系列第 2 期 · 承接第 1 期《你的AI缺了一个大脑》

DATA PLATFORM TO AI PLATFORM

你的数据中台离AI就差三层

语义层 · 工具层 · 记忆层 — 从数据中台到智能中台的升级路径

很多伙伴在问：概念有了，怎么落地？

第一期讲了本体论的底层逻辑 — 为什么企业AI需要一个"大脑"。很多伙伴看完后的共同问题是：**概念认同了，但不知道从哪里下手。**

最常见的问题：我们有数据中台、有数仓、有指标体系，接下来做什么？

答案是：**补三层**。不是推翻重来，是在现有基础上加装三层能力 — 让数据从"人能看懂"变成"AI能理解、能操作、能记住"。

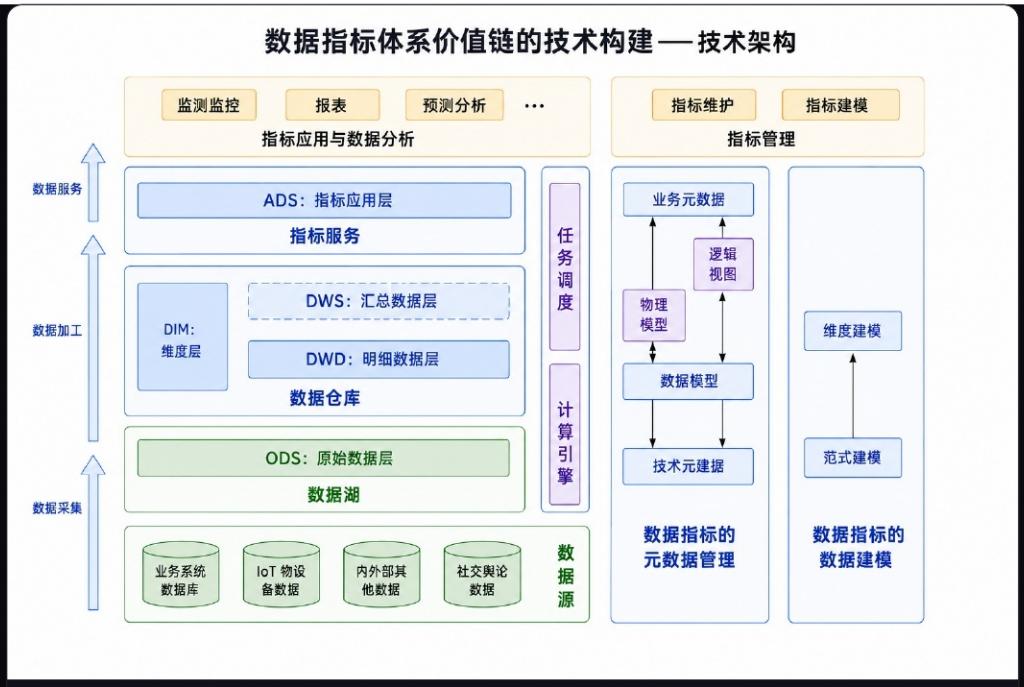
> 你的数据中台离AI不远。缺的不是数据，是让AI理解数据的语义层、操作数据的工具层、记住经验的记忆层。

