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

基于工业互联网标识的园区网络应用蓝皮书

工业互联网产业联盟（AII）
2026年6月

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

基于工业互联网标识的园区网络应用蓝皮书

工业互联网产业联盟（AII）

2026 年 6 月

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

编写说明

牵头编写单位：中国联通研究院

参与编写单位（排名不分先后）：中钢集团邢台机械轧辊有限公司、华为技术有限公司、东集技术股份有限公司、联通华盛通信有限公司、中国信息通信研究院、联通雄安产业互联网有限公司、联通数字科技有限公司、中国联合网络通信有限公司黑龙江省分公司

编写组成员（排名不分先后）：

中国联通研究院：史可、贾雪琴、韩政鑫、曹畅、张岩；

中钢集团邢台机械轧辊有限公司：朱新宁，李超，郑培青，杨卜；

华为技术有限公司：张镇伟、张婷、吴应根、张印熙；

东集技术股份有限公司：于海斌、金明明、寇玉龙、叶文宁；

联通华盛通信有限公司：衣莉莉、孙阳阳、王海涛、王振宇；

中国信息通信研究院：张恒升、陈洁；

联通雄安产业互联网有限公司：胡华磊、罗园、高少品、安自鹏；

联通数字科技有限公司：刘岩松、崔马剑、崔莹莹、范勇杰；

中国联合网络通信有限公司黑龙江省分公司：张笑泳、董建、张莹。

1. 愿景

传统园区信息化建设主要是为邮件、上网等办公业务服务，已经远不能满足数字化转型的需要，工业园区网络正在向提供超宽、极简、高品质体验和智能运维的方向发展。同时也将进一步融入新技术，以支持网络服务、园区业务、应用和终端的不断演进。

工业互联网标识解析体系作为工业互联网网络架构的重要组成部分，不仅是支撑网络互联互通的基础设施，也是实现数据共享的核心。将工业互联网标识与高品质万兆园区网络相结合，依托统一的工业互联网标识解析体系，在不升级存量工业终端 / 设备硬件、不改造固件的前提下，通过网络侧与外置辅助载体联动，实现工业终端的极速安全入网，以极简统一的网络架构支撑多工业终端厂商的数据互联互通，并依据工业互联网标识解析出的网络性能要求数据,为不同的工业终端、业务提供新的网络体验。这既能确保网络的高可靠性和业务的零中断，也极大简化了网络管理员的运维工作。

本蓝皮书聚焦园区网络与工业互联网标识的融合创新，研究基于工业互联网标识的工业园区网络技术方面的创新方案，助力工业园区端、网、云等产业链端到端协同、智能化发展，希望为工业企业数字化的推进提供支持与帮助。

2. 核心价值

2.1. 终端统一身份标识，极简安全入网

在工业园区网络中，不论是在工业办公区域，还是工厂生产区域，均存在大量物联网（Internet of Things，IoT）终端通过以太网（Ethernet，Eth）/WiFi/5G 等方式接入到园区网络中，覆盖了从工业办公区域到工厂生产区域的广泛场景。这些工业终端数量多，种类多，厂商多，往往资源受限（内存、CPU 等），且由于缺乏统一的身份标识体系以及传输协议，导致各工业终端在园区网络上的身份识别通常只能采用终端 MAC 地址，基于终端 MAC 地址做园区入网的准入控制。这样的方式存在以下两类问题：

- MAC 地址易被仿冒带来的安全风险。在园区网络中，最常见的仿冒行为，可以轻松的将 PC 的 MAC 地址修改为工业终端的 MAC 地址，由此该 PC 即可通过网络认证并获取到相应的工业终端的网络权限，会给园区网络带来极大的安全隐患。
- 随机 MAC 导致的基于 MAC 认证机制失效。工业无线化的趋势越发明显，越来越多的智能工业终端均可采用 WiFi 接入网络，而且部分终端默认采用随机 MAC 方式接入，这意味着该 MAC 地址无法成为该终端的唯一身份标识，使得传统基于 MAC 认证的网络准入控制方式失效。

为了解决上述问题，建立一种统一的终端身份标识体系对于工业园区网络的准入安全至关重要。这一体系需要跨越传统的身份标识方式，实现不同技术域的策略协同。具体而言，基于工业互联网标识解析体系的园区网络准入控制系统可以很好的解决MAC地址作为终端身份标识面临的相关问题，使每个终端均有全球唯一的身份标识，且难以仿冒；基于全球统一的标识解析系统，网络准入控制系统通过统一的API即可获取丰富的终端信息，为终端在网络上的可视可控可管提供了强有力的支撑。通过这种跨域的策略协同，网络准入控制系统针对新终端可内置标识、存量终端不升级仅通过网络侧关联标识,实现了终端身份标识的统一和难仿冒性，还为终端在网络上的可视、可控、可管提供了强有力的支撑。这有助于提升工业园区网络的整体安全性和管理效率，推动工业互联网的深入发展。

2.2. 精细化网络切片，策略随行

工业运行的各类指标数据至关重要，稳定可靠的网络是确保“数据上得来，智能下得去”的基础。随着工业IP化的发展，IP网络已成为承载多样化工业IoT业务的统一平台，有效避免了重复建网与繁复的网络维护工作。然而，这一模式也带来了新挑战：

- 性能需求的多样化：不同工业IoT业务对网络性能（如

带宽、时延、抖动等）有着各异的需求。如何使网络自动感知并响应这些具体诉求，为各业务提供定制化的性能保障，成为亟待解决的问题。

- 安全隔离的严格要求：基于安全考虑，各 IoT 业务间通常需保持隔离，不允许直接互访。这要求网络能够自动识别各业务所需的开放端口与通信对象，并迅速部署相应的访问策略。

由此可见，对工业终端业务所需的网络质量、网络安全诉求的自动感知，是提升工业 IP 网络一网承载品质的重要基础。

基于工业互联网标识解析体系和主动标识载体，对新终端可在内部置入工业互联网标识；对存量工业终端及设备不升级、不置入标识，由网络侧通过终端唯一物理特征关联全球唯一的工业互联网标识，并将终端对网络的性能、安全策略诉求等信息预置到工业互联网标识解析节点，为网络感知工业终端、网络与终端协同提供了一种有意义的解决方案：当终端接入 IP 网络时，向网络提供代表其身份的工业互联网标识，IP 网络即可通过工业互联网标识解析系统获取到终端对网络的性能、安全策略诉求等信息，智能为终端划分可独立使用的网络切片，确保带宽不会被其他业务所抢占；同时可根据标识获取到终端对网络访问权限的诉求，自动的生成网络安全策略；做到真正的网络业

