KUTESMART · KTOS

KTOS

企业智能操作系统
产品白皮书

以**企业治理**为根，让业务事实、流程、人员与**数字员工**在同一套责任体系中协同运行，把 AI 真正带进企业的业务现场。

治理驱动 · 事件驱动 · 规则打底 · 证据闭环

V4.1 2026 年 10 月

青岛酷特智能股份有限公司

关于本白皮书

本白皮书系统介绍 KTOS 企业智能操作系统的产品定位、设计理念、产品体系、架构与运行机制、应用场景、集成与安全、交付与实施方法，以及客户价值的测算与评价方式。

文档名称	KTOS 企业智能操作系统产品白皮书
版本	V4.1（2026 年 10 月）。在 V4.0 基础上做结构性优化：统一产品全景与能力归属口径，补充经营目标闭环、数字员工体系、端到端交付、能力转移、收益测算与能力状态矩阵。
适用读者	企业决策者、业务负责人、信息化与数字化负责人、实施顾问及产业合作伙伴
产品范围	KTOS 统一底座；酷小易、酷小智、酷小匠三大原生产品；EOS 业务运行底座与制造业务应用
发布单位	青岛酷特智能股份有限公司

按角色阅读

读者	建议重点	可以获得的答案
企业决策者	执行摘要、第 1–4 章、第 15 章	KTOS 解决什么问题、经营目标如何落到执行、价值如何测算
业务负责人	第 4、7–10 章	岗位如何办理工作、数字员工承担什么、异常如何被处置
信息化负责人	第 5、6、11、12 章，附录 C	产品边界、部署拓扑、非功能要求、安全责任与能力现状
实施与合作伙伴	第 13–15 章、附录	端到端交付、能力转移、阶段验收与收益测算方法

版权与使用说明

本白皮书版权归青岛酷特智能股份有限公司所有。未经书面许可，任何单位和个人不得以任何形式复制、修改或传播本文内容。

本文介绍的产品能力会随版本迭代。各项能力的当前状态见附录 C“能力状态矩阵”；模块启用、算法约束、外部接口及具体交付范围，以所选版本、双方正式合同、项目方案及验收标准为准。

文中图示用于解释产品机制，示例订单、数量、测算数据均为说明用途，不构成客户效果承诺。客户名称与量化案例在获得授权并完成事实核验后方可用于公开传播。

目录

从企业问题出发，经过产品定义、核心机制与业务场景，落到交付方法与价值测算。

— **执行摘要** 4

01 **行业背景与企业挑战** AI 时代的企业核心断点 5

02 **产品概述** 定位、设计理念与系统关系 7

03 **核心价值与差异化优势** KTOS 的六项关键主张 9

04 **企业治理与经营目标** 从经营目标到执行证据与复盘的闭环 11

05 **产品全景与能力归属** 产品全景图 · 能力归属矩阵 · 三大原生产品 13

06 **架构与工程化** 技术分层、部署拓扑、非功能要求与容错 16

07 **核心运行机制** 对象、主锚、主线、流程、工作卡与数字员工 19

08 **智能工作台** 岗位任务、批次办理与对话即工作 22

09 **制造业务应用** 订单、研发、计划、制造、质量、仓储、采购等 24

10 **典型应用场景** 订单全生命周期四流 · 缺料 · 变更 · 质量 26

11 **集成与开放** 业务承担方、数据映射与可靠写入 28

12 **安全与可信治理** 身份、权限、模型约束、审计与安全责任边界 30

13 **企业初始化与持续进化** 酷小智从需求到可验收应用的端到端机制 32

14 **实施方法与能力转移** 阶段交付物、角色分工、验收标准与陪跑 34

15 **客户价值与收益测算** 指标基线、测算模型与投入产出 36

16 **源于实践，走向产业** 实践基础与发展愿景 38

附 **附录** 术语表 · 技术规格 · 能力状态矩阵 40

EXECUTIVE SUMMARY

执行摘要

KTOS 是面向 AI 时代的企业智能操作系统。它构建在企业现有系统之上，以企业治理为根基，让业务事实、知识、规则、流程、人员与数字员工在统一的责任体系中协同运行。

企业面临的问题

多数企业已拥有 ERP、MES、WMS、CRM 等系统，数据也已在线，但跨部门工作仍依赖人工查数、解释和催办。一张临近交期的订单可能同时牵涉技术资料、物料缺口、生产安排和质量放行，需要有人把分散的事实组织成处理方案。通用 AI 助手让回答变快，但回答与业务责任、正式操作之间依然隔着一道墙。

KTOS 的解决方式

KTOS 把企业的经营目标、岗位、制度和经验转化为可运行的结构：以**业务本体**统一业务语义，以**业务事件**捕捉变化，以**业务主线**判断进展，以**流程**组织办理，以**数字员工**承担资料准备与受控判断，以**工作卡**把需要处理的事项、材料和允许动作交到责任人手中，并用一条**证据链**串起全过程，最终回到经营指标的复盘。

酷小易 · 企业 AI 经营执行官

让风险主动浮现、判断有据、行动可追踪，连接经营洞察与执行闭环。

酷小智 · 企业 AI 应用生长官

把管理方法与业务变化转化为模型、规则、流程与数字员工，负责交付与持续生长。

酷小匠 · 制造业产业智能体

把客户需求语言转译为产品方案、BOM、工艺与生产协同，让需求直达制造。

三大原生产品运行在 KTOS 统一底座之上，由 **EOS 业务运行底座**把能力落到订单、计划、生产与交付现场。

六项差异化主张

① 治理驱动，而非工具堆叠

先定义企业应如何运行，再让 AI 参与运行。

② 激活现有系统，按领域选择承担方

保留 ERP、MES、WMS 等投资，也可选用内置应用，自由组合。

③ 规则打底，模型增强

能算清的交给规则，需要理解的交给数字员工；模型不可用时业务不中断。

④ 流程驱动，责任落人

数字员工绑定岗位，只做准备与受控判断；正式决定与写入经授权确认。

⑤ 以证据判定完成

业务是否完成看真实凭证，而不是按钮状态；一条证据链可追溯全过程。

⑥ 交付即产品，持续生长

标准能力预制 + 企业初始化 + 灵活配置，变更分层、版本可回退。

如何开始

从一条订单履约链或一类高频异常切入，建立数据、责任与指标基线，用真实业务结果验证异常发现、跨部门等待与交付表现，再逐步扩展。

01 INDUSTRY CONTEXT

行业背景与企业挑战

系统、数据和 AI 工具越来越多，企业却仍缺少统一的理解、判断、协同、执行与持续进化能力。

本章要点

- 企业软件正在从“记录工具”走向“智能运行环境”。
- 新的瓶颈不是系统数量，而是把信息组织成责任与行动的能力。
- AI 若不能进入企业的语境、权限、流程与责任，就只能停留在局部助手。

1.1 企业软件正在进入新的角色阶段

ERP、MES、CRM、OA 和各类 SaaS 把企业业务带入系统，完成了记录、标准化和流程在线化的使命。但当市场变化更快、客户需求更分散、跨部门关系更复杂时，企业面对的新问题是：数据已经在线，为什么风险仍靠人发现？系统很多，为什么经营仍需层层汇报？经验丰富，为什么组织每次仍从头判断？

阶段	系统主要角色	解决的问题	企业获得的能力
信息化	记录工具	把纸面业务搬进系统	业务可记录
网络化	连接平台	连接客户、供应商与员工	组织可连接
数字化	流程与数据系统	规范流程、呈现数据、提升效率	业务可协同
智能化	**企业智能操作系统**	**理解变化、辅助判断、驱动行动**	**组织可感知、可决策、可进化**

1.2 四个普遍存在的断点

断点一　信息在线，工作仍靠人串联

销售看订单与交期，计划看资源与排程，采购看供应承诺，生产看工单与报工，质量看检验与放行。一次交期风险往往需要同时读取这些事实；缺少共同对象和状态口径时，同一问题在报表、群聊和会议纪要中被反复解释。

断点二　变化发生，处理机制滞后

供应商修改到货时间、工艺版本变化、现场出现不合格品，都可能影响订单履约。变化发生后，如果没有监听条件、责任岗位和处置入口，就只能等人主动发现并协调。

断点三　经验在个人，难以复用

资深人员知道何时催料、如何判断延期影响、哪些变更必须复核。这些方法若不能沉淀为对象、规则与作业规程，组织每次都要重新判断，对“个人英雄”的依赖难以降低。

断点四　AI 可用，却进不了责任体系

通用大模型能回答问题、起草文本，却不知道企业的岗位、权限、单据状态和审批要求。“建议调拨”与“仓库已经调拨”之间，缺少一条可确认、可执行、可核验的路径。

1.3 企业真正需要的能力

传统软件擅长回答“记录了什么”和“流程走到哪里”，管理者更需要回答：**哪张订单受影响、影响来自哪里、哪些事实仍不确定、当前谁负责处理、下一步允许做什么**。把多个系统的数据集中展示，能够改善信息获取；进一步把信息连接到责任与行动，才能推动业务结果。

