工业互联网园区网络白皮书

工业互联网产业联盟（AII）

2020 年 4 月

工业互联网产业联盟

Alliance of Industrial Internet

声　　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

工业互联网产业联盟

Alliance of Industrial Internet

前　言

工业园区作为工业企业集聚区，为工业企业提供了大量基础设施和公共服务。随着工业互联网的发展，传统工业园区的转型已成为未来发展的必然方向。目前我国工业互联网网络体系正在全方位推进中，工业园区网络作为企业外网和企业内网之间的纽带，是工业互联网的重要基础设施，是工业互联网网络的重要组成部分。随着工业互联网业务需求的日益丰富，园区网络的能力提升成为推进工业互联网网络化改造与应用中的关键环节。

在此形势下，工业互联网产业联盟（以下简称“联盟/AII”）组织多家企业联合撰写了《工业互联网园区网络白皮书》。本白皮书从园区网络发展现状入手，探讨了工业互联网新形势下园区网络内涵、架构、业务场景需求、创新技术与应用等，引导工业互联网园区网络建设，帮助构建、运维新型的工业互联网园区网络。

本白皮书编写过程中得到了联盟成员及国内外众多企业的大力支持。经过多次深入调研和探讨，为白皮书观点的形成与编写提供了有力支撑。后续我们将根据业界的实践情况和反馈意见，在持续深入研究的基础上适时修订和发布新版白皮书。

组织单位：工业互联网产业联盟

编写单位（排名不分先后）：中国信息通信研究院、华为技术有限公司、中国泰尔实验室、新华三技术有限公司、中国电信集团有限公司、山西云时代技术有限公司、中电工业互联网有限公司、华核（北京）科技有限公司、北京邮电大学、网络通信与安全紫金山实验室

编写组成员（排名不分先后）：

中国信息通信研究院：陈洁、朱瑾瑜、张恒升、曹蓟光、刘泰、徐越

华为技术有限公司：李兴、刘文斌、沈宁国、邓海洋

新华三技术有限公司：郭晓军、刘淑英、宋玉兵、柳晴

中国电信集团有限公司：孙慧、金嘉亮、孙丽楠、李成、文常强

山西云时代技术有限公司：梁永、杨少封、魏鹏、谷哲

中电工业互联网有限公司：胡单、彭东、张伟

华核（北京）科技有限公司：黄金

北京邮电大学：朱海龙

网络通信与安全紫金山实验室：何斌

目 录

1 工业互联网园区网络概述

1.1 工业园区发展现状

工业园区作为推进我国改革开放和经济发展的重要载体，一直被视为经济建设的主战场。近年来，随着我国工业化进程推进及传统产业转型升级，工业园区的建设和发展取得了显著成效，工业园区在数量和规模呈现出双增长。目前全国各地已有近五百个国家级的经开区、出口加工区、保税区等，省级各类开发区超一千个，全国各类工业园区超两万个。

我国工业园区发展总体经历了三个阶段：1979 年-1990 年为工业园区的创建试点期；1991 年-2000 年为工业园区的高速增长期；2001 年到现今为工业园区的稳定和优化期。工业园区的发展模式也由简单要素集群向产业主导发展，工业园区的功能更加复合，与城市的发展关系也愈发紧密。

2017 年 11 月，国务院印发了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，指出构建区域协同发展体系，推动工业互联网产业示范基地建设。《工业互联网发展行动计划（2018-2020 年）》中也将支持和建设一批工业互联网产业示范基地作为近期重点任务之一。工业互联网园区作为工业互联网产业生态中的一个重要环节受到各界的高度重视，目前已形成杭州工业互联网产业园、中关村工业互联网产业园、湖北工业互联网示范园、东土科技（宜昌）工业互联网产业园等工业互联网特色园区，成为区域进一步开放创新、经济增长、产业合作转移的有利支撑。

1.2 工业园区网络发展现状

随着互联网+时代的到来，互联网与社会经济深度融合，一方面催生出新应用、新服务、新业态，改变了人们的生产方式、生活方式，另一方面推动了经济的转型升级和高质量发展。在这种趋势下，传统工业园区的发展方向、发展模式、建设方式等均面临着新挑战和新需求。工业园区应紧密围绕企业快速发展需求，利用新一代信息技术，快速提升自身服务水平和质量，实现转型发展，获取信息化环境下的核心竞争能力。网络作为工业园区最重要的基础设施之一，通过融合新一代信息与通信技术，具备迅捷信息采集、高速信息传输、高度集中计算、智能事务处理和无所不在的服务提供能力，可以实现园区内及时、互动、整合的信息感知、传递和处理，可以显著提高园区产业集聚能力、企业经济竞争力、园区可持续发展能力。

但就目前工业园区基础设施建设情况来看，大多数工业园区仍聚焦于交通运输、供水、供电、排污等市政基础设施，园区信息化建设起步晚、时间短，信息化配套设施及服务还不够完善。目前工业园区网络存在的问题可以归纳为以下几点：

1、工业园区网络架构无法满足工业互联网新业务需求。

工业互联网业务的发展对园区网络基础设施提出了更高的要求和需求。传统层级化的网络架构影响了信息交互的效率。现阶段园区网络的每个层面承担不同的网络功能，都需要用户来进行接入和控制。随着园区内企业规模的不断扩大、用户数目增多，导致网络规模和网络功能上不断激增，网络部署和管

理会变得复杂。

2、工业园区网络宽带性价比低，不足以支撑工业互联网推广应用。

海量数据对容量和带宽提出更高的要求，工业互联网须建立在连续采样、大体量的工业大数据基础上，而海量数据的传输和存储，对网络的带宽、稳定性和覆盖率提出更高的要求。多数工业园区的网络基础以满足办公、生产相关的软件应用为主，传输速率、覆盖率、稳定性不足以支撑工业互联网应用。其次工业专线宽带价格偏高，工业网络在设备、安装、使用、入场等费用上都有差别，相同带宽的商用产品收费较高，存在较大的价格调整空间。另外工业宽带的发展环境还不成熟，对网络的要求迫切性没有体现，需求没有完全释放，国家对工业领域的宽带支持政策尚有欠缺。

3、工业互联网网络标准不统一，产品集成难以实现。

工业互联网要实现企业、机器、产品、用户之间全流程、全方位、实时的互联互通，达到研发、生产、管理、服务的高度协同，对标准化提出了新要求，需要制定统一的技术标准、服务标准、管理标准和安全标准。工业园区网络异构性普遍存在，网络接口不同，统一的工业互联网标准尚未形成，严重制约着产品、服务的集成。另外，由于缺乏大量工业互联网成功应用案例的示范引领，使很多企业难以下定决心改变现在的生产和经营模式。

4、综合网络化系统集成企业缺乏，不能满足工业互联网发展需求。

工业互联网将无处不在的传感器、嵌入式终端系统、智能控制系统、通信设施连接成一个智能网络，使人与人、人与机器、机器与机器、服务与服务之间能够互联，最终支撑智能化生产、网络化协同、个性化定制和服务化延伸等工业互联网新模式新业务的实施，这对系统集成企业提出了更高的要求。目前，系统集成企业主要分布于各个细分行业，从事分领域的系统集成业务，能提供综合网络化系统集成服务的集成商较少，难以满足工业互联网的发展需求。

5、缺乏工业控制系统的网络安全保障体系。

工业控制系统的安全防护措施普遍不足，利用工业控制系统的漏洞感染数据采集与监控系统，从而导致工业设备停止运转、数据丢失等安全事件时有发生，工业控制系统存在的安全隐患不容小觑。

1.3 工业互联网园区网络内涵

工业互联网园区是以高质量发展为目标，按照工业互联网内涵要求，规划、建设、运营、提升的新型园区。园区应以供给侧结构性改革为主线，以协同创新、集群集约、智能融合、绿色安全为导向，通过网络、平台、安全三大体系和新模式、新业态的构建，来指导新园区建设和已有园区的转型发展。

工业互联网园区网络是指在工业互联网园区内部部署的以实现园区企业设备互联和信息互通的网络基础设施，由园区到厂区、由管理到生产的综合性基础网络体系。工业互联网园区网络主要由工业生产网、企业信息网、园区公共服务网以及云

基础设施组成。其中：

- 工业生产网是指部署在园区各企业内部的，用以实现生产现场各类生产设备、传感器、执行器、工控机等互联，以及工业数据采集、工业操控与维护的网络；
- 企业信息网是指部署在园区各企业内部的办公区域内，用以实现部门互通的网络；
- 园区公共服务网是实现园区内工业企业间互联互通并向园区内各企业提供基础公共服务的网络；
- 云基础设施作为工业互联网园区内部信息汇聚的重要基础设施，实现园区内多家企业私有云和公有云的承载。

1.4 工业互联网园区网络利益相关方

工业互联网园区网络建设的核心是建设低延时、高可靠、广覆盖的工业互联网网络基础设施，集合网络、软件、物联网技术和服务，实现数据在工业各个环节的无缝传递，支撑形成实时感知、协同交互、智能反馈的生产模式，提升园区产业服务水平，提高服务的明确性、高效性、灵活性，建立自主创新的网络服务体系。

工业互联网园区网络利益相关方包括四种角色，分别是建设方、运营方、维护方、使用方。

- 建设方是指执行工业互联网园区建设计划，组织、督促基本建设工作，支配、使用基本建设投资的基层单位。一般表现为：行政上有独立的组织形式，经济上实行独立核算，编有独立的总体设计和基本建设计划，是基本

建设法律关系的主体。

- 运营方是整个园区的内部专门设置的对园区网络各项事宜进行统一管理的单位。
- 维护方是指负责园区网络基础设施日常维护。
- 使用方一般是指入驻园区的各工业企业，他们从运营方租用网络等资源。

2 工业互联网园区网络需求

工业互联网园区网络的运营模式对园区网络的复杂程度和网络技术选型会产生影响。因此原则上可依据是否存在“租用”的情况，将园区网络分为私有园区网络和公有园区网络。此外物理形式上分离，但存在统一管理、统一业务需求的虚拟化园区也增加了园区网络的复杂程度。

2.1 私有园区网络

（1）场景描述

通常来说，单个企业的企业园区或者以某个企业为核心，聚集少量配套企业的工业园区可以归属为私有园区。私有园区网络的使用者只有一个企业，因此私有园区网络的建设方、运维方和使用方通常是合一的。使用方会针对自己的核心业务特点去设计、建设符合业务需求的完整网络。

私有园区网络是一个业务驱动的网络，使用方会针对企业的业务特点自底而上的设计网络，即针对不同的业务分别进行需求分析，网络规划和设计，然后再叠加多张网络，进行融合设计，最终形成一张完整的网络。

（2）需求描述和主要功能

企业典型的业务网络（图 1）可分为生产网、办公网、视频会议网、安防网、互联区、租赁网等。

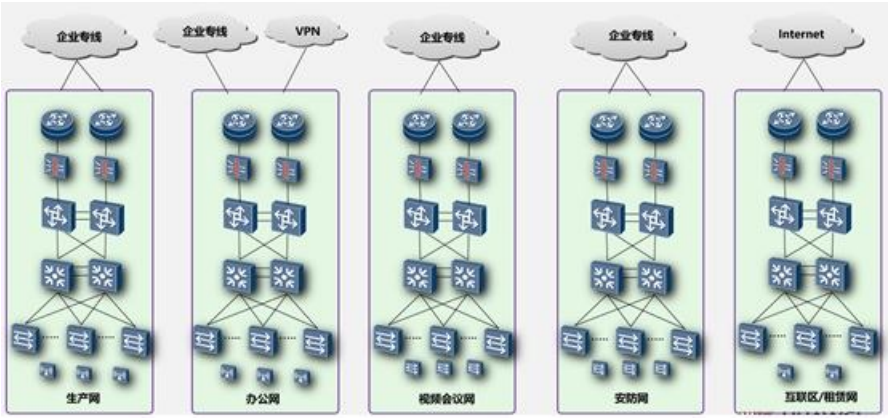


图 1 企业典型业务网络

(a) 生产网：生产网络通常指承载企业核心生产经营活动的网络。对于不同类型的企业，由于生产经营活动的不同，生产网络特别是前端网络，差异非常大。但是，生产网络依然有其共性。主要包括:

- 高性能：这里的高性能用来特指性能和特性能够满足前端网络的要求。例如：低时延、高带宽、无丢包、抗恶劣环境等。
- 可靠性：生产网络是不允许中断的，必须保证 7*24 小时的可靠性。因此，生产网络通常采用严格的冗余以实现高可靠。冗余包括但不限于电源冗余，位置冗余，链路冗余，设备冗余，AB 平面备份等各种冗余技术。
- 安全性：为了保证绝对的安全性，生产网络通常要求和其它网络隔离。根据重要性的不同，可能是绝对的物理隔离，也可能是逻辑隔离，严格受限访问。

(b) 办公网：指企业用于日常办公的网络，通常运行企业的邮件系统、OA、ERP、PLM、CRM 等信息系统。

- 性能和服务质量保证：办公网要能保证网络上各种业务

的服务质量，避免因为带宽、无线网络不稳定等问题导致应用缓慢，避免因为服务质量保证能力不足影响业务实施;

- 可靠性：办公网对可靠性有较高的要求，通常会采用链路冗余、设备冗余等技术提升可靠性;
- 用户接入控制和账号管理：应增加用户接入控制和账号管理功能，以解决接入安全性问题。;
- 网络虚拟化：办公网能够提供网络虚拟化功能，实现部门间网络隔离及承载多种业务。

(c) 视频会议网：为视频会议系统服务的承载网络。由于视频会议对网络的服务质量有特别的要求，并且视频会议系统的位置固定，数量有限。传统上，我们会构建视频会议专网来保证视频服务质量。随着及时通信系统的发展，个人级的视频会议服务开始普及，同时，办公网络的带宽和质量有很大的提升，部分企业开始使用虚拟化的视频会议网进行服务。

(d) 安防网：用于提供企业环境安全服务的网络。安防网业务流通常包括视频监控、楼宇自控、门禁控制和电梯控制，主要访问流向指向监控中心和服务存储区，监控视频流量对时延和带宽较为敏感，要求设备支持高可靠性和高带宽，接入交换机保证低时延、双交流电源高可靠设计。

(e) 互联区：互联区主要用于同一个企业的不同园区网络之间的互联，以及和其他企业的互联。互联区的拓扑较简单，但对管理系统要求较高。由于涉及到广域互联，链路的使用率和效率尤为重要，需要部署合适的设备，监控和管理互联网络上

的流量和业务，进行精细调整，以提高链路利用率，降低运营成本。

(f)租赁网：指向关联企业提供基础的网络服务，同时提供严格受控的公司内部网络访问权限。关联企业通过租赁网接入企业内部网络，和企业的相关自动化系统实现对接，从而实现端到端的自动化。

（3）管理

私有园区网络由单一管理者进行管理，通常是企业的 IT 管理团队。IT 管理团队根据企业业务特点规划和设计网络，并自行进行管理维护。园区网络的管理功能也是网络的重要功能组件，需要进行合理规划，并部署相应的软硬件。由于园区网络的使用者包括生产部门、行政部门、企业员工及外部相关企业员工，制定网络使用的各项规章制度成为重要管理手段之一。通过规章制度约束使用者的行为，从而简化管理。

（4）环境

不同于普通的网络，园区内部的环境多变，既有一般的生产办公区域，也有需要考虑防水宽温的室外区域，更有环境多变的生产区域。选择设备时，要充分不同环境的要求:

- 办公区域：可以选择普通的室内款型。但是，室内的电磁环境相对复杂，需要关注各种无线信号，包括 Wi-Fi 信号间的相互干扰。必要时，需要选择内置带通滤波器的款型，以提高对干扰的抑制能力;
- 室外区域：环境相对复杂，对设备的防水、宽温等有较高要求。一般来说，各种网络设备都有室外型号，或者

有支持室外安装的室外柜组件，可以合理使用；

- 生产区域：生产区域环境复杂，并且各行业有自己的环境和安全规范。例如：很多行业有本安的要求。采购设备时，需要选择符合相应要求的，通过相关认证的设备。

（5）可靠性

园区网络高可靠和高可用是整个园区健康运行的重要条件之一，所以对网络整体架构的高可用性和高可靠性部署需考虑全面。网络架构必须能够达到园区对服务级别的要求，并且通过多层次的冗余容错考虑，使得整个网络架构能够满足业务系统不间断稳定运行的需求，同时实现网络层面的负载分担和灾难恢复。

（6）扩展性和兼容性

在园区网络建设中，从可扩展性角度出发，采用业务功能模块化和网络拓扑层次化的部署方式，使得网络架构在功能、容量、覆盖能力等各方面具有易于扩展的能力，以适应快速发展的业务对网络基础架构的要求。从兼容性的角度出发，园区网建设在技术上采用开放式的构架和协议，消除未来扩容时的设备局限性。

（7）安全

从整体园区网层面，要实现有线和无线层面的接入安全，构建能够具备安全接入能力的基础网络平台，以满足未来统一接入安全需求。同时在园区网核心层、汇聚层和接入层完全物理隔离，从而最大可能保证两网互访的安全性。

（8）投资保护

园区网络架构设计必须满足未来 3-5 年的使用需求，提高整网的利用率和扩展能力，使得可能的后续投资最小化。同时结合运维等方面的要求，获得最佳总体拥有成本。

2.2 公有园区网络

（1）场景描述

公有园区网络的使用者有多个企业，即存在多个使用方，但通常会有一个运维方负责运维整个网络，运维方负责设计网络，满足园区的基础服务需求以及园区各企业的通用性需求。使用方从运维方租用网络以部署企业的各种服务，满足企业需求。

因此，公有园区网络的构建重点是:

- 统一提供园区基础的服务，从而降低各企业运维的成本。运营方需要构建多网融合的基础网络，服务于各种基本服务。例如：安防网，能耗管理网等。
- 提供统一的公共服务网，供园区企业租用，降低企业基本服务的开销。例如：视频会议网络;
- 提供统一的公共 Internet 服务，供园区内部人员使用。例如：覆盖住宿区的宽带接入；覆盖公共区域的无线接入。运营方需要建设强大的用户管理系统，以简化用户管理复杂度;
- 提供支持多租户的基础网络和管理系统，向企业提供核心网络连接服务，并支持企业进行定制化改造。

（2）需求描述和主要功能

需要建设完整的园区网络，提供园区网络基础服务。由于存在着多租户场景，因此网络和业务的管理都被复杂化了。运营方要能够快速理解最终用户的需要，并且进行快速响应。在安全，扩展性等方面与私有园区需求大致相同。但公有园区本质上看是连接园区内各个企业的骨干网，在可靠性上有更高的要求。

网络架构必须能够达到园区对服务级别的要求，并且通过多层次的冗余容错考虑，使得整个网络架构能够满足业务系统不间断稳定运行的需求，同时实现网络层面的负载分担和灾难恢复。