务跟随终端而行，无论终端在 IP 网络的任意位置接入，均可获取到相同的业务体验。

2.3. 应用-网络-终端信息共享，提升园区网络品质

园区网络工业系统的基本模型可以抽象为由部署在云、边缘云或者数据中心等设施之上的工业应用、部署在工业现场的工业终端以及连接两者的园区网络组成，见图 1。为了满足工艺流程、生产调度、运行维护等各方面需求，工业应用通过网络从终端获取数据或者向终端发送控制指令。

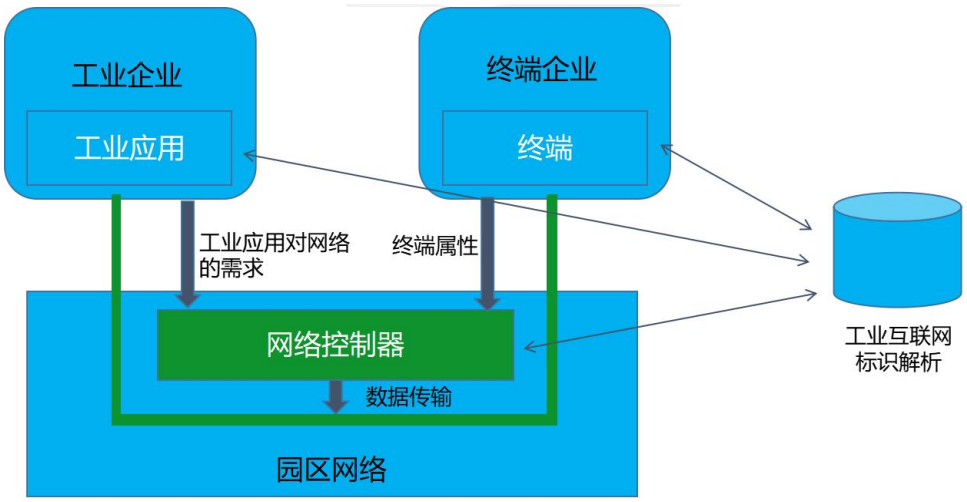

图 1 园区网络工业系统基本模型

当前，由于工业应用、园区网络以及终端三者之间的信息缺乏共享机制，工业应用、终端、网络无法高效协同，导致园区网络不能高效地在同一张网络上同时承载运动控制、基于视觉的生产控制、超低时延的相关业务等。

工业互联网标识解析系统为工业企业、终端生产企业、网络运营企业提供了信息共享的有效机制：工业企业将工业应用的相关信息（如端到端时延、网络带宽、网络抖动等）发布在工业互联网标识节点上；终端生产企业也将终端的软硬件属性（如网络协议、网络带宽、CPU、存储空间等）发布在工业互联网标识节点上；当工业应用与工业终端发生数据交互时，网络可从工业互联网标识节点获取工业应用和终端的相关信息，从而形成有效的网络性能保障策略。

3. 高品质园区网络技术框架与关键技术

3.1. 技术框架

高品质园区网络基于工业互联网标识解析系统，借助工业互联网标识贯通工业应用的网络传输策略、终端属性信息与园区网络控制，为云/网/边/端高效协同、智能生产提供重要技术基础。该种网络不仅强调极速接入、极简架构、极致体验和极简运维，还以工业互联网标识为纽带，实现园区内数据要素的动态流动与信息共享。

如图 2 所示，工业终端通过蜂窝网络、WiFi 或者以太网络接入到园区承载网络，来自工业终端的业务数据通过接入网、园区承载网最终到达企业平台。

为了保障工业终端可信，高品质园区网络的网络 SDN（Software Defined Network，软件定义网络）控制器与主动标识载体服务平台、工业互联网标识解析节点等对接。高品质园区网络的 SDN 控制器作为核心组件，负责智能地管理和优化园区网络。SDN 控制器与工业互联网标识解析系统、主动标识载体服务平台等对接，实现终端的身份验证、网络策略的动态配置与优化。通过综合分析园区网络各网元状态，利用机器学习等技术，SDN 控制器可动态推演出最优的网络配置方案，并发送给相应网元以完成网络性能保障。高品质园区网络可以部署为单独网络，也可以跨多个运营商网络实现互联互通。SDN 控制器的智能管理能力使得网络能够灵活适应不同运营商网络的环境，确保终端在任何位置都能获得稳定的网络接入和优质的服务。

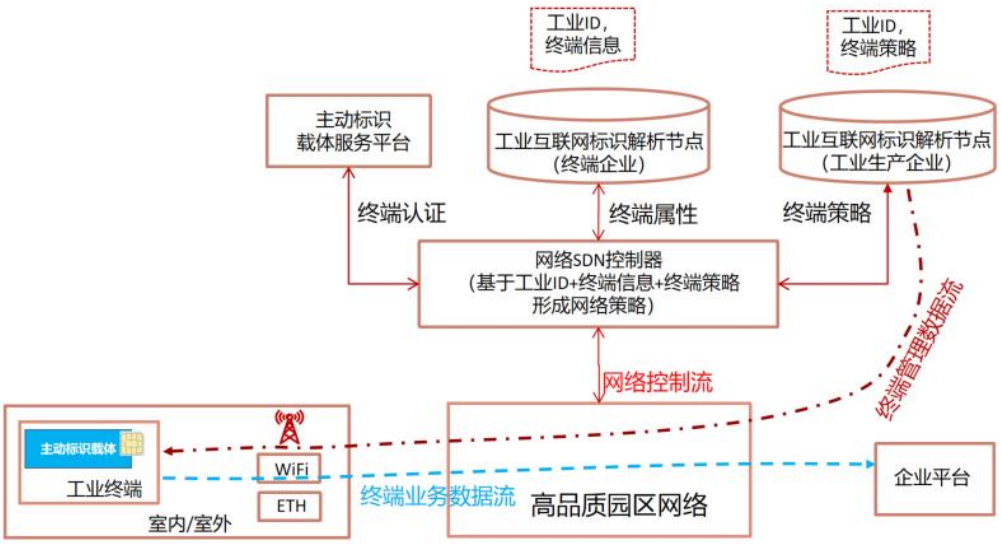

图 2 基于工业互联网标识的高品质园区网络方案架构

主要功能说明如下：

主动标识载体服务平台对来自工业终端的工业互联网标识及凭证进行验证，以验证工业终端的身份；

工业互联网标识解析节点包括为终端企业服务的节点（简称终端企业节点），也可包括对工业企业服务的节点（简称工业企业节点）。其中终端企业节点中可包含终端的工业标识、终端属性等信息；工业企业节点中可包含终端的工业标识、工业应用的端口号、工业应用对网络带宽、时延和抖动的策略等。

