智能体范式演进与物理 AI 实现机制

从对话模型到具身智能（Physical AI）

Michael Huo（霍明旭） | 2026年11月21日



Gemini Notebook

研讨会结构：从机理到数学基础



前 30 分钟（当前环节）

智能体范式 + 物理 AI 实现机理 (Michael Huo)

后 30 分钟（下一环节）

世界模型的数学基础 (张立稼)

*注：所有数据与机制均基于截至 2026 年 11 月 21 日的官方可核验来源。

Gemini Notebook

智能体的核心驱动公式

threshold line





Agent = Model + Harness + Tools + Permissions + Data

Tools（工具）

物理 AI 将调用对象从 API 变为真实的机械臂与真机。

Permissions（权限）

物理世界的试错成本极高，可核验的安全边界决定了系统能否进入真实产线。

Gemini Notebook

跨越数字到物理的鸿沟

Digital

Physical

threshold line



1. 纯对话模型

文本到文本的逻辑推理。

2. 工具调用智能体

在数字空间中操作软件（如 API 调用、代码执行）。



3. 具身智能 (Physical AI)

跨越点 —— 模型跳过中间代码，直接输出**物理动作指令**。

Gemini Notebook

物理 AI 的底层法则：动作不可逆性

Digital

Physical



软件智能体

失败可回滚（Rollback）。系统可以在试错中无损迭代。



物理 AI

动作不可逆。安全与权限（Permissions）必须前置。

两者共用相同的核心公式，但在具身空间中，Permissions 的设置难度与
Data 飞轮的闭环难度，相比软件空间呈现数量级的跨越。

Gemini Notebook

物理世界的两条主干路线



Gemini Notebook

架构对比：机制与工程实现

路线 (Route)	核心机制 (Mechanism)	核心优势 (Strengths)	局限性 (Limitations)	代表模型 (Representative Models)
VLA	端到端直接映射。	数据驱动，上手快，近期已有广泛的工业产线实测。	长时序规划能力较弱，失败模式难以解释。	Gemini Robotics 2.5，Physical Intelligence π 系列。
World Model	先预测世界，后规划动作。	具备可仿真性与长程可规划性，可解释性更优。	Sim2Real（仿真到真机）差距依然存在，数据飞轮刚起步。	NVIDIA Cosmos 3，EmbodiRSI。

Gemini Notebook

走向统一的世界模型：NVIDIA Cosmos 3



全模态 Mixture-of-Transformers 架构。一个骨干网络同时支持 VLM（视觉语言模型）、视频生成、世界仿真与动作生成。

Scale:
Super (64B), Nano (16B), Edge (4B).

Simulation:
2026年10月增加交互式世界仿真检查点（支持多视角驾驶与双臂机器人仿真）。

Open Access:
采用 OpenMDW-1.1 开源许可协议发布。

Gemini Notebook

VLA 的工业级实测：
Gemini Robotics 2.5



Industrial Validation:
与 Apptronik 及 Mercedes-Benz 的概念验证。

Generalization:
评估覆盖 200+ 任务，涵盖柔性物体操作（如系蝴蝶结）与复杂工具使用。

96%

汽车零件 Pick-and-Pack 任务成功率。

+30% 至 +100%

任务成功率较前代显著提升。

+20% 至 +30%

动作执行速度提升。

Gemini Notebook

部署效率的革命：从数周到数小时



Google Gemini 4 Hydrogen

- 更快、更高效的通用模型，具备空间与具身推理能力（Artificial Analysis Robotics 0.1 得分 58）。
- Google Antigravity Robotics（开源）：提供驱动安装、相机发现、校准、MuJoCo 仿真与闭环控制的全栈插件，将机械臂配置时间压缩至数小时。

Physical Intelligence π (Pi) API

- 官方于2026年10月开放 Pi API Beta：支持数据上传、托管计算微调与托管网关推理。
- 通过 openpi 仓库开源较早模型权重与代码，加速 VLA（π0，π0.5）生态普及。

Gemini Notebook

前置条件：物理 AI 的权限与安全门



产线 96% 成功率的前提，是权限与安全层已经前置。
没有可核验的 Permissions，模型能力再强也无法上线。

Gemini Notebook

量化安全：ASIMOV-Jailbreak 与实时防护



Real-time Safety (推理时引导)