2.3 虚拟化园区网络

通常情况下园区网络是物理上相互连续的网络。但在实际的应用中，存在着一些物理上分离，但需要统一管理、统一业务的需求。随着虚拟化技术的发展，特别是 2over3 技术的发展，可以将多个园区虚拟化成一个园区。虚拟化园区网络又可以被细分为本地多园区虚拟化网络和远程多园区虚拟化网络。

（一）本地多园区虚拟化网络

本地多园区虚拟化网络指的是将两个或者多个物理上距离不远的园区网络，通过虚拟化技术虚拟成一个完整的工业园区网络。

（1）场景分析

同一个工业园区因为土地的限制，有可能被分为地理上有一定距离的多个区域。传统上，需要为每个区域单独构建园区

网络分别管理，并通过 Internet 互通。但在实际使用中，会存在以下问题：

- 管理复杂度。网络管理、维护部门需要面对两张网络，两套网络管理系统。网络中的配置、管理等需要人工同步，复杂且错误概率高。
- 业务连续性需求难以满足。例如：实验室的需要二层连接；接入希望在两张网络获得一致的体验。
- 强行二层互联，则会导致网络的效率、可靠性等极大下降。

（2）组网方案

我们可以采用网络级多虚一的技术，采用专门的二层连接将多个园区直接相连，使用统一的控制器部署业务。组网拓扑如图 2 所示。

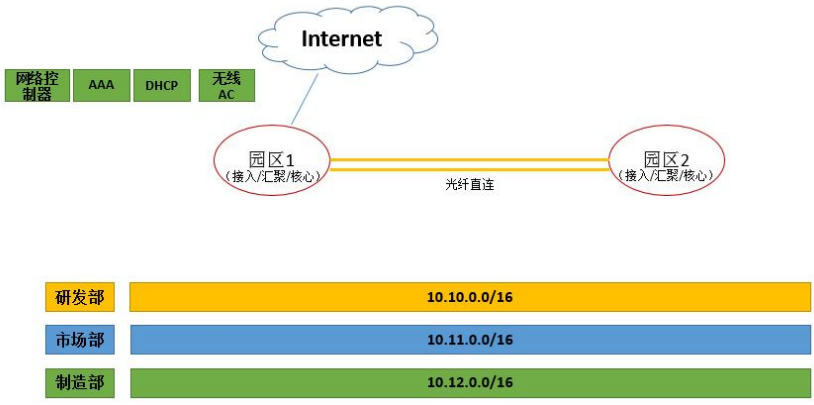


图 2 本地多园区虚拟化网络组网拓扑

本地多园区虚拟化网络建设需要考虑以下几点：

- 架构层面，需要统一管理/统一策略。园区间互联多使用光纤直连，可构建虚拟化的跨园区打通的 overlay 网络，地址可以跨园区统一规划，网络策略可以跨园区统

一规划，并实现网随人动。

- 可以跨园区构建端到端的虚拟 VPN 专网，实现一网多业务承载。
- 网络控制器及业务组件应集中部署于主园区，一套管理人员，一套管理系统，降低人力成本和复杂度。
- Internet 出口一般集中在主园区统一出口，安全策略集中部署，主/副园区共享一致的出口策略。
- 可靠性方面，所有管控组件可采取双机或者多机热备方式部署。对于可靠性要求高的企业，可以进一步将 AAA 和无线 AC 控制器下沉各个园区，实现园区内本地业务处理，在园区间线路中断的情况下提供业务连续性。网络架构本身可采用双机堆叠，ECMP 等冗余机制实现园区内部的高可靠性。

（二）远程多园区虚拟化网络

远程多园区虚拟化网络指多个物理上距离较远的园区独立运行，但通过虚拟化技术实现二三层互通，业务层面上实现虚拟化的网络。

（1）场景分析

对于大型企业来说，往往会存在多个园区，包括办公园区，生产园区以及派出机构等。不同的园区可能地理上间隔很远，甚至分布在不同的国家。传统上，这些局域网络之间互不关联，各自独立管理和运行。如果需要互通，则通过向第三方租用的 VPN（通常为 BGP MPLS VPN）实现三层互通。如果采用网络多虚一的方式进行管理，则会存在以下的问题:

- 由于大型网络的管理需要本地化，因此，对于多张网络，采用统一网络、统一管理的方式进行网络虚拟化并不适用。否则，会涉及到大量的管理团队之间的沟通和协调。
- 多虚一的方式会导致管理组件集中部署，在广域链路发生故障时，业务连续性会受较大的影响。

（2）组网方案

我们可以采用虚拟网络互联+控制器协同的方式，建议组网拓扑如图 3 所示。

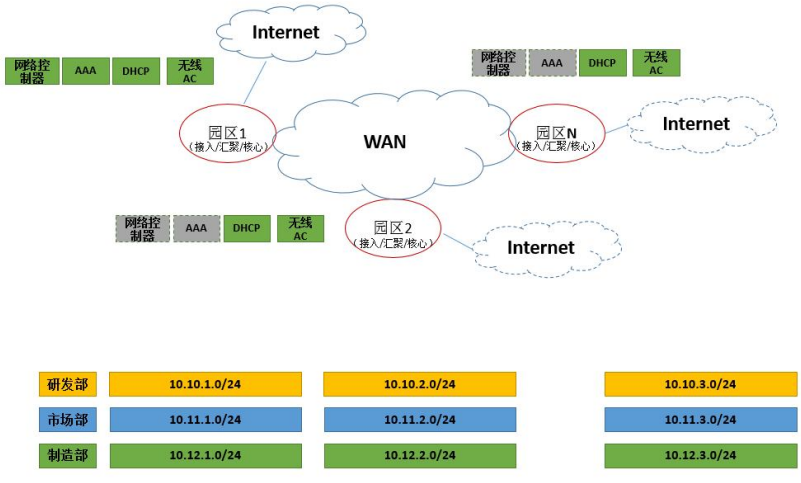


图 3 远程多园区虚拟化网络组网拓扑

远程多园区虚拟化网络建设需要考虑的几个点：

1）管理上统分结合，提供简便性和可靠性：

- 用户组，网络策略，VPN 全网统一规划和拉通
- 地址规划各园区独立进行，园区间三层路由互通
- 无线 AC 组件下沉各自园区
- internet 多出口
- 网络控制器分级分权：总部控制器负责规划网络业务公共/统一的部分，并下发给所有分控制器，分控制器

在各个园区本地管控各自的网络组件，可以免受 WAN 网故障的影响

- AAA 组件分级分权：AAA 组件是最常使用的部件，也需要在总部和各分部分别部署，免受 WAN 网故障的影响。总部 AAA 定义统一的接入策略和接入场景，同步给所有其他园区的 AAA，各园区的 AAA 本地执行
- 各路由节点的路由按需下发，节约资源，提供扩展性

2）园区和 WAN 网的协同

- WAN 网若是自营可控的，则可以通过控制器实现园区和 WAN 网的一体化管理，园区关注业务快速转发，策略控制，WAN 网强调最优调度，通过在控制器上一体化编排简化使用体验
- 若 WAN 是租用线路，不可控，只提供 IP 透明传输，则多关注其承载能力指标，比如 MTU，时延，带宽等指标。园区出口需要使用合适的多出口选路策略与 WAN 网做对接和匹配

3 工业互联网园区网络架构

3.1 园区网络组网架构

工业互联网园区网络主要由工业生产网络、企业信息网络、园区公共服务网络以及云基础设施组成。其架构示意图见图 4 所示。

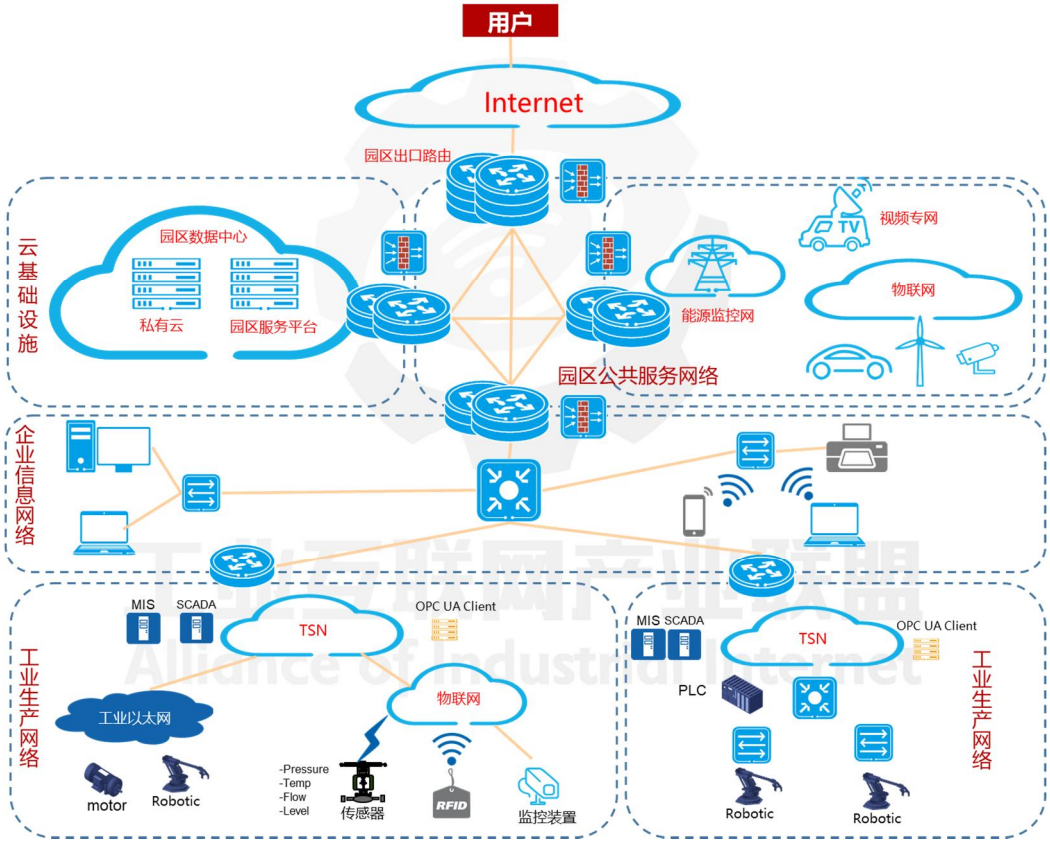


图 4 工业互联网园区网络架构示意

3.1.1 工业生产网络

（1）概述

工业生产网络主要连接工厂内部的各种要素，包括人员（如生产人员、设计人员、外部人员）、机器（如生产装备）、材料（如原材料、过程件、制成品）、环境（如仪表、监测设备）等。

工业生产网络一般使用现场总线、工业以太网、工业无线等通信方式，通过PLC、RTU、DCS、工业边缘网关等设备采集、控制、监测生产过程。各个生厂区之间通过隔离网闸，对工厂内区域分别进行保护。HMI（人机交互接口）、SCADA（数据采集与监视控制）等生产应用通过工业以太网、工业无线等对工厂整体进行监控和管理。外部网络访问需经过工业防火墙控制、过滤，并由审计网关对访问操作进行记录和安全审计回溯。

工业生产网络是工业系统互联和工业数据传输交换的支撑基础，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。

（2）功能和性能

工业生产网络架构、技术多样，需要合理考虑布置成本、使用场景要求，在生产现场布设工业有线通信和工业无线通信相结合互补的网络，满足生产控制管理和工业应用的需求。

工业有线主要适合带宽、可靠性、实时性要求高且位置相对固定的设备接入。工业有线主要分为现场总线与工业以太网。现场总线协议有几十种，主流协议有 Modbus、Profibus、IO-link、CAN/CANopen、CC-Link，主要用于 PLC 南向的简单数据量和模拟量接入，传输距离一般较短，数据传输速率较低，抗干扰能力、安全性相对较差。工业以太网协议数量众多，主流协议有 DeviceNet、Profinet、EtherCAT、EtherNet/IP、

Modbus-TCP，多用于 PLC 北向输出，通信速率高、网络拓扑灵活，存在协议间互联互通性较差等问题，难以进行灵活部署与快速扩展。

工业无线适合广覆盖、移动性强的场景，以可靠性、带宽要求不高的传感器网络、移动机器人等应用为代表，适合灵活的工业应用布置。其中 Wi-Fi 技术具有部署容易、组网灵活和可移动等优势，但可靠性和安全性难以足工业级需求。LoRa 技术，适用于低速率、低功耗的中长距离场景。ZigBee、ISA 100.11a、Wireless Hart、WIA FA/PA 等技术受限于传输距离或者传输速率，多用在传感器、仪表等传输距离有限、传输速率不高的使用场景。RFID、UWB 等技术多用于定位应用。基于公共蜂窝网络的 NB-IoT 等技术，具有广域覆盖、可靠性保障、QoS 等优点，适用于低速率、低功耗的传感设备接入。

因此，为适应智能制造发展，工厂内部网络需要进行扁平化、IP 化、无线化及灵活组网等各方面的改进。

1）工厂内网络扁平化。扁平化包括两个方面，一是工厂 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。

2）工厂内网络以太网/IP 化趋势。随着工业互联网技术的发展演进，现场总线正在逐步被工业以太网替代。未来，工业内有线将被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。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使用。

3）工厂内无线网络成为有线网络的重要补充。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场景，Wi-Fi、Zigbee、2G/3G/LTE、面向工业过程自动化的无线网络 WIA-PA、WirelessHart 以及 ISA100.11a 等技术已在工厂内获得部分使用。同时无线技术正逐步向工业实时领域渗透，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。IEC 也正在制定工厂自动化无线网络 WIA-FA 技术标准。

4）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。智能机器可在不通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。

新型 IO-link 总线在传统模拟量采集的基础上，增加了数据传递功能，增加了传统气动阀门、传感器等的可维护性。以 OPC UA over TSN 为代表的标准化工业有线网络正在加速落地。同时，5G uRLLC、eMTC 将为工业低时延应用和大连接应用提供理想的无线接入方式。

（3）管理

工厂环境涉及多个运行区域，联网设备众多，一般使用基于 Netconf、YANG 模型，以及 SNMP 协议进行网络管理。通过自动化配置、拓扑分析等网管软件，实现整个工业网络的自动发

现与连接。

（4）环境

工业现场环境复杂，网络设备和线路设施等可能处于综合的电磁、物理、化学环境中，需要具备抗电磁干扰、防水防尘、耐极端温度、以及耐化学腐蚀等等能力。并且在不同的工厂、同一工厂的不同区域，环境都会有所不同。对于工业场景的环境描述，可参考 ISO/IEC 11801 系列标准对于工业场景通信布线系统定义的 MICE 环境条件体系。

表 1 ISO/IEC 11801 系列标准中 MICE 环境条件体系

环境条件分组和项目	环境条件等级		
机械作用（M）	M_1	M_2	M_3
冲击/碰撞	峰值加速度：40ms^{-2}	峰值加速度：100ms^{-2}	峰值加速度：250ms^{-2}
振动	幅度(2Hz to 环境 9Hz)：1.5mm 加速度(9Hz to 500Hz)：5ms^{-2}	幅度(2Hz to 9Hz)：7.0mm 加速度(9Hz to 500Hz)：20ms^{-2}	幅度(2Hz to 9Hz)：15.0mm 加速度(9Hz to 500Hz)：50ms^{-2}
拉伸	根据现场安装环境和具体产品规范确定	根据现场安装环境和具体产品规范确定	根据现场安装环境和具体产品规范确定
压扁	最小值：45N/25mm (平均分布)静电	最小值：1100N/150mm (平均分布)	最小值：2200N/150mm (平均分布)
撞击	1J	10J	30J
弯曲、曲挠和扭转	根据现场安装环境和具体产品规范确定	根据现场安装环境和具体产品规范确定	根据现场安装环境和具体产品规范确定
异物入侵	I_1	I_2	I_3
防尘	最大直径:12.5mm	最大直径:50μm	最大直径:50μm
防水	无要求	喷水流量：≤12.5L/min 喷嘴直径：≥6.3mm 距离：＞2.5m	喷水流量：≤12.5L/min 喷嘴直径：≥6.3mm 距离：＞2.5m 及浸水：≤1m，≤30min
环境和化学	C_1	C_2	C_3
环境温度	-10℃ ～ +60℃	-25℃ ～ +70℃	-40℃ ～ +70℃
温度变化速率	0.1℃/min	1.0℃/min	3.0℃/min
湿度	5% ～ 85%(不结露)	5% ～ 95%(结露)	5% ～ 95%(结露)
太阳辐射	700Wm^{-2}	1120Wm^{-2}	1120Wm^{-2}
液体污染物（浓度单位：10^{-6}）			
氯化钠(食盐/海水)	0	＜0.3	＜0.3
油(干燥空气下的浓度)(油的类型根据现场安装环境和产品规范确定)	0	＜0.005	＜0.5
硬脂酸钠(肥皂)	无要求	＞5×10^4 液体非凝胶	＞5×10^4 液体非凝胶
洗涤剂	无要求	待研究	待研究
导电材料	无要求	暂时接触	长期接触
气体污染物（均值/峰值，浓度单位：10^{-6}）			

硫化氢	＜0.003/＜0.01	＜0.05/＜0.5	＜10/＜50
二氧化硫	＜0.01/＜0.03	＜0.1/＜0.3	＜5/＜10
三氧化硫	＜0.01/＜0.03	＜0.1/＜0.3	＜5/＜10
氯（＞50% 环境湿度）	＜0.0005/＜0.001	＜0.005/＜0.03	＜0.05/＜0.3
氯（＜50% 环境湿度）	＜0.002/＜0.01	＜0.02/＜0.1	＜0.2/＜1.0
氯化氢	-/＜0.06	0.06/＜0.3	0.6/＜3.0
氟化氢	＜0.001/＜0.005	＜0.01/＜0.05	＜0.1/＜1.0
氨气	＜1/＜5	＜10/＜50	＜50/＜250
氮氧化物	＜0.05/＜0.1	＜0.5/＜1	＜5/＜10
臭氧	＜0.002/＜0.005	＜0.025/＜0.05	＜0.1/＜1
电磁	E_1	E_2	E_3
静电接触放电(0,667μC)	4kv	4kv	4kv
静电空气放电(0,132μC)	8kv	8kv	8kv
辐射抗扰度	3V/m(80～1000)MHz 3V/m(1400～2000)MHz 1V/m(2000～2700)MHz	3V/m(80～1000)MHz 3V/m(1400～2000)MHz 1V/m(2000～2700)MHz	10V/m(80～1000)MHz 3V/m(1400～2000)MHz 1V/m(2000～2700)MHz
射频场感应的传导抗扰度	3V@150kHz～800MHz	3V@150kHz～800MHz	10V@150kHz～800MHz
电快速瞬态脉冲群（共模）	500V	500V	1000V
浪涌(暂态接地电位差),线对地	500V	500V	1000V
工频磁场(50/60 Hz)	$1Am^{-1}$	$3Am^{-1}$	$30Am^{-1}$
工频磁场（60Hz～20000Hz）	待研究	待研究	待研究

（5）安全

随着更多的工业设备、工业应用使用网络，工厂间的流程互联互通，相应的安全性风险激增。特别是底层工业控制网络的安全考虑不充分，安全认证机制、访问控制手段的安全防护能力不足，攻击者一旦通过互联网通道进入底层工业控制网络，容易实现网络攻击。

