



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

工业互联网产业联盟标准

AI1/001-2025

工业边缘操作系统总体技术要求

General Technical Requirements for
Industrial Edge Operating Systems

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

工业互联网产业联盟

(2025 年 1 月 22 日)

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
Alliance of Industrial Internet

工业互联网产业联盟

联系电话：010-62305887

邮箱：aia@caict.ac.cn

目 次

编写说明	3
前言	4
1. 范围	5
2. 规范性引用文件	5
3. 缩略语	6
4. 术语和定义	7
4.1 操作系统 (Operating System)	7
4.2 边缘计算 (Edge Computing)	7
4.3 边缘节点 (Edge Computing Node)	7
4.4 边缘控制器 (Edge Controller)	7
4.5 边缘网关 (Edge Gateway)	7
4.6 边缘云 (Edge Cloud)	8
5. 工业边缘操作系统概述	8
5.1 工业云边端系统架构	8
5.2 工业边缘操作系统概念	9
6. 工业边缘操作系统参考架构	10
7. 工业边缘操作系统总体技术要求	11
7.1. 内核技术要求	11
7.1.1. 任务管理	11
7.1.2. 任务同步与通信	12
7.1.3. 内存管理	12
7.1.4. 中断管理	12
7.1.5. 时钟与定时器管理	13
7.1.6. 多硬件平台支持	13
7.1.7. 驱动管理	13
7.1.8. 其他要求	14
7.2. 基础能力组件技术要求	14
7.2.1 基础网络协议栈	14
7.2.2 容器框架组件	14
7.2.3 系统升级组件	15
7.2.4 远程管理组件	15
7.3. 工业能力组件技术要求	16

7.3.1 工业控制组件	16
7.3.2 工业通信组件	17
7.4. 安全能力组件技术要求	17
7.4.1 信息安全要求	17
7.4.2 功能安全要求	18
7.5. 混合部署技术要求	21
7.6. 应用接口技术要求	21
附 录 A	22
A.1 工业边缘操作系统典型业务场景	22
A.2 工业边缘操作系统典型部署方案	24
参考文献	26



编写说明

新型工业化以信息化与工业化深度融合为主线，以技术创新为驱动，以提高质量和效益为中心，通过产业结构优化升级，推进制造业向智能化、绿色化和服务化转型，提高产业链的附加值，促进经济高质量发展。国家高度重视新型工业化，并将其提升至关系全面推进强国建设的战略高度。随着信息化与工业化融合不断深入，传统工业 ISA-95 架构向云边端架构演进，L1 设备控制和 L2 过程控制将主要由边缘设备节点承载，工业边缘业务大幅增多。

工业边缘操作系统作为关键基础软件，是工业边缘应用和硬件系统的桥梁。工业边缘操作系统允许在边缘设备本地进行数据处理，减少了对云服务的依赖，提高了数据安全性、隐私保护和效率，能够支持多种协议和标准，以适应不同类型的工业设备和应用场景。工业边缘操作系统对下可屏蔽底层硬件差异，对上应用生态的核心。目前工业边缘操作系统缺少统一能力要求，影响工业边缘应用生态发展。通过编制工业边缘操作系统总体技术要求标准，可为工业边缘应用提供通用、标准的基础能力，对降低工业边缘设备研发成本，促进边缘应用生态繁荣，具有重要的技术价值和生态价值。

前言

本文件依据 GB/T1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由工业互联网产业联盟提出并归口。请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件起草单位：

中国移动通信集团有限公司、华为技术有限公司、中国信息通信研究院、中兴通讯股份有限公司、麒麟软件有限公司、施耐德电气（中国）有限公司、英特尔（中国）有限公司、高通无线通信技术（中国）有限公司、中国联合网络通信集团有限公司研究院、北京东土科技股份有限公司、飞腾信息技术有限公司、北京国科环宇科技股份有限公司、思博伦通信科技（北京）有限公司、鹏城实验室、北京邮电大学

文件主要起草人：刘玮哲、张悦、杨博涵、马帅、李蒙、李波、严镭、陈波、余德钊、蔡圣明、王元、张文远、王哲、胡钟颢、徐立锋、赵孝武、楚俊生、束裕、郭皓、王震、张衍顺、陈俊瑀、张亚平、王虎文、张宇、陈卓、刘洋、张文博、安岗、程远、郭丽萍、王迥波、宋加侨、杨威、李壮、徐微、刘志立、王岩、王彬、蒋俊、唐泉、李弘宇

