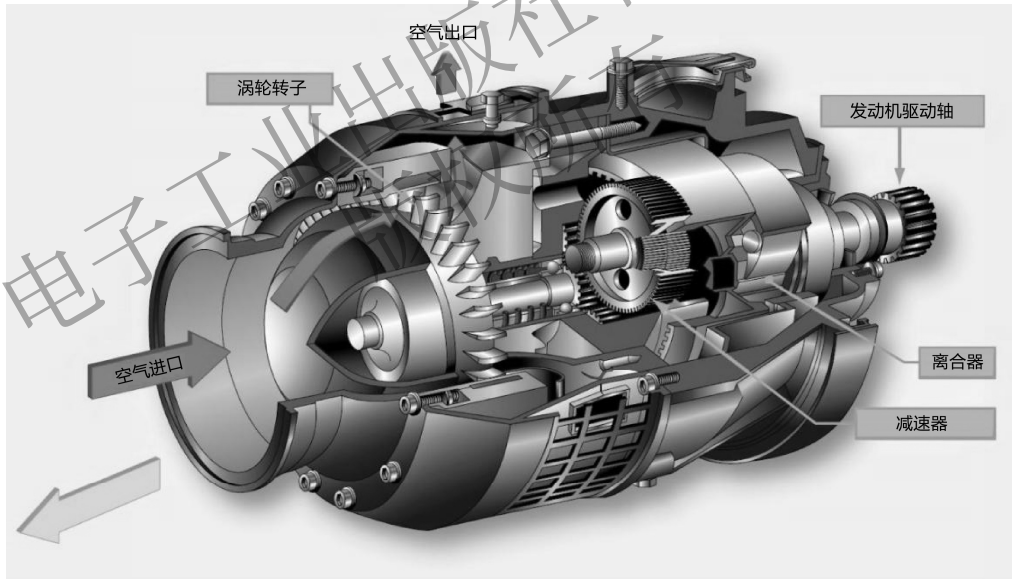


图 3-26　工程建模仿真

随着物联网和大数据等技术的发展，建模仿真技术的应用场景也越来越广泛。目前，建模仿真技术分为工程建模仿真、虚拟样机建模仿真、数字孪生等类型。作为工业领域的典型应用，建模仿真技术也在现代化领域发展，如网络、虚拟化、智能、协作、分销和服务。未来，随着工业互联网的推进和普及，工程建模仿真技术、虚拟样机建模仿真技术、数字孪生技术等会得到越来越多的应用。

3.6.1　工程建模仿真技术

工程建模仿真技术是一种工程应用形式，用于建模和分析具体的工程问题，其使用物理或

电子工业出版社有限公司

数学方法描述工程系统，并通过建模和验证描述物理对象的一个或多个属性。例如，工程仿真中制造领域的仿真涉及产品全生命周期各个阶段的仿真技术，如开发设计、加工、制造、使用、维护，以及企业运营和决策分析等。随着工业互联网等的发展，以 CAD、CAM、CAE 为代表的工程建模仿真技术在向集成化、网络化、智能化和标准化方向发展。

1．共性建模仿真技术

共性建模仿真技术主要包括建模仿真技术体系中的建模技术、建模仿真支撑技术及仿真应用中的共性应用技术，其中共性应用技术包括系统 VV&A（Verification，Validation &Accreditation）技术、仿真运行实验技术、仿真结果评估技术等，其为各工程领域的仿真应用提供了技术、环境、评估等支撑。

共性建模仿真技术是一种多学科集成的综合性技术。其以网络化技术为支撑，以计算机、多类型物理效应设备为工具，进行系统建模、仿真运行、试验评估。从仿真方式来看，共性建模仿真包括数字仿真、模拟仿真、混合仿真；从仿真类型来看，共性建模仿真包括连续系统仿真、离散系统仿真、混合系统仿真、定性系统仿真；从实现的手段来看，共性建模仿真包括实物仿真、半实物仿真、计算机仿真；从仿真运行时间来看，共性建模仿真包括欠实时仿真、实时仿真、超实时仿真。

2．多学科建模仿真技术

多学科建模仿真技术主要应用于结构、动力学、控制、电磁学和力学领域，利用专门的仿真分析工具和数据模型建立仿真模型，反映一个或多个系统行为属性的趋势，用于实验、分析和评估。仿真工具之间的数据接口可用于将数据模型和仿真结果传输给下一环节的工程师，以进行“链式”协作仿真，或者通过跨学科的“合作”建模仿真，对几个学科的相互关联的影响进行仿真和分析。

多学科建模仿真技术可以减少对物理实验的依赖，加速产品的开发和改进，并提升市场反应能力。经过几十年的发展，多学科建模仿真已经在多个领域形成了成熟的工具和产品，仿真技术呈现出多层次发展的态势。一方面，在特定专业领域，经典的单学科仿真工具依然是设计的基石，如用于多体动力学仿真的 ADAMS、用于结构仿真的 ANSYS Mechanical、用于模拟电路仿真的 SPICE 及用于数字电路设计的 VHDL/Verilog 等。另一方面，支持系统级设计的多学科仿真平台正变得越来越重要，如用于多物理场系统耦合仿真的 ANSYS Simplorer 和广泛应用于控制及多领域系统建模的 MATLAB/Simulink 等。此外，还有一些支持跨学科深度合作的建模平台，如北京仿真中心的 COSIM 等。

3.6.2　虚拟样机建模仿真技术

虚拟样机建模仿真技术是一种跨学科领域、系统级的建模仿真应用形态。特别是，它解决了不同学科和建模阶段之间的整合和互动问题，以及在跨学科互动的作用下，单一学科的建模过程在复杂系统的不同功能、性能和行为的模拟优化中的重用问题。通过整合各种单一学科的技术，并以协作建模为核心，跨学科的建模和虚拟原型仿真技术得到了越来越多的应用。虚拟样机建模仿真技术是基于 CAX（如 CAD、CAM、CAE）和 DFX（如 DFA、DFM）技术，融合了先进的系统建模技术、多学科仿真技术、先进的信息技术、先进的设计和生产技术、交互式界面互动技术、虚拟现实技术的一种综合应用技术，是从外观、功能和行为，甚至视觉、听

电子工业出版社有限公司 版权所有

觉和触觉等方面模拟真实产品，并将三要素（技术、管理和组织）和四类技术（建模仿真技术、信息技术、设计和制造技术及管理技术）有机集成的系统工程。

在虚拟样机建模仿真技术中，建模是仿真的基础。建模技术针对制造中的载体（如数控加工机床、机器人等）、制造过程（其相关因素包括加工过程中的力、热、液等问题）和被加工对象（如被制造的汽车、飞机、零部件），甚至是智能车间、智能调度过程中一切需要研究的对象，应用机械、物理、力学、计算机和数学等学科知识进行近似表达。而仿真技术则是在建模完成后，结合计算机图形学等计算机科学手段，对模型进行图像化、数值化、程序化等表达，以便进行更深入的研究和分析。

此外，虚拟样机还强调系统的观点，涉及产品全生命周期，支持对产品的全方位测试、分析与评估，并强调不同领域虚拟化的协同设计。虚拟样机可在一定程度上取代物理样机，应用于新产品的设计、实验、测试、生产和评估过程，有效地解决制造企业面临的与新产品相关的时间、质量、成本、维护和环境问题，使他们能够缩短产品开发周期，提高产品质量，降低产品制造成本，提高灵活性并提升对客户需求的响应能力。

1．虚拟样机基本概念

虚拟样机（Virtual Prototyping，VP）是一种基于产品的计算机仿真模型的数字化设计方法，进一步融合了先进建模/仿真技术、现代信息技术、先进设计制造技术和现代管理技术，应用于复杂产品全生命周期和全系统的设计，并对它们进行综合管理。这种技术能够在计算机上建立机械系统的数字化模型，并进行三维可视化处理，模拟在现实环境下系统的运动和动力特性。通过仿真结果，用户可以对系统进行精化、优化，从而获取最优设计方案，进而提升产品研发效率和产品质量，降低产品生产成本，提高企业的产品创新能力和市场竞争能力。虚拟样机技术在多个领域具有广泛应用，包括航空航天、船舶、轨道交通等先进制造业。