核心问题

企业拥有越来越多的系统、数据和 AI 工具，却缺少一个把它们组织到**同一业务对象、同一责任体系、同一证据链**中的运行环境。这正是 KTOS 要解决的问题。

1.4 制造企业的典型场景挑战

业务环节	常见现象	根本原因
订单履约	交期风险在临近发货时才暴露	订单、计划、供应、质量事实分散，缺少共同进度口径
物料供应	缺料靠人工比对表格、反复催料	需求、可用库存、占用与到货承诺没有被持续核对
技术变更	在制工单仍按旧版本生产	变更影响范围依赖经验判断，版本引用未被冻结
质量异常	不合格品处置与库存、对账脱节	收货、检验、入库、退货各环节缺少回执闭环
经营管理	会议多、汇报多、催办多	问题没有直接连接到责任人与可办理动作

02 PRODUCT OVERVIEW

产品概述

构建在企业现有系统之上的统一智能运行环境，让数据、知识、流程、人员与数字员工共同工作。

2.1 产品定义

KTOS（Enterprise Intelligence OS）是面向 AI 时代的企业智能操作系统。它位于企业现有业务系统之上，组织业务对象及其关系，明确人员与数字员工的岗位职责，管理规则、流程、工具与结果依据，为不同岗位提供统一的智能工作入口，并在受控边界内调度数字员工与人员协同完成业务。

> **原有系统负责记录和交易，KTOS 负责连接、理解、判断、协同与进化。**
>
> —— 一句话理解 KTOS

2.2 设计理念

理念一

治理先于智能

先告诉 AI 这家企业应该怎样运行，再让 AI 参与运行。目标、岗位、制度与经验被转化为对象、规则、流程与技能，成为系统的运行依据。

理念二

激活而不替代

不要求推倒重建。企业已有系统继续承担专业业务；KTOS 按领域确认承担方、数据权威与操作入口，在统一环境中组织协同。

理念三

确定性打底，模型增强

能用字段和条件表达的判断交给结构化规则；需要理解资料、解释差异的工作交给数字员工。模型只提议，正式写入经过人的确认。

理念四

结果以证据为准

“已安排入库”不等于“库存已过账”。业务进展依据真实状态和完成凭证判断，每一步都能沿证据链追溯。

2.3 KTOS 在企业技术栈中的位置

层级	主要内容	KTOS 的作用
基础模型层	大模型、多模态模型、专业模型	提供可被调用的通用与专业智能
KTOS 智能操作系统	**统一底座、EOS 业务运行底座、三大原生产品与制造业务应用**	**把模型智能组织成受企业治理约束的运行能力**
存量业务系统	ERP、MES、CRM、PLM、WMS、SRM、OA、财务、HR	保留主数据、交易与确定性业务执行
真实业务世界	客户、订单、物料、设备、供应商、员工、工厂	产生业务事件并接收执行结果

KTOS 内部的产品层级、能力归属和部署位置，以第 5 章“产品全景图”和“能力归属矩阵”为唯一口径。

2.4 KTOS 与常见系统的关系

已有能力	继续承担	KTOS 增加的能力
ERP / MES 等业务系统	交易记录、主数据与确定性流程	跨系统理解、事件响应与协同执行，正式写入回到原系统并核验回执
单点 SaaS	局部业务	统一岗位入口与跨部门闭环
数据分析与 BI	指标展示与分析视图	解释原因、判断影响，并把问题连接到责任人与可办理动作
通用大模型 / Copilot	通用知识、理解与生成	让 AI 进入企业语境、权限、流程与业务责任，产出可核验结果

为什么称为“操作系统”

模型提供智能，单个 Agent 提供任务能力；KTOS 统一管理人员与数字员工的**身份与权限、业务上下文、知识与工具、任务调度、执行边界和结果追溯**。就像计算机操作系统为应用程序管理资源、权限与进程，KTOS 为企业中的人与 AI 管理责任、依据与执行，因而承担企业智能运行环境的角色。

03 VALUE & DIFFERENTIATION

核心价值与差异化优势

KTOS 的差异不在于“多了一个 AI”，而在于让 AI 在企业的责任体系中可靠地工作。

01 治理驱动，而非工具堆叠

先定义企业如何运行，再让 AI 参与运行

经营目标对应指标与监听条件，岗位对应身份、责任与权限，制度对应规则、审批与例外，经验对应知识、流程与技能。治理不再是一段理念，而是系统每一次判断与动作的运行依据；业务结果反过来检验这些配置是否有效（见第 4 章）。

02 激活现有系统，按领域选择业务承担方

保护既有投资，同时补齐缺失能力

每个业务领域都可以选择由客户已有系统承担，或由 EOS 内置应用承担，二者可以按领域组合，并可在评估后切换。无论由谁承担，工作卡、业务主线和岗位待办都保持一致；同一项事实和正式操作始终有清楚的权威来源。

03 规则打底，模型增强

能算清的交给规则，需要理解的交给数字员工

“库存不足且到货晚于需求日期”由数量和日期直接计算；自由文本归类、资料一致性解释等交给数字员工受控判断。确定性基线先出结果，模型只能在封闭选项内给出结论并附证据。模型不可用、资料不足或输出不合格时，任务退回人工处理，业务功能不缺失，失败也不会被包装成已完成。

04 流程驱动，责任落人

模型只提议，写入过人；边界由系统强制，而不只靠提示词

流程负责组织办理步骤，数字员工必须绑定岗位，只在分配的步骤中完成资料准备与受控判断，不自行推进整条业务、不直接写入业务数据。批准、过账、对外承诺等正式动作，由有权限的人员确认后通过相应业务能力执行，并取得实际回执。

05 以证据判定完成，全链路可追溯

事项办结 ≠ 流程办结 ≠ 业务完成

订单是否进入下一节点，由对象状态、业务事件、人工确认或其他已声明证据判断，而不是看某个按钮是否被点击。数据变化、事件、规则判断、流程步骤、人工决定、数字员工任务与接口调用，由同一条追溯标识串联，形成可审计、可复盘的证据链。

06 交付即产品，持续生长

标准能力预制 + 企业初始化 + 灵活配置

主锚、批次卡、订单主线、模块设置均以声明表达，企业差异进入声明而不是散落在代码中。酷小智把企业资料转化为可运行版本；上线后的变更按参数、配置、代码三个层次选择最浅的路径。所有定义版本化、可回退，在办业务钉住其采用的版本，升级时保留企业本地差异（见第 13 章）。

3.1 与常见方案的对比

维度	传统业务系统	通用 AI 助手 / Copilot	KTOS 企业智能操作系统
核心定位	记录交易、固化流程	回答问题、生成内容	**组织责任、依据与执行的智能运行环境**
变化感知	依赖人查询与报表	依赖用户提问	**业务事件与周期检查主动发现，并路由到责任岗位**
跨系统协同	按系统边界割裂	可读取但难以办理	**围绕同一业务对象串联多系统事实与动作**
AI 的位置	无或局部附加	独立于业务责任之外	**嵌入流程步骤，绑定岗位与权限**
写入与执行	人工操作	通常无法安全写入	**建议转为明确参数，确认后通过正式动作执行并核验回执**
完成判定	单据状态	回答即结束	**以真实凭证与声明的证据条件判定**
可追溯性	系统内日志	对话记录	**一条证据链贯穿事件、判断、决定与执行**
个性化与演进	二次开发、周期长	提示词调整	**声明式配置 + 分层变更 + 版本管理**

04 GOVERNANCE

企业治理与经营目标

治理的价值最终要体现在经营目标上。KTOS 把经营目标逐级落到业务指标、主线节点、岗位责任与执行证据，并用复盘修订运行依据。

本章要点

- AI 转型首先是治理转型：先把企业应如何运行表达清楚。
- 一条完整闭环：经营目标 → 业务指标 → 业务主线 → 岗位责任 → 执行证据 → 经营复盘。
- 治理配置要能在真实业务样例中被检验，复盘结论回写到规则、流程与数字员工规程。

4.1 为什么 AI 转型首先是治理转型

如果战略停留在管理者脑中、数据分散在部门系统、流程依赖人工催办、经验依赖少数个人，AI 即使接入，也只能成为局部助手。真正释放 AI 能力，需要企业把目标、角色、业务流程、数据规则、权责边界和评价反馈组织成可运行、可追溯的结构。



图 4-1　企业治理驱动 AI 原生组织：从层级管理走向人机协同

4.2 从管理语言到产品对象

治理要素	KTOS 中的产品对象	形成的组织能力
经营目标	指标、经营信号、监听条件、场景范围	目标连接到业务变化，逐级落到行动
岗位与权责	组织、人员、岗位、数字员工身份、办理范围	人机分工与业务责任清晰
制度与规则	结构化规则、准入条件、审批阈值、例外处理	制度从文件转化为可执行约束
SOP 与流程	业务事件、主线节点、流程步骤、正式动作	工作自动衔接并能处理例外
经验与 Know-How	企业知识、案例、技能、数字员工作业规程	个人经验转化为组织可复用资产
评价与反馈	业务事实、执行回执、证据链、版本迭代	组织在受控机制中持续学习