工业边缘操作系统总体技术要求

1. 范围

本文件规定了工业边缘操作系统的参考架构以及工业边缘操作系统各层级技术要求。同时资料性附录 A 给出了工业边缘操作系统典型业务场景和工业边缘操作系统典型部署方案。

本文件适用于工业边缘操作系统以及应用的设计、开发和测试，也为应用软件开发商提供参考。

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。

GB/T 11457—2006 信息技术 软件工程术语

GB/T 20438—2017 电气/电子/可编程电子安全相关系统的功能安全

GB/T 34040—2017 工业通信网络 功能安全现场总线行规 通用规则和行规定义

YD/T 4494—2023 工业互联网边缘计算 边缘节点模型与要求 边缘网关

YD/T 4670—2024 工业互联网边缘计算 总体架构与要求

YD/T 1665T—2018 工业互联网边缘计算 需求

T/CSAE 298—2023 智能网联汽车车控操作系统功能安全技术要求

A11-007/2021 工业互联网边缘计算 边缘控制器技术要求与测试方法

A11-008/2021 工业互联网边缘计算 边缘网关技术要求与测试方法

3. 缩略语

下列缩略语适用于本文件。

AMP: 非对称多处理 (Asymmetric Multi-Processing)

BI: 商业智能 (Business Intelligence)

BO: 业务对象 (Business Object)

CMSIS: (ARM) Cortex 微控制器软件接口标准 (Cortex Microcontroller Software Interface Standard)

ERP: 企业资源计划 (Enterprise Resource Planning)

FOTA: 空中固件升级 (Firmware Over-The-Air)

GUI: 图形用户界面 (Graphical User Interface)

IEC: 国际电工委员会 (International Electrotechnical Commission)

IPC: 进程间通信 (Inter-Process Communication)

ISA-95: 国际自动化协会95标准 (International Society of Automation 95)

ISO: 国际标准化组织 (International Organization for Standardization)

ISR: 中断服务程序 (Interrupt Service Routine)

MES: 制造执行信息系统 (Manufacturing Execution System)

MMU: 内存管理单元 (Memory Management Unit)

NTP: 网络时间协议 (Network Time Protocol)

OS: 操作系统 (Operating System)

POSIX: 可移植操作系统接口 (Portable Operating System Interface)

PTP: 精确时间同步协议 (Precision Time Synchronization Protocol)

SMP: 对称多处理 (Symmetric Multiprocessing)

SOTA: 空中软件升级 (Software Over-The-Air)

TSN: 时间敏感网络 (Time-Sensitive Networking)

USB: 通用串行总线 (Universal Serial Bus)

4. 术语和定义

下列术语和定义适用于本文件。

4.1

操作系统 (operating system)

控制各种程序的执行并可提供资源分配、调度、输入输出控制以及数据管理等服务的软件。

4.2

边缘计算 (edge computing)

在靠近物或数据源头的网络边缘侧,融合联接、计算、存储、应用核心能力的开放平台,就近提供边缘智能服务,满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私等方面的关键需求。

4.3

边缘节点 (edge computing node)

边缘网关、边缘控制器、边缘云等具有数字化、网络化、智能化的共性特点,在边缘计算中提供网络、计算、存储等 ICT 资源的物理设备。

4.4

边缘控制器 (edge controller)

工业制造现场,将生产数据汇总发送到云端的边缘控制器(单元)。

4.5

边缘网关 (edge gateway)

用于局域网范围的时间同步，按需保证生产单元或者设备维度的精准交互。通过网络联接、协议转换等功能联接物理和数字世界，提供轻量化的联接管理、实时数据分析及应用管理的网关。

4.6

边缘云（edge cloud）

位于网络边缘侧，连接多个边缘网管，提供连接管理、数据管理、应用管理功能的低延时、轻量化的服务器。

5. 工业边缘操作系统概述

5.1 工业云边端系统架构

ISA-95（IEC/ISO 62264）通过制定工业控制系统与企业信息系统集成框架，推动企业全局运营与车间生产的集成，从而被广泛接受和应用。随着工业数字化、智能化和网络化的发展，工业生产体系架构进一步扁平化，工业体系架构向端边云三层体系架构演进，参见图 1。



图 1 ISA-95 向云边端架构演进

上述架构演进中，工业云平台是一种基于云计算技术的面向工业领域的综合性服务平台。工业云平台主要帮助制造业企业实现资源优化配置、生产效率提升、产品质量改进以及服务创新，包括 BI/BO、ERP、MES 等功能，对应 ISA-95 架构中 Level-3-Level-5 层级。工业边缘包括工业现场边缘和工业网络边

缘，主要对应 ISA-95 架构中 Level-1、Level-2 层级以及部分 Level-3 层级。典型的工业边缘设备包括边缘控制器、工控机、边缘网关、边缘服务器等。工业终端则包括工业现场的传感器、执行器、仪器仪表等，对应 ISA-95 架构中 Level-0 层级。

5.2 工业边缘操作系统概念

工业边缘操作系统是管理工业边缘设备硬件并为工业边缘应用提供服务的系统软件。工业边缘操作系统运行在工业边缘设备上，为其提供硬件抽象描述，管理分配计算、存储、网络资源，为应用提供任务切换、任务间通信、安全防护等基础功能以及工业相关的行业能力，同时为应用提供相关调用接口。工业边缘操作系统可以承载工业控制、数据采集、连接汇聚、工业 AI 等各类业务。

