ADNET 智能工厂网络建设方案

新华三技术有限公司

网络改造技术篇/成熟技术/工厂内网改造

---

1 概述

本方案旨在为制造业企业提供一套可靠的智能工厂网络建设方案。方案利用工业物联网、SDN、IPv6 等新兴技术，实现工业场景下人员、设备、物料、产品的海量互联，为工厂实现智能生产、协同制造和柔性制造提供网络支撑。

1.1 背景

近年来，制造业企业正面临着供给侧改革的时代命题，转型升级的需求十分迫切。而传统工厂 IT 系统与工控系统间的通信往往存在较多障碍，具体表现在：

1）工业控制协议标准各异，各厂家设备难以互通；

2）工业现场存在很多信息孤岛，网络性能亟待提高。

这些问题导致现有工厂网络无法支撑数字经济下的制造业生产运营模式。随着物联网、SDN、IPv6 技术的日渐成熟，ADNET 智能工厂网络建设方案（ADNET 即应用驱动网络）的提出，帮助制造业企业完成工厂网络的升级改造。

1.2 实施目标

1）实现工厂有线无线网络全覆盖，解决信息孤岛的问题。有线网络的时延、稳定性达到工业现场要求，同时兼容

IPv4/IPv6双栈。无线网络根据工厂实际需求支持Wi-Fi、RFID、4G/5G、NB-IoT、LoRa、ZigBee、蓝牙等信号中的一种或几种，同时无线信号质量高，满足场景要求。