4.3 经营目标闭环：一个完整案例

以“订单准时交付率”这一常见经营目标为例，说明目标如何经过六个环节进入每天的工作，并在复盘中修订运行依据。



图 4-2　经营目标—业务指标—业务主线—岗位责任—执行证据—经营复盘闭环

环节	在 KTOS 中如何表达	示例
① 经营目标	在酷小易中登记目标、口径与考核周期，明确目标负责人	订单准时交付率提升至年度目标值
② 业务指标	把目标分解为可从业务事实计算的先行指标，并为每个指标设定监听条件	交期前 N 天未齐套的订单数；技术准备超时订单数
③ 业务主线	指标对应到订单主线的具体节点：节点声明完成证据、时效与可能的异常	“供给与计划”节点超时或缺料，进入缺料处置流程
④ 岗位责任	节点与流程声明负责岗位；数字员工绑定岗位做准备与判断，人负责决定	计划员确认方案，采购员办理补货，数字员工整理供给与风险
⑤ 执行证据	正式动作取得业务回执，节点按证据推进，证据链记录每次判断与决定	采购承诺、到货入库过账、计划正式下达
⑥ 经营复盘	按同一口径回看指标；分析超时、改判、重复例外，修订规则、阈值、流程或员工规程	把反复人工判断的“承诺不足”分组沉淀为规则

闭环的关键

每个经营指标都能追到具体订单、具体节点和具体责任人；每次复盘的结论都落到可版本化的规则、流程或规程上，而不是停留在会议纪要中。

4.4 人机分工、规则与例外

人负责

目标设定、价值判断、复杂关系处理、例外处置、创新，以及对结果承担责任。销售对订单承诺负责，计划对安排负责，质量岗位对放行负责。

数字员工负责

信息处理、资料整理、知识检索、差异比较、持续监控与过程跟踪，在授权范围内完成准备与受控判断（体系见 7.5）。

规则可执行、可解释：能用明确字段和比较条件表达的判断形成结构化规则，字段、适用范围和结果含义清楚，用户能解释某项工作为何被归入某个分组、调整阈值会影响哪些业务。**例外有责任和出口：**资料缺失、交期变更和结果不一致时，约定交给哪个岗位、补充什么材料、允许什么处置；数据不足时保留“未判定”状态，不把缺少依据解释为业务已经通过。**检验标准：**只检查页面和字段是否存在，无法证明岗位真正具备办理权限或结果可追溯；治理配置要通过样例业务、权限反例与执行结果验证。

05 PRODUCT PORTFOLIO

产品全景与能力归属

一张全景图、一张能力归属矩阵，作为研发、销售与交付共同使用的唯一产品口径。

5.1 产品全景图



图 5-1 KTOS 产品全景图（交付平台运行在平台侧，其余各层随每家企业的运行时部署在企业侧）

5.2 产品层级与口径约定

名称	是什么	不是什么
KTOS	产品体系总称：企业智能操作系统，包括统一底座、三大原生产品、EOS 业务运行底座与制造业务应用	不是某一个单独模块

名称	是什么	不是什么
KTOS 统一底座	所有产品共用的本体、身份权限、规则、知识与技能、模型接入、工具目录和安全审计能力	不直接面向业务办理
酷小易 / 酷小智 / 酷小匠	面向经营协同、应用建设与交付、需求到制造三个方向的原生产品	不各自维护一套业务数据
EOS	部署在企业侧的业务运行底座（事件、主线、流程、数字员工、工作卡、集成、证据）与制造业务应用	不是与 KTOS 并列的另一套产品
交付平台	酷小智的平台侧部分：管理多个企业项目的调研、初始化、内容包、定制、发布与升级	不读取、不存放企业业务明细

5.3 能力归属矩阵

能力	归属	运行位置	主要使用者	交付方式
身份权限、审计、模型接入	KTOS 统一底座	企业侧	企业管理员	标准能力
业务本体、规则、知识与技能	KTOS 统一底座	企业侧	流程管理员、顾问	标准 + 配置
业务事件、主线、流程、证据链	EOS 运行机制	企业侧	全体岗位	标准 + 配置
主锚、工作卡与事项中心	EOS 运行机制	企业侧	全体岗位	标准 + 配置
数字员工执行	EOS 运行机制（档案与技能由酷小智建设）	企业侧	岗位负责人	配置
经营目标、态势、风险与决策辅助	酷小易	企业侧	管理者、业务负责人	标准 + 配置
对话即工作	酷小易（运行于 EOS 工作台）	企业侧	全体岗位	标准能力
订单、研发、计划、制造、质量、仓储、采购等应用	EOS 制造业务应用	企业侧	各业务岗位	按领域选用
调研、初始化、内容包、定制、发布升级	酷小智	平台侧 + 项目	实施顾问	平台 + 服务
使用期配置调整与本地变更	酷小智（企业侧能力）	企业侧	企业管理员	配置
需求解析、方案生成、工艺转译	酷小匠（衔接 EOS 研发）	按版本装配	销售、技术岗位	按项目配置
外部系统集成	EOS 集成执行 + 酷小智映射设计	两侧	IT 对接人	按项目交付

各项能力当前是已发布、验收中、按项目交付还是规划中，见附录 C“能力状态矩阵”。

5.4 三大原生产品

酷小易 · 企业 AI 经营执行官

连接经营目标、经营数据、风险问题与执行动作，形成“感知—判断—决策—执行—复盘—进化”的经营闭环。能力：经营态势、风险识别、决策辅助、行动组织、经营复盘。

变化：从“人找数据、会中判断、会后催办”，走向“风险主动浮现、判断有据、行动可追踪”。

酷小智 · 企业 AI 应用生长官

把产业 Know-How、管理要求与业务变化转化为业务模型、页面、规则、流程、岗位与数字员工，并负责交付、配置、定制与升级（端到端机制见第 13 章）。

变化：从“购买软件、需求等待开发”，走向“把 Know-How 持续生长为自己的应用能力”。

酷小匠 · 制造业产业智能体

把自然语言、图片、语音及参数化需求转化为可确认的产品方案，再经 EOS 研发与技术准备落为选配、BOM、工艺与生产要素。

变化：从“需求反复沟通、专家人工转译”，走向“客户需求更快连接工厂生产能力”。

三者共享同一套业务对象、岗位与证据：需求和经营变化带来新的工作，应用建设使企业具备处理能力，业务运行形成结果与反馈。企业可从最迫切的场景切入，逐步扩展。

06 ARCHITECTURE & ENGINEERING

架构与工程化

从技术分层、部署拓扑、非功能要求到容错机制，说明 KTOS 如何在企业环境中稳定、可控地运行。

6.1 技术分层架构



图 6-1　KTOS 技术分层架构

6.2 部署拓扑

KTOS 按“运行位置”分为平台侧与企业侧。二者只通过登记的契约交换元数据、配置、契约文档与证据摘要，**业务数据与凭据不离开企业边界**。每家企业拥有独立的代码仓、独立的数据库与独立的运行时，不与其他企业共享业务库。

