

resic AI Semiconductor ERP Agent Technical Architecture Analysis

Introduction

The system shown in the video, **resic AI - Semiconductor ERP Agent**, represents the latest trend in the deep integration of enterprise resource planning (ERP) and artificial intelligence (AI). It goes beyond the passive data-management model of traditional ERP systems, transforming into an intelligent, conversational "agent." This report provides an in-depth analysis of the technical architecture that resic AI likely employs, with a particular focus on how it integrates large language models (LLMs) with the semiconductor industry's domain-specific business logic.

Core Concept: AI Agentic Architecture

At the core of resic AI is an **AI Agentic Architecture** 6 6 . This architecture endows the system with the ability to understand complex instructions, plan tasks, use tools, and execute actions to accomplish user goals. It converts the databases and business processes of traditional ERP into "tools" and "knowledge bases" that an AI agent can operate.

Technical Architecture Components

The technical architecture of resic AI can be divided into the following key modules:

1. User Interface (UI)

- Web application: The video demonstrates a modern web application interface providing intuitive dashboards, tabular views, and forms for data display and user input.
- Conversational input: In particular, the "Ask" feature provides a natural-language input box that serves as the primary entry point for users to interact with the AI agent.

2. AI Agent Core / Orchestrator

This is the system's "brain," responsible for coordinating the modules to respond to user requests 6 .

- Intent understanding: Receives user natural-language input and parses the underlying business intent (e.g., "query orders", "create material").
- Task planning: Decomposes complex tasks into a sequence of executable subtasks and decides which internal tools or functions need to be invoked.

- Context management: Maintains conversational state and business context to ensure the AI agent can understand follow-up instructions and provide coherent responses.

3. Large Language Model (LLM)

The LLM is the foundation of Resic AI's intelligent interactions. The video mentions "requires local LLM," suggesting its deployment strategy 6.

- Natural language processing (NLP): Interprets user natural-language queries and converts them into structured instructions.
- Knowledge reasoning: Uses its training knowledge and the ERP database context to perform business-logic reasoning, for example determining which materials are "Controlled."
- Local deployment: Deploying the LLM on on-premises servers or a private cloud may be motivated by:
 - Data privacy and security: Semiconductor data is highly sensitive; local deployment reduces the risk of data leakage.
 - Performance and latency: Reduces reliance on external APIs, lowering latency and improving response times.
 - Cost efficiency: Long-term operational costs may be lower, and the model can be optimized for the specific domain.

4. Natural Language to SQL Engine (NL2SQL Engine)

This is the key module enabling the "Ask" feature, responsible for converting LLM-interpreted natural-language intents into executable database queries 6 6.

- Database schema understanding:
 - Semantic descriptions: Human-authored semantic descriptions help the LLM understand the business meaning of tables, fields, and relationships in the ERP database 6.
 - Automatically generated schema: Automatic extraction of the physical database schema (tables, column names, data types, constraints, etc.) is provided to the LLM as reference 6.
- SQL generation: The LLM generates syntactically correct SQL statements based on the user query and schema knowledge.
- SQL validation and optimization: This may include a "Critic" agent that performs syntax checks, semantic validation, and performance assessment of generated SQL and provides feedback for iterative improvement of the LLM output 6.

- SQL execution: Submits the validated SQL statements to the ERP database for execution and retrieves results.

5. ERP Database

- Structured data storage: Stores all structured data related to semiconductor business operations, including orders, bills of materials, supplier information, inventory, production schedules, etc.
- High availability and security: As the carrier of core enterprise data, it must provide high availability, data consistency, and strict access controls.

6. Business Logic & Domain Knowledge Module

- Semiconductor-specific rules: Built-in business rules specific to the semiconductor industry, such as material purity grades, storage conditions, and the "Controlled" material labeling logic demonstrated in the video 6 .
- Workflow automation: Defines business processes such as order creation, duplication, and approval, and works in concert with the AI agent.
- Compliance engine: Automatically checks and flags sensitive materials and transactions according to international export control regimes (e.g., the Wassenaar Arrangement, U.S. export controls) and domestic security regulations 6 .