随着工业边缘计算的蓬勃发展，边缘设备类型和业务种类不断增多。尽管边缘设备硬件规格伸缩范围大，边缘业务对操作系统的要求各异，操作系统的实现方式也各不相同，但工业边缘操作系统具有统一的技术特征：

a) 从云边端整体架构看，工业边缘操作系统运行在工业边缘设备硬件与工业边缘应用之间，同时与工业端侧和工业云侧通信，支持端侧接入和云侧对接。

b) 从操作系统自身结构看，工业边缘操作系统主要由操作系统内核、能力组件和应用接口等部分组成。其中，分层结构和提供工业相关行业能力是工业边缘操作系统的典型特征。参见图 2 所示工业边缘操作系统组成。

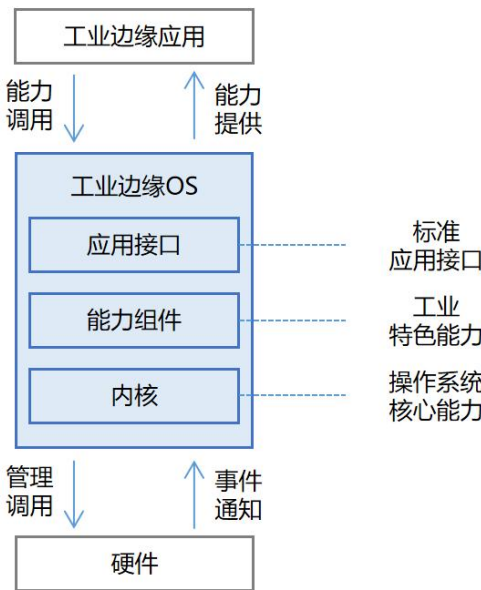


图 2 工业边缘操作系统组成

c) 从工业边缘应用看，工业边缘操作系统主要包括：

- 1) 互联互通：支持工业网络、IT 网络中各网元的连接互通、协议转换、柔性组网等。
- 2) 数据处理：支持端侧数据采集、数据加工、数据存储、数据诊断等。
- 3) 工业控制：支持逻辑控制、运动控制、过程控制等工业控制应用。
- 4) 工业 AI 集成：支持工业视觉检测、实时监控与预测性维护、生产过程优化等。

更多典型业务场景以及对功能、性能要求分析参见附录 A.1.

d) 从工业边缘操作系统部署方式看，典型的部署方案可分为：

- 1) 实时部署：为边缘应用提供实时性保障，支持工业控制、实时数据处理等业务。
- 2) 非实时部署：为边缘应用提供更高的灵活性，允许在不影响系统稳定性的情况下进行软件更新和系统配置更改。适用互联互通、数据采集类业务。
- 3) 混合部署：在同一设备上提供实时应用与非实时应用并行环境，以实现高效、稳定和灵活的工业自动化解决方案，支持工业控制集中化部署或者工业控制与 AI 融合等业务。

具体部署方式分析参见附录 A.2.

6. 工业边缘操作系统参考架构

工业边缘操作系统参考架构参见图 3，其中实线框图属于必选组件，虚线框图属于可选组件。整体上遵从分层设计，从下向上依次分为：

- a) 虚拟层提供虚拟化功能，允许在单一物理硬件上运行多个独立的操作系统实例或虚拟环境；
- b) 内核层包括内核和驱动两部分。内核是工业边缘操作系统的核心部分，为操作系统提供保障运行的核心功能，主要包括任务管理、内存管理、中断管理、时钟管理、IPC 通信以及多核管理等。驱动为操作系统提供硬件支撑，是

操作系统与硬件设备之间进行交互和控制的软件组件，提供硬件设备统一接口等；

c) 能力层包括基础能力组件和工业能力组件，其中基础能力组件通过内核接口来调用操作系统的各个内核功能，同时开发者也可以直接通过内核接口调用内核功能。工业能力组件是面向工业应用提供的多个功能组件模块，如各种控制等；