工业生产网络系统需要在保证生产这一前提条件下，对整个工业网络进行隔离控制，保证工业网络与应用运行的安全可靠。各个生产区域内使用多冗余备份的控制设计，采用隔离网闸对网络进行隔离管理。工业生产网络安全一般通过对多种工业协议完整性、功能码、读写地址（读写权限）、工艺参数值的深度解析和过滤等方式，对异常数据、异常指令进行阻断和安全过滤的，同时，一般工业网络有多级的安全隔离设备，形成多层次的防护结构，最大程度的保障生产设备的平稳运行。

（6）可靠性

整个工厂网络的可靠性可以分为线路可靠、设备可靠和系统应用可靠。工业网络线路在满足环境适应性的要求上，在重要线路可采用多冗余的网络设计，使用线路备份、环形网络拓扑等方式保障线路的可靠。工业设备通过数据驱动的预测性维护，提升使用的可靠性。重要设备使用双机热备份、虚拟化多冗余备份、冗余电源、UPS 等方式进一步提升设备的可靠性。重要工业系统应用软件使用多级备份、定时备份的方式，保障工业系统应用的可靠运行。

3.1.2 企业信息网络

（1）概述

企业信息网络是企业办公、科研、生产数据以及相关信息存储与提炼的载体，是形成工业互联的关键网络环节。企业信息网络需要确保控制设备能够与管理工厂或公司的应用系统和设备之间进行正常通信。它是一个必须能够处理由大量数据组成的复杂信息的网络。

（2）功能和性能

企业信息网络中运行了常见的办公业务系统，例如邮件系统、OA 系统等，还运行了对于工业企业正常运营极为重要的 ERP、CRM 和 MES 等业务系统。为了实现应用需求，布线方式通常采用有线或无线方式，对吞吐量及时延的要求较高，通常采用高速以太网络，使用常见 TCP/IP 协议进行通信。

随着移动办公的需求越来越多，需要网络资源和策略以人

为核心进行定义，用户在哪里接入、资源就下发到哪里，无论用户移动到哪里，策略和体验不变。企业信息网络提供丰富的认证策略来满足不同场景下的终端认证需求，并能支持策略集中控制和策略随行保障，终端接入网络后 IP 地址不变，实现精确溯源。

园区企业信息网络的用户量庞大、业务应用逐渐丰富，对网络带宽的需求越来越高，需要在设备性能、带宽能力、接入用户能力、安全防护等多个方面考虑性能保障。

（3）安全

园区企业信息网络应建立系统级安全防护体系。在此体系中，用户、计算机终端、网络设备、安全设备、安全管理中心应充分协同，在安全事件出现前极力规避、预警，出现时能够及时发现，并具备能够依据事先定制好的应急方法进行自动化处理的能力，最后还需要输出完整的安全防护日志报表，供管理人员查看、分析并进行策略调整。

（4）可靠性

园区企业信息网络建设对设备的可靠性要求很高，因此，必须从设备自身和网络架构角度确保网络系统的稳定性，并且对于安全防护也需要考虑一定的可靠性保障，防止安全防护导致的可靠性降低。设备角度，核心层设备可采用多级交换架构设备，利用引擎、交换矩阵关键部件的分离提高物理可靠性；架构方面，两台物理设备利用智能虚拟化或者堆叠技术提高故障的切换速度。

3.1.3 园区公共服务网络

（1）概述

园区公共服务网是向园区内各企业提供基础公共服务，实现园区内工业企业间互联互通的网络。

园区公共服务网络典型业务包括:

- 室外 Wi-Fi:在公共区域使用 Wi-Fi 覆盖整个园区户外区域，提供高品质的数据接入服务，同时可以作为园区物联网的承载网，支持无线接入业务和无线回传业务。
- 物联网：支持园区公共部分管理的各种物联网应用，实现园区智慧管理。常见的 IOT 类应用包括资产管理、人员管理、健康管理、能效管理等。
- 能源等基础设施监控：园区公共服务网络应该能够对园区内的摄像头，水，电，煤，天然气，机房内设备等基础设施各种重要参数（包括温度、压力、流量、电量、液位等）以及园区环境进行集中的动态监控。
- 互联互通：园区公共服务网络应确保各企业之间办公、科研等相关数据能够进行正常通信，并确保网络具备足够的性能及健壮性，已支撑各企业互联需求。
- 外部互联网络：进驻园区的企业通过园区公共服务网络作为出口访问互联网，以及进行园区外部互连(如业务上公有云)，这些外部互联网络需要借助运营商网络的优势，而部分采用无线方式进行包括 5G、卫星、GSM 等。

（2）功能

随着企业互联互通要求的快速发展及应用，园区公共服务网络需要维护的互通通道数量以及需要隔离的企业逻辑网络数量均会呈现爆发式增长，网络自身的规模也会随之增长，所以需要网络设备在首次部署、扩容以及故障替换时，能够自动化上线，作到即插即用，能根据网络设备的角色自动下发相应的配置，同时管理员对网络的隧道等业务部署能够集中管控，自动化下发,大幅提升网络的部署效率，降低部署成本。

工业互联网园区中存在着海量的物联终端，如 IP 摄像机、门禁控制器、智能照明、能源管理终端、传感器等。数以千计的物联终端应能够高效的接入到园区网络中，并且自动识别终端类型进入到各自对应的逻辑业务网络，并自动下发对应的网络安全策略，以与其他逻辑业务网络之间安全隔离。终端接入网络之后，网络系统能够探测终端的设备类型，当发生终端被仿冒时，能够自动将其隔离并及时告警，保障业务系统的安全运行。

园区公共服务网络提供的安防监控、车辆管理、智能楼宇管理、信息发布等业务，通过 SDN 等技术实现一张物理网络承载多个业务并保证多业务之间的安全隔离，并通过图形化用户界面实现分钟级端到端虚拟业务网络的创建并自动化下发配置。

（3）性能

大型园区企业众多，业务应用丰富，对网络带宽的需求越来越高，需要在设备性能、带宽能力、接入用户能力、安全防护等多个方面考虑性能保障。

鉴于园区公共服务网络本质上是园区内骨干网，因此设备

性能上，基于 CLOS 架构的骨干设备为基本诉求，设备必须可提供为高密度万兆接口，并具备 40G/100G 扩展能力。

链路带宽上，有线网络骨干采用万兆甚至 100GE 互联、接入各企业侧需要采用千兆或者万兆互连。

（4）安全

园区公共服务网络承担着园区内所有企业之间互联互通以及企业公网出口的任务，因此园区公共服务网络的安全极为重要。园区公共服务网络安全防护不应是孤立的设备堆砌，应该在整个园区协同各企业，构建 E2E 安全防护体系。在此体系中，园区公共服务网络，各企业网络，使用者、计算机终端、网络设备、安全设备、安全管理中心应充分协同，在出现安选时间之前可以预警，并能快速隔离受影响网络，避免安全威胁扩散到其他企业中。最后还需要输出完整的安全防护日志报表，制定相应策略并通告园区内进驻的各企业。

（5）可靠性

园区公共服务网络本质为园区骨干网，因此可靠性要求很高。一旦网络系统运行不正常或者出现故障中断将直接导致整个园区业务中断，因此，必须从设备自身和网络架构角度确保网络系统的稳定性，并且对于安全防护也需要考虑一定的可靠性保障，防止安全防护导致的可靠性降低。可靠性度量指标包括：MTTR、MTBF 和可用度。尽量减少 MTTR 和 MTBF，增加系统可用度，园区公共服务网络可靠性包括一系列技术。它主要涉及到系统及硬件可靠性设计方法、软件可靠性设计方法、可靠性测试验证方法和网络可靠性设计。

（6）管理运维

园区公共服务网络的整体运行状态应该在一个视图内进行完整呈现，不仅局限在拓扑的发现、事件告警，还应观察到具体事件的处理进程，以及最终是否完成闭环操作。

园区公共服务网络关注的重点应该是各进驻企业的互连带宽，各企业出口使用多少流量等 SLA，要可以提供相应报表给各进驻企业，以明确园区公共服务网络提供的 SLA。

园区公共服务网络需要具备感知企业业务的能力。新一代园区公共服务网，应具备接管各企业内用户带宽管理、安全控制、行为审计的能力，以在企业内部网络出现重大灾难时作为备份接管业务，支撑生产的无中断。同时，需要提供企业内部网络及业务向园区公共服务网络迁移的方案及设计。

3.1.4 云基础设施

（1）概述

云基础设施作为工业互联网园区内部信息汇聚的重要基础设施，实现园区内多家企业私有云和公有云的承载。随着私有云应用的不断成熟，越来越多的园区网络开始构建自己的数据中心，通过数据中心承载和提供各类业务，以数据中心为节点重构基础网络。工业互联网园区数据中心强调如何高效的使用数据中心中的各种资源，园区更倾向于集中建设数据中心，集中部署计算资源，实现资源高效实用。各企业或者各部门从数据中心中租用计算资源。

同时，云计算扩大了计算资源的能力边界，更多的业务受

益于云计算，并引发了多种业务部署模型的变化，越来越多的业务依赖云计算，迁移到数据中心中。

（2）性能

数据中心网络是整个园区网络中对性能要求最高的一个部分。通常通过采购专门的数据中心交换机，实现性能、功能和成本的平衡。

数据中心网络不同部分的业务流特性和园区网络其它部分不一致，对网络的其他性能指标也会有要求。例如:

- HPC 等业务对网络的时延和丢包等要求有极高的要求，需要数据中心交换机提供低时延网络等能力。
- 视频传输类业务，链路始终处于连续的高负载状态，这种场景下，端口的突发缓冲能力会极大的影响网络的性能，需要采用专用的大 Buffer 交换机。

（3）可靠性

数据中心要求高可靠性。通过组网（冗余备份，胖树）等提供拓扑高可靠，通过网络虚拟化提供组网和业务高可靠以及通过多数据中心备份提供备份和容灾。

（4）管理

和传统中心机房的管理不同，工业互联网园区数据中心建设有强大的管理系统，通过应用层和控制器的协同，对转发层进行自动化管理，快速发放各种业务。

新一代的管理系统通过引入 AI，能够最大程度的实现管理和故障定位的自动化。管理系统通过大数据引擎，采集网络中的全方位信息；通过基于 AI 的分析器，对网络故障进行实时定

位。

3.2 园区网络组网实现

3.2.1 传统三层架构网络

传统的三层架构网络基于标准的以太网交换机，整体拓扑简单，建设成本相对较低，支持的业务也比较简单。同时，因为没有针对网络维护进行优化，传统组网的可维护性较差。因此，传统三层架构网络主要适合业务场景相对简单的场景，包括以下几种场景:

- 适合业务简单，不需要经常变更网络配置的私有园区网络;
- 规模较小的工业园区;
- 仅向租户提供基础互联业务的大型工业园区。

3.2.1.1 三层组网架构

如图 5 所示，网络被分为三层：接入层，汇聚层和核心层。

- 接入层

接入层是用户/终端接入网络的第一层。接入层通常由接入交换机组成，通常是简单的二层交换机。

- 汇聚层

汇聚层是接入层与核心骨干之间的分界线，主要用于转发用户间的“横向”流量，同时提供到核心层的“纵向”流量。汇聚层作为部门或区域内部的交换核心，实现与部门或区域专用服务器区的连接。

- 核心层

核心层是园区数据交换的核心，连接园区网络的各个组成部分，如数据中心、汇聚层、出口区等。核心层负责整个园区网络的高速互联。

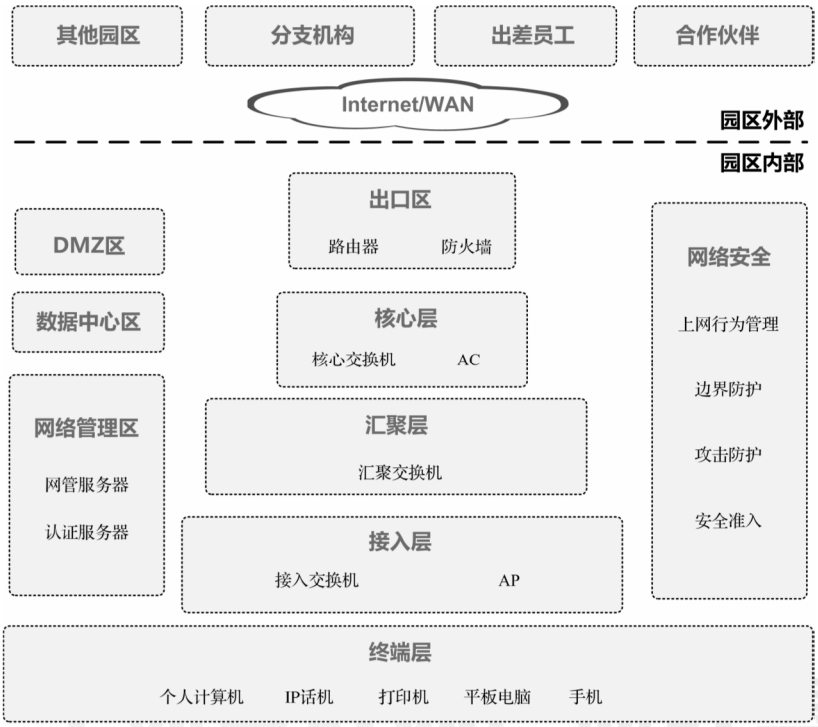


图 5 三层（核心、汇聚、接入）架构 + 传统 VPN

对于较小型的园区网络，可能不设置独立的核心层，由汇聚层设备承担核心层功能，合称为核心汇聚层。

3.2.1.2 传统 VPN 实现网络隔离

园区中不同的企业间的网络必须完全隔离，同一企业内部不同部门的网络往往也需要隔离。通过业务隔离，不同的业务部署之间可以相互独立，从而降低管理复杂度。例如：视频监控网络可以独立为一张视频监控虚拟网，视频监控负责人可以独立管理自己的设备和网络，视频设备的扩容调整无需和网络管理服务人进行协调。

三层组网采用传统的 VPN 技术包括:

- VLAN VPN
- BGP MPLS VPN

3.2.2 大二层架构网络

在移动化和新的业务需求的驱动下，传统网架构逐渐暴露出“僵化”和“复杂”的问题。如 IP、VLAN 等往往与物理位置紧耦合，导致用户难以大范围移动，策略无法自动跟随。网络运维工作量巨大，网管人员 80%-90%的时间都陷在网络运维的泥潭里不能自拔。

为了克服传统三层架构网络业务承载能力弱，配置管理复杂，自动化程度有限的缺点，基于大二层 SDN 化的新一代园区架构被提出来，其最基本的特征是柔性和极简。

“柔性”一方面指网络架构本身非常灵活，业务部署（可以做到与位置无关；另一方面指网络架构本身开放可编程。

“极简”指网络管理大幅简化，SDN 新园区架构的目标是消灭命令行，采用 SDN 控制器全面管理网络。

3.2.2.1 适用场景

大二层园区网络采用 VxLAN/EVPN 的 overlay 架构，在这种灵活架构之上，业务与网段可以对应，用户和 IP 可以绑定，策略部署可以极大简化，无线业务得到优化，服务链得以轻松部署，完全满足了移动化条件的诉求。同时管控面引入控制器，解决了传统网络管理复杂的难题，实现软件定义园区网的目标，最终达到部署随心、接入随意、业务随行的效果。大二层园区

网络适用于以下部署场景:

- 一张物理网需要安全承载多种业务
- 业务对网络灵活性有较高要求
- 有线无线一体化
- 多园区统一组网
- 海量物联设备安全纳管

3.2.2.2 大二层网络架构

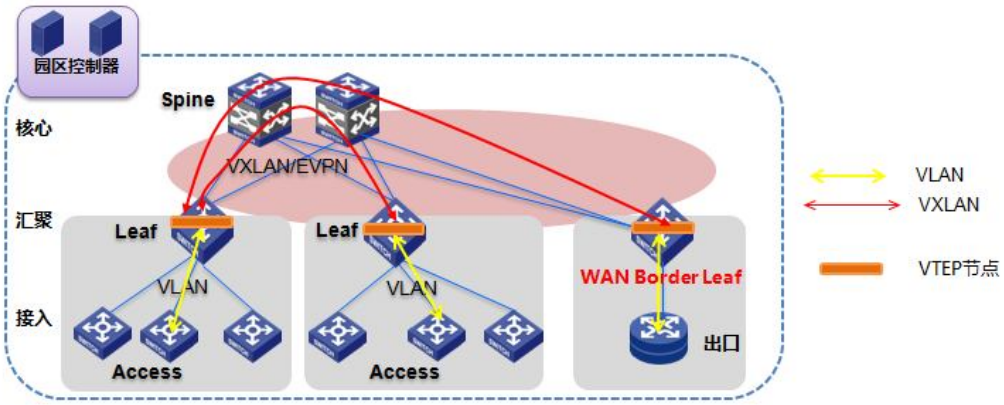


图 6 大二层网络架构

如图 6 所示，大二层架构网络的标准模型采用接入（access）/汇聚（leaf）/核心（spine）三层结构，基于 SDN VxLAN 技术，逻辑上核心层（spine）设备作为三层 VxLAN 网关，汇聚层（leaf）设备作为二层 VxLAN 网关，接入层（access）设备仅仅完成用户接入和简单的 VLAN 隔离能力。

在汇聚（leaf）和核心（spine）设备之间构建一个大二层网络。在 leaf 层以上采用基于 VxLAN 的 overlay 技术，leaf 层以下采用传统 VLAN 技术，在 leaf 上进行 VLAN—VxLAN 的映射，在 access 及 leaf 上配置 VLAN，实现每个用户一个 VLAN，用户之间相互隔离。

出口可以部署专门的 wan border leaf 角色和外网进行对接，实现 VxLAN 域和外网的路由互通。

网络的控制平面采用了 EVPN（Ethernet VPN）技术，通过 BGP 协议来实现园区网内用户终端的 ARP/MAC 信息的同步/扩散。同时在汇聚层设备支持 ARP 代答机制，有效抑制 ARP 广播。

网络的转发平面采用了基于 VxLAN 的 overlay 转发（隧道转发）。封装和解封装节点称为 VTEP（Virtual Tunnel End Point，虚拟隧道端点），这些节点完成普通报文到 VxLAN 的封装（上行）和解封装（下行），外层转发是标准的 IP 转发，容易为熟悉 IP 的人们理解和掌握，这也是 VxLAN 技术在众多 overlay 技术中能胜出的关键。

总的来看，大二层园区网络既能做到本地 L3 转发，最大限度地释放交换机的大带宽交换能力，又能限定广播域到极小的范围，避免广播风暴。同时整个网络架构又是一个大二层扁平化结构，非常好地解决了用户移动办公带来的体验/策略难以跟随的挑战和困难，是一种非常灵活/弹性的新一代网络架构，也是传统网络难以具备的。基于大二层技术实现业务解耦、策略随行。