不同于传统的概念，工业互联网环境下的虚拟样机强调在“大协作、大制造”背景下，充分利用各类软硬件资源，基于并行工程等理念，实现跨组织、多人员、跨地域、全过程的虚拟样机仿真应用。多人员指的是外观/功能/行为等多领域、多学科专业人员及各任务相关方；跨地域指的是在工业互联网环境下，任务相关方在地域上是分布的，其通过统一的工业互联网云端环境，开展协同建模、协同仿真、协同评估等应用；全过程指的是虚拟样机需求提出、协作设计、设计验证、产品交付等典型过程。

2．虚拟样机建模方法

虚拟样机建模方法是一种集成了产品全生命周期不同学科领域知识的计算机建模仿真技术，是对复杂产品系统的建模和完整描述，涉及不同学科领域的专业要素（如对象、方法和技术）及各学科间的耦合关系，以实现仿真分析和模型重用。随着系统模型的日益复杂，虚拟样机建模方法已经从几何和功能建模发展到并行和分布式建模、数据建模、知识建模、分层建模和多模式建模等建模技术。针对复杂产品的虚拟样机建模，已有相关的国家标准进行规范，如《复杂产品虚拟样机建模方法》（GB/T 36457—2018），该标准规定了复杂产品虚拟样机建模的体系框架、高层模型组成等内容，为虚拟样机建模提供了指导和依据。目前具有代表性的虚拟样机建模方法有以下几种。

（1）基于统一建模语言的多领域建模方法。基于统一建模语言的多领域建模方法具有与领域无关的通用模型描述能力，有助于建立高度可靠的复杂系统模型，实现不同领域子系统模型

电子工业出版社有限公司 版权所有

之间的无缝集成。多领域建模是一种有效整合机械、电气、流体、光学和磁学领域模型的方法，基于统一建模语言的多领域建模方法，能够完成异构系统及其构件的一致性描述，实现领域模型间的无缝集成和数据交换，已成为虚拟样机的主要建模技术之一。该技术的典型代表是由国际开放组织 Modelica 协会提出的 Modelica 语言。

（2）基于高层体系结构（High Level Architecture，HLA）的分布式协同建模技术。基于 HLA 的分布式协同建模技术是一种高效、灵活的建模仿真方法，适用于复杂系统的建模仿真。它通过提供通用的支撑服务程序、定义清晰的接口规范和对象模型样板，可以支持各建模人员之间的协同工作，实现数据的交互和共享，从而提高建模效率和仿真系统的互操作性和重用性。HLA 是美国国防部（DoD）于 1995 年提出的一种分布交互式仿真的技术框架。HLA 通过运行支撑环境（Run-Time Infrastructure，RTI）提供通用的、相对独立的支撑服务程序，将仿真应用层与底层支撑环境功能分离，即将具体的仿真功能实现、仿真运行管理和底层通信传输三者分离，从而使各部分可以相对独立地进行开发。模型开发者需要熟悉各种 HLA/RTI 服务协议，并编写相关的应用程序。此外，系统顶层的建模能力相对较弱，基本上是在子系统层面进行集成建模与应用协同仿真方法。

（3）多学科虚拟样机高层建模方法。多学科虚拟样机高层建模是一种基于多学科和多模型建模技术，以及分层合作系统工程建模规范的虚拟样机系统建模方法，其实质是基于各学科组件模型，对虚拟样机系统的结构和行为进行统一高层建模与描述，并通过协同仿真实现虚拟样机的系统构建与仿真应用。多学科虚拟样机高层建模方法可以实现自顶向下的层次化分解与自底向上的系统组合，支持模型的分布式协同建模与异地协同仿真及重用。该方法既对已有各专业建模仿真工具和模型进行了很好的继承与重用，又增强了虚拟样机系统的顶层建模能力，并且可以很好地支持高层体系结构（HLA），实现了分布式协同建模与仿真应用。

应用工业互联网平台的虚拟样机建模仿真技术，能够实现分布建模、协同工作，支持跨领域、多尺度、多层次虚拟样机模型的构建，提供了标准化的接口和集成，具有良好的可扩展性。

3.6.3 数字孪生技术

数字孪生技术（Digital Twin Technology）是一种通过构建物理对象的数字映射，实现虚拟与现实同步的技术，如图 3-27 所示。该技术集成了物联网、云计算、人工智能、大数据等多种前沿技术，能够对物理世界进行全方位的仿真和管理。数字孪生技术通过传感器，以及数据分析、建模仿真等手段，将物理实体的状态和行为实时映射到虚拟空间中，形成一个与之对应的数字化模型，从而实现对物理世界的监控、预测和优化。随着国家数字化战略的推进，数字孪生技术得到了广泛的应用与发展，特别是在智慧城市、工业、医疗健康等领域。在智慧城市建设中，数字孪生通过对城市基础设施进行数字化建模，实现了对交通、能源、水资源等关键领域的精细化管理。在工业领域，数字孪生技术被广泛应用于生产线的优化和设备的预测性维护，提高了生产效率和资源利用率。

1．数字孪生概念的由来

数字孪生技术最早可以追溯到 20 世纪 70 年代末，美国国家航空航天局（NASA）开始使用数字孪生技术对航天器进行建模和仿真。在 2002 年的美国生产工程管理协会论坛上，PLM 顾问 Michael Greaves 博士首次提出了数字孪生概念模型。2010 年，NASA 在两个技术路线图（“建模、模拟、信息技术和加工”及“材料、结构、机械系统和制造”）中保留了“数字孪生”

电子工业出版社版权所有

的名称。随后，该技术在制造业、医疗健康、交通运输等多个领域得到了广泛的应用和发展。在制造业，借助该技术预测机械设备的损耗并据此制订维护计划；在医疗健康领域，借助该技术模拟人体器官功能，助力医生精准诊断病情，推动了个性化医疗的发展；在交通运输行业，借助该技术模拟交通系统的人车流动，为制订城市交通规划提供了参考依据。

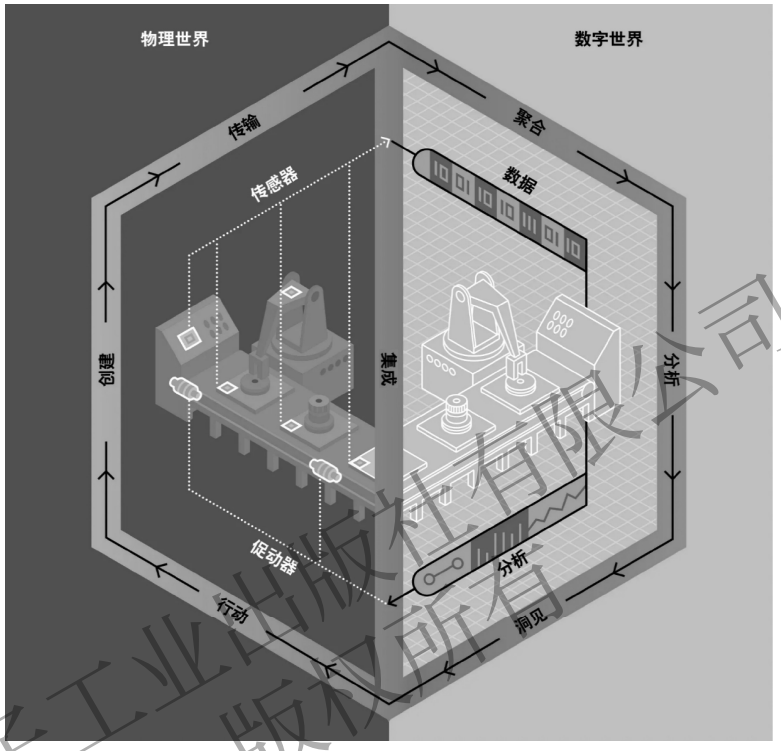


图 3-27　数字孪生

电子工业出版社有限公司
版权所有

2. 数字孪生的特征和关键技术

数字孪生具有以下典型特征：数据驱动、模型支持、软件定义、精准映射和智能决策。例如，基于模型支持和数据驱动，对物理对象进行数字化建模、绘图和智能应用，并通过模型和数据驱动的分析和预测实现对物理对象的控制和优化。基于工业互联网的数字孪生的关键技术主要有以下几种。