d) 接口层面向开发者提供工业应用开发的系统调用接口、能力组件接口、Posix 接口和 CMSIS 接口；

e) 信息安全组件提供数据安全、网络安全、系统安全和固件安全；

f) 功能安全组件提供内核、通信层、接口层和虚拟化层的功能安全保障。

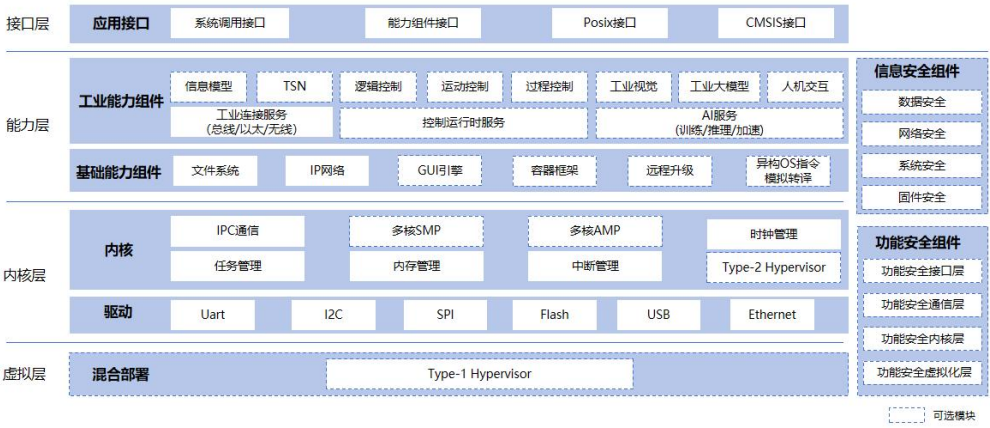


图 3 工业边缘操作系统参考架构

7. 工业边缘操作系统总体技术要求

7.1. 内核技术要求

内核的功能应包括任务管理、内存管理、中断管理、时钟管理和定时器管理等，宜支持多核管理。

7.1.1. 任务管理

任务管理实现对任务的创建、启动、睡眠、阻塞、挂起、唤醒及销毁等操作和资源分配或调度。其中，任务调度作为任务管理的关键部分，负责任务在

多种状态之间切换，包括初始状态、就绪状态、运行状态、睡眠状态、阻塞状态、挂起状态和关闭状态等。

a) 非实时部署时，任务调度支持功能包括：

- 1) 应支持抢占式调度和非抢占式调度；
- 2) 应支持不少于一种的调度器。调度器可分为公平调度、空闲调度、限期调度、停机调度、实时调度等；
- 3) 应支持任务调度器设置与优先级设置；
- 4) 应支持任务与特定CPU核绑定；
- 5) 应支持负载均衡。

b) 实时部署时，任务调度支持功能包括：

- 1) 应支持优先级继承，防止优先级翻转；
- 2) 应支持实时任务；
- 3) 任务调度开销应满足任务实时性要求；
- 4) 应支持任务与特定CPU核绑定。

7.1.2. 任务同步与通信

通过任务间通信，实现任务同步、数据交换。

- a) 应支持任务同步，包括但不限于互斥锁、读写锁、信号量。
- b) 应支持任务间通信，包括但不限于管道、消息队列、共享内存等。

7.1.3. 内存管理

内存管理用于对系统中内存空间进行动态管理，使得系统中的任务可以根据实际情况动态申请和释放内存。

1. 应支持任务的虚拟内存和物理内存的分配和回收。
2. 应对不同任务的物理内存进行隔离。
3. 应支持虚拟地址与物理地址转换。
4. 应支持不同任务对内存的访问权限保护，如读写权限保护。
5. 宜提供内存使用情况的诊断和监控工具，帮助维护人员了解系统状态，及时发现问题。

7.1.4. 中断管理

中断管理负责处理系统软硬件中断，响应系统软硬件事件。

1. 应支持中断优先级的配置和管理，确保系统能够根据中断的重要性和紧迫程度及时响应。确保高优先级的中断能够优先得到处理，而不会因为低优先级的中断而延迟。

2. 宜支持中断嵌套，允许更高优先级的中断打断当前正在处理的中断服务例程。

3. 应支持用户编写ISR来响应特定的中断事件，ISR通常要求简短且无参数传递。

4. 应支持中断的启动和禁用。

5. 应支持中断处理的注册和注销。

6. 宜支持中断屏蔽，提供开启或关闭中断机制，以及在必要时屏蔽中断，以保护关键代码段不被打断。

7. 宜同时支持硬实时中断和软实时中断。硬实时中断由外设或硬件定时器触发，软实时中断由系统根据需要进行处理。

7.1.5. 时钟与定时器管理

负责管理系统时钟和定时器的创建、执行、超时处理等。

1. 应支持系统时钟节拍管理。

2. 应支持创建微秒级单次定时器和周期性定时器。

3. 应支持触发超时时间等定时器设置。

4. 应支持定时器查询。

5. 宜支持多种时钟源，以适应不同的精度和环境要求。

6. 宜支持时钟的校准和调整，以补偿时钟源的漂移。

7.1.6. 多硬件平台支持

实现内核在不同架构下的移植运行等功能。

1. 宜支持ARM、RISC-V、X86、MIPS、LoongArch、Alpha等处理器架构。

2. 宜支持对运行操作系统内核的CPU核心数量的配置。

7.1.7. 驱动管理

驱动程序管理是操作系统内核中负责管理和控制硬件设备的一组软件组件和接口，它定义了驱动程序与操作系统及其他硬件或软件组件之间的交互方式（如实现设备管理、资源分配、数据传输、错误处理、性能优化等）。驱动程

序框架是指为开发特定操作系统的驱动程序所需的软件和硬件的集合，即驱动程序开发环境。

1. 应允许驱动以内核模块的形式存在，方便加载和卸载。
2. 宜支持统一的驱动程序框架，便于驱动程序开发集成。
3. 宜针对不同的处理器架构提供优化驱动程序，提高系统整体性能。

