ICS 35.240.50
L 67

DB61

陕　西　省　地　方　标　准

DB 61/T 1232—2019

工业云系统建设技术规范

Technical specification for Construction of Industrial cloud system

2019－03－25 发布　　2019－04－25 实施

陕西省市场监督管理局　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则编写。

本标准由陕西省工业和信息化厅提出并归口。

本标准起草单位：西安邮电大学、陕西省信息化工程研究院、陕西工业云中心管理运营有限公司、陕西汽车控股集团有限公司、陕西思德睿产业发展研究院。

本标准主要起草人：朱志祥、张勇、刘翔、查虹、吴晨、董化一、潘正泰、宋文文。

本标准由陕西省工业和信息化厅负责解释

本标准首次发布。

联系信息如下：

单位：陕西省信息化工程研究院

电话：029-87303602

地址：陕西省西安市茶张路1号

邮编：710075

引　言

随着云计算、物联网、大数据等信息技术向工业领域融合渗透，工业云应运而生。工业云是一种面向工业的、通过网络将弹性的、可共享的资源和业务能力，以按需自服务方式供应和管理的模式。在我国，工业云是推进工业化和信息化深度融合的重要抓手。近年来，国家出台了《中国制造2025》、《关于深化制造业与互联网融合发展的指导意见》等一系列鼓励工业云发展的政策文件，明确指出应大力加强工业云建设。在国家政策的指导下，全国各地方政府纷纷着手制定工业云发展规划，着力建设工业云平台，积极推广工业云应用。

陕西省工业云经过几年的建设和发展已初具规模，并初显成效，为提高企业信息化水平、研发水平和制造能力、促进企业转型升级发挥了积极的作用。虽然业界对工业云市场发展前景一致看好，但目前陕西省工业云还处在初期建设阶段，工业云构建和实施过程中，缺乏有效指导，缺乏标准规范等导致工业云产业面临着一定的发展困境和障碍。因此，制定工业云建设与实施相关标准以促进工业云的快速发展和推广、提升陕西省工业云的市场竞争力，对促进陕西省智能制造、两化融合、产业升级等具有重要的意义。

工业云系统建设技术规范

1 范围

本标准规定了工业云系统建设过程中的设计、功能、实施、安全和运行维护要求。

本标准适用于工业云系统的总体规划、方案设计、工程实施、检验验收、运行维护以及与之相关的系统工程质量控制。

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，仅所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。

GB/T 9361 计算机场地安全要求

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/Z 20986 信息安全技术 信息安全事件分类分级指南

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 24363 信息安全技术 信息安全应急响应计划规范

GB/Z 24364 信息安全技术 信息安全风险管理指南

GB/T 50174 数据中心设计规范

GB/T 50326 建设工程项目管理规范

GB 50462 数据中心基础设施施工及验收规范

ISO/IEC 20000 信息技术服务管理

3 术语、定义

下列术语和定义适用于本文件。

3.1

工业云 industrial cloud

一种面向工业的通过网络将弹性的、可共享的资源和业务能力，以按需自服务方式供应和管理的模式。

3.2

工业云平台 industrial cloud platform

工业云基础设施及其上的服务的集合。

3.3

工业云系统 industrial cloud system

通过云计算、物联网、大数据和工业软件等技术手段，将人、机、物、知识等有机结合，为工业企业构建一种特有的服务生态系统，向用户提供资源和能力共享服务。

4 概述

工业云平台是工业云系统的承载平台，工业云系统是工业云平台的重要组成部分，负责对外提供工业云服务。工业云系统的建设活动包括：组织开展系统设计，明确系统功能，实施系统测试与验收，开展系统安全保障，开展系统运行维护工作。本标准围绕工业云系统建设活动的系统设计、系统功能、系统实施、系统安全和系统运行维护环节提出要求。

5 系统设计要求

5.1 总体规划

工业云系统应明确其总体规划，并满足以下要求：

a) 参照国家相关法律、法规、标准与规范要求，制定近期和远期工业云系统规划；
b) 制定工业云系统总体规划，包括总体目标、体系架构、基础设施、支持软件、信息资源服务、安全保障体系、运行保障体系等；
c) 根据系统实施的结果适时调整和修订总体规划及相关配套文件。

5.2 需求分析

需求分析是在总体规划指导下，对工业云系统需求的调研、梳理和分析，要求如下：

a) 应成立多方组成的团队，成员包括：建设者、管理者、使用者、运营者、专业机构等；
b) 应梳理和分析工业云系统的市场需求和应用发展需求；
c) 应以充分利用已有资源、节约成本、促进共享为原则，从实现业务应用、基础资源共享、互联互通、运行维护、安全保障等方面进行分析；
d) 需求分析形成的成果应以文档化方式呈现。