2) 对主流工业现场总线协议进行适配，实现生产网和信息网的双网融合互通。

3) 基于 SDN 技术部署工厂网络，向上对接工厂云平台，实现网络设备自动配置和业务快速部署，提升产线效率，减少人力投入。

4) 建立工厂网络安全保障系统，实现人、机、物、系统的可控接入和行为审计，保证工厂的设备安全、网络安全、控制安全、应用安全和数据安全。

1.3 适用范围

该解决方案适用于制造业工厂内网络的建设和升级改造，建设完成后的网络能够满足工厂柔性制造、协同生产、个性化定制的业务需求。

1.4 在工业互联网网络体系架构中的位置

该解决方案属于工厂内网络建设方案，在下图中所处位置包含1、2、3、4、5、6六部分的内容。

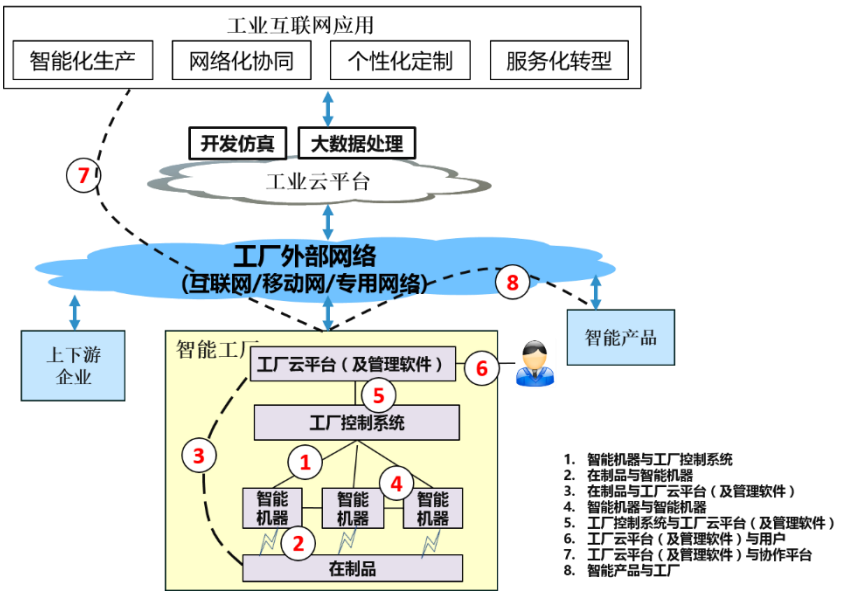

图 1 工业互联网互联示意图

2 需求分析

传统的工业网络存在以下问题：

1）工业现场总线协议标准各异，不同厂家设备无法互通，存在数据孤岛；

2）数据孤岛的存在使设备状态无法得到有效监控，进而导致企业需要在计划排产、物料配送、生产协同、质量控制、设备检测等环节投入大量的人力物力；

3）传统 IP 网络采用尽力而为的传输机制，时延不稳定且存在丢包，因此在一些时间敏感型场景无法使用；

4）网络安全问题层出不穷，工控设备普遍不打补丁，一旦设备联外网就容易遭到入侵攻击，导致工厂大面积瘫痪；

5）生产区域的任意设备都可以随意接入网络，缺乏接入管控；

智能工厂网络的建设目的是构建连接人、机、物、系统的高

性能泛在互联网络，实现工业数据的充分流动和处理。为此，需要解决如下问题：

1) 传统工控协议的适配问题

2) 设备物料的泛在接入问题

3) 数据稳定低时延传输问题

4) 网络智能化运维管理

5) 网络安全可控、终端准入

3 解决方案

3.1 系统架构

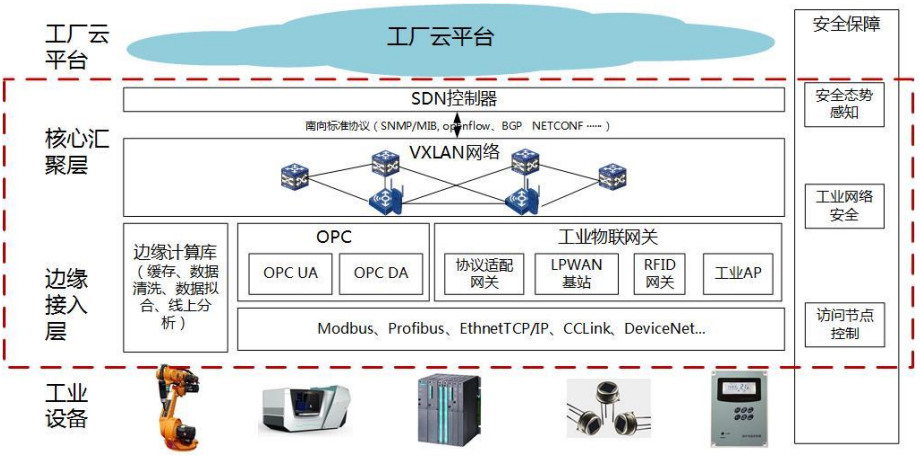

图 2 工厂内网络逻辑架构图

ADNET 智能工厂网络的建设内容位于上图红框中，含边缘接入层、核心汇聚层和安全保障三部分，其中：

●**边缘接入层：**主要负责边缘设备接入、数据采集与边缘计算。边缘接入设备应支持海量物联网传感器和智能硬件的快速接入和数据服务，满足物联网领域的设备连接、协议适配、数据存储、数据安全、数据分析等服务需求。

●**核心汇聚层：**本次方案采用 SDN VxLAN 技术设计工厂内核

心汇聚层网络，网络可以抽象为物理承载网络和面向应用的 Overlay 网络。这种网络设计方式的两大特征是柔性网络和软件定义。柔性一方面指网络架构灵活，业务部署（应用/终端）与位置无关；另一方面指以人和业务应用为核心，所有网络资源根据人和业务需要移动。软件定义指基于 SDN 思想将网络控制平面集中，实现网络设备的自动部署、业务按需交付，将运维人员从重复劳动中解放出来。

