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

工 业 互 联 网 产 业 联 盟 标 准

AII/001-2017

工业互联网平台　通用要求

Industrial Internet Platform, General Requirements

工业互联网产业联盟

（2017-XX-XX 发布）

目录

前　言

本标准是工业互联网平台系列标准之一。

随着技术的发展，还将制定后续的相关标准。

标准牵头单位：中国信息通信研究院、航天云网科技发展有限责任公司

标准起草单位和主要起草人：

- 中国信息通信研究院：李海花、黄颖、陈屹立、刘钊、李强、魏凯、刘阳、杨希、陈文弢、栗蔚、沈彬、李铮
- 航天云网科技发展有限责任公司：柴旭东、李潭、于文涛
- 阿里云计算有限公司：刘松、贾宁、郑王力、马铁宝、李俊平
- 三一集团有限公司：贺东东、王锦霞
- 树根互联技术有限公司：文博武、张茂森
- 中兴通讯股份有限公司：邵伟翔、林兆骥、张博山、高峰
- 北京和利时智能技术有限公司：龚涛
- 中国电信集团公司：张东、杨震、李洁、叶锦宇
- 浙江中控技术股份有限公司：俞文光
- 中国移动研究院：陈维、刘琨
- 机械工业仪器仪表综合技术经济研究所：杜孟新、方毅芳
- 北京长河朗锐网络技术有限公司：施磊

工业互联网平台 通用要求

1 范围

本标准规定了工业互联网平台的通用要求，包括平台的定义和内涵、平台参考架构、云基础设施要求、平台基础能力要求、基础应用能力要求、安全可信要求、运维管理要求和性能要求，适用于工业互联网平台的研发、建设及部署。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

工业互联网产业联盟报告　　《工业互联网体系架构（版本 1.0）》

数据中心联盟标准　　《云计算服务协议参考架构》

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业互联网平台　Industrial Internet Platform

是指可集成工厂内部和/或工厂外部的各种数据、服务、用户等各类资源，在此基础上提供工业数据集成分析、应用支撑能力和基础应用能力，以支撑各种工业互联网应用，是构建产业生态重要基础。

4 缩略语

下列缩略语适用于本文件。

缩略语	英文全称	中文全称
AII	Alliance of Industrial Internet	工业互联网产业联盟
AR	Augmented Reality	增强现实技术

COAP	Constrained Application Protocol	受限制的应用协议
DAG	Directed Acyclic Graph	有向无环图
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
DM	Device Management	设备管理
DTLS	Datagram Transport Layer Security	数据包传输层安全性协议
EDP	Electronic Data Processing	电子数据处理
GRE	Generic Routing Encapsulation	通用路由封装
GSMA	Global System for Mobile Communications assembly	全球移动通信系统协会
HDFS	Hadoop Distributed File System	Hadoop分布式文件系统
HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
IPSec	Internet Protocol security	互联网协议安全
L2TP	Layer Two Tunneling Protocol	第二层通道协议
LWM2M	Lightweight M2M(Machine to Machine)	轻量级M2M(机器到机器通信)
MQTT	Message Queuing Telemetry Transport	消息队列遥测传输
NoSQL	Not Only SQL(Structured Query Language)	不仅仅SQL（结构化查询语言）
OLAP	On_line Analytical Processing	联机分析处理
OPC	OLE(Object Linking and Embedding) for Process Control	用于过程控制的OLE(对象连接与嵌入)
OPC UA	OPC Unified Architecture	OPC统一架构
OT	Operational Technology	操作技术
PII	Personally Identifiable Information	个人可识别信息
SBOM	Service BOM (Bill of Material)	服务BOM(物料清单)
SDK	Software Development Kit	软件开发工具包
SQL	Structured Query Language	结构化查询语言
SSL	Secure Sockets Layer	安全套接层
SVM	Support Vector Machine	支持向量机
TLS	Transport Layer Security Protocol	安全传输层协议
VLAN	Virtual Local Area Network	虚拟局域网
VR	Virtual Reality	虚拟现实
VXLAN	virtual Extensible LAN	虚拟可扩展局域网
XMPP	Extensible Messageing and Presence Protocol	可扩展消息与存在协议

5 工业互联网平台的位置

参考工业互联网产业联盟发布的《工业互联网体系架构（版本1.0）》中“应用支撑的实施”部分，从实施部署角度，工业互联网平台可以部署在工厂内部，也可以部署在工厂外部，如图1所示。本文件中统称为工业互联网平台。