7.1.8. 其他要求

1. 应具有信息安全相关设计，包括安全启动等，具体参见 7.4 节。
2. 应提供内核裁剪、配置工具，根据不同芯片规格、业务场景选择内核能力。
3. 宜支持低功耗管理功能包括：
 - a) 处理器开关、频率和电压调整等。
 - b) 休眠和唤醒机制等。

7.2. 基础能力组件技术要求

7.2.1 基础网络协议栈

基础网络协议栈组件提供 TCP/IP 网络协议栈，实现 TCP/IP 网络连接功能。

1. 应支持 IPv4 网络协议，宜支持 IPv6 网络协议。
2. 应支持 TCP、UDP 等传输协议。
3. 应支持 HTTP 协议，宜支持 HTTPS 协议。
4. 宜支持 MQTT、WebSocket 等应用协议。

7.2.2 容器框架组件

容器作为一种轻量级虚拟化技术，在低资源开销条件下为应用提供了虚拟化隔离、可移植、跨环境一致性能力，具有易于部署扩展、易于支持微服务架构等优势。容器编排也为应用提供了自动化部署能力。若操作系统提供容器框架组件，需满足：

1. 应支持容器虚拟化框架，包括容器镜像的加载、运行、停止等。
2. 应支持容器编排框架，包括容器的部署、管理、扩展和网络连接等。

3. 容器编排框架宜支持服务发现和负载均衡，确保应用程序的可访问性和性能。

4. 容器编排框架宜支持集中式日志记录和监控，持续监控应用程序的运行状况和性能，以排除故障。

7.2.3 系统升级组件

该组件提供系统升级能力，支持系统版本更新、漏洞修复、系统或应用更新等。需满足：

7.2.3.1 离线系统升级

1. 应支持外部存储介质升级，将升级文件存储到 USB 闪存、SD 卡等外部存储介质，激活升级功能或进行系统重启后完成升级。

2. 宜支持局域网络升级，将升级文件存储到升级组件内置的文件服务器上，激活升级功能或进行系统重启后完成升级。

3. 宜支持系统升级失败后自动回退升级前的版本。

7.2.3.2 在线系统升级

1. 宜支持 FOTA 升级，通过网络下载更新包并对完整性、安全性校验后，对操作系统、驱动程序和底层固件进行更新，系统重启后完成升级。建议采用差分方式进行 FOTA 升级。

2. 宜支持 SOTA 升级，通过网络下载应用开发者提供的应用更新包，由应用加载器进行加载，无需重启设备即可对具体应用进行更新。

3. 宜支持系统升级失败后自动回退升级前的版本。

7.2.4 远程管理组件

该组件提供对边缘设备的远程接入、远程监控、远程调试等功能。远程接入是指用户通过网络连接访问位于不同地理位置的计算机系统或资源。远程监控是通过网络对远程设备、系统或环境进行实时监测和管理的过程。远程调试是在远程位置通过网络对软件、硬件或系统进行调试和故障诊断的过程。若操作系统提供远程管理组件，需满足：

1. 宜支持用户访问远程计算机上的文件、应用程序和数据库等资源。

2. 宜支持管理人员远程登录服务器进行系统配置、更新和维护等操作。
3. 宜支持实时监控设备的运行状态和性能指标，及时发现并处理异常情况。
4. 宜支持远程连接到服务器或设备，检测硬件组件及软件的状态，定位并解决故障。

7.3. 工业能力组件技术要求

7.3.1 工业控制组件

工业控制组件为用户提供工业控制相关能力。若操作系统提供工业控制组件，需满足：

7.3.1.1 控制运行时服务

工业控制运行时服务能够加载用户逻辑控制程序，高速率、低延迟、稳定可靠地运行。

1. 应支持 IEC-61131-3 或 IEC-61499 工业控制标准。
2. 应支持控制任务的创建、加载、调度、终止，且具有执行模式、周期、优先级管理能力。
3. 应满足控制任务实时性要求。包括工业控制系统的响应中断、任务调度、执行任务的时间延迟和抖动的要求。
4. 应满足控制任务长时间稳定运行要求，提供相关错误处理、日志诊断、故障恢复机制。
5. 宜支持控制任务的在线调试和监控。
6. 宜支持 C/C++、Python、Lua 等高级语言控制程序执行。

7.3.1.2 运动控制

1. 应支持速度控制与精确位置控制能力，满足基本的运动轨迹规划功能。
2. 宜支持高级轨迹规划功能，满足高精度和复杂运动的需求，提升运动控制性能。

7.3.1.3 过程控制

1. 应支持基本的逻辑运算与判断能力，并做出相应的控制决策。
2. 宜支持定时驱动或事件驱动的逻辑控制能力。
3. 应支持复杂逻辑表达式的解析和执行，以满足复杂控制需求。
4. 应支持 PID 控制等过程控制能力，实现对生产过程的某一或某些物理参数的自动控制。
5. 应支持优化控制提高过程性能和效率。