7. Tool Integration

The AI agent can invoke a set of predefined "tools" to perform tasks 6 . In resic AI, these tools likely include:

- Database operation tools: Execute SQL queries, data inserts, updates, etc.
- Business function APIs: Call various ERP internal business functions, such as creating orders, updating material status, sending notifications, etc.
- External system interfaces: Potential future integrations with external supplier systems, logistics platforms, and so on.

8. Human-in-the-Loop & Safety

- Intent clarification: Before executing complex or ambiguous instructions, the system may request user clarification to ensure correct understanding by the AI 6 .
- Operation confirmation: Critical business actions (e.g., submitting an order) may require final user confirmation to prevent erroneous AI actions.
- Audit log: Records all user operations and the AI agent's decision-making processes for traceability and governance.

Conclusion

The technical architecture of resic AI exemplifies a domain-specific AI agent system. It skillfully combines the natural-language understanding capabilities of LLMs, the database interaction capabilities of an NL2SQL engine, and deep semiconductor domain knowledge. This architecture transforms ERP from a traditional data-management tool into an intelligent partner capable of understanding, reasoning, and assisting users with complex business tasks—particularly valuable when addressing the highly specialized and tightly regulated requirements of the semiconductor industry.

References

- [1] SEMI. Agentic AI For Next-Generation Semiconductor Manufacturing.
<https://www.semi.org/en/event/agentic-ai-next-generation-semiconductor-manufacturing>
- [2] AWS Machine Learning Blog. (2025, April 24). Enterprise-grade natural language to SQL generation using LLMs: Balancing accuracy, latency, and scale.
<https://aws.amazon.com/blogs/machine-learning/enterprise-grade-natural-language-to-sql-generation-using-llms-balancing-accuracy-latency-and-scale/>
- [3] arXiv. (2025, July 31). Chatting with your ERP: A Recipe.
<https://arxiv.org/html/2507.23429v1>
- [4] IBM. What Are AI Agents?. <https://www.ibm.com/think/topics/ai-agents>
- [5] Video content analysis (resic AI - Semiconductor ERP Agent, YouTube:
<https://youtu.be/cGsUv4r85Fo?si=56yZ4vkUxqgg8yVz>)

resic AI 半導體 ERP Agent 技術架構分析

引言

影片中展示的 **resic AI - Semiconductor ERP Agent** 系統，代表了企業資源規劃（ERP）領域與人工智慧（AI）深度融合的最新趨勢。它超越了傳統 ERP 系統的被動數據管理模式，轉變為一個具備智慧化、對話式互動能力的「代理人」。本報告將深入分析 resic AI 可能採用的技術架構，特別聚焦於其如何整合大型語言模型（LLM）與半導體產業的特定業務邏輯。

核心理念：AI Agentic Architecture

resic AI 的核心是一個 **AI Agentic Architecture**（AI 代理人架構）^{6 6}。這種架構賦予系統理解複雜指令、規劃任務、利用工具並執行行動的能力，以達成用戶目標。它將傳統 ERP 的數據庫與業務流程，轉化為 AI 代理人可操作的「工具」和「知識庫」。

技術架構組成

resic AI 的技術架構可分為以下幾個關鍵模組：

1. 用戶介面 (User Interface, UI)

- **網頁應用程式：**影片中展示的是一個現代化的網頁應用程式介面，提供直觀的儀表板、表格視圖和表單，用於數據展示和用戶輸入。
- **對話式輸入：**特別是「Ask」功能，提供一個自然語言輸入框，作為用戶與 AI 代理人互動的主要入口。