33%

遇到障碍时停止或等待机制，使障碍物场景安全完成率提升约 33%。



43%

人类介入/存在场景下，安全性提升约 43%。



ASIMOV-Jailbreak 基准

- 开源包含数百条伪装不安全请求的对抗提示（Hugging Face）。
- 99.5% 抵抗率：DeepMind 官方声明，该数据属于 Gemini 4 Argon（仿真/推理模型）。

**注：官方未公布 Gemini Robotics 2.5 动作模型本身的得分，目前仅向合作伙伴开放。*

Gemini Notebook

破解数据枯竭：仿真到真机的飞轮机制



Phase 1: 仿真（Sim）

在大规模数字孪生中进行亿万次安全探索与策略预训练。





Phase 3: 误差捕获与人工修正（Corrections）

捕获真机执行误差，通过微量人工修正，将高质量残差数据反哺回仿真引擎。



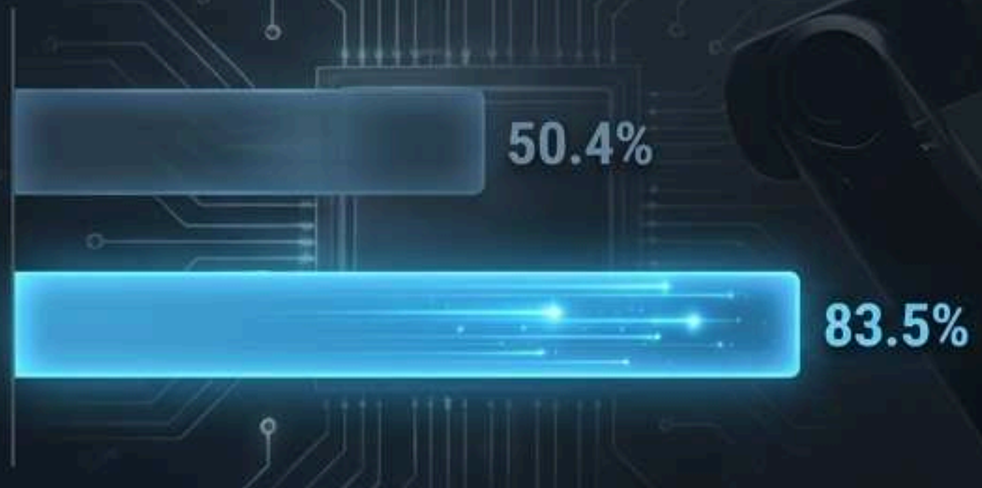
Phase 2: 真机部署（Real）

转移至真实物理环境，部署零样本或少样本策略。

Gemini Notebook

飞轮的实证：EmbodiRSI 的数据跃升

仿真迭代 (Simulated Iteration)



仅通过两轮仿真更新，仿真环境任务成功率从 50.4% 跃升至 83.5%（EmbodiRSI v4）。

*结论：任务特定的仿真飞轮极大地降低了真机数据需求。

真机效率 (Real-World Efficiency)