3.2.2.3 大二层业务隔离

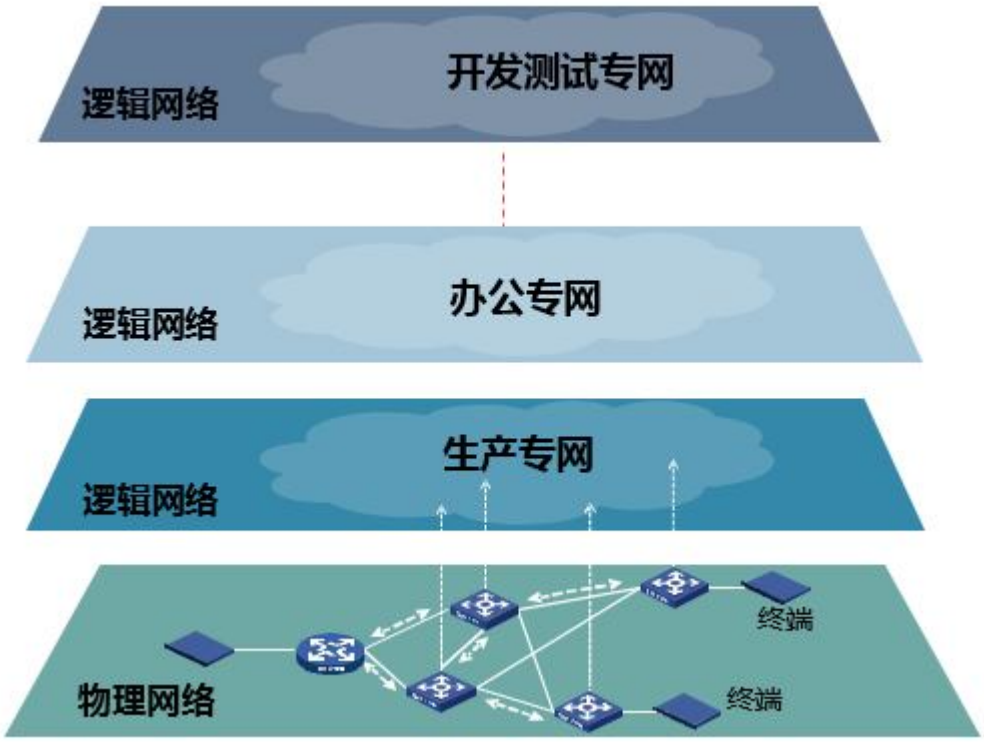


图 7 基于 overlay 的逻辑网络

整网采用 VxLAN overlay 的技术，实现基于业务的网络切片，为每个专用业务分配一个逻辑网络，且具备跨区域的通道隔离能力，相比 MPLS 的隔离方式，SDN VxLAN 的隔离只需要在端点（VTEP）做隔离，不需要全网隔离，端点之间只需要 IP 可达。

提供两种隔离方式，一是类似 MPLS 的 VRF 隔离，每个用户组在 VTEP 节点分配不同的 VRF，VRF 之间在路由层面实现隔离。二是 ACL 的隔离方式，不同用户组在接入之后获取的是不同 IP 网段，一条 ACL 就可以实现不同用户组之间的网络隔离。

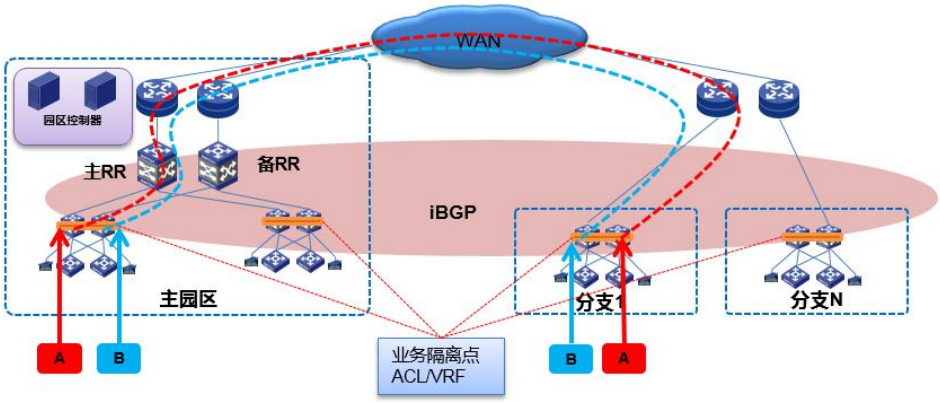


图 8 大二层园区网络的业务隔离方式

3.2.2.4 基于 SDN 的网络架构

传统的方案存在网络僵化，难以满足用户移动需求，运维复杂等问题。基于 SDN 的架构可对园区网中的移动用户和固定用户和各类终端进行识别，按照用户所属的用户组，或者终端所代表的一类应用进行标记后下发策略。用户和终端可以不受位置限制，部署可以随意、位置接入可以随意，但是最终获取的网络资源和网络权限保持一致，最终达到网随人动的效果。

SDN 架构中管理员不需要逐台设备配置 VPN，只需在控制器的图形界面上配置“私网”及其“二层网络域”，相关的网络配置会自动下发到所有的交换机。

终端上线后，根据认证自动进入其对应的逻辑网络。同一私网内的业务可以互通，不同私网之间的业务完全隔离。通过组间访问控制，控制用户组和资源组以及不同用户组之间的访问权限。通过组内访问控制，控制各个用户之间以及用户服务器互访。

对于移动地点的用户，因其所属用户组不变，其资源访问体验一致。对于访问部门服务器的用户，可以创建“相关的用

户组及其关联的接入场景、安全组，保障用户访问体验一致。

总体说来，SDN 场景下，整网的核心是园区网控制器组件。所有对网络的自动化上线、接入管理、用户组/策略管理、业务配置管理、网络运维管理全部在控制器上通过图形化界面完成。从而实现业务快速部署，网络可视运维。

3.2.3 无线网络架构

3.2.3.1 Wi-Fi 的 AC/AP 叠加式组网架构

AC/AP 叠加式组网架构是一种传统的组网方式。AP/AC 间通过 CAPWAP 隧道连接，可以叠加在任意有线网络上，适合于在已有有线网络上新建无线网络的场景，也可用于对无线网络要求较低的场景。

对于小型网络，AC 和 FIT AP 可以部署在一个二层网络下，AC 和 FIT AP 在同一个广播域，AP 通过本地广播可以直接找到 AC。此时，AC 和 FIT AP 之间的网络可部署专用回传网络。

对于大型网络，通常不会构建专用的 Wi-Fi 回传网络，而是借用有线网络回传。三层组网下，AC 和 FIT AP 不在同一网段，中间网络必须要保证 AP 和 AC 路由可达，AC 和 FIT AP 间会通过三层 CAPWAP 建立回传通道。图 9 为一个典型的大型网络的 Wi-Fi 组网架构。

- 回传网络

回传网络本身是基于交换机的有线网络，可以是传统三层组网，也可以是大二层架构的网络。在构建有线网络时，我们需要考虑是否有无线回传的需求，需要预留出相应的资源，如

VLAN 资源，IP 地址资源，VN 资源等。

构建回传网络时，需要考虑无线网络采用隧道转发模式还是直接转发模式。对于隧道转发模式，所有的控制都在 AC 上进行，回传网络需要保证所有 AP 和 AC 之间路由可达、带宽足够即可；对于直接转发模式，有线网络的网关和地址池设置需要考虑 Wi-Fi 接入的特点并进行针对性调整。

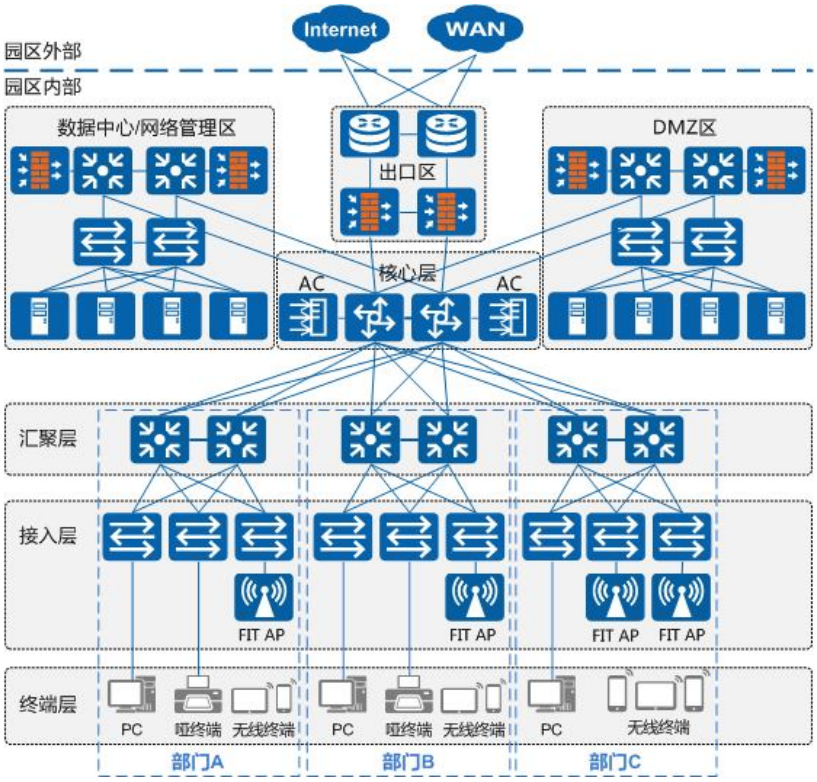


图 9 大型网络的 Wi-Fi 组网架构

- AC 部署

理论上，AC 可以部署在网络的任意地方，仅需要保证 AP/AC 间路由可达。但是，AC 作为无线网络接入控制点、业务提供点、漫游控制点，在隧道转发模式下是转发核心节点，对连接的可靠性和性能要求非常高。因此，AC 通常会和网络中的核心交换机部署在一起，通过多条捆绑的链路旁挂在核心交换机上。

● AP 部署

AP 按需部署在网络中，直接接入无线终端。对于企业级 AP，为了保证可靠性，通常采用吸顶式的安装方式，AP 被固定在天花板上，从而降低外部各种因素对 AP 的影响。企业级的 AP 都支持 PoE 供电技术，因此需要接入交换机的 POE。

实际部署 AP 时，应该提前使用厂家提供的规划软件进行精细的规划；实际部署过程中，可能会出现 AP 部署位置偏离规划位置的情况，还需要使用厂商提供的验收工具对覆盖效果进行测量和验收。

在选择 Wi-Fi 供应商时，不能仅仅考虑系统的功能和性能，还需要重点考察厂商的场景化解决方案提供能力，以及网络规划和网络安装工具的完备性。

● AC 热备

AC 一旦出现异常，会对网络造成极大的影响。通常建议部署 AC 热备方案。AC 热备方式及差异如表 2 所示。

表 2 三种备份方式比较

对比项	VRRP 双机热备	双链路双机热备	N+1 备份
切换速度	主备切换速度快，对业务影响小。通过配置 VRRP 抢占时间，相比于其他备份方式实现更快的切换。	AP 状态切换慢，需等待检测到 CAPWAP 断链超时后才会切换，主备切换后终端不需要重新上线。	AP 状态切换慢，需等待检测到 CAPWAP 断链超时后才会切换，AP、终端均需要重新上线，业务会出现短暂中断。
主备 AC 异地部署	VRRP 协议是二层协议，不支持主备 AC 异地部署。	支持。	支持。
适用范围	对可靠性要求高，且无须异地部署主备 AC 的场景。	对可靠性要求高，且要求异地部署主备 AC 的场景。	对可靠性要求较低，对成本控制要求较高的场景。

● Navi AC

大型企业在部署无线网络时，在为内部员工提供接入服务的同时，通常还需要为访客用户提供无线接入。通过Navi AC组网，如图 10 所示，企业可以将访客流量引导到安全的半信任区（Demilitarized Zone，DMZ）的 Navi AC 进行集中管理，从而达到内部员工接入和访客接入安全隔离。

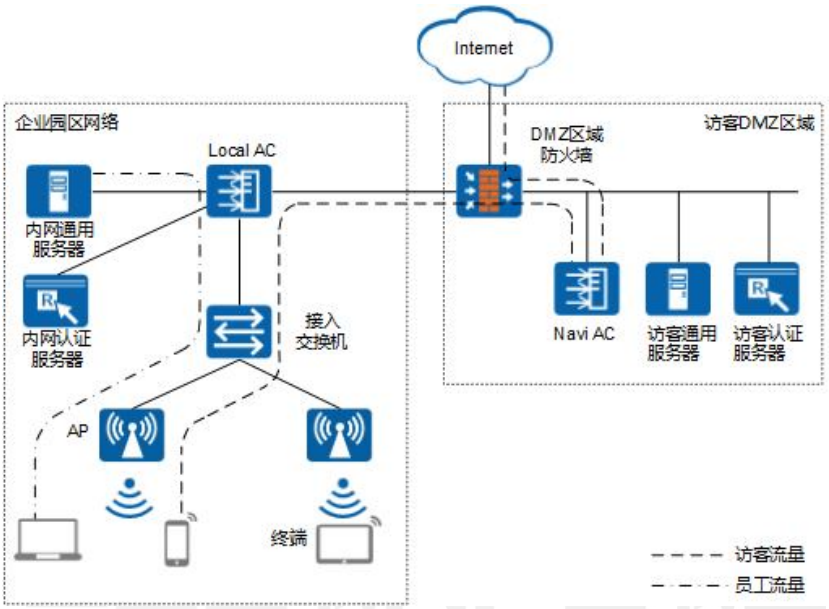


图 10 NaviAC 典型组网

3.2.3.2 多网融合架构

多网融合架构性能高，WLAN 网络品质好，但是需要有线网络的配合。因此，适用于新建整个网络的场景，特别是对 WLAN 网络有较高品质要求的网络。

1）多网融合架构提出的原因

传统 AC/AP 组网中，采用 AC 集中部署，集中转发的架构，Wi-Fi 网络通过 CAPWAP 隧道，承载在有线网络中。这种架构很好的隔离了有线网络和无线网络，部署简单快速。但是，这种架构下，所有的流量都要穿越整个网络到核心层的 AC 上进行汇

聚和分发，存在着效率低下的问题，对 AC 造成巨大的压力。

随着 Wi-Fi 技术演进，无线网络的性能和有线网络已经在一个水平线上，系统效率问题被放大。业界开始提出本地转发的系统架构，本地的用户数据报文直接进行转发。AC 简化为用户和 AP 接入管理，以及用户漫游流量的转发。本地转发部分解决了效率问题，但带来另外两个问题:

- 有线无线网络转发耦合: 例如门厅效应问题需要 IP Pool 进行解决。但是，本地转发引入后，这些问题被直接放到有线网络上，需要有线网络通过精细规划和配置进行解决。这给网络规划管理人员带来很大的压力;
- 有线无线网络控制分离: 虽然有线流量和无线流量无差异的跑在有线网络中，但业务控制点却有两个，有线的交换机和无线的 AC，再叠加上隧道承载的漫游的无线流量。这导致网络中几乎不可能部署任何业务策略。另外，有线用户和无线用户分别在不同设备上进行接入控制和管理，也给管理人员带来更多的压力。

基于以上考虑，业界提出了“有线无线融合”的解决方案，通过将 Wi-Fi 的 AC 特性融合进交换机，使得网络可以统一承载有线无线流量，再将 IOT 融合进来，形成多网融合架构。

2）有线无线融合架构

通过将有线业务的管理控制点和无线网络的管理控制点进行有机融合，使得单一设备能够同时接入管理有线和无线业务，这种设备通常体现为交换机，内置了 Wi-Fi AC 特性，本文称之为融合交换机。

基于融合交换机的 Wi-Fi 网络，AP 被和有线交换机一样进行管理，主要差异均被融合交换机所屏蔽。

基于融合交换机的解决方案同样有利于无线业务的简化。如 11 图所示，无线业务无需单独考虑高可靠解决方案，基于交换机成熟的可靠性技术（堆叠，链路聚合等等）天然具备高可靠能力。

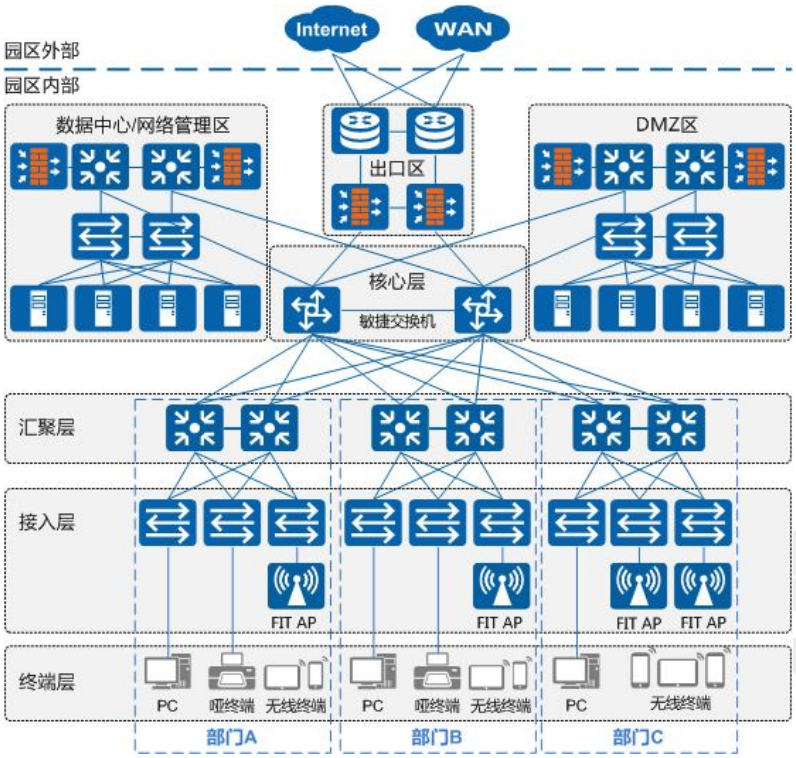


图 11 基于融合交换机的有线无线融合解决方案

3）Wi-Fi 和 IOT 融合架构

传统的 IOT 网络部署时，多张 IOT 网络并行的部署在网络中，分别承载不同的业务。例如：Zigbee 用于承载智能能效管理业务，RFID 用于承载资产管理业务，各种 IOT 网络有自己的网关和接入网络。主要存在部署成本高昂、站点资源冲突、频谱资源冲突，干扰严重等问题。为此可以在网络中引入“无线锚点”的概念，无线锚点统一提供安装点位、电源和回传资源，

统一协调各种无线技术，实现多网融合。Wi-Fi AP 是提供“无线锚点”特性的最合适载体。

目前主流的 Wi-Fi /IOT 融合方案包含两种:

- 外置融合方案。Wi-Fi AP 提供供电和回传接口，IOT 设备旁挂 AP，使用 AP 提供的供电和回传资源;
- 内置融合方案。Wi-Fi AP 提供内置插槽，IOT 设备以内置插卡的形式存在，使用 AP 提供的供电和回传资源。

