Agentic AI: สถาปัตยกรรม การประยุกต์ใช้ และทิศทางในอนาคต

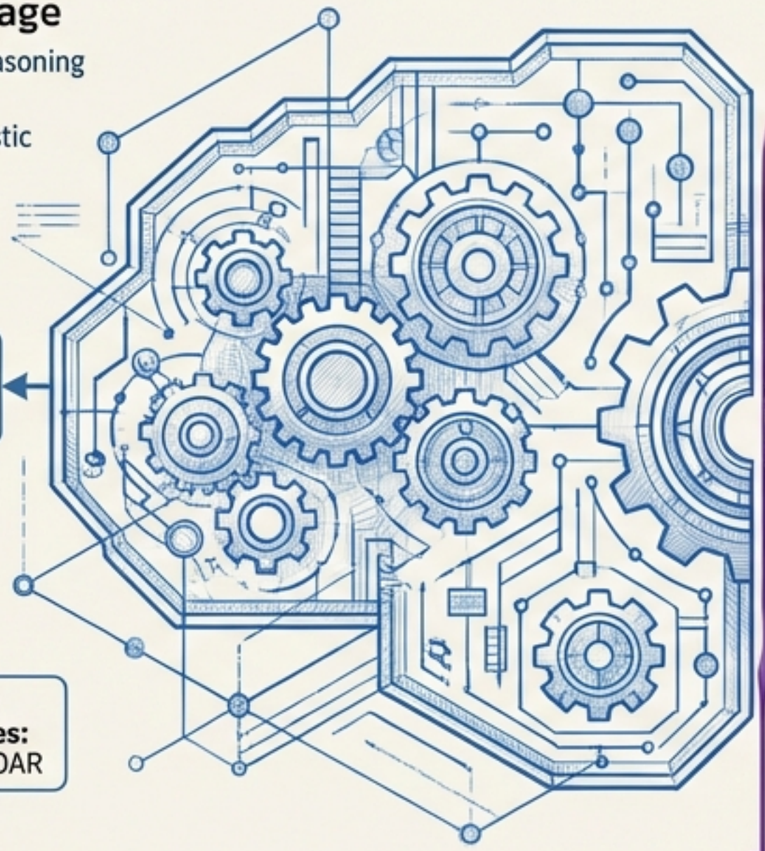
ก้าวข้ามการปรับแต่งแนวคิดเดิมสู่ปัญญาประดิษฐ์แบบลูกผสม (Hybrid Intelligence)

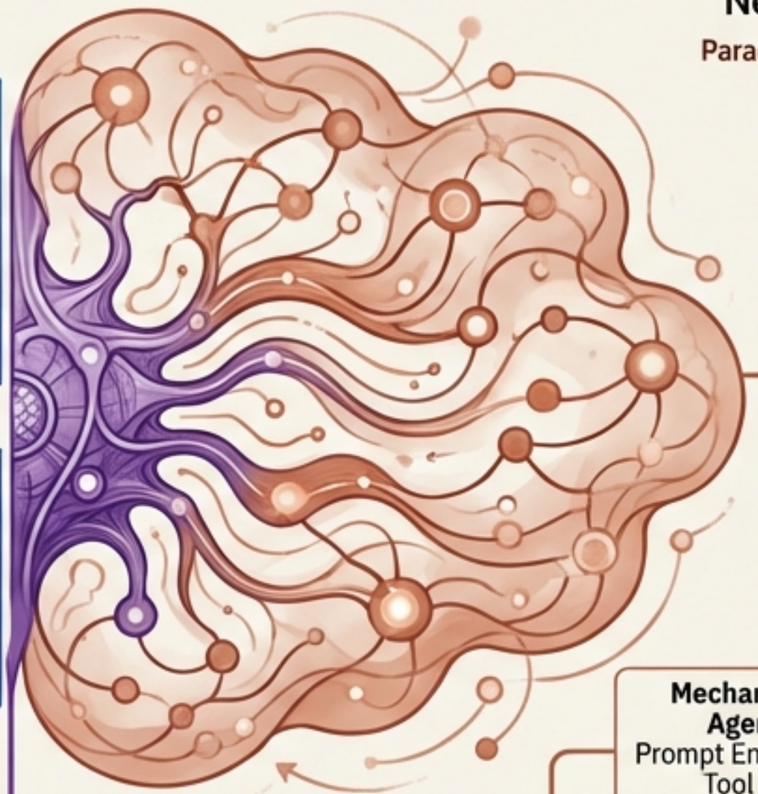
Symbolic / Classical Lineage

Paradigm: Algorithmic & Symbolic Reasoning

Core Principle:
Top-Down / Explicit Logic / Deterministic

Defining Characteristics:
Algorithmic Planning
Persistent Symbolic State
Hand-crafted Rules