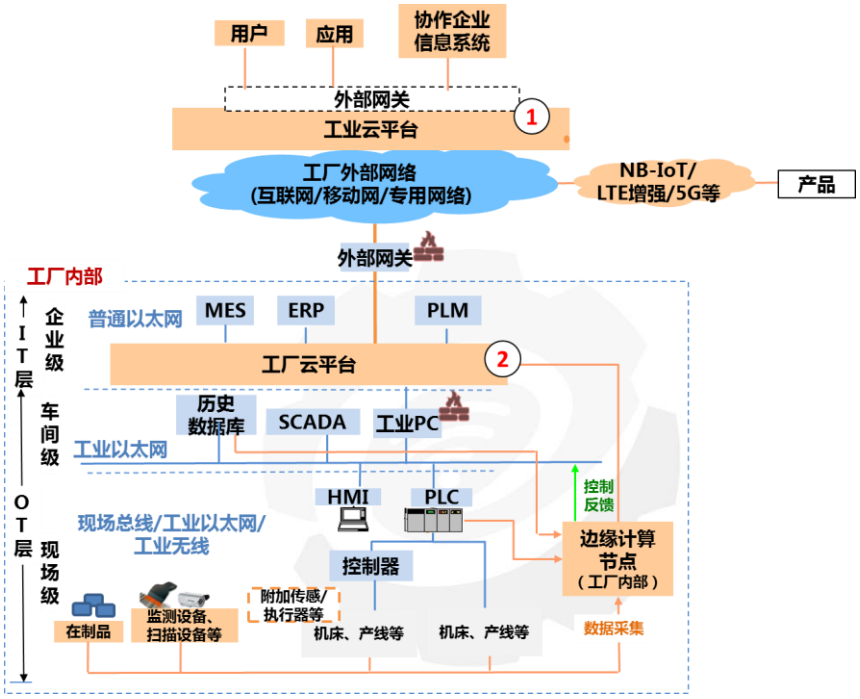

图1 工业互联网平台部署示意

6 工业互联网平台参考架构

工业互联网平台是指可集成工厂内部和/或工厂外部的各种数据、服务、用户等各类资源，在此基础上提供工业数据集成分析、应用支撑能力和基础应用能力，以支撑各种工业互联网应用，是构建产业生态重要基础。

本文件主要从功能视角出发，给出了工业互联网平台应提供的功能、性能、安全等基本通用要求，但在具体实现上，不同企业可以根据自己的产品和市场定位，选择实现部分能力，如电信运营商可以侧重提供设备接入和连接性管理，同时具体功能、性能、安全等的实现和技术选择还需要与具体应用领域相结合。