7.3.2 工业通信组件

工业通信组件为用户提供工业总线、工业以太、工业无线等互联互通能力。工业通信组件包含如下技术要求：

- a) 应支持 NTP（网络时间协议）或 PTP（精确时间协议），以确保各个设备和节点的时钟同步。
- b) 宜支持 Modbus、CANopen、Profibus、DeviceNET、CC-LINK 等工业总线协议。
- c) 宜支持 EtherCAT、Profinet、Ethernet/IP、Powerlink 等工业以太协议。
- d) 宜支持 TSN、DetNet 等确定性传输技术。

7.4 安全能力组件技术要求

7.4.1 信息安全要求

7.4.1.1 数据安全要求

1. 宜支持数据加密。在边缘设备上对敏感数据进行加密存储和传输，确保数据的机密性和完整性。加密算法应选用经过广泛验证和认可的算法：

- a) 应支持国密算法 SM2/3/4。
- b) 宜支持 RSA、AES、轻量化对称密钥算法 KeyWrap。
- c) 宜支持断点解密。
- d) 宜支持链式循环解密算法。

2. 宜支持设备敏感信息安全存储。确保边缘设备用户数据存储安全，包括抗篡改设计、安全退役。

3. 宜支持数据备份和恢复。建立数据备份和恢复机制，确保在发生安全事件或系统故障时，能够快速恢复数据和业务。

7.4.1.2 网络安全要求

1. 宜支持端到端加密。在数据传输过程中采用端到端加密技术，确保数据在传输过程中不被窃取、伪造或篡改。

2. 宜支持安全通信协议。采用安全的通信协议（如 TLS/DTLS）进行数据传输，确保数据的机密性和完整性。

7.4.1.3 系统安全要求

1. 宜支持安全隔离，将不同的应用、服务或用户群体隔离在不同的安全区域中，降低安全风险。

2. 宜支持实时监控。采用实时监控工具，对边缘计算环境中的网络流量、系统日志、安全事件等进行实时监控。

3. 宜支持日志分析。建立日志分析机制，对收集的日志进行关联分析，发现潜在的安全威胁和异常行为。

7.4.1.4 安全固件管理

1. 宜支持安全启动。确保设备在启动时只加载经过验证的引导程序和内核，防止 rootkit 恶意软件的植入。

2. 宜支持固件签名验证。对固件进行签名验证，确保固件未被篡改，来自可信的源。

3. 宜支持安全更新。定期发布安全更新和补丁，修复已知的安全漏洞和弱点。

7.4.2 功能安全要求

参考 GB/T 20438-2017（IEC61508）功能安全定义，作为相关受控设备（EUC）总体安全的一部分，功能安全依赖于电气/电子/可编程电子（E/E/PE）安全相关系统功能正确的 EUC 控制系统以及其它安全相关系统技术和外部风险降低措施。若操作系统支持功能安全要求，需满足：

7.4.2.1 内核层功能安全要求

安全能力组件的内核层包含如下功能安全要求：

a) 操作系统内核的地址空间应被保护，并为应用程序提供访问内核地址空间的安全接口；

b) 操作系统内核应为用户态应用程序提供资源隔离机制，以保证资源访问相互隔离，并提供措施约束每个进程在执行过程中不会使用超过其预先分配的资源；

c) 操作系统内核应支持内核空间的异常处理。当非法系统调用、堆栈溢出、指针异常访问、内存越界、死循环、死锁、超时等异常发生时，内核应立即调用异常处理程序并进入相应的安全状态（如内核日志转储、报警、降级、重启或关闭等）；

d) 操作系统内核应支持安全相关线程的异常处理。当一个安全相关线程出现超时错误、内存错误、指令错误等异常时，操作系统内核应立即调用该线程的异常处理程序；

e) 操作系统内核应支持接口调用安全保护。当出现传递非法地址、无效参数、非法的上下文等不正确的内核服务接口调用时，内核调用接口不应执行对应的服务，不应导致内核崩溃，并且立即返回错误代码；

f) 操作系统内核应监控每个用户态进程的 CPU、内存等资源消耗；

g) 在多核处理器上，当操作系统内核在一个处理器核心上检测到异常并且需要关闭操作系统时，应同时在所有其他处理器核心上关闭该操作系统。

7.4.2.2 虚拟化层功能安全要求

虚拟化管理器需具备相关硬件及软件故障的诊断、故障上报、故障处理以及故障恢复机制。

a) 虚拟化管理器应支持对硬件和软件的安全诊断测试。在初始化虚拟环境时，应对硬件模块进行功能验证、对低安全等级的软件组件进行功能安全监控。如果安全诊断测试不通过，应根据故障类型停止初始化，同时应上报故障。

