New Generation of ERP in Manufacturing Based on Model Context Protocol

梁耘豪

April 12th 2025
https://github.com/YunhaoLiang/NewGenerationERP--In-Process

1 Introduction

制造业的数字化转型正迈入一个新阶段，传统 ERP 系统亟需与新兴技术融合以实现更高的自主性和智能化 [3]。随着工业 4.0 的发展，大量物联网设备部署在车间，实现海量数据的实时采集.[3]。但是，传统 ERP 往往难以实时处理复杂动态环境，无法充分利用非结构化信息。为提高制造系统的适应性，学术界提出了多智能体系统（Multi-Agent System, MAS）架构，使多个自主代理协同决策和沟通 [1]。然而，早期 MAS 代理在应对新规范或理解人类指令方面能力有限，难以处理文本等非结构化数据。大型语言模型（Large Language Model, LLM）的兴起为这一瓶颈提供了全新解决方案：LLM 拥有强大的自然语言理解和生成能力，能够解释并执行自然语言指令，根据动态变化做出决策，提升制造系统对变化的自适应响应能力 [1]。

1.1 Scheme

针对以上背景，我提出一套下一代 ERP 系统架构方案，融合 MCP 协议 [4]、大模型、IoT、联邦学习与智能 Agent，以制造业核心生产与管理流程为应用场景，打造端到端的自动化解决方案。本方案的创新在于：以模型上下文协议（Model Context Protocol, MCP）作为核心通信机制，将 LLM 智能体与各类业务模块、物联网装置连接起来，实现标准化、安全的交互，RPA 与 IPA 的概念实施 [2]；通过多 Agent 协作架构，将订单处理、生产计划、供应链采购、仓储物流、财务核算等功能模块解耦为自主智能体，各司其职又通过共享上下文紧密协作；在数据层面，支持边缘计算和私有部署，敏感数据在本地处理，并通过联邦学习实现跨地点的模型协同优化，确保数据隐私与模型精度的兼顾。下文将详细阐述本系统的总体架构、智能 Agent 设计、端到端业务流程、部署方案以及安全与弹性设计，并给出分阶段的实施路线图。

1.2 Related Work

各大 ERP 厂商也开始将生成式 AI 引入业务流程：微软在其 Dynamics 365 ERP 中集成了 OpenAI 的模型，SAP 于 2023 年推出了名为“Joule”的 AI 助手，用于增强用户决策 [5]。这些趋势表明，新一代 ERP 将以智能化和自动化

为核心特征。不仅如此，制造企业对数据隐私和部署自主权的要求日益提高。在跨工厂或跨企业协作中共享数据会带来隐私风险，这促使研究者探索联邦学习（Federated Learning, FL）等分布式训练方法，在不共享原始数据的前提下协同训练模型。FL 使得中小企业能够通过共享模型提升预测精度，同时保持各自数据的机密性 [6]。

1.3 Current ERP Structure

传统 ERP 系统采用模块化架构，通常围绕企业的核心运营流程划分为多个子系统，如财务管理、供应链管理、生产控制、人力资源管理和销售客户管理等。下图展示了一个典型的传统 ERP 系统结构框架。