2. AI 代理人核心 (AI Agent Core / Orchestrator)

這是整個系統的「大腦」，負責協調各個模組以響應用戶請求 6。

- **意圖理解 (Intent Understanding)：**接收用戶的自然語言輸入，解析其背後的業務意圖（例如「查詢訂單」、「建立材料」）。
- **任務規劃 (Task Planning)：**根據用戶意圖，將複雜任務分解為一系列可執行的子任務，並決定需要調用哪些內部工具或功能。
- **上下文管理 (Context Management)：**維護對話狀態和業務上下文，確保 AI 代理人能理解連續的指令並提供連貫的響應。

3. 大型語言模型 (Large Language Model, LLM)

LLM 是 resic AI 智慧互動的基石。影片中提到「requires local LLM」，這暗示了其部署策略 6。

- **自然語言處理 (Natural Language Processing, NLP)：**理解用戶的自然語言查詢，並將其轉化為結構化的指令。
- **知識推理 (Knowledge Reasoning)：**利用其訓練知識和 ERP 數據庫的上下文，進行業務邏輯推理，例如判斷哪些材料是「Controlled」。
- **本地化部署 (Local Deployment)：**將 LLM 部署在本地伺服器或私有雲環境中，可能基於以下考量：
 - **數據隱私與安全：**半導體產業數據高度敏感，本地部署可避免數據外洩風險。
 - **性能與延遲：**減少對外部 API 的依賴，降低延遲，提升響應速度。
 - **成本效益：**長期運營成本可能更低，且可針對特定領域進行優化。

4. 自然語言轉 SQL 引擎 (NL2SQL Engine)

這是實現「Ask」功能的關鍵模組，負責將 LLM 理解的自然語言意圖轉化為可執行的數據庫查詢

- **數據庫 Schema 理解：**

- **語義描述：**透過人工編寫的語義描述，幫助 LLM 理解 ERP 數據庫中表格、欄位及其關係的業務含義 6。
- **自動生成 Schema：**自動提取數據庫的物理 Schema（表格、欄位名稱、數據類型、約束等），提供給 LLM 作為參考 6。
- **SQL 生成：**LLM 根據用戶查詢和 Schema 知識，生成符合數據庫語法的 SQL 語句。
- **SQL 驗證與優化：**可能包含一個「Critic」代理人，對生成的 SQL 進行語法檢查、語義驗證和性能評估，並提供反饋給 LLM 進行迭代優化 6。
- **SQL 執行：**將驗證後的 SQL 語句提交給 ERP 數據庫執行，並獲取結果。

5. ERP 數據庫 (ERP Database)

- **結構化數據儲存：**儲存所有半導體業務相關的結構化數據，包括訂單、材料清單、供應商資訊、庫存、生產排程等。
- **高可用性與安全性：**作為企業核心數據的載體，需具備高可用性、數據一致性和嚴格的存取控制。

6. 業務邏輯與領域知識模組 (Business Logic & Domain Knowledge Module)

- **半導體特定規則：**內建半導體產業特有的業務規則，例如材料的純度等級、儲存條件、以及影片中展示的「Controlled (受管制)」材料標籤邏輯 6。
- **工作流自動化：**定義訂單建立、複製、審批等業務流程，並與 AI 代理人協同工作。
- **合規性引擎：**根據國際出口管制法規（如瓦聖納協定、美國出口管制）和國內安全法規，自動檢查和標記敏感材料和交易 6。

7. 工具整合 (Tool Integration)

AI 代理人能夠調用一系列預定義的「工具」來執行任務 6。在 resic AI 中，這些工具可能包括：

- **數據庫操作工具：**執行 SQL 查詢、數據插入、更新等。
- **業務功能 API：**調用 ERP 系統內部的各種業務功能，如建立訂單、更新材料狀態、發送通知等。
- **外部系統接口：**未來可能整合外部供應商系統、物流平台等。

8. 人機協作與安全機制 (Human-in-the-Loop & Safety)