4）多网融合架构和基础网络

多网融合架构中，基础网络通过虚拟网络为不同的业务提供回传服务。例如: 为 Zigbee 承载的智能能效管理业务，RFID 承载的资产管理业务以及视频回传业务等，分别创建不同的虚拟网络。

对于传统三层架构网络，通常使用 VLAN VPN 进行构建。针对不同的业务，规划不同的业务 VLAN，全网部署 VLAN VPN，实现业务隔离和回传。

对于大二层架构网络，可以直接使用 VN 承载不同的业务。通过 SDN 控制器，自动化部署 VN，实现业务隔离和业务回传。

3.3 园区网络业务部署

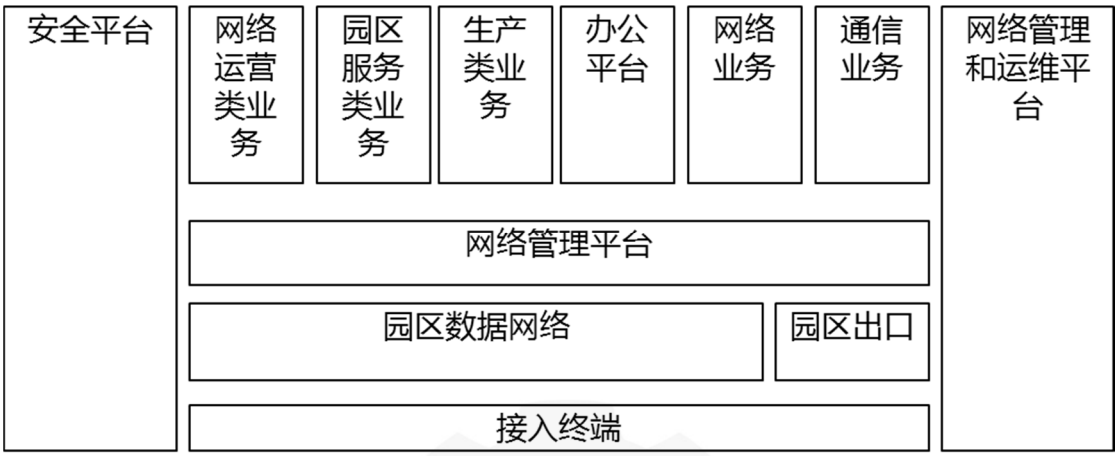


图 12 园区网络业务部署

如图 12 所示，园区网络中通常存在一个网络管理平台。该平台本身承担业务部署的功能，同时作为业务底座。

网络管理平台通常是一个云化平台，部署在园区数据中心里。基于该底座的各业务平台（模块）通常也部署在园区数据中心。

3.3.1 园区网络主要业务

园区的业务包含基础服务类业务和生产力类业务两大类。

1）基础服务类业务

基础服务类业务主要指直接服务于园区用户的基础服务和网络基础服务。一般包括:

- 网络管理和维护类：对网络本身的运营状态进行管理，对网络故障进行快速定位恢复;
- 网络运营类：对多租户服务提供支持，分别服务于不同的租户企业;
- 园区服务类：典型如：视频监控网络，能耗管理网络等。

每种服务需要独立的物理/逻辑网络承载，需要独立的进行管理维护。

2）生产力类业务

生产力类业务直接服务于企业的各业务流程，包括网络业务类，安全业务类，通讯类等:

- 网络业务类: 针对园区企业内部的各种组织和组织的通讯需要，通过合理的组织网络，给予支持。一般包括各种子网配置管理、VPN 配置、远程接入等;
- 安全业务类: 一般包括基本的防火墙和高级的 APT 防护。防火墙的部署一般放在不同的安全区域的边界处。例如: 接入网络和数据中心网络交界处。APT 防护通常包含三部分: 探针散布在网络的各设备中，分析器和其他服务器共同部署在企业数据中心中，流量清洗设备部署在网络核心层;
- 通讯类: 通讯类业务一般包含语音电话，视频通话，视频会议，视频直播等多种业务，对网络服务质量有较高要求。一般需要部署通讯服务器，通讯网关，CDN 网关等设备。

3.3.2 分层业务部署

1）三层部署架构

一般来说，业务部署采用三层架构。网络中有三处位置通常被用来部署业务类服务器或者探针，从而实现业务部署。

数据中心或者中心机房。很多的业务服务器需要提供复杂

的业务逻辑或者需要高性能的通用计算能力，这类业务服务器通常基于通用的计算平台。

网关，一般是核心交换机，由于几乎所有的南北向流量都会经过核心交换机，因此，核心交换机是另一个适合的业务服务器部署点。

接入层网络设备。接入层网络设备适合用来部署探针，从而在网络边缘对流量进行识别与控制。新兴的基于 AI 的各种业务服务需要大数据的支持，需要接入层网络设备支持Telemetry能力，从而能够最大程度的提供原始流量信息。

2）业务服务器虚拟化

三层部署架构下，需要根据业务服务器部署情况，对网络进行配置，将业务引导到相应的业务服务器上。这就意味着，业务的部署和网络耦合在一起，不利于业务的快速部署和快速调整。

对于实现了大二层架构的网络，使用虚拟化技术，结合SDN集中控制的思路，可以实现业务的灵活和快速部署。这就需要引入业务服务器虚拟化的概念，包括业务服务器云化和业务服务器池化。

- 业务服务器云化

基于通用计算平台架构的业务服务器适合云化，云化后，业务服务器被部署在园区内部数据中心的私有云或者外部公有云上。云化服务器包括两种方式：基于虚拟机的云化和基于微服务的云化。

基于虚拟机的云化对业务服务器的改造较少。业务服务器

直接运行在虚拟机中，通过虚拟机的动态创建或者删除，实现服务器的弹性扩展。

微服务化对业务服务器的改造相对较大，但虚拟化效果更好。业务服务器呈现为多个微服务，运行在网络云操作系统中，可以实现更精细的负载调整和弹性扩展。

- 业务服务器池化

使用专用硬件平台业务服务器，需要通过虚拟化技术，降低部署的复杂度和对网络架构的影响。池化技术可以实现业务自动部署和动态调用。

基于业务链技术，业务可以动态连接到服务器资源池中，按需分配资源。业务链的创建和撤销由 Controller 动态管理，在 VN 的层面上进行配置和实施，无需人为干涉。

3.3.3 管理和维护

管理和维护是网络运行过程中最为复杂的环节。传统上，网络管理人员必须依靠人力和经验对网络进行维护，所能依赖的，只有厂商提供的纸质或者电子的故障排除手册以及基于 SNMP 的网管。

随着云计算的普及，运维工作开始逐步变化。云化的管理平台存储、运算能力极大提升，成本极大降低。能够在有限的成本下提供近乎无限的存储和计算扩展能力。因此，基于云计算平台的管理运维系统快速抛弃了信息采集能力有限的 MIB 和 SNMP，转向基于 Telemetry 的大数据采集技术。

AI 技术逐步成熟。云化管理运维系统拥有网络大数据后，

再结合数据驱动的 AI 技术，可以实现故障的自动定位。从前依靠经验猜测的故障定位过程变成基于大数据的人工智能故障定位。再结合知识库，可以提供易于操作的恢复指导，甚至能够实现网络自愈。

附录 1：工业互联网园区网络创新技术与应用

1.1 Wi-Fi 6

（1）技术简要介绍

Wi-Fi 6 是最新一代 Wi-Fi 标准的简称。传统上，我们直接使用 Wi-Fi 标准号来描述 Wi-Fi 技术，例如：早期的 802.11a/b/g/n，当前主流的 802.11ac。为了便于用户轻松了解其使用的 Wi-Fi 网络的先进性，WFA 选择使用数字序号来对 Wi-Fi 重新命名。根据 WFA 的公告，现在的 Wi-Fi 命名分别对应如下 802.11 技术标准，如表 3 所示。

表 3　802.11 标准与新命名

发布年份	802.11 标准	频段	新命名
2009	802.11n	2.4 GHz 或 5 GHz	Wi-Fi 4
2013	802.11ac wave1	5 GHz	Wi-Fi 5
2015	802.11ac wave2	5 GHz	
2019	802.11ax	2.4 GHz 或 5 GHz	Wi-Fi 6

Wi-Fi 6 提供了大量新功能，包括增加的吞吐量和更快的速度、支持更多的并发连接等。同时，Wi-Fi 6 兼容之前的标准，Wi-Fi 4 和 Wi-Fi 5 终端可以无缝接入 Wi-Fi 6 网络。对比 Wi-Fi 5，Wi-Fi 6 增加了许多针对高密部署场景的新特性。

（2）技术特点

Wi-Fi 6 引入了一系列新特性，从而获得更多的技术优势，能够有效的提高 Wi-Fi 使用效果，扩展应用范围。

1)OFDMA 频分复用技术

Wi-Fi 6 中引入了一种更高效的数据传输模式-OFDMA，通过将子载波分配给不同用户并在 OFDM 系统中添加多址的方法来实现多用户复用信道资源。更细的信道资源分配，使得系统效率

更高，并能提供更好的 QOS。

2) DL/UL MU-MIMO 技术

MU-MIMO 使用信道的空间分集来在相同带宽上发送独立的数据流，与 OFDMA 不同，所有用户都使用全部带宽，从而带来多路复用增益。终端受天线数量受限于尺寸，一般来说只有 1 个或 2 个空间流（天线），比 AP 的空间流（天线）要少，因此，在 AP 中引入 MU-MIMO 技术，同一时刻就可以实现 AP 与多个终端之间同时传输数据，大大提升了吞吐量。Wi-Fi 5 支持了 DL MU-MIMO 特性，Wi-Fi 6 增加了对 UL MU-MIMO 技术的支持。

3) 更高阶的调制技术 (1024-QAM)

Wi-Fi 5 采用的 256-QAM 正交幅度调制，每个符号传输 8bit 数据（2^8=256），Wi-Fi 6 将采用 1024-QAM 正交幅度调制，每个符号位传输 10bit 数据（2^10=1024），Wi-Fi 6 的单条空间流数据吞吐量提高了 25%。

需要注意的是 Wi-Fi 6 中成功使用 1024-QAM 调制取决于信道条件，信道质量要求高于其他调制类型。

4) 空分复用技术（SR） & BSS Coloring 着色机制

Wi-Fi 6 中引入了一种新的同频传输识别机制，满足条件时，两个 Wi-Fi 设备可同信道同频并行传输。可以降低系统内干扰，提升系统容量。

5）扩展覆盖范围 (ER)

Wi-Fi 6 标准采用 Long OFDM symbol 发送机制，每次数据发送持续时间从原来的 3.2us 提升到 12.8us，更长的发送时间可降低终端丢包率；另外 Wi-Fi 6 最小可仅使用 2MHz 频宽进行

窄带传输，有效降低频段噪声干扰，提升了终端接受灵敏度，增加了覆盖距离。

（3）技术典型应用

Wi-Fi 6 设计之初就是为了适用于高密度无线接入和高容量无线业务，比如室外大型公共场所、高密场馆、室内高密无线办公、电子教室等场景。

在这些场景中，接入 Wi-Fi 网络的客户端设备将呈现巨大增长，另外，还在不断增加的语音及视频流量也对 Wi-Fi 网络带来挑战，根据预测，到 2020 年全球移动视频流量将占移动数据流量的 50%以上，其中有 80%以上的移动流量将会通过 Wi-Fi 承载。我们都知道 4K 视频流（带宽要求 30Mbps/人）、语音流（时延小于 30ms）、VR 流（带宽要求 50Mbps/人，时延有小于 15ms）对带宽和时延是十分敏感的，如果网络拥塞或重传导致传输延时，将对用户体验带来较大影响。而现有的 Wi-Fi 5 网络虽然也能提供大带宽能力，但是随着接入密度的不断上升，吞吐量性能遇到瓶颈。而 Wi-Fi 6 网络通过 OFDMA、UL MU-MIMO、1024-QAM 等技术使这些服务比以前更可靠，不但支持接入更多的客户端，同时还能均衡每用户带宽。

在工业园区场景中，Wi-Fi 6 的应用场景丰富。例如：工业制造场景中存在大量高清视频回传以进行质量检验的场景，使用 Wi-Fi 6 可以同时提供支持更多的高清摄像头同时回传更高质量的视频数据，同时提高检验质量和效率。

1.2 WIA

（1）技术简要介绍

工业无线网络 WIA(Wireless Networks for Industrial Automation)技术是我国具有自主知识产权的高可靠、超低功耗的智能多跳无线传感器网络技术，该技术提供一种自组织、自治愈的智能 Mesh 网络路由机制，能够针对应用条件和环境的动态变化，保持网络性能的高可靠性和强稳定性。目前 WIA 与 Wireless HART、ISA100 并列为主流的工业无线技术体系。

WIA 网络由主控计算机、网关设备、路由设备、现场设备和手持设备 5 类物理设备构成。此外还定义了两类逻辑设备：网络管理器、安全管理器，在实现时可位于网关或者主控计算机中。其中网关主要负责 WIA 网络与工厂内的其它网络的协议转换与数据映射，冗余网关负责网关的热备份，网络管理者负责构建由路由设备构成的 Mesh 网络及监测全网性能，安全管理者负责路由设备及终端设备的密钥管理与安全认证。

WIA 网络采用星型和 Mesh 结合的两层网络拓扑结构。第一层是 Mesh 结构，由网关设备及路由设备构成；第二层是星型结构，由路由设备及终端设备或手持设备构成。

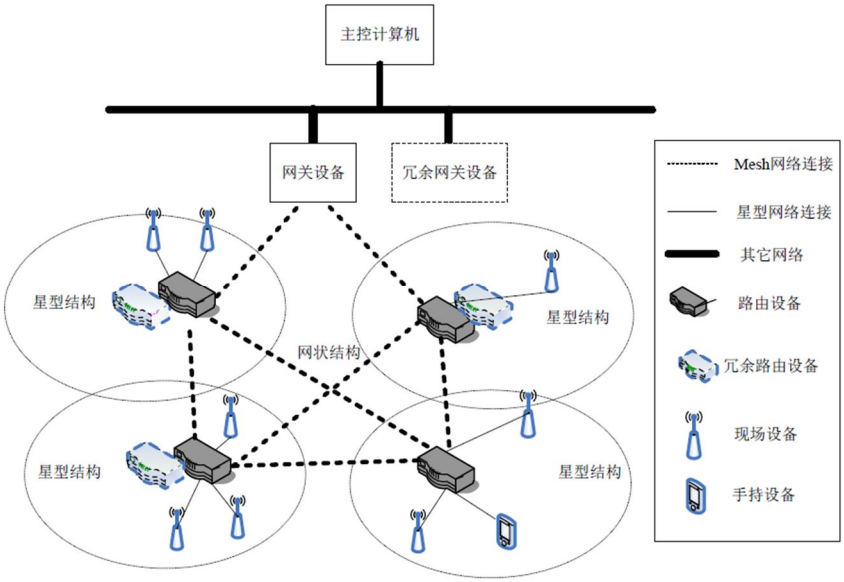


图 13 WIA 网络架构

（2）技术特点

1）支持扩频通信与窄带通信

WIA 网络物理层工作频带低频频带支持窄带通信，其优点是通信距离远，绕障能力好，同频其它设备少，干扰较小；在高频频带支持扩频通信，其优点是通信速率高，抗干扰能力强。WIA 网络可同时支持扩频通信与窄带通信，并将它们无缝地集成到同一网络中。

2）兼容 IEEE802.15.4、无线 HART 标准

WIA 网络在链路层兼容 IEEE802.15.4 的超帧结构，并对其进行了扩展。WIA 在应用层支持 HART 命令和操作，兼容于现有的 HART 工具，应用和系统集成技术。

3）超低能耗

WIA 网络支持簇内的报文合并，通过簇首将多个簇成员的周期性报文合并，提高了报文中的有效数据比例，降低报文头部的通信开销，从而有效地降低了网络开销，延长了电池寿命。

4）分层组织模式

WIA 网络在路由设备组成的 mesh 网络中采用了集中式的管理策略，在终端设备组成的多个星型网络中采用了分布式的管理策略。这种分层的组织模式，对网络拓扑的维护更加灵活、快速。

6）高可靠自组织网络

WIA 网络采用全网 TDMA 模式,避免了报文冲突。通过跳频通信方式提高了点到点通信的抗干扰能力。在链路层采用自动请求重传机制保证报文传输成功率。在网络层采用智能 Mesh 路由机制提高了端到端通信的可靠性。

（3）技术典型应用

工业无线网络 WIA 技术主要应用于石油、石化、冶金、环保、污水处理等领域。通过使用工业无线网络 WIA 技术，用户可以以较低的投资和使用成本实现对工业全流程的“泛在感知”，获取传统由于成本原因无法在线监测的重要工业过程参数，并以此为基础实施优化控制，来达到提高产品质量和节能降耗的目标。

1.3 TSN

（1）技术简要介绍

TSN(Time Sensitive Networking，时间敏感网络)指在 IEEE802.1 标准框架下，基于特定应用需求制定的一组“子标准”，旨在为以太网协议建立“通用”的时间敏感机制，以确保网络数据传输的时间确定性。TSN 位于数据链路层，从底层架构

中改变了以太网的不确定性，触发了以太网本身的一次自我迭代。

TSN 是一种具有有界传输时延、低传输抖动和极低数据丢失率的高质量实时传输网络。它基于标准以太网，凭借时间同步、数据调度、负载整形等多种优化机制，来保证对时间敏感数据的实时、高效、稳定、安全传输。TSN 通过一个全局时钟和一个连接各网络组件的传输调度器，实现网络内的确定性实时通信。调度器依据相应调度策略，控制时间敏感数据流的实际传输时间和传输路径，以避免链路争抢所导致的传输性能下降和不可预测性，从而保证时间敏感应用的点对点实时通信。当前，IEEE 802.1 正在推进 TSN 系列标准的制定，核心内容涵盖时间同步、数据帧控制、数据流调度、传输可靠性保障等多个协议。我国也在同步推进工业互联网 TSN 系列标准的研制。

（2）技术特点

时间敏感网络（TSN）是由 IEEE 802 组开发的一套标准，它提供以下功能:

- 时间敏感应用的定时和同步，IEEE802.1ASbt
- 计划流量的增强功能，IEEE802.1Qbv
- Frame Preemption，IEEE802.1Qbu
- 冗余网络的路径控制和保留，IEEE802.1Qca
- 流保留协议(SRP)增强功能支持 IEEE802.1Qbu/ IEEE802.1Qbv/ IEEE802.1 Qca/ IEEE802.1CB ，IEEE802.1Qcc
- 无缝冗余，IEEE802.1CB

TSN技术有机会统一目前工业网络标准，未来各厂家将可以基于统一的基础网络“TSN+IPv6”进行数据协议设计和应用开发，改变现有“烟囱式”的产业格局。 TSN技术面向1000Mbps接口设计，兼容现在工业网络广泛使用的 100M 接口，是工业网络最被看好的向千兆以太网演进的技术方案，现有的PROFINET、EtherCAT、SERCOS III 等工业以太网均在研究与TSN 技术的兼容、互通和演进问题。