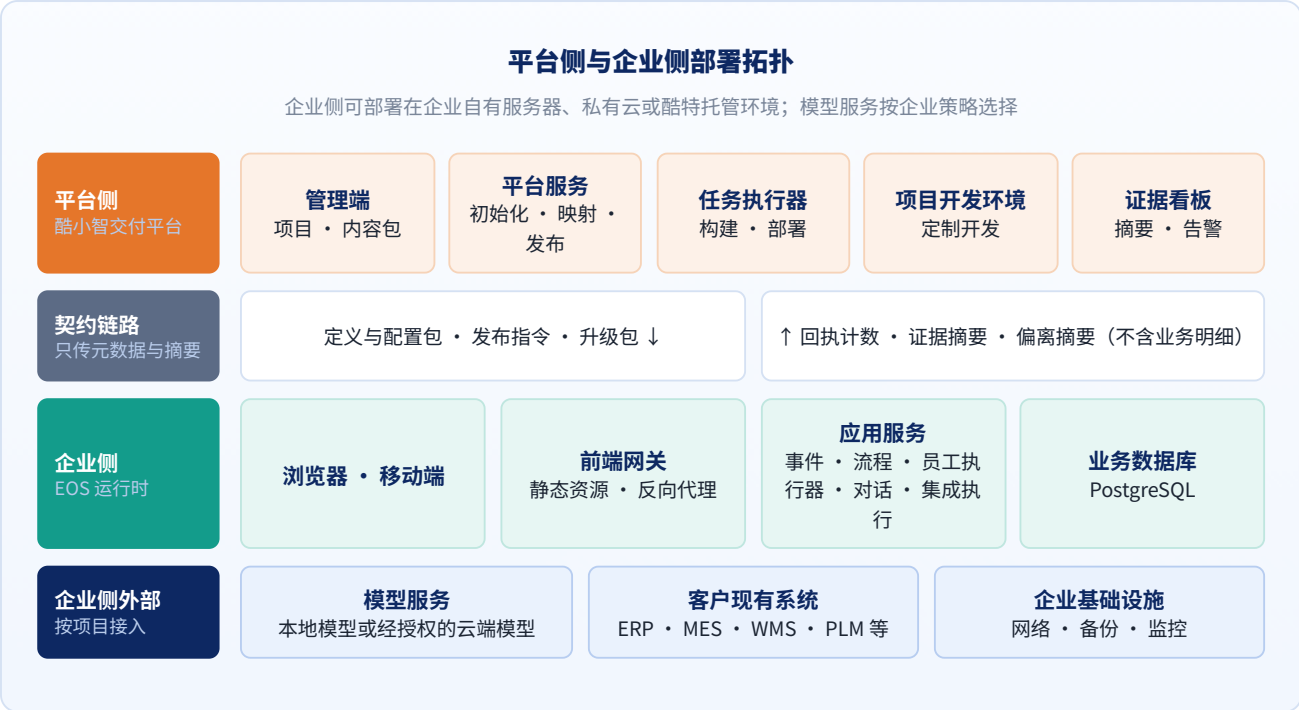


图 6-2　平台侧与企业侧部署拓扑

企业本地部署

运行时部署在企业服务器或私有云，业务数据与凭据留在企业内部；平台通过受控链路完成升级与运维协同。

托管部署

运行时部署在酷特交付环境，按项目独立隔离，适合希望快速启动、减少运维投入的企业。

混合部署

运行时在本地，模型服务按策略选择本地或经授权的云端模型，可发送给模型的事实范围单独确认。

6.3 关键非功能要求

非功能指标与企业规模、业务量和基础设施直接相关。KTOS 提供相应的产品机制，具体目标值在项目方案中确认，并纳入验收。

要求	产品机制	项目中需确认的指标
可用性	容器化交付；数据库、应用就绪与基础数据三项检查全部通过才对外服务；健康检查与运行状态可见	服务时段、可用性目标、计划停机窗口、是否需要主备
性能与容量	周期扫描水位线与去重；批次办理逐行处理；事件、事项与证据可分页查询	用户并发、日订单与事件量、扫描周期、关键页面响应时间
数据可靠	数据库结构经版本化迁移管理，只增不删；业务写入幂等；结果未知时冻结对账	数据保留周期、归档策略
备份与恢复	提供备份恢复说明；凭据密钥与数据库一同纳入备份；重新部署须具备可验证备份与恢复计划	备份频率、恢复点目标（RPO）、恢复时间目标（RTO）、演练周期
监控与告警	证据摘要与运行告警回传平台侧；数字员工任务、接口调用与异常均有记录	告警对象、通知渠道、响应时限
多企业隔离	每家企业独立代码仓、独立数据库、独立运行时；平台侧不读业务明细	部署形态与网络隔离方式
升级与回滚	定义与配置采用不可变版本和追加式回滚；在办业务钉住原版本；升级保留企业本地差异	升级窗口、回归验证范围

6.4 系统容错机制

故障情形	系统行为
模型服务不可用或超时	准备任务说明未准备原因，判断任务转人工；确定性规则与流程照常运行，业务功能不缺失
模型输出不合格	结构、结论选项与证据检查不通过时拒收，转人工并保留原任务
外部系统超时	标记为“结果未知”而不是“失败”，先查询已有回执再决定是否重发，不自动重放
重复请求	稳定操作标识去重，同一业务动作不会执行两次
对象被他人修改	版本冲突时重新读取并核对业务意图，不覆盖他人的新结果
批次部分失败	逐行反馈成功与失败，重试只处理未完成的行
服务重启	运行中的流程、等待时钟与已选事件按原记录恢复，只核对、不重算

安全责任在产品、企业与模型服务方之间的划分见 12.6。

07 CORE MECHANISMS

核心运行机制

本体统一语义，事件捕捉变化，主线判断进展，主锚定义工作，流程组织办理，数字员工承担准备与判断，正式动作留下回执，证据链串起一切。



图 7-1　核心运行环：同一追溯标识贯穿每一步

7.1 业务本体：建立共同语义

业务本体把企业中的对象、属性、关系、状态、规则和动作组织成一致的模型。订单是客户需求与交付承诺的载体，订单行关联产品及数量，产品关联 BOM 与工艺版本，物料需求关联库存和供应，工单关联计划、报工及质量结果。外部系统的表和字段通过映射接入本体，而不是反过来让业务迁就数据库结构。

信息性质	示例	处理原则
业务事实	当前库存、已确认报工、实际发货	来自权威来源的可信同步或回执，展示值与 AI 解释不能覆盖
计划与承诺	预计到货、候选排程、交期承诺	有来源、有效时间和确认条件，旧计划不能覆盖新事实
建议	AI 提出的替代方案、影响说明	保持建议性质，经确认转为正式动作后才产生业务效果

7.2 主线、主锚、流程与工作卡：四者关系

这四个概念分属不同层次，容易混淆。KTOS 统一按“**定义层**”与“**运行层**”区分：定义层回答“企业规定了什么”，运行层回答“此刻发生了什么”。



图 7-2　业务对象、主锚、主线、流程与工作卡的层级关系

概念	层次	定义	与其他概念的关系
业务主线	定义	订单等主对象要经过的节点，每个节点声明负责岗位、完成证据、时效、可能的异常及挂接的流程	引用主锚与流程；节点变化时派生节点待办卡
主锚	定义	一类业务对象在工作台上的完整工作契约：数据来源、事实口径、可执行动作、负责岗位、可发起流程	绑定业务对象；被主线引用；呈现为工作卡
流程	定义 / 运行	围绕局部目标组织人员、数字员工与系统动作的办理步骤；定义有版本，运行时为流程实例	由工作卡上“发起 · 流程名”启动；完成后回写证据
工作卡	运行	主锚在工作台上的呈现，分为对象卡、批次卡和由主线派生的节点待办卡	卡上的每一件待处理工作是一个事项

三种“完成”需要分清

事项办结表示当前工作已处理；流程办结表示对应办理过程结束；业务完成还需满足主线节点声明的证据条件。例如“已经安排入库”不等于“库存已实际过账”，工作卡同时展示办理进展与仍在等待的业务凭证。

7.3 事件驱动：从变化进入处理

业务事件记录发生了什么变化、关联哪个对象、变化时间和必要事实。工作周期定期检查临近交期、缺料或超时等条件，对象变化也会产生事件。事件进入处理前先核对是否已有在办工作，避免同一问题被重复发起。



图 7-3　事件处理中的规则、人工与 AI 路径

人可以针对本次事件选择办理方式，也可以在复核后起草适用于后续同类事件的规则。事件登记、候选建议、人工选择与正式发起是不同阶段，运行记录分别说明各自结果。

7.4 正式动作、回执与证据链

批准订单、下达计划、确认报工、库存过账等正式动作，执行前检查身份、权限、对象版本、数量与状态；每个动作在动作目录中声明风险等级、审批要求与回执。外部系统返回“已受理”只代表请求进入处理，仍需核对业务单号、终态或实际流水。数据变化、业务事件、规则判断、流程步骤、人工操作、数字员工任务与接口调用携带同一条追溯标识，汇入统一证据视图：采用了哪一版定义、使用了哪些事实、谁作出决定、产生了什么结果，均可追溯。

7.5 数字员工体系

数字员工是绑定岗位、按作业规程完成工作的产品角色。企业建设数字员工，与建设一支岗位团队类似：先定岗位与边界，再配技能，经审核后上岗，上岗后持续评价。

岗位模型

类别	承担的工作	示例
业务数字员工	在业务流程中做资料准备与受控判断，服务于具体业务岗位	计划助理整理缺料供给；质量助理比对检验资料
系统集成数字员工	处理与外部系统之间的数据同步、映射核对与回执跟踪	核对 ERP 回执、标记结果未知的事务
AI 编程数字员工	在使用期起草配置变更与定制代码，由人审核后进入发布	根据变更需求生成本地配置增量

员工档案与任务边界

身份与使命

员工名称、绑定岗位、服务的业务范围与目标；每个员工都有对其结果负责的人类岗位。

技能与作业规程

规程分三段：取数（引用登记的只读查询，派活时冻结）、核对（声明式条件，能判的直接出结论）、技能（剩余推理交给模型）。规程不含分支、等待、人工步骤和写操作。

工具与边界

只读工具白名单、事实读取范围、可交回的结论选项；风险分低、中、高三级，结果门分为无、审计、人工确认三种。

自主等级：员工设 L0 至 L3 四级自主等级。较低等级的结果须经人工确认后采纳；较高等级只能在声明的自动围栏内自动采纳并留审计，系统拒绝“高等级却要求人工确认”这类自相矛盾的配置。业务放行不能仅依赖未经复核的模型原始输出。

上岗与版本

1 **草稿** 编辑档案与技能 › 2 **待审核** 提交发布门 › 3 **已批准** 审核人确认 › 4 **已发布** 上一版自动替代 › 5 **停用** 可随时下岗

发布门逐项审核：身份与使命、技能与阶段、工具与能力目录、边界与结果门、自主等级与自动围栏，以及**基于真实冻结事实的回放**，没有回放样本不能发布。管理员工与审核员工是两种不同权限。员工可绑定自己的模型，技能随员工版本一起发布。

运行评价

评价维度	观察指标	用途
完成质量	准备完成率、证据完整率、输出合格率	判断规程与取数是否充分
判断质量	人工采纳率、改判率、转人工率	决定是否调整自主等级或技能
时效	任务处理时长、超时次数	评估对流程周期的贡献
业务影响	所在流程的周期、返工与例外变化	与经营指标复盘对齐（4.3）