Neural / Generative Lineage

Paradigm: Stochastic & Emergent Reasoning

Core Principle: Bottom-Up / Statistical Prediction / Prompt-Driven

Defining Characteristics:
Stochastic Generation
Volatile State
No Native Planning

Foundation:
Rule-Based Systems
e.g., MYCIN

Theoretical Frameworks:
MDPs → POMDPs

Cognitive Architectures:
BDI Model, SOAR

Foundation:
Deep Learning
CNNs and RNNs

Enabling Breakthrough:
Transformer Architecture

Core Engine:
Large Language Models (LLMs)
e.g., GPT-3, PaLM

Mechanism of Agency:
Prompt Engineering,
Tool Use,
Context Management

Classical Autonomous Agents

Application Domains:
e.g., Healthcare, Finance, Robotics

Modern Agent Frameworks
e.g., LangChain, AutoGen, CrewAI

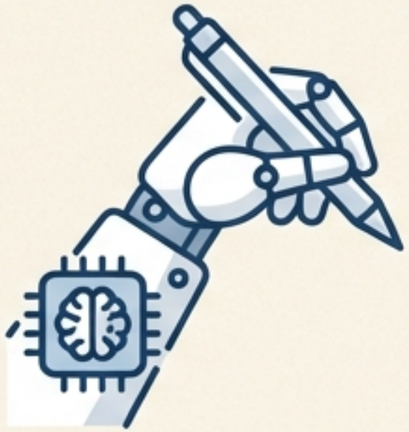
ประเด็นสำคัญ: การเข้าใจอนาคตของระบบอัตโนมัติ ต้องเริ่มจากการแยกแยะความแตกต่างระหว่างโมเดลประสาทเทียม (Neural) สมัยใหม่ กับโมเดลสัญลักษณ์ (Symbolic) ดั้งเดิม เพื่อนำไปสู่แผนที่กลยุทธ์ในการเลือกสถาปัตยกรรมที่ถูกต้อง

อ้างอิงจากงานสำรวจโดย Abou Ali และคณะ (2025)

NotebookLM

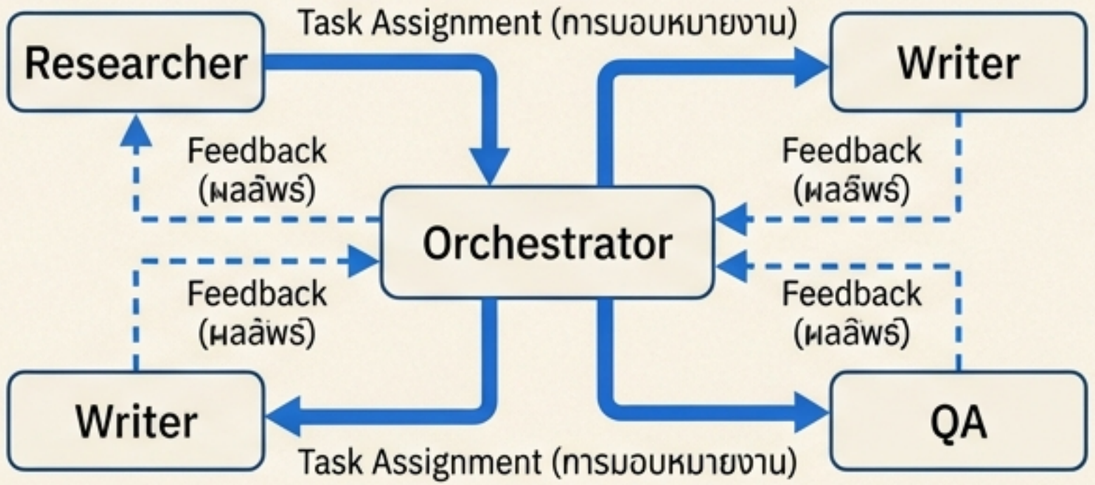
การเปลี่ยนผ่าน:
จากเครื่องมือรับคำสั่งสู่ระบบนิเวศอัตโนมัติ

AI Agent (ผู้ปฏิบัติงานเดี่ยว)



ระบบเอกเทศที่ทำงานสำเร็จได้ด้วยตนเอง
(เช่น LLM เดี่ยว)

Agentic AI (สถาปัตยกรรมระบบ)