TSN 具备优秀的上层支撑兼容能力，能够更好的支持IP/IPv6、TCP/UDP等协议，实现 OT与IT网络层次结构的融合;并且能够与上层的 DetNet、SDN 等技术的数据模型良好的兼容互通，更好的支撑各类上层应用；能够解决工厂内的数据互通问题，将 OPC-UA 的数据采集延伸到现场级，实现生产环境全方位实时数据汇集。时间敏感网络能够消除这种不确定性和不可预测性，使分配的网络带宽恰满足要求的时延，从而允许针对应用的实际需求进行带宽分配，既提高了带宽利用率，也保证了传输时延上限。

（3）技术典型应用

工业控制网络存在大量对时间非常敏感的应用，比如机械手臂控制、传感器数据实时上报、音视频文件传输、控制指令下发、工业机器人控制等。这些数据需要在确定时限内发送到目标，以支持工控设备和应用的正常运转。时间敏感网络将基于通用的以太网标准来建设，具备确定性网络的属性，能够满足工业网络对于定时、安全和可靠性等方面的要求，现有的专有工业控制网络可以通过网关来连接到时间敏感网络，实现互

联。

利用 TSN 实时网络技术，改造传统工业网络，实现如下功能:

- 减少时延: 实现微妙级时延，纳秒级时钟同步
- 高带宽: Gb+数据传输，满足工业互联网大容量数据传输要求
- 互通性强: 基于标准以太网，互通简单，减少厂商对接和数据收集难度

1.4 OPC UA

（1）技术简要介绍

在工业互联网园区网络的智慧工厂建设时，数据的互联互通成为关键。特别在工业现场的数据采集、传输与运营中，我们需要对运行的机器状态、设备报警信息、产品质量以及生产相关参数进行采集，不管上层架构如何能够进行智能分析与优化，如果缺乏统一的标准与信息模型，都很难落地。

OPC UA（OPC 统一架构）是一套安全、可靠且独立于制造商和平台，可使不同操作系统和不同制造商的设备之间可以进行数据交互,适用于工业通讯的数据交互规范。OPC UA 的目的是为工厂车间和企业之间的数据和信息传递提供一个与平台无关的互操作性标准。OPC UA 已经成为 IEC 标准，并在 2017 年成为中国国家标准，在 2018 年发布了基于 Pub/Sub 的机制作为 OPC UA 的补充机制，在 Part 13 部分由 IEC 发布。通过 OPC UA 真正实现 IT 与 OT 的融合，真正解决工业场景下数据互联问题。目前

OPC UA 技术还正在积极考虑与 TSN 等技术进行结合，提高数据互联的实时性和可靠性，向现场设备端延伸。

（2）技术特点

OPC UA 具备以下特点：

- 功能对等性：所有 COM OPC Classic 规范都映射到 UA
- 平台独立性：从嵌入式微控制器到基于云的基础设施，横向和纵向扩展
- 安全性：信息加密、身份验证和审核
- 可扩展性：添加新功能而不影响现有应用程序的能力，面向未来的框架
- 综合信息建模：用于定义复杂信息

图 14 展示了 OPC UA 层模型架构图。

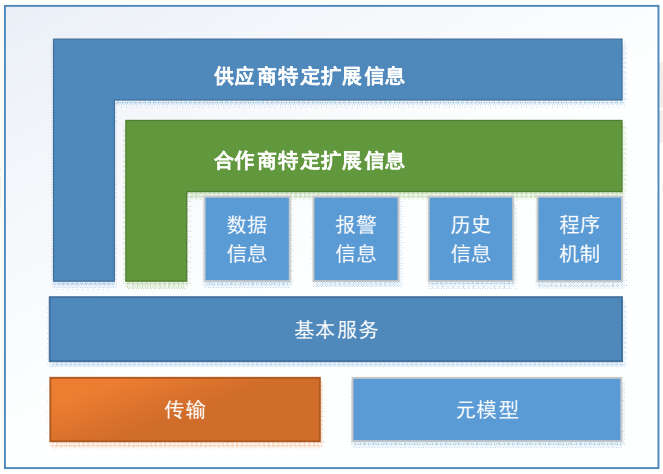


图 14 OPC UA 层模型架构

（3）技术典型应用

工业互联网需要在园区各个企业之间以及企业内部建立各环节信息的无缝链接，实现底层设备、控制层、MES、ERP 的纵向集成。主要解决企业内部信息网络与物理设备之间的联通问题。如图 15 所示，OPC UA 不仅仅针对 MES、SCADA、PLC 和 DCS

接口，而且也提供了更高级别功能之间的互操作性。

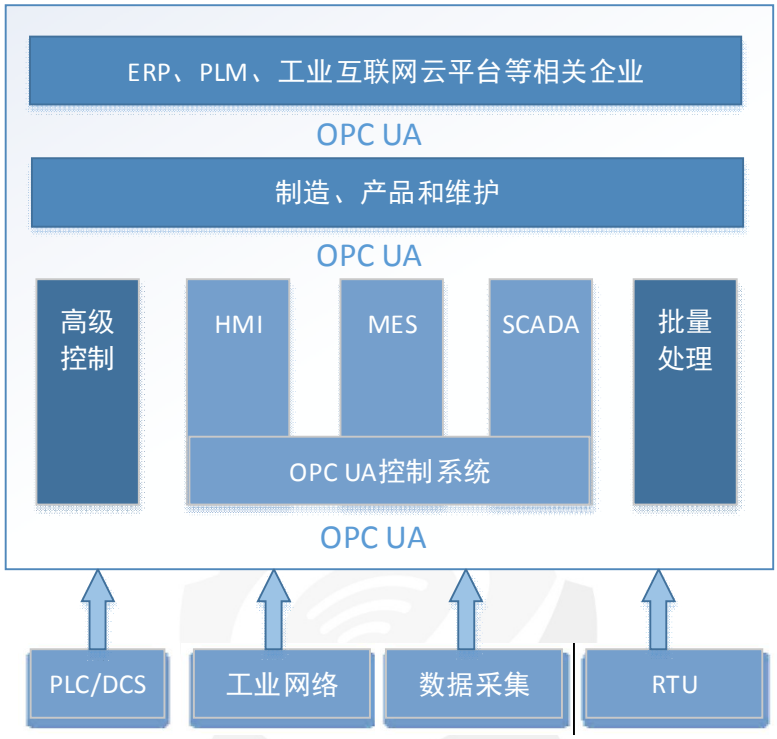


图 15 OPC UA 应用架构

1.5 室内无线定位技术

（1）技术简要介绍

位置服务是现代自动化系统的基础能力之一。室外环境下，我们可以使用基于卫星的无线定位技术，例如：北斗系统；但在室内环境下，由于卫星信号被屏蔽，必须使用其它的室内定位技术。一般来说，室内定位技术包括两大类：无线室内定位技术和非无线室内定位技术。

非无线定位技术，例如：视觉定位，二维码定位，激光定位，都需要专用终端进行支持，且通常只能进行客户端定位。无线定位技术可以复用无线通信系统，投资少，且可以对通用终端进行网络侧定位，便于集中管理和业务部署。

目前业界主流的无线定位技术可以按照图 16 进行划分。

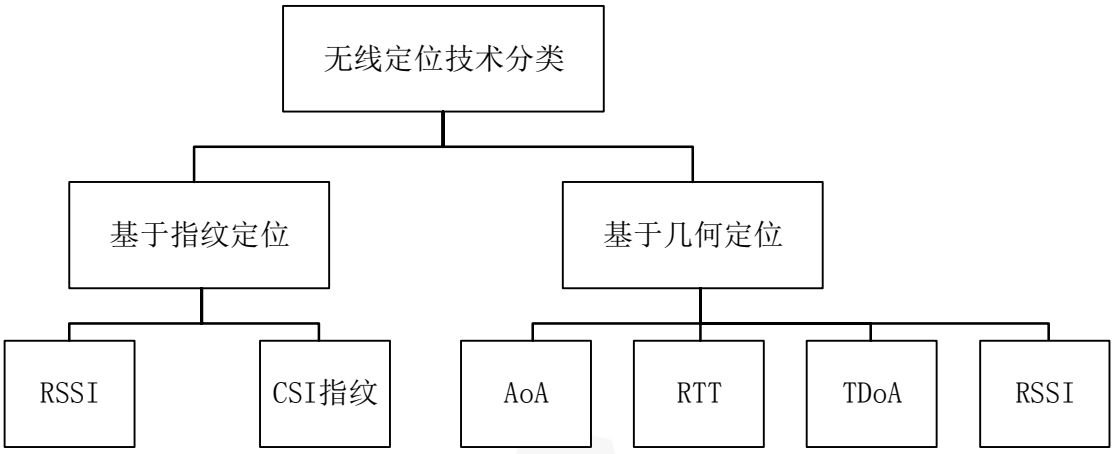


图 16 无线定位技术细分

指纹定位技术是指将实际环境中的位置和接收到的无线信号的“指纹”特征联系起来，一个位置对应一个独特的指纹。将实时获得的无线信号特征与预先建立好的无线信号特征指纹库中的特征数据进行匹配，根据匹配结果来估计信号源的位置。

基于几何的定位技术是利用无线信号的到达角度、时间等参数，根据传统的三角定位、三边定位以及双曲线定位法对信号源的位置进行估计。这些技术最早应用在雷达系统中，通过对接收信号在空、时、频域的处理结合相应的定位技术实现对目标的位置估计与跟踪。

对于不同的无线定位技术，我们可以从以下三个维度进行评估:

1）精度

定位精度是空间实体位置信息（通常为坐标）与其真实位置之间的接近程度。

2）功耗

功耗反应了待定位终端的续航能力。主要依赖于无线信号

的调制方式和刷新率。

3）成本

- 设备成本：用于搭建定位系统所必须购买的设备花销，包括硬件、软件。
- 部署成本：在部署安装定位系统时，投入的人力成本，比如指纹的采集、设备安装位置的调整等。

（2）技术特点

目前，室内无线定位技术有以下几个主流标准：

1）Wi-Fi

Wi-Fi 无线系统中，最常见的为 RSSI 定位技术。AP 接收终端的上行信号，并估计出信号的 RSSI，将 RSSI 送至定位引擎，定位引擎根据三边定位原理计算出终端位置。由于空间环境复杂等多种因素，Wi-Fi 系统中的 RSSI 波动较大，最终的定位精度也仅在 3-7 米。

为了进一步提高精度，可以采用指纹法辅助定位。采用指纹定位时需要首先对指纹库进行建立。将 AP 覆盖区域划分为多个定位方格，采集每个定位方格的 RSSI 特征建立指纹库。在定位时，定位引擎匹配最接近的 RSSI 特征对应的定位方格坐标作为最终位置。该种方式精度可达到 3—5 米。指纹定位部署和维护成本高。

AoA 定位技术测量信号到达角度，不受信号强度波动影响，定位精度高。AoA 利用芯片物理层采集到的 I/Q 数据或 CSI 信息，结合阵列信号处理技术，可在室内环境下实现 1—3 米的定

位精度。但是由于需要特定结构的阵列天线进行角度测量，故该方案在硬件成本上要比RSSI高很多。同时AoA定位的AP需要进行精确角度校准，安装部署成本高。

随着802.11 FTM协议的公布以及主流芯片厂家相继支持该功能，FTM也开始受到业界的普遍关注。由于Wi-Fi工作带宽为20/40/80/160MHz，利用多载波宽带系统可以实现高精度的信号接收时间测量，从而实现高精度的距离测量。通常在80MHz的系统带宽下，FTM的测距精度可以达到1¯2m。随着支持FTM功能终端的普及，基于FTM的室内定位方案会得到广泛应用。

2）蓝牙

在基于蓝牙的无线定位系统中，主流的方案采用基于RSSI的定位技术（指纹或三边定位），其定位方式与Wi-Fi RSSI定位类似。随着BLE标准的发布，具备低功耗特性的标签设备可采用电池供电方式，其续航能力可达数年，这使得蓝牙定位方案十分适用于资产管理。将支持BLE的蓝牙模块集成在网络设备中，在三个广播信道上利用跳频的方式收集标签发送的上行信号并测量出RSSI。基于BLE的定位方案精度可达3 - 5米，略好于Wi-Fi RSSI定位。iBeacon功能也可以实现智能终端的定位。锚点以电池供电的方式被高密度的固定于室内环境中，智能终端会在广播信道上监听周边锚点发送的报文，利用收集到的RSSI信息实时刷新自己的位置。

3）UWB

基于UWB的定位方案主要依赖于三边定位和双曲线定位两种技术，借助于500MHz/1GHz的超大带宽，可以获得百皮秒级

别的时间测量进度。通常情况下 UWB 系统的测距精度可以达到 10¯20cm。部分厂商通过物联网集成的方式，将 UWB anchor 集成于 AP 内，实现了双网合一的低成本高精度定位解决方案。

（3）技术典型应用

表 4 典型定位技术对比

	Wi-Fi RSSI	Wi-Fi指纹	Wi-Fi AoA	Wi-Fi FTM	蓝牙RSSI	UWB
精度	3-7米	3-5米	1-3米	1-2米	3-5米	10厘米
功耗	高	高	高	高	低	高
部署成本	Wi-Fi 建网成本	在 Wi-Fi 建网成本之上，大幅增加了人力成本	在 Wi-Fi 建网成本之上，安装 AP 耗费成本高。	Wi-Fi 建网成本	部署密度略高于Wi-Fi，成本高于 Wi-Fi RSSI	专用设备、网规条件严格，部署成本高。

针对不同的场景，我们可以合理的选择对应的方案进行部署。例如:

对于园区保安巡查管理，对于定位精度要求不高，但要求覆盖全面，成本敏感；可以使用基于 WIFI 的 RSSI 定位技术，基于全面覆盖的 WIFI 网络，提供对保安手持终端的网络侧无缝的定位能力，实时管理保安的巡查的实时监控管理;

对于生产系统的电子围栏，由于涉及人身安全，要求定位精度极高。可以部署 UWB 网络，实现高精度的定位；为人员配发基于 UWB 的工卡或者手环，实现高精度的电子围栏。同时，UWB 网络还可以实现工作任务管理;

对于 AGV 小车，要求精度较高，同时需要有 WIFI 连接以实现任务下发和状态上报。可以部署基于 WIFI 的 AoA 定位，实现 1 米的定位精度；同时，WIFI 网络可以为 AGV 小车提供数据连接，实现上传下载。

1.6 大二层

（1）技术简要介绍

新一代的网络中，由于企业业务强力依赖网络，业务的任何变化都需要网络进行调整以适应；同时，新的业务需求不断涌现，需要网络能够快速响应。因此，网络的敏捷性成为新一代网络的关键特性。为了解决这一问题，SDN 被提出，通过控制器实现业务的自动化部署，从而能够快速的调整网络配置和业务配置。

然而，现有的网络解决方案中，业务和网络拓扑/配置本身是强耦合的，任何业务配置修改都需要考虑网络拓扑现状和现网配置，这就导致控制器的业务逻辑异常复杂，开发周期长，并不能很好的满足敏捷网络的需要。

为了解决这个问题，就需要业务跟网络解耦。如果网络本身是标准化并且业务网络是相互隔离的，控制器就可以聚焦于业务逻辑的开发和配置下发上。大二层技术可以很好地满足网络标准化这一需求。通过在物理网络（underlay)之上，创建逻辑上的叠加网络（overlay），以此实现业务跟网络的解耦，叠加网络可以基于业务实现多实例化，可以实现业务相互隔离。从而实现在不改变基础网络的情况下，实现业务的灵活快速部署。

针对 NVO3（Network Virtualization over Layer 3，跨三层网络虚拟化）技术，除了 VXLAN，IETF 还提出过其他两种技术方案：NVGRE（Network Virtualization using Generic

Routing Encapsulation，采用通用路由封装协议的网络虚拟化）和 STT（Stateless Transport Tunneling Protocol，无状态的传输隧道协议），这 3 种方案都是通过 MAC in IP 技术在 IP 网络上构建虚拟网络。3 种技术方案的对比如下表 5 所示。

表 5 网络虚拟化技术对比

	NVGRE	VxLAN	STT
封装方式	MAC in GRE	MAC in UDP	MAC in TCP
技术实现	NVGRE 采用RFC 2784 和RFC 2890 所定义的GRE 隧道协议，将以太网报文封装在GRE内进行隧道传输。与VXLAN 的主要区别在对流量的负载分担上，因为使用了GRE 隧道封装，NVGRE 使用了GRE 扩展字段 flow ID 进行流量负载分担，这就要求物理网络能够识别 GRE 隧道的扩展信息	VXLAN 是将以太网报文封装成UDP 报文进行隧道传输，UDP 目的端口为已知端口，可按照源端口进行负载分担，标准五元组方式有利于在IP 网络转发过程中进行负载分担	STT 是无状态传输协议，通过将以太网报文封装成TCP 报文进行隧道传输。与 VXLAN 和NVGRE 的主要区别是隧道封装格式使用了无状态TCP，需要对传统 TCP 进行修改

目前最流行的虚拟化技术方案是 VxLAN，VxLAN 具有以下技术优势:

- 不需要对现有网络改造，而 NVGRE 需要网络设备支持 GRE。
- 使用标准的 UDP 传输流量，对传输层无修改，而 STT 需要对传统 TCP 进行修改。
- 业界支持度最好，商用网络芯片大部分都支持这种方案。

（2）技术特点

RFC 7348 定义了 VLAN 扩展方案 VxLAN，VxLAN 采用 MAC in UDP 封装方式，是 NVO3 中的一种网络虚拟化技术。

1）VxLAN 基本概念

● VNI（VxLAN Network Identifier，VXLAN 网络标识）

类似传统网络中的 VLAN ID，用于区分 VXLAN 段，不同 VXLAN 段的用户不能直接进行二层通信。VNI 由 24 bit 组成，支持多达约 1600 万个 VXLAN 段。

● BD（Bridge Domain，广播域）

类似传统网络中采用 VLAN 划分广播域方法，在 VXLAN 中通过 BD 划分广播域。在 VXLAN 中，将 VNI 以 1∶1 方式映射到广播域 BD，一个 BD 就表示着一个广播域，同一个 BD 内的用户就可以进行二层互通。

● NVE（Network Virtualization Edge，网络虚拟边缘）

NVE 是实现网络虚拟化功能的网络设备实体，NVE 间构建 VxLAN 隧道，建立虚拟网络。NVE 根据功能不同可以区分为 Edge 节点或 Border 节点。

