硅谷前沿技术与中国制造的融合趋势

作者：SVSAC 硅谷战略顾问委员会

核心判断

硅谷技术与中国制造的结合，值得从具体产品和工程问题切入；合作价值最终要由可交付的成果体现。对企业而言，值得优先推进的是：先把企业需求翻译为技术任务，再明确知识产权、接口、验证与商业分工，按项目寻找适配伙伴。本篇结合公开资料与分析，讨论企业可以如何识别机会、组织能力并安排下一步投入。

关键词：硅谷技术；中国制造；工业人工智能；技术转移；知识吸收；系统集成

SVSAC - sv-sac.org

硅谷技术与中国制造的结合，值得从具体产品和工程问题切入；合作价值最终要由可交付的成果体现。

我们的建议是：先把企业需求翻译为技术任务，再明确知识产权、接口、验证与商业分工，按项目寻找适配伙伴。企业可以先据此梳理自己的产品、客户、能力与投入边界，把讨论推进到可以分工、可以验证的具体任务。

对管理层来说，这个议题值得放进经营议程。围绕“先做什么、凭什么做、做到哪一步再扩大投入”形成共识，往往比同时铺开多个方向更有推进价值。下文保留相关资料、比较和推演，供企业判断自身条件与行动顺序。

一、问题界定：技术跨境不等于制造融合

讨论“硅谷前沿技术与中国制造的融合”，首先要把“融合”从口号还原为可观察的工程和组织关系。算法在论文发表、软件公开、企业宣布合作、设备进入厂房、生产线形成稳定应用，是不同事件。只有明确技术对象、制造地点、承担者和验证阶段，才能避免把可接触误作已采用，把采用误作有效果。

本篇将“硅谷”作为需逐例验证的地理和机构标签，而不是技术优越性的代名词。ACT 作者项目页标注 Stanford、UC Berkeley 和 Meta；RSS 会务页面则将 Vikash Kumar 标为 University of Washington，并列出 Stanford 与 UC Berkeley。不同页面的作者机构标注存在口径差异，因此本篇仅把该研究视为湾区关联的跨机构网络案例，而不把它归为单一硅谷团队。机构归属说明知识生产网络，不自动说明技术唯一来源、所有权或产业收益归属。[1][2]

“中国制造”也不是单一主体。分析必须分别记录企业控制权、技术产权、工厂位置和实际生产环节。大陆企业在海外的厂房、大陆境内的外资或合资生产基地、台资企业运营的海外工厂，不能只因供应链名称或网站语言就合并成同一现场。工厂案例的地理定位，应以材料明确指向的生产地为准。

还需区分“制造 AI 所需的产业”与“AI 改造制造”。服务器、芯片、供电、散热和数据中心是算力供给链；视觉检测、机器人操控、质量预测、排产或数字孪生才是制造流程中的应用。前者市场或投资变化可以影响技术可得性，却不能直接证明一条产线已使用 AI，更不能单独说明产量、良率或劳动组织发生了何种变化。

技术迁移的分析单位应是具体任务与工艺，而不是抽象“智能工厂”。例如抓取不规则零件、插接精密连接器、识别表面缺陷和重排车间物流，需要不同传感

SVSAC | sv-sac.org

器、容差管理、控制周期及安全边界。即使都称机器人 AI，任务对象、物理接触方式和出错后果也会改变部署难度，因而不能用单一成功率代替跨任务比较。

我们提出的核心问题是：湾区可识别的研究与技术供给，经何种数据、仿真、控制、设备和组织接口进入中国制造现场？什么证据只表明技术可用或合作计划，什么材料能说明现场持续应用？进一步说，现场应用与绩效之间还隔着基准、观察期和替代解释，不能将应用标签当作因果结论。

将技术视作可独立搬运的软件包，会忽略生产任务中的隐性知识。工艺工程师知道工件变形、夹具偏差、节拍冲突和异常恢复规则；系统集成商要把这些条件转译为传感器位置、坐标变换、控制逻辑和验收程序。若这类知识没有进入模型、控制器和维护手册，仿真中的动作即使正确，也可能在实际工位无法重复。

因此，跨区域融合往往是“技术供给–本地吸收–系统集成–生产反馈”的循环，而非单向设备输入。外部技术可能由本地团队重新标定、筛选和改造；制造端也可能把异常数据、工艺模板和故障处理方式反馈给集团其他工厂或平台供应商。有关企业间知识吸收与输出的研究提示，跨组织 IT 连接可能成为知识流动的条件，但其西班牙一般企业样本并不能证明中国 AI 制造部署效果。[3]

公开证据至少可分为六层：研究原理与实验室基准、工具可公开获取、产品或平台可用、伙伴关系或部署计划、特定工厂在用、跨工厂复制及独立绩效评估。高层级证据不能由低层级自动推出。企业公告适合确认其在某一日期宣布的产品、合作或部署阶段，却通常不提供独立审计的净效果；论文实验适合分析机制，也不等于现场运营记录。

比较不同证据时，应问清观察对象、时间和评价单位。研究论文可能以一次插接是否成功为单位，企业报告可能以项目上线、机器人交付或工厂数字模型为单位，经营评估则需要把停机、质量、人工介入和维护成本放入完整周期。若三个单位被概括为同一种“落地”，读者就无法知道论断指向技术可行性、采购实现还是经营表现。

技术路径也需要拆成可以追踪的接口：输入数据如何形成，现场状态如何感知，算法输出如何成为可执行动作，设备控制如何满足安全要求，MES 或其他生产系统如何提供任务和回传结果。接口故障可能造成模型看起来准确、实际生产却不可用。反过来，流程设计和工装更新即便有效，也不能未经比较就归功于 AI。

制造现场的“成功”不是一次动作完成，而是能否在产品、零件、批次、班次和设备状态变化时继续达到验收要求。需要把首件调试、换型、持续运行、版本

SVSAC | sv-sac.org

升级和异常恢复纳入观察。将部署日的演示成绩外推为量产能力，会遗漏维护、工艺漂移、人员轮班和来料差异等长期约束。

研究与企业材料的利益位置不同。学术论文会强调新方法的贡献并在特定基准上验证；平台供应商的客户案例会突出产品接口和合作价值；制造企业的中期报告可能同时承担投资者沟通功能。它们均可提供事实线索，但事实要按来源原话的范围引用，效果和因果则需独立数据或明确的比较设计支持。

分析中需要把功能、技术来源、产权、服务和收益拆开。模型可能来自学术团队，仿真器由平台企业提供，机器人由设备厂制造，产线改造由集成商实施，工艺数据由工厂掌握。发生故障时，责任也可能按设备、软件、数据或工艺划分。把整套系统统称为某一国家或公司的技术，会遮蔽互补投入及真正的控制节点。

地缘规则和芯片许可可影响某些算力供给及部署架构，但规则文本只界定特定物项与适用条件。它既不证明某笔交易已申请或获批，也不证明受影响的工厂无法完成本地部署。制度变化在本次分析中是技术路径的条件之一，不是对具体企业合法性、供给数量或运营结果的替代证据。[4]

地方或全国投资统计同样有限。实际使用外资、制造业投资或高技术产业分类能够交代某一期间的总体背景，却没有直接识别硅谷来源、AI 项目、设备采购或知识转移。把总量趋势转换成某一工厂采用技术的证据，是层级和对象的双重错置；因此相关统计只在需要解释背景时谨慎使用。[5]

原稿资料截止 2026 年 10 月 23 日，指定原段于 10 月 28 日再核，不能据新网页还原未存档的历史版本。本篇采用定向公开资料的叙述综述与机制比较，不报告原创企业实验、访谈或穷尽性普查。研究材料包括同行评议机器人论文、企业公告和公开监管文本，证据等级和利益关联均需说明。关键判断使用“研究显示”“公司公告称”或“可据此提出”等不同表述，以免把观察事实、企业主张和作者推论混成同一语气。

本篇不试图判断谁拥有“制造 AI”的普遍领先地位，而关注技术跨界后如何被工程化和组织化。对中国制造而言，吸收能力不只意味着工程师能调用代码，还包括获取工艺数据、维持接口、形成可靠测试、授权操作和持续更新。对外部技术提供方而言，能否理解现场限制并支持改造，也影响其技术能否从演示走向稳定使用。

后文首先讨论示范学习和仿真到现实的工程链条，重点分析其输入、控制和失败位置；继而比较数字孪生、平台合作及企业现场案例，区分计划、在用和跨

SVSAC | sv-sac.org

厂复制。最后再提出可检验的融合命题与评价框架。这样的顺序将先说明技术在何处可能失效，再判断企业案例究竟证明了哪一层。

总体而言，“融合”最好被理解为一组可验证的连接关系：知识从何处来、由谁转译、与何种工艺和设备相接、怎样经过验证、出现偏差时由谁处理，以及哪些经验能够迁移。只有这些环节都能被具体描述，关于区域技术合作的讨论才不会停在品牌合作、产品名词或宏观叙事上。

二、示范学习：把专家动作变成可重复的控制序列

ACT 研究的贡献不只是提出一种网络，而是把低成本双臂硬件、遥操作示范采集与动作序列学习组合成可运行系统。作者指出，拉扎带、插入电池等精细任务需要闭环视觉及接触控制，通常依赖高端设备或精密标定；其方案以示范直接学习，旨在降低实验装置门槛。[6]

ALOHA 系统由主从式双臂遥操作接口提供示范，操作者通过主臂控制机器人完成任务，系统记录视觉观测、关节状态和动作。这个设置将人的技巧变成训练样本，但并未消除人的作用：示范质量、覆盖的起始状态和操作一致性，决定数据包含哪些策略。一次演示采得快，不等于形成适用于任意零件的训练集。

传统行为克隆逐时刻预测下一动作，长序列任务中小误差可能不断累积，使策略逐渐离开训练分布。ACT 用 Transformer 预测一段未来动作，并以条件变分自编码器表征示范中的动作差异；固定长度动作块减少逐步预测负担。执行时再对重叠预测作时间集成，有助于平滑控制并保持反馈更新。[6]

动作块长度不等于观察更新间隔。朴素做法执行完整块后才纳入新观测，会降低反馈频率；ACT 则在每一时步查询策略，用时间集成组合相互重叠的动作预测。[6] 因而不能笼统推断块越长，ACT 就越晚响应。实际反馈还受相机、推理、集成权重和底层控制延迟影响。动作分块不自动解决碰撞及安全约束，须按执行实现和任务风险分别评价。

论文与项目页展示低成本双臂平台的多种技能，但须区分遥操作演示与 ACT 学习任务。链条装配和动态乒乓球等平台展示不能全部记为 ACT 自主学习结果；开杯、插电池等学习任务的成功率须依对应实验读取。[6] 这种区分保留平台能力，同时避免用人的遥操作表现扩大策略的已验证范围。可控工作台与短周期任务也不同于连续多班次产线。

作者项目页报告四项任务各以 50 次示范训练，其任务成功率分别为 96%、84%、64%和 92%[1]；RSS 论文摘要另称六项现实任务中，部分任务用约 10 分钟

SVSAC | sv-sac.org

示范达到 80%–90%成功率[6]。两组数字来自不同任务、训练条件和页面，不应合并为统一基准。它们显示样本效率潜力，也显示任务间表现差异，不能将最高值概括为稳定制造成功率。

失败视频本身也有分析价值。电池插槽或开杯动作可能受物体初始位置、柔性材料变形、遮挡和接触反力影响；当测试分布超出示范样本，策略可能重复已学动作而无法有效修正。论文展示对某些扰动的反应能力，也展示失败示例，提醒我们“反应式”来自有限扰动范围的测验，而非对任意产线异常的鲁棒保证。[6]

低成本平台有助于扩散研究实践，却不能等同低成本工业部署。研究系统说明硬件采购与复现可以降低门槛；工厂还要支出防护、节拍优化、集成接口、质量追溯、设备维护和安全认证等费用。研究报价或台架预算只能描述实验设备，不代表把机器人接入某条中国生产线的全生命周期成本。

从工程机制看，示范学习链至少包含示范记录、视觉与关节状态同步、任务动作表示、训练、策略推理、控制器执行和失败恢复。每个环节对应不同故障：同步误差会破坏动作对应关系，少见姿态可能导致分布外输入，控制器带宽和机械回差则使预测动作无法精准实现。训练集越小，是否覆盖关键异常越重要。

面向制造场景的迁移问题，应从“学会动作”转向“产线工艺是否允许该动作”。零件公差、夹具定位、上下料节拍和设备通信接口可能被固定化，降低学习难度；也可能因批次差异、柔性线缆或污染而扩大变化。部署前要确认自动化边界究竟由算法、专用工装还是环境标准化共同形成，而非把能力都归给模型。

示范产生的知识也存在产权与反馈安排。操作员或集成工程师贡献轨迹，制造企业提供工艺环境，模型开发方维护代码，平台企业提供硬件和训练栈。若合同或项目制度未明确训练数据用途、异常视频留存、知识产权和可迁移格式，现场经验可能难以在供应商更换后复用。这是部署治理问题，不是 ACT 论文已观察到的合同事实。

跨工厂迁移不会只靠复制权重。不同产线的相机视角、机械手型号、坐标系、末端夹具和物料位置要重新标定；若动作以关节目标而非与设备无关的任务空间表达，更换机器人时还涉及运动学和控制映射。权重文件只是工件之一，校准参数、数据版本、任务定义和验收脚本同样决定复现结果。

工厂评估还需观察节拍与恢复能力。ACT 论文报告的任务成功率和示范评估没有验证特定产线 takt time、故障恢复时间、轮班连续性或人工接管成本；这些是需要按具体工艺另行检验的验收指标。部署设计还须说明策略与状态机、异常分类、安全停机、重抓、剔除及人工接管机制如何衔接。报告成功率时，应同时记录周期时间、失败后恢复时间和人工干预频次。

SVSAC | sv-sac.org

ACT 作者项目页标注 Stanford、UC Berkeley 和 Meta；RSS 会务页面则将 Vikash Kumar 标为 University of Washington，并列出 Stanford 与 UC Berkeley。[1][2] 这反映页面版本和作者机构标注口径不同，不宜汇总成唯一机构清单。该研究可作为湾区关联研究网络中的一项公开技术能力，显示算法、示范接口和低成本机械系统如何降低精细操作研究门槛；但作者机构本身既不证明中国企业采用，也不能确定技术控制或产业收益归属。

与模型效果相伴的一个替代解释是任务本身被精心设计为适合示范学习。若零件、照明、相机和工作台在训练及测试中高度稳定，较高成绩可能反映环境控制，而非策略适应复杂现场的能力。公平评价需要同时报告随机化范围、未见状态、工具变化、扰动类型和失败样本；仅给出平均成功率会隐藏适用边界。

工业验证需要建立不同于论文基准的验收链：先在离线数据上检查动作质量，再在隔离工位低速运行，继而增加物料和姿态变化，最后在班次和版本变更中检查持续表现。每一步都设置停止条件和人工安全接管。这样的阶梯式验证是我们提出的评价方案，不是 ACT 项目已经执行的工厂验证。

因此，ACT 的证据强度可概括为：论文及开源项目说明示范驱动的双臂精细操作在研究硬件上可实现，并在若干任务上呈现特定成功率；它不提供中国大陆制造企业部署、长期稳定性、与原有自动化相比的净收益或劳动力影响证据。后几项问题需要工厂级数据和对照，而不能由项目网页补足。[6]

这项研究对“融合”的启示在于接口可复用性。若遥操作设备、动作数据格式和开源训练代码降低研究门槛，不同工程团队就可在本地复制并改造实验；但复制研究环境与复制生产能力是两种不同扩散。要从前者走向后者，需把工艺知识、控制权限、维护能力和质量验收嵌入系统，不能只下载代码。

同一系统中，学习策略与传统控制并非互斥。策略可提供复杂动作序列，底层控制器仍负责轨迹跟踪、力限制和安全状态。工厂可将 AI 限定在可逆、低风险或高变化任务，将安全关键步骤交给确定性逻辑；这种分层不是对研究先进性的判断，而是根据失效后果、可观测性和回退成本作出的工程选择。