人机协同组织机制

每个岗位由“人 + 数字员工”共同组成：岗位负责人对员工结果承担业务责任，并参与员工规程的审核；员工的改判、转人工与例外样本定期复盘，可规则化的沉淀为规则，仍需语境理解的进入规程与知识；员工版本升级同样经过发布门。

08 WORKBENCH

智能工作台

工作台把当前需要关注的工作卡、相关材料与允许的动作放在一起，支持从发现问题直接进入处理。

8.1 围绕岗位组织事实与入口

工作台首先回答“当前登录人有哪些工作”。事项来自业务对象、流程步骤、异常和周期检查，按岗位责任和权限展示。用户可以查看处理状态、关注时限和关联单据，再进入具体办理。管理员看到的管理视图，不自动赋予其业务审批资格。

工作卡

呈现问题的核心事实，如订单交期、缺料数量、供给承诺与当前节点；展开后查看相关材料、流程记录与执行结果。

动作含义清晰

批准、调整、登记直接进入正式业务动作；“发起 · 流程名”进入多人多步协同；认领与转交处理的是工作责任。

状态与应用一致

工作台与业务应用共享状态。事项关闭后真实执行结果仍可追溯；未达完成条件时持续显示等待原因与下一责任环节。

8.2 批次办理：同类工作集中处理

同一岗位可能同时面对多张缺料订单、多条超时任务或多批待检物料。批次卡按规则组织这些记录，展示每组的判据与数量。例如按是否已有采购承诺、预计到货与需求日期的关系分组，再分别进入跟进、协调或人工判断；对“待定组”，可由数字员工先给出建议结论，再由人确认。分组是对事实的整理，不等于模型已经完成决策。

批量发起流程或执行动作时，每一行仍对应明确的业务对象与办理结果。部分成功、部分失败分别反馈，重试不会重复执行已完成的记录；数量守恒、对象版本与权限检查不会因批次处理而省略。

8.3 对话即工作

对话不是孤立的聊天页面，而是当前岗位、对象、单据与流程的上下文入口。用户在订单、事项或流程旁发起对话，可以要求解释缺口、比较材料或整理变更影响；助手读取授权上下文，回答中关联事实、资料及适用时间。对话中的推测和草稿保留建议性质。



图 8-1　从对话建议到正式操作

对话回答“建议调拨”，与仓储已经执行调拨之间，保留明确的操作与核验过程。补充资料、人工决定、流程步骤和接口执行结果围绕同一业务上下文串联，后续办理人能理解已做过什么、哪些事实发生了变化、本次决定依据什么。



图 8-2　一个订单异常从感知、判断、人工确认到受控执行与经验回流的完整闭环

09 MANUFACTURING APPLICATIONS

制造业务应用

EOS 提供覆盖订单到交付的制造业务应用，每个领域都可由内置应用承担，也可由客户现有系统承担。模块之间的贯通见 10.1。

OMS **订单** 评审、变更、交付与售后	**RDC** **研发** 选配、BOM、工艺、技术文件	**APS** **计划排程** 物料计划、工序安排、试排	**MES** **制造执行** 工单、开工、报工、完工	**QMS** **质量** 来料、过程、成品检验与处置
WMS **仓储** 入出库、库位、批次、盘点	**SRM** **采购** 需求、寻源、合同、收货、对账	**EAM** **设备** 档案、维护计划、点检、维修	**FIN** **财务协同** 往来、结算与经营口径衔接	**MDM** **主数据** 物料、往来单位、组织与编码

9.1 订单与研发：连接需求与技术依据

订单管理关注客户、订单行、产品、数量、交期与办理状态，把评审、变更、交付与售后连接到业务主线；订单进度由主线声明和真实证据计算。订单变化保留前后差异与影响范围，已有实际执行的部分保留来源与处置依据。**研发**覆盖工序与工艺路线、产品选配、BOM、技术文件及工时规则；订单技术准备在执行前形成快照或冻结引用，工单与计划可追溯当时采用的版本，在制工单不会因档案变化而悄然切换。

9.2 计划与 APS：连接需求、资源与执行

计划区分物料层面的生产计划、工序在时间与资源上的安排，以及落实到批次和人员的执行任务。APS 依据需求日期、工艺路线、可用资源、工作日历与物料供给等约束计算候选方案，以排程版本保留结果，由计划人员确认后发布。插单或交期调整可先试排比较；正式执行中的变化保留与原排程的差异，不直接覆盖历史方案。基础数据清楚的企业可逐步扩大自动排程范围。

9.3 制造执行与质量管理：共用生产事实

制造执行围绕工单、工序任务、生产资源、开工、报工与完工组织现场工作，计划数量、确认产出、合格数量与未完成量分开记录。**质量管理**连接检验对象、标准、记录、结论与处置；来料、过程与最终检验对应不同业务阶段，不合格品经正式处置并可追溯批次。质量放行对应具体对象及有效结果，处理一张异常事项不能代替实物的质量放行。

9.4 仓储：维护实际库存与流转依据

业务状态	应核对的结果
待收货 / 待入库	来源单据与待处理数量已明确
检验合格	对应批次具有有效放行结果

业务状态	应核对的结果
实际入库	库存过账与正向流水已经形成
实际出库	来源分配、库存扣减与反向流水一致
撤销或冲销	引用原记录并保留恢复或差异依据

在库、可用、预留、在途与冻结数量含义不同，口径明确后缺料判断与发料动作才能引用一致的数量依据。仓储还覆盖移库、调拨、盘点与差异处理。

9.5 采购：连接需求、供应与协同结果

采购覆盖采购需求、询比价、招标、采购合同、采购订单、收货退货、业务对账与采购发票八个环节，单据保留来源与明细关系。收货确认供应交接，质量检验形成合格与处置结果，仓储执行实际入出库；对账根据真实收货、退货与已处理数量形成明细，防止同一来源重复核销。

9.6 设备、财务协同与数据基础

设备管理连接设备档案、维护计划、点检与维修，到期或异常形成待处理工作。**财务协同**把订单、采购、库存与生产中的业务依据连接到可核对的经营信息，并明确往来、结算、成本、资金等范围由谁承担。**主数据与资源模型**建立客户、供应商、物料、单位、分类与编码的共同标识，以及工厂、车间、产线、工作中心、仓库与库位的业务结构。

各业务应用的当前状态见附录 C；完整会计核算、税务等专业财务要求需单独确认适用功能。

10 USE CASES

典型应用场景

先用一张订单的全生命周期，展示业务流、数据流、责任流与证据流如何贯通各个模块；再看缺料、变更、质量异常等典型局部场景。

10.1 一张订单的全生命周期：四流贯通

示例订单需交付 10 件产品，关联已确认的产品配置、BOM 与两道顺序工序。下图按主线节点展开四条流：**业务流**（做了什么）、**数据流**（哪些对象在模块间传递）、**责任流**（谁负责，数字员工做什么）、**证据流**（凭什么进入下一节点），最后一行是各节点的异常出口。

	受理评审 OMS	技术准备 RDC	供给与计划 APS · SRM	生产执行 MES	质量放行 QMS	入库发货 WMS · OMS	交付反馈 OMS · FIN
业务流	接收订单，核对客户、产品、数量、交期	确认选配、BOM、工艺并冻结	核对库存与承诺，试排并下达计划	开工、两道工序报工	成品检验，形成结论	合格品入库，分配并发货	签收、对账与售后
数据流	订单、订单行 → 主线	技术快照 → 计划与工单	需求、可用量、承诺 → 计划版本 → 工单	工单、任务 → 报工、产出数量	检验批 → 合格 / 不合格数量	入库单、库存流水 → 出库凭证	累计发货 → 对账明细
责任流	销售确认承诺；员工整理客户附件差异	技术岗位复核；员工起草差异说明	计划员确认方案；员工汇总供给风险	班组长与操作员	质检员放行；员工比对检验资料	仓管员执行	销售、财务
证据流	评审确认记录	技术版本冻结	计划正式下达，供给满足	确认报工及合格产出	有效检验结论	入库过账、出库凭证	签收与对账结果
异常出口	资料缺失 → 补资料	技术变更 → 变更流程	缺料 → 缺料处置	停线、返工	不合格 → 处置流程	库存不足 → 调拨	交期变更 → 协调流程

图 10-1　订单全生命周期中的业务流、数据流、责任流与证据流（节点按企业配置）

模块之间的约束

计划只能引用已冻结的技术版本；工单开工要满足物料与前序条件；入库数量受有效合格产出约束；发货受实际库存与订单行分配约束；对账以实际收发数量为准。每一处数量都来自上一环节的真实凭证，而不是人工转录。

与经营结果的连接

各节点的停留时长和异常次数，汇总为准交率、齐套率、技术准备周期、一次合格率等经营指标（见 4.3）。若未道合格只有 9 件，系统保留 1 件余量和下一步处理，而不会按 10 件入库或发货。