当工业终端入网时，工业终端需要向网络 SDN 控制器上报工业标识。通过该工业标识，一方面，网络 SDN 控制器从工业企业节点获得相关工业终端的网络策略；另一方面，网络控制器从终端企业节点获得工业终端属性信息。基于以上信息综合分析园区网络各网元状态后，利用机器学习等技术，网络控制器可动态推演出最优的网络配置方案，并发送给相应网元以完成相应的网络性能保障。

本方案架构可有效支持园区网络的极速接入、极简架构、极致体验和极简运维四大特征，呈现园区网络高品质特点。

3.2. 工业互联网标识解析系统

工业互联网标识解析系统的整体架构采用分层、分级模式构建，系统主要元素包括国家顶级节点、递归节点、

二级节点、企业节点，见图 3。工业互联网标识解析系统既能够与国际上各种主要标识解析体系根节点实现互联互通，也能够面向各行业、各类工业企业提供标识解析服务。

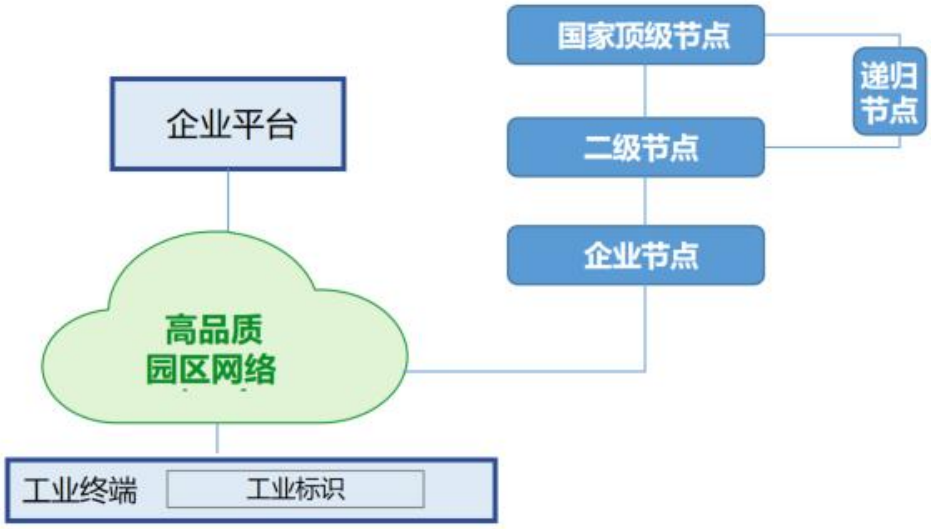

图 3 工业互联网标识解析系统

国家顶级节点能够面向全国范围提供标识注册分配、解析、审核认证及数据托管等服务，并为行业节点和企业节点提供查询指引，中国已经建立北京、上海、重庆、广州、武汉 5 个国家顶级节点，以及南京、成都 2 个灾备节点。

递归节点由运营商参与建设，通过提供递归解析服务来支持标识解析系统运行，通过缓存等技术手段提升整体服务性能。递归节点收到来自终端的标识解析请求，首先查看本地缓存是否有查询结果，没有则返回应答路径查询，直至最终查询到标识所关联的地址或者信息，返回给终端，

并将请求结果进行缓存。

二级节点以行业、区域第三方服务龙头机构为主，负责面向行业或区域提供标识编码注册和标识解析服务。

企业节点则是边缘端的标识管理与解析节点是连接工业企业与设备的节点，用于企业内部提供对工业设备的标识解析和访问服务。

工业互联网标识解析能够根据工业标识（即工业标识编码）查询目标对象所在网络位置，对机器和物品信息进行唯一性的定位和信息查询，是实现工业系统的各种元素互联的问题、产品全生命周期管理和智能化服务的基础和前提。

高品质园区网络以工业标识为纽带，连通园区网络、平台、安全，畅通数据要素在园区各个环节的动态流动，实现有效的信息共享和数据交互，可赋能工业设备的数据采集应用、园区网络服务、产业链信息共享、安全保障等多个层面，促进工业园区更好的发挥产业集聚优势和产业链协同治理能力，构建更加开放的协同生态体系。

3.3. 主动标识载体服务平台

主动标识载体服务平台承担的主要功能是管理企业提供的载体标识，并向企业开放数据认证的功能，针对无法搭载主动标识载体的存量工业终端及设备，支持通过网络

侧端口、物理位置、固定 IP 等信息与标识绑定映射，保证企业侧收到的业务数据的安全性，完整性。该平台由主动标识载体管理模块和安全认证服务平台模块两部分组成。

(一) 主动标识载体管理模块

主动标识载体管理模块是面向企业侧开放的数据录入功能模块。保障数据安全是数据录入的前提。系统管理员可在该模块中新建用户，为企业客户提供账号，控制随意注册的风险。企业客户通过得到的账号登录后，即可在系统进行数据录入以及绑定操作。主要包括工业标识、UICC 卡和终端信息，以及三者之间的绑定关系等信息。除了手动录入外，载体管理模块同时也向企业平台提供相关的操作接口，方便平台直接的接口调用操作。基于信息保护原则，载体管理模块不会对企业信息进行额外的存储操作，而是会通过透传的方式，将数据直接存储在安全服务认证平台上，控制存储范围，降低泄露风险。

