ICS 35.240.50
CCS L 66

团 体 标 准

T/CEATEC XXX—2025

自主无人系统具身智能体通用架构规范

General architecture specification for embodied agents in autonomous unmanned systems

（征求意见稿）

2025-X-XX 发布 2025-X-XX 实施

中国欧洲经济技术合作协会 发 布

目　　次

前言

本文件按照GB/T 1.1—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。

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专利的责任。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件为首次编制。

自主无人系统具身智能体通用架构规范

1 范围

本文件规定了自主无人系统具身智能体（以下简称“具身智能体”）的设计原则、总体架构和接口规范等内容。

本文件适用于各类自主无人系统的具身智能体研发设计、生产制造、测试验收、应用部署及升级维护。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 34977 信息安全技术 移动智能终端个人信息保护技术要求

GB/T 35114 公共安全视频监控联网信息安全技术要求

GB/T 35116 物联网 传感器接口规范

GB/T 35134 信息技术 数据元素值格式记法

GB/T 39218 信息安全技术 工业控制系统信息安全防护能力评价方法

GB/T 41867 信息技术 人工智能 术语

3 术语和定义

GB/T 41867界定的以及下列术语和定义适用于本文件。

3.1

具身智能体 embodied agent

基于人工智能、机器人学、物联网等技术，具备物理实体载体，通过“感知-决策-执行-反馈”闭环与物理环境实时交互，实现自主感知环境、动态认知决策、精准执行任务及持续学习进化的智能系统。

3.2

具身感知 embodied perception

结合载体自身物理形态、运动状态与环境交互数据，实现多维度、多尺度环境信息采集与解读的感知方式，区别于脱离物理载体的纯数据感知。

3.3

多智能体协同 multi-agent collaboration

多个具身智能体通过数据交互、任务分工、资源共享实现复杂任务协同完成的模式，包括分布式决策与集中式调度两种核心类型。

3.4

动态认知决策 dynamic cognitive decision-making

具身智能体架构的核心功能，指基于具身感知层输出的标准化数据，通过场景建模、目标识别分类、任务规划、行为决策及自主学习模块，实现动态环境适配与突发情况应对的过程。

4 设计原则

4.1 具身融合原则

架构设计需深度结合载体物理特性（尺寸、载重、运动方式、机械结构），实现感知、决策、执行与载体形态的有机统一，确保智能功能与物理载体协同适配，避免智能模块与载体脱节导致的性能损耗或功能失效。

4.2 动态适配原则

支持对不同任务场景的自适应调整，核心参数可配置率≥90%，场景切换时无需重构核心架构，仅通过参数优化即可实现适配。

4.3 高可靠原则

关键模块（感知核心模块、认知决策模块、能源管理模块、安全控制模块）采用冗余设计，单点故障不导致系统整体失效，重要功能模块应具备故障自诊断与自动切换能力。

4.4 伦理安全原则

决策逻辑设计需要建立人类优先的决策机制，避免产生危害人类生命安全、侵犯个人隐私、破坏生态环境或违背公序良俗的行为。

4.5 可迁移原则

架构核心模块（如认知决策算法框架、数据治理模块、交互协同接口）应具备跨载体迁移能力，可迁移至不同类型自主无人系统载体（如从无人机迁移至无人地面车辆），迁移适配成本≤30%（以研发工时计）。

4.6 模块化原则

采用模块化、组件化设计，各功能模块边界清晰、接口标准化，支持模块的按需拆卸、替换与扩展，模块更换时不影响其他模块正常运行。

5 总体架构

5.1 架构框架

具身智能体采用“五层两支撑”的模块化、可扩展架构设计，实现感知、认知、执行、协同的全流程闭环智能，同时通过安全防护与数据治理两大支撑体系保障系统稳定、安全、可靠运行。具体架构框架如图1。