YOUR CURRENT STACK

你现在有什么

大多数做过数据建设的企业，数仓分层已经比较清晰。核心是四层架构：





PPT截图：数据指标体系价值链的技术架构 — ODS → DWD → DWS → ADS 完整分层

核心问题：人能看懂，AI看不懂。

为什么看不懂？因为你的数据停留在"符号"层面。AI需要三层语义才能真正理解：

01

符号层

"gross_margin_rate" 是个字段名，是个符号。AI看到的是一串字符。

02

指代层

这个符号指的是"毛利率"，口径是（营收-成本）/营收。AI知道它代表什么。

03

解释层

毛利率下降意味着什么？应该沿哪些维度下钻？什么阈值算异常？AI能推理。

大多数企业的数据中台只覆盖了第一层（符号层），最多到第二层（指代层）。**第三层 — 解释层 — 几乎空白。**这正是AI理解业务最需要的东西。

LAYER 1 — SEMANTIC LAYER

第一层：语义层

语义栈厚不厚、活不活，直接决定了AI的准确率上限。

语义层不是一个单一的"字典"，而是一套7+1的规范体系。每一维都让AI对业务的理解更深一层：

7+1 语义规范（点击展开）

1. 实体 Entity

业务世界的核心名词：客户、订单、产品、供应商、合同。每个实体有唯一标识、属性定义、生命周期状态。

不只是数据库的表名 — 实体定义要包含业务含义、所有者、变更规则。AI需要知道"客户"在你公司到底意味着什么。

2. 关系 Relation

实体之间的连接：客户→下单→订单，产品→使用→原材料，供应商→提供→SKU。

关系不只是外键。它有方向、有基数、有时间窗口。"铜价上涨影响了哪些产品线的毛利率"— 如果关系没定义，AI根本不知道从铜跳到毛利率。

3. 事件 Event

业务世界的动态变化：促销活动启动、供应商涨价、竞品发起补贴。事件有发生时间、影响范围、因果链。

指标只告诉你"毛利率降了"，事件告诉你"为什么降了"。没有事件层，AI的归因分析就是猜测。

4. 规则 Rule

业务约束和决策逻辑：毛利率低于30%触发预警、战略客户享受额外折扣、铜料长单对冲比例不低于45%。

规则是AI行为的护栏。没有显式化的规则，AI给出的建议可能违反你的业务策略。

5. 指标 Metric

不只是数字的定义，而是完整的指标语义：计算公式、口径版本、数据源、刷新频率、可下钻维度、正常范围。

"毛利率"这三个字，在你的企业里有几个口径？含不含营销分摊？哪个版本是最新的？这些都是语义。

6. 词表 Glossary

术语统一和同义词映射：华北区=北区=North China Region、GMV=成交总额=Gross Merchandise Volume。

这是NL→SQL的第一道翻译关。用户说"北区毛利率"，没有词表，AI不知道北区=华北大区。

7. 模型 Model

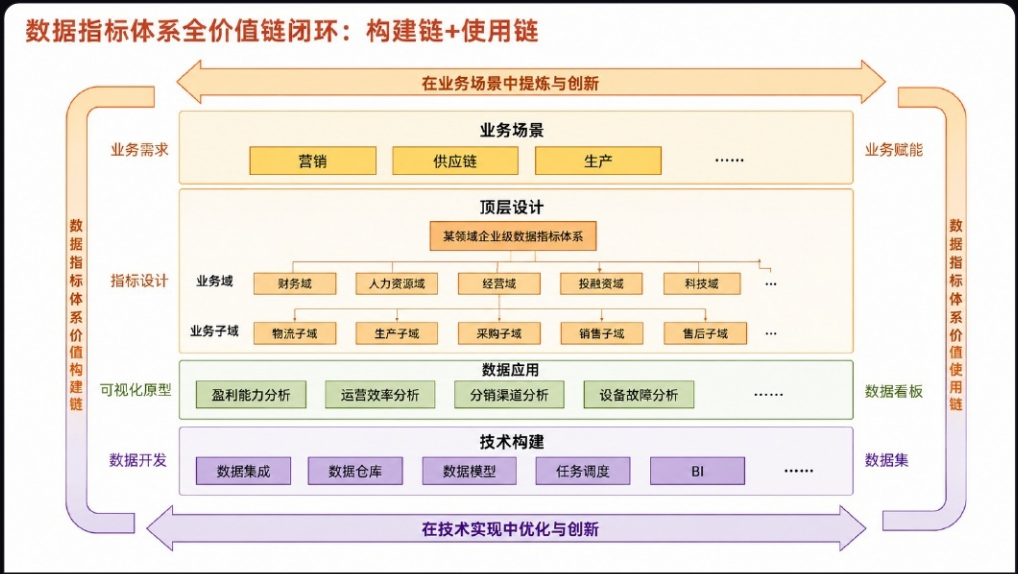
概念模型和领域模型：零售行业的"人-货-场"模型、供应链的"采-产-销"模型。

模型规范让AI理解你所在行业的思维框架，而不只是孤立的数据点。它是AI做行业推理的前置知识。

+1 治理引擎 Governance

横切以上所有维度的持续治理机制：谁定义的？什么时候更新的？版本冲突怎么解决？废弃的口径怎么处理？

没有治理引擎，语义层就是一次性工程。有了治理引擎，语义资产才能持续增厚。



PPT截图：Data Agent 语义栈 8 层架构 — 从锚定语义到会话反馈的完整分层

NL → DSL → SQL：三条技术路径对比

自然语言查数据，目前有三种主流方案。准确率差异巨大：

NL → SQL 风险高

50-70%