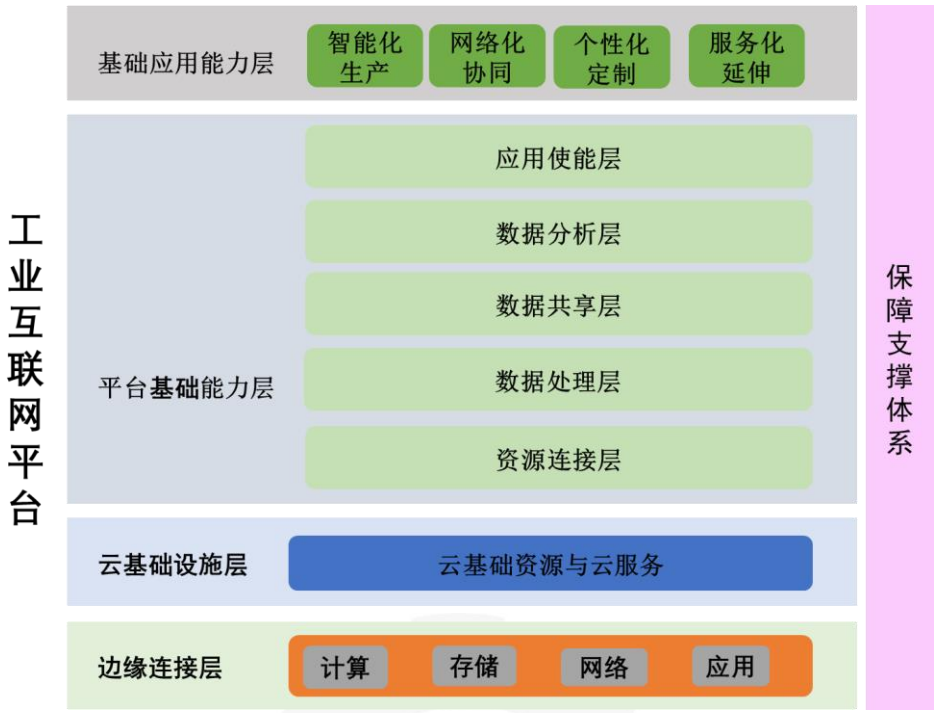

图2 工业互联网平台参考架构

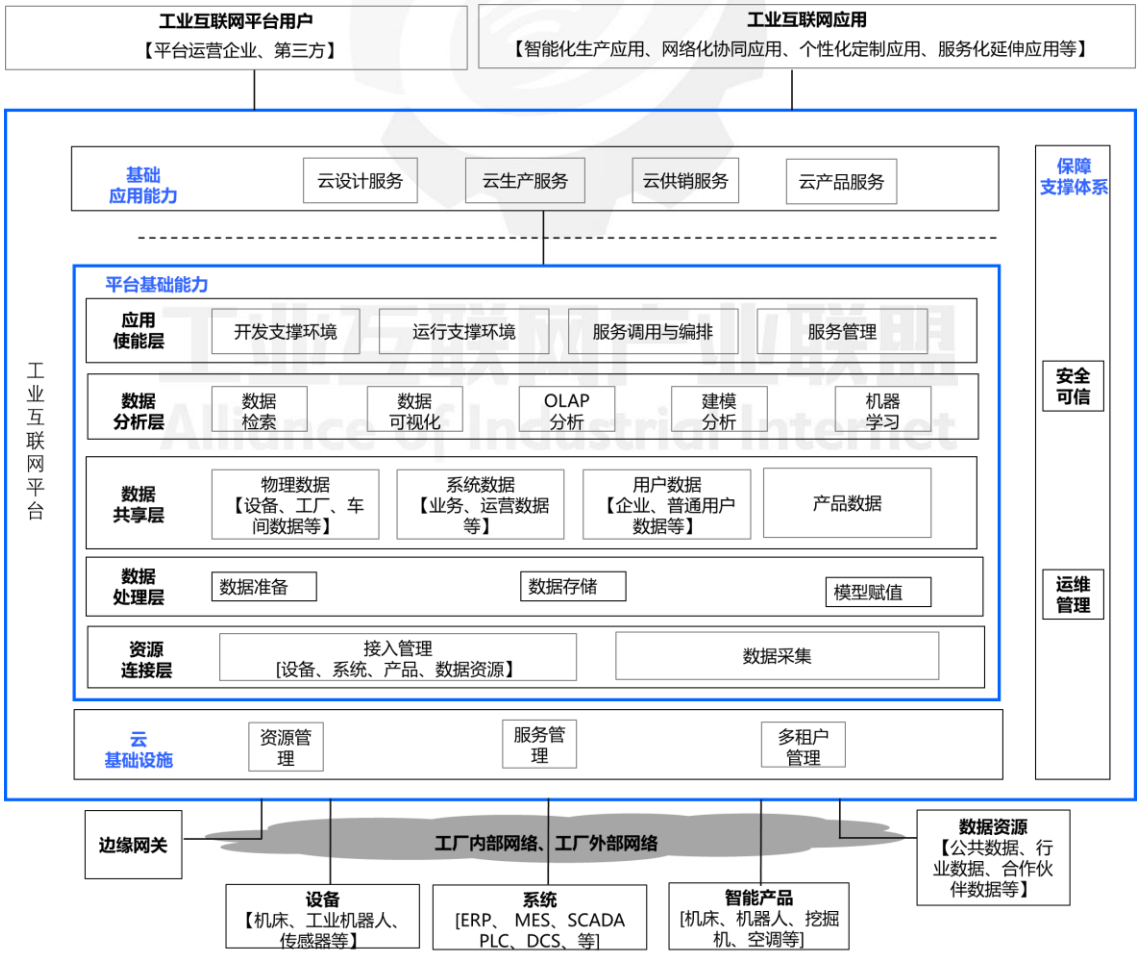

图3 工业互联网平台功能要素

工业互联网平台参考架构及主要功能要素如图2、图3所示。

工业互联网平台可以与设备、系统、智能产品互联，获取各种历史数据和实时数据，也可以与与各种提供数据资源的系统互联，以丰富平台可采集与分析的数据，在此基础上实现更加综合与智能的分析。

工业互联网平台为各种工业互联网应用提供基础共性支撑。同时工业互联网平台与平台用户交互，为平台用户提供边缘连接、云基础资源、应用开发环境、基础应用能力等，以支撑应用的快速开发、部署和运行。

从功能实现上，工业互联网平台架构可以划分为边缘连接、云基础设施、平台基础能力、基础应用能力、保障支撑体系，其中边缘连接提供靠近边缘的分布式网络、计算、存储及应用等智能服务，云基础设施提供云资源及云资源管理、运行和云服务调用相关的框架支撑，平台基础能力提供以数据采集、处理和服务的通用基础功能，保障支撑体系提供平台运维管理和安全可信能力。

从安全实现上，平台建设与平台安全可信应同时设计、建设、验收、运营。平台的建设方需在建设方案中考虑安全可信措施，平台安全可信保障应采用与建设方不同安全能力提供方，进行平台的风险识别、安全设计、安全服务以保证相互监督和相互制衡。

7 边缘连接要求

提供靠近边缘的分布式网络、计算、存储及应用等智能服务，相关要求待定。

8 云基础设施要求

云基础设施为提供虚拟化的计算、存储和网络资源，以及基础框架（如Hadoop、OpenStack、Cloud Foundry）、存储框架（如分布式文件系统 HDFS）、计算框架（如 MapReduce、SPARK）、消息系统等支撑能力，工业互联网平台及平台用户、工业互联网应用可以调用这些资源和支撑能力。