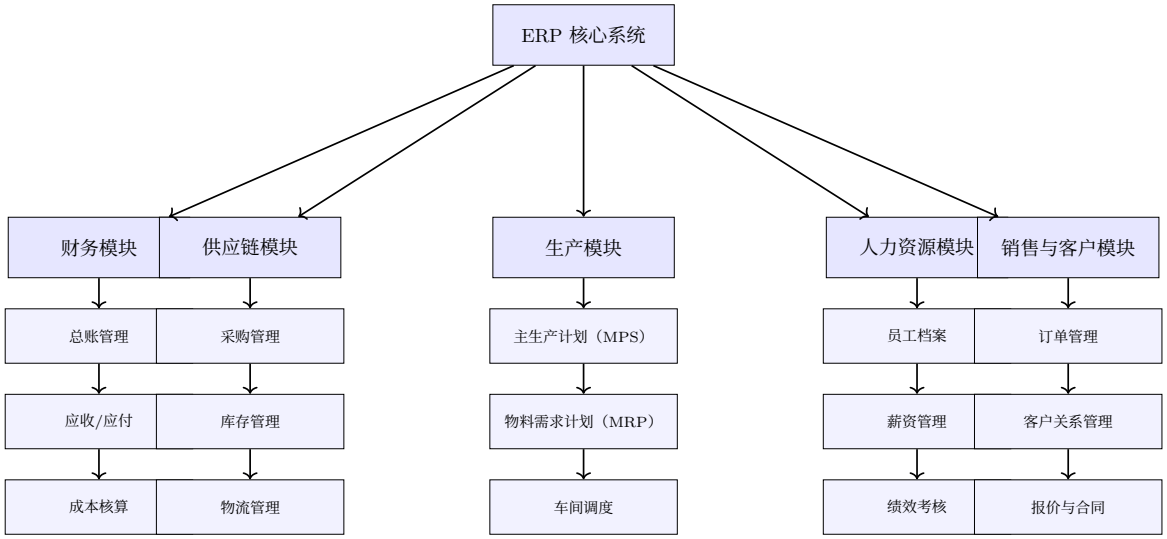

Figure 1: 传统 ERP 系统模块结构图（以制造业为例）

1.4 ERP General Process

ERP 系统整合销售、采购、生产、库存与财务等关键环节，实现信息流、物流与资金流的协同管理。典型流程如下:

客户下单后，系统生成**销售订单**（若库存不足）–> **采购订单** –> **采购入库** 根据任务单及 BOM –> **生产领料** –> 成品完成后**产品入库**。

产品交付时执行**销售出库**，系统自动进行**存货核算**，处理**采购发票**、**入库单价**、**费用分摊**等信息，最终**生成财务凭证**，实现业务与财务的一体化。

2 New Generation

在传统 ERP 结构的基础上，本系统提出一种以大语言模型（LLM）与模型上下文协议（MCP）驱动的下一代智能 ERP 架构，旨在实现端到端的业务自动

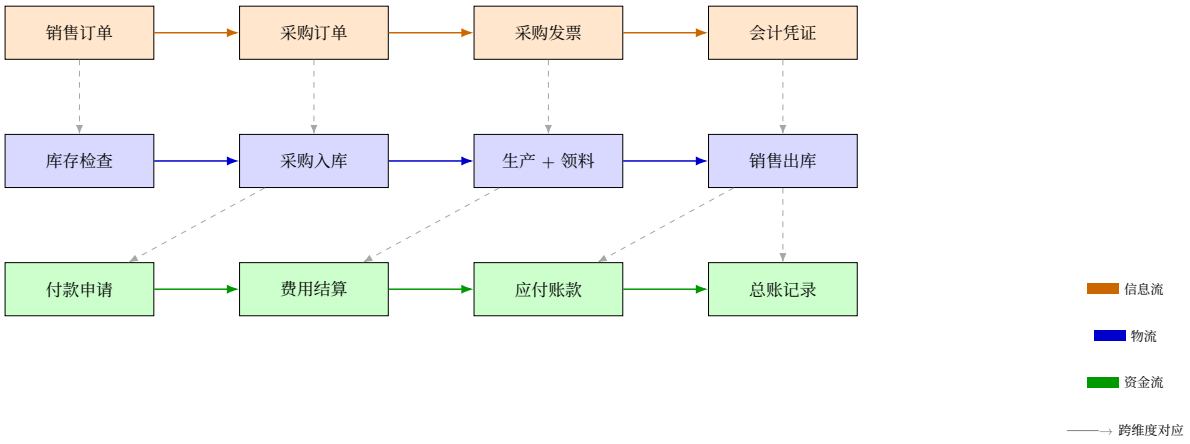

Figure 2: ERP 系统中的信息流、物流与资金流流程图

化、柔性化与智能化。整体设计体现了多智能体系统（MAS）与模型驱动架构（MDA）的融合。

2.1 System Architecture

该架构主要包括三层:

- LLM Orchestrator：负责接收自然语言任务、解析语义、调用对应 Agent 并协调信息流。相当于 MCP Host，控制调用链。
- Agents：每个 Agent 为一个 MCP Server，承担特定任务（如订单解析、排程优化、库存补货等），并通过 MCP 接口暴露其服务能力。
- Edge+Cloud：IoT、数据库、模型推理引擎、Gurobi 优化器等组成的混合边缘 + 云环境，作为 Agent 的后端支撑系统。

2.1.1 LLM Orchestrator

LLM Orchestrator 相当于架构中心，作用是接收业务指令，譬如订单文本，将其生成对应的子任务，然后调用具体的 Agent。

理想实现方式:

- 理解层: 首先对接用户自然语言任务，基于大模型微调，例如 ChatGLM，接受业务指令，转换成字任务（结构化参数）
- 决策层：根据理解层意图选择/调用组合 Agent，结合 rule-based 规则树完成任务，后续的 rule 也只需增添删减 rule 就可以了（规则引擎）
- 通过 MCP Client 调用相应 MCP Server

该模块既可部署于中心服务器，也支持本地，确保系统对数据隐私和实时性要求的适应。

2.2 Intelligent Agents

当前版本考虑多个面向不同功能域的自主 Agent，每个 Agent 开放受控接口供 LLM Orchestrator 调用。例如，当有新的生产订单时，LLM Orchestrator 调用 order Agent 解析需求，调用 planning Agent 进行产能预测和排程，调用采购 Agent 检查原料库存及下单采购。

2.2.1 Agents Type

新一代 ERP 将主要功能划分为若干智能 Agent，每个 Agent 负责特定领域的业务逻辑和决策。各 Agent 内部集成相应的 AI 模型、算法和数据处理模块，以实现智能化的自主运行。它们通过 MCP 接口与 LLM 编排器和其它 Agent 通信，协同完成端到端流程。下面定义主要 Agent 及其职责与技术实现：

Agents	**主要职责**	**实现技术/方法**
Order Agent	解析来自 LLM Orchestrator 的结构化订单请求，提取产品类型、数量、交期等信息，并传递给生产计划模块。	NLP 模型，规则引擎，JSON 结构映射
Planning & Scheduling Agent	根据订单需求、产能状态与物料库存，构建主生产计划（MPS）与作业调度模型（如 JSSP），优化任务分配与排程。	混合整数规划（MIP），Gurobi 或 CPLEX 优化器
Supply Chain Agent	结合 MRP 结果与实时库存数据判断补货需求，制定原料采购计划与库存调拨策略，保障供应稳定性。	安全库存规则，采购批量模型，Gurobi 优化
Prediction Agent	分析 IoT 数据与业务日志，提供预测性维护、质量预测或交期风险预警服务（可选模块）。	联邦学习，时序预测模型（如 Transformer）或接入现成生态软件如 zeryth
Finance Agent	根据订单、入库、出库等业务事件自动生成会计凭证，完成成本核算与收入确认，支持财务对账与报表输出。	规则引擎即可

Table 1: 智能 ERP 系统中各类 Agent 的职责与实现建议

各 Agent 之间通过 LLM Orchestrator 协调，任务与数据在统一上下文中流转，构成一个语义可解释、逻辑自治、流程协同的智能制造系统。

2.2.2 IoT 与数据感知层

在智能 ERP 架构中，IoT（物联网）承担着数据采集与实时感知的底层角色，是连接物理世界与 Agent 决策层的桥梁。工厂中的各类传感器（温湿度、压力、振动、能耗等）与边缘设备（如工业摄像头、RFID 设备、PLC 控制器）通过边缘节点实时上传关键状态信息，为系统提供持续的“数据流”。

在部署架构上，推荐在每个工厂的边缘节点部署微型网关与轻量级采集程序（如 Zerynth），这些模块将原始传感数据转换为统一的 MCP 消息格式，并缓存于本地数据库（如 SQLite），保障低延迟与高安全。

感知层的数据一方面可用于实时控制与设备联动（如设备故障自动停机），另一方面作为输入传递给 Prediction Agent、Scheduling Agent 等上层 Agent，用于预测性维护、排程调整等高阶决策任务。