LLM直接把自然语言翻译成SQL。简单场景可以，稍微复杂就翻车 — 口径歧义、表关联错误、过滤条件遗漏。

NL → SQL + RAG 可用

70-90%

加了检索增强，LLM能查到表结构和字段注释。但注释质量参差不齐，复杂多表关联依然困难。

NL → DSL → SQL 推荐

98%+

先把自然语言翻译成领域语义语言(DSL)，DSL再确定性生成SQL。语义层做了最难的翻译，SQL生成变成模板渲染。

dbt Labs 基准数据：有完整 Semantic Layer 的情况下，NL → DSL → SQL 准确率可达 98% 以上。没有语义层的 NL → SQL，在 JOIN 超过 3 张表时准确率骤降至 50% 以下。

LAYER 2 — TOOL LAYER

第二层：工具层

> AI的能力上限，取决于它接了多少工具。语义层让AI"看懂"，工具层让AI"动手"。

MCP协议 — AI的USB接口

什么是 MCP (Model Context Protocol)?

Anthropic开源的标准协议。类比USB — 过去每个设备需要专用数据线，USB统一了接口标准。MCP做的是同样的事：让任何AI模型能标准化地接入任何工具/数据源。

一个 MCP Server 暴露一组能力（查指标、查事件、查知识库），AI通过MCP Client按需调用。工具和模型彻底解耦。

核心优势：**写一次工具接口，所有模型都能用**。Claude、GPT、开源模型 — 换模型不用改工具层。

渐进式学习路径 — shareAI 20课

不需要一步到位。从最简单的工具开始，逐步加厚：

第1课
Claude基础
理解AI Agent的基本交互模式。从一个简单的对话开始。

第3课
MCP入门
搭建第一个MCP Server，理解工具定义和调用协议。

学会让Agent在多

毛利率归因案例 — 三种工具

回到第一期的毛利率归因场景。Agent至少需要三种工具才能完成归因分析：

📊

指标查询

查毛利率的值、同环比、按维度下钻。走语义层的DSL，确定性查询。

⚡

事件查询

查时间窗口内的业务事件：促销、涨价、竞品动作。事件是归因的线索。

📚

知识检索

查非结构化知识：市场报告、运营文档、历史分析记录。RAG支撑的深度推理。

> 数据权限提醒：工具层必须内置权限控制。不同角色看到的数据粒度不同 — VP看大区汇总，BU Head看品类明细，一线看SKU级别。权限不是可选项，是生产级必须。

LAYER 3 — MEMORY LAYER

第三层：记忆层

本体就是Agent的长期记忆。

Agent没有记忆，每次对话都是"失忆重来"。记忆层让AI积累经验、沉淀知识、越用越准：

业务规则

毛利率低于30%要预警。战略客户有折扣豁免。铜料长单比例不低于45%。这些规则AI需要记住，不能每次重新问。

领域知识图谱

实体关系网络 — 铜→家电→华北线下，供应商→原材料→产品线。这是AI跳转推理的"地图"。第一期讲的本体论核心。

历史分析记忆

上次分析毛利率下降时，用户纠正了铜料对冲比例是45%不是30%。这个纠正要记住，下次不再犯同样的错。



PPT截图：本体 + 指标体系打造 AI Agent 资产底座 — 本体是Agent的长期记忆基础

没有记忆的Agent

- 每次对话从零开始
- 重复犯相同的错误
- 不知道业务规则和约束
- 无法积累经验
- 输出质量不稳定

有记忆的Agent

- 记住历史对话和纠正
- 从错误中学习迭代
- 自动应用业务规则
- 分析越来越精准
- 输出质量持续提升

记忆层的关键洞察：语义层是静态知识（什么是什么），工具层是动态能力（能做什么），记忆层是进化能力（学到了什么）。三层叠加，Agent才能从"能用"变成"好用"再变成"越来越好用"。