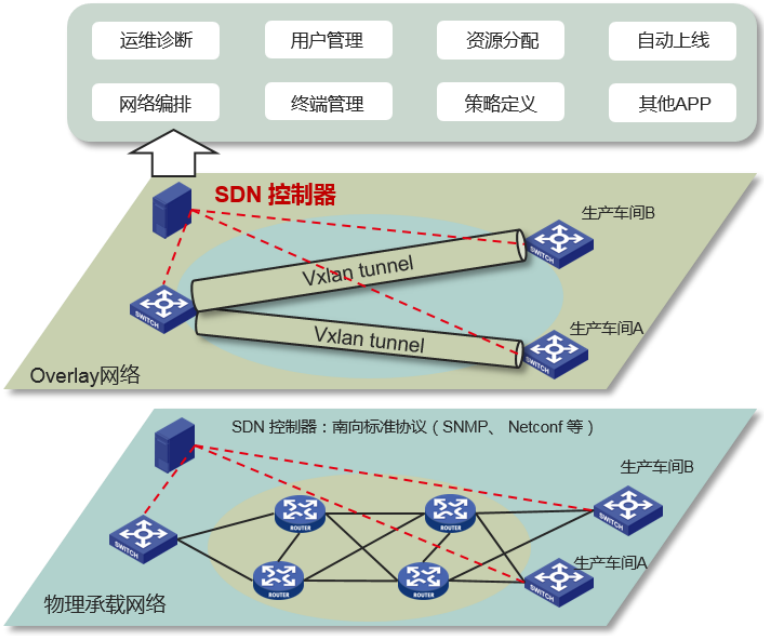

图 3 核心汇聚层网络的物理/逻辑架构

- **安全保障：**网络安全是工厂业务平稳运行的基础，ADNET 智能工厂网络方案具备完整的安全防护体系，包括安全态势感知、网络安全保护、数据节点接入控制，保证工厂 IT 基础设施安全、业务系统安全、资产安全。

3.2 网络拓扑设计

根据上述系统架构，工厂实际部署的网络拓扑如图 4 所示，

根据地理位置可分为生产车间网络、办公接入网、核心汇聚网三部分：

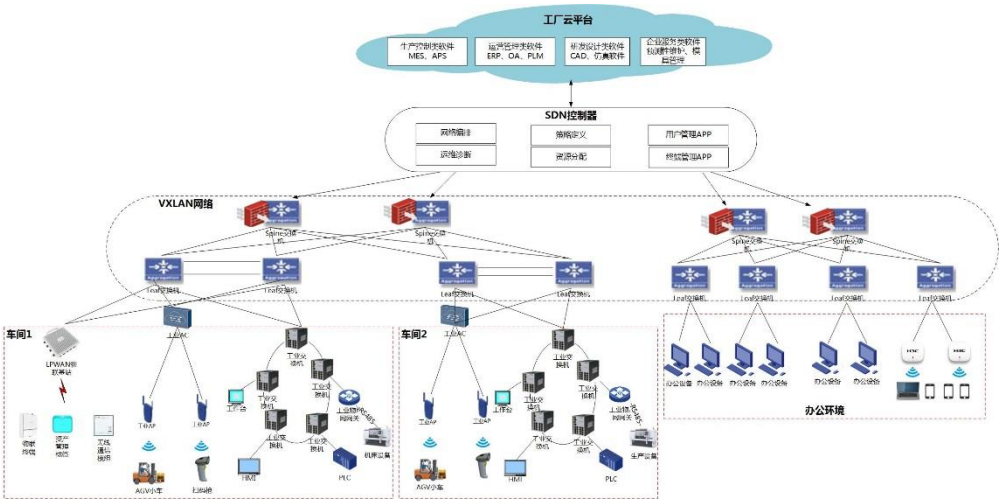

图 4 ADNET 智能工厂网络实际拓扑图

1）生产车间网络

- 边缘接入

在工业现场，数据接入方式有：传感器类型的离散点(IO 信号，模拟信号)采集接入、设备工业现场总线协议或专有协议类型接入和网络 TCP/IP 直接数字接入。目前，ADNET 智能工厂网络方案涉及的工业物联网设备已具备 GB/T 33474-2016 感知控制域中所列举的数据接入能力。