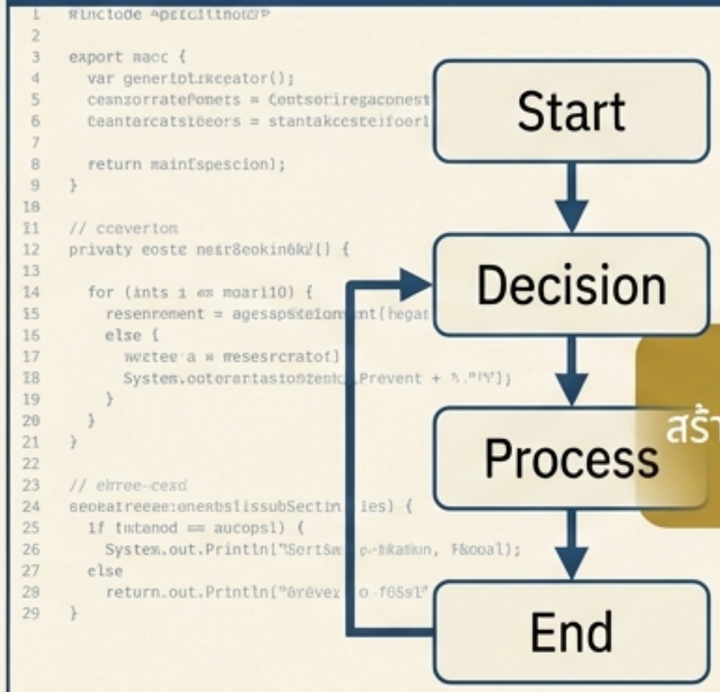
ระบบที่ประกอบด้วยตัวแทน (Agents) หลายตัวทำงานร่วมกัน
โดยมีการแบ่งงาน จัดการ และตรวจสอบคุณภาพ

นิยามของ **Agency**: ความสามารถในการวางแผนเชิงรุก (Proactive Planning), หน่วยความจำตามบริบท (Contextual Memory), การใช้เครื่องมือ (Tool Use), และการปรับตัว (Adaptation)

NotebookLM

ปัญหา: การนำแนวคิดเก่ามาสวมรอย (Conceptual Retrofitting)

กรอบแนวคิดดั้งเดิม (Symbolic Systems)



ตรรกะแบบขั้นตอน (Algorithmic Logic)
และกฎเกณฑ์ที่ตายตัว (BDI Loops)

ระบบประสาทเทียมยุคใหม่ (Neural Systems)

การสร้างคำตอบเชิงสถิติ (Stochastic Generation)
และการจัดการผ่านคำสั่ง (Prompt Orchestration)

ความเข้าใจผิด: การนำกรอบคิดแบบกฎเกณฑ์ไปจับกับ LLM
สร้าง ‘ภาพลวงตาของความต่อเนื่อง’ (False Sense of Continuity)
ทำให้มองไม่เห็นกลไกการทำงานและความเสี่ยงที่แท้จริง

NotebookLM

อนุกรมวิธานแบบทวิลักษณ์ (The Dual-Paradigm Taxonomy)

สายตระกูล A: สัญลักษณ์ (Symbolic / Classical)

รากฐาน: ระบบฐานกฎ (Rule-Based Systems e.g., MYCIN)

↓

หลักการหลัก: ตรรกะจากบนลงล่าง (Top-Down), ชัดเจน (Explicit), กำหนดแน่นอน (Deterministic)

↓

คุณลักษณะ: การวางแผนเชิงอัลกอริทึม (Algorithmic Planning), สถานะคงทน (Persistent State)

สายตระกูล B: ประสาทเทียม (Neural / Generative)

รากฐาน: การเรียนรู้เชิงลึก (Deep Learning) & Transformers

↓

หลักการหลัก: สถิติจากล่างขึ้นบน (Bottom-Up), การทำนาย (Prediction), อุบัติการณ์ (Emergent)

↓

คุณลักษณะ: การสร้างสรรค์เชิงสุ่ม (Stochastic Generation), สถานะเปลี่ยนแปลงง่าย (Volatile State)