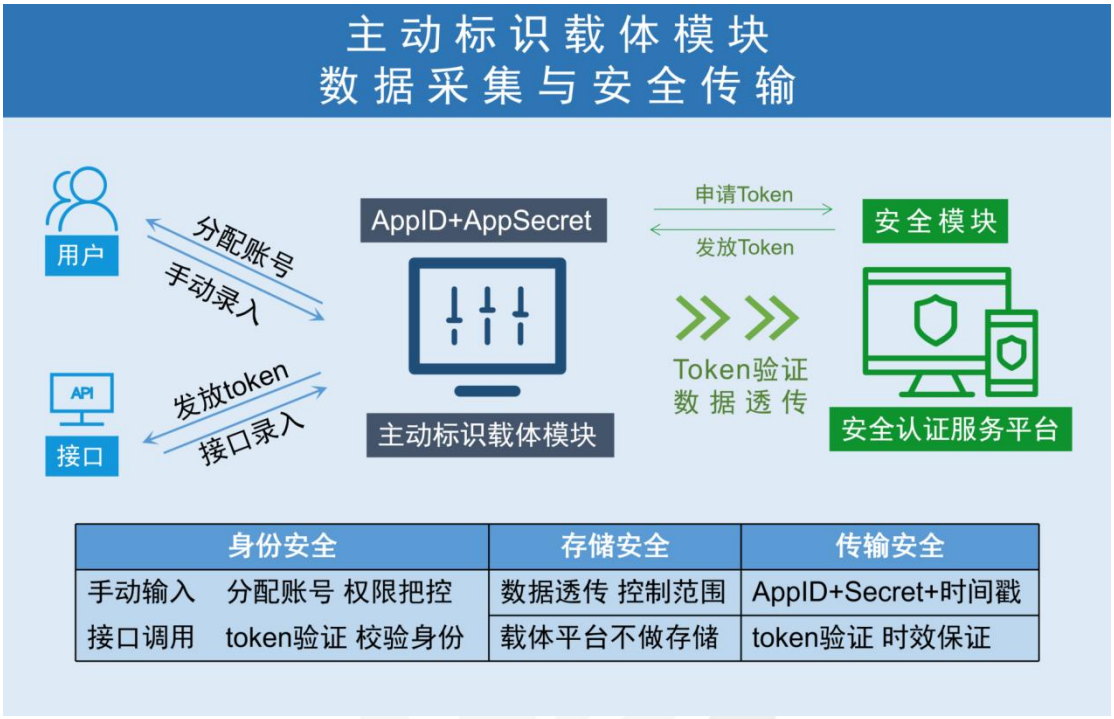

图 4 主动标识载体管理模块

主动标识载体管理模块通过权限控制及 token 验证来保证数据录入的合法性。管理模块为每个用户提供具有唯一性的 appID 和 appSecret 号。在和安全认证平台交互时，主动标识载体管理模块会将这两者连同请求时的时间戳，一起发送给安全认证平台，后者根据接收到的信息生成唯一的 token 并设置相应的有效期，随后将 token 和有效期信息反馈给载体平台。载体管理模块的每一次请求，都需要携带该 token，安全认证平台在收到请求的同时，会验证 token 的时效性以及正确性，两者都验证通过后才会进行数据处理操作，从数据源头保证了数据的安全可靠性。

（二）安全认证服务平台

安全认证服务平台是保证业务数据安全可靠的主要模

块之一。其核心作用在于帮助企业数据服务平台验证其终端业务数据的合法性以及完整性，确保系统数据安全可靠，为业务运行保驾护航。安全认证服务平台的认证服务主要体现在给企业终端侧颁发证书和向企业平台侧提供数据验证服务两个方面。通过接收企业侧提供的工业 ID，卡 ID，终端信息以及三者之间的绑定关系等，来向 CA 申请数字证书，并在工业终端初始化时，将证书和工业 ID 颁发给工业终端，这是颁发证书的服务流程。而验证服务的流程是在企业平台侧接收到来自企业终端侧上传其收集的业务数据后，可以向认证平台发起验证申请，从而确保数据来源是未被篡改，未被伪造的，保证了企业业务安全。

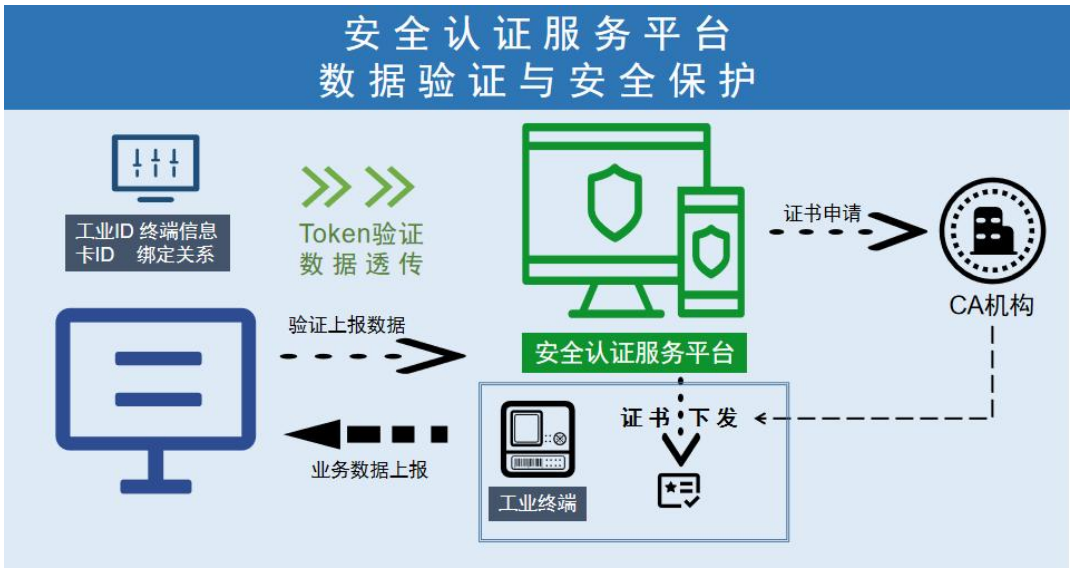

图 5 安全认证服务平台

安全认证服务平台采用数字签名技术和数字加密技术来保证数据交互的过程可信和结果可信。数字签名技术是对接收与存储的数据进行签名，其目的是验证涉及数据交

互的各方，并对数据完整性进行校验。而数字加密技术是对数据进行加密保护，避免传输和存储过程中的数据泄露意外。

3.4. 主动标识载体

主动标识载体可分为内置型（嵌入新工业设备内部）与外置型（独立部署、不接入设备内部）两类，均可承载工业互联网标识编码以及必要的安全证书、算法和密钥，具备联网通信功能，能够主动向标识解析服务节点或标识数据应用平台等发起连接(无需借助标识读写设备来触发)。以下三种终端部件可作为安全性能较高的工业互联网主动标识载体，如下图所示：

- 通用集成电路卡（Universal Integrated Circuit Card，UICC）：是在全球移动通信系统中使用的智能卡，主要用于存储用户信息、鉴权密钥、短消息、付费方式等信息，还可以包括多种逻辑应用，例如用户标识模块（SIM）、通用用户标识模块（USIM）、IP 多媒体业务标识模块（ISIM）、以及电子签名认证、电子钱包等非电信应用模块。
- 通信模组：是连接工业终端和网络的关键底层硬件之一，具备不可替代性，与终端存在一一对应关系，同时也是终端应用访问 UICC 卡的通道。