5.3 系统方案

依据需求分析对工业云系统进行设计，要求如下：

a) 系统方案内容包括体系架构、基础设施、信息资源、功能性能、部署、安全、运行维护、投资估算等；
b) 识别工业云系统建设相关的风险要素，提出风险规避措施；
c) 持续跟踪和评估工业云系统建设和实施情况，并视情更新方案。

6 系统功能要求

6.1 基本要求

工业云系统包含资源子系统、数据子系统、支撑子系统、应用子系统和运营子系统，要求如下：

a) 资源子系统负责与设计资源、制造资源、产品资源、人力资源等进行对接；
b) 数据子系统支持工业云的数据生命周期管理；
c) 支撑子系统提供工业云应用支撑能力；
d) 应用子系统为工业云用户提供个性化应用服务，支持产业链全环节的生产经营活动；

e） 运营子系统为工业云运营者和用户提供系统运营服务。

6.2 资源子系统功能

6.2.1 资源接入管理

资源接入管理要求如下：

a） 应支持通过工厂内部网络与各种连接设备、系统和数据等资源的接入；
b） 应支持专网、移动网和互联网等不同网络的接入；
c） 宜支持专用数据通道进行信息传送，并提供数据安全机制；
d） 应支持负载均衡和数据路由功能；
e） 应提供资源接入的认证鉴权功能，并支持防攻击和防篡改功能。

6.2.2 源状态监控

针对制造资源、产品资源等资源进行监控，要求如下：

a） 应支持对资源运行状态、使用率、流量等的监控；
b） 应支持对网络链路、传输时延、路由等状态的监控。

6.2.3 资源质量要求

针对制造资源、产品资源等资源提出质量要求如下：

a） 应保障资源的接入带宽、速率、时延、优先级等；
b） 应保障资源的稳定性和系统可用性。

6.2.4 资源对象管理

资源对象管理功能通常满足以下要求：

a） 应提供资源连接对象的远程管理能力；
b） 宜支持连接对象的远程操控能力，如对象接入、监控、隔离、关闭等。

6.3 数据子系统功能

6.3.1 数据采集

数据采集应满足以下要求：

a） 支持通信协议适配；
b） 支持数据格式转换。

6.3.2 数据处理

数据处理应满足以下要求：

a） 提供对工业云数据的清洗,将数据与主题相关联，并存入相应的主题数据库；
b） 支持数据预处理功能，包括数据一致性检查，异常数据、缺失数据识别和处理，冗余数据以及无用数据清理等；
c） 支持数据质量监控，包括完整性、可用性、准确性等方面。

6.3.3 数据存储

数据存储应满足以下要求：

a） 具备规范和完备的元数据；

b) 支持批量计算、流计算、实时计算、查询计算等能力；
c) 支持结构化及非结构化存储；
d) 支持高并发、低延时的数据处理；
e) 支持数据存储空间动态扩展；
f) 提供安全、可靠、冗余、备份与恢复的存储能力。

6.3.4 模型赋值

模型赋值应满足以下要求：
a) 根据统一服务描述规范封装和控制功能组件；
b) 支持构建设备、产线过程等实体模型；
c) 支持不同类别企业数据的模型化赋值。

6.3.5 数据共享

数据共享应满足以下要求：
a) 支持数据目录服务；
b) 支持不同主题数据库的交换和共享；
c) 不同主题数据之间可组合形成集成性的主题数据库，如产线、工厂等主题数据库。

6.3.6 数据分析

数据分析应满足以下要求：
a) 提供数据报表、可视化分析、知识库、数据分析工具；
b) 支持多维信息、特定问题、工业过程建模和统计分析等数据分析手段；
c) 支持数据分析结果的多形式可视化展示。

6.4 支撑子系统功能

支撑子系统功能应满足以下要求：
a) 提供大数据应用开发、部署、建模和分析环境；
b) 具有用户及权限管理机制；
c) 能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；
d) 提供业务应用建模，支持服务的调用、组合、调整、优化和路由能力。

6.5 应用子系统功能

6.5.1 云设计服务

云设计服务包含以下内容：
a) 可提供研发设计、项目管理、流程管理等工具；
b) 可支持在线协同研发设计、在线仿真与分析、在线工艺设计等；
c) 可支持研发设计任务在线跟踪、查询以及数据管理、文件模型的会签、变更流转等。