- **意圖澄清：**在執行複雜或模糊的指令前，系統可能要求用戶澄清意圖，確保 AI 理解正確 6。
- **操作確認：**對於關鍵業務操作（如提交訂單），可能需要用戶最終確認，以防止 AI 誤操作。

- **審計日誌 (Audit Log)**: 記録所有ユーザー操作と AI 代理人の決策過程，便於追溯和監管。

結論

resic AI の技術架構是一個典型的領域特定 AI 代理人系統，它巧妙地結合了 LLM の自然語言理解能力、NL2SQL 引擎的數據庫互動能力，以及半導體產業的深度業務知識。這種架構使得 ERP 系統從傳統的數據管理工具，轉變為一個能夠理解、推理並協助用戶完成複雜業務任務的智慧夥伴，尤其在處理半導體產業高度專業化和嚴格合規性的需求時，展現出其獨特的價值。

參考文獻

- [6] SEMI. Agentic AI For Next-Generation Semiconductor Manufacturing.
- [6] AWS Machine Learning Blog. (2025, April 24). Enterprise-grade natural language to SQL generation using LLMs: Balancing accuracy, latency, and scale.
- [6] arXiv. (2025, July 31). Chatting with your ERP: A Recipe.
- [6] IBM. What Are AI Agents?.
- [6] 影片內容分析 (resic AI - Semiconductor ERP Agent, YouTube: <https://youtu.be/cGsUv4r85Fo?si=56yZ4vkUxqgg8yVz>)

resic AI 半導體 ERP Agent 技術アーキテクチャ分析

はじめに

映像で示された **resic AI - Semiconductor ERP Agent** システムは、企業資源計画（ERP）分野と人工知能（AI）の深い統合を示す最新動向を代表しています。本システムは従来のERPの受動的なデータ管理モデルを越え、対話的で知的な「エージェント」へと変革しています。本報告では、resic AI が採用していると考えられる技術アーキテクチャを詳細に分析し、特に大規模言語モデル（LLM）と半導体産業特有の業務ロジックの統合方法に焦点を当てます。

コアコンセプト：AI Agentic Architecture

resic AI の中核は **AI Agentic Architecture**（AI エージェントアーキテクチャ）66 にあります。このアーキテクチャは、複雑な指示の理解、タスクの計画、ツールの利用および行動の実行を通じてユーザーの目的を達成する能力をシステムに付与します。従来のERPにおけるデータベースと業務プロセスを、AIエージェントが操作可能な「ツール」および「ナレッジベース」へと変換します。

技術アーキテクチャの構成要素

resic AI の技術アーキテクチャは以下の主要モジュールに分割できます。

1. ユーザーインターフェース (User Interface, UI)

- **ウェブアプリケーション**: 映像ではモダンなウェブアプリケーションインターフェースが示されており、直感的なダッシュボード、表形式ビュー、およびフォームを通じてデータ表示とユーザー入力を提供します。
- **対話型入力**: 特に「Ask」機能は、自然言語入力ボックスを備え、ユーザーとAIエージェントの主要なインタラクション入口となります。

2. AI エージェントコア (AI Agent Core / Orchestrator)

システム全体の「脳」に相当し、ユーザー要求に応答するために各モジュールを調整します ⁶。

- **意図理解 (Intent Understanding)**: ユーザーの自然言語入力を受け取り、その背後にある業務的意図（例: 「注文を照会する」、「部材を作成する」）を解析します。
- **タスク計画 (Task Planning)**: ユーザーの意図に基づき、複雑なタスクを実行可能なサブタスクに分解し、どの内部ツールや機能呼び出すべきかを決定します。
- **コンテキスト管理 (Context Management)**: 対話状態および業務コンテキストを維持し、連続する指示を理解して一貫した応答を提供できるようにします。

3. 大規模言語モデル (Large Language Model, LLM)