- 数据路径：`IoT 设备 → 边缘采集脚本 → 本地缓冲/筛选 → 转换为 MCP 格式 → 上送 Orchestrator/Agent`
- 可嵌入部署设备：树莓派、NVIDIA Jetson、Arduino + WiFi 模组

这是由 ChatGPT 创建的图，或许它可以更好地说明结构。

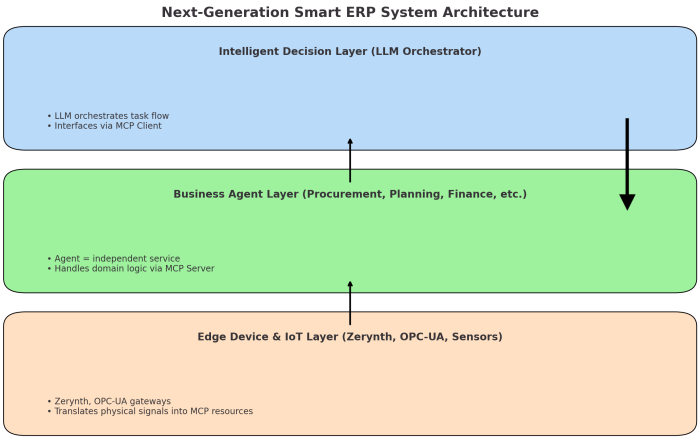

Figure 3: 系统架构图：LLM + MCP 驱动的智能 ERP

3 Workflow(end2end)

基于上述架构，ERP 系统实现了从接单到生产、发货再到财务结算的端到端全流程自动化。以制造业为例，系统工作流程如下：

1. **订单接收与解析**：客户订单通过电子接口进入系统，由 Order Agent 负责解析 LLM 编排器输出的结构化请求，提取产品类型、数量、交期等信息并存入数据库。
2. **生产计划与调度**：Planning & Scheduling Agent 根据当前产能、工艺路线与库存信息构建 MPS 和 MRP 模型，并调用 Gurobi 求解作业排序与物料配置，生成排产结果。
3. **供应链执行**：Supply Chain Agent 接收 MRP 结果，判断原料是否需补货，调用采购接口或联动库存模块下发采购申请。原料到达后自动更新库存状态并触发入库流程。

4. **生产执行与监控**：根据排程结果生成工单，设备通过 IoT 接口执行生产任务，数据同步至系统。若传感器检测到异常，Prediction Agent 进行判断并通知排程模块重构计划。