- 微控制单元 (Microcontroller Unit，MCU)：又称单片微型计算机，是将中央处理器（CPU）、存储器、外设接口集成在单一芯片上的微型计算系统，负责终端的运算与控制逻辑。MCU 属于工业控制类芯片，广泛应用于各类工业终端与消费电子中。工业终端中的基带芯片、射频芯片、存储芯片等，均属于独立于 MCU 的功能芯片，见图 6。

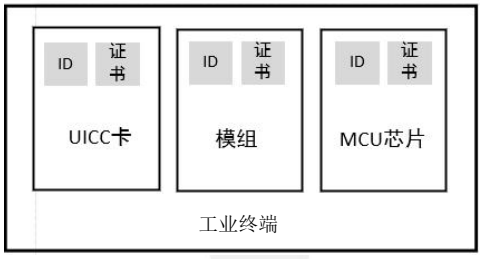

图 6 主动标识载体类型

现有方案中通常选用 UICC 卡作为主动标识载体，主动标识载体 UICC 卡具备为工业标识和终端身份凭证提供可信存储空间，以及利用与终端身份凭证相关的密钥为终端上的工业 APP 数据签名，以标记工业 APP 数据来源等基本功能。

主动标识载体服务平台为主动标识载体 UICC 卡预置、发放终端身份凭证，通过主动标识载体为行业终端提供可信终端的认证服务。工业终端需要与主动标识载体 UICC 卡适配以支持工业终端上的工业 APP。如下图所示，安全认

证SDK为工业终端提供适配主动标识载体UICC的软件开发包；SDN 协议为工业终端提供基于主动标识载体UICC卡的Eth/WiFi/Eth/5G入网能力。

图7 工业终端集成主动标识载体UICC卡

3.5. 终端元数据

标识解析相关数据的统一描述是工业互联网标识解析体系支持行业发展需要解决的重要基础之一。对生产中涉及的人、机、物、法、环等方面数据要素在统一行业规范下进行定义，才能形成以工业互联网标识为索引的对象识别、认识和描述。需要按照工业互联网标识解析核心元数据整体框架，规范行业工业互联网标识解析体系中人、机、物、法、环等方面数据要素的描述标准。

根据YD/T 4496-2023《工业互联网标识解析 核心元

数据》中的定义，元数据是定义和描述其他数据的数据。工业终端的元数据可以分为三类，见下图，包括：

- 静态的终端属性数据（如终端生产厂家）；
- 随着时间/空间改变的终端状态数据（如感知到的室内温度数据）；
- 由于事件触发而产生的动作指令类数据(如室内温度低于阈值触发空调开启指令）。

工业互联网标识解析节点中存储的数据遵循标准化的元数据可促进通过工业互联网标识解析系统进行系统间的互操作。

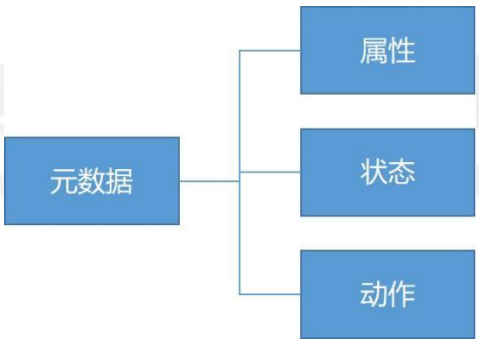

图 8 工业终端的元数据类型

为规范通信终端行业工业互联网标识解析元数据规范，推动工业互联网标识解析在通信终端领域的应用，中国通信标准化协会（CCSA）正在制定行业标准《工业互联网标识解析 通信终端 元数据》。

该标准在编制过程中，充分参考了行业骨干企业，及

重要配套产品企业的相关数据规范，同时对行业研究论文、现行国家标准等进行调研学习，从中吸取了共通内容，反映到通信终端行业元数据规范中。在规定技术特征信息等基础元数据要求时，遵循了兼容性、可扩展性、实用性的原则。

3.6. 基于工业标识的 SDN 园区网络

基于工业互联网标识体系的 SDN 园区网络整体解决方案由工业互联网标识解析系统，企业平台，主动标识载体服务平台，工业 IP 终端和 SDN 园区网络五部分组成。其中 SDN 园区网络通常由 SDN 网络控制器与 SDN 网络设备（交换机、WLAN-AP 等）组成。如图 9 所示：