LLM は resic AI の知的インタラクションの基盤です。映像内の「requires local LLM」という言及は、そのデプロイ戦略を示唆しています ⁶。

- **自然言語処理 (Natural Language Processing, NLP)**: ユーザーの自然言語クエリを理解し、それを構造化された指示へ変換します。
- **知識に基づく推論 (Knowledge Reasoning)**: トレーニング済みの知識とERPデータベースのコンテキストを活用して業務ロジックの推論を行い、例えばどの部材が「Controlled」であるかを判断します。
- **ローカル展開 (Local Deployment)**: LLM をオンプレミスもしくはプライベートクラウド上に展開することには以下の利点が考えられます:
 - **データプライバシーとセキュリティ**: 半導体産業のデータは高度に機密であるため、ローカル展開によりデータ漏洩リスクを低減できます。
 - **性能とレイテンシ**: 外部APIへの依存を減らし、レイテンシを低減して応答速度を向上させられます。

- **コスト効率**：長期運用コストが低くなる可能性があり、特定ドメイン向けに最適化が可能です。

4. 自然言語→SQL エンジン (NL2SQL Engine)

「Ask」機能を実現するための主要モジュールであり、LLM によって理解された自然言語の意図を実行可能なデータベースクエリへと変換します 6 6。

- **データベーススキーマの理解**：
 - **セマンティック記述**：手作業で作成されたセマンティックな記述を通じて、LLM がERP データベース内のテーブル、カラム、およびそれらの関係の業務的意味を理解できるよう支援します 6。
 - **スキーマの自動抽出**：テーブル、カラム名、データ型、制約など、データベースの物理スキーマを自動抽出してLLMに参照情報として提供します 6。
- **SQL生成**：LLM はユーザークエリとスキーマ知識に基づき、データベース構文に適合したSQL文を生成します。
- **SQL検証と最適化**：生成されたSQLに対して文法チェック、意味検証、性能評価を行う「Critic」代理（代理人）を含み、LLM にフィードバックを与えて反復的に最適化する可能性があります 6。
- **SQL実行**：検証済みのSQL文をERPデータベースに送信して実行し、結果を取得します。

5. ERP データベース (ERP Database)

- **構造化データの格納**：受注、部品表、サプライヤ情報、在庫、生産スケジュールなど、半導体ビジネスに関連する全ての構造化データを格納します。
- **高可用性とセキュリティ**：企業の中核データを保持するため、高可用性、データ整合性、および厳格なアクセス制御が求められます。

6. 業務ロジックとドメイン知識モジュール (Business Logic & Domain Knowledge Module)

- **半導体特有のルール**：材料の純度等級や保管条件、映像で示された「Controlled（受管制）」材料ラベルのロジックなど、半導体業界特有の業務ルールを組み込みます 6。
- **ワークフロー自動化**：受注の作成、複製、承認などの業務プロセスを定義し、AIエージェントと連携して実行します。
- **コンプライアンスエンジン**：ワッセナー協定（Wassenaar Arrangement）や米国の輸出管理規制等の国際的輸出管理法規や国内の安全法規に基づき、敏感な材料や取引を自動的にチェックしてマークします 6。

7. ツール統合 (Tool Integration)

AIエージェントは一連の定義済み「ツール」を呼び出してタスクを実行できます ⁶。resic AI におけるこれらのツールには次が含まれる可能性があります：

- **データベース操作ツール**：SQLクエリの実行、データの挿入、更新など。
- **業務機能API**：受注作成、部材ステータス更新、通知送信など、ERP内部の各種業務機能を呼び出すAPI。
- **外部システムインターフェース**：将来的には外部サプライヤシステム、物流プラットフォーム等との統合を行う可能性があります。

8. 人間の介入と安全機構 (Human-in-the-Loop & Safety)