示范学习由此给出一个可检验命题：当任务重复、示范覆盖主要变化、末端控制与数据格式标准化时，本地集成商可能以较低样本量复现精细动作；若零件接触和异常超出示范分布，人工干预及失败恢复成本将上升。验证需按任务和工厂记录示范量、分布覆盖、成功率、节拍与人工接管，而非只比较模型名称。

SVSAC | sv-sac.org

三、仿真到现实：接触丰富装配中的物理差距与系统接口

IndustReal 把问题推进到更接近工业装配的接触任务：机器人必须先识别零件，再抓取、对齐并插接，精度误差会在接触中累积。作者指出传统自动化常通过高精度硬件、专用夹具和轨迹工程达到精度，但这些定制工程耗时且对工位扰动敏感。仿真可减少实机试错，却不能自动消除物理模型与现场之间的差异。[7]

研究团队由南加州大学、Stanford、NVIDIA、悉尼大学和华盛顿大学等机构成员组成。[7] 这是跨地区实验室与企业研究网络的实例，而不是单一硅谷团队。NVIDIA 人员参与研究且论文使用其 Isaac Gym 仿真工具，说明平台供给与算法研究相交；同时作者分布表明技术开发并非只在某一地区完成，不能据此推断后续产业收益由平台方独占。

方法由多部分共同构成：simulation-aware policy update 按网格相互穿透程度过滤或降低仿真回报权重，减少策略利用不真实碰撞动力学；有符号距离场奖励为复杂几何提供对齐信号；基于采样的课程学习调节训练任务难度；部署时的 policy-level action integrator 则降低未建模动力学造成的稳态误差。[7] 这些组件分别作用于训练、任务难度和实机控制，不能简单概括为“数字孪生自动训练机器人”。

研究在仿真中以 Factory 接触动力学处理销孔和齿轮组件任务，报告 82%–99%的任务成功率，并在约 26.5 万次仿真试验中评估算法组件。[7] 大量仿真试验提高了实验内比较的规模，却不是对真实零件分布的抽样。结果有效范围取决于 CAD 几何、摩擦参数、碰撞模型和任务定义是否覆盖将来工厂的实际差异。

实体系统采用 Franka Panda 协作机器人和 RealSense D435 RGB-D 相机，作者刻意避免专用夹爪及力/扭矩传感器，并以不大于约 0.5–0.6 毫米的间隙构造装配基准。[7] 这种设计强调使用常见研究硬件并展示算法能力，但研究级机械臂和传感配置仍不等于工厂的高节拍自动化设备。基准工件和光学平台也比复杂生产单元更易控制。

仿真策略输出须经过实际通讯和控制链才能转为运动。作者以部署时动作积分器将策略动作转成目标状态，再交由低层阻抗控制器跟踪；其作用是应对例如摩擦未建模等误差，而不是改写策略本身。[7] 这说明“从仿真迁移”不只是把权重下载到机器人，还要设计策略输出、控制器、机械系统和扰动补偿之间的边界。

感知模型也并非在通用数据上直接可用。论文附录说明，COCO 预训练的 Mask R-CNN 在研究自有零件上初次测试失败，因此团队采集每类约 10–30 张真实图像微调，再通过背景移除、合成与颜色扰动扩大数据；文中报告典型精确率

SVSAC | sv-sac.org

和召回率高于 85%。[7] 这说明即使策略在仿真训练，视觉识别仍需针对本地工件与成像条件适配。

相机标定是另一个不可省略的接口。研究团队用 AprilTag、机器人末端位姿样本和 Tsai–Lenz 方法估计相机与机器人坐标关系，再与包含相机安装结构的 CAD 组件进行校验。[7] 工厂复制时，支架振动、换相机、维护后重新安装都会改变外参；标定记录与验证程序因而应作为部署工件保存，而不是只留在集成商工程师的个人笔记中。

论文报告真实系统在 600 余次试验中，各任务成功率处于 83%–99%范围。[7] 这是固定实验平台、指定工件和有限扰动条件下的任务级结果，而非产线可用率。试验次数能够提高对该设置中重复性的认识，却没有覆盖多年磨损、连续班次、换批、维修、生产节拍或停线成本。将这组数字转写为“工业机器人可靠率”会改变其观察单位。

例如拾取实验中，系统对多个销钉的总体成功率为 98.8%，失败主要包括漏检和夹取物件及托盘。[7] 这一高成功率表明感知与抓取链在定义好的工作台上可运行；同时托盘误抓说明动作决策不仅依赖目标识别，也受夹具边缘和场景布局影响。工业验收还需测量误抓是否损坏产品、引发停线或可被下游检测及时拦截。

插接任务更清楚地展示“部分接合”和“完整装配”不能混为一谈。对销钉、齿轮和连接器，论文报告部分插入率分别为 86.7%、95.0%和 100%，而完整插入成功率为 76.7%、92.5%和 85%；销孔策略还泛化至未见过的 NEMA 连接器。[7] 任务推广说明具备有限的几何迁移，但完整插入率更接近实际验收，且仍不能代表复杂线束或多品种量产。

失败机制并非抽象的“仿真鸿沟”。研究中部分接合失败主要来自物件在夹爪中滑动，完整插入失败主要来自插头与插座楔紧。[7] 两者分别指向夹持力、接触摩擦、间隙公差、插入方向和控制顺应性。若部署方只通过提高模型规模应对，可能忽略真正的工装、传感或机械柔顺问题；失效分类比总体准确率更能引导工程修正。

端到端抓取–放置–插接演示还需承受前序误差传播。论文把零件随机放置并对目标位置加入噪声，显示整个动作链可在测试条件下运行；但每个阶段的误差会改变下一阶段初始状态。[7] 生产验证因此应分开记录感知、抓取、定位、插接的失效，再记录级联失败，不能仅用最终是否完成来判断该由视觉、夹爪、运动控制或工件夹具负责。

SVSAC | sv-sac.org

研究强调无需真实世界策略适配阶段，并提供部署代码及训练工具。[7] 这是一项重要研究结果，但含义是在其经过设计的任务和系统配置中，不需要额外实机策略微调，不等于无需标定、感知微调、机器人配置、通讯测试和安全调试。作者实际仍需为零件训练检测模型、校准相机，并把控制与策略通过 Frankapy 链路接起来。

作者将主要限制之一明确指向任务外推：研究大多围绕 NIST 启发的装配基准；更复杂的弹性线缆套轮等任务可能没有足够准确且高效的仿真器。[7] 仿真精度不是可通过数据规模无限弥补的常数。柔性体接触、摩擦、变形和长时间相互作用可能需要新的物理模型、传感方式或控制策略，原有迁移流程并不保证顺利推广。

论文讨论的后续方向包括仿真与真实视觉触觉、提升摩擦建模以及同时优化策略、控制器和被动机械顺应性，并提出从现场回到仿真的反馈循环。[7] 这揭示了工程部署与研究迭代之间的双向关系：真实故障提供模型缺项，仿真帮助筛查新策略，但回传数据要经过清洗、标注和参数更新。是否能形成闭环取决于现场数据权限与责任安排，不是平台自带属性。

部署软件的可复现性也依赖具体通讯协议。论文附录描述的链路是：策略从 Isaac Gym 训练 checkpoint 生成动作，由 PLAI/IndustRealLib 形成目标状态，再由 FrankaPy 经 ROS 传送至 franka-interface；libfranka 和任务空间阻抗控制器（TSI）随后映射至低层关节力矩。物体检测另有相机图像和微调模型。[7] 这是该实验平台的软件栈，并非所有工业设备的通用架构；迁移仍需适配控制柜、现场总线、急停逻辑和安全 PLC。

IndustRealKit 公开 CAD 模型、零件清单和软件库，作者称已在两台不同城市的 Franka 机器人上使用工具链。[7] 这类可复现工件降低学术同行重复实验的成本，也为本地研发团队提供了起点；但设备型号有限、工件和场景有定义边界。工业复制需额外提供版本兼容矩阵、硬件替代验证、安装维护手册以及发生重大偏差时的回滚方法。

由此可见，仿真迁移是多层互补：几何与物理模型、课程和奖励设计、感知标定、夹爪与机械顺应性、策略动作接口、低层控制和异常恢复共同决定结果。只报告模型算法会把集成工作隐去；只展示设备运行又会掩盖训练数据和仿真参数的作用。两种叙述都不足以解释怎样在异地工厂复制技术。

一个可证伪的推论是：在接触状态可感知、零件公差稳定、仿真参数经现场校准、且恢复流程标准化的装配任务中，仿真训练有望减少实机试错；若滑移、楔紧、柔性变形或工件批次变化超过模型与传感能力，优势会明显减弱。测试需

SVSAC | sv-sac.org

同步记录仿真参数、装配完整率、人工恢复、节拍与不同批次表现，而不能把一次成功演示当作迁移完成。

四、数字孪生的可迁移性：几何模型之外的语义、数据与运行接口

数字孪生在制造中的作用，不只是把厂房做成三维可视化，而是为设计、仿真、调试和运行建立可更新的系统表示。若虚拟模型只复现建筑外观，不能表达设备状态、物料流、工艺顺序和性能约束，它对工程决策的价值有限。因而评价数字孪生应先问其模型连接了哪些对象、数据和决策动作，而非观看画面是否逼真。

一套可运行的孪生通常至少涉及几何/资产模型、工艺和资源语义、现场传感数据、生产执行或车间控制系统，以及仿真与分析模块。制造执行系统（MES）描述订单、工序和生产状态；车间控制（SFC）及自动化系统连接设备和局部控制。不同系统对同一设备、工单、时间戳和状态码可能定义不同，接口集成需要语义映射，不是简单连上数据管线。

设计期孪生与运营期孪生也需区分。前者帮助比较设备布局、维护空间、物流路线及安装顺序，现场数据更新频率可以较低；后者希望监控状态、预测异常并支持调度，对时延、数据质量和责任要求更高。一个模型用于虚拟规划，不能因此被称为实时控制系统；静态设计成果与在线生产决策的证据等级不同。

仿真模型的准确性应与决策问题相匹配。物流拥堵分析关注路线容量、到达时间和缓存区；机器人碰撞检查关注几何、碰撞体与运动轨迹；热流计算需要边界条件与物理求解。一个可视化孪生不一定具备足以支撑这些分析的物理保真度。系统声称“物理精确”时，仍需说明经过何种基准、设备或工况验证。

跨厂复用的价值来自可迁移工件，而非渲染引擎名称。可复用对象可能包括标准化资产、工位模板、工艺流程、物流规则和接口定义；但设备品牌、厂房结构、当地劳工规则、供应链节奏和安全规范会使本地配置不同。真正复制的是经验证的约束与模板，并为新地点保留差异化参数，而不是期待一个场景文件直接驱动另一座工厂。

OpenUSD 等场景描述标准能帮助多个工具共享几何、层级与属性数据，但格式开放本身不保证工业语义完整。设备状态机、工艺节拍、控制权限和数据血缘若未被一致表达，资产仍需手工转译或专有扩展。互操作性应以跨工具往返转

SVSAC | sv-sac.org

换、属性保留、版本升级与实际工程使用测试，而不是以支持某种格式的产品宣传作结论。

仿真结果与现场输出之间还存在模型维护责任。设备改造、传感器替换、软件升级和工艺变更都会使模型过时；如果数字孪生由中央工程团队维护而工厂现场不能校正，状态会逐步偏离。需要明确谁负责更新、谁审批模型版本、哪些数据可以回传，以及模型不一致时运行决策应以何者为准。

数据同步本身有多种失败方式：时钟不同步使因果顺序错乱，设备标签重复使事件映射错误，短暂断连导致缺失，质量指标统计口径不一致则会误导比较。把数据流显示在仪表盘上只证明系统读取到数据，不证明其语义正确或决策得到验证。工业部署应有数据完整性、延迟、异常值和版本追溯的监控。

NVIDIA 公开的 Foxconn 客户案例称，工业富联开发 FODT，以 Omniverse 与 OpenUSD 构建工厂数字孪生，并连接现场运营数据及来自 MES、SFC 和自动化系统的关键指标。[8] 这一材料可用于分析供应商如何描述孪生、执行系统与运营数据的连接；它是 NVIDIA 发布的客户案例，非第三方审计，也不自动提供所有工厂的部署状态。

该案例进一步说明数字孪生不等于单一模型，而是围绕不同工作负载组合多种工具：工厂布局和设备单元仿真、机器人开发、AGV 路径优化、热流分析及现场指标呈现。[8] 不同模块有不同的物理和数据依赖，例如 AGV 路线优化取决于实时物料状态和通道约束，机器人运动仿真依赖标定与碰撞模型。产品清单或案例首页不能证明每个模块在每个基地均已部署。

Foxconn 案例中的供应商陈述称，其标准化场景资产支持产线在全球工厂间快速迁移，举出的地点例子是台湾到墨西哥。[8] 这是一条明确的跨区域迁移线索，但不应改写成中国大陆工厂落地证据；也不能据此断定迁移后产线节拍、良率或投产周期独立改善。台湾与墨西哥的实例更适合作为观察可迁移工件及适配工作的案例。

客户案例还称 PhysicsNeMo 模型将 CFD 模拟加速约 150 倍，并引用工业富联负责人对营收周期、厂房建设和生产规划整体时间缩短 50%的预期。[8] 前一数据是供应商案例中具体热分析任务的陈述，不等于全厂生产率提升；后一数字明确属于管理者预期，不是已测结果。两者应分别标为客户/平台方报告与前瞻估计，不能当独立因果估计。

案例边界同样受企业身份和生产地点影响。Foxconn 案例说明工业富联和富士康集团内制造网络使用其方案的客户陈述；其“全球工厂”叙述和台湾至墨西哥示例不等于已证明大陆工厂采用。即便企业集团与中国大陆制造关系密切，也应

SVSAC | sv-sac.org

逐个核验地点、法人、生产流程和部署阶段，不能把集团整体标签当作单一工厂证据。[8]

数字孪生工具还可能造成“虚拟先行、现场滞后”。规划阶段可通过模型发现布局冲突，但生产数据接入、设备控制权限、工艺工程师参与和维护预算可能在投产后才显现。若预算只覆盖三维建模而未覆盖数据维护与现场服务，模型可能在建设后失去更新价值。项目的生命周期资金安排与组织责任应纳入孪生可持续性分析。

供应商主张的效率改善必须拆解成受益活动。若模型减少了机器人单元重新编程，受益是工程设计时间；若热流模拟让设备冷却方案更快收敛，受益属于特定仿真任务；若数字看板缩短异常发现，则需记录从事件发生到识别、处置和恢复的时间。把这些局部效益统称“工厂效率”会混淆技术指标、流程指标和经营结果。

评价孪生是否支持扩散，可观察新厂建模工时、接口调试次数、资产复用比例、现场校正量、调试周期和模型偏差变化。若从第一座到第二座工厂的配置工作下降，且功能验收保持一致，才初步支持模板复用机制；但不同产品组合和厂房复杂度也可能改变成本。比较设计前后应记录变化因素，不直接以供应商宣称的倍数作为可推广收益。

跨地点的数据治理会进一步影响能否复用。工艺数据可能包含客户订单、设备参数和供应商知识产权；集中云平台可降低多站点协作成本，也会增加访问控制和跨境数据处理要求。可行的架构可能是区域部署、聚合指标回传或数据不出厂的联邦管理；选择取决于数据敏感度和运行时延。法规适用需按具体系统与处理活动核验，不能从一个客户案例推断普遍合规方式。

虚拟模型也可能强化供应商锁定。专有资产库、脚本、仿真插件与数据格式累积后，客户迁移到另一平台可能承担重建成本。若企业保留原始 CAD、场景描述、设备映射、仿真脚本和验证记录，切换成本可能降低；但保留文件不等于工具链替代成熟。应在采购阶段确认导出范围、许可证、版本兼容和退出测试。