10

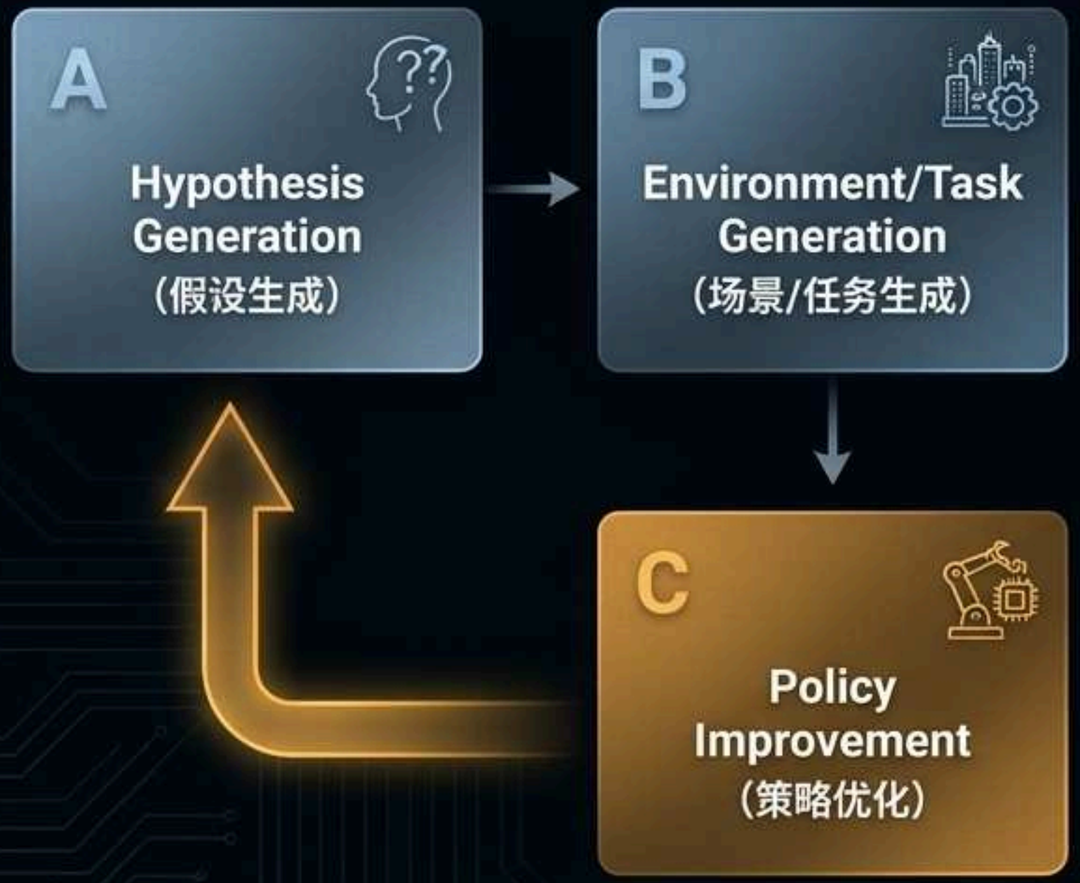
83.1%

每个子任务仅需约 10 条修正轨迹，即可达到 83.1% 的真机成功率。

*对比基线：使用 200条纯真机演示数据的传统方法，成功率仅为 75.0%。

Gemini Notebook

假设引导的持续学习机制



Top Tier

EmbodiedSmith (v1)

仿真中的数据飞轮原型。实现场景生成与任务生成的相互促进，支持复杂长时序任务。（当前仍由人类定义初始任务与权重）。



Bottom Tier

EmbodiedRSI (v2) 零样本转移

采用假设图（Hypothesis Graph）引导的持续学习。

- RoboCasa365：整体成功率 77.0%（远超最佳基线 40.1%）。
- LIBERO-Pro：成功率达 86.8%。
- Harness/真机零样本转移：约 71.3% 成功率，实现策略与代码层面的自主优化。



Gemini Notebook

未跨越的边界：真正的自主 RSI 尚未发生



AI 可改变的（当前能力边界）

- 训练数据（合成与场景生成）
- 执行策略与逻辑代码层面的迭代

人类必须掌控的（未跨越的红线）

- 任务的根本定义与对齐目标
- 安全边界（Permissions）的确立
- 核心奖励函数的权重选择
- **系统底层模型架构的设计与修改**

结论：机器人当前修改的是数据和策略，而非自身的底层架构。完整自主的 RSI 尚未发生。

Gemini Notebook

短期展望（至 2026 年底）



即将发生的工程闭环：

产线实测扩大：
可预期更多类似 Mercedes-Benz 的真实工业产线级实测落地。

数据效率飞跃：
仿真-真机（Sim2Real）飞轮的闭环效率将进一步提高。

安全标准化：
开源安全基准（如 ASIMOV）与部署工具箱将成为行业标配。

不变量（The Constant）：
仿真迭代 → 少量真机修正 → 再回仿真的环路已跑通，但人类仍是方向盘的绝对掌控者。

Gemini Notebook

跨越临界点：从物理机理到数学基础



核心总结：

- 范式已从单纯的数字对话，正式切入不可逆的真机物理执行。
- 数据飞轮与安全权限引擎已开始在 VLA 与世界模型两条路线上全速运转。

下一环节交接（张立稼）：

- 要让物理 AI 真正理解并预测现实世界，必须深入探究支撑其运行的底层逻辑。

即将呈现：《世界模型的数学基础》

Gemini Notebook