8.1 基本要求

（1）物理资源无锁定

平台对物理设备资源无厂商锁定策略，保证平台的正常维护以及物理资源扩

容的灵活性。

（2）资源弹性伸缩

平台具备计算、存储、网络等资源的弹性扩容，并根据业务负载情况进行弹性的自动伸缩。

（3）高可用架构

平台能够实现物理机、虚拟机的高可用，当单个的物理、虚拟节点发生故障，能够保证业务连续性。

（4）数据容灾备份

采用分布式存储技术，具备数据容灾设计，能够实现对全平台存储数据的周期性全量、增量备份机制。

（5）组网能力

平台支持多种网络类型，如 VLAN、VXLAN、GRE 等，提供灵活高效的组网能力。

8.2 资源管理要求

（1）云管平台

平台能够按照资源池进行管理，并对计算、存储、网络资源进行管理。

（2）异构能力

平台至少能够满足计算、存储资源的异构纳管能力。

（3）资源监控

平台能够对计算、存储、网络资源状态进行监控，对异常状态进行故障告警。

8.3 服务管理要求

（1）服务管理

对平台其他服务进行管理，如数据库、负载均衡、对象存储等服务进行集中管理，包括服务全生命周期的管理。

（2）服务编排

平台具备对多种服务进行资源编排，实现资源的水平扩展，快速交付。

9 平台基础能力要求

9.1 概述

工业互联网平台应采用功能模块化设计，并能够进行服务化封装，以方便不同功能模块之间的相互调用。工业互联网平台在实现时，应具有较强的弹性可扩展能力，以适应功能模块、数据资源、应用能力等的不断发展。

9.2 资源连接层要求

资源连接层负责与生产设备、自动化系统、智能产品、边缘网关以及外部数据源进行对接，主要包括接入管理功能和数据采集功能。

9.2.1 接入管理功能

9.2.1.1 连接功能要求

（1） 支持接入能力要求

a) 部署在工厂内部的工业互联网平台，应支持通过工厂内部网络与各种连接对象（指设备、系统、智能产品、边缘网关、数据资源）互联。

b) 部署在工厂外部的工业互联网平台，应支持固定网、移动网和互联网、专网等接入。

c) 应考虑支持数据通道、消息通道等多种信息传送通道。对于数据通道，应提供必要的数据安全机制，如支持 SSL、DTLS、TLS 等加密安全协议，支持 IPSec、L2TP 和 GRE 等隧道协议，并支持 IPv6/IPv4 双栈。

d) 支持数据路由功能。

（2） 支持接入安全

a) 连接对象在接入工业互联网平台时，应提供必要的认证鉴权过程，对非法接入进行拦截。

b) 连接对象功能限定，只能交互预定义的信息和内容，防止访问和篡改系统内部信息。

c) 应支持均衡连接，防止接入过载。

（3） 支持状态监控

a) 实时监控状态，如设备或智能产品的运行状态、电量状态等信息。

b) 监控网络链路状态，如链路通断状态、传输时延状态、路由状态等。

c) 监控设备应用状态。

（4） 接入质量要求

a) 保障连接对象的接入带宽、速率、时延、优先级等。

b) 保障接入数据的稳定性和系统可用性。

（5） 故障定位能力要求

需具备连接对象状态监测、连接链路状态监测等信息，判断故障所属范围和故障具体节点等。

9.2.1.2 连接对象管理要求

（1） 提供连接对象，特别是设备、智能产品、边缘网关的系统版本远程管理能力和系统配置远程更新能力。

（2） 提供连接对象的远程操控能力，如连接对象的关闭和接入隔离能力、管控设备在离线状态等。

（3） 可参考国际主流的连接性管理模型，如：GSMA DM 模型、OneM2M、LWM2M 模型。

9.2.2 数据采集功能

（1） 协议适配

资源连接层应支持Modbus、Profinet等工业以太网，实现对工厂内工业专用设备/控制系统的数据连接；应支持MQTT、RESTful、EDP、HTTP、OPC /OPC UA、COAP、XMPP等接口协议，实现工厂外智能产品数据的采集。