10.2 临近交期的缺料处置

2400
需求数量（件）

1600
当前可用供给（件）

800
缺口（件）

500 + 300
补货 + 调拨方案（件）

- **发现并冻结依据：**系统在约定周期或相关事实变化后核对需求、可用库存、占用与到货时间，记录本次检查依据，关联受影响订单与责任岗位。

- **规则分组与方案准备：**已有承诺且能覆盖需求日期的进入跟进组；承诺不足、日期冲突或信息不明的进入协调组。数字员工整理供给来源、时效与风险，负责人比较补货、调拨、替代或计划调整。
- **确认后进入专业执行：**补货与调拨分别进入采购与仓储的正式办理；可用供给何时形成，取决于真实承诺、到货与库存结果，而非方案中写了多少。
- **复核后关闭：**供给变化后重新计算缺口，条件满足时按规则关闭并保留处置记录；仍有风险时进入交期变更或升级流程。

10.3 技术与交期变更的影响协调

客户调整产品配置或交付日期时，原订单、技术版本、计划和执行事实仍然有效存在。系统关联当前主线节点、在制任务、采购承诺与库存，使各岗位看到同一份影响上下文。数量差异、日期先后、对象版本和已执行状态由规则核对；替代方案是否可接受，由数字员工起草说明、业务人员确认。尚未执行的计划按规则修订，已领料、生产或发货的部分采用相应调整、冲销或后续处置；对外交期承诺由有权岗位确认。

10.4 来料质量异常的跨业务协同

事实	示例数量	所需业务依据
收货	100 件	真实收货来源及交接记录
合格入库	80 件	检验放行、入库过账与库存流水
不合格退回	20 件	质量处置、退货来源与实际交接
对应对账	80 件	按收货减实际质量退货核对来源

不合格的 20 件若尚未入库，实际退回只记录交接，不再扣减账面库存；若已入库，则需引用实际批次、完成仓储出库后确认。某一步审核通过只证明该步决定成立，最终对账仍需核对有效数量与来源，防止重复扣减或重复核销。

10.5 经营洞察、需求直达制造与部门场景

经营洞察与决策执行：酷小易连接订单、生产、库存、质量、交付与财务等事实，主动组织经营事实、异常原因、影响范围和可选方案，并把确认后的决策转化为工作台上的责任人、事项与处理跟踪。**客户需求直达制造：**酷小匠理解自然语言、图片、语音及参数化需求，形成可确认的产品方案，再经 EOS 研发与技术准备进入计划与执行。

业务领域	典型问题	KTOS 可形成的能力
销售与客户	客户理解依赖个人、跟进难沉淀	客户洞察、方案建议、风险提醒、过程复盘
服务与质量	问题重复发生、客户声音难进入改进	问题识别、知识推荐、工单协同、缺陷归因
采购与供应链	供应风险分散、协调成本高	交付风险预警、备选方案与协同处置
项目与运营	进度靠人工追踪、复盘难复用	任务拆解、风险监控、行动跟踪与知识沉淀
人力与组织	岗位经验分散、新人成长慢	岗位知识、学习辅助与人机协同岗位设计

11 INTEGRATION

集成与开放

企业可以使用 EOS 内置应用，也可以保留已有专业系统，通过明确的数据与动作边界形成协同。

11.1 按业务领域确定承担方



图 11-1　EOS 内置应用与客户现有系统的业务承担方式

实施时先按领域确认业务由谁承担。例如订单继续在 ERP 维护，生产由已有 MES 执行，仓储由客户 WMS 管理，EOS 负责关联业务事实与跨部门工作；也可选用 EOS 内置的订单或制造应用。模块是否启用与模块由谁承担是两个不同问题；切换承担方前，检查历史数据、在办工作、映射与动作路径。

11.2 接入方式

接口与消息

API 调用、消息队列、状态通知，适合需要双向写入与实时回执的领域。

数据库与文件

只读数据库、文件与文档交换，适合查询事实与批量导入；只读连接不会自然产生批准、过账等正式操作。

页面嵌入与统一身份

嵌入既有系统页面，结合统一身份实现单一入口；也可按项目编写适配代码。

11.3 映射对象、标识与状态

外部订单号与本地对象身份、物料编码与单位、工厂组织与数据范围，需要明确映射。状态转换结合业务含义：已提交、已审批、已过账和已关闭可能是不同阶段。同步频率、来源时间、失败记录及补偿方式共同决定展示事实是否可靠。每个字段都有清楚的权威来源，本地展示值及 AI 解释不能覆盖原系统事实。

11.4 可靠写入：确认、回执与幂等

- **业务写入使用正式能力：**通过相应系统的正式能力办理，保留请求对象、参数、执行身份与操作标识。
- **受理不等于完成：**外部系统返回“已受理”只表示请求进入处理，没有最终凭证时，工作保持“处理中”或“待核验”。

- **重试先查后发：**超时可能发生在外部操作完成之后，系统先查询已有回执再决定是否重发，重复请求以稳定标识去重。
- **版本冲突重新核对：**对象版本变化时，重新读取并核对业务意图，而不是覆盖他人的新结果。

11.5 分层验收



存在一条映射声明，只说明已经定义接法；需要同步运行、业务调用与回执核验后，才能确认该领域已经接通。

11.6 集成分工

事项	酷特交付团队	企业 IT	外部系统厂商
接口与账号	提出所需对象、字段与动作清单	开通网络、账号与最小权限	提供接口文档与测试环境
映射与适配	编写映射声明与适配代码	确认编码、组织与数据范围	说明状态含义与限制
写入与回执	实现确认、去重与回执核验	确认哪些动作允许系统写入	保证正式能力返回可查凭证
分层验收	出具 L1–L4 验收记录	按领域签字确认接通	配合处理接口缺陷

具体分工以项目合同与实施方案为准；外部系统的升级与变更需提前通知，以便同步调整映射。

12 SECURITY & TRUST

安全与可信治理

可信运行需要回答三个问题：谁可以读取什么，依据什么作出决定，实际执行了什么。

12.1 企业级可信 AI 框架

治理域	关键机制	用户价值
身份与权限	统一身份、岗位与安全角色、数据范围、字段访问、办理资格	不同角色获得恰当能力
数据与知识	数据边界、脱敏、来源与版本、权威来源管理	企业信息安全可用
数字员工与工具	岗位绑定、只读工具、工具白名单、自主等级、发布门与回放	智能执行不越权
流程与责任	流程步骤责任、异常升级、高影响操作确认与审批	业务责任不失控
审计与运营	全链路证据、运行监控、版本发布与回滚、结果评价	结论可解释、动作可追溯

12.2 人员、数字员工与服务身份分别授权

人员按账号、组织、岗位和安全权限访问业务；数字员工按流程步骤声明的事实范围与工具边界工作，调用平台接口时使用绑定任务与权限快照的短期凭据，只放行低、中风险操作；后台服务按人批准的、有期限和预算的委托执行，只能读取或提出建议，提议仍需真人确认。能看见一个菜单、具有对象读取权限、能够批准一项业务，是三种不同资格，在实际办理时分别检查。

12.3 高影响操作与人机边界

交期承诺、关键数量调整、审批、库存过账及其他重要写入，执行前需满足业务准入与确认要求。对话提出的方案先转换为明确参数，审批结论绑定具体对象和版本。

人机边界

KTOS 构建的不是无人企业，而是高智能企业。读取、整理、识别、比较、生成草稿可以由数字员工完成；涉及**价值判断、重大资源配置、合同、付款、敏感人事、对外承诺及不可逆操作**时，由具备责任的人员确认。

12.4 模型输入与输出受约束

模型只使用经过授权与筛选的上下文，敏感字段、凭据与不必要信息按策略控制；输出经过结构、结论选项与证据要求检查。模型结果被采用时，保留采用方式及决定依据。企业可为不同数字员工配置不同模型，并单独确认允许发送给模型的事实与资料范围。

12.5 数据边界与平台安全基础

平台侧与企业侧之间只传输元数据、配置、契约文档与证据摘要；业务明细与凭据保留在企业边界之内，跨边界回执只带计数，带有数据行、样例或单号的回执会被契约校验拒收。

访问控制

默认所有业务接口需有效身份访问；口令以加盐哈希存储，首次登录强制修改初始口令；预留与企业统一认证（SSO）对接的扩展方式。

凭据保护

模型密钥、外部系统连接口令等敏感凭据加密存储、不回显，密钥文件与数据库一同纳入备份策略。

审计留痕

登录、权限变更、业务操作、数字员工任务与接口调用全部进入审计记录，并与证据链关联。

版本与回滚

定义与配置采用不可变版本和追加式回滚；在办业务钉住采用的版本，恢复时只核对、不重算。

12.6 安全责任边界

责任方	主要责任
酷特（产品与交付）	产品内的身份、权限、数字员工边界、写操作确认、凭据加密、审计与证据机制；交付平台不读取业务明细；安全缺陷修复与版本升级
企业（客户）	账号与岗位授权的日常管理；运行环境的网络、主机、备份与监控（本地部署时）；确认允许发送给模型的数据范围；高影响操作的人员确认
模型服务方	模型服务自身的可用性与数据处理承诺；云端模型的数据使用条款由企业审阅确认
托管环境（托管部署时）	由酷特按合同承担运行环境的隔离、备份与基础监控