- **意図の明確化**：複雑または曖昧な指示を実行する前に、システムはユーザーに意図の明確化を求め、AIの理解が正確であることを確保する可能性があります ⁶。
- **操作確認**：受注の確定など重要な業務操作については、AIの誤操作を防ぐためにユーザーの最終確認を要求する場合があります。
- **監査ログ (Audit Log)**：すべてのユーザー操作とAIエージェントの意思決定プロセスを記録し、追跡および規制対応を容易にします。

結論

resic AI の技術アーキテクチャは、典型的な「ドメイン特化型AIエージェントシステム」といえます。これは、LLM の自然言語理解能力、NL2SQL エンジンによるデータベース相互作用能力、および半導体産業に関する深い業務知識を巧みに組み合わせています。本アーキテクチャにより、ERP システムは従来の単なるデータ管理ツールから、複雑な業務タスクを理解し推論しユーザーの支援を行う知的な協働者へと進化します。特に半導体産業の高度に専門化され、厳格なコンプライアンス要件に対応する場面で、その独自の価値が発揮されます。

参考文献

- [6] SEMI. Agentic AI For Next-Generation Semiconductor Manufacturing.
<https://www.semi.org/en/event/agentic-ai-next-generation-semiconductor-manufacturing>
- [6] AWS Machine Learning Blog. (2025, April 24). Enterprise-grade natural language to SQL generation using LLMs: Balancing accuracy, latency, and scale.
<https://aws.amazon.com/blogs/machine-learning/enterprise-grade-natural-language-to-sql-generation-using-llms-balancing-accuracy-latency-and-scale/>
- [6] arXiv. (2025, July 31). Chatting with your ERP: A Recipe.
<https://arxiv.org/html/2507.23429v1>
- [6] IBM. What Are AI Agents?. <https://www.ibm.com/think/topics/ai-agents>
- [6] 映像コンテンツ分析 (resic AI - Semiconductor ERP Agent, YouTube):
<https://youtu.be/cGsUv4r85Fo?si=56yZ4vkUxqgg8yVz>
-

resic AI 반도체 ERP 에이전트 기술 아키텍처 분석

서론

영상에서 소개된 **resic AI - Semiconductor ERP Agent** 시스템은 기업자원관리(ERP) 분야와 인공지능(AI)의 심층적 결합을 보여주는 최신 동향을 대표합니다. 이 시스템은 전통적인 ERP의 수동적 데이터 관리 방식을 넘어, 지능화되고 대화형 상호작용이 가능한 '에이전트'로 전환됩니다. 본 보고서는 resic AI가 사용할 수 있는 기술 아키텍처를 심층적으로 분석하며, 특히 대규모 언어 모델(LLM)과 반도체 산업의 특정 비즈니스 로직을 어떻게 통합하는지에 중점을 둡니다.

핵심 개념: AI 에이전트 아키텍처

resic AI의 핵심은 **AI 에이전트 아키텍처 (AI Agentic Architecture)** 6 6 입니다. 이 아키텍처는 시스템이 복잡한 명령을 이해하고, 작업을 계획하며, 도구를 활용하고 행동을 실행하여 사용자 목표를 달성할 수 있도록 합니다. 전통적 ERP의 데이터베이스와 비즈니스 프로세스를 AI 에이전트가 조작할 수 있는 '도구'와 '지식 베이스'로 전환합니다.

기술 아키텍처 구성

resic AI의 기술 아키텍처는 다음의 주요 모듈로 구분됩니다.

1. 사용자 인터페이스 (User Interface, UI)

- 웹 애플리케이션:** 영상에서는 직관적인 대시보드, 테이블 뷰 및 폼을 제공하는 현대적 웹 애플리케이션 인터페이스가 시연되었습니다. 데이터 표시 및 사용자 입력에 사용됩니다.
- 대화형 입력:** 특히 'Ask' 기능은 자연어 입력창을 제공하며, 사용자가 AI 에이전트와 상호작용하는 주요 진입점입니다.