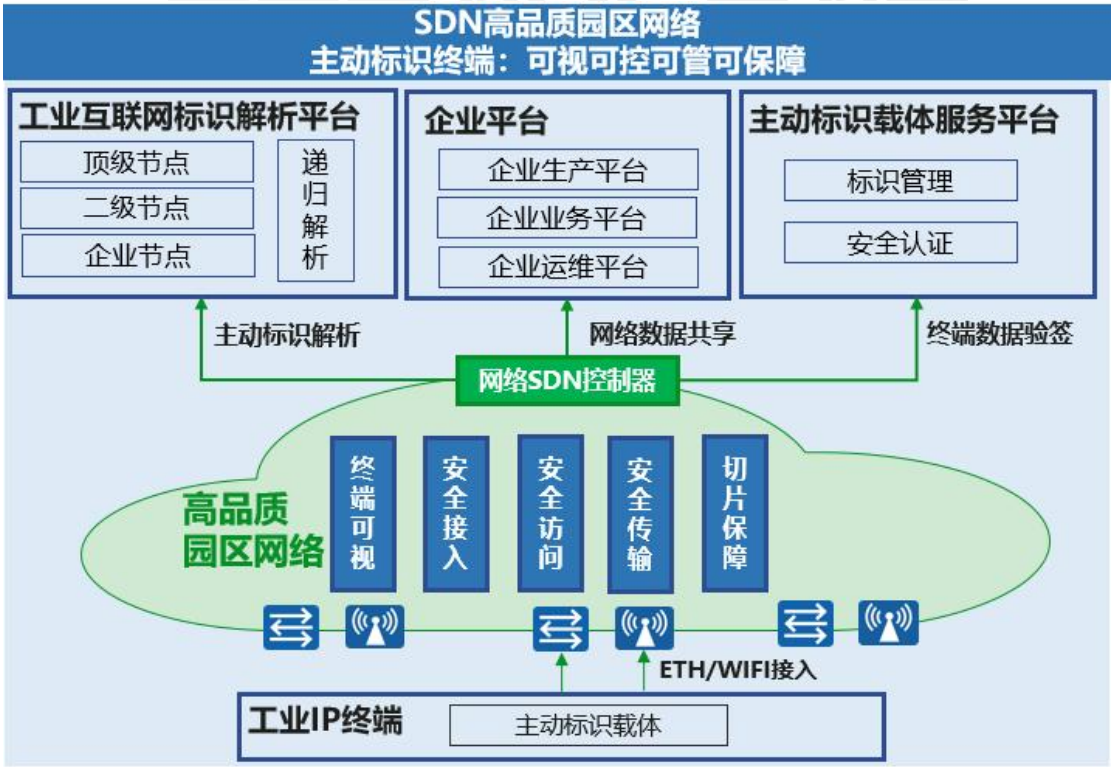

图 9 基于工业互联网标识体系的 SDN 园区网络方案

该网络解决方案以 SDN 网络控制器为核心，结合企业平台、工业互联网标识等多个平台，为园区工业终端提供了终端可视、安全接入、安全互访、安全传输、切片保障的能力；同时基于工业互联网标识，也可为上层企业平台内的多个业务系统提供终端丰富的网络数据信息。其中关键技术如下：

- **终端可视：**

图 10 终端可视方案流程

工业 IP 终端出厂时将工业互联网标识预置到主动标识载体中，当终端接入到园区网络，终端可通过自动发现协议自动连接 SDN 园区网络，并将工业互联网标识逐级传递到 SDN 网络控制器， SDN 网络控制器调用统一的标识解析 API 获取到该标识的所对应的基础信息数据（如：属于 xx 厂商，xx 产品，xx 型号），由此实现了主动标识终端的全可视能力。

- **安全接入：**

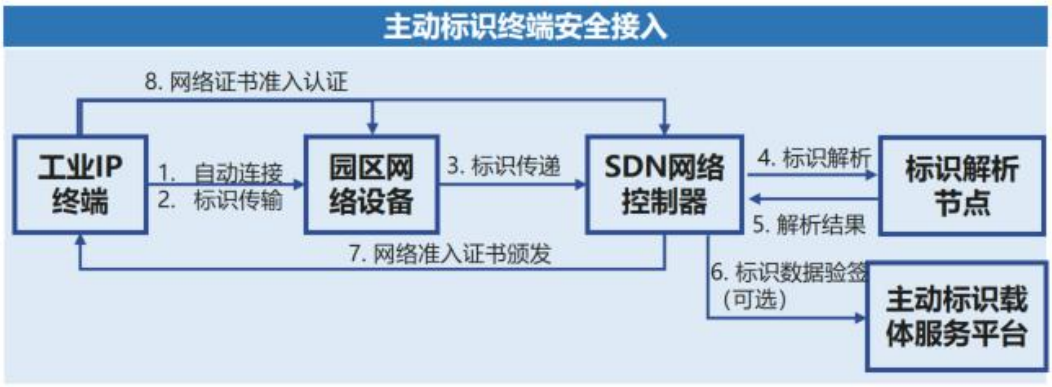

图 11 安全接入方案流程

SDN 控制器在收到终端发出的工业标识数据之后，可发往主动标识载体服务平台进行安全认证，进行数据验签，确保 IP 终端的合法性，也可根据标识解析出的基础信息人工审批其合法性。SDN 控制器直接根据该终端的工业互联网标识生成网络准入证书并颁发给终端，终端进行基于证书的网络安全准入认证。

- **安全访问：**

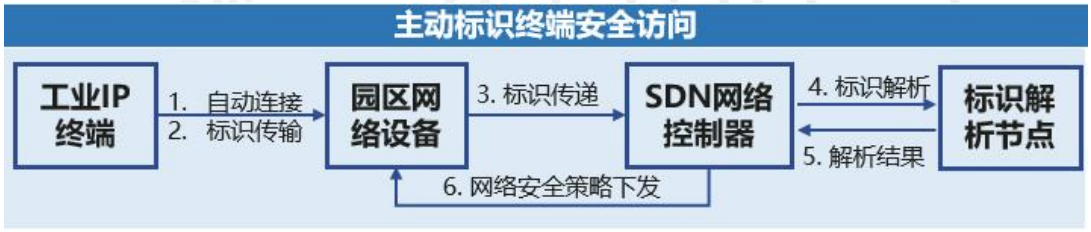

图 12 安全访问方案流程

SDN 控制器从标识解析节点收到该终端所需的网络安全策略解析结果后（如服务域名，访问端口等），自动翻译为网络语言（如 ACL 等）并下发到对应的接入网络设备，使得终端获取到所需的安全访问的权限。

- **安全传输（针对高安全类应用）：**

图 13 安全传输方案流程

载有主动标识载体的工业 IP 终端具备传输数据加签能力，基于该能力，SDN 网络可对终端传输数据进行抽样并送检主动标识载体服务平台进行安全认证，并根据验签结果灵活调整该终端的网络访问权限。

➢ **切片保障：**

图 14 切片保障方案流程

SDN 控制器从标识解析节点收到该终端所需的网络性能数据解析结果后（如：保障带宽 xxMbps 等），自动为该终端生成网络切片，提供 E2E 的网络带宽保障。

4. 应用验证

4.1. 基于工业互联网标识，轧辊定位系统安全极简入网

➢ **应用场景：**

本场景将以钢铁企业生产制造设备轧机中的关键部件

轧辊为实例，实现主动标识在轧辊定位跟踪方面的应用。对轧辊进行编码标识，并通过加装定位芯片以及现场布置的无线网络终端将相关数据传输到定位系统平台，实现对轧辊产品的远程定位管理和数据自动采集。通过工业互联网标识解析系统，查询某具体轧辊在制造过程和使用过程中的位置信息、使用情况，以及关联设备运转信息等。