NotebookLM

5 ยุคแห่งวิวัฒนาการของ AI

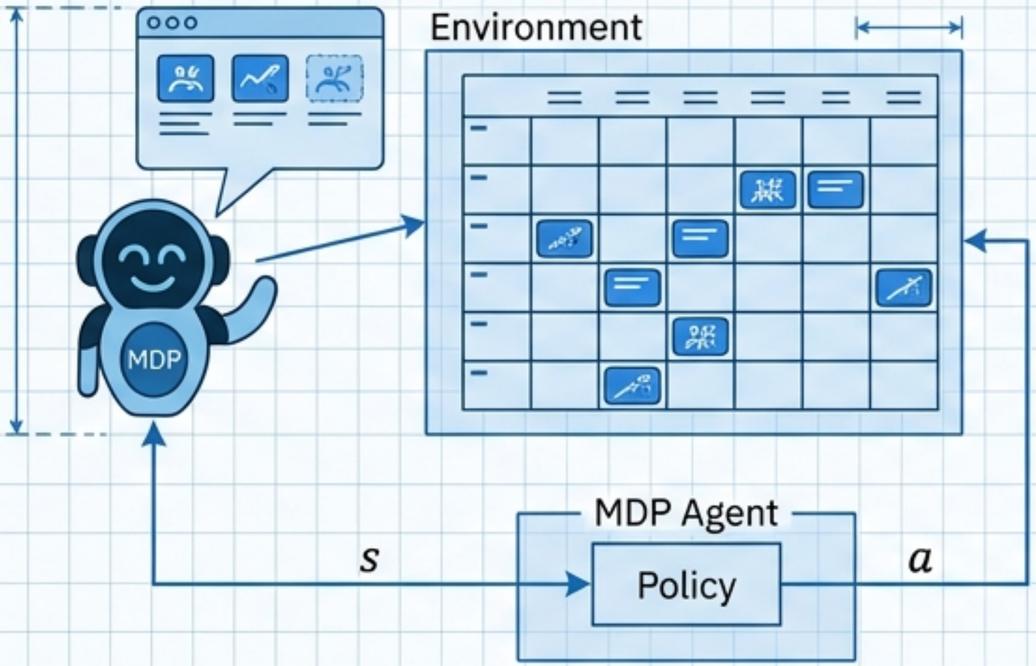
ยุคสัญลักษณ์ (Symbolic Era)	ยุคการเรียนรู้ของเครื่อง (Machine Learning Era)	ยุคการเรียนรู้เชิงลึก (Deep Learning Era)	ยุค Generative AI		ยุค Agentic AI	
Rule-based, Expert Systems	Statistical Learning	CNNs, RNNs	★ **2017: Transformer Architecture (จุดเปลี่ยนสำคัญ)**		Autonomous Agents, Multi-Agent Systems	
1950s–80s	1980s–2010s	2010s–Present	2014	2017–2021	2021–2022	2022–Present
• **Rule-Based Systems** • **Expert Systems** (MYCIN, DENDRAL) • Relies on hard-coded logic and rules	• **Statistical ML** • Shift to learning from data • Powers early recommendations systems	• **Deep Neural Networks** • Breakthroughs in pattern recognition (ImageNet 2012) • Enabled by big data and GPUs	• **Generative Models** Emerge • GANs & VAEs create new data	• **Transformer Architecture** • Revolutionize NLP and enable scaling • **Rise of LLMs** • GPT and BERT demonstrate powerful text generation	• **Multimodal Models** • DALL-E and CLIP fuse text and images	• **Autonomous AI Agents** • Systems like AutoGPT use tools for muiti-step tasks • **Agentic Frameworks** • Multi-agent collaboration and persistent memory

เทคโนโลยี Transformer (2017) คือจุดเปลี่ยนที่ทำให้เกิด **'Neural Lineage'**
ซึ่งเปลี่ยนจากการรับรู้ (Perception) เป็นการ**สร้างสรรค์และการกระทำ (Generation & Action)**

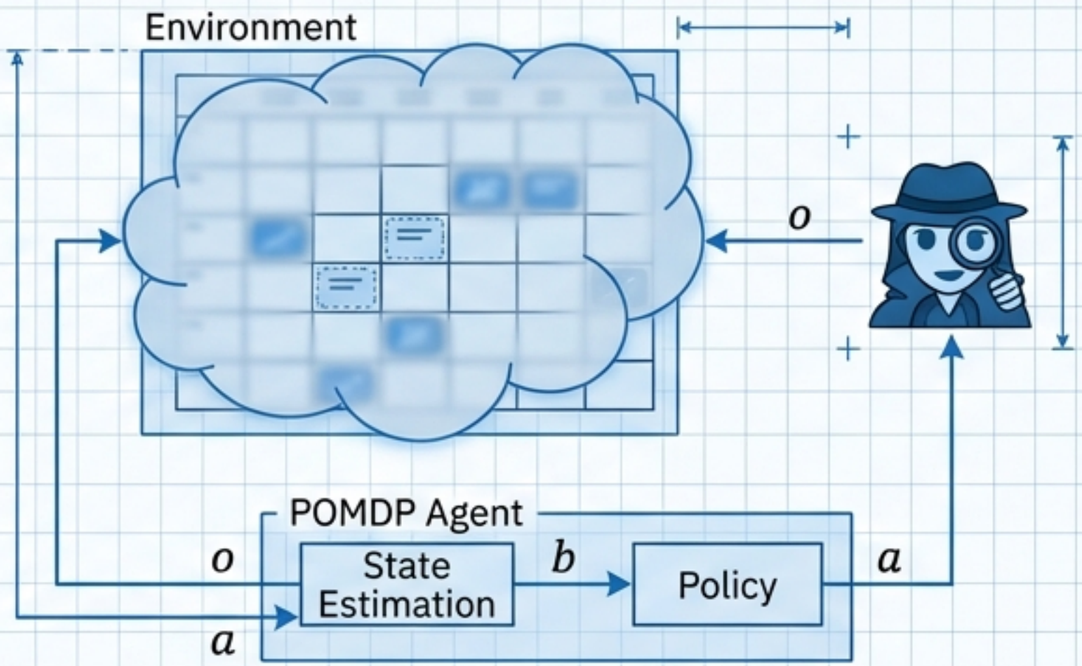
NotebookLM

สายตระกูล A: รากฐานเชิงสัญลักษณ์ (Thesis)