5. **入库与出库物流**：产品完工后扫码入库。出库由系统自动生成拣货任务，AGV 或仓储机器人执行搬运任务，物流记录实时写入系统。

6. **交付与服务**：客户可通过接口查询订单状态，LLM 汇总订单、库存、物流等信息生成可读反馈。签收完成后，系统更新交付状态。

7. **财务结算**：Finance Agent 自动记录采购、销售和生产等业务事件，生成应收应付、库存结转等财务凭证，并定期输出财务报表供管理层审阅。

该流程实现了高效闭环的智能协同，各模块各司其职，LLM 在关键环节提供语义补全与任务调度，大幅提升系统自动化水平与业务透明度。

4 TimeLine

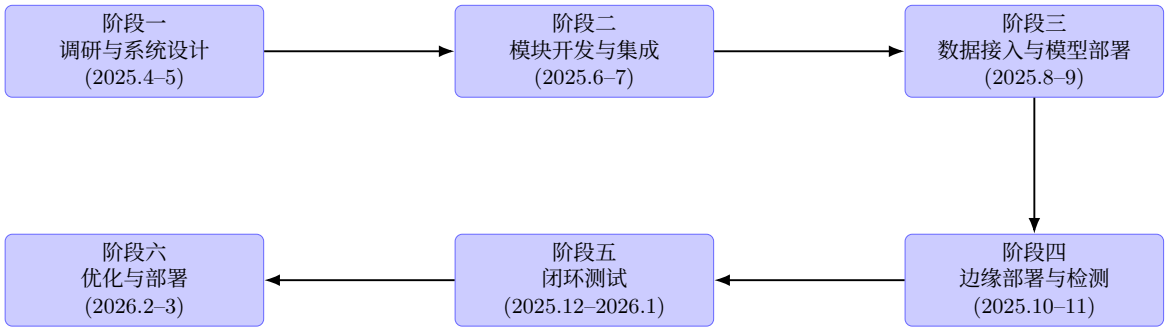

Figure 4: 项目实施时间线

5 Secure and scalable design

5.1 About Security

由于制造业企业非常关注数据安全和系统自主可控，该系统推荐避免纯云端依赖，支持在企业本地或混合云环境下灵活部署：系统的各 Agent 和 LLM 编排器可部署在企业自有的服务器或边缘计算节点上。例如，在每个工厂内部署一套完整的 Agent 服务集群和 LLM 实例，使数据就地处理，避免将敏感生产数据上传到公共云。同时，关于系统的各组件可以采用容器化技术封装，如 docker。每个 Agent 以及 LLM 服务都封装为独立容器，通过容器编排系统（如 Kubernetes）进行部署管理。这样可以根据负载进行弹性伸缩。

5.2 Scalable design

当企业增加新的工厂、产线或业务模块时，可以方便地将新节点接入现有架构。例如，新建一个工厂时，部署新的边缘节点 Agent 实例，并在中央注册；LLM 编排器通过服务发现机制识别出新的 Agent 服务（因为 MCP 的标准接口具有自描述能力，可以注册到服务目录）。同理，如果需要增加新的业务功能模块（比如引入一个环保监测 Agent），只需开发符合 MCP 接口规范的 Agent 服务并部署，即可被编排器调用，从而扩展系统功能。这种插件式扩展不会影响已有系统。

6 Conclusion

本文提出了一套面向制造业的下一代智能 ERP 系统架构，基于大语言模型（LLM）、模型上下文协议（MCP）、多智能体系统（MAS）与优化建模工具（如 Gurobi），实现了订单接收、生产计划、供应链执行、物流入库、财务核算等环节的端到端自动化与智能化处理。

通过将各业务模块抽象为可插拔的智能 Agent，并使用统一的 MCP 协议完成任务注册与调用，系统具备高度的模块解耦性与语义集成能力。LLM Orchestrator 在系统中起到语义理解与任务编排的核心作用，能够根据自然语言输入协调多个 Agent 协同完成复杂业务流程，实现人机融合的业务执行模式。

此外，系统支持私有部署、边缘部署与多工厂扩展，具备良好的可扩展性、安全性与容器化部署能力。该架构不仅适用于中大型制造企业的数智化转型，也为未来多模型、多 Agent 协同的智能工业平台提供了参考蓝图。

References

[1] Large language model-enabled multi-agent manufacturing systems.

[2] Valentin Florentin Dumitru, Bogdan Ștefan Ionescu, Sînziana-Maria Rîndașu, Laura-Eugenia-Lavinia Barna, and Alexandru-Mihai Crîjman. Implications for sustainability accounting and reporting in the context of the automation-driven evolution of erp systems. *Electronics*, 12(8):1819, 2023.

[3] Oumaima El Hairech and Abdelouahid Lyhyaoui. The new generation of erp in the era of artificial intelligence and industry 4.0. In Janusz Kacprzyk, Valentina E. Balas, and Mostafa Ezziyyani, editors, *Advanced Intelligent Systems for Sustainable Development (AI2SD' 2020)*, pages 1086–1094. Springer International Publishing, 2022.

[4] Xinyi Hou, Yanjie Zhao, Shenao Wang, and Haoyu Wang. Model context protocol (mcp): Landscape, security threats, and future research directions. *ACM*, 1(1):1–20, April 2025. arXiv:2503.23278.

[5] IBM. Ai 在企业资源计划（erp）中的作用. `https://www.ibm.com/cn-zh/think/topics/ai-in-erp`, 2024.

[6] Farzana Islam, Ahmed Shoyeb Raihan, and Imtiaz Ahmed. Applications of federated learning in manufacturing: Identifying the challenges and exploring the future directions with industry 4.0 and 5.0 visions.