（2） 格式转换

资源连接层应能够规则引擎，将采集到的各种不同格式的数据转换成统一的格式。

（3） 数据清洗

资源连接层应支持对数据的清洗，去除无用数据。

（4） 数据传递

资源连接层进行初步数据处理后，应能将处理后的数据传送至数据共享层供进一步处理。

9.3 数据处理层要求

数据处理层主要提供对工业互联网数据的初步清洗、存储，并将数据与主题相关联，使数据进入相应的主题数据库。

9.3.1 数据准备功能

（1） 应支持数据预处理功能，包括检查数据一致性，对异常数据、缺失数据进行识别和处理，对冗余数据以及无用数据进行清理，以便适用于后续的建模分析。

（2） 应支持数据质量自动化监控，满足用户能够按照特定业务需求定制个性化的数据质量监控规则的要求。

（3） 应支持数据转换功能，根据数据存储方式对数据进行格式转换，并向用户开放数据的重组、拆分、映射等权限。

9.3.2 数据存储功能

（1） 应提供关系型数据库、离线大数据处理、分析型数据库、对象存储（非结构化数据存储）、NoSQL 数据库、缓存数据库等。

（2） 应提供批量计算、流计算、实时计算、查询计算等能力。

（3） 应支持结构化及非结构化存储；

（4） 应支持集中式存储和分布式存储

（5） 应支持 DAG（有向无环图）模式的并行作业模式；

（6） 应支持标准 SQL 和 MapReduce 分布式计算框架；

（7） 应支持基于图计算编程框架；

（8） 应支持流计算产品无缝集成；

（9） 应支持高并发低延时的数据处理。

（10） 应支持高速写入、读取；

（11） 应支持数据存储空间动态扩展；

（12） 应支持数据过滤，根据不同数据类型存入不同的数据库或数据表，同时对于一些干扰数据、错误数据进行过滤；

（13） 应支持数据字典，对于非规则数据的存储，例如用户二次打包的数据等，数据存储功能可以利用数据字典进行比对分析，获取真实数据，

进行存储；

（14） 应支持数据分级存储，对于实时性要求较高或访问频次比较高的数据，存入实时性较高的数据库，对于实时性要求不高或不经常访问的数据，直接存入长期数据保存数据库。同时，以天为单位，高实时性数据库将内容同步至长期保存数据库。

9.3.3 模型赋值功能

（1） 应支持根据连接对象和关注的主题，通过统一服务描述规范的封装方和控制功能组件，将数据进行组织和封装。

（2） 应能够确定数据库需管辖的范围和数据的组织形式。

（3） 应支持设备对象模型（通过抽象构建设备对象模型，以快速实例化不同设备）、生产过程模型（对不同产线进程过程模型化构建，实现系统协同机制）。

（4） 支持多类型多维度语义及模型，形成通用语义/模型库，支持不同类别企业数据的模型化赋值。

9.4 数据共享层要求

数据共享层主要提供物理数据、经营数据、能力数据、用户数据、产品数据相关的主题数据库，供数据分析层调用。

通过数据共享层进行共享的数据分为以下几类：

（1） 物理数据：指设备、车间、工厂等生产单元与智能制造相关的各类数据；

（2） 经营数据：指使用工业互联网平台的各类企业用户，在经营过程中产品销售、企业运营的各类数据；

（3） 能力数据：指可以通过工业互联网平台技能工人、各类专家、专业化服务机构进行开放能力，及相关能力被调用相关的描述数据，如能力定义、能力参数、能力提供的时间范围等；

（4） 用户数据：指使用工业互联网平台的企业、普通用户自身的描述数据；企业数据需包含企业名称、行业、业务范围、经营状况等数据；普通用户数据需包含用户名称、用户属性、年龄、资信状况等数据；

（5） 产品数据：指工业互联网平台可提供各类产品的相关数据，如产品名称、型号、应用领域、使用方法、操作手册等。

数据共享层应提供以业务共享主题数据为对象的数据仓库管理，以元数据、主数据、数据字典、编码数据为对象的基础数据管理、共享、调用服务，以工程协同数据为对象的工程协同数据管理、共享、调用服务。

不同主题数据之间可以组合形成集成性的主题数据库，如产线、工厂等主题数据库，构建对物理世界的完整视图和虚拟映像。

9.5 数据分析层要求

数据分析层主要提供数据报表、可视化、知识库、数据分析工具及数据开放功能，为各类决策的产生提供支持数据可视化、数据挖掘具体描述，看是否增加其他功能。

（1） 数据检索功能

根据用户请求从结构化或非结构化的大型数据库中实时地提取所需要信息的过程。

（2）OLAP（联机分析处理）功能

针对多维信息和特定问题的数据分析技术，需预先组建多维数据模型

（3）建模分析功能

a) 采用基于工业过程机理的建模，结合实际工业生产设备或场景进行数据分析

b) 采用特定的数据建模工具，结合实际工业生产设备、生产流程、应用场景以及分析目标，建立通用的基于统计的分析模型以及异常检测模型等，满足用户对于数据分析的通用性要求。

（4）机器学习功能

a) 利用线性回归、支持向量机（SVM）、神经网络等算法自动学习数据特征，并进行分析。

b) 利用 R、Python 等主要算法分析工具进行机器学习的预测性分析。

（5）数据可视化功能

a) 利用图形、图像处理、计算机视觉以及用户界面，通过表达、建模以及对立体、表面、属性以及动画的显示，对数据加以可视化解释。

b) 应支持助于图形化手段，清晰有效地传达与沟通信息。如统计图、2D/3D展示、AR/VR 等技术。

c) 根据可视化的原理不同可以划分为基于几何的技术、面向像素技术、基于图标的技术、基于层次的技术、基于图像的技术和分布式技术等。

9.6 应用使能层要求

应用使能层向应用开发者，提供开发支撑环境、运行支撑环境、服务调用与编排、业务运行管理和多租户管理等支撑功能，应用可以通过统一的调用接口（如SDK、WEB 服务）获取平台提供的云基础设施、数据、分析处理等能力。