（1）数字孪生的建模技术。建模技术是数字孪生的核心技术，主要包括传感器网络技术、三维建模技术、物理仿真技术和数据处理技术。传感器网络技术可以快速获取现实世界中的数据，并将这些数据传输到数字孪生的数据处理系统中，保证了数字孪生数据的可靠性和实时性。三维建模技术可以将物理系统的几何形态、材质特性和运动状态等信息建模到数字孪生中。物理仿真技术可以在数字孪生中实现物理现象的精确模拟，以便进行预测和优化。数据处理技术可以提供高速、高效的数据处理和存储功能，以便数字孪生系统能够支持实时数据的处理和管理。

（2）数字孪生的数据驱动技术。数据驱动技术是数字孪生实现更高精度仿真、更智能化应用的重要手段，主要包括机器学习技术、数据挖掘技术和深度学习技术。机器学习技术可以通过数字孪生中的大量数据实现模型的训练和预测，在保证数字孪生可信度的情况下，提高系统的效率和精度。数据挖掘技术可以在数字孪生中自动发现数据间的关系和隐藏规律，并提供精

确预测和决策支持。深度学习技术可以实现更高层次的数据抽象和自主决策能力，并可以应用于自动化制造、城市工程和医疗健康等领域。

（3）数字孪生的边缘计算技术。数字孪生的边缘计算技术可以将数字孪生处理系统部署在物理系统的控制端，以保证系统的实时响应和高效传输。边缘计算技术可以在数字孪生中实现资源共享、系统互联和协作，并可以与物理系统融合，实现更高效、智能的生产和服务。同时，边缘计算技术可以实现异常监测、可视化识别和自主控制等功能，并可以应用于工业制造、智慧城市等领域。

（4）数字孪生的安全技术。数字孪生的安全技术是保证数字孪生安全运行的重要保障，主要包括网络安全技术、数据安全技术和隐私保护技术。网络安全技术包括网络防御技术和数据传输加密技术，以保护数字孪生系统免受网络攻击和恶意访问。数据安全技术可以对数字孪生系统中的数据进行备份、加密和恢复，以保证数据的安全可信。隐私保护技术可以保护数字孪生系统中与个人相关的信息不被非法使用和泄露。

3.7 信息安全技术


信息安全技术

随着工业互联网的发展，企业上云端已成为工业数字化转型的重要手段。在将传统工业的核心业务转移到云端的过程中，最重要的是安全问题。与传统的工控安全、互联网安全相比，工业互联网背景下的企业信息安全面临的防护对象范围更大、类型更多。安全威胁从信息环境延伸至物理环境，网络安全和工控安全互相交织，防御措施需要更加完备。具体来说，工业互联网环境下的信息安全与传统信息安全相比发生了以下三个转变：安全内涵转变，从网络信息安全转向网络信息/物理（CPS）安全；安全重心转变，从以信息系统安全为重心转向以数据安全为重心；安全模式转变，从边界安全转向零信任安全。

工业互联网背景下的信息安全，包括终端安全、网络安全、平台安全、数据安全、控制安全等诸多方面，采用的安全技术更加复杂，包括信息与数据防护技术、信息与数据加密技术、网络隔离技术和工业控制系统安全技术等。同时，在工业互联网的开放环境下，存在比较模糊的安全边界问题，需要采用零信任安全框架实施安全防护。通过以上技术和策略，强化不同人/设备的身份鉴别和访问控制，从而保护工业现场设备、工业控制系统、工业网络、工业应用及工业数据的安全。

3.7.1 信息与数据防护技术

信息与数据防护技术是利用数学或物理手段对电子信息在传输过程中和存储体内进行保护，以防止泄露的技术，常见的有加密技术、防火墙技术、反病毒软件技术等。随着工业互联网的推广应用，数据成为企业的重要资源，数据的积累、分析和应用打破了部门和企业的边界，协同效应越来越被人们重视。如何以最经济、最有效的方式保护信息安全，已经成为生产制造企业共同关注的问题。就工业互联网而言，需要保护的信息除了工业设备/主机、传输网络、数据中心内的信息数据，还包括在边缘接入系统的信息数据。常用的信息与数据防护技术主要包含以下几种。

1. 信息数据的认证系统

认证理论是密码学的一个重要和新兴分支。在认证理论中，信源识别和发送信息的完整性

电子工业出版社有限公司 版权所有

检验是密不可分的。换句话说，信源识别可以验证发送者身份的真实性，并确认其发送的信息在传输过程中是否被篡改、复制或延迟，从而保证传输信息的完整性。常用的认证方法包括用户名和密码认证方法、IC 卡认证方法、动态密码认证方法、PKI 认证方法、生物识别认证方法和 U-Key 认证方法。

应该注意的是，作为信息安全的重要方面，认证和保密性具有不同的功能和目的，是不同的问题。认证可以通过识别防止来自第三方的主动攻击，而保密性用于防止信息泄露。认证系统不能自动提供保密性，保密性也不能自动提供认证。

2．边缘接入系统的身份认证

与基于密码、数字证书和访问权限的传统认证方法相比，边缘接入系统可以根据物理层面的执行设备或生命形式，利用生物识别特征（如脉搏、指纹和虹膜）生成认证密钥。对于与用户没有联系的物理过程，边缘接入系统可以通过在访问控制期间将认证与特定的硬件相结合来实现认证。例如，Michael 等人提出了一种基于 SRAM 等硬件的轻量级认证方案，该方案使用一个物理上不可还原的函数，可以生成一个由硬件定义的特定密钥，并将访问请求与硬件相关联。该方案保证了基于位置的访问控制和加密，可广泛用于解决数据来源、完整性和设备身份管理问题。

3．用户密码

识别用户的方法有多种，其中最常见的是采用用户密码。用户密码识别的主要类型有以下几种。

（1）CALL BACK MODEM：CALL BACK MODEM 通过获取用户账户，挂断电话，然后回拨到用户终端来提供用户认证。这种方法的优点是，系统用户可以被限制为存储在 MODEM 中的电话号码的所有者，这样未经授权的人就不能从其他地方打电话来登录。然而，由于 MODEM 只能唯一地识别用户发起呼叫的地点，因此用户的自由度受到限制。

（2）标记识别：标记识别是指使用物理介质进行密码认证。物理介质包括一张含有随机代码的卡片，编码方法使代码难以复制。通过将卡片与终端上的读卡器 ID 连接，或在协助过程中输入密码，可以自动识别用户（通过代码），从而提高安全性。其优点是标识是随机的而且长于密码，缺点是卡片和读卡器必须一起使用，这给用户带来了不便。

（3）一次性口令系统：一次性口令系统也被称为“询问–应答系统”。与标记识别一样，该系统也必须在物理介质上实现，如便携式口令发生器。当用户登录时，系统向用户的口令生成器发送随机数，用户通过口令生成器向系统发送加密的口令，系统通过用相同加密程序、关键词和随机数产生的口令与用户输入的口令进行比较，识别并控制用户登录。这种方法具有强大的灵活性，只需要对口令生成器进行安全保护而不需要对口令进行保密，用户可以每次输入不同的口令。

（4）个人特征检测：通过个人特征检测来识别访问者的技术带有实验性特征，价格昂贵且不能达到完全可靠。因为无论是指印、签名还是声音、图案，在远程系统中都存在被非法入侵的风险，非法入侵者可以通过将入侵获得的系统校验信息重新显示来破解此类安全防护。

4．密码协议

密码协议是指两个或两个以上的参与者为完成密码通信中某项特定任务而约定的一系列

电子工业出版社有限公司 版权所有

步骤。密码协议通常涉及密码设备之间、密码管理者之间、密码管理者与被管理者之间，以及密码系统与所服务的用户之间，为完成密钥传递、数据传输，或者状态信息、控制信息交换等与密码通信相关的活动，而约定的通信格式、步骤，以及规定的密码运算方法、所使用的密钥数据等。该技术有许多细分研究领域，如身份或信息的认证、模态逻辑、密钥恢复及捆绑机制等。该技术还存在重大缺陷：如果密码协议逻辑设计不当，攻击者就可以方便地通过漏洞去攻击密码，从而攻破防护堡垒。