● 二层网关

类似传统网络的二层接入设备，在 VxLAN 中通过二层网关解决用户接入虚拟网络，也可用于同一 VXLAN 段虚拟网络的子网通信。

2）VxLAN 网络特点

可以参照表 6VLAN 与 VxLAN 对比，来理解 VxLAN。

表 6 VLAN 与 VxLAN 对比

概念	VLAN	VxLAN
网络存在形式	在逻辑上将一个物理局域网划分成多个广播域，并且将网络范围限制在一个较小的地域范围内	在已有的任意路由可达的网络上叠加的虚拟网络，不受地域范围限制，具备大规模扩展能力
支持的虚拟网络范围	VLAN 作为当前主流的网络隔离技术，在IEEE 802.1Q 协议中定义有12	VXLAN 作为新型的网络隔离技术，在RFC 7348中定义有24 bit，支持多达约

	bit，因此可用的VLAN 数量仅4 096 个。对于公有云或其他大型虚拟化云计算服务这种动辄上万甚至更多租户的场景而言，VLAN 的隔离能力无法满足其需求	1 600 万租户隔离，有效地解决了云计算中海量租户隔离的问题
网络划分方式	通过VLAN ID 划分广播域，同一个广播域之间的主机能进行二层互通	通过BD 划分广播域，同一个BD 内的主机可以进行二层互通
封装方式	在报文中添加VLAN 标签	原始报文在封装过程中先被添加一个VXLAN 帧头，再被封装在UDP 报头中，最后使用承载网络的IP、MAC 地址作为外层头进行封装
网络间互通方式	VLAN间互访通过VLANIF 接口实现，VLANIF 接口是一种三层的逻辑接口，可以实现VLAN 间的三层互通	VXLAN 间互通以及VXLAN 和非VXLAN 之间的通信通过VBDIF 接口实现。VBDIF 接口在VXLAN 三层网关上配置，是基于BD 创建的三层逻辑接口
受益	限制广播域：广播域被限制在一个VLAN 内，节省了带宽，提高了网络处理能力。 增强局域网的安全性：不同VLAN 内的报文在传输时是相互隔离的，即一个VLAN 内的用户不能和其他VLAN内的用户直接通信	位置无关性：业务可在任意位置灵活部署，缓解了服务器虚拟化后相关的网络扩展问题。 网络部署灵活性：在传统网络架构上叠加新的网络，部署方便，同时避免了大二层的广播风暴，可扩展性极强。 适合云业务：支持千万级别租户隔离，支持云业务的大规模部署。 技术优势：采用MAC in UDP 封装方式，无须关注主机的MAC地址，降低了大二层网络对MAC地址规格的需求

对比 VLAN，VxLAN 在物理网络上虚拟化出一个和物理网络拓扑无关虚拟的 VxLAN 网络，便于控制器自动化的对该网络进行业务配置部署；24Bit 的 VNI 扩展能力强，便于实现多租户和 VN。

3）VxLAN 典型组网

VxLAN 网络的典型组网集中式网关和分布式网关组网两种，如图 19、20 所示。基于集中式网关的组网，网络可以被虚拟化为一张一跳的星型网络（或者双星型网络），基于分布式网关组网，网络可以被虚拟化为一张一跳的全连接网络。控制器可以基于这些确定的拓扑，进行多租户或者多 VN 的划分和配置。

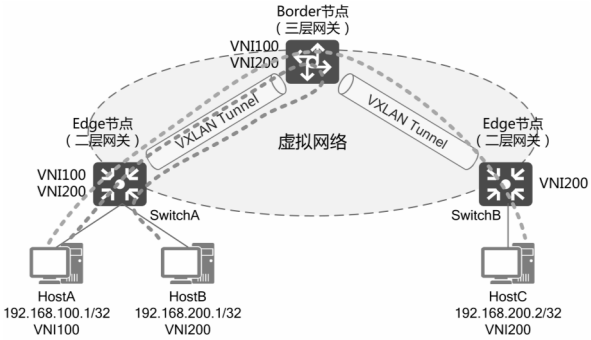


图 17 集中式网关示意图

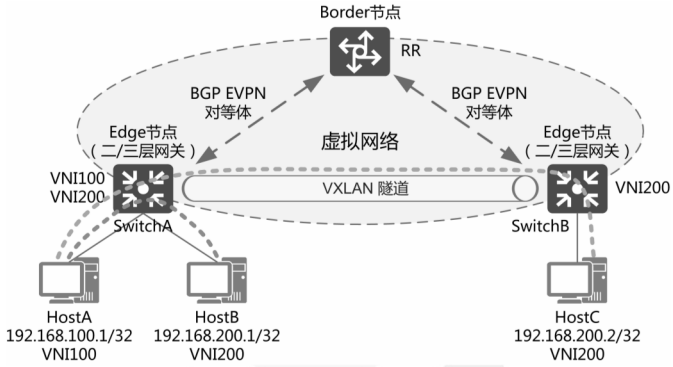
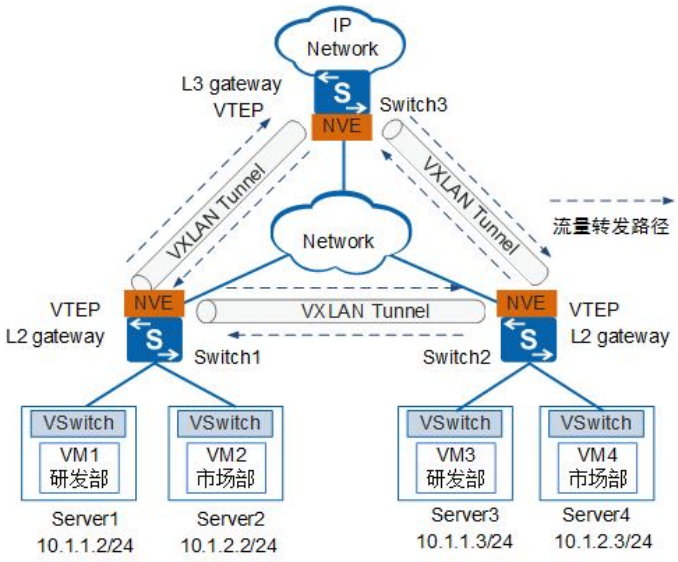


图 18 分布式网关示意图

（3）技术典型应用

某个案例中某企业已经建成比较成熟的园区网络，但是没有专用的数据中心网络，所有的服务器分布在不同的部门，并且不具备集中放置的条件，不同地域之间的服务器依靠园区网络互联。通过 VxLAN 技术，在园区网络之上构建虚拟网络，实现资源整合和业务灵活部署。为了方便管理与维护，将具有同一业务需求的 VM 规划为同一网段，不同业务需求的 VM 规划为不同网段。例如：研发部门的 VM 之间需要互通，属于同网段互通；研发部和市场部的 VM 之间需要互通，属于不同网段互通。



VxLAN 提供数据中心网络之间的二层通信。如图 22 所示，研发部门的 VM 之间进行互通时，Switch1 与 Switch2 作为 VxLAN 二层网关，二者之间建立 VxLAN 隧道，实现同网段终端用户互通。

VxLAN 提供数据中心网络之间的三层通信。例如：研发部与市场部进行互通时，Switch3 作为 VxLAN 三层网关，分别与 Switch1 和 Switch2 建立 VxLAN 隧道，通过 VxLAN 三层网关实现不同网段终端用户互通。

在 Switch 上静态配置 VxLAN 隧道后，VxLAN 网络中 MAC 地址表项、ARP 表项等信息流表均可动态学习得到。所有表项建立好后，通过 VxLAN 隧道，实现同网段与不同网段终端用户互通。

1.7 SDN

（1）技术简要介绍

工业 SDN（Software Defined Networking，简称 SDN）网

络由多种协议的终端设备、可编程的工业 SDN 交换机和集中式的工业 SDN 控制器构成。终端设备通过北向接口向工业 SDN 控制器提交数据的流量特征和传输需求，集中式的工业 SDN 控制器根据流量特征和传输需求，生成工业 SDN 网络的转发规则，通过标准化的南向接口下达到工业 SDN 交换机中执行。

工业 SDN 的核心是通过软件定义的方式，对交换机等网络设备进行管理和配置，同样也可以支持面向未来的 TSN 网络设备。工业 SDN 网络能够支持 IT 设备和 OT 设备的统一接入和灵活组网，为 IT 业务提供高带宽的传输保障，为 OT 业务提供端到端实时性的保障。通过工业 SDN 网络，可以对 IT 和 OT 设备和流量进行统一的监控和管理。

（2）技术特点

转发与控制分离。SDN 具有转发与控制分离的特点，采用 SDN 控制器实现网络拓扑的收集、路由的计算、流表的生成及下发、网络的管理与控制等功能;而网络层设备仅负责流量的转发及策略的执行。通过这种方式可使得网络系统的转发面和控制面独立发展，转发面向通用化、简单化发展，成本可逐步降低;控制面可向集中化、统一化发展，具有更强的性能和容量。

控制逻辑集中。转发与控制分离之后，使得控制面向集中化发展。控制面的集中化，使得 SDN 控制器拥有网络的全局静态拓扑，全网的动态转发表信息，全网络的资源利用率，故障状态等。因此，SDN 控制器可实现基于网络级别的统一管理、控制和优化，更可依托全局的拓扑的动态转发信息帮助实现快速的故障定位和排除，提高运营效率。

网络能力开放化。SDN 还有一个重要特征是支持网络能力开放化。通过集中的 SDN 控制器实现网络资源的统一管理、整合以及虚拟化后，采用规范化的北向接口为上层应用提供按需分配的网络资源及服务，进而实现网络能力开放。这样的方式打破了现有网络对业务封闭的问题，是一种突破性的创新。

（3）技术典型应用

工业园区网络中，工业 SDN 网络在能够保证工业控制业务实时性与可靠性的前提下，提高了网络的灵活性，适合在生产设备经常发生变化的场景中使用，比如个性化定制，柔性生产或批量定制生产。在个性化定制，柔性生产或批量定制生产中，生产过程会根据订单的切换而发生变化，导致生产设备的管理和控制逻辑发生变化，进而影响设备之间的通信关系。与传统工业控制网络往往需要重新组态不同，工业 SDN 网络可以支持设备的灵活组网，重新组网之后的管理和控制业务同样可以得到相应的传输保障。同时，工业 SDN 网络具备网络的统一接入和管理能力，能够快速发现设备重新组网时出现的问题，指导现场人员快速进行处理。

1.8 NFV

（1）技术简要介绍

工业网络通常是由一定规模并且迅速增长的多种多样的硬件设备组成。为了适配一个新的生产业务，通常需要开发新的网络模型，新类型的设备，而为这些设备需找空间、提供电源变得越来越困难；同时还伴随着能源成本的增加、投资额的挑

战，基于硬件设备的复杂度提升，也增加了对设计、集成、运营所需要的各种稀有技能的要求。

更严重的问题是，基于硬件的设备很快就到了生命周期，这需要更多的“设计-集成-部署”循环，但收益甚少。糟糕的是，硬件生命周期变得越来越短而业务创新则在不断加速，所以这抑制了新的部署，并且限制了工业领域的创新。

NFV，即 Network Functions Virtualization（网络功能虚拟化）通过借用 IT 的虚拟化技术，将传统的 CT 业务部署到云平台上（云平台是指将物理硬件虚拟化所形成的虚拟机平台，能够承载 CT 和 IT 应用），从而实现软硬件解耦合。

（2）技术特点

NFV 的本质就是通过虚拟化就是对低层硬件资源（计算资源，存储资源，网络资源）进行虚拟，屏蔽物理实现，供上层应用使用，使用者不用关心使用的是资源的具体物理形态。

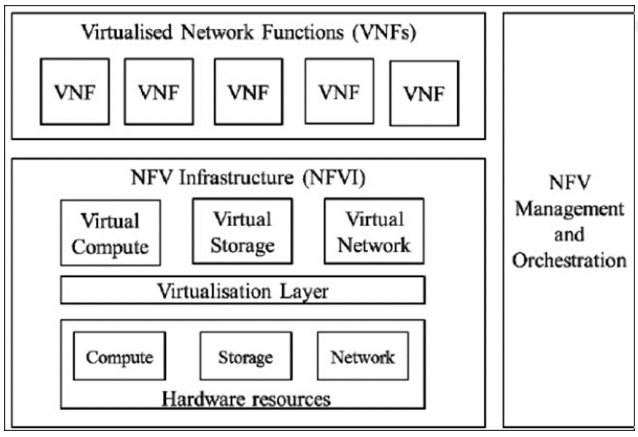


图 19 ETSI NFV 标准架构

图 19 显示了 ETSI NFV 标准架构，包括 NFVI、VNFs、NFV Management and Orchestration（MANO）这几部分，其中：

- NFVI (Network Functions Virtualization

Infrastructure): NFVI 就是云计算结构中的 I 层，它将硬件相关的 CPU/内存/硬盘/网络资源全面虚拟化。

- VNF（Virtualized Network Function，虚拟的网络功能）：作为一个纯软件实现的网络功能，能够运行在 NFVI 之上，对应传统物理网络功能。它们向下看到的资源全部是被虚拟化软件封闭隐藏后的“虚资源”。可以认为它是云计算中 P 层+S 层。其中原有电信设备中的平台层可以对应云计算的 P 层，业务层对应云计算的 S 层。从安装部署的角度来看，VNF 是一个 VM。从软件应用开发商的角度来看，VNF 就是部署在一个或多个互联的 VM 中的软件实现。
- NFV MANO（NFV Management and Orchestration，NFV 管理与编排）：其负责对 NFVI 的软硬件资源的生命周期管理和编排，以及对 VNFs 的生命周期管理和编排。NFV MANO 重点关注的是 NFV 框架下所有的虚拟管理任务。

（3）技术典型应用

NFV 适用于固定、移动，园区，DC 等网络中任何数据面的分组处理和控制面功能。部分例子如下:

- 交换单元: BNG, CG-NAT, 路由器
- 移动网络节点: HLR/HSS, MME, SGSN, GGSN/PDN-GW, RNC, Node B, eNode B
- 隧道网关单元: IPSec/SSL VPN 网关
- 流量分析: DPI, QoE 测量
- 服务保证, SLA 监控、测试和诊断

- NGN 信令：SBC 系列，IMS
- 扩展网络功能的融合： AAA 服务器，策略控制和计费平台
- 应用级优化： CDN、 Cache 服务器，负载均衡器、应用加速器
- 安全功能：防火墙、病毒扫描器、入侵检测系统、蠕虫防护
- 家庭路由器和机顶盒所包含的功能，用于生成虚拟家庭环境
- 工业服务器相关功能

1.9 工业 PON 技术

（1）技术简要介绍

参考工业互联网分层架构，工业 PON 在工业互联网体系架构中主要处于车间级网络位置（图 20），通过 ONU 设备实现现场级设备与上层网络的连接，实现数据采集、生产指令下达、传感数据采集、厂区视频监控等关键功能；通过 ODN 的汇聚以及 OLT 设备，实现与企业生产网和办公网络的联接，从而实现生产线数据到工厂/企业 IT 系统的可靠有效传输。同时，工业 PON 网络也可适用于工厂级网络的承载，可参考现有政企接入网的建设模式，通过 PON 设备进行工厂内办公网络和生产网络的接入网建设。

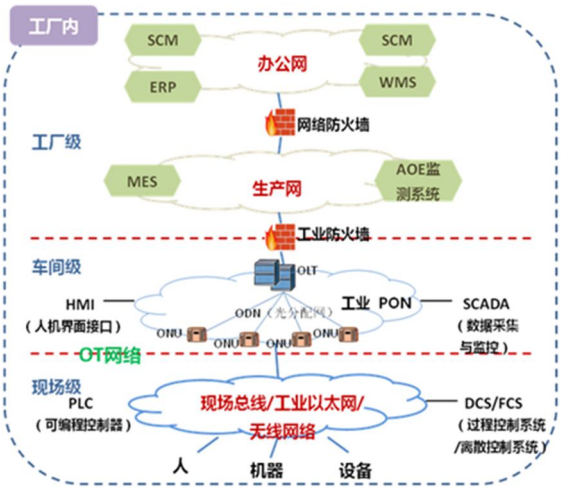


图 20 工业 PON 在工业互联网架构中位置

工业 PON 网络最常用的组网方式是基于 Type D 保护方式的手拉手保护链型组网和星型组网，实现全光路保护，提高了车间通信网络的可靠性，为制造企业的通信可靠性提供了坚实的保障。

（2）技术特点

工业 PON 网络具有以下优点：PON 通过无源器件组网，ODN 网络不受电磁干扰和雷电影响；支持多种保护倒换方式，切换时间短、抵抗失效能力强；点到多点传输架构，终端并行接入，部署灵活；仅需单根光纤线传输，最远覆盖 20 公里范围；多业务承载，支持数据、视频、语音、时间同步等多种业务；高安全性，PON 网络设置 ONU 安全注册机制，下行数据传送支持加密算法，上行数据传送通过时分机制实现不同终端设备上行数据的隔离。

（3）技术典型应用

工业 PON 技术比较多的用于离散型制造场景，由于离散制造车间管理过程较为复杂：生产计划难以预测，产品工艺流程

差异大，设备自动化水平参差不齐，现场单据多，作业繁琐，不易掌控等。

以下案例展示了工业 PON 技术用于工厂部署，将采集到的信号进行协议转换、数据转换和地址空间映射，统一转换成 OPC-UA 协议，通过工业 PON 系统进行传输，实现多业务数据采集和传输。工业 PON 网络的组网方案如图 21 所示。

在这个案例中为客户实现的价值主要体现在：1）实现了网络扁平化和大带宽、多业务承载；2）实现了现场设备的数据采集和分析；3）提高了网络稳定性和安全性。

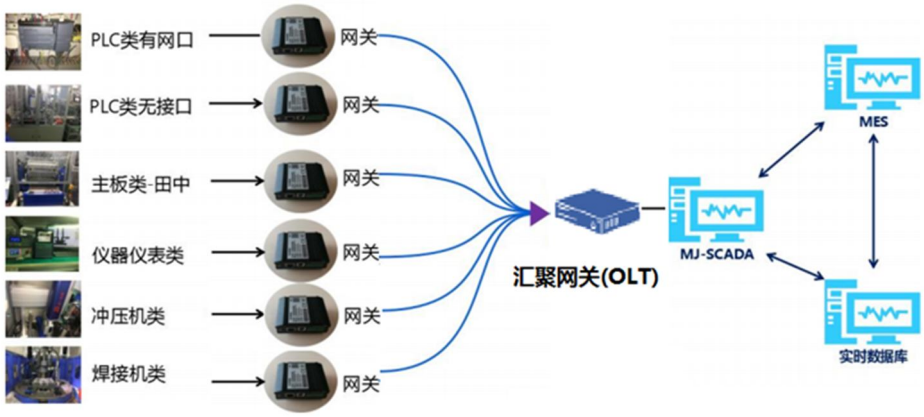


图 21 工业 PON 组网架构

1.10 5G

（1）技术简要介绍

5G 网络技术的蓬勃发展，为前沿信息技术在工业园区领域的应用落地提供支持。大带宽、低时延、高可靠等特性，使工业互联网的智能感知、泛在连接、实时分析、精准控制等需求得到满足，加速了行业智能化升级的步伐。