因此，判断数字孪生是否已从可视化工具成为制造系统能力，应分开核验：模型内容、数据更新、工作流嵌入、工程决策、现场动作和结果评价。对每一层设置责任人、版本和验收标准，可避免“有孪生”掩盖数据缺失或无人维护。此框架用于审阅公开案例与设计后续观察，不表示本篇已获得 Foxconn 内部项目日志。

一个可检验命题是：当资产和接口语义标准化、现场数据持续更新、责任跨设计与生产团队明确时，数字孪生可能降低新工厂调试的重复工程量；若模型缺

SVSAC | sv-sac.org

少运行语义、无法与执行系统对齐或现场无人维护，跨厂复用收益会消失。验证应比较至少两座工厂的可迁移资产、工程投入、校准偏差和投产过程，并控制产品、产能与工艺差异。

五、BMW 沈阳 Plant Lydia：虚拟规划、生产应用与 AI 标签的边界

BMW 集团 2022 年宣布沈阳 Plant Lydia 启用，并将其定位为电动化、数字化工厂扩展项目。[9] 这一材料提供一个实际制造地点和明确时间点，可用于观察跨国集团如何把虚拟规划嵌入工厂建设。其证据价值在于识别数字化规划的组织场景，而非证明所有工厂功能均由人工智能驱动。

公告对 Lydia 规划工具有清楚说明：Epic Games 的 Unreal Engine 3D 平台是虚拟规划与仿真的骨干，工厂从起始阶段就在虚拟环境中规划生产过程。[9] 这项区分很重要，因为同一集团与 NVIDIA 另有 Omniverse 合作公告。将两个平台名称交叉拼接，会制造来源材料没有写出的技术链。就 Lydia 本身，应按 BMW 对该厂的明确表述称 Unreal Engine。

虚拟规划的工程作用主要发生在建设和投产前：设计团队可在实体施工前检查产线空间、设备关系和生产流程，并让不同地区团队查看共同模型。BMW 称虚拟与现实结合缩短规划时间、支持跨地区及时区协作。[9] 这是公司对项目机制的叙述，但没有公开足够的施工计划版本、工时或对照厂数据来估算净节省，因此分析宜将其视为可识别的工作流程主张。

公告还提到，新厂按冲压、车身、涂装和总装等主要生产环节设计，并为电动汽车生产留出柔性。[9] 这让数字规划面对的不只是三维布局问题，也涉及工艺顺序、物流连接和生产线之间的协同。不过，新闻稿没有列出每个工序的模型精度、现场接口或使用者验收记录；不能推断整个生产系统已经由同一个数字孪生持续控制。

BMW 称虚拟与现实的整合缩短了规划时间，并帮助项目应对疫情带来的不利影响。[9] 公告还提到建设时间缩短六个月，但原句的指代关系不够清晰，且没有可识别的比较基准。这里仅保留公司对虚拟协作和项目应变作用的描述，不将该数字归因于疫情因素或 Unreal，也不把它作为经验证的数字化节省。

生产运营与规划阶段的证据需要分开。BMW 称 Lydia 在 2022 年 5 月已开始生产面向中国市场的纯电动车型，并将其扩展至沈阳生产基地整体产能。[9] 这表

SVSAC | sv-sac.org

明工厂进入生产阶段；但工厂生产汽车不等于此前的每个虚拟模型功能均在运营，也不等于产线 AI 系统的效能获得独立验证。

新闻稿说沈阳生产基地当时约有 100 项人工智能应用，表述对象是 Shenyang production base，而不是仅指 Lydia 厂房。[9] 因而这项数字只能说明企业在基地层面报告的 AI 应用数量，不能改写成“Lydia 部署 100 个 AI 系统”，也无法从页面判定这些应用是视觉质检、能源分析、维护还是其他任务，更不能断定均属生成式 AI。

公告描述质量保障区域布置多功能相机并生成大量数据，配以 5G 网络和数据中心基础设施。[9] 这些设施说明运营 AI 依赖的不仅是算法，还包括网络覆盖、数据处理和现场设备。该数据量属于企业新闻稿中的基地描述，缺少独立测量方法与任务分解；引用时应保留企业来源和范围，不用它估算整个汽车行业的数据需求。

生产数字化链可以拆为传感采集、数据治理、质量或能耗分析、工艺决策和现场执行。每步需要不同责任主体：设备厂保证传感与接口，IT 团队维护网络与数据平台，工艺团队定义可接受偏差，质量部门制定放行标准，操作人员处理例外。BMW 公开稿给出部分基础设施与总体应用信息，却没有披露其各项 AI 应用的具体责任配置。

Lydia 案例因此适合用于研究“建设期虚拟规划如何连接量产组织”，不适宜直接作为 AI 算法工业效果案例。可能的验证问题包括：规划模型发现多少冲突、现场变更如何回写、设备调整是否减少、调试历时如何定义、质量和节拍是否以可比基线测量。公开材料未给这些记录，研究者不能用企业宣传语填上数值答案。

数字规划和 AI 运营还可能构成两条并行技术路径。Unreal 引擎用于空间与流程可视化仿真，并不自动生成预测性维护或视觉检测模型；后者可能调用统计学习、规则模型或其他软件。把两者合称“工业 AI”会模糊规划工具和决策模型的不同验证要求，也使技术来源和错误责任难以厘清。

2021 年 BMW 与 NVIDIA 合作公告讨论 Omniverse 用于复杂制造系统的虚拟规划，并将跨工具数据整合、实时协同和未来全球生产网络数字化描述为发展方向。[10] 公告还提到先前在物流机器人和 BMW 自研运输机器人上的试点。它支持“BMW 与 NVIDIA 宣布合作以及某类机器人试点”的主张，却没有说 Lydia 采用 Omniverse 或该合作平台已覆盖所有工厂。

两份公告时间不同，技术对象也不同。2021 年材料围绕 BMW 与 NVIDIA 的平台合作及未来愿景；2022 年 Lydia 稿明确指出 Unreal Engine 承担该厂虚拟规划

SVSAC | sv-sac.org

骨干。[9][10] 将它们作为两个技术关系对照，有助于说明大型企业可以并行使用不同供应商工具；只有逐一核对具体工厂、系统模块和时间范围，才可判断它们是互补、替代还是各自独立的项目。

“虚拟工厂”名称可能让人以为从设计到运营已实现数字闭环。实际要检验闭环，需要追踪现场设备数据是否更新几何/工艺模型、规划变更是否同步至控制和作业指令、偏差是否被记录，以及模型输出是否改变决策。新闻稿所述全面规划和生产基地数据化并不自动证明以上所有机制已运行，需避免从概念名称推导技术成熟度。

一个替代解释是，新厂建设本身伴随大额资本投入、新设备、流程重排和管理升级。即使数字规划与投产速度或质量同时改善，若无同类工厂基线、前后设计周期和项目变更记录，也无法分解其贡献。疫情期间的施工、供应链和人员安排又可能影响建设时程，因果判断尤其不能只依靠单一企业的回顾性新闻稿。

厂区 AI 数量也可能反映不同粒度的统计口径：单个模型、应用模块、工作站软件或业务流程都可能被计为一个“应用”。若不说明计数规则、运行频率、使用范围和停用项目，数量只表示管理层对部署组合的概括，不是系统覆盖率、自动化程度或绩效变化。此类统计须连同定义一并引用。

可复制性要看工厂模型中哪些对象能够跨项目保留。基础建筑、标准工位和某些设备族可模板化；车型、电池结构、物流路径、当地法规及供应商配置则会带来差异。对跨国集团而言，内部标准能促进复用，也可能因本地工艺和劳动力条件不同而需要改造。复制模板的效率须与新厂重新验证的成本共同考察。

Lydia 的资料还说明中国制造现场并非只能作为被观察对象：大型跨国企业在华生产基地也可以成为工厂设计与运营知识的形成地。要识别这种反馈，仍需集团内部文件或后续工厂公告说明哪些流程、布局或经验被转移。单凭 Lydia 建成和集团全球化战略，不能断言其具体设计已经输出至其他国家工厂。

因此，企业案例评价应把“设备在厂”“系统被使用”“模型影响决策”“工艺绩效改善”逐层区分。前两层可以从公告或现场材料验证；第三层需要决策记录和版本日志；第四层还需要对照基线与观察期。这个分层能保留企业公告对技术路线的价值，同时避免把部署状态直接当作收益结论。

针对 Lydia 可提出一个可检验命题：当虚拟规划模型与工艺、设备、施工数据保持同步，且跨地区工程团队共享版本和变更记录时，工厂建设阶段的重复设计与现场改造可能减少；若模型仅用于视觉展示或未回写现场变更，规划收益将有限。验证需取得设计版本、冲突清单、变更工单与同类工厂周期数据，目前公开公告不足以完成该检验。

SVSAC | sv-sac.org

六、从沈阳到德布勒森：制造流程知识的反向传递

BMW 于 2025 年 3 月发布德布勒森工厂装配线启动进展，称匈牙利新厂吸收集团全球生产网络的创新，并把沈阳 Plant Lydia 明确列为流程和布局参考来源。[11] 这份公告为中国制造经验向欧洲新厂反馈提供了一个可识别方向；但它记录的是 BMW 在当时对装配启动和生产准备的说明，而非后续全生命周期运营评估。

公告称德布勒森装配线启动后运行顺利，管理负责人将其与虚拟规划、测试及新员工和集团专家协作联系起来。[11] 这是管理层对初期启动状态的自述，未提供生产统计、缺陷率或连续月份数据。其证据可说明企业如何解释投产准备机制，不能据此断言该线长期零故障，也不能估算虚拟规划单项贡献。

公告所述的知识来源不止中国。德布勒森的装配规划参考了沈阳 Lydia 和德国莱比锡既有工厂的结构与流程。[11] 因此，较准确的描述是集团内多工厂经验汇合：莱比锡提供物流结构经验，沈阳提供部分装配布局和生产流程参照，匈牙利团队承担新厂适配。将其简化为“中国技术输出欧洲”会丢掉共同设计的多来源结构。

BMW 特别称德布勒森装配车间与完整输送系统按 Lydia 的布置相同，使用经过实践验证的技术，以简化新生产线调试。[11] 这是有明确对象的流程复制：装配区域和输送系统的组织方式。它比一般的合作公告更能支持“从中国生产现场借鉴流程”的论点，但仍是公司披露的复制关系，没有公开原始布局版本、改造比例或调试工时。

同一公告将另一项可迁移结构归于莱比锡：所谓“手指式”或梳状物流结构最初由莱比锡工厂开发，使零部件和预装模块可直接供给装配线；德布勒森进一步调整为双侧供应。[11] 该案例说明一座新厂可组合来自不同旧厂的设计工件。集团内部标准并非一个单一模板，而可能是若干局部方案的模块化拼接。

将 Lydia 与莱比锡的做法用于德布勒森，也不代表完整工厂被复制。新厂仍须匹配 Neue Klasse 车型的模块化设计、线束结构、供应商布局、当地建筑条件和产量爬坡安排。公告提到 Neue Klasse 线束减少线长和重量、减少不同连接件等设计特点，[11] 这些产品架构变化本身可能影响装配复杂度，不能把其全部表现归因于跨厂流程移植。

迁移的价值对象可以分成空间布局、工位关系、物料供应规则、预装流程和调试经验。它们的标准化程度并不相同：车间与输送结构可由工程图纸描述，供应节奏可能依赖供应商能力，异常应对与班组协作则更多依赖实践知识。公开公告验证了若干布局和流程被参考，未说明知识如何编码、培训或组织转交。

SVSAC | sv-sac.org

工厂间知识转移可能通过设计审查、工程师驻厂、共享模型、标准作业文件和供应商协同实现。BMW 公告称全球生产网络专家参与协作，也称新厂完全虚拟规划；但没有逐项列出具体人员流动和数字文件。[11] 因而这些渠道可作为待检验的机制假设，不能写成已由公告证实的完整转移流程。

这一案例的方向性值得注意：常见叙述把中国工厂视为接收德国或美国技术的地点，而 BMW 材料显示沈阳生产现场可以成为集团新厂的参照之一。它支持“在华制造节点可能贡献集团生产知识”的有限推论；不代表所有技术研发或知识产权都源自中国，也不改变外资集团的所有权和平台控制结构。

更重要的是，报道的转移对象主要为生产布局、输送系统与装配流程，而非机器学习模型、AI 软件、芯片或 Omniverse 平台。[11] 若核心问题关注“前沿技术融合”，这一区别避免将所有跨厂经验都包装成 AI 扩散。工艺知识的输出本身仍是制造能力的重要组成，但它与技术平台来源应分别论证。

公告提到德布勒森生产线数字化质量检查，并称后续将把相关程序用于其他工厂，慕尼黑将是下一处使用地点。[11] 这一描述在 2025 年 3 月是已在德布勒森采用、未来计划向慕尼黑扩展的阶段性陈述。要判断截至后续时点是否实际扩散，需查新的工厂公告或运行记录，不能将 2025 年的计划写成已经完成。

数字检查流程是否可迁移，取决于检验对象、采集设备、判定阈值、工艺版本和误报处理是否一致。相同的软件在车型、材料或装配公差变化后，可能需要重训、重新标定或由质量工程师重设阈值。BMW 公告仅确认应用方向和计划，不公开模型类型、准确率、抽检比例或质量部门验收标准，因此不能据此报告 AI 质检效果。

德布勒森案例还展示从“设计复用”到“生产复制”之间的时间差。新厂可先吸收布局模板，随后才经过设备安装、虚拟试验、试生产、爬坡和稳定量产。2025 年公告称工厂正在启动装配并计划当年稍晚开始系列生产；这一日期是当时的前瞻信息，不是对后续生产达成情况的证明。[11]

工程上需要区分被复制的文件与被复制的能力。图纸、模型、工位坐标和设备清单可以传递，团队识别异常、调节节拍和维护供应流的能力则需要培训与共同运行积累。若新厂只获得图纸而没有权责、技能和调试支持，复制结果可能形式相同、运行性能不同。公开材料未说明团队学习曲线，仍需案例数据验证。

跨厂复制还可能受到成本和路径依赖约束。沿用成熟布局可降低重新设计风险，但若旧工厂工艺与新产品不匹配，过度复用会牺牲空间效率或灵活性。新厂规划需比较直接复用、局部修改和重新设计的总工程量，不能把标准化程度视为越高越好。适配边界本身是技术移植的重要结果。

SVSAC | sv-sac.org

知识回流的分配问题也值得观察。沈阳团队提供现场经验，集团总部制定标准，新厂团队进行适配，设备供应商维护特定模块；谁有权批准模板、谁承担后续故障、哪些改进归入集团标准，会影响知识是否继续流动。该问题在现有公告中未被展开，属于未来研究需获取的组织材料，而非可从企业新闻推定的安排。

用德布勒森与其他新厂比较时，应控制新车型、厂房设计、自动化设备、供应商基础和建设期差异。若该厂调试时间较短，可能来自布局复用，也可能来自产品架构简化、设备预集成或团队经验提升。没有相似新厂作对照，任何节省的因果归属都只能是机制推测。

可行的过程追踪资料包括布局版本及变更记录、调试问题单、设备验收、工程人员跨厂协作记录、供应商培训、工艺标准修订和投产后质量数据。对每项流程标明来源工厂、修改内容与验收人，可区分“复制原样”“在地改造”和“共同开发”。该记录设计是建议，不代表 BMW 或其他企业已向研究者开放数据。

据此可以提出一个具体命题：当集团内新厂使用过往工厂经验证的布局和物料输送模板，同时保留本地团队的修改权限时，重复工程和调试问题有望下降；若产品、厂房或供应链条件差异过大，模板复用可能增加返工。可通过版本差异、调试工单、首次通过率及新厂爬坡周期检验，并与未采用相似模板的项目比较。