b) 虚拟化管理器应支持安全故障处理。对于需要立即处理的安全相关故障，虚拟化管理器宜使系统进入安全状态（如日志转储、报警、重启或关闭等）。

c) 虚拟化管理器应支持虚拟机之间的通讯访问权限管理。

7.4.2.3 通信层功能安全要求

参照 IEC61784-3 定义的黑色通道实现安全通信，检查通信数据包中由于硬件随机故障、现场干扰、伪装攻击、软件逻辑问题产生的大部分数据错误，保证数据的完整性、身份鉴别和时间正确性。

a) 应通过反馈报文、数据完整性保证（包括奇偶校验、CRC 校验、和校验及异或校验）等方式避免数据的讹误。

b) 应通过序列号、时间戳、带交叉验证的冗余等方式避免数据的错序或意外重复。

c) 应通过序列号、反馈报文、带交叉验证的冗余等方式避免数据的丢失。

d) 应通过时间戳、时间预期等方式避免数据的不可接受的延时。

e) 应通过序列号、时间戳、连接认证、反馈报文、带交叉验证的冗余等方式避免数据的插入。

f) 应通过连接认证、反馈报文、不同的数据完整性保证系统等方式避免数据的伪装。

g) 应通过连接认证等方式避免数据的寻址出错。

7.4.2.4 接口层功能安全要求

安全能力组件接口层包含如下功能安全要求：

a) 系统调用接口应支持接口调用安全保护。当传递非法地址、无效参数、非法的上下文等不正确的调用时，系统调用接口应返回错误代码或执行回滚等，不应执行对应的服务，不应导致内核崩溃或安全隐患；

b) 应用软件接口应满足以下安全要求：

1) 应用软件接口应提供默认初始化参数值，以在启动时进行初始化处理；

2) 应用软件接口应对输入参数的类型、取值范围进行校验，当检测到参数异常时，需要返回异常值，并明确具体的错误种类；

3) 应用软件接口宜通过不同的模块来进行数据校验，并对安全相关的数据进行备份，来保证功能数据的正确性；

4) 当不能收到功能模块的通知或调用 API 返回异常或调用 API 无法返回时, 应用软件接口应进入相应的安全状态 (如读取默认的配置数据、模块重启、记录日志或通知应用模块等)。

7.5. 混合部署技术要求

工业边缘操作系统宜支持混合部署技术要求。混合部署技术有利用工业现场减少部署成本, 降低部署难度, 并实现简单高效的资源动态调整。若操作系统提供混合部署组件, 需满足:

- a) 宜支持虚拟化混合架构部署, 可作为混合架构的一个子操作系统被其他虚拟化平台管理。
- b) 宜支持 AMP 混合架构部署, 多个操作系统独立部署在不同核心上运行。
- c) 宜支持至少一种 AMP 通信技术, 包括 rpmsg、ivshmem、virto 接口等。

7.6. 应用接口技术要求

工业边缘操作系统应用接口包含如下技术要求:

- a) 应符合具体某个操作系统编程接口规范, 如 GJB、IEEE1003.1、ISO 26262、IEC 61131 等;
- b) 对 ARM 芯片架构, 宜支持 ARM 微控制器软件接口标准 CMSIS 规范。

附录 A

(资料性)

工业边缘操作系统典型业务场景与部署方案

A.1 工业边缘操作系统典型业务场景

工业边缘典型业务场景包括：

a) **互联互通**：包括网联无人车、AGV 作业生产调度、远程设备操控等。具体业务场景如下：

- **网联无人车**：依托车辆管理平台，实现多类型网联无人车统一管理运营，远程操控无人车实现工业园区的无人化巡逻作业。
- **AGV 作业生产调度**：AGV 作业生产调度平台通过从 AGV 获取视频及位置等数据，实现作业计划编排、作业规范及完成度监控等功能。
- **远程采掘**：控制中心通过将远程控制信令下发至采煤机、掘进机等矿用设备控制终端，实现设备的一键启停、远程操作控制等功能。

面向上述场景，操作系统需支持低延迟内存管理，最大内存延迟应小于 10ms，避免内存碎片，支持至少 16GB 内存分配和动态调整。调度系统应支持多核处理器（六核以上），任务调度时延小于 10ms，确保实时任务优先。网络协议栈需保证端到端时延小于 200ms（远程控制小于 100ms），上行带宽至少 30Mbps，下行带宽 40Mbps。视频流传输应保证每台摄像头 4Mbps 上行、2Mbps 下行，网络可靠性 99% 以上。提供硬件加速支持，确保网络处理和视频编解码无阻塞，系统可靠性需达到 99.99%。

b) **数据处理**：包括传大规模数据采集、工厂设备监控等。具体业务场景如下：

- **大规模数据采集**：通过将工厂内大量不同设备数据进行解析并上传至平台，实现对数据的统计分析、可视化呈现，生产管理人员可掌握工厂的实时生产状态，辅助其优化生产决策，提升生产效率。业