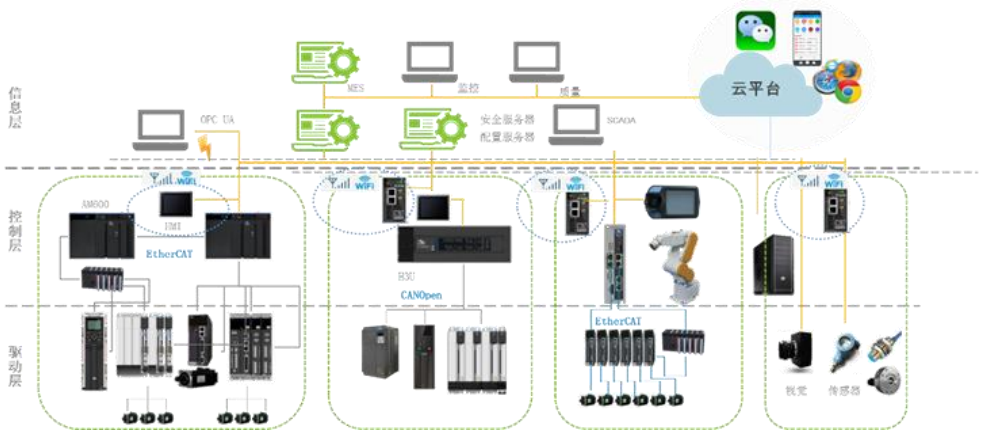

图 5 数据采集接入示意图

针对工业协议的适配，方案采用工业网关完成不同现场总线的接入转换，实现 Modbus、PROFIBUS、EtherNet/IP、SIEMENS S7Comm 等协议的接入适配。

另一方面，方案也支持采用 OPC UA 的采集接入方式。OPC UA 技术为工业生产各系统提供了统一接口标准。其中，OPC UA 服务器和客户端是系统实现数据采集的核心环节。OPC UA 服务器负责对底层设备数据进行采集封装，并将历史数据存放于外加的数据库内，使多个客户端以统一的方式获取不同底层设备的数据。OPC UA 客户端的主要功能是搜索并连接 OPC UA 服务器，浏览服务器的地址空间并读取其中存放的实时数据和历史数据，并通过客户端显示界面将数据以图表的形式展示给工作人员。

- 工业以太网

工厂生产线上温湿度、电磁干扰等环境相对复杂，方案拟在接入密度较高的区域采用机架式工业交换机，交换机支持 Modbus TCP/IP、ProfINet、Ethernet/IP 等工业以太网协议。另外，在一些特定场景将卡轨式工业交换机直接安装在电器柜，交换机从电器柜内取电。工业交换机按照产线做 RRPP 环路部署。按照这种部署方式，关闭生产线上的任一台工业交换机，除直连到该交换机的设备网络不通，其他网络不受影响。

- 工业无线网

WLAN 网络：针对工业无线网的需求，方案基于 802.11ac 技术，采用无线控制器 AC+瘦 AP 的部署方式构建无线网络。其中，

Wi-Fi 信号质量和漫游问题是部署过程中的两个难点。为保证 WLAN 网络的信号覆盖质量，需要依据实际环境设计交付方案并进行测试，最终完成部署。空旷区域部署室外 AP，用 POE 供电盒供电。对信号要求无死角的区域，部署放装 AP。针对漫游问题，可提供二层漫游、三层漫游、跨 AC 漫游三种方案，其中跨 AC 漫游的最大延迟时间为 50ms。

LPWAN 网络：在 NB-IoT 领域，方案拟提供 NB-IoT/eMTC/E-GPRS 基站实现物联终端接入，通过内置 LPWAN 通信模组将终端联网。管道方面，基站部署方式灵活，有三种模式可供选择（独立部署、保护带部署、带内部署）。

在 LoRa 领域，方案提供 LoRa 基站、终端、模组，其中基站的有效覆盖范围为 2~3KM，支持 10 万终端并发，用于工厂电力抄表，水力抄表及温湿度环境监控等远距传输控制。方案支持超高频无源 RFID，用于仓储物流定位场景。