2. AI 에이전트 코어 (AI Agent Core / Orchestrator)

전체 시스템의 '두뇌'로, 사용자 요청에 응답하기 위해 각 모듈을 조율합니다 6.

- 의도 이해 (Intent Understanding):** 사용자의 자연어 입력을 수신하여 그 이면의 비즈니스 의도를 분석합니다(예: '주문 조회', '자재 생성').
- 작업 계획 (Task Planning):** 사용자 의도에 따라 복잡한 작업을 실행 가능한 하위 작업으로 분해하고, 어떤 내부 도구나 기능을 호출해야 할지를 결정합니다.
- 컨텍스트 관리 (Context Management):** 대화 상태와 비즈니스 컨텍스트를 유지하여 에이전트가 연속적인 명령을 이해하고 일관된 응답을 제공할 수 있도록 합니다.

3. 대규모 언어 모델 (Large Language Model, LLM)

LLM은 resic AI의 지능형 상호작용의 기반입니다. 영상에서는 'requires local LLM'이라는 언급이 있어 배치 전략을 시사합니다 6 .

- **자연어 처리 (Natural Language Processing, NLP):** 사용자의 자연어 질의를 이해하고 이를 구조화된 명령으로 변환합니다.
- **지식 추론 (Knowledge Reasoning):** 학습된 지식과 ERP 데이터베이스의 컨텍스트를 활용하여 비즈니스 로직을 추론합니다. 예를 들어 어떤 자재가 '규제 대상(Controlled)'인지 판단합니다.
- **로컬 배포 (Local Deployment):** LLM을 로컬 서버나 프라이빗 클라우드에 배포하는 것에는 다음과 같은 고려사항이 있습니다:
 - **데이터 프라이버시 및 보안:** 반도체 산업 데이터는 매우 민감하므로 로컬 배포는 데이터 유출 위험을 낮출 수 있습니다.
 - **성능 및 지연:** 외부 API 의존도를 줄여 지연을 줄이고 응답 속도를 향상시킬 수 있습니다.
 - **비용 효율성:** 장기 운영 비용 측면에서 유리할 수 있으며, 특정 도메인에 대한 최적화가 가능합니다.

4. 자연어 → SQL 엔진 (NL2SQL Engine)

'Ask' 기능을 구현하는 핵심 모듈로, LLM이 이해한 자연어 의도를 실행 가능한 데이터베이스 질의로 변환합니다 6 6 .

- **데이터베이스 스키마 이해:**
 - **의미적 설명:** 인위적으로 작성된 의미 설명을 통해 LLM이 ERP 데이터베이스의 테이블, 컬럼 및 이들 간의 관계가 갖는 비즈니스 의미를 이해하도록 돕습니다 6 .
 - **스키마 자동 생성:** 데이터베이스의 물리적 스키마(테이블, 컬럼명, 데이터 타입, 제약조건 등)를 자동으로 추출하여 LLM에 참조로 제공합니다 6 .
- **SQL 생성:** LLM은 사용자 질의와 스키마 지식을 바탕으로 데이터베이스 문법에 맞는 SQL 문을 생성합니다.
- **SQL 검증 및 최적화:** 생성된 SQL에 대해 문법 검사, 의미 검증 및 성능 평가를 수행하는 'Critic'에 이진트가 포함될 수 있으며, LLM에 피드백을 제공하여 반복적으로 최적화합니다 6 .
- **SQL 실행:** 검증된 SQL 문을 ERP 데이터베이스에 제출하여 결과를 획득합니다.

5. ERP 데이터베이스 (ERP Database)

- **구조화된 데이터 저장:** 주문, 자재 명세서(BOM), 공급업체 정보, 재고, 생산 일정 등 반도체 비즈니스 관련 모든 구조화된 데이터를 저장합니다.
- **고가용성 및 보안성:** 기업 핵심 데이터로서 높은 가용성, 데이터 일관성 및 엄격한 접근 제어를 갖추어야 합니다.