务需求：端到端传输时延要求小于 50ms，需要至少 10Mbps 的上行带宽、10Mbps 的下行带宽，可靠性 99.99%。

- 工厂设备监控：工厂设备监控系统可接入多种工厂物联网设备，如智能电表、智能水表、烟感传感器等。设备采集来的数据接入管理后台，通过对数据加工、汇总，可视化展示工厂的经营情况，并可在平台上对设备进行管理，预防设备故障和安全隐患。业务需求：端到端传输时延要求小于 50ms，需要至少 10Mbps 的上行带宽，可靠性 99.9%。

面向上述场景，操作系统需支持高效内存管理，最大内存分配至少 16GB，内存延迟小于 10ms，避免碎片。调度系统需支持多任务并发，任务切换延迟小于 10ms，确保实时响应。优化网络协议栈，支持 10Mbps 上行和下行带宽，端到端时延小于 50ms，网络可靠性 99.99%。数据处理能力要求达到 10MB/s，确保大规模数据采集与处理。提供容错机制和自动恢复功能，确保系统可靠性达到 99.9%，稳定支持设备监控与数据统计分析任务。

c) **工业控制**：包括离散控制、运动控制，过程控制、远程控制等。具体业务场景如下：

- 离散控制：广泛应用于产线输送和物流等领域，例如：电动单轨输送系统（Electrified Monorail System, EMS）、工艺 AGV、分拣机、堆垛机等。
- 运动控制：在需要精确机械移动的应用中，如 CNC 机床和机器人臂，边缘计算可以实现低延迟的运动控制，确保机械设备按照预设路径精确移动。通过边缘控制技术，可以实现多轴或多机同步操作，这对于实现复杂组装或搬运任务尤为重要，保证操作的高效性和准确性。
- 远程控制：广泛应用于流程行业远控类业务，例如行车远控、龙门吊远控、煤机远控等，主要通过监测和调节生产参数来确保产品质量、优化生产效率。

面向上述场景，操作系统需支持低延迟内存管理，内存分配延迟小于 5ms，最大内存分配至少 16GB，确保高吞吐量数据处理。调度系统应具备实时任务

优先级调度，任务切换时延小于 5ms，支持高频次中断处理，满足端到端传输时延要求。网络协议栈需保证端到端时延小于 30ms（运动控制 2-10ms），且支持 10Mbps 以上带宽，确保数据传输稳定。抖动控制应小于 1ms（运动控制），提供 99.99%至 99.9999%的系统可靠性，确保高效稳定运行。

d) **工业 AI 集成**：包括生产安全行为分析、无人智能巡检、机器视觉质检等。具体业务场景如下：

- **生产安全行为分析**：针对垂直行业工业领域的智慧车间、智慧工厂、工业园区等细分行业的生产安全场景，基于 AI 视频结构化分析技术实现生产安全行为分析应用。
- **无人智能巡检**：利用机器人对工厂设施进行定期巡检，提高巡检效率和准确性。
- **机器视觉质检**：通过将高清图像实时回传至 AI 平台，经过图像识别后进行控制指令快速下发，实现远程图像数据解码与数据不出厂。

面向上述场景，操作系统需支持高效内存管理，最大内存分配至少 128GB，内存分配延迟小于 10ms，确保 GPU 处理和大规模数据缓存。调度系统需支持实时任务优先级调度，任务切换延迟小于 5ms，确保图像处理和控制指令快速响应。网络协议栈需保证端到端传输时延小于 20ms（无人巡检 15ms），上行带宽 100Mbps、下行带宽 20Mbps，可靠性 99.99%。支持高效视频流传输与图像解码，确保数据处理不出厂且网络稳定。

A.2 工业边缘操作系统典型部署方案

从工业边缘操作系统部署方式看，典型的部署方案可分为以下三种。

a) **实时部署**：为边缘应用提供实时性保障，支持工业控制、实时数据处理等业务，能够有效管理复杂的系统资源，为争夺 CPU、内存、网络带宽等资源的多个实时任务合理地分配资源，使每个实时任务在最坏情况下的实时性要求都能得到满足，同时可以实现 us 级任务、中断响应，时间响应确定性等功能。采用实时部署的典型设备如边缘控制器。

b) 非实时部署：为边缘应用提供大吞吐保障，适用互联互通、数据采集类业务，负责管理众多的进程并为它们分配系统资源，尽量缩短系统的平均响应时间并提高系统的吞吐率，在单位时间内为尽可能多的用户请求提供服务。采用非实时部署的典型设备如边缘网关或边缘服务器等。

c) 混合部署：在同一设备上提供实时应用与非实时应用的并行环境，支持工业控制集中化部署或者工业控制与 AI 融合等业务，在保障实时性的同时，提供丰富的应用能力。采用非实时部署的典型设备如边缘网关或边缘服务器等。

	实时部署	非实时部署	混合部署
边缘控制器	●		●
边缘网关		●	●
边缘服务器		●	●

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

参考文献

- [1] 面向工业智能化时代的新一代工业控制体系架构白皮书，2023，工业和信息化部装备工业发展中心
- [2] 面向 5G 行业终端的实时计算技术研究报告，2022，5G-AIA



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