具体责任划分以合同和项目安全方案为准，项目验收按实际环境确认。

13 ONBOARDING & EVOLUTION

企业初始化与持续进化

把交付本身做成产品：酷小智以“标准能力预制 + 企业初始化 + 灵活配置”，把企业需求变成可验收、可升级的应用。

13.1 从企业需求到可验收应用：端到端机制



图 13-1　酷小智端到端交付机制

阶段	做什么	产出	关口
1 需求采集	三路输入：企业描述；企业资料（文件、图片、Excel，表头可映射到导入字段）；系统接入登记（凭据加密、不回显）。另含企业档案基本信息	材料库与证据	材料可追溯到来源
2 业务建模	模型只在封闭的能力目录中匹配，提出条目答案、流程选型与调整、缺口清单；模型未覆盖的由内置基线补齐；冲突与证据交顾问和客户逐条确认	确认后的初始化条目、缺口清单	完备性门：必需条目全部人工确认
3 生成	写进项目：生成声明清单、客户层内容包与配置数据集（定义与数据分开）；缺口转为定制单交开发，附“原来 → 改后 → 影响”变更说明书	项目仓中的定义、数据与定制提交	声明只增改、不删除
4 测试	装包门与契约校验；试点订单走通主线；权限反例；数字员工以真实冻结事实回放	测试记录	各道门全部通过
5 发布	按固定版本部署；一次性初始化任务按“平台基线 → 客户层 → 工厂段 → 定义 → 数据”顺序装载，然后启动应用	运行中的企业版本	就绪检查通过
6 验收	分别记录“写进项目完成”“装载成功”“真实业务就绪”三项回执，再做业务验收	部署回执与验收记录	客户签认
7 升级	使用期按参数、配置、代码分层变更；升级时用偏离摘要保留企业本地差异	新版本与变更记录	回归验证通过

基线始终成立

行业基线随产品提供，空库首次启动即装入；企业提供多少资料就升级多少，不必等待一次性全面梳理。能够在编辑器中保存配置，不等于配置已装入或业务数据已写入，“装进去”与“跑得起来”分别验证。

13.2 变更分层：选择最浅的一层

变更层次	典型内容	处理方式
参数层	阈值、显示参数、时限	企业管理员按权限直接调整，即时生效并留痕

变更层次	典型内容	处理方式
配置层	岗位、流程、表单、工作卡、对象声明	检查依赖与权限，形成本地版本，可回退
数据维护	档案、名册、初始事实	由相应业务能力办理
代码层	超出现有表达能力的需求	转为定制单交由平台开发，附变更说明书供业务审核

数据结构变更只增不删：改名与改类型通过“新字段 + 清洗 + 校验 + 旧字段停用”完成，回滚只需回退代码。给审核人看的是业务影响，而不是代码差异。

13.3 定义版本与运行实例分别管理

在办流程保留其采用的定义与输入依据，新模板不会静默改写历史运行。升级时检查对象、流程、工作卡、规则与运行依赖是否一致，并保留企业本地差异；出现冲突时，明确待处理内容和责任。发布目录中存在某项能力，不等于项目已安装、生效或完成验收。

13.4 用运行反馈完善规则与技能

企业分析人工改判、重复补充资料与经常出现的例外，判断哪些问题已具备明确规则。可结构化的经验进入规则或流程修订，仍需语境理解的内容进入数字员工规程与知识；规则候选经业务审核与验证后再启用。规则处理占比上升时，同时观察改判率、错误放行、人工返工与结果质量。

14 IMPLEMENTATION

实施方法与能力转移

从一个高价值场景切入，每个阶段有明确的交付物、角色与验收标准，并在交付过程中把运营能力逐步转移给企业。

14.1 适合 KTOS 的企业与起点

企业已具备一定的数字化基础，业务链较长、跨部门协同较多，拥有大量行业 Know-How，并希望 AI 真正进入经营与业务执行时，KTOS 能更快形成价值；离散制造、定制与柔性制造企业尤为适合。若基础数据严重缺失、责任体系尚未成形，应先围绕具体场景完成必要的治理与数据梳理。适合先行的场景具有清楚的业务对象、稳定的责任岗位、可取得的输入和可核验的结果，例如订单评审、临期缺料、技术复核或质量异常协同。

14.2 阶段、交付物与验收标准

阶段	关键工作	交付物	验收标准与签认
1 诊断与选场景	识别经营目标、管理痛点、系统基础，选定可验证的业务闭环	场景范围书、价值基线表（15.2）	基线口径与数据来源经业务负责人签认
2 治理建模	梳理对象、岗位、主线、流程、规则、数字员工与指标闭环	业务蓝图、岗位与责任清单、承担方清单	关键用户评审通过
3 连接与初始化	连接存量系统，完成企业初始化与必要定制	可运行版本、接口清单与 L1–L3 检查记录、变更说明书	装载与就绪回执齐全
4 验证与上线	试点订单走通，验证权限反例、数量回执与异常恢复	业务验收记录（L4）、上线方案	验收清单逐项通过，客户签认上线
5 运营与扩展	按同口径复盘指标，沉淀规则与技能，复制到更多业务链	价值复盘报告、扩展计划	复盘结论经管理层确认

14.3 角色分工

角色	所属	职责
项目经理	双方	计划、范围、风险与阶段验收组织
实施顾问	酷特	调研、治理建模、初始化与配置、培训
交付工程师	酷特	集成、定制开发、部署与升级
业务负责人	客户	确认目标与指标口径、主线与责任、验收签认
关键用户	客户	提供资料与样例、参与评审和验收、带教岗位用户
企业管理员	客户	账号与岗位授权、参数与配置层变更、日常运行
流程与员工管理员	客户	维护流程、规则与数字员工规程，审核员工发布

角色	所属	职责
IT 对接人	客户	系统接入、网络与基础设施、备份与监控

14.4 能力转移与陪跑模式

交付主导

酷特承担建模、配置与上线，客户关键用户全程参与；适合首个场景。

联合共建

客户管理员在酷特指导下完成配置层变更与员工维护；适合扩展到第二、第三个场景。

自主运营 + 陪跑

客户自主完成参数与配置变更，酷特按约定周期陪跑复盘，代码层需求经定制单承接。

能力级别	面向角色	掌握内容	转移方式
使用	岗位用户	工作台办理、批次处理、对话即工作	岗位培训、关键用户带教
配置	企业管理员	参数与配置层变更、账号与岗位授权	实操培训、联合共建
治理	流程与员工管理员	规则维护、员工规程审核、复盘与修订	复盘工作坊、陪跑
扩展	业务负责人	选场景、定基线、组织下一轮扩展	价值复盘、扩展规划

交付周期取决于资料质量、标准能力匹配度和现场条件；陪跑周期与服务内容按合同约定。

15 CUSTOMER VALUE

客户价值与收益测算

从单点效率提升走向组织智能升级；价值用可核验的基线与测算模型表达，可直接用于项目诊断、方案报价与验收。

15.1 五个层次的企业价值

从效率到智能
不仅做得更快，更能回答为什么发生、如何判断、谁来执行

从经验到能力
个人经验沉淀为规则、流程、技能与数字员工

从数据到认知
分散记录转化为对客户、订单与经营状态的持续认知

从控制到协同
风险主动浮现，任务自动衔接，异常及时升级

从静态到生长
判断、动作与结果持续回流，组织在运行中进化

15.2 价值基线与测算模型

测算按“基线 → 改善 → 收益”三步：先用实施前的真实数据建立基线，再按试点实测或可推算的改善幅度计算年化收益。

价值项	基线取数	年化收益测算公式
效率	相关岗位人数、每人每周用于查数、整理、催办的时长、人工成本	人数 × 每周节省小时 × 年工作周数 × 小时人工成本
库存	平均库存金额、资金成本率、呆滞金额	库存降低额 × 资金成本率 + 呆滞减少额
履约	准交率、加急运费、违约扣款、因延误流失订单的毛利	（加急费 + 违约扣款）× 降低比例 + 保留订单毛利
质量	返工、报废、客诉处理损失	质量损失 × 降低比例
经营利润	上述各项对应的利润表科目	各项收益汇总后，按科目核对对毛利与费用的影响

测算示例（数据均为假设）

价值项	假设基线	假设改善	年化收益
效率	计划、采购、质量岗位共 20 人，人工成本 120 元 / 小时	每人每周节省 4 小时，按 48 周	约 46 万元
库存	平均库存 8000 万元，资金成本率 6%	库存降低 5%；呆滞减少 30 万元	约 54 万元
履约	加急运费与违约扣款每年 200 万元	降低 25%	约 50 万元
质量	返工与报废损失每年 300 万元	降低 10%	约 30 万元
合计			**约 180 万元 / 年**

15.3 投入产出与收益分级

年化净收益 = Σ（各项年化收益 × 可靠度系数）− 年化运营投入
投资回报率 ROI = 年化净收益 ÷ 一次性投入
投资回收期 = 一次性投入 ÷ 年化净收益
一次性投入：软件、实施、接口与定制；年化运营投入：模型服务、运维、陪跑与组织参与

收益分级	判定条件	可靠度系数
已验证收益	试点期按同口径实测得到	1.0
可推算收益	由已验证收益按业务量合理外推	0.5
潜在机会	尚无实测依据	0（单列说明，不计入）