沈阳–德布勒森材料提供的不是 AI 绩效证明，而是中国制造节点可能向集团内部输出流程知识的公司证据。其重要性在于修正单向技术扩散想象；其局限在于企业自述、缺少过程档案与绩效基线。将技术平台、流程知识和组织学习分开，才能判断跨区域制造网络究竟传递了什么。

七、BYD 与 NVIDIA：车端算力、云端研发和工厂规划是三种不同连接

NVIDIA 于 2024 年 3 月在投资者关系新闻稿中宣布 BYD 扩大双方合作，并将车载计算、云端 AI 研发和虚拟工厂规划并列介绍。[12] 该稿由平台供应商发布，适合确认其当时披露的合作内容及技术定位。其证据性质不同于 BYD 工厂验收报告、产线运行日志或第三方效果研究，引用时应保持发布主体可见。

公告称 BYD 将基于 NVIDIA DRIVE Thor 打造下一代电动车车队，并计划使用 NVIDIA AI 基础设施进行云端 AI 开发和训练，同时使用 Isaac 与 Omniverse 开发虚拟工厂规划工具及零售配置器。[12] “将基于”车载平台与“计划使用”云端及工厂用途对应不同部署阶段；车载计算平台的选择不等于工厂系统已经投产。

SVSAC | sv-sac.org

车端 AI 主要嵌入车辆计算、自动驾驶和座舱功能，目标是在车型产品中提供车载算力；制造 AI 则要服务工艺设计、设备调度、质量控制或物流。前者芯片设计定点或车型规划，与后者的生产流程变更之间不存在自动推论。两类业务可能共享云端训练资源或数据，但须有具体系统接口证据才能说明相互作用。[12]

云端研发平台也不同于工厂控制。云基础设施可用于模型训练、仿真或软件开发，实际生产现场仍涉及工厂网络、数据隔离、控制器、安全逻辑和工艺审批。供应商新闻稿未说明云端开发工具如何与 BYD 的生产执行系统连接，也未指出哪些工厂或产线会接入这些工具。[12]

虚拟工厂规划工具可以在工厂建成或改造前支持布局、设备和生产路线的设计讨论；但规划阶段成果与投产后运营孪生仍有差别。若公告只说明计划开发工具，便不能推断该工具已接入实时设备数据、MES、质量系统或机器人控制，也不能认定已形成持续的虚实闭环。[12]

零售配置器是另一类应用，帮助客户组合车辆选项和呈现产品配置，不属于制造控制。平台公告同时列出工厂规划和零售工具，说明同一技术平台可能服务多个价值链环节；但每个应用有独立的数据来源、用户和验证标准。将零售体验功能算作制造智能化，会扩大“工厂应用”的统计范围。

新闻稿称 BYD 将使用 NVIDIA AI 基础设施和工具，并非独立证据证明所有规划应用已被部署到中国大陆工厂。[12] 需要明确工厂地点、法人主体、项目时间和实际模块；BYD 在全球供应链中的业务覆盖不能替代某个厂区的采用记录。若后续公开资料显示项目落地，应以更具体的一手材料更新阶段判断。

“采用”本身也有多个含义：评估候选平台、选定路线、签署合作、研发原型、上线某个应用、纳入车型或扩展到多厂。新闻稿所称的合作扩大可说明商业关系及规划意图，但未给出采购量、生产部署范围和长期使用数据。研究者应在每次引用中说明究竟能确认哪一环。

车载计算方案还受车型开发周期、功能安全验证、芯片供给、软件版本与售后周期约束；工厂规划工具受 CAD 和设备模型兼容、工程师工作流、现场布局变化及工厂数据权限约束。即使同一供应商提供平台，两端工程交付仍由不同技术团队、质量体系和验收责任管理，不能把供应商品牌视为已完成集成。

如果工厂规划软件与车端数据或云端模型训练共享资产，可能带来模型复用、数据治理或安全方面的交叉问题，但现有公告未披露其数据架构和信息流。[12] 因而可提出“云端研发与制造规划如何共享仿真资产”的核心问题，不能写成 BYD 已经实现工厂数据训练车载模型，或车辆运行数据已经进入产线优化。

SVSAC | sv-sac.org

平台合作还有供应商与客户之间的责任分配。平台方可能提供计算硬件、仿真引擎与开发工具；车企提供需求、车型和生产环境；本地工程团队负责模型接入、适配与测试。新闻稿不披露合同、接口控制权和数据权属，因此这只是分析可能的责任链，不能把公告的合作描述成具体的工作分配事实。[12]

要检验虚拟工厂规划的工程价值，应观察其是否在设备下单前发现布局冲突、减少现场返工、缩短虚拟调试与实体调试之间差距，并将已验收模板复用至后续工厂。需记录规划模型版本、问题关闭率、现场变更、实际调试周期和对照项目。公告没有提供这些指标，所以无法以“数字化工厂”表述推出生产率或建设周期效果。[12]

车辆算力公告中的前瞻语气还意味着项目实现时间存在不确定性。技术路线在车型量产前可能更换，供应链条件或验证结果可能导致功能调整；云端工具则可能从内部试用扩展，也可能保持在研发阶段。只引用初始公告容易把路线图当成实际配置，后续研究必须找到产品发布、交付或工厂验收层面的材料。

这一案例的地理叙述亦需克制。NVIDIA 是湾区平台供应商，BYD 是中国汽车制造企业；但公告没有指明虚拟工厂规划软件对应的具体中国制造基地。[12] 可以说明湾区技术企业与中国车企的合作路线，却不宜宣称某个大陆工厂已使用 Isaac 或 Omniverse，更不宜把所有 BYD 制造系统归为硅谷技术。

替代解释包括车企既有的数字工程能力、设计软件供应商、设备厂的仿真工具和内部工程平台。若未来公布规划周期缩短，即使 NVIDIA 工具同时参与，也需拆解其他软件和流程标准化的贡献。要识别平台作用，应比较项目使用前后工作流和工具链，或寻找相同企业内不同技术配置的项目对照。

对车端与工厂端分别设置验收更有意义。车端重点包括算力性能、功耗、热管理、功能安全、系统更新和量产稳定；工厂端重点包括模型兼容、布局和过程验证、数据同步、现场变更及与 MES/控制系统接口。两个领域可以共享部分底层计算或仿真资产，却不能用同一个“采用率”衡量。

从产业分工看，平台供应商能够提供标准化软硬件和开发环境，整车企业拥有车型定义、产线工艺和客户数据，集成商及设备供应商负责具体现场接口。该分工是否形成新的依赖或更快部署，取决于资产可移植性、供应替代、测试权限及客户工程能力。现有公告主要说明合作意图，不足以评估利润分配或议价变化。

一个可证伪命题是：当云端研发工具与工厂规划共享可复用的资产模型、且客户保有数据和格式控制权时，跨项目的设计与调试重复工作可能下降；若数据

SVSAC | sv-sac.org

接口封闭、工厂执行系统不兼容或项目停留在规划阶段，部署效益不会兑现。未来验证应区分车端项目和工厂项目，按各自的阶段、功能和验收记录建立样本。

该公告的关键研究价值不是证明“中国制造已全面融合 AI”，而是展示车端计算、云端 AI 开发与工厂虚拟规划被平台供应商纳入同一合作叙事。[12] 研究者可以借此追踪一个技术生态如何跨越产品与生产环节，同时检验每个连接的实现程度。对外宣传结构本身不是应用证据，具体工厂材料才决定是否升级结论。

综合而言，BYD—NVIDIA 材料能够支持“车企与湾区平台商扩大技术合作，且公告提出云端研发和工厂规划用途”的有限陈述；不能支持具体产线应用、生产绩效或独立因果结论。[12] 后续若出现明确部署数据，可进一步判断技术对象、责任边界和本地工程适配，但在此之前，合作路线与制造现场融合必须保持为两个不同证据层级。

第八章　机器人平台合作与中国交付：相邻事实不等于同一技术链

美的集团 2026 年中期报告提供了一组有分析价值、但必须分开读取的事实：报告称 KUKA 与 NVIDIA 在 GTC 2026 展示三年合作成果并发布 KUKA AMP；同一报告另称 KUKA 在中国市场向零跑汽车批量交付机器人，并向广汽埃安提供移动机器人解决方案。[13] 这让研究者能够观察跨国工业自动化集团、计算平台商与本地制造客户在同一企业披露中的不同接口，却不能据文本相邻就推定客户交付采用了该平台。

这种证据结构代表工业 AI 常见的商业拼接：一家设备商的能力、一个平台商的联合发布，以及本地客户的采购/部署信息同时出现，读者容易自动补成闭环。严格的技术链应能指出同一合同、产品版本、项目地点、部署模块或验收记录之间的连接。若披露没有列出这些桥接项，应把合作关系和客户交付分别作为组织事实，而非同一解决方案的端到端实绩。

报告将 KUKA AMP 称为“面向 Physical AI 时代的全新自动化管理软件平台”。[13] 该报告本身已将其定位为连接确定性自动化与意图式自动化；以下关于所需工程环节的讨论则是作者分析，并非已披露的产品实现。这类定位具有明确产品逻辑：传统机器人以程序、工艺约束和受控状态运行；面向意图的界面试图允许操作人员用更抽象的目标触发能力。两者中间必须有任务编译、权限校验、设备状态读取、异常处理和安全边界。产品名称或发布本身不说明这些环节怎样实现，因而不应把“意图式”直接等同于自然语言驱动机器人自主作业。

SVSAC | sv-sac.org

确定性自动化的优势在于行为可预期、循环稳定且便于验证，代价是换型、编程和边界条件扩展需要工程投入。意图式接口可能降低某些操作的表达成本，却会增加语义歧义与状态不完整的风险。现场系统必须判断目标是否可执行、对象是否识别正确、动作是否越权，以及执行中环境变化是否令计划失效。若这些功能仍由既有 HMI、PLC 和机器人程序承担，AI 界面的作用可能主要是翻译与编排；若由学习策略控制运动，则安全验证和异常覆盖要求明显不同。

因此，评价 AMP 一类产品不能只问“是否使用生成式 AI”，还需拆解其技术边界：模型是在生产边缘、工厂服务器还是云端运行；它是建议动作、生成任务程序，还是直接闭环控制；何种操作需要人工确认；断网、模型超时或输出不符合工艺约束时系统如何回退。美的披露将平台描述为连接两类自动化范式，但没有给出具体客户部署配置、模型运行位置或性能验收数据。[13] 公开材料尚未回答这些问题。

平台商与机器人厂商的互补资产也不对称。计算平台可以贡献训练与推理框架、仿真软件和开发者生态；机器人厂商掌握控制器、运动学、设备接口、安全认证、安装团队和既有客户关系。价值产生于双方接口，而非单方模型。若接口开放且控制器能提供可验证状态，平台能力更容易跨设备使用；若关键动作、诊断信息或参数格式封闭，用户可能获得界面便利，却同时加深对设备原厂和软件生态的依赖。

在制造现场，安装并联调一台机器人还不等于交付稳定工艺。集成商通常须理解零件公差、夹具刚度、节拍目标、工位布局、上下游互锁和安全区域；工艺工程师须判定变异是否可被感知与恢复；设备商需负责控制器及机械本体的可用性。若模型改变轨迹或任务序列，验收还需覆盖边界零件、低质量视觉、夹取失败、工件偏移、急停复位和人工恢复。该工作往往决定技术能否被纳入班组日常，而公告没有给出相应工程工时或长期故障记录。

“批量交付”具有比展示原型更强的商业含义，但仍须解释批量所对应的单位和范围。美的报告没有在相邻表述中公开零跑项目的台数、车型、工厂地点、具体工位、运行时长或验收标准。[13] 因而可将其作为公司披露的交付阶段证据，不应转写成已验证的产能提升、缺陷率下降或全厂智能化。交付数量只有与工位覆盖、实际运行周期和维修响应相结合，才能判断扩散深度。

报告另称 KUKA 向广汽埃安提供移动机器人解决方案。[13] 移动机器人所需的能力组合与固定机械臂不同：导航地图、定位、动态避障、车队调度、充电规划、载荷变化和行人与叉车共存都影响可用率。若方案包含多厂商设备，还需要调度系统对接仓储管理、制造执行系统和安全控制。一个“解决方案”标签尚未说

SVSAC | sv-sac.org

明部署边界，研究者应确认设备是否在现场运行、覆盖何种物流流程，以及方案由 KUKA、客户或本地集成商中的谁维护。

固定机器人与移动机器人项目的收益评价也应区分。固定机器人可能以替代重复焊接、搬运或装配工序为目标，需核对换型时间、质量一致性、停机损失和工装投资；移动机器人更可能改变物料配送、在制品等待和人员路线，需量测路径冲突、任务调度、等待时间及对既有物流的扰动。只比较设备购置成本会漏掉软件集成、改造停线、人员培训和备件保障，而只引用厂商所称的自动化范围又不能证明净收益。

本地交付伙伴是平台从全球产品走向中国工厂的重要互补资产。客户需要普通话技术支持、现场备件、既有系统兼容、工艺变更跟进和符合本地采购流程的合同责任。服务能力不仅是销售渠道，它承载故障分类、版本回滚、工程变更、工人培训和跨班组知识转移。若供应商只提供远程软件而现场集成由客户承担，维护成本和停机风险会在价值链中向用户侧转移；若本地集成商掌握全部接口，平台商也可能失去对终端使用质量的可见性。

集团内部的跨国组织关系进一步影响知识如何落地。KUKA 是美的集团旗下工业机器人企业，但该归属不意味着所有研发、软件、数据和售后活动集中在中国，也不意味着其技术可简单归为某一国籍。分析应区分品牌与法律实体、产品知识产权所在地、制造与配置地点、工程团队角色及客户合同主体。对客户而言，更直接的治理问题是：软件更新由谁签发，模型或日志数据由谁持有，事故时由谁提供根因分析，设备停机的赔偿边界如何约定。

更可行的部署方式通常不是让意图模型独自承担完整工艺，而是将其限制在可审查的接口层：把自然语言或高层目标转换为有限任务集合，经规则和状态检查后交给传统控制器执行；超出允许状态时停机或转人工。这是工程上可检验的架构选项，不是对 KUKA AMP 既有实现的事实描述。要判断某产品是否采用类似设计，需获得架构说明、现场操作规程或公开技术演示，并标明这是供应商披露还是独立验证。

对现场收益进行因果判断还需排除工艺成熟和项目选择效应。企业可能首先把新平台部署到产品稳定、工位规整、管理能力强的工厂，因而观察到的高利用率不一定由 AI 造成；同期的设备更新、布局优化、产品换代或班组训练也可能解释改善。可信的比较至少需记录上线前基线、部署时点、工序边界、产量与产品组合，并观察较长周期的停机、维修和返工。公司中期报告本身没有提供这些项目级对照数据。[13]

SVSAC | sv-sac.org

技术失败也可能以“局部成功”的形式出现：机器人本体按计划交付，但视觉与工件变化不匹配；移动机器人能运行，却因调度冲突无法满足生产节拍；意图界面可生成任务，安全审核和重新标定仍需专家逐次介入。此时设备不会被完全弃用，然而预期的工程师减负和跨线复制并未出现。要识别这种结果，企业披露需同时报告正常运行比例、人工干预、任务失败原因、恢复时间和维护投入，而不能只报告安装、演示或设备发货。

供应商合作公告与客户交付之间的断点还可能来自商业合同结构。平台商可能只授权软件或提供参考架构，机器人厂商承担本体和调试，系统集成商负责现场接口，制造企业则负责工艺确认和运营。若合同把“模型可用”作为交付标准，而客户预期是“工位达产”，双方对成功的定义便不一致。验收条款应把技术能力拆到可测试的场景，并规定数据访问、故障升级、版本兼容和变更责任，否则合作的品牌叙事容易掩盖责任空档。