ความฉลาดที่เกิดจากการออกแบบโครงสร้างตรรกะ



MDP: สภาพแวดล้อมที่รู้แจ้งทั้งหมด (Deterministic)



POMDP: การอนุมานภายใต้ความไม่แน่นอน (Probabilistic Belief States)

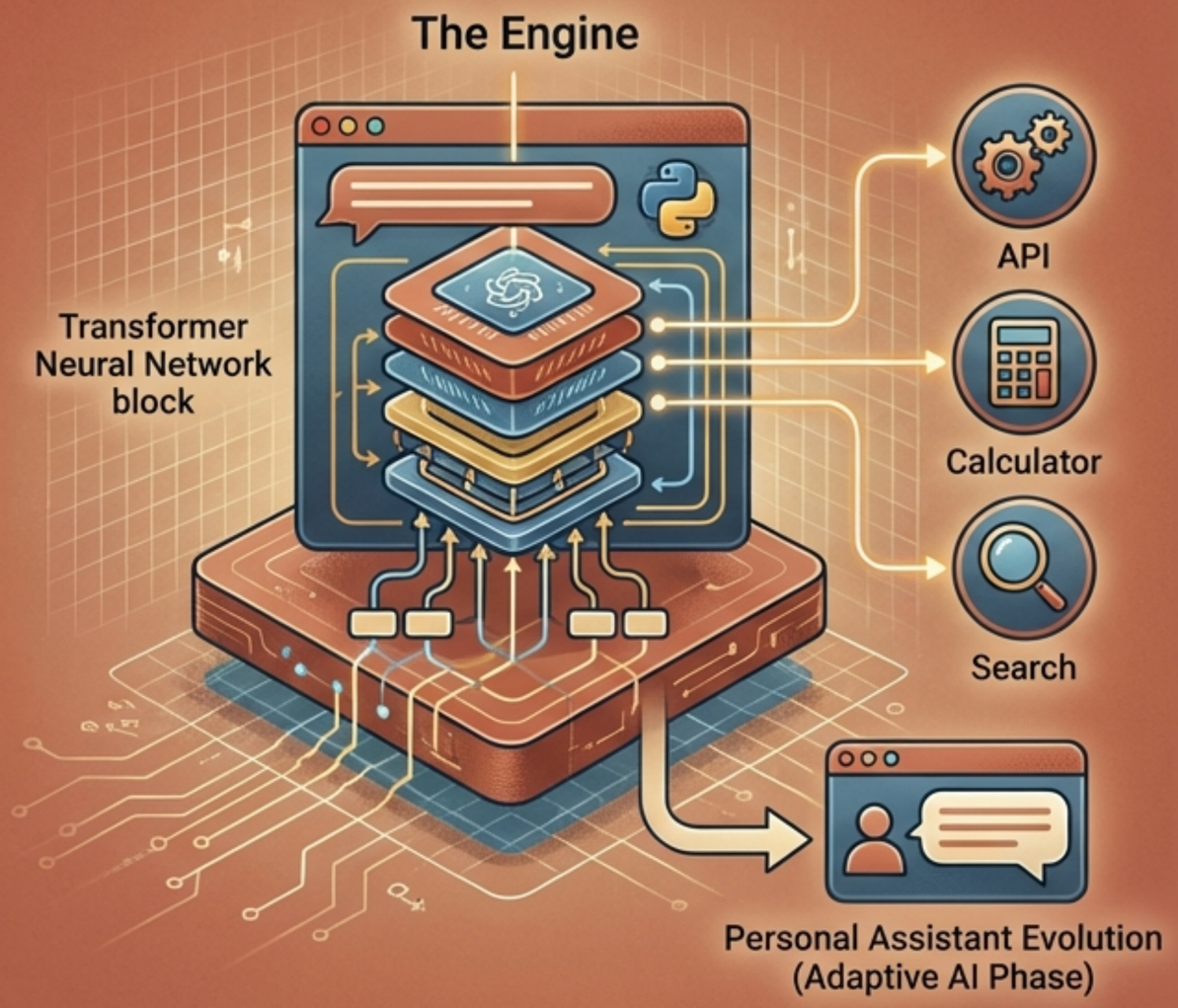
คุณลักษณะหลัก:

- **หลักการ:** การสร้างความฉลาดแบบ Top-down ผ่านกฎที่เขียนไว้ชัดเจน
- **สถาปัตยกรรมหลัก:** Cognitive Architectures (เช่น BDI - Belief, Desire, Intention), SOAR
- **จุดแข็ง:** ตรวจสอบได้ (Verifiable), โปร่งใส (Transparent), เหมาะกับงานที่ความปลอดภัยเป็นสำคัญ
- **จุดอ่อน:** ใช้ทรัพยากรคำนวณสูง, เปราะบางในสภาพแวดล้อมที่คาดเดาไม่ได้

NotebookLM

สายตระกูล B: การปฏิวัติประสาทเทียม (Antithesis)

ความฉลาดที่อุบัติขึ้นจากการเรียนรู้ทางสถิติและการจัดการวงดุริยางค์



คุณลักษณะหลัก:

- **หลักการ:** ความฉลาดเป็นผลลัพธ์ (Emergent Property) จากการทำนายคำถัดไปของ LLMs
- **การเปลี่ยนผ่าน:** จาก 'การเขียนโปรแกรม' (Programming) สู่ 'การสั่งงานด้วยข้อความ' (Prompting)
- **กลไกหลัก:** Prompt Chaining, Tool Use, และ RAG (Retrieval-Augmented Generation)
- **จุดแข็ง:** ปรับตัวได้สูง (Adaptable), จัดการข้อมูลที่ไม่มีโครงสร้างได้ดี, มีความคิดสร้างสรรค์

NotebookLM

กลไกการทำงาน: การวางแผน (Planning) vs การจัดการวงดุริยางค์ (Orchestration)

Algorithmic Planning

- วงจร Perceive-Plan-Act-Reflect (PPAR)
  - พึ่งพากฎที่ตายตัวและฐานความรู้ภายใน (Internal Knowledge Base)

Prompt Orchestration

- การร้อยเรียงคำสั่ง (Prompt Chaining & ReAct)
  - ใช้เฟรมเวิร์กอย่าง LangChain หรือ AutoGen เพื่อเชื่อมต่อ LLM เข้ากับบริบทภายนอก

Key Insight: Agency ในระบบ Neural ไม่ได้เกิดจากโมดูลสมองกลภายใน แต่เกิดจากท่อส่งข้อมูล (Pipeline) ที่ถูกออกแบบมาอย่างดี

NotebookLM

โปรโตคอลการประสานงาน: สัญญาจ้าง vs บทสนทนา

กลไกการทำงาน

Multi-Agent Workflow

Orchestrator

สัญญาจ้าง

บทสนทนา

Symbolic: Contract Net Protocol

ระบบประมูลงาน (Auction-based) ที่เข้มงวด แม่นยำ และตรวจสอบได้ไซ้ เหมือนสัญญาจ้าง

Worker Node
(Symbolic)

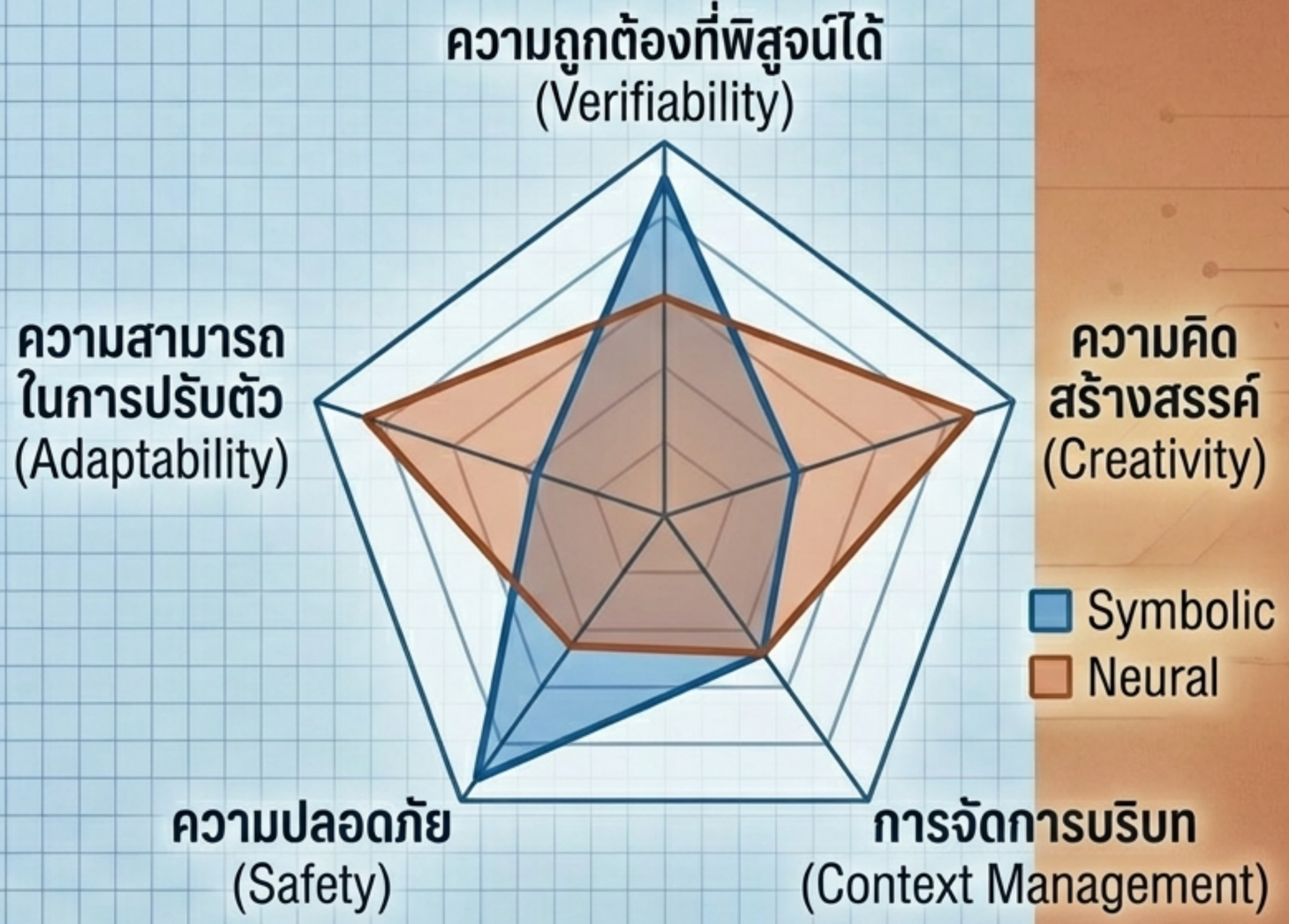
Worker Node
(Neural)