5．信息伪装

信息伪装是指将真实的信息伪装成其他真正要传输的与其无关的信息，即将机密资料隐藏到非机密文件中并通过网络传输，其目的在于使隐藏的信息以非机密资料的形式出现而免受网上拦截者的攻击。信息伪装技术不同于传统的用户密码技术。用户密码仅仅隐藏了信息的内容，而信息伪装不但隐藏了信息的内容，还隐藏了信息的存在。其形式可以是任何一种数字媒体，如图像、声音、视频等。信息伪装技术研究的内容包括信息隐藏和信息的产权认证、信息访问的合法身份认定等。一般来说，信息伪装技术具有隐蔽性、安全性、对称性和可纠错性四大特性。信息伪装技术包含的内容范围十分广泛，可以分为伪装术、数字水印、数据隐藏和数据嵌入等。

3.7.2　信息与数据加密技术

信息与数据加密技术是网络化信息安全的核心技术之一，在保护边缘接入系统、工业控制网络系统和数据中心的信息数据方面发挥着不可或缺的作用。

1．加解密过程原理

加解密过程原理如图 3-28 所示，其中 P（Plaintext）代表原文件，C（Ciphertext）代表加密后的文件，E（Encryption）代表加密算法，则有 $E(P)=C$，即 P 经过加密后变成 C。如果用 D（Decryption）代表解密算法，则有 $D(C)=P$，即经过加密后的文件 C 再经过解密返回原文件 P，也可用 $D(E(P))=P$ 表示。

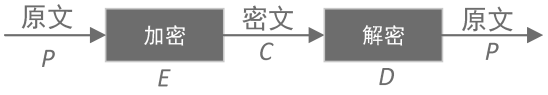


图 3-28　加解密过程原理

因为现代加密和解密算法是公开的，所以必须与非公开的密钥相结合，才能满足保密性要求。用 K 代表 Key（密钥），根据算法中加密所用的密钥是否相同可分为对称性算法和非对称性算法，其加解密过程原理分别如图 3-29 和图 3-30 所示。对称性算法加解密过程为 $E_k(P)=C$，$D_k(C)=P$，$D_k(E_k(P))=P$，算法中加解密所用的密钥是相同的（即 Symmetric Algorithm），有时也叫单钥。

非对称性算法则相反，加解密用不同的密钥，其过程为 $E_{k1}(P)=C$，$D_{k2}(C)=P$，$D_{k2}(E_{k1}(P))=P$，有时也叫双钥。（$K1$，$K2$）是成对出现的，其中一个加密的文件只能用另一个密钥才能解密，反向操作是不成立的，即不能用加密的密钥去解密。在两个密钥中，一个是保密的，称为私钥（Private Key，由密钥的所有者掌握），另一个是公开的，称为公钥（Public Key，

电子工业出版社有限公司 版权所有

任何人都可以获取）。在通常情况下，企业向不同的客户公布其公钥，客户用它来加密发送给该企业的信息，并将其发送给该企业，然后该企业可以用只有该企业拥有的私钥来解密该信息。

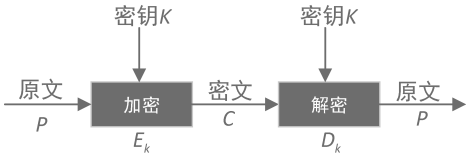


图 3-29　对称性算法加解密过程原理

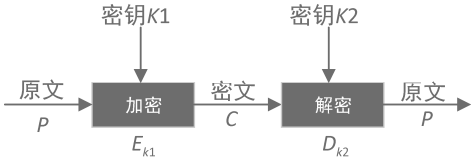


图 3-30　非对称性算法加解密过程原理

2．常用加密算法

常用的信息反馈加密方案有多种：单钥加密方案，如 DES 加密算法、IDEA 加密算法和 LOKI 加密算法；公钥系统，包括 RSA 算法、Elgamal 公钥、PGP 等；面向边缘设备数据隐私保护的加密算法；基于访问控制的加密算法。

（1）DES 加密算法：DES（Data Encryption Standard，数据加密标准）是全球著名的保密密钥或对称密钥加密算法之一，由 IBM 在 20 世纪 70 年代提出，1976 年 11 月被美国政府采用，并得到美国国家标准局和美国国家标准学会的认可。

（2）RSA 体制：RSA 方案由 Ronald L. Rivest、Adi Shamir 和 Leonard M. Adleman 于 1978 年提出，是理论上十分成熟的公钥加密方案，基于非对称性算法加密。该算法的体制构造基于 Euler 定理，通过大整数的分解（已知大整数的分解是 NP 问题）来保障信息的安全。用户首先选择一对不同的素数 p 和 q，计算 $n=pq$，$f(n)=(p-1)(q-1)$，找到一个与 $f(n)$互为素数的数字 d，并计算其逆数 a，即 $da=1 \bmod f(n)$，那么密钥空间 $K=(n,q,a,d)$。如果 m 和 c 分别是明文和密文，则加密过程为 $ma \bmod n=c$，解密过程为 $cd \bmod n=m$。在不知道 d 的情况下，从公钥 n、a 计算 d 的唯一方法是分解一个大整数 n。而根据 L. Rivest、Shamir 和 M. Adleman 的估计，使用最好的算法和运行速度为 100 万次/秒的计算机，一个 500 位 n 的分解时间为 4305 年。因此，RSA 保密性很好。

（3）面向边缘设备数据隐私保护的加密算法：边缘设备数据隐私保护有两条主要技术路线，即安全的多方计算和数据匿名化。安全的多方计算是基于数据编码的，每一方都可以根据商定的协议参与计算，并确保计算不会泄露个人数据，因为每一方只知道自己的输入和计算结果，而不知道其他方的参与情况。然后，数据被匿名化。数据匿名化是指有选择地披露少量信息以实现隐私保护，在完整性的丧失和隐私披露之间取得平衡。特别是 K-匿名化等技术可以确保数据隐私，同时最大限度地减少有效信息的损失。

（4）基于访问控制的加密算法：传统的访问控制技术通常是基于角色的访问控制，即通过使用户扮演适当的角色来产生关联。就工业互联网而言，由于它是一个由传感器和生产设备组成的传感网络，因此很难将角色分配给端点作为用户。此外，由于工业互联网融合了信息处理、控制和决策过程，对资源的访问控制需要高度动态化。这使得其不适合使用传统的访问控制技术。ABAC（Attribute-Based Access Control）通过响应用户属性的动态变化来更新访问控制策略，提供了一种更细化和灵活的访问控制方法。然而，这种算法的效用有限，因为其效率随着

电子工业出版社有限公司 版权所有

属性数量的增加而降低。有两个技术方向通常被用来提高基于属性的加密算法的性能：基于密钥的策略和基于密码文本的策略。

3.7.3 网络隔离技术

网络隔离技术是一种网络安全手段，旨在隔离有害的攻击，在保证可信网络内部信息不外泄的前提下，在可信网络之外完成网间数据的安全交换。在工业控制系统中，网络隔离技术得到了广泛的应用。通过防火墙和网闸等网络隔离技术，可以有效地限制网络流量的传播范围，减少攻击面，防止横向攻击和威胁传播，保护机密数据和敏感信息的安全。同时，网络隔离技术结合已建立的统一访问机制，限制用户访问权限和可使用的计算和网络资源，对云平台的关键资源进行访问控制和管理，从而达到用户隔离和数据隔离的目的。

1．防火墙技术

防火墙是当今被广泛使用的信息安全技术之一。它是一组配置在不同网络或网络安全域之间的组件的组合，根据设定的安全策略控制不同网络域之间的信息流，并具有很强的抗攻击能力。配置的安全策略包括限制从内部到外部或从外部到内部系统资源的未经授权的访问，以及为具有不同内部安全级别的系统之间的访问设置适当的权限。防火墙的隔离作用如图 3-31 所示。