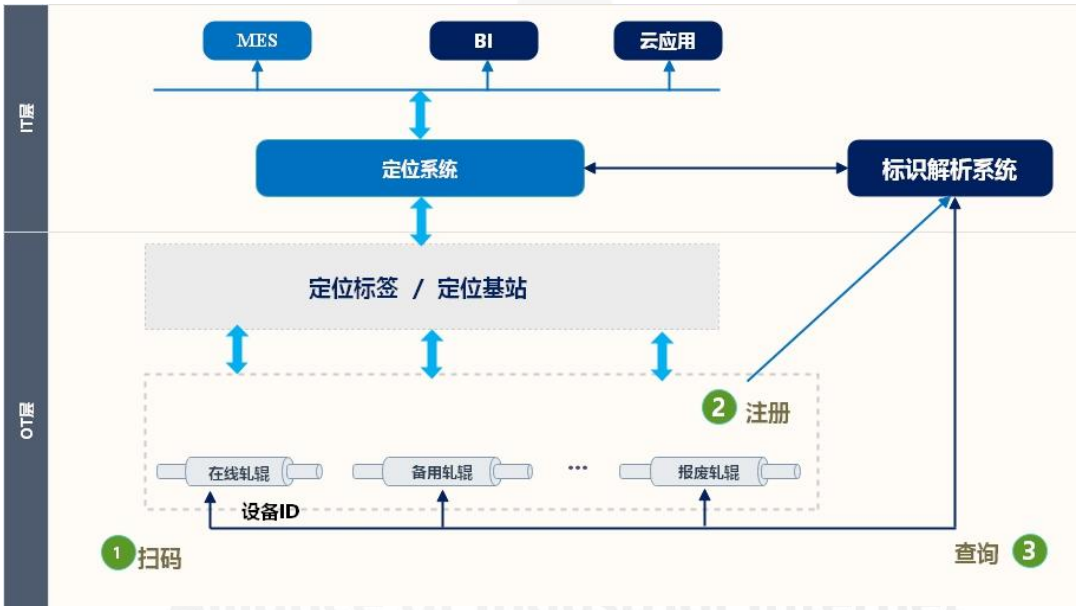

图 15 轧辊产品标识解析空间定位场景

定位系统通过电子标签和基站设备采集轧辊的位置和姿态变化信息，采集后的数据通过园区网络发送至企业数据平台，各种数据信息被存储在基础数据库中，定位引擎通过分析解算后形成业务需要的数据，并通过协议接口将数据汇聚至企业业务平台，其平台可对轧辊实时位置展示、轧辊使用统计、轧辊库存管理、轧辊效能评估等信息进行展示。

在整个轧辊定位系统中，定位基站可通过有线以太网、

WiFi、5G 等多种方式接入园区网络，然而工业级网络的准入安全性要求高，若以定位基站 MAC 地址为认证凭据，由于 MAC 地址易被仿冒性，以及无线环境下 MAC 地址的随机性问题，必将导致安全隐患与定位基站认证失败离线的风险，因此需要一种可替代 MAC 地址的，具备一般通用性的标识作为入网的身份凭证，可采用定位基站的工业互联网标识直接作为入网凭证，达到极简安全入网的目的。

- **场景解决方案：**

为了保证园区网络准入控制的安全性，我们采用了基于工业互联网标识的安全认证准入方案，整体方案如下：

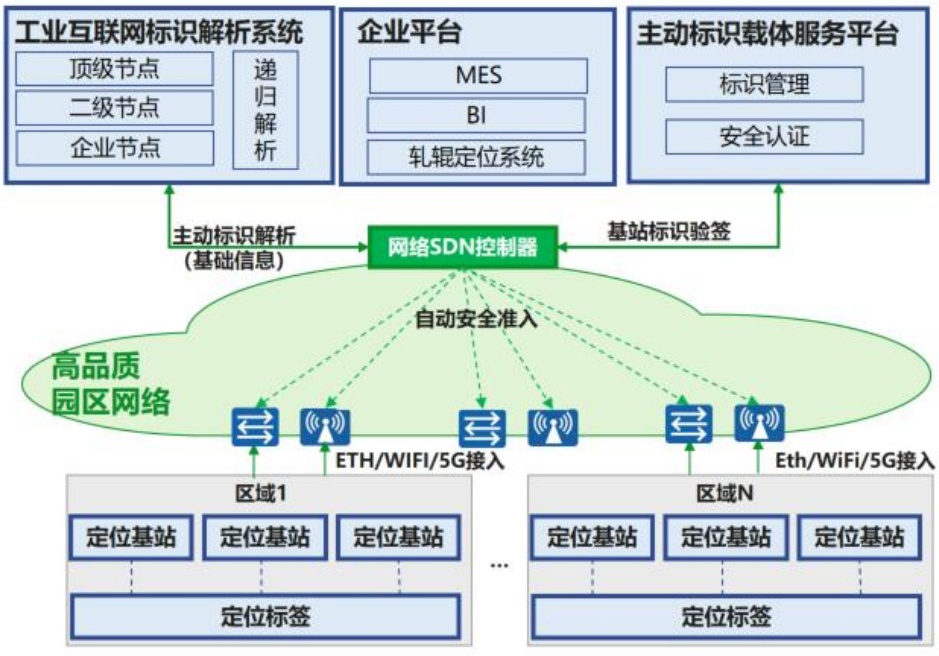

图 16 基于工业标识的轧辊定位系统入网方案

定位基站在接入网络的过程中以工业互联网标识为身份，自动在主动标识载体服务平台上进行标识验签通过后，

即可通过网络 SDN 控制器自动下发网络安全准入策略，大幅提升了多区域多定位基站的安全入网效率，降低了入网投资开销。

4.2. 基于工业互联网标识，轧机数据安全可靠传输

- **应用场景**

轧辊是钢铁生产过程中产生物理形变的重要部件，轧辊的使用寿命、磨损消耗、表面变化、精度直接关系到金属表面品质和工作效率。为此，以标识解析技术为基础，构建了以轧辊为对象的产品在线寿命评估及状态检测系统，通过将轧辊使用过程性能参数采集到企业产品在线寿命评估及状态检测系统，实现对轧辊运行时长、健康状态等情况监控。

基于标识解析体系，以某客户轧线轧机为对象，对轧机设备进行工业标识编码，利用标识解析技术和传感器实现对轧机设备的数据采集，实时监测轧机设备的运行状态，针对不同传感器设定报警阈值，通过系统对设备采集数据的自动比对，发现问题并报警处置。