不同客户的收益分配也取决于谁拥有稀缺互补资产。设备商通过本体销售和生命周期服务获益，平台商可通过软件生态与计算需求获益，集成商依靠工程项目和维护续约，制造客户则期待减少节拍波动或提高柔性。若客户无法导出程序、模型配置或运行数据，转换供应商的成本会上升；反之，标准接口和可移交文档会增强客户议价权。公开中报没有披露这些合同细节，因此不能从“联合发布”推断各方利润或控制权如何分配。[13]

把该案例与前述 BYD 公告对照，可以看到“同一平台供应商进入制造”有不同证据路径：BYD—NVIDIA 新闻稿给出车端芯片、云端研发及虚拟工厂规划等合作方向；美的报告则并列 KUKA—NVIDIA 平台合作和 KUKA 对中国客户交付。[12][13] 前者主要是供应商合作路线，后者增加了设备商披露的本地交付层，但二者都没有完成从技术组件到特定工厂绩效的公开证据闭环。

因此，后续案例比较可采用“接口链”而非品牌链：记录平台、机器人、集成商、工厂工艺和售后服务各自提供何物；再追踪数据、指令、异常和责任如何跨接口流动。若平台能力只能在原厂工程师驻场时工作，说明知识尚未充分转移；若本地团队能独立调试、诊断和恢复，才有更强的可复制性证据。该判断应建立在部署观察和维护记录上，而非企业国籍或产品发布所在会议。

就现有公开材料，最稳妥的结论是：美的中报确认了公司所述的 KUKA—NVIDIA 合作发布，并分别披露 KUKA 在中国市场的机器人交付与移动机器人方案；中报没有证明这些客户交付使用了 KUKA AMP，也没有给出独立绩效评估。[13] 这不是案例的缺陷，而是产业研究需保留的证据边界。下一步有价值的材

SVSAC | sv-sac.org

料将是项目配置、工厂与工位、交付验收、持续服务和故障记录，才能判断合作是否转化为可持续的制造能力。

第九章　知识吸收不是下载：本地集成能力如何形成

跨境技术的落地常被描述为知识流动，但“流”容易制造无需学习成本的错觉。Branstetter 与 Maskus 对国际知识流研究的回顾强调，技术知识常具黏性、依赖人员与隐性能力；接收方须掌握基础知识并投入能力建设，转移方也须积极配合。[14] 据此类知识转移机制对机器人、仿真和工业 AI 作分析性延伸，获得模型权重或软件接口只是接触知识，尚未形成理解、修改、诊断和改进技术的能力；Branstetter 与 Maskus 并未直接研究这些工业部署。

至少要区分四个组织步骤：识别外部技术与本企业问题的相关性；理解其原理和前提；将知识转成适配本地设备与工艺的配置；在生产中验证并将经验留存。某一环节中断，会造成“买到了但不会用”“能由供应商做但客户不能维护”或“单点可运行却无法复制”。这个分层是对技术吸收过程的分析框架，而不是对本篇所讨论案例企业内部能力的实测结论。

“接收方”本身也不是一个统一主体。制造企业的工艺部门掌握问题定义与质量窗口，自动化部门掌握控制接口和安全逻辑，设备商掌握本体与控制器，软件集成商掌握数据管道、模型部署及版本管理，操作人员掌握异常发生的现场知识。若各方只沿采购合同分别交付，技术诀窍会分散在供应商的工程师个人和临时项目资料中，难以沉淀为企业能力。

跨职能协作的关键不是建立一个笼统的“AI 团队”，而是让过程知识能被机器接口表达、机器状态能被工艺人员理解。举例而言，控制团队可能记录关节误差和碰撞信号，工艺团队关注装配偏差、材料批次和返工原因；只有把这些变量映射到同一任务与故障分类，才能判断策略性能变化来自模型、夹具、工件还是操作流程。缺乏共同数据定义时，跨专业会议容易退化为各自提供局部解释。

系统集成商在这一结构中承担翻译与协调的“边界跨越”角色：把模型输入输出映射到 PLC、机器人、视觉及 MES 接口，把客户的产线需求转换成可测试的配置，并将故障信息传回设备和平台供应商。其价值不只是安装，而是处理一个系统边界内的异构语义和责任。如果集成商没有过程工程能力，它可能只能完成协议连通，无法处理节拍、质量和异常恢复；若过度依赖单一集成商，客户又可能失去维护与更换服务商的能力。

SVSAC | sv-sac.org

知识吸收也具有明确的先决条件。团队需要足以理解传感器数据、运动控制、工艺约束和统计验证的基础知识；这并不要求每家工厂自行训练基础模型，却要求有人能识别训练分布与现场分布的差别、检查坐标变换和传感器校准、解释异常日志，并知道何时停止自动化。基础技能薄弱时，模型输出的偶然成功更易被误认作稳定能力，失败则容易归咎于“算法不够先进”而错过工装或数据问题。

现有研究可为这类组织机制提供背景而非直接的制造业结论。Braojos 等对西班牙企业的同行评议研究考察组织间 IT 整合与知识吸收/释出关系；本篇依据其可读摘要指出该研究把 IT 连接与知识流作为组织层面问题，但因全文未取得，不使用其样本、估计值或具体效应方向来支撑本地制造判断。[3] 这一区分避免把文章题目或摘要误当成本章所需的中国工厂证据。

技术转移还需要转出方配合。复杂平台的错误可能涉及模型、驱动、固件、机械磨损或数据同步，若供应商不提供必要日志、接口文档和故障升级通道，客户即使拥有高技能人员也难以定位根因。相反，能够访问诊断信息、获得版本变更说明并在合同内安排联合排障，才使接收方能逐步把隐性知识变成标准操作。转移并非设备交付的自然副产品，而取决于双方对知识共享和控制边界的安排。[14]

知识的“吸收”与“释出”是同一关系的两面。外部平台商输入算法、软件和接口规范；本地工程师输入设备限制、工艺参数和异常样本；企业内部团队再把调试经验沉淀为通用规范，并可能反馈给集团其他工厂或供应商。若本地只提供数据与工艺专家时间，却没有获得配置权、文档和学习机会，协作可能提高供应商的产品知识而不增加客户能力。反向流动要通过责任、访问权与文档交接具体识别。

在工厂中，人员学习通常发生在“偏离标准状态”的处置，而非成功演示。常规周期由自动化系统完成，真正暴露知识缺口的是零件变形、相机遮挡、夹具松动、设备重启、网络中断和批次切换。若每次异常都由原厂工程师远程登录修复，系统的可运行性不代表客户已掌握故障诊断；若本地班组能依照手册定位、恢复并记录复发原因，才显示组织能力在积累。

因此，维护记录是检验知识转移的核心资料。记录应能连接软件和模型版本、故障代码、工件批次、操作模式、停机起止、临时绕行方案、修复责任人和复发情况。只保存工单文本而缺少系统状态，难以区分模型回归、传感器漂移、机械松动和操作误差；只保存遥测数据而没有工艺语境，也难以解释故障对质量和产量的影响。数据治理的价值在此不只是合规，而是建立可累积的故障知识。

SVSAC | sv-sac.org

跨班组交接进一步决定学习是否可复用。白班工程师现场调参、夜班操作员只看到设备恢复，可能导致同类问题重复出现；若更新内容没有变更单、验证记录和风险提示，人员轮换会使经验失效。较成熟的知识闭环会把变更转成受控版本，把关键异常加入培训与模拟，并设置回退标准。此举既能减少重复排障，也避免将未经验证的“现场窍门”传播成新的安全风险。

集成能力本身还须经过分层验证。接口连通只证明信号可传；单件测试证明有限样本可完成任务；工位测试才纳入夹具、节拍和互锁；跨班次运行检查人员交接、恢复与稳定性；跨产品和跨工厂复制则要求适配工艺变异和设备差异。验证阶梯不是线性升级的保证：更换工件、灯光或控制版本都可能令既有结果失效。研究报告应指出验证级别、样本边界和变更条件。

评价组织吸收能力不能只看培训人数或数字化项目数量。更接近能力的观察指标包括本地团队独立调试比例、故障定位时间、无需供应商介入的恢复比例、参数变更可追溯程度、跨产品复用时新增工程时间，以及重要知识是否由至少两名员工掌握。指标需说明分母、观察期和工位复杂度，否则把简单工序的高自主率与复杂工序直接比较，会误判差距。

部署后能力若没有随时间提高，可能有多种原因。任务输入不断变化，供应商频繁升级，基础数据质量差，员工流动快，或客户组织没有为维护留下工时，都可能阻断学习。也可能是应用本身并不适合该任务，无法通过更多培训解决。区分这些解释需要观察变更历史、故障构成、人员技能和任务经济性，而不能将一切失败归为“吸收能力不足”，否则会把产品设计缺陷和供应商支持不足转嫁给用户。

供应商依赖也并非必然等于坏结果。对于安全关键、更新复杂且客户使用频率很低的设备，长期由原厂维护可能比内部自建团队更经济可靠。关键在于依赖是否可见且有替代安排：接口与日志是否能导出、服务级别是否明确、关键备件是否可获得、供应商停止服务后能否维持安全运行、客户是否保留必要的系统管理权限。掌握所有源码并非唯一自主标准，具备可执行的持续服务与退出方案同样重要。

反过来，强调“本地化”也不必然形成知识外溢。销售和交付团队本地雇佣、服务器位于本地或在中国设立服务中心，分别说明运营落点，却不能单独证明工程决策、模型改进或故障诊断能力已经转移。需要追踪本地员工实际执行的工作、权限范围、训练方式、复杂故障是否仍需境外总部处理，以及本地团队能否将案例转化为产品和工艺改进。

SVSAC | sv-sac.org

集团内部迁移与供应链转移也应分开。BMW 关于 Debrecen 参考沈阳流程的公告属于同一跨国企业网络内的生产布局与流程经验转用，而不是独立中国供应商向匈牙利客户扩散平台技术。[11] 集团拥有共同标准、管理系统和人员调动通道，知识转移成本可能低于无股权关系的供应商合作；但只有有时间记录、人员角色、文件版本和当地适配过程的材料，才能判断究竟转移了设计、工艺经验还是正式技术模块。

由此可提出一组可反驳的机制命题：有过程工程师和自动化能力的接收企业，更可能把外部平台从试点转成稳定工位；客户本地团队获准访问诊断数据和参与联合维护的合作，更可能缩短本地团队独立恢复时间；但高复杂度或低使用频次任务可能继续由供应商承担。验证时可比较类似设备与任务在支持强度不同的工厂中的学习曲线，并控制工艺复杂度、员工流动和设备年龄。这里提出的是研究设计，不是已完成的企业实证结论。

对中国制造的具体判断仍须回到企业和工厂层材料。国家层面的工程师供给、产业规模或设备制造能力不能直接推出某家企业具备 AI 集成与维护能力；同样，跨国平台的本地销售也不证明知识已被吸收。只有能够跟踪岗位技能、配置权、诊断记录、生产验证和跨班组复用，才能区分“买到技术”“供应商替客户部署”与“客户获得可持续能力”。这一层级差异决定技术合作是否成为长期产业能力。

第十章　从试点到复制：跨工厂扩张的工程经济

“可复制”经常被用于描述工业 AI 平台，但工厂间复制并非把同一软件包安装到更多服务器。项目必须把应用对象、机器接口、工艺边界、现场服务和验收标准一并迁移。复制成本下降，意味着后续工厂不必重新发现同一类问题；如果每个新厂仍需全套重新建模、逐设备调参和重写安全逻辑，扩张的只是项目数量，不是技术的边际可移植性。

复制对象可分为四层：可复用的软件组件；机器或产线的工程模板；工艺规则与故障知识；以及供应商与客户共同执行的部署流程。前两层较易封装为代码和文档，后两层通常依赖经验、现场判断与组织关系。只证明数字资产可复制，不能说明本地工程团队能够适配，也不能证明部署后的运营能力会随之复制。

跨厂迁移的工作量可按“共同核心+现场差异”理解。共同核心包括机器人驱动、通信接口、仿真资产结构和故障分类；差异项包括机械型号、坐标和相机视角、零件批次、厂房布局、班组操作及安全规则。工程团队需先识别哪些变量可

SVSAC | sv-sac.org

参数化，哪些需要重新测量，哪些变化会改变任务本身。如果差异没有显式建模，所谓模板会把默认条件隐藏在配置文件和工程师记忆中。

以机器人装配为例，迁移模型不应仅报告权重文件或目标位姿，还应包含工具坐标、相机内外参、工作空间限制、接触策略、力矩阈值、工件容差范围及动作超时处理。视觉系统更换镜头或安装位置，可能导致姿态估计系统性偏差；夹具磨损也会改变接触几何。版本化资产应把这些参数同基准工件、校准记录和验收脚本关联，方能判别跨站差异来自软件还是机械条件。

虚拟工厂规划的复制同样有模型治理成本。布局、设备几何、管线和工艺步骤若采用不同坐标系、命名和更新规则，多厂模型就只能由项目团队手工拼接。NVIDIA 对富士康 FODT 的案例强调连接 Omniverse/OpenUSD、MES/SFC 和工厂运营信息，并叙述台湾到墨西哥的迁移。[8] 这说明跨国复制涉及数字资产与业务系统连接，但案例页没有披露迁移的总工时、后续维护成本或独立基准，不能据此计算其复制效率。

所谓“数字孪生”也需考虑实物和模型之间的持续校准。新设备入场、工位改造、工具更换、产线节拍调整后，虚拟模型若未更新，仿真结果可能逐渐偏离现场。跨厂模板需要规定模型所有者、变更触发条件、版本审批、现场扫描频率和失配纠正流程。一个大型首厂模型的高精度并不自动产生低成本扩张；若模型与现场持续偏离且没有明确更新责任，会积累维护工作。这里借用 Sculley 等将“技术债”作为机器学习系统维护权衡的隐喻，但本篇并未对该维护积压作严格度量或案例实测。[15]

实体机器人部署的关键瓶颈常在现场几何与动态条件。首个工厂可能拥有人工精调过的夹具、固定零件批次和工程师驻线；第二个工厂的零件供应商、工位光线和地面状况都不同。若系统只在“黄金样件”运行，实验室成功率不能代表跨厂稳定性。迁移验证应预先定义变化包络，对批次、光照、工装偏差和设备状态作分层，而非仅在新站重复演示一件样品。

场景间异质性决定平台复用是否成立。重复搬运的静态工位可能以位置校准和抓取点映射为主要差异；柔性线缆装配需要处理形变、摩擦和接触反馈；物流机器人则依赖地图、车队密度和动态障碍。把“机器人”作为统一部署单位会掩盖任务结构差异。供应商可以共用底层计算和管理工具，但每类任务仍需独立的感知、规划、控制和恢复验收。

软件升级与工厂变更之间还存在时序冲突。云端平台或模型可能按更快节奏更新，而生产线验证、停线窗口和安全审批周期更长。若新版本自动覆盖现场配置，模型改善可能带来接口回归；若客户长期冻结版本，又可能累积安全修补和

SVSAC | sv-sac.org

兼容性风险。可控模式要求明确发布通道、预生产验证、回滚窗口、工厂差异清单以及跨版本追踪，不能将消费软件的持续部署方式直接套用于生产控制。

跨境服务为复制增加一项经济变量：首厂项目的能力不只来自软件，还来自供应商工程师能否赴现场、当地是否有备件和认证人员、客户是否拥有足够停线窗口。Fii—NVIDIA 案例涉及台湾工厂经验向墨西哥工厂的流程迁移叙述，但并不能证明大陆工厂采用了同一系统。[8] 其启示是迁移关系必须把技术资产、人员支持和运营地点分开描述；地理跨越越大，语言、时区、劳务与采购流程也可能增加边际服务成本。

集团内部流程复制与供应商向不同客户销售产品，面对的边界不同。BMW 关于 Debrecen 的公告将部分装配车间和输送布局称作参考 Lydia 流程，并将另一项手指/梳状物流结构联系到 Leipzig。[11] 同一集团可共享工程标准和管理通道；跨企业销售则必须面对客户不同的控制系统、供应商组合、合同责任和知识产权边界。前一种迁移不能直接用来推断平台对陌生客户的通用性，后一种销售也不能假定集团内部的文档与信任已存在。