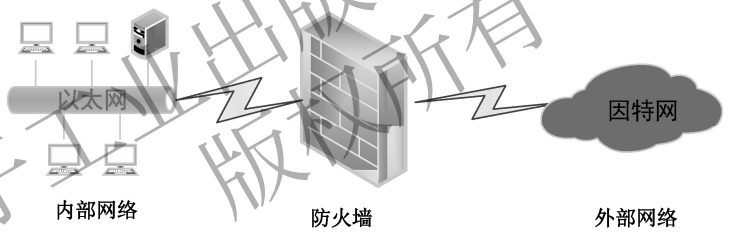


图 3-31　防火墙的隔离作用

防火墙是一个由计算机硬件和软件组成的系统，部署于网络边界，是内部网络和外部网络之间的连接桥梁。它对进出网络边界的数据进行保护，防止恶意入侵、恶意代码的传播等，从而保障内部网络数据的安全。防火墙技术不仅涉及硬件和软件的组合，还包含一组安全策略，这些策略定义了哪些数据可以进出网络，以及如何进行访问控制。其主要功能包括安全过滤和安全隔离，防火墙能够阻断外部通过网络对本网络的威胁和入侵，提供扼守本网络的安全和审计的关卡；访问控制，防火墙对内部与外部、内部不同部门之间实施隔离，确保只有被授权的通信才能通过；记录与监控，防火墙通过记录通过它的信息内容和活动，对网络攻击进行检测和告警，有助于后续的安全分析和审计。

2．网闸技术

网闸技术是一种信息安全设备技术，通过使用带有多种控制功能的固态开关读/写介质，连接两个独立的主机系统，实现它们之间的安全隔离与数据交换。网闸技术的实现原理是将两套各自独立的系统分别连接到安全和非安全的网络，两套系统之间通过网闸进行信息摆渡，保证两套系统之间没有直接的物理通路。在通信过程中，当存储介质与安全的网络连通时，断开

电子工业出版社有限公司 版权所有

与非安全网络的连接；当与非安全网络连通时，断开与安全网络的连接。通过分时使用两套系统中的数据通路进行数据交换，以达到隔离与交换的目的。此外，在数据交换过程中，需要同时进行防病毒、防恶意代码等信息过滤，以保证信息的安全。

网闸技术的核心在于物理隔离与协议转换。物理隔离意味着两个独立的主机系统之间不存在直接的物理连接、逻辑连接及信息传输协议。同时，网闸技术涉及协议转换。在数据交换过程中，网闸会对数据进行格式转换、内容过滤和脱敏等技术处理，将数据从源网络的格式转换为目标网络可接受的形式，并去除可能包含恶意代码或敏感信息的部分。这种处理方式确保了即使数据在传输过程中被截获，也无法被直接利用或解析。此外，网闸技术还具有单向/双向控制功能：网闸可以是单向的（例如，数据只能从高安全级别网络流向低安全级别网络），也可以是双向的（数据可在两个网络间双向流动，但受到严格控制）。这种控制功能进一步增强了数据交换的安全性。

3.7.4　工业控制系统安全技术

工业控制系统安全是工业互联网整体安全不可或缺的组成部分，包括网络安全、设备安全、应用安全和业务安全，常见的工业控制系统安全技术有系统安全防护、数据安全保护及网络隔离技术等。随着工业互联网的发展，工业控制系统现在被更多种类的进入点渗透，攻击目标范围更广，攻击深度也在不断加大。工业控制系统通常使用防火墙、网闸、OT 网络流量审计、恶意代码检测和隔离保护及工业主机安全保护等方法来提供安全防护。目前，以下关键技术可用于应对工业控制系统的信息安全威胁。

1．工业控制系统的漏洞挖掘与分析技术

漏洞挖掘是主动寻找源代码、协议标准、二进制代码和中间语言代码中已知和未知漏洞的过程。工业控制系统的漏洞挖掘与分析技术主要包括静态分析技术、基于攻击图的安全漏洞挖掘模型等。

静态分析技术是通过对二进制程序代码进行词法、语法和语义分析来发现潜在漏洞的方法。它可以在程序未运行时对代码结构、函数调用关系、变量使用等进行全面检查，有助于发现内存泄漏、缓冲区溢出、代码逻辑缺陷等常见漏洞。此外，静态分析技术能够自动处理大量代码，提高了漏洞挖掘的效率和覆盖面。

基于攻击图的安全漏洞挖掘模型也是一种重要的方法。该模型通过构建攻击图，对工业控制系统的安全漏洞进行挖掘和分析。攻击图模型可以帮助分析人员快速识别攻击路径和攻击点，从而发现潜在的安全漏洞。同时，它可以根据攻击路径的长度、攻击难度和攻击后果等因素，对安全漏洞进行优先级评估，从而帮助分析人员集中精力解决最关键的问题。

工业控制系统的漏洞挖掘与分析技术还在不断发展中，包括针对私有协议的漏洞挖掘、基于协议分析的漏洞挖掘、固件反向分析、软件动态调试、软件反向编译分析和状态监测等在内的多种新技术和新方法正在被研究和应用。

2．工业控制系统的数据采集与融合分析技术

工业控制系统的数据采集与融合分析技术涉及工业控制网络的信息采集、数据格式化、数

电子工业出版社有限公司 版权所有

据预处理、协议的深度解析和业务数据关联等环节，以此支撑工业控制系统威胁监测预警和态势感知。其通过采集与处理实时数据流量、网络协议、各种通信行为、操控指令、生产设备状态及行为的数据，在已建立的工业控制协议及未知私有协议分析模型的基础上，深度解析工业控制协议，结合工业控制的工艺和业务流程，分析数据报文的关联关系。

3．工业控制系统的威胁监测预警技术

工业控制系统的威胁监测预警技术主要包括已知漏洞攻击检测、未知威胁检测、威胁建模与等级划分、基于工业控制协议的业务攻击检测等技术。其根据攻击的危害程度，进行工业控制攻击威胁等级划分；通过漏洞攻击数据和代码的特征匹配识别来发掘已知漏洞的攻击；利用沙箱动态执行技术，监测网络行为的未知威胁；融合动态行为仿真分析、行为基线分析、数据建模分析等技术，实时监测工控特种木马、未公开漏洞、APT 等未知威胁；结合工艺业务流程，对工业控制协议数据包进行关联分析，挖掘数据包之间的逻辑关系，识别基于工业控制协议的特定攻击。

4．工业控制系统的攻击取证与追踪溯源技术

工业控制系统的攻击取证与追踪溯源技术是一个综合性的体系，它依赖于实时监测、日志分析、取证技术及人工智能技术的深度应用。其使用基于日志的协作与追踪溯源技术、网络恶意行为的特征、跳板主机的回溯、工业控制系统蜜罐、攻击代码的分析、威胁情报库等技术和资源，对工业控制系统的攻击源主机、攻击组织及攻击路径进行追踪溯源，支撑工业控制系统深度防御和反制。

3.7.5　零信任安全

零信任安全是一种网络安全框架，要求用户在访问组织的数字资产和网络之前，证明自身身份、访问权限和行为不具有恶意。零信任安全代表了新一代的网络安全防护理念，它的关键在于打破默认的“信任”，即“持续验证，永不信任”。它默认不信任企业网络内外的任何人、设备和系统，而是基于身份认证和授权重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信。零信任安全摒弃了传统网络安全策略中基于网络边界的信任模型，转而采用一种更为严格的访问控制机制。零信任安全成为工业互联网时代网络安全的新理念、新架构。零信任既不是技术，也不是产品，而是一种安全理念。零信任安全的本质是访问控制范式的转变，从传统的以网络为中心转变为以身份为中心进行动态访问控制。

零信任安全基础设施一般由三部分组成：设备和用户认证代理、可信访问网关和智能身份识别平台。其中，设备认证通过设备初始化和注册、设备认证和连续设备评估等举措实现设备状态转换，而用户认证则包括初始、连续和二次认证。可信访问网关作为服务访问代理，提供统一的传输加密机制和完整的流量日志输出功能，接管所有的服务访问请求并连接到智能身份识别平台。智能身份分析技术智能地支持自适应访问控制和身份治理。零信任架构适应广泛的商业环境和使用场景，在数据中心和远程办公室等实际情境下提供了更好的解决方案。图 3-32 所示为奇安信零信任架构。