（1）开发支撑环境

a) 应提供统一的大数据应用开发环境，支持 SQL、MapReduce、编程语言等，提供数据仓库可视化建模工具、大数据统计及分析（分布式）算法库和数据分析探索环境等。

b) 应提供 SDK 工具包，以及 Web 开发、APP 前端等集成开发环境。

（2）运行支撑环境

a) 应具有用户及权限管理机制，满足不同业务应用按需共享或独享同一平台内的相关资源，应支持用户按需使用不同模型算法分析处理所属范围的数据，同时支持细粒度授权方式的数据共享。

b) 应能够对平台内的所有作业任务进行统一的调度管理和运行监控，涵盖整个数据链路（数据同步、数据清洗、数据加工、数据分析等），涉及平台内所有的分布式计算能力。

（2） 服务调用与编排

应支持服务的调用、组合、调整、优化和路由，实现业务模型的敏捷建立。

（4）多租户管理

指面向客户需求的，以提高底层资源利用率，满足租户基础资源需求，同时满足数据、设备的安全性要求下的管理功能。需具备以下技术要求：

a) 资源与功能分配。应根据租户需求动态划分硬件、网络和计算资源，启闭服务和软件功能。

b) 环境与资源隔离。应对不同租户的应用程序运行环境和数据资源进行有效隔离，保证应用程序互不干扰、用户数据安全不泄密。

c) 计量管理。应能够对各租户使用的资源量、服务调用次数进行记录、统计和计费。

10 基础应用能力要求

工业互联网平台基础应用能力主要围绕产业链上下游协作，提供可重用的微服务或行业服务，支持面向产业链全环节的生产经营活动（如研发设计、生产制造、供应链和物流、产品运维等）开展数据和服务的供需对接和交易，实现平台用户之间、企业内部以及不同企业间的信息共享和服务协同。