2）办公接入网

- 办公有线

由于办公楼宇规模不一，配线间数量不定，所以每个配线间接入设备数量在 2-X 台不等。为了节省光纤，简化管理，接入层设备采用 IRF2 多虚一技术，将每个配线间的设备虚拟化一台设备后通过 10G 带宽上行至汇聚层设备。

- 办公无线

在建筑物内,每层建筑楼根据使用功能部署 AP 数量，方案拟

部署的无线 AP 支持最新无线传输 802.11n 协议，提供理论上 300M 传输带宽。为建设高可靠、高性能的无线网络系统，室内无线 AP 采用 POE 供电。通过在每层楼部署千兆 POE 交换机，为无线 AP 提供千兆接入的同时，还能通过以太网线对无线 AP 供电。无线系统采用瘦 AP（FIT）+无线控制器部署方案。无线控制器部署采用在核心交换机上部署 1 块无线控制器功能板卡，实现无线网络系统的高可靠性。

3）核心汇聚网络

整个工厂网络由核心、汇聚、接入三层设备组成，再搭配园区 SDN 控制器。其中接入层设备部署在生产线附近，而汇聚、核心设备之间则构建 overlay 网络，同时采用分布式 L3 网关并通过可靠机制来抑制广播风暴。接入层设备采用不同的 VLAN 进行接入位置的标识，通过 TRUNK 的方式上行到汇聚层，汇聚层完成 VLAN 到 VxLAN 的映射。

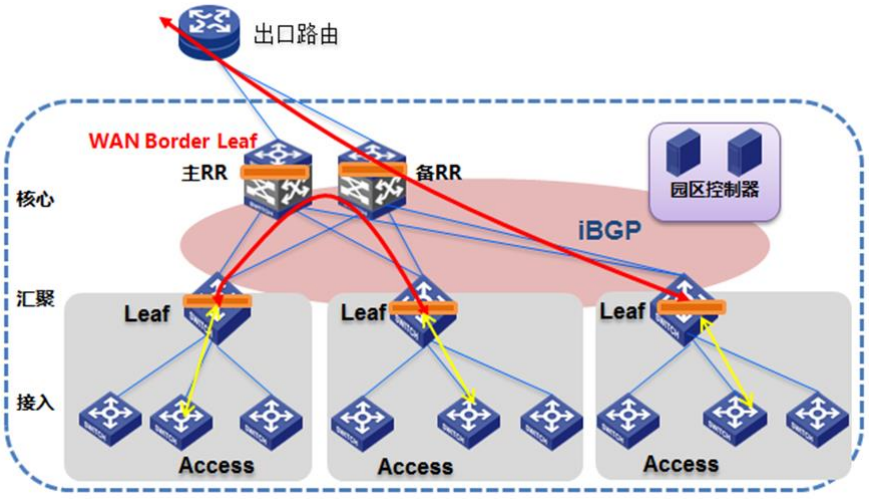

图 6 工厂核心汇聚层 VxLAN 网络示意图

该网络方案的核心是 SDN 控制器。所有网络自动化上线，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直观的图形化界面完成。同时通过开放控制器接口，允许第三方进行业务定制开发，满足用户个性化、定制化、可编程的需求。

该网络方案的另一大特性是实现有线无线一体化管理。传统有线/无线网络存在管理不统一、转发不统一、策略控制不统一的问题(比如跨 L3 网段漫游要么支持不了，要么需要在 AC 之间打隧道,增加成本),而方案通过SDN控制器极大解放了AC和AP，真正实现有线无线的统一管理、统一转发、统一认证和统一拓扑展示。

4）整体安全保障系统设计

- 终端接入管控

在工厂内部署一套终端准入控制系统，与防病毒软件、WSUS补丁管理相配合。防毒软件、WSUS 负责专业杀毒、补丁下载，终端准入控制系统采用接入层 802.1x 部署方案，与交换机配合实现网络接入控制、桌面管理、用户行为审计和终端安全管理。