电子工业出版社有限公司
版权所有

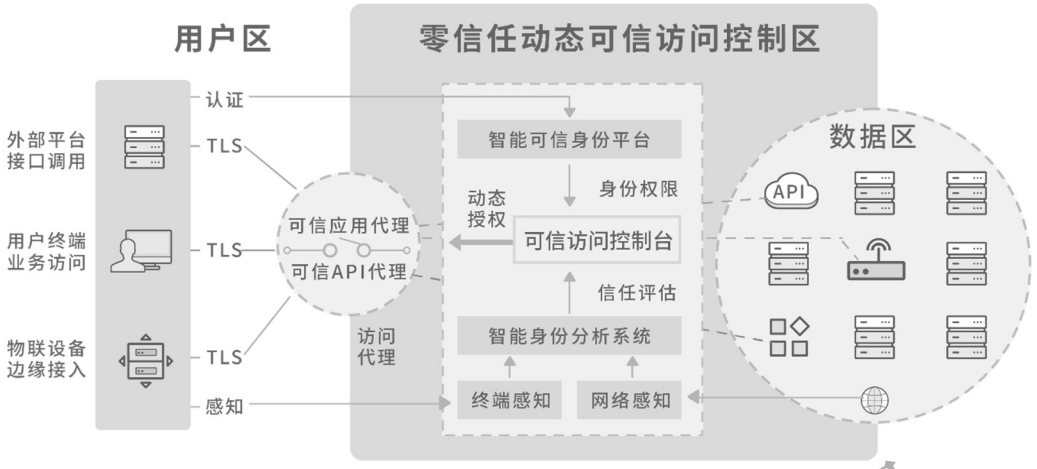


图 3-32　奇安信零信任架构

零信任架构的技术实践具有以下特点。

以身份为中心：网络上的人、设备和系统应被赋予逻辑身份，并根据身份进行细粒度的授权设置和决策。

业务安全的访问：所有的访问请求（应用程序、接口等）都应该被授权和被加密。

持续的信任评估：终端和用户等访问实体应被持续感知以评估其可信度，访问权限应根据可信度评估进行动态调整。

动态访问控制：访问权限不是静态的，而是根据主体属性、客体属性、环境属性和持续的信任评估结果进行动态计算和确定的。

零信任安全是为帮助企业应对数字化转型中的安全挑战而提出的一种理想的安全架构。零信任安全的特点是无边界设计，信任的建立不能简单地基于网络位置；情景感知，访问权限取决于系统对用户和设备的了解；动态访问控制，基于多维属性产生动态 ACL，所有访问都必须被认证、授权和加密。

企业中零信任安全理念的落实取决于实现零信任的技术解决方案。NIST 标准的《零信任架构》白皮书列出了三种技术解决方案，总结如下。

（1）软件定义边界（Software Defined Perimeter，SDP）：SDP 是实践零信任安全理念的技术架构与方案，是国际云安全联盟（CSA）于 2013 年提出的基于零信任（Zero Trust）理念的新一代网络安全技术架构。它在一个或一组企业应用程序周围创建基于身份和环境的逻辑访问边界。企业应用程序被隐藏，访问这些企业应用程序的实体必须经过信任代理。在允许访问之前，代理网关先验证指定访问者的身份、环境和是否遵守访问策略，以此将企业应用程序从网络用户的公众视线中移除，减少攻击面。

（2）增强的身份管理（Identity Access Management，IAM）：身份管理使企业可以自动访问越来越多的信息资产，同时管理潜在的安全和合规风险，为所有用户、应用程序和数据启用并保护数字身份。在企业环境中，IAM 定义和管理每个网络用户的身份角色及其所需资源的访问权限，并根据网络用户身份角色生命周期，对其所需资源访问权限进行动态管理。IAM 通过在整个组织中一致地应用用户访问规则和策略来增强企业对信息资产的保护力度，解决了企业的身份权限管理需求、应对合规和安全要求等问题。

（3）微隔离（Micro-Segmentation）技术：微隔离有别于传统防火墙单点边界上的隔离，微

电子工业出版社有限公司 版权所有

隔离的控制中心平台和策略执行单元是分离的，具备分布式和自适应特点。它可以将数据中心在逻辑上划分为各个工作负载级别的不同安全段，然后定义安全控制，并为每个唯一段提供服务。微隔离使信息技术人员可以使用网络虚拟化技术在数据中心内部部署灵活的安全策略，而不必安装多个物理防火墙。此外，微隔离技术可在具有策略驱动的应用程序级安全控制的企业网络中用于保护每台虚拟机（VM）。微隔离技术可以显著增强企业对网络安全风险的抵御能力。

小　　结

本模块围绕工业互联网的基础技术展开，详细介绍涵盖支撑工业互联网系统搭建与应用实施的各类技术，主要分为网络、数据、安全三个维度，包括物联网技术、网络通信技术、云计算技术、工业控制技术、工业大数据技术、建模仿真技术及信息安全技术。

在网络维度，网络技术是工业互联网的基础核心，主要包括物联网和网络通信技术。物联网通过传感器、RFID 等技术实现物物互联，而网络通信技术则包括移动互联网、天地一体化网络和网络通信基础技术（包括通信网络技术和高性能计算技术）。移动互联网结合了移动通信设备和互联网的优点，具有灵活性、实时性、定位性和保密性等特点。天地一体化网络通过卫星、飞机等实现全球无缝覆盖，支持高速、宽带、大容量信息传输。高性能计算技术通过集群计算、云计算等方式提升计算性能，支持大规模数据处理。

在数据维度，工业大数据是工业互联网的核心价值创造者，其来源包括企业经营管理数据、制造全生命周期数据和技术/产品/设备数据。工业大数据具有数据量大、多样、快速和价值密度低，以及时序性、强关联性、准确性和闭环性等特征。其关键技术包括大数据集成与清洗、存储与管理、分析与挖掘、可视化和安全等。通过大数据技术，企业可以实现数据量的积累，以及进行深入的数据分析和优化数据管理，从而提升工业生产的效率和质量。

在安全维度，工业互联网的安全保障至关重要，涉及终端安全、网络安全、平台安全、数据安全和控制安全等方面。信息安全技术包括信息与数据防护技术、信息与数据加密技术、网络隔离技术和工业控制系统安全技术等。同时需要采用零信任的安全框架实施安全防护。信息与数据防护技术包括信息数据的认证系统、用户密码、密码协议和信息伪装等。信息与数据加密技术通过加解密过程保护数据安全，常用的加密算法包括 DES、RSA 等。网络隔离技术通过防火墙和网闸等手段来确保网络安全。工业控制系统安全技术包括漏洞挖掘与分析、数据采集与融合分析、威胁监测预警和攻击取证与追踪溯源等。零信任安全框架可持续验证用户身份和访问权限，以确保身份可信、设备可信、应用可信和链路可信。