复制经济可用边际工程量而非发布数量检验。对于第 n 个部署，记录从现场勘察、数据映射、校准、接口开发、安全测试到稳定运行所需的人时，并按工艺复杂度、设备异质性和运行时间分层。若新项目数量增长而每站集成工时不降，说明需求在扩大但标准化能力有限；若工时下降而故障率、返工和供应商驻场增加，节省可能只是把成本推迟或转移给运营环节。

复制效果还要观察“尾部条件”。平均任务成功率可能掩盖少见但高损失的部件错位、机器人碰撞、日志缺失或停线恢复失败。多厂应用应记录故障分布、最差站点、恢复时长和版本回归，而不是只报平均值。对不同工厂的比较至少需保留共同任务定义、暴露量、生产批次和班次信息；否则低故障率也可能只是该站运行时间短、任务少或异常被人工提前剔除。

供应链可移植性也依赖设备替换能力。若一个应用只与特定机器人品牌、视觉相机或专用控制器兼容，企业跨厂采购其他设备时，平台迁移就可能需要重新做运动映射和安全认证。标准化接口能降低替换成本，但标准本身不保证语义一致：同一“停止”命令在安全 PLC、控制器和上层调度中的优先级与复位逻辑可能不同。验证需查看具体数据模型和故障行为，不只检查接口是否采用通用协议。

企业组织结构会改变复制路径。中央工程团队可以建设公共组件和配置治理，地方工厂保留工艺参数与异常处置权；这种联邦结构平衡标准化与现场适配，但需要明确哪些参数可由工厂修改、何种变化必须回总部审批。完全集中会

SVSAC | sv-sac.org

形成排队瓶颈和远程团队不了解现场的风险，完全分散则可能造成版本碎片化和重复开发。比较案例时应跟踪决策权，而不是仅看系统架构图。

还必须把复制失败纳入观察样本。项目终止、推迟扩展、重新采购传统自动化或只保留人工复核，可能由安全、节拍、设备兼容、财务回报或运维组织等不同原因引起。只观察公开展示的成功工厂，会产生幸存者偏差。可靠评估需记录入选和退出项目的条件，并比较原计划站点、实际部署站点与未部署站点；否则无法知道是技术模板有效，还是企业有选择地只在最易成功的环节复制。

由这些机制推出的可检验判断是：当工艺任务稳定、设备接口可标准化、变化可参数化、客户保留配置和故障数据权利时，跨厂复制的新增工程工时应随重复部署下降；对于接触复杂、品种变化大或服务到达慢的任务，维护与恢复成本可能抵消模型复用收益。检验需同步追踪代码复用率、工程人时、现场调试周期、跨班次故障、客户自行恢复比例及未扩展项目，而不是只数合作工厂。

目前公开案例能展示一些复制要素，却没有提供统一、可比的工时与稳定运行数据。Foxconn 案例给出跨地域数字孪生与业务系统连接叙述，BMW 材料提供集团内流程参照，机器人论文给出固定平台实验和特定任务的实机结果。[7][8][11] 三者各自处于不同分析单位，不能合并成“技术跨厂复制已成熟”的总体结论。比较的价值在于提出各自应补的观测指标，而非把不同阶段拼成单一成功率。

平台供应商和制造客户的收益亦可能随着复制阶段变化。首厂的集成工程与定制成本高，设备商或集成商可能承担较多不可复用工作；规模部署后，软件许可、模块更新或服务合同可能成为主要收入来源；制造客户则只有在工时、停机、质量或柔性改善超过全生命周期成本时受益。若合同不明确配置权、升级责任和数据访问，规模扩大可能增加客户锁定而非提高净价值。

第 10 章据此把复制判断落在新增工程量、恢复、知识保留与退出选择，而非演示点数量。初期费用未降但形成可审计模板和本地服务网络，仍可能具有后续价值；扩张若持续依赖驻场、人工兜底或封闭资产，则不能仅凭站点增加认定可持续。判断须同时保留质量与运营后果，不能只追求工程工时下降。

第十一章　制造现场怎样验证：从模型成功率到运营指标

机器人论文中的任务成功率不能直接代表工厂绩效，因为研究单位、时间边界和失败定义并不相同。制造验证首先要规定决策单位：单次动作、一个零件、一个工位循环、整线班次，还是一座工厂的月度交付。相同模型在这些单位上的

SVSAC | sv-sac.org

表现可完全不同；结论须指明它回答的是“会不会完成动作”“能否稳定运行”还是“是否改善业务结果”。

需求节拍（takt time）是可用生产时间除以客户需求，表达需求要求的目标节奏；它不是单工序实测耗时，也不是模型推理延迟。[16] 例如，某线达到需求节拍并不证明每台设备都需以同样速度连续动作，因为线内缓冲、工序并行和产品组合都会改变各站负荷。工程评估应先确定需求时段与计划可用时间边界，再讨论 AI 工位是否妨碍整线交付。

Cycle time 则是实际测得完成一个零件或工序所需的时间；effective machine cycle time 还可能纳入上下料以及按批量分摊的换型时间。[16] 论文中单次策略执行时间并不等于工厂 cycle time：物料定位、夹具闭合、PLC 握手、质量确认和安全联锁都可能加入周期。若一个控制器更快，但上游等待或下游检验成为瓶颈，整线吞吐不会按单机速度同比提高。

端到端 lead time 回答另一类问题：物料或订单从流程起点到终点经过多久。价值流图会把加工时间与等待、搬运、库存等过程同时呈现，并可区分当前状态与目标状态。[16] 因而“模型令某动作更快”不自动表示订单交付更快。部署前后比较应定义起止事件、处理在制品和停机等待的办法，以及观察期内的订单或产品类型。

可用率、运行率与停机恢复也不能混成一个比例。计划运行时间、非计划停机、换型、维护、饥饿/阻塞和质量返工可能按企业制度采用不同分类。若自动化单元完成动作的时间很短，但需要频繁复位，单次成功率高仍可能伴随低可用率。公开案例未提供可统一套用的指标定义，因此比较不同企业的“利用率”前必须核实分母和停机分类。

对于 AI 系统，故障暴露量尤为重要。应记录策略实际执行的动作次数、生产零件数、运行小时、切换批次和触发的异常数。只报成功次数会掩盖系统是否遇到过困难场景；只报任务成功率也可能将重复尝试、人工重置和剔除件从分母中移除。公开论文的受控试验适合回答特定任务条件下的可行性，而产线评价须补充运行暴露和失败处置过程。

成功口径要把首过合格与最终合格分开。若策略先失败、人工纠偏后工件仍合格，质量部门可能计入最终良品，自动化系统却没有独立完成任务。需要并列记录首过合格率、返工率、报废率、质量偏差类型和人工介入。若质量检测本身也由 AI 承担，则还需有独立抽检或传统测量基准，以避免系统用自己的判定证明自己的成功。

SVSAC | sv-sac.org

故障恢复时间不宜只报平均值。短时可重试的抓取失败和需技术人员重新标定的控制异常，应分层报告中位数、分位数、最长持续时间及停线损失。某类长尾故障即使发生频率低，也可能决定是否允许无人值守或跨班运行。验证计划可把安全风险、质量影响和生产中断分别作为严重度维度，而不是把所有“失败”编码成同一二元变量。

为保证前后比较有意义，需固定或记录产品组合和客户需求。多品种订单中，工序时间和异常概率会随型号、批次及定制选项变化；若 AI 部署后产品结构同时转向简单型号，表面周期改善不能归因于技术。应按产品家族与关键工艺分层，必要时报告加权平均及各层结果，同时说明权重如何定义。

资本与工装变化同样是重要混杂因素。新机器人可能与 AI 部署同时更换，线体布局、夹具、传感器、光源或上料机构也可能一起升级。若新系统表现更好，改善可能来自机械改造而非模型。项目记录应列出同期设备、工艺和维护变化；可用分阶段部署、同类未改造工位或功能关闭/开启对照分解贡献，但现场安全和生产要求优先于实验性随机化。

把模型与传统自动化作比较时，比较对象需具有相同的任务边界和质量标准。人工作业、固定程序机器人和学习型策略各有培训、换型、监督和安全成本；将传统方案的成熟运行与新方案的初始磨合直接比较，会系统性低估或高估某一方。至少应观察从稳定基线到完整部署的过渡期，并分别报告调试期和稳态期表现。

故障日志必须与生产数据有共同时间基准。模型输入、控制器状态、PLC 事件、MES 工单、质量记录及人工接管时间若使用不同钟表或标识，事后无法判定哪个事件先发生。任务 ID、设备 ID、工件批次、模型版本和操作模式需要在受控权限下关联。若数据保留受限，可采用脱敏事件摘要，但须保存足够信息重建因果顺序和复发模式。

测量设计还需处理样本选择和删失。试点可能只挑选容易的工位；被取消的项目与运行时间很短的站点往往没有公开报道。安全停机后手工完成的工件、供应商驻场期间的运行和现场工程师的例外处理均需纳入观察。若项目终止，不能把停止前的最佳周期当作稳态结果；应说明观察截止日和未达到验收条件的原因。

设备安全是独立的终点，而不是生产成功率的附属项。需明确机器人工作空间、急停与防护联锁、意图或策略输出权限、人工授权层级及断网/超时行为，并记录危险事件和近失事件。模型达到高成功率不意味着安全已被证明；相反，系

SVSAC | sv-sac.org

统可通过保守的速度上限和人工确认维持安全，却牺牲节拍。生产验证应将安全约束写入功能边界，而不是事后用质量和效率指标代替。

人力投入应拆为直接操作、监督、调试、维护和异常响应。自动化可能减少重复动作，却增加程序员和设备工程师的现场支持；只计算被替代岗位会漏算新增劳动。对于多班次运行，还要记录夜班是否有能力恢复、白班专家是否持续远程支援，以及培训和交接时间。评价单位应是总劳动工时及岗位技能结构，而不只是单个操作员的手工动作时间。

成本与时间的分母也要按运行阶段整理。一次性集成和校准、计划停线、模型/软件订阅、推理计算、备件、服务合同、复训和回退方案，属于不同成本项。若 AI 与新设备同时采购，应将整套资本支出和传统替代方案比较，不把“模型”视作零成本，也不将实验团队的人力排除。没有客户合同和项目账目时，可以提出成本表结构，不能据公开发布计算 ROI。

一种可行的评估是阶梯式分阶段上线：先在单一工位建立安全基线和故障分类，再在受控生产窗口验证需求节拍、质量和恢复，随后扩展到相邻工位与其他班次。每一步都设定继续、暂停和回滚阈值。只有在每阶段持续进行安全评估与监测，并明确触发停线和回滚的条件时，分阶段上线才可能在控制风险的前提下观察系统行为；这不能保证整线安全。受需求季节性、员工熟练度和设备差异影响，阶段比较仍需记录同期变化。

若有相似的多个工位，可用匹配对照而非简单前后对照。依据工艺、产品、设备年龄、班次和基线故障率匹配，比较 AI 介入站与未介入站的变化；当条件允许，轮换部署顺序有助于分离时间趋势。此方法仍不能消除所有选择偏差，特别是管理层往往优先选出最有准备的工位。研究报告应说明选择规则与不可观察差异，而不是把配对形式等同随机试验。

四类材料的可比单位不同。IndustReal 报告受控装配任务及连接链，能定位滑脱、楔紧等实验内失败；Foxconn FODT 材料描述平台、执行系统与数据连接，具体热分析加速仍是供应商案例陈述，整体时间缩短则为预期。美的中报能定位公司披露的机器人交付与方案，不能替代客户工序验收。BMW 资料中，Lydia 规划与德布勒森具名流程参照比笼统合作更能定位迁移对象，但启动期自述仍不能识别长期收益。比较的不是材料类型谁一概更强，而是哪种材料能回答任务可行、已用何物、迁移何物或效果多大中的哪一问。[7][8][13][9][11]

Lean Enterprise Institute 的词典可帮助界定 takt、cycle、lead time 和换型等制造术语，但不是 AI 应用效果证据。[16] 完整验证应把需求目标、单站实测、整线流动、停机恢复、质量、劳动与成本共同纳入，并预先写明数据来源和失败处理

SVSAC | sv-sac.org

规则。若企业不公开这些运营资料，结论应停留在功能演示或部署阶段；这不是否认其价值，而是限制研究者对运营影响的判断。

第十二章　工艺异质性：制造 AI 与相邻数字规划不是同一类部署

“制造 AI”不是单一任务类别，且并非所有相邻数字规划工具都是 AI。接触装配中的学习策略和智能物流功能直接涉及 AI 决策；虚拟工厂规划可能依赖 3D 引擎、仿真和数据接口而不含 AI 组件。本章比较前两类 AI 应用与后一类相邻数字化机制，分别讨论其数据、失败后果和验收单位，避免将平台连接或规划软件计入 AI 部署率。

接触装配的核心不确定性来自局部几何和力学交互。插接、对孔和柔性件抓取要求系统感知位置误差、接触状态、摩擦和零件变形。IndustReal 在 Franka 平台研究高接触装配，并通过仿真奖励、课程采样和策略层动作积分器处理误差累积。[7] 其研究价值在于展示一种特定控制链能够跨越仿真与实机任务，不等于已经解决高速量产中的夹具寿命、质量批次与长期磨损。

这类任务是否适合学习策略，取决于失败能否被安全、低成本地观察和恢复。轻微偏孔可允许退回并重新定位；零件被楔紧、夹具损坏或工具与人员发生危险接近，则不能简单按“再试一次”处理。验收需预先区分可重试偏差、可回退故障和必须急停的危险状态，并定义每种情况的可感知信号、授权动作和质量隔离方式。算法的探索能力不应由生产线承担未经限制的风险。

装配任务还受到工艺窗口影响。柔顺控制可以容忍一定位置误差，但力阈值过低会导致未插到底，过高会损伤脆弱部件。批次公差、材料温度和表面润滑改变接触力学，因而同一轨迹对不同部件未必安全。实验平台所报告的特定间隙和任务成功率只能对照其零件和控制设置；现场应用需通过测量工件分布、夹具偏差和损伤率重新界定适用范围。[7]

厂内物流的主要问题往往不是单台移动机器人能否导航，而是车队如何与生产节奏、物料优先级和共享通道协调。移动机器人可能在独立测试路线运行正常，但当叉车、行人、临时堆料和多个任务同时出现，调度延迟会积累到工位缺料。当车队调度需与生产和物料系统协同时，系统才需要在仓储与制造执行系统之间交换任务、库存和完成状态；实施时还须与人工道路管控和安全规则衔接。单车定位精度不能替代对全物流网络交付的观察。

SVSAC | sv-sac.org

物流自动化还会改变物料流而非单纯替代搬运。若配送批量变小、频率提高，工位空间和缓冲策略可能改变；若车队调度优先某产品族，也可能挤占其他生产路线。部署前需绘制物料和信息流，测量缺料等待、在制品、路径冲突与人车混流，并观察变更后这些指标是否转移到其他环节。KUKA 对广汽埃安提供移动机器人方案的披露确认有此类方案陈述，但未列出具体工艺配置和运行数据。[13]

因此，固定机械臂与移动机器人不能以同一套验收脚本互换。机械臂需验证抓取、接触、精度、周期、工具换型和安全空间；移动机器人需验证定位连续性、地图更新、避障优先级、充电策略、拥堵和任务调度。两者可能共享云端监控、车间地图或机器人管理软件，却仍需要不同传感基准、故障分类和责任分工。把共同平台当作共同验证结果，是软件模块可复用与整机工艺可复用之间的概念混淆。

虚拟工厂规划是与制造 AI 相邻的数字工程机制，常发生在设备采购和建设前。几何模型和仿真可分析布局冲突、设备可达性、物流路径、维护空间或操作员视线，但其本身并不意味着应用了 AI。规划工具的价值需在现实装机前验证为减少返工、缩短调试或改善方案比较。BMW 关于 Lydia 的公告称其使用 Unreal Engine 进行规划与仿真；这是数字化规划流程的企业披露，不是 AI 部署证据，也不是相对于未用工具工厂的独立效果估计。[9]