- 网络安全设计

工厂网络安全涉及到南北向安全防护和东西向安全防护。网络部署中的安全资源可以是软/硬件安全资源，也可以是虚拟化的安全资源。

南北向安全防护：负责处理南北向的业务流量，涉及 DDoS、IPS、防火墙等安全设备，以及负载均衡设备做流量分配。每个

安全服务模块中涉及硬件安全设备和软件形态NFV设备。对于不同等级的用户分配不同的安全资源，高等级用户分配硬件安全资源，低等级用户分配软件形态NFV安全资源。

一个开启全功能安全服务的互联网租户与半安全域交互的流量会依次经过DDos、IPS、LLB、防火墙、WAF等安全设备，最终来到安全域。

东西向安全防护：东西向服务链负责工厂内部不同安全域安全流量处理。

- 安全态势感知

为了做到对工厂网络风险的主动发现和提前防御，工厂需要采集安全日志、网络流量、用户行为、终端日志、业务数据、资产状态等数据。结合外部情报，通过安全态势感知系统对攻击趋势分析、异常流量判断和终端行为检测，实现“安全趋势可预测”；通过对未知威胁的智能检测识别、流量/行为/资产的状态监控和多维度风险分析，实现“安全风险可感应”；通过对攻击溯源取证、云网端协同联动、工单流程闭环处理和设备策略自适应调整，实现“风险行为可管控”。

5）工厂网络整体IPv6升级思路

目前大量工厂网络都是IPv4网络，随着IPv6逐渐部署，很长一段时间是IPv4与IPv6共存的过渡阶段。过渡阶段所采用的过渡技术主要包括：

- 双栈技术：双栈节点与IPv4节点通讯时使用IPv4协

议栈，与 IPv6 节点通讯时使用 IPv6 协议栈。

- 隧道技术：提供了两个 IPv6 站点之间通过 IPv4 网络实现通讯连接，以及两个 IPv4 站点之间通过 IPv6 网络实现通讯连接的技术。
- IPv4/IPv6 协议转换技术：提供了 IPv4 网络与 IPv6 网络之间的互访技术。

对于小型工厂,方案推荐通过 IPv4/IPv6 双协议栈部署 IPv6 网络。这种方式可以同时提供 IPv4 应用和 IPv6 应用，但缺点是需要所有网络节点支持 IPv4 和 IPv6 路由协议。因此对于大型旧工厂，升级工作量大。

如果企业需要跨越 IPv4 网络连接不同的 IPv6 域,则需要通过隧道技术部署 IPv6。这种场景需要设备提供 IPv6 DNS 查询功能，同时边界路由器需要支持 6 Over 4 隧道。这种方式投资和风险很小。缺点是使用隧道使网络拓扑复杂，不易管理，出现问题难以定位。另外,由于使用隧道封装,对转发效率有一定影响。

3.3 功能设计

1) 设备物料的泛在接入能力

智能工厂网络提供多种 OT 终端接入能力，包括以太网有线接入、无线接入（Wi-Fi/IEEE 802.15.4/ ISA100.11a/ WIA-FA/IoT/LTE/5G/蓝牙等）、PON 接入；支持 Modbus、PROFIBUS、EtherNet/IP 等主流工业以太网协议,提供海量终端的接入能力。

2) 无阻塞、易扩展的网络架构设计

基于 SDN 的（ACCESS/LEAF/SPINE）三级网络架构，构建无阻塞工业网络。根据企业接入能力不同选择两级或者三级架构部署，每层网络可以横向无限扩展，配合 SDN 实现扩展自动化，减少人力投入。

3）自动化部署

通过 SDN 控制器对网络设备分类，不同的设备采用和角色对应的配置文件，设备初始上线后，根据拓扑连接关系、角色从控制器下拉基础配置文件，保证设备实现批量自动上线，减少管理员操作。