这些基础技术共同构成了工业互联网的支撑体系，推动了工业生产的智能化、自动化和高效化发展。

实训 3：数字化工厂建模实验

1. 实验目的

（1）了解数字化工厂的概念。

（2）掌握数字化工厂的建模技巧。

电子工业出版社有限公司 版权所有

（3）理解工厂数字化转型的基本形式。

2. 实验步骤

（1）打开 Factory IO 数字化软件，其界面如图 3-33 所示。

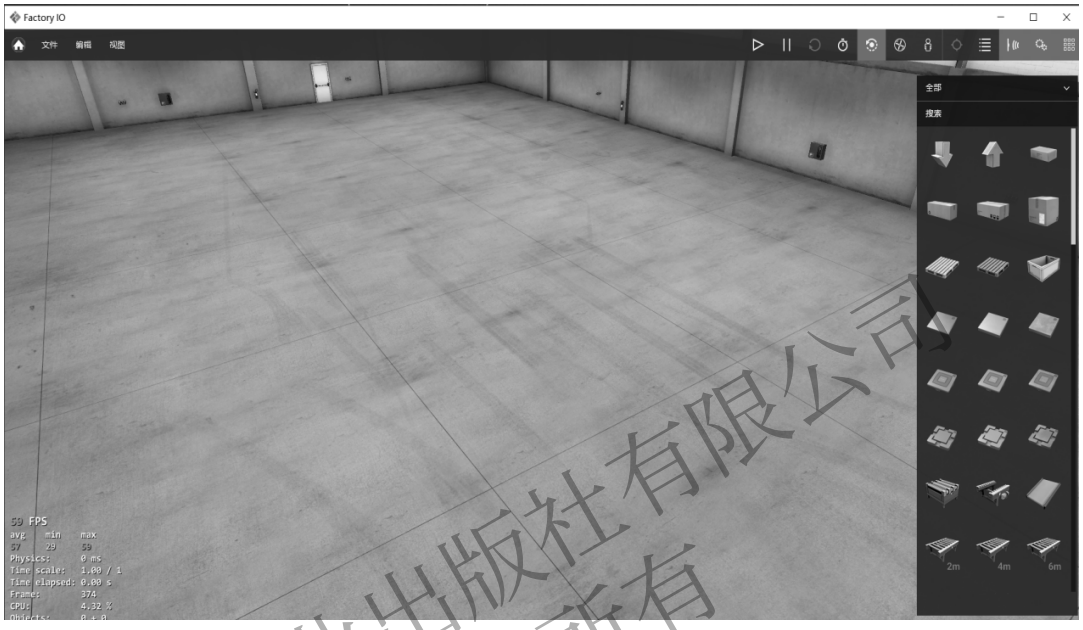


图 3-33　Factory IO 界面

（2）从右边工具栏中拖曳目标工厂组件，搭建一条加工生产线，如图 3-34 所示。

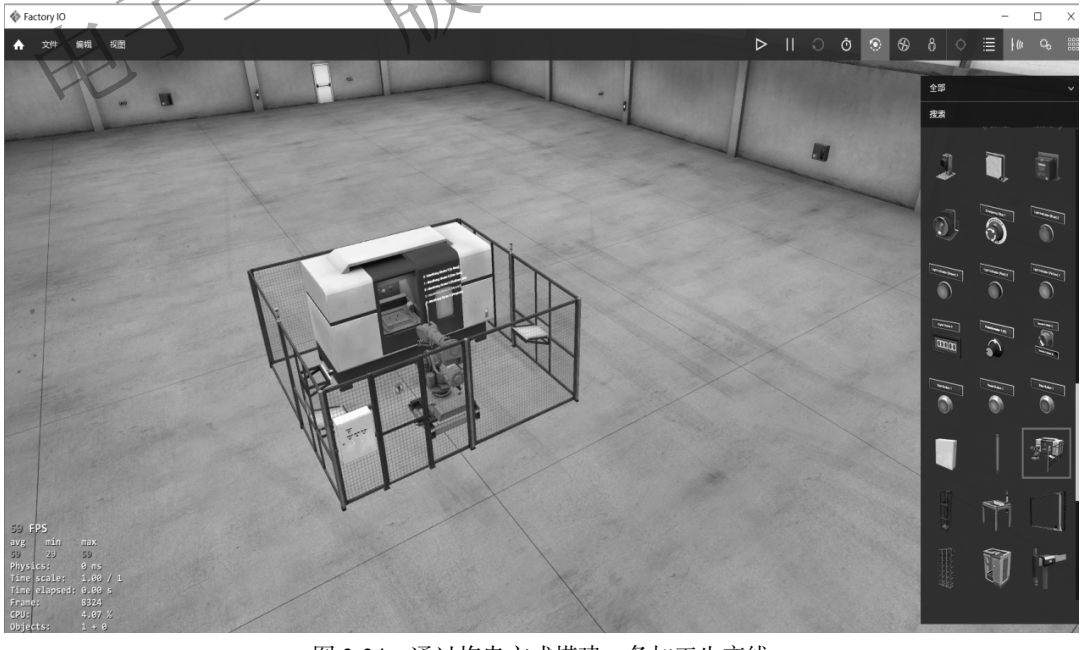


图 3-34　通过拖曳方式搭建一条加工生产线

（3）利用快捷键对工厂组件进行微调，如图 3-35 所示。

电子工业出版社有限公司 版权所有



图 3-35　利用快捷键微调工厂组件

（4）完成数字化工厂搭建，如图 3-36 所示。

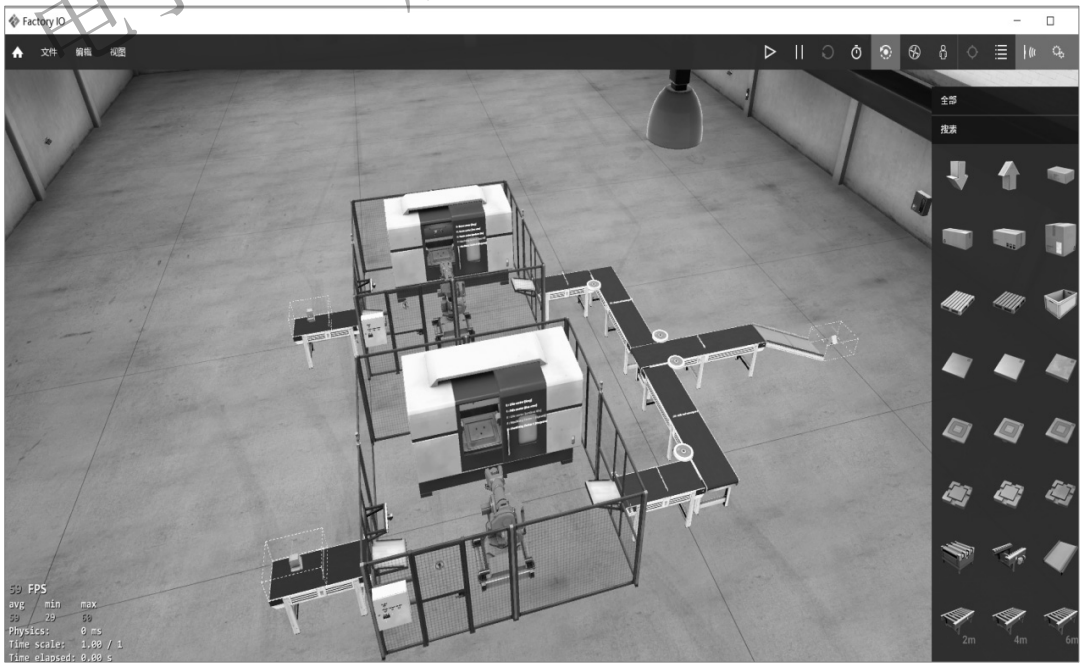


图 3-36　完成数字化工厂搭建

电子工业出版社有限公司 版权所有

（5）选择关键控制节点，手动完成生产线的调试，如图 3-37 所示。



图 3-37　手动完成生产线的调试

（6）完成上述数字化工厂搭建，并完成实验报告。

3．实验总结

数字化工厂（Digital Factory）是指利用数字技术和先进的信息通信技术（ICT）来实现工业生产高度自动化和智能化运行的生产模式。在数字化工厂中，物理系统、设备和流程与计算机系统、软件和互联网等相互连接，实现生产过程的数字化、可视化和实时化。

数字化工厂的目标是提高生产效率、质量和灵活性，优化资源利用率，实现可持续发展。以下是数字化工厂的一些关键特点和应用。

（1）自动化和机器人技术：数字化工厂重点应用自动化生产线和机器人技术，实现生产过程的高度自动化和智能化。

（2）物联网和传感器技术：通过在设备和物品上安装传感器，将各种设备和系统连接起来，实现实时数据采集和互联互通。

（3）数据分析和人工智能：利用大数据分析和人工智能技术，对生产过程中的数据进行实时监测和分析，以提高生产效率和质量。

（4）虚拟仿真和数字化：通过虚拟仿真技术建立数字化的工厂模型，以便优化生产过程。

（5）供应链和物流管理：数字化工厂通过实时追踪、优化物流与供应链流程，提升物料流转和信息传递的效率和准确性。

（6）员工培训和协作工具：数字化工厂为员工提供培训和协作工具，以提升员工的技能水平和工作效率。

数字化工厂的优势包括生产效率提高、生产成本降低、质量提升、生产过程可追溯等。然而，数字化工厂的实施也面临一些挑战，如数据安全和隐私保护、设备和系统互操作性、技术更新和管理变革等。