6. 비즈니스 로직 및 도메인 지식 모듈 (Business Logic & Domain Knowledge Module)

- **반도체 특유의 규칙:** 자재의 순도 등급, 보관 조건, 영상에서 시연된 'Controlled(규제 대상)' 자재 표기 로직 등 반도체 산업 특유의 비즈니스 규칙을 내장합니다 6.
- **워크플로우 자동화:** 주문 생성, 복제, 승인 등 비즈니스 프로세스를 정의하고 AI 에이전트와 협업합니다.
- **컴플라이언스 엔진:** Wassenaar Arrangement(와센나 협정), 미국 수출관리 규정 등 국제 수출 규제 및 국내 보안 규정을 기반으로 민감 자재와 거래를 자동으로 검사하고 표시합니다 6.

7. 도구 통합 (Tool Integration)

AI 에이전트는 일련의 사전정의된 '도구'를 호출하여 작업을 수행할 수 있습니다 6. resic AI에서는 다음과 같은 도구들이 포함될 가능성이 있습니다:

- **데이터베이스 조작 도구:** SQL 쿼리 실행, 데이터 삽입, 업데이트 등.
- **비즈니스 기능 API:** 주문 생성, 자재 상태 업데이트, 알림 전송 등 ERP 내부의 다양한 비즈니스 기능 호출.
- **외부 시스템 인터페이스:** 향후 공급업체 시스템, 물류 플랫폼 등 외부 시스템과의 통합 가능성.

8. 사람-기계 협업 및 안전 메커니즘 (Human-in-the-Loop & Safety)

- **의도 명확화:** 복잡하거나 모호한 명령을 실행하기 전에 시스템이 사용자에게 의도를 확인하도록 요구할 수 있어 AI의 이해를 보장합니다 6.
- **작업 확인:** 주문 제출과 같은 핵심 비즈니스 작업에 대해서는 AI의 오작동을 방지하기 위해 최종 사용자의 확인을 요구할 수 있습니다.
- **감사 로그 (Audit Log):** 모든 사용자 작업과 AI 에이전트의 의사결정 과정을 기록하여 추적 및 규제 준수를 가능하게 합니다.

결론

resic AI의 기술 아키텍처는 전형적인 영역 특화 AI 에이전트 시스템입니다. 이 아키텍처는 **LLM의 자연어 이해 능력**, **NL2SQL 엔진의 데이터베이스 상호작용 능력**, 그리고 **반도체 산업에 대한 심층적인 비즈니스 지식**을 정교하게 결합합니다. 이를 통해 ERP 시스템은 전통적인 데이터 관리 도구에서 벗어나 복잡한 비즈니스 작업을 이해하고 추론하며 사용자와 함께 수행할 수 있는 지능형 파트너로 진화하며, 특히 반도체 산업의 고도로 전문화되고 엄격한 컴플라이언스 요구를 처리할 때 그 가치를 발휘합니다.

참고문헌

[6] SEMI. Agentic AI For Next-Generation Semiconductor Manufacturing.

<https://www.semi.org/en/event/agentic-ai-next-generation-semiconductor-manufacturing>

[6] AWS Machine Learning Blog. (2025, April 24). Enterprise-grade natural language to SQL generation using LLMs: Balancing accuracy, latency, and scale.

<https://aws.amazon.com/blogs/machine-learning/enterprise-grade-natural-language-to-sql-generation-using-llms-balancing-accuracy-latency-and-scale/>

[6] arXiv. (2025, July 31). Chatting with your ERP: A Recipe.

<https://arxiv.org/html/2507.23429v1>

[6] IBM. What Are AI Agents?. <https://www.ibm.com/think/topics/ai-agents>

[6] 영상 내용 분석 (resic AI - Semiconductor ERP Agent, YouTube:

<https://youtu.be/cGsUv4r85Fo?si=56yZ4vkUxqgg8yVz>)