数字规划系统的主要失效模式是模型与现实不同步。设备几何简化、工程变更漏录、制造商模型版本不一致或工艺数据缺失，会使碰撞检查和物流仿真给出看似精确但条件错误的结果。项目需把模型误差作为工程风险，明确数据来源、可信等级和最后校准日期，并在设备变化时重跑相关验证。可视化精细程度不是模型真实度的替代指标。

不同工厂的虚拟模型也难以仅凭渲染格式互通。传感数据、设备语义、坐标框架、工位命名和过程状态都会影响仿真与 MES、设备控制和工程数据库的连接。NVIDIA 的 FODT 案例强调 Omniverse/OpenUSD 与 MES/SFC 及运营数据的衔接，支持该个案存在数字资产和业务数据接口的描述；这些组件本身不是 AI 证据。[8] 案例未报告跨客户或供应商的互操作覆盖率，也不能由单一客户案例推出普遍能力。

Lydia 与 FODT 不能合并为通用 AI 方案。BMW 关于 Lydia 的数字规划明确采用 Unreal Engine；NVIDIA 的 Foxconn 案例涉及 OpenUSD 和运营系统连接，并明确介绍 PhysicsNeMo 的 AI 热分析。[8][9] 后者不能被概括为没有 AI 证据，也不能

SVSAC | sv-sac.org

反过来把所有几何、MES 或数据接口都称为 AI。各组件须按任务归属；不得移植供应商名称、把规划等同生产控制，或从一家工厂推断全集团部署。

BYD—NVIDIA 公告提出的内容也处于不同阶段：车端计算和云端 AI 研发方向之外，还提出 Isaac、Omniverse 用于虚拟工厂规划。[12] 车端和云端研发明确属于 AI 相关方向；虚拟工厂规划则是数字工程计划，不能仅因工具属于 NVIDIA 生态或带有仿真能力就判定为 AI 部署。公告未指明规划所对应的具体生产基地。比较时应把产品 AI、工厂规划、设备集成和实体运营作为不同事件。

三类任务对“实时”的含义也不同。机器人策略需在动作控制闭环内满足延迟和稳定性要求；物流调度需在路线冲突和任务到达变化下及时重排；虚拟规划可在建设前离线计算，但设计变更仍要赶上采购和施工节点。仅报告推理速度不能说明信息更新、规划审批和现场执行是否及时。时间约束应根据实际决策周期定义，而不是把 AI 模型的单次推理延迟当作整套流程效率。

反馈信号也随任务变化。装配策略可利用相机、关节状态或接触信息；移动物流系统需融合地图、定位、通道占用、任务优先级和电量；数字规划需要设备参数、工程变更、产能假设及现场扫描。每种反馈都可能滞后、缺失或错误。若决策系统没有显示输入的新鲜度和缺失状态，操作员就难以区分模型判断与过期数据，因此验收应涵盖数据质量与降级行为。

维护责任也因任务而异。装配单元常由自动化与工艺团队共同排查机械和策略；移动机器人故障可能属于设备、网络、地图或调度软件；数字孪生偏差则需工程设计部门更新模型和工艺版本。将全部维护交给“AI 团队”会形成责任黑箱。案例研究应识别谁收到告警、谁可修改关键参数、谁批准恢复生产，以及故障是否回流到原平台开发者。

学习能力的收益亦不对称。接触装配的策略可能从多样示范和扰动中获益；移动机器人地图和调度更多依赖场景建模、规则和运行反馈；虚拟规划主要受制于模型与工程数据质量。某一类任务的模型更新收益不能推出其他任务也需要在线学习。部署前应说明策略何时更新、使用何种数据、由谁批准、如何回滚，以及更新后是否重新进行安全与质量验证。

产业采购合同最好按功能风险分层。装配采购可将任务成功、质量损伤和恢复时间纳入验收；移动物流合同可规定任务完成、交通安全、可用时段和调度接口；虚拟规划合同则需规定模型交付、数据更新责任、冲突识别和现场变更复核。所有方案还应区分硬件保修、软件服务和工艺结果责任。若合同只写设备交付或平台上线，客户对整线效果的预期就可能超出供应方承诺。

SVSAC | sv-sac.org

部署替代方案应按任务特点比较。装配可能继续采用精密夹具、视觉引导或固定程序；物流可优化路线和班次、增加缓冲或采用不同运输设备；规划可使用传统 CAD/BIM、实体布局试验或现有仿真工具。比较要包括切换成本和未来产品变化，不能只把新 AI 方案与“完全人工、完全低效”的假想基线对照。技术的价值在于相对于实际可行方案改善约束，而非与抽象的无技术状态相比。

这组差异可形成任务匹配命题：闭环可观测、失败可恢复且变化能被参数化的装配步骤，更可能适合学习策略辅助；路径共享、动态阻塞和全局优先级较强的物流系统，瓶颈可能在调度与流程协调；虚拟规划的收益则取决于模型更新纪律和工程变更闭环，并不必然来自 AI。检验时应把是否存在明确 AI 组件、任务类型、信息条件和失败成本作为解释变量。

因此，第 11 章的证据比较须与本章任务差异配对：装配先检验接触误差能否感知并恢复，物流先看共享通道与任务优先级是否形成全局瓶颈，规划则核模型是否及时进入工程变更。机械臂的成功率不能回答后两类问题，三维场景或 MES 连接也不能替装配策略通过现场验证。跨境复制只有在对应任务、接口和处置权限保持可用时才有明确含义；平台相同不是共同验收结果。[7][12][8][9][11]

第十三章　工厂数据与跨境协作：部署位置不等于治理安排

工业 AI 运行会产生多类性质不同的数据：工件图像与缺陷标注、机器人轨迹和控制状态、生产订单与设备节拍、员工操作或告警记录、模型参数和日志。它们分别揭示产品设计、工艺能力、人员行为或软件内部状态，访问主体和泄露后果并不相同。把所有信息笼统称为“工业数据”，会令技术架构无法对应到具体治理责任。

项目启动时应绘制数据流，而非只确认服务器在哪个国家。需要记录数据由哪种传感器或系统生成，经何种网关、标注工具和训练流程处理，向哪些供应商或集团团队提供，保留多久，是否用于其他客户模型，以及出现事故如何取证。生产控制日志、员工视频、匿名化统计和模型权重可能经过不同路径，不能由单一云端/本地部署标签替代。

中国《促进和规范数据跨境流动规定》第三条规定，在国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集产生、向境外提供且不包含个人信息或重要数据的数据，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。[17] 该条豁免的是列明的制度程序，不是免除其他数据安全、个人信息保护等适用义务。对跨国制造而言，不能把所有生产数

SVSAC | sv-sac.org

据视为一律不得出境，也不能因数据来自工厂就默认适用该条。数据类别与实际内容是判断前提。

同一规定第二条要求数据处理者按相关规定识别、申报重要数据；未被相关部门或地区告知、公开发布为重要数据的，不需要作为重要数据申报出境安全评估。[17] 这说明研究者不可凭“工艺数据很敏感”或“只是机器遥测”自行作法律分类。企业需按适用规则与主管要求识别数据，并分别处理个人信息、重要数据及其他生产信息。本章不对任何具体案例作合规判断。

工厂中个人信息可能以间接方式进入技术日志：员工面部或工牌出现在相机画面，语音操作记录含可识别身份，账号和时间戳可与排班表关联。即便算法目标只针对零件或设备，数据链也可能包含人员信息。技术设计可通过视野遮挡、边缘端裁剪、只保存事件摘要和区分身份映射表来降低无必要收集，但是否足够须结合具体处理目的和规则评估，不能只用“训练不需要姓名”作为合规论据。

本地部署解决的是部分计算位置和网络连通问题，并不会自动回答数据访问权、日志留存、供应商远程维护、软件更新和备份存储的治理问题。工厂内服务器若把遥测或调试包定时同步至境外，仍须识别数据内容和流向；云端平台若只接收经选择的状态摘要，也需要判断字段能否关联员工或工艺机密。部署拓扑与数据治理是两个相关但不同的决策层。

远程支持尤其需要细分权限。诊断人员可能只需读取设备错误码和软件版本，也可能需要访问完整相机画面、工艺配方或机器人控制权限。最小权限、临时授权、会话录制、双人审批和脱敏视图能降低故障处理期间的暴露面；但过度限制也可能延长恢复时间。应针对维护任务建立权限矩阵，并将服务响应时限与可访问数据范围一起写入合同。

训练用数据和运行数据的目的也不应混同。客户允许供应商为本厂调试而查看一次工件图像，不代表供应商获得把它用于通用模型训练或其他客户项目的许可；供应商保存系统日志以排障，也不等于制造企业可以任意将日志用于员工绩效评估。合同应说明适用法域下的个人信息处理角色及合同中的数据管理决定权、处理目的、二次使用、期限、删除和审计权，并将模型改进、故障分析和生产质量追溯分别约定。

模型权重也不是一种透明或天然无风险的替代数据。应把训练样本记忆或关联、权重及配置中包含供应商秘密、以及客户无法检查或修改等视为待验证的威胁模型，而非本次分析已核实的案例风险。企业须厘清预训练模型、微调参数、提示模板、配置、工艺规则和客户数据的知识产权与访问边界。若客户能够操作

SVSAC | sv-sac.org

系统却不能导出校准、验证集和版本记录，未来更换供应商或复查质量问题仍会受限。

跨境生产通常要求异地团队协同，但不等于所有数据都必须跨境。可以把模型推理放在本地，将经审核的统计指标发送给总部；将故障样本脱敏后用于集团工程诊断；或由集团下发模型与安全补丁而保留本地工艺数据。每种模式都会改变延迟、工程可见性和本地运维负担。架构设计应根据具体故障和更新任务测算需要共享的最小字段，而非把“全球统一平台”当作单一数据路径。

在地化微调可以提高模型对本地设备、零件或操作语言的适应性，但也会引入版本分叉。若每个工厂都独立调参，集团可能无法复用改进，也难以统一追踪安全边界；若所有更新由总部控制，本地异常可能等待过久。可行做法是将基础模型、工厂适配参数和安全规则分层管理，保留变更原因、数据来源、批准人、验证结果及回滚版本，并明确哪些层能够跨厂复用。

“匿名化”或“去标识化”应视作需要验证的风险控制措施，而非一劳永逸的标签。工位号、时间、特定零件型号与罕见故障组合重新关联，是一种应纳入威胁模型的场景；本章未估计其概率，也未核实任何案例发生过重新识别。分析团队可评估字段粒度、保留时间和关联权限，必要时减少时间精度、模糊身份或仅输出聚合统计。处理后的数据是否满足特定法律要求，仍须按适用标准评估。

联邦学习或本地训练也不能仅凭“数据不出厂”就判定没有数据治理问题。梯度、更新包、诊断日志和模型评估结果是否可泄漏信息，应作为待验证的威胁模型通过协议审查和测试评估；本地模型也涉及设备访问、更新审批和审计责任。本章不报告这些方式的泄漏概率或案例实测结果。它们可能减少原始数据集中流动，但不能据此推定其他安全风险已消除。

合规流程还会反过来影响现场服务能力。若远程工程师无法及时访问关键数据，工厂需建设本地诊断、缓存与日志分析能力；若总部需比较多厂故障，则要建立可共享但受控的事件模式。服务网络设计应同时考虑数据保留、加密、身份验证、跨境访问审计与应急响应。减少数据流动可能增加客户本地人员和工具投入，数据集中也可能减少重复训练，却提高集中泄露的系统性影响。

按本章前述第二、第三条的分类与程序边界，[17]审查顺序应是先定位数据字段、实际内容及用途，再核对应程序与其他适用义务。判断对象是具体数据流，服务器位于何处或“数据本地化”的统称都不能代替这一步。

在合同谈判中，关键是将技术控制与法律责任落实到角色。客户可能是数据处理者，供应商按指示处理数据，集成商访问生产网络，母公司接收集团运维信息；具体角色应依适用法域规定及实际处理目的、决定权和处理关系确认，不由

SVSAC | sv-sac.org

企业国籍或服务器产权单独决定。协议需确定通知、删除、分包商、事件报告、日志交付和跨境传输的协作责任。不可把商业合同的“数据归客户”一句话当成完整治理方案。

数据最小化与工程可诊断性之间存在现实张力。若只保留聚合告警，供应商可能无法复现偶发故障；若长期保存全部高清视频和轨迹，数据暴露面、存储成本和人员隐私风险会上升。可以按故障严重度设置分层保留：普通周期仅保存摘要，异常触发短时高分辨率缓存，重要事件经审批后留存并限制访问。该做法需要清晰的触发规则、存储期限及删除验证，而非无限期保留“以备训练”。

跨境和本地数据路径也可能改变平台供应商的产品设计。若应用依赖云端低延迟访问原始视频，则在网络中断或数据限制下难以运行；若推理和工艺控制可在本地完成，云端仅用于非实时模型更新，系统可更稳健但需要本地算力和更新运维。评估应把网络延迟、带宽、断网降级、模型版本同步和安全补丁周期纳入功能测试。数据位置不是纯法律参数，它可能决定软件架构和故障行为。

因此，比较跨国平台的本地化能力可观察一组具体指标：现场数据路径图是否完整，远程维护有无最小权限和审计，模型更新是否可回滚，供应商是否交付本地诊断文档，数据处理目的是否分层，跨境传输是否按字段而非品牌判断，关键故障能否在本地恢复。单凭数据中心位置、合同中的所有权措辞或公司承诺，均不足以判断治理与运维能力已经形成。

截至本篇资料截止日 2026 年 10 月 23 日，相关规定的使用范围仍限于前述已读条款。[17] 本章的研究增量是将法律类别、技术路径和现场责任对应到同一模型、日志或人员信息流，比较安全维护与跨厂学习的条件；本地部署可能减少部分暴露，也可能增加维护成本，不能由位置本身决定净结果。

第十四章　产业组织差异：谁定义任务，谁控制融合路径

相同算法嵌入不同产业组织时，价值和责任并不相同。整车厂通常掌握车型定义、整车质量和总装节拍；电子代工企业可能面对多客户、多产品和频繁换线；机器人制造商提供本体、控制器与服务；研究团队则优化可控任务。技术能力能否转化，取决于谁有权定义工艺目标、改变设备配置、访问生产数据和判定验收，而不仅是算法是否先进。

汽车制造商的产品开发与工厂工程之间存在紧密耦合。车端计算、软件功能和工厂规划可能由同一平台合作公告同时呈现，但车端质量责任、车型软件验证与工厂自动化验收完全不同。BYD—NVIDIA 公告同时提及下一代汽车平台、云

SVSAC | sv-sac.org

端 AI 开发以及工厂规划用途。[12] 这种跨环节合作可以形成共享工具链的可能性，却不能证明同一团队、数据或算法已经贯穿车辆和制造现场。

汽车总装具有工位和节拍约束，但工艺并非所有车型共用：车身结构、配置、选装和供应链变化会改变定位、连接及检验任务。若 AI 用于检查、工位调度或装配动作，系统必须适应型号变化并与质量追溯系统相连。评价不仅看单车循环，也要看换型、返工、车型混线和质量追责。公告中某项“AI 应用”若未说明工艺位置，就不足以推断它改变了总装核心流程。

电子代工的业务结构可能更强调快速换线、多客户订单和电子物料追溯。FODT 案例将 Foxconn 的运营数据、MES/SFC 与数字孪生连接作为方案组成，并称存在台湾至墨西哥的跨厂迁移叙述。[8] 这类平台可能服务布局、设备状态可视化或工程计划，不自动表示 AI 承担实时工艺控制。代工场景中的客户保密、产品生命周期短和不同客户信息隔离，也会限制数据复用和模型跨订单共享。