图 17 轧机运行监测

轧机运行数据的采集传输是轧机运行监测的基础，一个高安全高可靠的数据承载网络是支撑轧机数据无间断监测的必备基础设施。

➢ **场景解决方案：**

为了保障轧机运行数据的安全可靠传输，我们采用了基于工业互联网标识的安全可靠数据传输方案，整体方案如下：

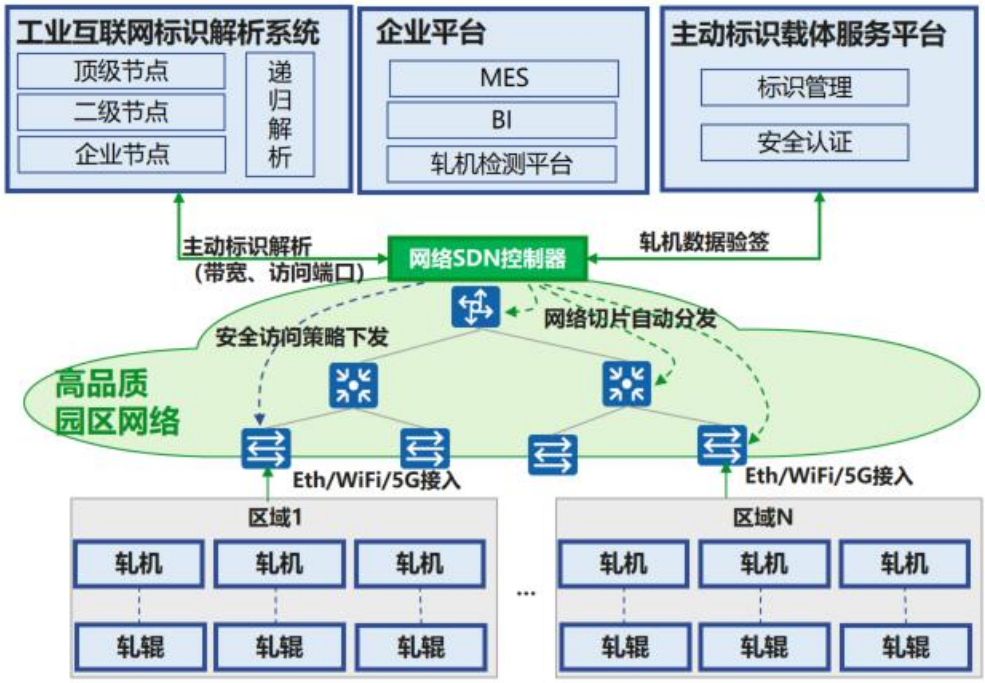

图 18 基于工业标识的轧机数据安全可靠传输方案

轧机在网络数据传输过程中，随流携带工业互联网标识，SDN 控制器通过工业互联网标识解析系统获取到轧机所需的带宽、访问服务器、端口等网络信息，并转换为网络配置策略，自动在全网生效。具体的，如将轧机所需的带宽等资源自动为轧机划分网络切片，全网下发，由此轧机数据传输可得到 E2E 的保障；将轧机所需的访问服务器、端口等信息自动转换为网络 ACL 等安全策略下发。综上所述，基于工业互联网标识，自动构建了一张高安全高可靠的数据传输网络。

4.3. 基于工业互联网标识，生产场景多方数据共享

- 应用场景

随着 ICT 技术的发展，轧辊生产企业的商业模式不断演进。从销售轧辊产品，到销售轧辊服务（即轧辊租赁服务），是一种既能满足轧辊用户需求又符合轧辊生产企业降本增效的新型商业模式。

新型商业模式需要轧辊生产企业能及时获得轧辊状态，如在机状态、转速、工作时长、位置等信息。这些信息涉及到 ICT 系统的多个部分。基于工业互联网标识解析系统的高品质园区网络可有效支持轧辊商业模式转型。

- **场景解决方案：**

如下图所示，借助工业互联网标识，终端企业将监控轧辊工作状态的 RFID PDA 的属性信息（如终端类型、带宽要求等）发布在终端企业标识节点上；轧辊生产企业将终端对应的业务信息（如监控业务、监控对象等）发布在工业企业标识节点上；网络运营商把从网络获得的终端信息也可以发布在运营商标识节点上。借助终端工业标识，园区网络 SDN 控制器可从终端企业节点获得轧辊监控终端信息（如终端类型、带宽要求等），也可以从工业企业标识节点上获得相关的业务信息（如监控业务、监控对象等）。此外，除了可以通过终端企业标识节点获得终端信息，工业企业也可以借助运营商标识节点获得轧辊监测终端的网络状态、位置等信息。

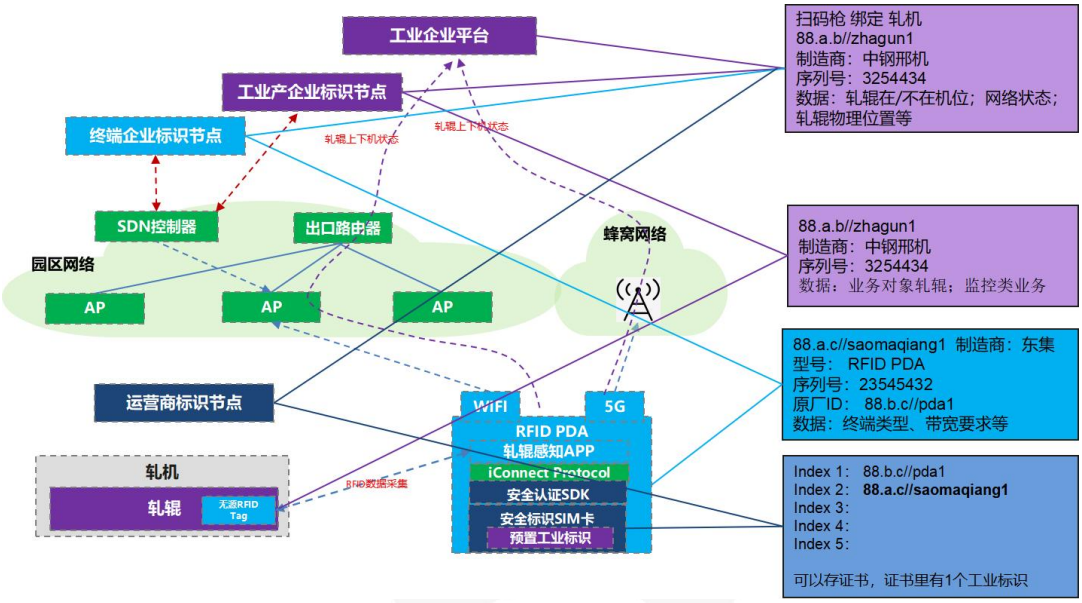

图 19 基于工业互联网标识的多方数据共享

总之，基于工业互联网标识解析的园区网络为企业获得极速接入、极简架构、极致体验和极简运维的高品质园区网络服务提供了有效解决方案。