HARNESS & ROADMAP

Harness架构 + 落地路线图

Agent = **Model** + **Harness**

智能体　　大模型　　运行时框架

Model是通用智能（别人家的），Harness是你自己的业务封装。Harness有四个核心组件：

Agent Loop 核心

思考→行动→观察→再思考的自主循环。Agent不是一问一答，而是持续推理直到任务完成。Loop的质量决定了Agent的"智商"。

权限控制 安全

谁能看什么数据、调什么工具、执行什么操作。生产环境必须有细粒度的权限控制，否则数据安全就是裸奔。

上下文管理 效率

Token是有限的。如何在有限的上下文窗口内，放入最相关的信息？上下文管理决定了Agent的"效率"和"准确度"。

Hooks系统 扩展

在Agent执行流程的关键节点插入钩子：发送前审核、工具调用前鉴权、输出后记录。Hooks让Harness具备可观测性和可扩展性。



PPT截图：Ontology vs ECA 三层架构对比 — 大脑与手脚的协同分工

四步走路线图

1. **指标语义化**
   从最核心的20-50个指标开始，补全计算公式、口径版本、维度定义、业务解释。不贪多，先把最常用的做透。这一步最快，2-4周可完成。
2. **查询接口化**
   用MCP标准把指标查询、事件查询、知识检索封装成工具。先做"只读"，让AI能查但不能改。降低风险，快速验证。
3. **试点场景落地**
   选一个高频、低风险的分析场景跑通全链路。比如"月度毛利率归因"— 需求明确、数据齐全、结果可验证。用这个场景证明价值。
4. **逐步加厚**
   场景验证成功后，扩展更多指标、更多工具、更多记忆。语义栈越厚，AI越准。这不是一次性项目，是持续积累的过程。

三个核心判断

01

数据中台不需要推翻重来。ODS/DWD/DWS/ADS的分层投资都是有效的。你需要的是在上面加装三层能力 — 语义层、工具层、记忆层 — 让存量资产发挥AI时代的新价值。

02

语义层的厚度决定了AI的准确率。NL → SQL 准确率50%的方案和98%的方案，差距就在语义层。这不是模型选型问题，是语义资产积累问题。

03

Agent = Model + Harness。Model会不断贬值（更便宜、更强），Harness的价值只会升值 — 因为它封装的是你独有的业务知识、工具能力和经验积累。