6.5.2 云生产服务

云生产服务包含以下内容：
a) 可提供智能生产经营管理服务，包括生产设备的集成控制与管理、生产任务在线跟踪管理和生产计划管理等；

b） 可提供网络化协同制造功能，包括跨企业计划排程、委托加工、异地协作等；
c） 可支撑个性化定制生产。

6.5.3 云供销服务

云供销服务包含以下内容：
a） 可向供应链提供订单生成管理、客户关系管理等功能；
b） 可实现订单、费用、成本、库存信息共享以及销售全过程管控；
c） 可提供面向协作配套、物资采购等业务的供需对接匹配；
d） 可提供与供销相关的统计、分析、挖掘、预测和评价等功能。

6.5.4 云产品服务

云产品服务包含以下内容：
a） 可实现产品在线检测、诊断、维护、优化等功能；
b） 可实现产品设计、生产、供销过程回溯，备品备件预测等功能；
c） 可提供产品租赁等功能。

6.6 运营子系统功能

运营子系统功能应满足以下要求：
a） 提供服务注册、发布、租用功能；
b） 提供服务的审核、监控、效能评估功能；
c） 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。

7 系统实施要求

7.1 系统实施

系统实施要求如下：
a） 系统实施过程应符合 GB/T 50326 的要求；
b） 应指定或授权专门的部门或人员负责实施过程的管理；
c） 应制定详细的部署方案；
d） 应制定实施方面的管理制度；
e） 可通过第三方机构协助控制实施过程。

7.2 系统测试

系统测试要求如下：
a） 应对系统执行功能测试；
b） 应对系统执行性能测试；
c） 应对系统执行安全测试；
d） 宜委托具有资质的第三方测试单位对系统进行测试，并出具测试报告。

7.3 系统验收

系统验收要求如下：
a） 应通过测试并经过试运行后组织系统验收；

b） 应指定或授权专门的部门负责系统验收管理；
c） 宜组织专家按照合同约定对系统进行验收，形成验收意见。

7.4 系统交付

系统交付要求如下：
a） 应制定详细的系统交付清单，按照交付清单核查所交付的软件；
b） 应对技术人员和用户进行培训；
c） 应指定或授权专门的部门负责系统交付的管理工作。

8 系统安全要求

8.1 基础环境安全

基础环境安全应满足以下要求：
d） 物理环境安全符合 GB/T 50174 和 GB 50462 的要求；
e） 物理环境场地安全符合 GB/T 9361 的要求；
f） 符合 GB/T 22239 中的三级及以上安全要求。

8.2 计算资源安全

计算资源安全应满足以下要求：
a） 启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
b） 当对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃取；
c） 严格控制用户对敏感信息的操作；
d） 保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录应至少保存 6 个月；
e） 对重要服务器进行监控；
f） 虚拟机宿主操作系统选择安全可靠，且通过国家安全测评认证的操作系统；
g） 实现平台虚拟主机的访问控制和身份鉴别，以及特权用户的权限分离；
h） 对虚拟资源的隔离提供有效的手段。

8.3 租户数据安全

租户数据安全应满足以下要求：
a） 建立多租户的服务组件隔离策略与规范；
b） 建立租户数据剩余信息保护、租户数据物理清除等规范与机制；
c） 建立多租户数据服务可用性保障策略和机制；
d） 建立覆盖数据生命周期的敏感数据监控和审计机制。

8.4 应用安全监测

应用安全监测要求如下：
a） 应建立应用程序注册和上线管理规程；
b） 应用系统试运行前应经过安全检查与安全扫描；
c） 应支持单点登录认证；
d） 宜建立有效的应用行为监控策略和规程；
e） 可支持用户自定义监控规则设置。

9 系统运维要求

9.1 一般要求

系统运维管理应符合ISO/IEC 20000的要求。

9.2 组织管理

组织管理应满足以下要求：

a) 建立运维管理部门，并配备管理人员，明确管理责任；
b) 建立运维责任制度，定期组织各项审查，形成审查报告。

9.3 人员管理

人员管理应满足以下要求：

a) 应根据运维服务内容为每个岗位配备运维人员；
b) 各岗位运维人员形成AB角色管理，关键岗位配备多人共同管理；
c) 制定培训计划并开展培训；
d) 建立运维人员管理制度，并严格执行。

9.4 风险评估

安全风险评估应符合GB/T 20984和GB/Z 24364的要求。

9.5 应急响应

应急响应应满足以下要求：

a) 信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件，具体分级参见GB/Z 20986；
b) 建立网络与信息安全事件信息接收机制；
c) 在统一的应急预案框架下制定不同安全事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
d) 应急预案符合GB/T 24363的要求；
e) 制定事件报告和处置管理制度，明确事件类型，规定事件的现场处理、事件报告和后期恢复的管理职责；
f) 在事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。