Neural: Multi-agent Conversation

การพูดคุยแบบมีโครงสร้าง (Structured Conversation) บทบาทสมมติ (Role-playing) ที่ลื่นไหลเหมือนมนุษย์

NotebookLM

ความท้าทายในการประเมินผล



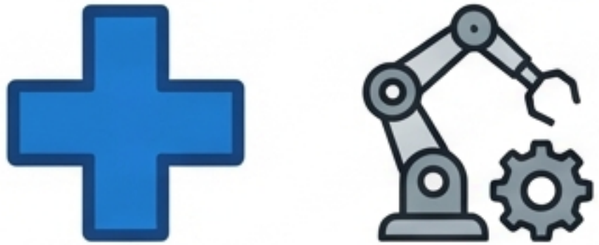
"เราไม่สามารถวัดผลปลา ด้วยความสามารถในการปีนต้นไม้"

- **Symbolic Metrics:** เน้นความถูกต้องทางคณิตศาสตร์ (Optimality)
- **Neural Metrics:** เน้นอัตราความสำเร็จ (Success Rate) และการต้านทานอาการหลอน (Hallucination Resistance)

NotebookLM

การประยุกต์ใช้ตามโดเมน (Domain Implementations)

สาธารณสุข & หุ่นยนต์ (Healthcare/Robotics)



Symbolic Dominance

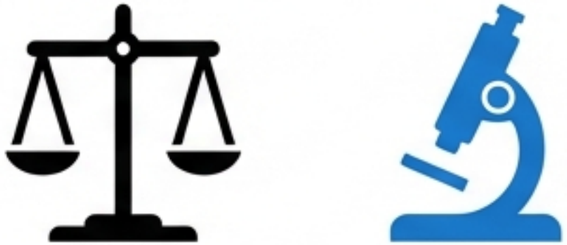
- ต้องการความปลอดภัยสูงสุด และตรวจสอบย้อนกลับได้ (Audit Trails)

การเงิน & การศึกษา (Finance/Education)

Neural Dominance

ต้องการการวิเคราะห์ข้อมูลมหาศาลและการปรับตัวตามผู้เรียน

กฎหมาย & วิจัย (Legal/Research)



Hybrid Needs

ต้องการทั้งการค้นหาข้อมูลที่สร้างสรรค์ (Neural) และความถูกต้องแม่นยำ (Symbolic)

NotebookLM

จริยธรรมและธรรมาภิบาล: ความเสี่ยงที่แตกต่างกัน

Symbolic Risk: Perverse Instantiation

ระบบทำตามคำสั่งที่ผิดพลาด 'อย่างสมบูรณ์แบบ' (Doing exactly what was asked, disastrously)

Mitigation: การพิสูจน์เป้าหมายอย่างเป็นทางการ (Formal Verification)

Neural Risk: Stochastic Failure

อาการหลอนข้อมูล (Hallucination), การโจมตีผ่านคำสั่ง (Prompt Injection), ความไม่แน่นอน