4）一体化运维

通过控制器实现端到端业务编排，并配合工业控制系统实现网络资源的按需调度；通过控制器对网络设备进行监控，建立统一的拓扑、统一的管理平台。

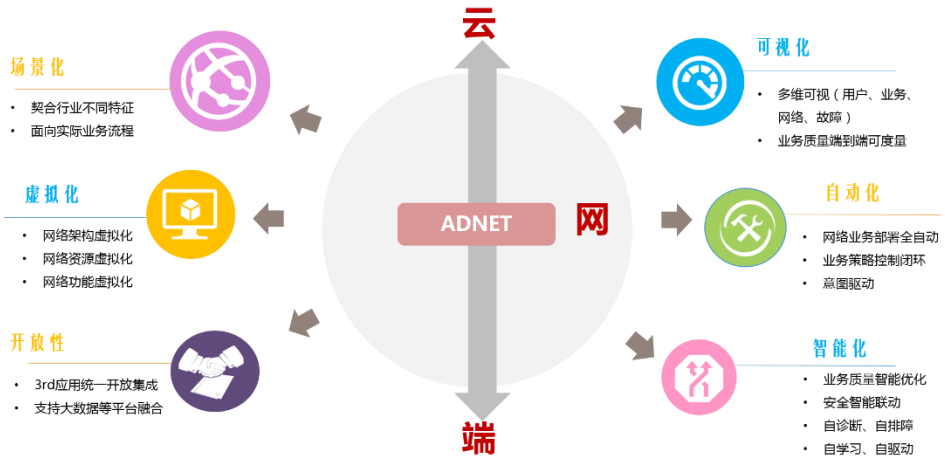

图 7 ADNET 智能工厂网络能力特征

3.4 安全及可靠性

●高可靠

工厂网络建设对设备可靠性要求很高。一旦网络系统运行不正常或者出现故障中断将直接导致工厂业务的中断。因此需要从设备自身和网络架构角度确保网络系统的稳定性。从设备自身角度，核心汇聚层设备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；从架构方面，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。

●系统化的安全防护

工厂网络安全保障方案不应该是孤立的设备堆砌，而是从工厂的实际情况出发构建系统的安全防护体系。在此体系中，使用者、生产设备、产品、个人终端、网络设备、安全设备、态势感知系统充分协同，在安全事件出现前极力规避、预警，出现时能够及时发现，并具备依据事先制定好的应急方法进行自动化处理的能力，最后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　成功案例

本解决方案已经在中车株机轨道交通车辆转向架智能制造车间项目中应用。转向架作为轨道车辆最为重要的零部件之一，起着导向、支撑车体、减震运行的作用，对轨道交通产品的安全平稳运行至关重要。基于 ADNET 智能工厂网络方案，为中车株机公司转向架车间建设互联网络，具体建设情况如下：

1）核心层设备采用高性能网络交换机，做横向虚拟化。汇聚层将生产网和办公网的交换机配置模块进行堆叠，将汇聚交换

机虚拟化为一台。接入层办公网保持不变，生产网增加工业交换机。

2）生产线上，采用工业交换机按照产线做环路部署。无线生产网部署满足工厂电磁环境的室外 AP，配置定向天线。

3)安全方面,在核心汇聚与生产区域之间部署一对防火墙，保护生产区域，同时将服务器区设置为防火墙 DMZ 区。另外，在服务器区部署堡垒机,实现对所有服务器及交换机操作进行监控、管理以及回溯。

4）软件层面，增加管理软件，对工厂网络设备进行统一监控管理；增加无线管理组件，实现整网无线统一管理；增加接入认证组件,对生产网终端接入进行认证;增加 IP 地址管理软件，对现网 IP 地址进行规划。

通过互联网络的建设,中车株机转向架车间网络的稳定性大大提升，设备故障切换时间由秒级提升为毫秒级。车间无线信号的覆盖状况大大提升,保证 AGV 小车等无线需求高的工业设备平稳运行。高可靠网络为中车株机转向架生产业务提供了保障，大大提高了工控系统的生产效率。在安全性上,工业安全软件统一接入和管理信息点，并监管工厂所有网络设备。同时加入网络安全设备，有效减少了工厂网络病毒木马造成的工业数据丢失、泄密风险。