在工业园区场景中的目标网络架构是以虚拟化技术为基础，实现控制面和用户面分离，核心网控制面（5GC）集中部署在省会城市或者主要城市，核心网用户面转发节点根据业务需求部署在靠近园区用户侧位置，甚至直接下沉至工业厂区，以便于引入网络切片和边缘计算，满足业务多样性需求，同时支持多种接入方式、网络功能微服务化、运营编排智能化等能力，具体如图 22 所示。

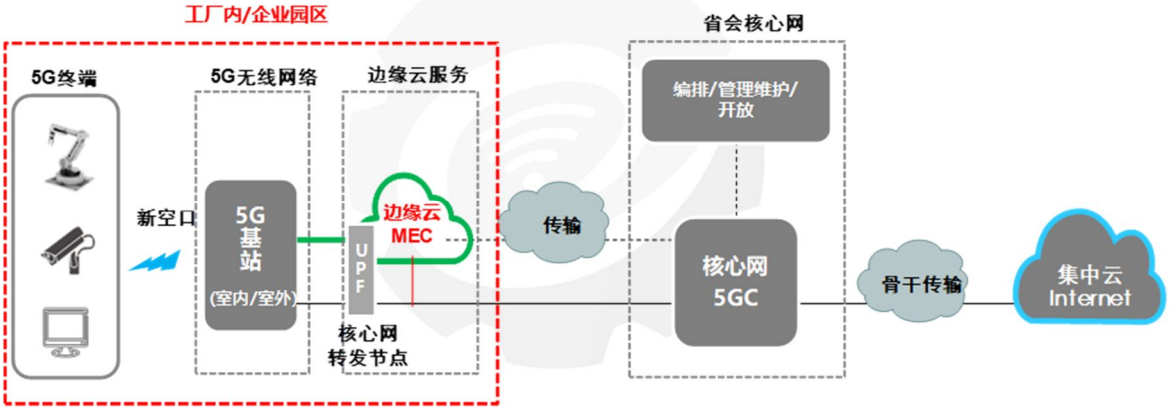


图 22 5G 园区网络部署

（2）技术特点

1）5G 切片特点

网络切片可以将网络资源灵活分配，网络能力灵活组合，基于一张 5G 网络虚拟出多个具备不同特性的逻辑子网络，提供面向不同场景的按需定制网络服务。

2）边缘计算特点

在工业场景下，边缘计算平台可以部署于工厂园区内，工厂的工业互联网平台、ERP 平台、虚拟交换机等系统均可以部署于运营商的边缘计算，实现工业场景的智能制造、无线局域网等场景，同时能够满足数据不出工厂的诉求。

（3）技术典型应用

1）5G 切片在园区的典型应用

技术类型	关键能力	空口技术	核心网技术	园区应用典型场景
网络切片	逻辑资源隔离	● 资源预调度 ● 带宽划分 ● 切片标识识别	● 虚拟化技术 ● 切片选择技术 ● 切片管理开通技术	● 视频监控专用切片 ● 企业专用切片等

2）边缘计算在园区的典型应用

技术类型	关键能力	空口技术	核心网技术	工业应用典型场景
边缘计算	● 本地分流 ● 边缘云服务 ● 用户识别	网络状态信息上报	● 本地分流策略控制 ● 用户地址控制 ● 云服务能力	● AR应用部署在园区边缘云平台 ● 工业互联网平台部署于园区边缘云平台等

附录 2：工业互联网园区网络解决方案

2.1 5G 工业园区场景---海尔智慧工厂

海尔的 5G 工业园区是将 5G 技术应用于一个园区内，连接多个厂房内部 ICT 设施，实现辅助生产和直接生产的数字化、云化。

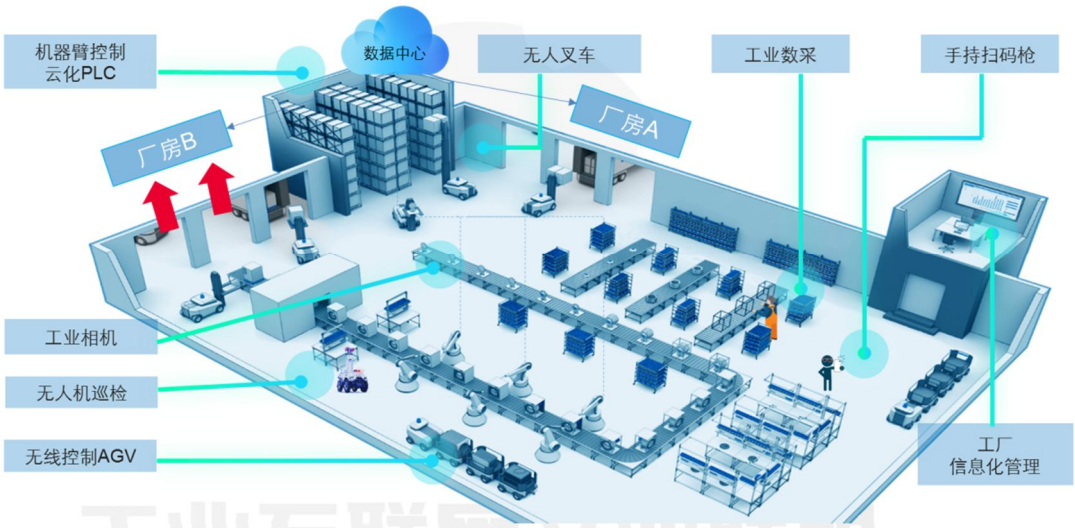


图 23 海尔 5G 工业园区典型应用全景

- 应用场景 1：天津 5G 园区智能监控平台

“天津 5G 园区智能监控平台”是中国电信天津分公司与天津大学共同为企业打造的，针对海量异构的物联网设备，进行实时跟踪检测、大数据统计分析、告警预警的一体化智能监控平台，旨在实现全方位、智慧化的监控、监管。

平台支撑高并发的物联网设备，能够满足十万级别的并发请求；分布式数据库热备，确保系统的高效、稳定；还具备高可扩展性，支持多设备厂商接入。

- 应用场景 2：AR 眼镜安保

园区内从原材料入园区到成品洗衣机出园区中各个生产、

运输环节需要多方人员配合。不同生产工作区域人员准入的权限不同。之前，对重要区域内非法进入人员的辨识完全依靠安监人员的“人眼”识别和“人脑”判断。现在安全监管人员可借助佩戴的 AR 眼镜，实时采集现场图像、通过 5G 回传至平台的图库进行比对，智能分析判断后，发现非准入的人员后眼镜将发出告警至监管人员，大大提高的准确性和工作效率。

● 应用场景 3：生产线视觉检测

原来对冲压钢板的品质检查，依靠质检人员人工完成。一个质检人员最多时需要对每块钢板在加工环节中检查十多个项目，人工识别及疲劳漏检的几率很大。

通过在冲压各环节上安装工业摄像机、利用 5G 网络实现与后端品控平台的通信、使用平台预置的品控算法判断检测、及时发现不合格产品（表面划痕、凹坑、冲孔不良等）并发出告警。

视觉检测在生产品控中的应用，大大提高了生产效率、提升了产品质量、降低了劳动强度。

● 应用场景 4：机器人(地面)巡逻

(地面)机器人实现园区内定期、规划路线和点位的巡逻检查，并通过覆盖园区的 5G 网络将高清视频回传到“天津 5G 园区智能监控平台”查看并分析。同时机器人的热成像技术，在夜间也可清晰看到每个细节，提高了巡逻效率减轻了安保人员劳动强度。

● 应用场景 5：无人机(高空)巡逻

对大面积园区进行全域巡逻、快速发现安全生产风险点

（比如火灾、气体泄漏等）之前除依靠人工加强巡逻的方法外，也没有较好的手段。现在，应用无人巡逻机可从立体、全域的视角空间进行厂区巡逻，将高清视频信号从无人机回传至监控平台进行分析处理，可以更有效地发现风险并快速处置，确保园区安全。

- 应用场景 6：智能讲解机器人

智能讲解机器人可以根据展馆特点，引来宾前行并进行演示项目的讲解。还可通过个性化的声音、语调等使讲解妙趣横生，不再单调乏味，来宾参与感更强。

在讲解过程中机器人可随时将现场来宾提出的问题通过 5G 网络上传中央控制平台，平台根据现场情况，经过 AI 计算后将最适合的回复内容通过 5G 网络下发至机器人回复来宾问题或引导来宾继续前行。

- 应用场景 7：智能井盖

监测器安装于井盖上，用于监控井盖开启状态和水位状态，当开启状态发生变化时，通过“天津 5G 园区智能监控平台”，即可自动将警情发送到井盖管理与施工的各方面人员。

- IP68 防水，防腐蚀、防爆、抗震、抗紫外线材质
- 低功耗设计，待机 3 年以上
- 支持 NB-IoT 通讯

- 应用场景 8：智能垃圾桶

园区内垃圾点位分布广泛，清运工作复杂。垃圾箱满溢后，管理人员往往后知后觉。通过智能垃圾桶监测终端，可让清洁人员掌握垃圾动态，及时对垃圾进行处理。

智能垃圾检测设备，通过超声波对垃圾箱满溢程度进行监控，一旦垃圾超过限制高度，随即触发告警信息，通过 5G 网络，将垃圾箱所在位置、编号等信息告知“天津 5G 园区智能监控平台”，实现对垃圾箱状态实时监控。

● 应用场景 9：智能路灯照明

传统路灯控制落后、亮灯率低、能耗高、运维效率低、成本大。园区采用智能路灯照明后，可远程调整、实时监控路灯开关和亮度。根据历史数据查询统计，通过大数据分析，找到最适合园区企业的用电方案，降低能耗。

通过“天津 5G 园区智能监控平台”，所有路灯的运行状态一目了然，方便管理人员及时、快捷地维护路灯，提高工作效率。

● 应用场景 10：智能停车管理

通过智能停车管理，实现园区内停车智能化管理。

- 停车位占用管理：园区内停车位占用情况一目了然；
- 非停车区域占用管理：非停车区域当出现车辆滞留时，可以直接通知管理人员赶到现场，及时制止占道现象；
- 僵尸车辆监控：对长期占用车位进行监控，有效排查僵尸车。

地磁感应设备安装于需要监控的点位上，通过园区内的 5G 网络回传至“天津 5G 园区智能监控平台”，所有点位的运行状态一目了然，方便人员管理，提高工作效率。

● 应用场景 11：智能烟感

园区就是一个微缩的服务员工生活的小社会，借助 5G 的万

物互联，天津海尔洗衣机工厂已经实现了园区消防烟感智能化管理，实现了对重点区域消防的预警检测。当烟感探测器监测到有烟气危险时，立即通过 5G 网络将警告信息上传至“天津 5G 园区智能监控平台”，通知预设管理人员处理。

2.2 矿山园区网络建设

（1）场景描述

我国煤炭资源赋存丰度与地区经济发达程度呈逆向分布的特点，使得煤炭行业工业互联网的建设起步较晚，就单一矿山园区（非露天矿山园区）而言，煤矿（仅单一矿山园区）相对于一般工业园区覆盖区域较广，地面环境与常见园区无异，但采掘作业工作面距地面调度室距离可达数十千米，矿山园区环境较常见园区环境而言也具有极大的特殊性。矿山园区井下有瓦斯等爆炸性气体，矿尘大、潮湿、有淋水，巷道空间狭小，巷道弯曲、分支等都制约着地面园区工业互联网技术直接在煤矿井下应用。

（2）网络建设现状

矿山园区的网络发展主要经历了两个阶段:

第一阶段：矿山园区工业互联网包括千兆工业以太环网及无线网络，实现信息井上下高速，建立可靠传输。

第二阶段：矿山园区工业互联网融合井上下千兆/万兆工业控制网络、矿山 4G/WIFI 网络等，实现井上下视频数据、语音的一体化传输；融合数字程控调度通信、移动通信、扩播通信及广播通信系统，实现统一调度、互联互通。

矿山园区网络主要涉及主干网、感知网、生产调度指挥中心网络以及计算资源建设。主干网建设包括井上、井下千兆及以上高速工业以太网和调度指挥控制中心工业以太网建设。感知网建设主要包括利用无线传感器网络建立覆盖全矿井，并与主干传输网络相结合的无线自组网系统，并结合其他无线网络如 RFID 网络、WiFi 网络以及无线通信网络，以实现井上、井下全面感知。目前，大部分矿山园区已经建立煤矿井上下 1000M 工业以太网环网+宽带无线通信网+无线传感网的一体化工业网络体系，实现矿山自动化控制、工业视频、安全监控与人员定位等多源信息、异构网络的融合，其中传输主干网建设以现有的数据传输主干网为基础。

矿山园区（非露天矿山园区）生产环境具有特殊性，煤矿园区网络当前存在以下问题:

- 电磁波传输衰耗大。煤矿井下空间狭小，有风门、机车等阻挡体，巷道介质、弯曲、分支、倾斜、表面粗糙度、巷道支护等会影响电磁波的传输，传输衰耗大。
- 无线发射功率不能超过 25W。本质安全型防爆电气设备的最大输出功率为 25W 左右。当电路中有电感和电容等储能元件时，将进一步降低电路中允许的最大电流和电压，功率也大大降低。
- 网络传输干扰强。煤矿井下空间狭小、机电设备相对集中、功率大，电磁干扰严重。特别是大功率变频器、大型机电设备启停、架线电机车电火花等对网络传输的干扰大。

- 传输距离相对较远。煤矿（仅单一矿井）相对于一般工业企业覆盖区域较广，采掘工作面距地面调度室距离可数十千米。
- 电源电压波动大。煤矿井下电网电源电压波动范围在75%-110% 之间，甚至达 75%-120%。
- 设备故障率高。煤矿井下环境恶劣，设备故障率高，顶板冒落等会造成电缆和光缆断缆、设备损坏。因此，网络设备需要具有较强的抗故障能力，当系统中某些设备发生故障时，不会造成整个网络瘫痪。
- 设备体积受限。煤矿井下空间狭小，因此，对煤矿物网络设备的体积有严格的限制和要求。

（3）工业场景现场场景和环境描述

煤矿生产环境恶劣，主要有瓦斯、煤尘、水、火和顶板五类灾害，并伴有空气湿度大，有害气体成分复杂、通风情况复杂、运输条件复杂等各类威胁。为了保障生产的顺利进行，目前已形成了基于矿井数据监测、通讯联络、视频监视等为基础的保障方式。

- 数据监测场景

为了预防瓦斯、煤尘、水、火和顶板等灾害的发生需通过各类传感器将井下各处的供电情况、设备设施状况、顶板压力、空气成分、风速风量、人员分布、水位高低等各类数据进行采集，传递至地面机房或调度室。

- 通讯联络场景

为了实现井上下语音信息的实时互通，应急指挥等要求，

需要通过本质安全型调度电话、矿用程控调度交换机(含安全栅)、防爆 wi-fi 移动电话等设备进行实时通信；通过防爆喇叭、防爆显示屏等设备对运输状态和灾害发布进行实时调度。

● 视频监视场景

为了对生产现场的违规行为、可疑目标、潜在威胁等突发事件进行直观的反映，需要进行实时视频监控。

工业生产网络要通过有线或无线两种方式进行数据传输。这类网络对实时性、可靠性、安全性和数据完整性有很高的要求。需要考虑传输信息的周期性、优先级、实时性、任务的紧要性以及网络安全等因素。依据煤矿业务需求的不同，网络层传输的信息主要为数据、语音和图像，这三种信息的特点和传输要求各不相同。

数据是指监测监控系统产生的数据，这些数据直接关系到煤矿各种子系统的运行，而数据传输的物质基础和载体为数据传输网络，数据的传输要求有很高的可靠性和实时性，其优先级明显要高于语音信号和视频信号。监测监控系统的数据涵盖井下和井上监测监控系统数据，包括环境数据（温度、湿度、气体浓度、煤尘浓度、风速、风量、矿压、微震等）、设备运行状态数据（运行、停止、温度、振动、转速、电压、电流、正常、故障等）、设备控制命令等。采集数据的主要设备和手段是通过各种智能传感器，各个监测监控子系统中的智能传感器把采集的数据通过有线或无线的方式传输到监控分站或网关，由监控分站接入到数据传输网（主干传输网），进而传送到地面传输网络或监控中心。

语音信号主要是生产调度电话、扩音电话、无线移动通信等系统产生，采用矿用有线通信网络传输语音信号的优先级高于视频信号。语音传输网络是实现井上下联系的重要途径，也是矿井通信系统的主要组成部分，其在煤矿安全生产调度、安全避险和应急救援中发挥着重要作用。语音传输网络需要由矿用调度通信网络、矿井移动通信网络、矿井广播通信网络、矿井救灾通信网络等组成。

煤矿监视信号是从各个分散的监视点将视频信号集中到地面调度中心，信号基本是从下而上的，视频监测信号中又分为重点监测区域和一般监测区，尽管视频监测信号对于人来说非常直观，但是它难以反映系统参数的变化，仅反映外观现象，因此其优先级最低。煤矿视频监控网络主要由井下和井上现场视频采集、视频传输、视频处理以及视频监控等部份组成。井下现场视频采集由矿用隔爆摄像仪实现，摄像仪的视频信号传输接口类型主要有光口、以太网接口、WiFi 无线等。根据不同的接口类型，视频信号可通过光纤、电缆或 4G、WiFi 无线传输。

目前综合信息传输网络的需求逐渐成为主要需要，这种以千兆以太主干环网+接入网+监测监控子系统+语音通信子系统+视频监控子系统为工业网络体系的综合信息传输网络中需要以千兆以太主干环网以数据传输网主干网为基础，接入网根据需要采用不同的接入方式来解决各个子系统的组网形式，在接入方式的需求中包括有线接入方式（电缆或光纤）的需求、无线接入方式（包括 WiFi、ZigBee、RFID、无线基站等）的需求。综合信息传输网也是目前矿山园区工业互联网的雏形，随着矿

山园区工业互联网应用技术的成熟，接入到综合信息传输网中的子系统会更多，传输的信息量会更大，这对传输骨干网的带宽会提出跟高的要求。因此，万兆矿山园区工业互联网环网是未来矿井传输主干网的发展趋势。

矿山园区工业互联网首先要保障数据传输的实时性、可靠性，其次矿山园区工业互联网需要解决不能组成快速冗余环型网络且不能快速收敛的问题，再次还需要解决在恶劣的电磁、高温、高湿、爆炸等环境中长期使用丢包的难题。矿山园区工业互联网要求传输带宽很高，针对不同应用需要达到 10Mbit/s、100Mbit/s、1000Mbit/s 到 10Gbit/s 的传输速度，在任何状态下全线速转发不丢包。同时，就网络设备而言矿山园区工业互联网还继需要实现在硬件技术上实现了设备的本质安全，低耗节能等特点。

（4）安全需求

矿山园区工业互联网是面向生产过程中的传输网络，对于网络安全性有着极高的要求。需要防止利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行攻击，工业互联网络需要保证其独立性，工业互联网要与办公网络和互联网进行物理或逻辑隔离，同时需要在网络的各个环节尽可能多的提供安全保密措施，来保证网络的安全性能。所采用的设备均需保证通过国家本质安全型认证。