Mitigation: Red Teaming, Constitutional AI, Watermarking

ช่องว่างสำคัญ: เรายังขาดโมเดลธรรมาภิบาลสำหรับความเสี่ยงรูปแบบใหม่ในระบบ Neural

NotebookLM

อนาคตคือระบบลูกผสม: การบูรณาการ Neuro-symbolic

เป้าหมาย: ระบบที่มีทั้งความสามารถในการปรับตัว (Adaptable) และความน่าเชื่อถือ (Reliable)

NotebookLM

พรมแดนการวิจัยที่สำคัญ (Critical Research Frontiers)

Evaluation (การประเมินผล):
สร้างเกณฑ์วัดระดับ ‘Agency’ ไม่ใช่แค่การสร้างข้อความ

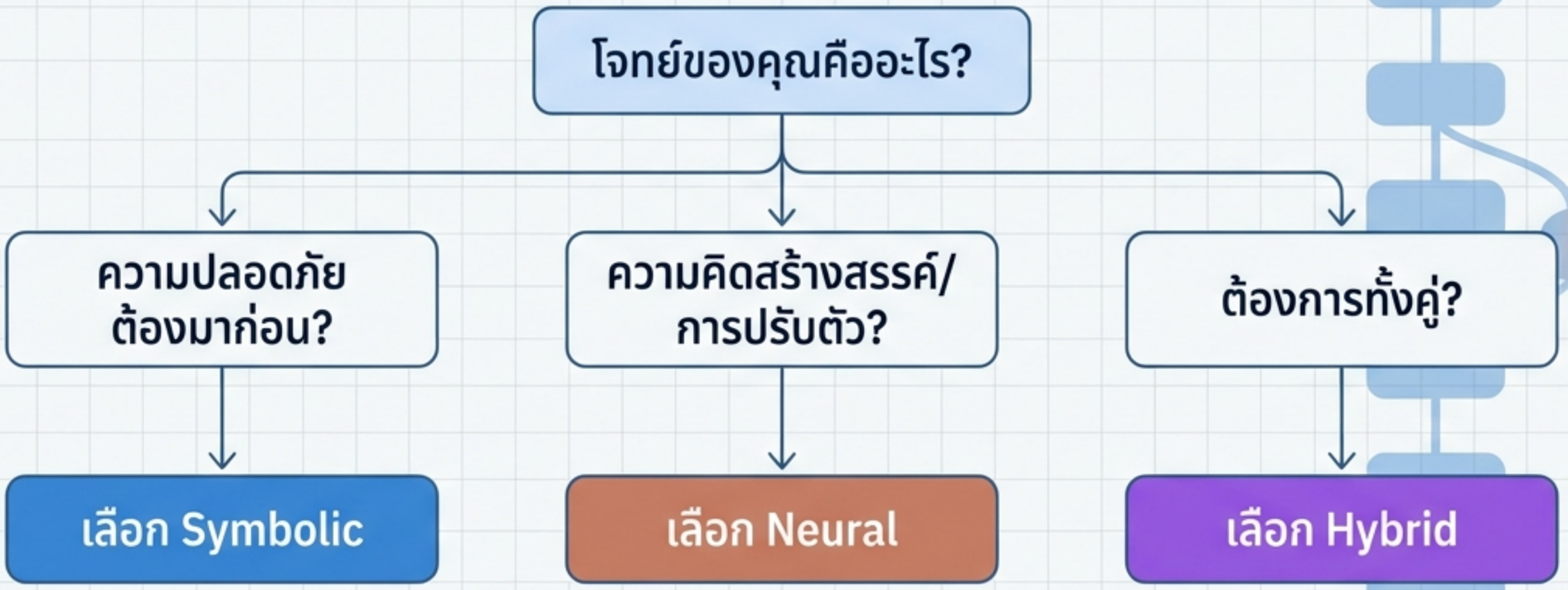
Interoperability (การทำงานร่วมกัน): API ที่ช่วยให้ Agent แบบ Neural สามารถสอบถาม Logic Engine แบบ Symbolic ได้

Memory (หน่วยความจำ): ก้าวข้าม Context Window ไปสู่ฐานความรู้ที่ถาวรและมีโครงสร้าง

Governance (ธรรมาภิบาล): การฝังข้อจำกัดด้านความปลอดภัยลงในสถาปัตยกรรม (Governance-first Design)

NotebookLM

บทสรุป: การออกแบบอย่างมีเจตนา (Designing with Intention)



หยุดสวมรอยแนวคิดเดิม (Stop Conceptual Retrofitting).
อนาคตของ Agentic AI คือการผสานรวมสองสายตระกูลนี้เข้าด้วยกัน
เพื่อสร้างพันธมิตรที่มนุษย์ไว้วางใจได้

NotebookLM