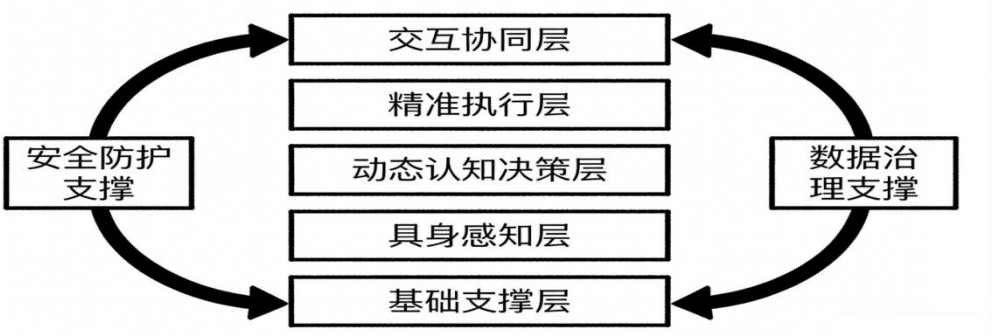

图1 自主无人系统具身智能体架构框架

5.2 分层架构定义

5.2.1 基础支撑层

为具身智能体提供硬件运行平台、能源供给与动态管理、系统资源调度及设备驱动适配，是整个架构的底层保障，支撑各功能层级的稳定运行。

5.2.2 具身感知层

基于多模态传感器实现环境、自身状态及任务目标的精准感知，通过数据融合技术提升感知可靠性与准确性，输出标准化、高质量的感知数据，支撑动态认知决策层功能实现。

5.2.3 动态认知决策层

架构的智能核心，基于具身感知层输出的标准化数据，实现场景建模、任务规划、动态决策及自主学习，具备动态环境适配与突发情况应对能力，输出精准的决策指令。

5.2.4 精准执行层

将动态认知决策层输出的抽象指令转化为载体的物理动作与任务设备的操作，实现运动控制、设备驱动及执行状态反馈，保障执行精度与响应速度。

5.2.5 交互协同层

实现具身智能体与人、其他智能体及外部系统的协同交互，支持指令输入、状态展示、任务协同及数据传输，保障交互的便捷性与协同的高效性。

5.2.6 安全防护支撑

以“嵌入式”方式融入所有功能层级，形成“事前预防-事中监控-事后应急”全链条防护机制，作为架构的“安全中枢”，提供功能安全、信息安全及伦理合规保障，避免系统故障、数据泄露或伦理风险导致的安全问题，为各层级运行提供强制性安全保障，确保系统在复杂场景下的可靠运行。

5.2.7 数据治理支撑

贯穿所有功能层级与业务流程，负责数据的全流程规范化管理，实现具身智能体全生命周期数据的采集、存储、传输、处理、销毁全流程管理，保障数据质量、安全与可用性，同时通过数据分析赋能智能决策，是系统自主学习与性能优化的核心支撑。

5.3 分层架构模块

5.3.1 基础支撑层

基础支撑层组成模块如下：

a) 硬件平台模块：采用模块化硬件架构，支持 CPU、GPU、FPGA 异构计算，CPU 主频≥2.5GHz，GPU显存≥8GB，FPGA 逻辑单元≥500K；硬件接口支持 PCIe 4.0、USB 3.2、Ethernet、CAN FD 等，接口数量满足至少8路传感器接入需求；

b) 能源管理模块：支持多类型能源接入，具备能源状态监测（电压、电流、剩余电量）、消耗预测、动态分配功能；配备过充、过放、过温、短路保护单元，支持节能模式切换，能源模块外壳具备防火、防冲击能力，意外碰撞时无爆炸、起火风险；

c) 资源调度模块：采用分布式资源调度算法，支持 CPU、GPU、FPGA 算力动态分配，算力分配误差≤10%，支持多任务并行调度，任务调度延迟≤20ms，核心任务（感知、决策）优先级最高，资源占用率保障≥70%；

d) 设备驱动模块：兼容主流传感器、执行器、通信模块的驱动协议，支持即插即用；驱动程序更新周期≤6个月。

5.3.2 具身感知层

具身感知层组成模块如下：

a) 多模态传感器配置模块：至少配置视觉传感器、激光传感器、惯性传感器、定位传感器和环境传感器组合，满足不同场景感知需求；

b) 数据预处理模块：采用卡尔曼滤波、中值滤波等算法进行数据降噪，降噪后数据信噪比≥30dB；支持多传感器时间同步，同步误差≤10ms，数据格式标准化为 Protobuf，支持批量数据压缩传输；

c) 多模态数据融合模块：采用基于贝叶斯估计的多传感器融合算法，具备传感器故障检测与容错融合能力，单一传感器故障时融合精度衰减≤10%。

5.3.3 动态认知决策层

动态认知决策层组成模块如下：

a）场景建模模块：采用基于 SLAM 的动态环境建模算法，支持障碍物分类与风险等级评估，建模数据支持三维点云、栅格地图两种格式输出，满足不同决策需求；

b）任务规划模块：支持全局路径规划（A算法）与局部路径重规划（RRT算法），支持多任务优先级调度，具备任务中断与恢复能力，恢复后任务执行连续性≥98%；

c）动态决策模块：基于强化学习算法构建决策模型，建立人类优先的决策机制，碰撞风险场景下优先避让人类，支持决策参数动态调整，适配不同任务场景；

d）自主学习模块：支持在线学习与离线学习两种模式，在线学习收敛时间≤2h，离线学习模型更新周期≤24h；学习过程不影响核心任务执行；具备基于任务执行反馈的模型优化能力。