10.1 云设计服务

（1） 可提供围绕研发设计的在线工具、计划管理、流程管理、数据、软件等资源。

（2） 可支持在线协同研发设计、在线仿真与分析、在线工艺设计。

（3） 可支持研发设计任务分发或众包、分工协作以及分布式、异地的研发设计协同等。

（4） 可支持研发设计任务在线跟踪、查询以及数据管理等。

（5） 可提供企业内和跨企业的设计文件/模型、工艺文件/模型的会签流转和模型管理功能。

10.2 云生产服务

（1） 可提供云 ERP、云 MES 等生产信息管理系统，并支持在线租用和调用。

（2） 可提供生产制造业务相关的跨企业计划排程、委托加工，可支持企业间生产制造业务的异地协作和无缝对接。

（3） 进行制造资源（如加工设备）的跨部门、跨企业、跨区域云端调用，可实现设备集成控制与管理。

（4） 可提供生产任务的在线跟踪、查询以及数据管理。

（5） 可支持个性化定制生产，可支持对产品尺寸、外形、数量、材料等个性化定制要求。

（6） 可提供智能生产经营管理服务，如车间生产管理与故障诊断维护、生产工艺与流程优化、生产制造过程的可视、透明、可控、智能等。

10.3 云供销服务

（1） 可向用户、生产企业、原材料供应商、物流企业、经销商提供接口，在平台上实现订单的生成及管理、信息跟踪等功能。

（2） 可实现生产企业内部，以及生产企业与渠道商之间订单、费用、成本、库存信息共享以及销售全过程管控。

（3） 可提供面向协作配套、屋子采购等业务的供需对接匹配。

（4） 可提供与工业企业营销为目的服务，如对供应链中的各个环节进行合理的评价与预测，对行业数据进行大范围的统计与挖掘分析。

10.4 云产品服务

（1） 可提供物联能力，实现产品信息采集，如设备的工况、位置、状态等。

（2） 可实现产品售后的在线检测、实时监控、故障预警、远程诊断、在线维护、预测性维护、质量优化、位置服务等。

（3） 可实现产品设计、生产、供销过程回溯，可提供解构分析能力，并以 SBOM（服务 BOM）为核心提供一机一册的构成分析查询。

（4） 可提供关联查询能力，提供设备与设备之间的关联关系查询，尤其是以成套设备组成的生产线的关联关系查询。

（5） 可提供备品备件预测能力。

（6） 可提供产品租赁功能。

（7） 可提供权证鉴定能力，包括资产所有权、资产控制权、资产管理权、资产使用权、资产出让权等。

（8） 可提供总体成本计算能力，通过记录设备的消耗，并汇总来计算该设备的总体拥有成本。

11 安全可信要求

11.1 管理视角下安全计划

工业互联网平台应在云基础设施、平台基础能力、基础应用能力的安全可信方面应制定五个基本计划活动：

（1）识别（Identify）：识别的管理系统，资产，数据和功能的安全风险。

（2）保护（Protect）：对平台实施安全保障措施，确保工业互联网平台能够提供服务。

（3）检测（Detect）：对平台使用、维护、管理过程实施适当的持续性监视和检测活动，以识别安全事件的发生。

（4）响应（Respond）：对平台使用、维护、管理过程制定和实施适当的应对计划，对检测到的安全事件采取行动。

（5）恢复（Recover）：对平台使用、维护、管理过程制定和实施适当的活动及维护恢复计划，以恢复由于安全事件而受损的任何能力或服务。

11.2 平台系统部署基本安全可信要求

11.2.1 端点保护

（1）云主机应进行监控和分析，包括完整性检查，检测恶意使用模式，拒绝服务活动。

（2）云主机实施安全策略和分析跟踪安全性能指标。

（3）采取数据保护手段以保持其数据的完整性，机密性和可用性。

11.2.2 通信和连接保护

（1）网络攻击防范

平台应部署高性能网络攻击防范手段，至少应支持入侵防御能力。

（2）DDoS 攻击防范

平台应部署 DDoS 攻击防范手段，至少支持对流量的按需清洗。

（3）鉴权管理

平台应支持多级权限管理体系（用户鉴权，应用鉴权，设备鉴权等），保证访问安全可监控。

11.2.3 安全性监视与分析

（1） 物理监视

应采取物理措施构造、管理和监视数据中心，提供 7X24 小时监视。

（2）监测预警

平台应部署网络安全监测手段，在发生严重入侵事件时应提供报警

（3）审计追溯

平台应对日常操作、网络流量进行记录审计，并能够对网络攻击行为进行追踪溯源。

（4）服务可审查性

应依法配合国家监管机构、司法机构等政府部门的安全检查，符合相关数据安全管理规定。应接受由政府或用户指定的第三方机构的审查和监测。

（5）监测无扰性

所有安全性监测行为应该无缝地贯穿平台的各层次，而不干扰任何操作业务过程。

（6）定期安全评测

平台应请第三方机构定期进行平台的安全评测，包括：风险分析、安全检查、安全评估、渗透测试等

11.2.4 安全配置与管理

（1）故障恢复能力

应具备完善的故障恢复机制，在服务发生故障时，应能在承诺时间内恢复业务至正常水平，并提供完整的故障报告。具体可参考数据中心联盟《云计算服务协议参考架构》第 5.10 节服务计量准确性。

（2）服务计量准确性

服务提供商应向用户提供服务计量的定价项和最小计量单位；在一个计费周期结束时提供计费详单。具体可参考数据中心联盟《云计算服务协议参考框架》第 9 章中的规定；如用户要求，应提供云主机服务的计费日志。

11.2.5 数据保护

不同的应用、数据应在独立隔离的环境中执行和保存。

11.3 云基础设施安全可信要求

（1）租户隔离

可根据不同用户需求，对不同租户进行物理或者逻辑隔离，保证业务服务不可互访，数据互不可见，或者在用户授权下进行有限访问。

（2）存储安全

平台采用分布式存储架构，且数据至少采用三副本，平台具备数据容灾备份能力，可定期对平台数据进行全量、增量进行备份，对于敏感数据，采用有效的数据加密方式。

（3）访问控制

平台具备外部访问鉴权机制，对用户权限进行集约化管理，遵循权限最小化原则，密码管理定期强制要求更换。

（4）运维审计

平台运维需通过堡垒机，运维人员操作日志异地备份，且可对高危操作进行审计。

（5） 漏洞管理

平台应具备自动化的漏洞管理控制，能够及时发现平台存在的安全漏洞并自动恢复。

11.4 数据安全要求

11.4.1 一般要求

（1）数据可销毁性

如用户终止服务、用户提出数据删除，除非有特殊约定，应立即删除数据；在存储设备报废时，应使用消磁、损毁等方式进行处理。

（2）数据可迁移性

在用户提出数据迁移需求时，应能够提供、镜像、数据和应用的迁入和迁出的服务。

（3）数据私密性

应实现不同用户的虚拟主机、应用的网络隔离，不同用户之间内网不可相互访问，或在用户授权的情况下才能获得数据。应遵守中国政府旨在保护用户信息

/隐私的相关法律法规。

（4）数据完整性

应能够检测到重要数据在传输、存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

（5）数据备份和恢复

应提供数据备份与恢复功能，应定期对重要数据进行备份并在灾难情况下及时恢复，保持业务连续运行。

11.4.2 接入安全

（1） 可提供面向连接对象和接入认证鉴权机制。

（2） 可提供安全的数据传送通道，如 HTTPS、TLS 等。

（3） 可提供加密机制，对连接对象（设备、系统、智能产品、边缘网关等）传送的数据进行加解密。

11.4.3 监控和分析数据保护

收集、通讯、存储敏感数据用于监控和分析的安全策略和规则要求如下：

（1） 禁止对员工和授权用户的监控，或者在监控前需要通知用户或者获得用户的许可；

（2） 禁止跨地理边界传输个人可识别信息（PII），或者在某个区域存储或者分析这类信息；

（3） 敏感数据需要防止被篡改。

11.4.4 配置和管理数据保护

安全管理维护不同时间安全的连贯性。安全管理不会因随操作过程而受到影响。安全元数据，例如连接状态和特征（加密的或者认证过的），收集设备安全控制状态并分享给运营管理系统。