随着信息技术的快速发展，数字化工厂已经成为制造业发展的重要趋势，许多企业和组织正在积极推动数字化转型，以应对市场竞争和技术变革。

电子工业出版社有限公司 版权所有

习　题

一、选择题

1. 1999 年，（　　）Auto-ID 中心率先提出建立在物品编码、射频识别技术和互联网基础上的物联网概念。

A. 美国　　B. 中国　　C. 德国　　D. 日本

2. RFID 的全称是（　　）。

A. 射频识别　　B. 生物计量识别

C. 语音识别　　D. 光符号识别

3. 工业互联网的基础技术，包括（　　）、网络通信技术、云计算技术、工业控制技术、工业大数据技术、建模仿真技术及信息安全技术。

A. 脑机接口技术　　B. 虚拟现实技术

C. 局域网技术　　D. 物联网技术

4. 移动互联网结合了移动通信设备和（　　）的优势，是两者相互融合所产生的通信网络。

A. 局域网　　B. 广域网　　C. 互联网　　D. 城域网

5. RSS 又称（　　），是一种应用于信息服务站点的简单 XML 技术。

A. 离散发布　　B. 网络爬虫

C. 可扩展标记语言　　D. 聚合内容

6. P2P 技术中每台计算机扮演（　　）角色。

A. 客户机　　B. 服务器

C. 既是客户端，又是服务器　　D. 不确定

7. 天地一体化网络包括技术体制和（　　）两大层面。

A. 天基骨干网　　B. 多层面安全防护

C. 用户终端网　　D. 网络系统设施

8.（　　）是一种充分使用网络边缘端的网络、存储、计算等资源来对边缘数据进行感知、分析、处理，进而就近为用户提供实时服务的新型计算模式，可作为云计算的有效补充，与云计算协同工作，共同为用户提供性能更优的服务。

A. 边缘计算技术　　B. 网格计算

C. 星群　　D. GPGPU 技术

9. 2006 年，（　　）首次正式提出了“云计算”概念。

A. 谷歌　　B. 百度　　C. IBM　　D. 微软

10. 目前，较为公认的云计算服务模式主要包括软件即服务、平台即服务及基础设施即服务三种。其中软件即服务的缩写是（　　）。

A. SaaS　　B. PaaS　　C. IaaS　　D. AaaS

11. 虚拟化云服务运行技术主要解决云计算服务在应用运行中的高效性、可靠性问题。（　　）是目前实现云服务高效化的主流技术手段。

A. HDFS　　B. MapReduce　　C. HBase　　D. Spark

12. 工业互联网环境下的（　　）是数据采集的新技术手段，已成为智能时代工业控制过

电子工业出版社有限公司 版权所有

程中数据采集的核心技术，是基于工业互联网的新型工业控制系统发展的关键技术。

A. 数据智能感知采集技术　　B. 机器学习

C. 神经网络　　D. 智能化判断推理

13. 在数据智能感知采集技术中，DCS 表示（　　）。

A. 集散控制系统　　B. 数据传输系统

C. 资料控制站　　D. 设计检验规范

14. 现场总线控制系统（　　）是由 DCS 和 PLC 发展而来的控制系统技术，其核心技术是现场总线技术。

A. FCS　　B. BCS　　C. CCS　　D. CS

15.（　　）将成为工业互联网获得真正意义上企业应用价值的制胜关键，也是“两化深度融合”“互联网 +”“工业互联网”等国家战略在企业落地和产业转型升级中的落脚点。

A. 工业大数据　　B. 智能化　　C. 互联网化　　D. 智慧制造

16. 从企业生产和运营的角度看，工业大数据按照不同环节、不同用途可分为三类：第一类是业务数据，第二类是生产数据，第三类是（　　）。

A. 静态数据　　B. 动态数据

C. 实时数据　　D. 环境数据

17. 在各类应用需求的牵引及有关学科技术的推动下，现代建模仿真技术已经形成专业技术体系，包括建模技术、建模仿真支撑技术、（　　）等。

A. 虚拟样机建模仿真　　B. 数字孪生建模仿真

C. 工程建模仿真　　D. 共性应用技术

18. 计算机辅助设计的缩写是（　　）。

A. CAM　　B. CAD　　C. CAE　　D. CAX

19. 数字孪生技术是（　　）技术与物联网、大数据、人工智能等新一代信息技术的结合应用和创新发展。

A. 建模仿真　　B. 数学建模　　C. 机器学习　　D. 人工智能

20. 工业互联网背景下的信息安全，包括终端安全、网络安全、平台安全、数据安全、控制安全等诸多方面，采用的安全技术更加复杂，以下哪项不是信息安全技术？（　　）

A. 信息与数据防护技术　　B. 信息与数据加密技术

B. 网络隔离技术　　D. 区块链技术

21. 以下哪项是非对称性算法？（　　）

A. RSA 算法　　B. DES 加密算法

C. IDEA 加密算法　　D. LOKI 加密算法

22.（　　）的体制构造基于 Euler 定理，通过对大整数的分解（已知大整数的分解是 NP 问题）来保障信息的安全。

A. RSA 算法　　B. DES 加密算法

C. IDEA 加密算法　　D. LOKI 加密算法

23. 以下哪项不是 NIST 标准《零信任架构》白皮书中列举的技术解决方案？（　　）

A. 软件定义边界　　B. 令牌环

C. 增强的身份管理　　D. 微隔离技术

电子工业出版社有限公司 版权所有

二、判断题

1. 移动互联网被普遍认为是继计算机、互联网和移动通信后引领信息产业革命的新一次浪潮。（　　）

2. RSS 又称离散发布技术，是一种应用于信息服务站点的简单 XML 技术。（　　）

3. 计算机辅助设计的缩写是 CAD。（　　）

4. 当前，工业控制系统的数据采集、传输与处理基本上遵循了“数据采集—数据传输—数据分析与逻辑控制”的应用模式。（　　）

5. 现场总线控制系统（FCS）主要有五种类型：数字控制、存储分配控制、物料经营控制、批量过程控制、连续过程控制。（　　）

6. 谷歌的两步验证属于一次性口令。（　　）

7. DES 加密算法是非对称性算法。（　　）

8. P2P 技术中每台计算机分别扮演客户端角色。（　　）

9. 云计算技术采用“无共享”架构，各节点相互独立且资源可自我满足，因此系统内不存在资源争夺问题，可扩展性得到了保证。（　　）

三、填空题

1. 工业互联网的基础技术主要包括支撑工业互联网系统搭建与应用实施相关的各类技术，覆盖工业技术与互联网技术，基本可从_____、_____、_____三个维度进行划分。

2. 5G 关键技术主要包括_____、_____、_____。

3. 天地一体化网络包括_____和_____两大层面。

4. 新型传感技术主要有_____、_____和_____等类别。

5. _____最早的概念模型由当时的 PLM 顾问 Michael Grieves 博士于 2002 年在美国生产工程管理协会论坛上提出。

6. 现场总线控制系统（FCS）是由_____和_____发展而来的控制系统技术，其核心技术是_____。

7. 目前，较为公认的云计算服务模式主要包括_____、_____及_____三种。

8. 一个完整的通信网络主要包括_____和_____。

四、简答题

1. 什么是物联网？
2. 物联网的关键技术包含哪些？
3. 射频识别技术主要有哪些种类？
4. 什么是无线传感器网络？
5. 什么是网络通信技术？
6. 移动互联网的特点是什么？
7. 移动互联网的关键技术主要包含哪些？
8. 什么是应用服务平台技术？其主要包含哪些方面？
9. 什么是 5G 技术？其有什么特点？
10. 网络安全控制技术主要有哪些？

电子工业出版社有限公司 版权所有

11. 什么是天地一体化网络？其有什么特点及包含哪些关键技术？
12. 什么是通信网络？
13. 什么是高性能计算技术？其体系结构主要包括哪些？
14. 什么是云计算技术？其有什么特点？
15. 简要说明云计算技术体系。
16. 新型工业控制系统主要包括哪几部分？
17. 数据智能感知采集技术是什么？其主要包括哪些内容？
18. FCS 主要有五种类型，它们分别是什么？谈谈它们的应用。
19. 边缘处理的关键技术有哪些？
20. 工业大数据的主要来源有哪些方面？
21. 工业大数据的关键技术有哪些？
22. 我国工业数据具有一定的规模优势，但在数据质量和管理上与发达国家相比存在较大的差距，主要原因是什么？
23. 当前建模仿真技术在工业领域可以归类为三种典型应用形态，它们分别是什么？
24. 什么是虚拟样机？
25. 什么是数字孪生？其关键技术有哪些？
26. 工业互联网背景下的信息安全技术有哪些？
27. 什么是信息伪装？
28. 什么是防火墙？
29. 网络隔离技术有哪些？
30. 工业控制系统安全技术有哪些？
31. 什么是零信任安全？其基础架构是什么？

电子工业出版社有限公司
版权所有