5.3.4 精准执行层

精准执行层组成模块如下：

a）运动控制模块：支持平移、旋转、启停等运动控制，采用 MPC（模型预测控制）与 PID 控制算法融合方案，支持运动参数动态调整，适配不同载体平台；

b）任务设备驱动模块：支持机械臂、作业工具、载荷设备等驱动控制和设备故障检测；

c）执行状态反馈模块：实时采集运动状态、设备运行状态数据，反馈数据包括位置、姿态、速度、设备工作参数、故障信息等，确保动态认知决策层实时获取执行状态。

5.3.5 交互协同层

交互协同层组成模块如下：

a）人机协同模块：支持多模态人机交互，包括语音交互、视觉交互、触控/按键交互；支持紧急干预功能，紧急停机响应时间≤100ms；

b）多智能体协同模块：支持多智能体分布式通信与集中式调度，采用 MQTT 协议进行协同数据传输，数据传输成功率≥99.9%（常规场景）、≥99.8%（复杂场景），支持任务分工、资源共享、冲突协调，协同任务完成成功率≥96%（常规场景）、≥90%（复杂场景）；

c）系统互联模块：支持与后台管理系统、第三方设备的互联互通，支持数据上传与指令接收，接口兼容主流工业协议（Modbus、OPC UA）。

5.3.6 安全防护支撑

安全防护支撑组成模块如下：

a）功能安全模块：监控安全相关系统的运行状态，包括执行器故障检测、安全回路完整性校验、紧急停机控制。支持 SIL 2 级避障功能与 SIL 3 级紧急停止功能，确保执行环节的安全可控；

b）信息安全基础模块：执行身份认证与数据加密，采用国密 SM2 算法实现身份鉴别，通过 SM4 算法完成数据传输与存储加密，为数据交互与存储提供基础安全保障，满足 GB/T 35114 三级保护要求；

c）伦理安全模块：负责决策逻辑的伦理合规校验，强制执行“人类优先”机制，在碰撞风险、人员靠近等场景中，优先触发避让、停机等安全指令；同时对采集的图像、位置等敏感数据进行脱敏处理，脱敏率100%，避免隐私泄露；

d）硬件安全增强模块：执行核心硬件监控、传感器/执行器冗余切换、环境防护状态监测功能；

e）入侵防御模块：具备实时入侵检测与主动防御能力，通过流量分析、行为识别等技术，精准识别暴力破解、恶意代码注入等攻击行为，并能自动阻断非法连接，保障系统网络安全。

5.3.7 数据治理支撑

数据治理支撑组成模块如下：

a）数据采集规范模块：制定统一的传感器数据采集标准，包括数据格式、采集频率（按传感器类型差异化配置）、数据合法性校验规则，确保原始数据的一致性，符合 GB/T 35134要求；

b）数据存储管理基础模块：负责结构化与非结构化数据的分类存储，配置 SSD+SD 卡冗余存储，支持本地存储与云端备份，数据保存期限可按需配置，保障数据的可存储性与完整性；

c）数据安全基础模块：建立 RBAC 三级权限控制体系（管理员、操作员、访客），符合 GB/T 34977 要求；

d）数据预处理与校验模块：执行数据清洗、去重、补全、同步校准功能。采用卡尔曼滤波、中值滤波等算法优化数据质量，为多源数据融合提供可靠基础，同时建立数据质量评估指标体系，实时监测数据质量状况，对低质量数据触发告警并自动启动数据修复流程。