模型会贬值，语义资产只会升值。

因为它是你的业务共识、领域深度和组织记忆的结晶。越用越厚，越迭代越精准。

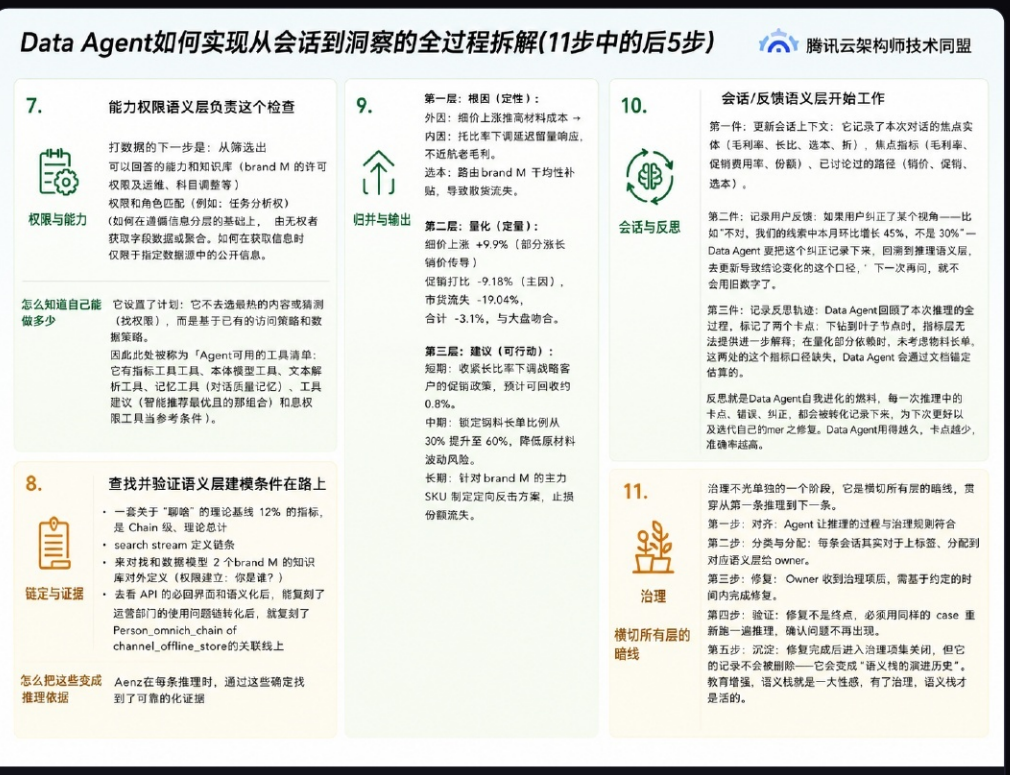
CASE STUDY — FULL WALKTHROUGH

案例回顾：11步归因全景

回到第一期的毛利率归因案例。11步中的每一步，对应语义层 / 工具层 / 记忆层 / Harness的哪个组件：



PPT截图：Data Agent 从会话到洞察 11 步拆解 — 前 6 步（意图解析到量化回填）



PPT截图：Data Agent 从会话到洞察 11 步拆解 — 后 5 步（规则安检到治理闭环）

▼ 点击每一步展开详情和层级标注

1 意图解析

AI识别"毛利率下降3.1个点"为指标归因类任务，自动拆解关键参数：指标、时间窗口、异常幅度、对比基准。

Harness · Agent Loop

2 指标语义层拆解

查询毛利率的完整语义定义：计算公式、口径版本、数据源、可下钻维度（时间/地区/品类/渠道/客户群）。

语义层 · 指标

3 维度下钻 — 三刀切

按地区切→华北降2.1点，按品类切→家电降1.8点，按渠道切→线下降1.8点。定位：华北 → 家电 → 线下。

工具层 · 指标查询　语义层 · 维度

4 跳出指标 → 本体层查询

AI沿关系网络跳转：SKU核心材料=铜→供应商=Supplier X→上游=Mine Z。同时发现促销强度标记为"高"，竞品有补贴活动。

记忆层 · 知识图谱　语义层 · 关系

5 事件层验证

铜价Q3环比涨12%、Brand M启动以旧换新补贴、华北区促销密度同比涨40%。三个事件，三条归因线索。

工具层 · 事件查询　语义层 · 事件

6 量化回填

回到指标语义层，量化每条路径的影响：铜价传导 -0.9点、促销折让 -1.8点、竞品补贴 -0.4点。三条加总 = -3.1点，闭合。

工具层 · 指标查询　语义层 · 指标

7 规则安检

检查数据权限、合规约束、运营规则。毛利率35.1%高于30%预警线。促销收紧建议需区分战略/非战略客户。

记忆层 · 业务规则　Harness · 权限

8 锚定文档

将市场报告锚定到 material:copper 节点，监测报告锚定到 brand_M 实体。Agent做多跳推理时，能追溯到原始证据。

工具层 · 知识检索　语义层 · 锚定

9 归并输出

三层结构输出：定性（原因是什么）+ 量化（影响多大）+ 建议（怎么办）。Agent的最终交付物。

Harness · 上下文管理

10 会话反馈

记录本次对话焦点：毛利率→华北→家电→线下。用户纠正的信息（如铜料对冲比例45%）回流更新。

记忆层 · 历史记忆　Harness · Hooks

11 治理闭环

推理过程中遇到的"卡点" — 语义歧义、数据缺失、规则冲突 — 结构化记录。分类→分配owner→修复→验证→沉淀。语义栈一轮轮迭代变厚。

语义层 · 治理引擎　记忆层 · 沉淀

色标说明：

语义层　提供语义理解和定义

工具层　提供数据查询和知识检索能力

记忆层　提供规则、图谱和历史经验

Harness　提供运行时框架和流程控制

11步中，**没有一步只靠Model**。每一步都依赖Harness的某个组件。这就是为什么说"Agent = Model + Harness"。

素材来源：腾讯云架构师技术同盟闭门会 · 2026.07

参考：shareAI-lab/learn-claude-code · Datawhale/hello-agents

by Tricia