比较时保持同口径：记录基线周期、业务量、产品组合、资源和数据质量，试点后用相同定义统计，并说明订单负荷、人员与范围是否变化；业务改善可能同时受管理调整与流程梳理影响，评价时保留这些条件。不用生成文本数量或模型调用量代替经营结果。

价值判断

不先承诺通用的提升百分比，而是先确定场景与基线，再用可核验的真实结果完成验收。

16 PRACTICE & VISION

源于实践，走向产业

以真实制造、真实订单和真实治理过程验证方法，再将能力沉淀为可复制的产品。

16.1 从大规模个性化定制中生长

酷特智能长期深耕大规模个性化定制与柔性制造。客户需求高度个性化，而工厂生产要求高度标准化，这种矛盾推动酷特持续建设数据、流程、组织与系统能力，并在真实业务中验证企业治理与产业智能方法。真实工厂为技术提供复杂场景，技术为制造提供持续优化能力，企业治理则把目标、岗位、流程、数据与责任组织起来。

16.2 在真实交付中打磨

EOS 的设计取向来自真实制造现场：老系统仍在运行、计划依赖表格、变更依靠会议通知。由此形成的原则贯穿整套产品：不替换老系统而是承接它；把手工节奏里的隐含规则写成系统规则；人在环上做持续改进；确定性打底、模型增强；装上即可用，资料越完整能力越强。

16.3 从单企能力到产业生态

KTOS 面向不同企业时，不是复制固定的软件菜单，而是连接企业自己的系统、数据、知识与治理结构。经业务验证的模型、规则、模板、技能与数字员工能力，可以沉淀为行业基线与产业能力，支持从单企实践走向产业复制。

16.4 认知型企业与数智生命体

工具型 → 智能型 数字化从工具走向智能	**流程型 → 认知型** 企业能够理解自身与变化	**人工协同 → 人机协同** 人与数字员工共同工作	**静态管理 → 持续进化** 组织成为数智生命体

未来企业的竞争，不只取决于资源、规模和渠道，也取决于企业理解自身、理解客户、理解市场并持续学习的能力。KTOS 致力于成为企业智能时代的基础操作系统，让不同规模、不同产业的企业都能基于自己的数据、知识、治理与业务，构建安全、可控、可持续进化的企业智能系统。

16.5 持续演进方向

- 扩大规则与数字员工的协同覆盖，让更多高频例外从人工判断沉淀为可复用规则；
- 丰富行业基线与内容包，降低同类企业的初始化成本；
- 深化与企业统一认证、更多业务系统的标准化对接；
- 在安全前提下逐步开放后台自动执行与事件自动发起流程。

以上方向在附录 C 中标注为“规划中”，不构成具体交付承诺；具体能力以发布版本为准。

EPILOGUE

结语

> **企业智能化的终点，不是部署更多工具，也不是追求无人化，而是形成新的组织能力。**

战略能够被理解
目标连接到指标、主线与行动

风险能够被感知
业务事件主动浮现，路由到责任人

知识能够被调用
经验沉淀为规则、规程与技能

任务能够被协同
人与数字员工围绕同一对象办理

决策能够被验证
每个结论都有证据与回执

经验能够被留下
结果回流，组织持续进化

KTOS 以企业治理为根，以业务本体、事件、流程与数字员工为基础，以酷小易、酷小智、酷小匠为核心产品载体，以 EOS 让智能落到业务现场，推动企业从流程型组织走向认知型组织，从人工协同走向人机协同，从静态管理走向持续进化。

KTOS，有灵魂的企业智能操作系统。

附录 APPENDIX

术语表、技术规格与能力状态

A 术语表

术语	在本白皮书中的含义
KTOS	企业智能操作系统产品体系总称
KTOS 统一底座	各产品共用的本体、身份权限、规则、知识与技能、模型接入、工具目录与安全审计能力
EOS	部署在企业侧的业务运行底座与制造业务应用，是 KTOS 的组成部分
交付平台	酷小智的平台侧部分，管理多个企业项目的初始化、定制、发布与升级
业务本体	对业务对象、属性、关系、状态、规则和动作的共同描述
业务事件	值得被处理的对象或事实变化，经显式确认后进入处理
业务主线	订单等主对象要经过的节点，每个节点声明负责岗位、完成证据、时效与异常（定义层）
主锚	一类业务对象在工作台上的工作契约：数据来源、事实口径、动作、负责岗位与可发起流程（定义层）
工作卡	主锚在工作台上的呈现，包括对象卡、批次卡与节点待办卡（运行层）
节点待办卡	由业务主线自动派生的工作卡，列出停在该节点的对象
批次卡	按规则把同类工作分组、集中办理的工作卡
事项	工作卡上轮到某人处理的一件具体工作（运行层）
流程 / SOP	组织人员、数字员工与系统动作的办理步骤；定义有版本，运行时为流程实例
数字员工	绑定岗位、按作业规程完成准备或受控判断的产品角色，分业务、系统集成、AI 编程三类
作业规程	数字员工一步之内的做法：取数、核对、技能三段
自主等级	数字员工结果被自动采纳的程度，分 L0 至 L3
发布门	数字员工上岗前的审核清单，包括基于真实冻结事实的回放
正式动作与回执	受权限与业务约束的操作，以及可核对的执行结果
证据链	以同一追溯标识串联事件、判断、决定与执行结果的记录
业务承担方	某一业务领域由 EOS 内置应用还是客户现有系统承担
企业初始化	把企业资料转化为适用定义与必要数据的建设过程
变更说明书	代码层变更附带的“原来 → 改后 → 影响”说明，供业务审核

B 技术规格（企业侧运行时）

项目	说明
服务端	Java 17 / Spring Boot 3，内置流程引擎、数字员工执行器、对话助手与集成执行
数据库	PostgreSQL，结构变更经版本化迁移管理
前端	React 单页应用，经前端网关访问服务端
部署方式	容器化交付（Docker Compose），提供配置初始化、就绪检查、升级与备份恢复说明
模型接入	配置默认模型，可为不同数字员工绑定不同模型
身份与安全	统一身份与会话令牌、口令加盐哈希、敏感凭据加密存储、全量审计
交付平台	平台服务与任务执行器，管理项目、初始化、内容包、集成映射与发布
契约	平台侧与企业侧之间以 JSON Schema 契约划界，每条边界配有反例校验

C 能力状态矩阵

本矩阵是产品演示、销售承诺与交付验收的共同依据。状态截至 2026 年 10 月，随版本更新，以正式发布说明为准。

已发布 标准版本可用　验收中 已实现，正在统一验收　按项目交付 需按项目配置、集成或定制　规划中 演进方向，不作交付承诺

领域	能力	状态
统一底座	统一身份、口令登录、岗位与数据范围权限	已发布
统一底座	全链路审计与证据链、敏感凭据加密	已发布
统一底座	模型接入与数字员工模型绑定	已发布
统一底座	业务本体、动作目录、内容包与版本	已发布
统一底座	企业统一认证（SSO）对接	规划中
运行机制	工作周期、业务事件、调度规则与人工发起流程	已发布
运行机制	流程引擎（人工、数字员工、系统步骤）	已发布
运行机制	订单主线、节点待办卡、主锚工作台、批次卡、事项中心	已发布
运行机制	对话即工作；经批准的定时任务	已发布
运行机制	事件自动发起流程、团队后台自动执行	规划中
数字员工	员工档案、技能版本、发布门与回放；准备与受控判断	已发布
数字员工	较高自主等级的自动采纳策略	按项目交付
数字员工	从运行反馈自动提炼规则	规划中
制造应用	订单（OMS）、研发选配 / BOM / 工艺（RDC）、制造执行（MES）、质量（QMS）、仓储（WMS）、主数据（MDM）	已发布
制造应用	计划排程：基础排程与试排	已发布
制造应用	计划排程：复杂约束求解	按项目交付
制造应用	采购（SRM）八个环节	验收中

领域	能力	状态
制造应用	设备维护（EAM）	已发布
制造应用	预测性维护	规划中
制造应用	财务协同（完整会计核算与税务不在标准范围）	按项目交付
制造应用	移动端、扫码与现场设备接入	按项目交付
原生产品	酷小易经营态势、风险识别与决策辅助	按项目交付
原生产品	酷小匠需求解析、方案生成与工艺转译	按项目交付
交付与集成	企业初始化：三路输入、目录匹配、写进项目、一次性装载与回执	已发布
交付与集成	初始化逐项对账与统一就绪报告	验收中
交付与集成	外部系统集成	按项目交付
交付与集成	分层变更、本地配置包与变更说明书	已发布
交付与集成	已有部署的重新部署与签名恢复计划	规划中

D 资料基础

- 《KTOS 企业智能操作系统产品白皮书》V3.2 综合版（2026 年 9 月）、V4.0（2026 年 10 月）
- EOS 产品设计文档、设计思想提炼报告、架构决策记录与术语表
- 酷小易、酷小智、酷小匠产品介绍材料；酷特企业治理与制造实践材料

KTOS

有灵魂的企业智能操作系统

让企业拥有智能大脑，让 AI 成为组织能力。

治理驱动 · 事件驱动 · 规则打底 · 证据闭环

青岛酷特智能股份有限公司 · KTOS 企业智能操作系统产品白皮书 V4.1 · 2026 年 10 月