6 接口规范

6.1 接口分类

接口分类如下：

a) 内部接口：涵盖架构各层级间、构件间的交互接口，用于内部数据流转、指令传输与服务调用，覆盖感知、决策、执行全流程内部协同需求；

b) 外部接口：涵盖人机交互、多智能体协同、跨系统互联接口，用于与操作人员、其他智能体、外部系统的交互协作，支撑多场景应用部署。

6.2 通用要求

6.2.1 协议要求

内部接口采用 TCP/IP、CAN FD、RESTful API协议；外部接口兼容 USB 3.2、蓝牙 5.0、MQTT 3.1.1、OPC UA等协议；所有接口需支持数据校验，校验失败支持自动重传，符合 GB/T 35116要求。

6.2.2 格式要求

格式要求如下：

a) 结构化数据采用 JSON 格式，非结构化数据采用 Protobuf 压缩传输，数据帧含帧头、类型、长度、内容、校验位、帧尾；

b) 指令类数据描述应符合 GB/T 35134要求。

6.2.3 时序要求

时序要求如下：

a) 内部接口延迟：层级间数据接口≤20ms，控制指令接口≤10ms，服务调用接口≤50ms；

b) 外部接口延迟：人机交互≤500ms，多智能体协同≤100ms，跨系统互联≤200ms；

c) 传输频率：感知数据≥10Hz，状态反馈≥5Hz，控制指令≥20Hz，支持动态调整。

6.2.4 容错要求

异常检测准确率≥99.5%，支持连接中断自动重连、数据丢失重传，关键数据必重传，非关键数据可填充默认值，重连失败触发告警，确保系统运行不中断，安全容错符合 GB/T 39218要求。

6.3 内部接口规范

6.3.1 基础支撑层与其他层级接口

基础支撑层与其他层级接口如下：

a) 供电接口：DC 12V/24V 双电压输出，电压波动≤±2%，供电功率≥500W（地面设备）/≥100W（空中设备），具备过充、过放、过温保护；

b) 算力调度接口：动态分配CPU/GPU/FPGA 算力，核心层级算力保障≥70%，调整步长10%；

c) 设备驱动接口：支持传感器、执行器即插即用，驱动加载时间≤500ms，适配成功率≥98%。

6.3.2 功能层级间交互接口

功能层级间交互接口如下：

a) 具身感知层与动态认知决策层：感知数据传输速率≥10Mbps，延迟≤20ms，数据准确率≥96%；决策层参数配置指令响应≤10ms；

b) 动态认知决策层与精准执行层：控制指令响应时间≤10ms，执行状态反馈频率≥20Hz，反馈数据完整性≥99%；

c) 交互协同层与各功能层级：外部指令按优先级传输，1级紧急指令响应≤5ms；系统状态数据更新频率≥5Hz。

6.3.3 支撑体系与功能层级接口

支撑体系与功能层级接口如下：

a) 安全防护支撑各层级：安全监控指令响应≤5ms，告警准确率≥99.8%，应急处置指令优先级最高；

b) 数据治理支撑各层级：数据存储响应≤50ms，检索响应≤100ms，数据备份频率≥1次/h。

6.4 外部接口规范

6.4.1 人机交互接口

人机交互接口如下：

a）语音交互接口：输入采样率 16kHz，安静环境识别准确率≥90%、嘈杂环境≥85%，支持30+常用指令；输出音质≥16bit/44.1kHz，音量可调，多语言切换响应≤500ms；

b）视觉交互接口：显示分辨率≥1920×1080，刷新率≥60Hz，画面无延迟；图像采集支持 1080P 分辨率，手势识别准确率≥85%、人脸解锁成功率≥95%，响应时间≤500ms；

c）触控/按键接口：触控支持≥5点多点触控，响应≤200ms，操作精度≤1mm；实体按键含紧急停机键、功能按键。

6.4.2 多智能体协同接口

多智能体协同接口如下：

a）协同通信接口：采用 5G/Wi-Fi 6传输，带宽≥100Mbps，延迟≤100ms，丢包率≤0.1%；身份认证采用 SM2 算法，认证流程≤500ms，失败拒绝通信；

b）协同控制接口：任务分配接口接收指令；冲突协调接口实时交互意图。

6.4.3 跨系统互联接口

跨系统互联接口如下：

a）后台管理系统接口：数据上传支持实时与批量两种模式，上传成功率≥99.5%；指令接收接口执行远程控制；

b）物联网平台接口：数据交互格式为 XML/JSON，交互成功率≥99.5%；资源共享接口共享状态信息、接收环境预警；

c）第三方设备接口：硬件扩展支持 PCIe 4.0/USB 3.2 等接口；数据交互采用自定义格式，延迟≤200ms，容错率与内部接口一致。