（1） 安全元数据应该通过单独的通讯信道发送。

（2） 根据数据的重要性，在某些情况下，安全元数据应通过单独的物理网络适配器发送，如果设备仅有一个物理网络适配器，安全管理数据应在逻辑上进行分离（如，划分 VLAN）。

（3） 安全元数据应该符合特殊网络需求。例如，如果由于 OT 数据，网络

带宽受限，那么安全元数据需要符合带宽的限制，或者在网络负载更低的时候间隔突发传输。

（4） 需要向管理服务器上报安全元数据更新频率、吞吐、容量和周期的控制。

（5） 平台设计时需要考虑保护敏感数据，对敏感数据匿名化，并控制其留存周期和存储位置，以保证敏感数据被妥善删除。

（6） 应保证安全元数据不会被非故意修改，对终端节点应实施访问控制，例如在设备的配置项中设定或者在管理服务器的数据库中和终端节点的通信中。

12 运维管理要求

12.1 一般要求

12.1.1 物理资源

（1）物理资源状态监控。提供可按照资源池、集群对物理设备的资源状态、如计算、存储、网络等运行状态进行监控。

（2）故障告警及通知。支持Email或者短信、微信等告警的实时通知消息。

（3）资源库存及资产管理。支持对物理设备库存及资产管理，需要扩充及时提供运维管理人员。

（4）故障分析报表。可按照故障级别、事件类别出具故障的分析报表，便于改善服务。

12.1.2 业务资源

（1）业务资源状态监控。可按照服务如虚拟主机、云数据库、块存储等进行资源状态监控。

（2）业务资源容量监控。对业务资源层的资源容量进行分别监控，可设置容量告警阈值提醒资源扩容。

（3）运维操作记录。记录运维相关的操作日志且存档期不少于半年。

12.2 云服务运维管理要求流程

制定云服务运维管理流程，包括：服务台、事件管理、问题管理、变更管理、

配置管理、发布管理、知识库管理、报表管理。

云服务运维管理系统应提供以下功能：

（1）监控管理，通过对各种物理资源、虚拟化资源数据的监控，将资源以用户可见的资源池形式提供给上层应用。统一资源管理，支持发现其管辖范围内的物理设备（包括服务器、存储设备、交换机）以及它们的组网关系。支持将这些物理设备进行池化管理，提供给应用管理模块使用。

（2）权限管理，可以创建和管理系统中管理员帐号、管理员所承担的角色和管理员管理区域，实现系统的分权分域的功能。系统支持对用户进行访问控制，支持用户组、分权、分域、密码管理，便于维护团队内分职责共同有序地维护系统。

（3）告警管理，是确保系统正常运行的重要活动，包括：系统故障预防设计、故障检测和处理等。告警管理是故障管理的重要部分，便于运维人员进行故障定位，保证系统稳定运行。

（4）拓扑管理，提供一个可视化界面，呈现全系统的所有资源信息。支持常用设备自动发现和识别，系统还对网络类型有很好的兼容性，可以很好的发现VPN、VLAN网络拓扑，还支持按照规则识别不同的设备类型（如三层交换机），方便更准确的呈现拓扑。

（5）日志管理包括日志记录、查看、审计。

（6）软件管理，支持云操作系统软件预安装和预置、软件自动化批量安装、软件升级和补丁更新等功能。

（7）统计报表管理，可以让管理员查看虚拟机登录、分配以及运行状态信息，有助于系统优化，调整提升。报表可以根据要求定制，内容主要包括之前描述过得监控内容，包括CPU、内存、网络流量、数据库性能、中间件性能等各类性能报表和故障报表。

（8）资产管理，是运维管理系统的核心功能，能够实现对云平台相关的软硬件信息资产信息的全面管理，同时，对资产信息进行实时监控变更等功能，满足企业对资产管理的需要。

（9）工单管理，系统提供完整的工单管理的功能，支持创建工单的流转流程。支持手工创建工单，也可以在告警响应动作中创建工单；支持以工单方式实

现对告警事件的应急响应、工作任务分配、工作任务管理，可以进行流程定制和流程查看，工作流可以跨多个中心进行联动。

（10）计费管理，不同的云服务按照各自的计费项计量并收费的能力。

（11）安全管理，是对数据、账号等IT资源采取全面保护，使其免受犯罪分子和恶意程序的侵害，并保证云基础设施及其提供的资源能被合法地访问和使用。

（12）对系统数据均实现多副本保存或其他冗余备份机制。

（13）可实现云服务运维管理系统的自动化管理。

13 性能要求

工业互联网平台应满足以下主要性能指标要求：

（1）实例可用性不低于99.99%，数据可靠性不低于99.99%，满足自动宕机迁移、自动快照备份等要求。

（2）服务的数据应有本地副本；具有跨机房或异地备份的能力；数据持久性宜不低于99.999%。服务可用性宜不低于99.9%。

（3）满足资源弹性、自由配置要求，CPU、内存、带宽等关键资源可随时升级，升级配置数据不丢失，业务暂停时间可控。

（4）应能按照服务协议中承诺的流程和时间，根据用户需求完成对虚拟主机及其各服务模块配置的更改。