电子制造的误差链可跨越贴装、焊接、检测和返修多个设备。若某一模型提高局部视觉判定，却不能与设备校准、批次追溯和质量系统共享结果，收益可能停留在单机。反之，若上游元件批次和下游失效分析可闭环，AI 检测信息可能改善工艺参数。需要观察误判、漏判、复检负担和返修成本，不能把“工厂数字孪生”或“AI-enabled”标签当成良率提升证据。

代工企业还面对数据控制的双边约束：客户可能拥有产品设计和工艺机密，代工方运营设备与人员，但平台供应商又要访问现场日志以提供服务。数据不能不加区分地跨订单、跨客户或跨工厂复用。若权限设计过粗，客户可能拒绝提供有用故障信息；若复用规则过宽，供应链伙伴会担心商业秘密泄露。平台化部署需按客户/产品域隔离并允许客户审核数据使用，而不是假定规模越大模型越好。

机器人制造商作为技术供应者，其核心资产是机械本体、控制软件、运动学、认证和售后网络；AI 平台伙伴可能带来开发环境、仿真工具或模型管理。美的中报展示 KUKA 与 NVIDIA 合作发布，同时披露 KUKA 向中国客户交付机器人和移动机器人方案。[13] 供应商角色有利于把技术集成到设备产品，但更需区分联合发布、产品功能、具体项目交付及客户产线成效。集团所属关系也不能替代客户侧的现场验证。

设备商在产品中嵌入 AI 的商业动机，可能是减少编程门槛、提高复杂任务能力或强化服务订阅；客户则关心其现有控制系统是否兼容、操作员能否掌握、旧设备是否可升级以及故障时谁负责。若 AI 功能只能随整机新购提供，旧设备基数可能限制采用；若可独立升级，版本兼容和安全认证成本会上升。上述选择

SVSAC | sv-sac.org

取决于技术架构和产品策略，公开中报尚未揭示 KUKA AMP 的具体计价和既有设备适配范围。[13]

研究装配平台的产业位置更靠近“可能的能力原型”。ACT 用遥操作示范学习精细双臂任务；IndustReal 以接触丰富装配研究仿真到现实的策略迁移。[6][7] 两类研究说明算法如何利用示范、动作块或模拟物理，但研究平台没有商业客户的产品组合、维修合同、供应链责任和生产保障。由论文到企业产品还需将实验系统变成可维护、可认证、可采购的工业组件。

因此，实验室–供应商–集成商–工厂不是单向“技术扩散链”，更像有回流的开发网络。研究团队提出方法，设备商将其改造成接口和产品，集成商在现场暴露边界条件，工厂反馈异常和质量约束，供应商再更新版本。若反馈只通过非结构化电话和个人经验流动，迭代难以累积；若客户不能分享数据或供应商不开放故障分类，学习网络同样断裂。各方应为知识反馈建立明确的数据和责任边界。

产业分工会影响失败的经济后果如何分摊。算法供应商可能以软件许可限制对输出结果的保证，设备商只保证机械本体，集成商按项目验收接口；制造企业通常直接面对产线停机和质量损失。安全义务则须按适用法域、产品与系统角色及具体合同确认，不能概括为由单一主体承担。合同形式会影响供应商是否参与工艺调优和长期监测。若责任只按各自组件划分，跨组件故障可能无人承担；需要有端到端事故升级机制，同时保留对每个组件的根因分析能力。

客户的议价能力不只来自采购规模，也来自能否替换技术组件。开放文件格式或标准通信协议有助于资产迁移，但仍需确认配置是否可读、模型是否可运行、数据是否可导出以及替代设备是否保持一致语义。FODT 强调 OpenUSD 与工厂数据连接，能支持其方案中的开放资产接口叙述，但不能由此推断完整供应商可替换性或客户数据主权。[8] “开放”必须在具体资产和运维权限层面定义。

不同产业的客户可能采用不同的风险接受方式。汽车安全或质量追溯缺陷可能影响整车，电子装配误判可造成大批返修，物流错配会导致缺料和产线等待，研究装配实验的单次失败则多为平台级试验损失。验证成本、事故外溢和可回滚性因此不同。不能把一个小批次实验中的高成功率直接移植到高后果工序，或假定企业会以相同速度开放 AI 控制权限。

供应链中的收益也可能不对称。平台商从计算和软件生态受益，设备商提升产品差异化，系统集成商赚取工程与维护服务，制造客户承担部署资本、工艺改变和运营风险。若应用提升了数据采集能力，客户可能同时贡献模型改进资产；若其未得到服务折扣、配置控制或数据访问，价值增量可能主要留在上游。对此需要合同、续约和维护资料，而企业发布公告不足以判断价值分配。

SVSAC | sv-sac.org

替代解释在跨产业比较中尤其关键。设备先进、生产管理成熟、客户需求稳定或工程人员充足，可能同时提高数字系统部署成功和产线绩效；产业链地位高的企业更能选择供应商、承担试错和持续迭代。观察到行业领先者使用某平台，不等于该平台造成领先。比较需考虑企业原有研发投入、资本更新、质量体系和产品复杂度等基础差异。

公开案例可支持的是具体合作与工厂位置：BYD 公告称 NVIDIA 为其车辆计算、云端研发及工厂规划方向的合作方；BMW Lydia 资料定位于沈阳；NVIDIA 的 Foxconn 案例描述台湾与墨西哥工厂间的迁移；美的中报讨论 KUKA 合作及中国客户交付。[12][8][13][9] 这些信息有助识别组织与地点，却不自动解释软件版权、数据权利、算法来源或利润归属。跨境融合仍需追踪法人、许可、工程团队和服务合同。

跨产业公开案例的可比性还受披露倾向影响：某行业的旗舰发布较多，不等于其采用更普遍，另一个行业的维护资料较少也不证明失败更多。按第 10 章及第 16–17 章的选样与阶段规则限定比较范围，才能把产业角色差异与公开样本选择分开；本章不由公告数量估计普及率。

跨产业比较的抽样单位应先按任务而非行业标签设定。可以选择相似的机器人装配任务比较不同设备及支持模式；也可以在同一工厂比较固定机械臂和移动机器人不同恢复需求；或者比较同一数字孪生平台在首厂与复制厂的更新工作。任务匹配能减少行业结构差异，但仍要控制工艺、产品和组织能力，不能将个案的相似名称当作真正同质的对照。

可检验的产业命题包括：在客户产品变更频率高的环境中，平台价值更依赖接口可配置与快速换型；在设备商提供完整维护网络的行业中，客户未必需要自行掌握全部模型，但需拥有独立审计和退出能力；在跨国集团内部，流程经验可能先于软件知识迁移。每个命题都需用合同、工程变更、维护和生产数据验证，不能从产业名称或企业组织结构直接推定。

产业差异的分析结论是，融合路径由工艺风险、客户权利和互补资产共同塑造。汽车、电子代工、机器人供应与研究基准在任务、采购、维护和证据边界上并不等价；同一平台可横跨多个领域，却不能因此把各领域结果合并。有效的产业比较应定位明确技术组件、特定工艺与承担责任的组织，并将尚未公开的接口和运营数据留作未决问题。

SVSAC | sv-sac.org

第十五章　本地服务与产业集群：外溢需要重复互动和共享能力

跨境技术在本地形成持续应用，依赖的不只是设备销售，也包括安装、校准、维护、培训、软件更新和工艺改造服务。美的中报披露 KUKA 在中国市场向客户交付机器人、提供移动机器人方案，并称昆山设有“华东智能制造中心”。该中心在报告中属于制造布局，不能只凭名称当作已建成的本地服务或知识转移能力，更不能单独证明其服务授权范围、响应时限或客户自主维护能力。[13]

服务体系至少有三种层次：基础维修和备件保障；系统级接口、配置及故障排查；工艺改造、模型适配与多厂复制。第一层能缩短设备停机，第二层帮助客户恢复系统，第三层才可能沉淀客户自身的工艺和数据能力。企业说“本地服务”时应识别团队授权、服务范围、备件位置和故障升级路径，不应把销售办公室、培训点与复杂工程支持视为同一能力。

服务响应时间也须拆解：从故障发生到报警、确认、初步诊断、到场、修复和恢复生产，各阶段由不同组织承担。远程监测可能缩短告警发现时间，但若权限不足或现场需要更换备件，恢复仍会延迟；本地工程师可快速到场，却可能缺少模型或控制器诊断权限。合同中的“24 小时支持”若没有定义起算点和解决标准，难以比较供应商服务质量。

系统集成商常处于设备商与工厂之间，掌握控制协议、数据映射和工位调试知识。其能力可能来自多个行业项目的重复实施，但经验是否可迁移取决于设备接口与工艺相似度。熟悉汽车焊装的团队未必能处理柔性线缆装配，熟悉仓储调度的团队也未必掌握安全 PLC 和工艺质量。集成商规模或项目数不能直接替代任务级能力评估。

本地服务网络的价值可通过“故障闭环是否留在本地”观察：本地工程师能否读取完整诊断信息、形成根因报告、更新受控配置、验证恢复并将经验写入知识库。若所有复杂故障都需总部远程审批，本地团队可能只是执行维修；若客户和集成商可独立处理，部署能力更可能成为区域内可复用资产。人员身份和办公地址本身无法区分这两种状态。

跨境部署首先涉及工程操作权限，而非抽象的“知识共享”。本地团队可能获准查看报警和更换部件，却无权访问源代码、模型权重、控制器深层日志或跨境调试环境；这些权限决定故障能否在本地定位，还是必须等待总部升级。对每个部署，应分别核实远程访问主体、范围、审批时限、日志留存和紧急撤权机制。没有公开合同或权限说明时，这些是需逐项核实的变量，不能由“本地支持”字样推定。

SVSAC | sv-sac.org

总部升级依赖可能以产品安全、出口管制、网络隔离或知识产权保护为由而合理存在，但它也可能形成排队瓶颈。关键不是要求所有权限下放，而是确认哪些故障级别可由本地处理、总部何时响应、临时授权如何审计，以及升级失败时工厂如何恢复生产。若本地工程师不能访问所需诊断工具，即使其名义上承担现场服务，复杂问题的控制权仍在总部。这个区分取决于法域与具体合同，不应仅凭国家来源判断。

跨境供应商的本地工程授权可以分层：一级服务读取状态和更换模块，二级服务调整经批准的参数并执行校准，三级服务修改控制逻辑、模型或生产配方。每层均涉及不同的安全、知识产权与产品责任风险。实际分析应把授权清单与故障工单对应，观察发生的复杂故障是否由获授权层级关闭、是否需要总部签核，以及恢复后由谁验证。服务点的地理存在不能替代这一权限图。

总部版本升级常包含安全补丁、控制策略和功能更新，工厂却需要在产线停机窗口内完成兼容测试。若升级节奏由总部统一而本地验证资源不足，客户可能推迟更新；若本地自行分叉版本，后续维护与安全修复又可能变难。应追踪版本发布日期、工厂验证日期、延迟原因、分支差异和回退结果，从而区分合理的本地验证周期与供应商治理失灵。现有公开案例不足以估计这类延迟的普遍程度。

承接第 9 章的吸收框架，本章把能力检验具体到：工程师能否解释关键参数与失效条件、独立复现验收、提出有效变更并维护受控版本，生产团队能否识别适用域外工件并安全回退。测试须按角色、班次和设备类型分别核实，不能把授权层级本身当作能力得分。接收方既有能力与双方协作在此仍是知识转移研究提供的机制参照，不是对本篇案例的直接实证。[14]

第 13 章已列数据流与角色核查项，本章关注其中的知识收益：模型更新可能把本地工艺经验转成供应商通用产品能力，合同所写的控制与实际处理链条也可能不同。应据实际目的和访问关系判断谁取得可复用知识，而不能从“数据归客户”推定客户保留全部学习收益。适用法域及程序边界仍按第 13 章前述条款核对，不扩写为普遍传输许可。[17]

集团内部网络与区域产业集群具有不同的扩散治理。集团可通过共同工程标准、内部人员轮岗和统一采购降低跨厂协调成本，但知识流动通常限于集团可控制的组织边界；区域集群则可能连接互不隶属的工厂、设备商和集成商，扩散面更广，却需要协商知识产权、竞争敏感信息和服务收费。两者不能仅以地理密度或项目数量比较，须考察参与关系、可复制资产和外部企业是否实际获得服务。

集团网络的潜在优势是反馈可沿既有汇报线回流：某一厂的工艺变更、质量异常和调试经验可能进入其他厂的工程标准。但组织边界内的信息通道不保证知

SVSAC | sv-sac.org

识自动吸收，跨厂复制仍需有人维护文档、判断差异并承担再验证。讨论 Debrecen 对 Lydia 及 Leipzig 流程的参照时，可分析集团内流程借鉴；不能据此推断相同软件、AI 模型或生产结果已原样迁移。[11]

跨境服务授权还决定收益和风险如何分配。供应商可能保留高级诊断与更新权，地方经销或集成商承担到场成本，制造客户承担停线的经济后果；若合同没有区分响应义务、根因分析、软件缺陷修复和生产验收，现场争议容易转化为“设备正常”或“工艺不当”的归责冲突。合同未公开时不能断言现实责任分配，但项目研究可以核对服务级别、升级记录与故障责任闭环是否一致。

“本地能修”与“本地能改”是不同能力。前者意味着按既定程序恢复设备，后者涉及判断工艺变化是否需要改控制策略、校正模型或变更质量阈值。为了判断知识转移，需追踪本地团队在多复杂任务上拥有决策权、其变更能否进入受控版本、总部拒绝或批准的理由，以及客户能否在供应商不在场时完成验证。也应避免把必要的总部安全审查误判为能力缺失。

独立区域集群的知识扩散需要跨组织的可信中介：集成商或培训机构可能把多家客户反复遇到的接口问题提炼为通用诊断工具，但必须剔除可识别客户的配方和生产数据，并允许客户验证工具适用范围。若客户担心敏感信息外泄，或供应商不愿披露诊断逻辑，经验将停留在双边关系中。相较集团内共享，区域扩散的参与门槛和治理成本更高，其效果需要通过多个非关联客户的复用记录证明。

跨境工程依赖可以用过程指标描述：各级工单从开单到升级、授权和关闭的时间；本地团队可独立处理的故障类别；版本升级从发布至验证的间隔及其原因；供应商缺席时客户能否执行回退；以及内部人员提出的有效工艺变更数。指标应按故障严重度和接口类型分层，避免把复杂控制缺陷与常规备件更换混在一起。这些是建议的观察量，并非现有披露已提供的绩效结果。

结合第 9 章诊断协作与第 17 章本地结单命题，本章应比较授权变动前后同类故障的复发、总部介入频次和客户独立验收比例，并控制设备复杂度与项目年限。第 15 章的权限配置、能力测试和第 15 章过程指标分别回答“能否做”“是否会做”及“实际怎样完成”，不能合成一个吸收分数；尤其要按故障复杂度排除简单任务转交造成的表观自主率上升。

集团内部网络和外部集群的比较，可从边界内外的知识复用率着手，而非笼统评价“生态”。集团内追踪一个工厂的故障方案是否进入另一工厂标准、经过何种再验证；区域网络则追踪集成商的通用模块是否被无关联客户采用、如何保护首家客户知识。若只在母子公司内复用，证据支持内部扩散；若跨独立客户且接

SVSAC | sv-sac.org

口仍兼容，才支持区域外溢。比较还需考虑集团统一投资与客户自选集成商的差异。

本地化是否深化，最终可从控制权和吸收能力而非办公地点判断：复杂故障由谁诊断，更新由谁批准，工艺知识是否留在客户组织，非关联工厂能否复用而不泄露首家客户信息。跨境供应商、本地集成商、客户工程团队与集团总部之间的授权矩阵，构成观察技术转移的具体对象。这样的分析将集团内部流程迁移与区域集群外溢分开，也避免把本地服务存在直接等同于技术自主。

第十六章　失败机制与替代解释：从技术缺陷到证据选择

跨案例比较若只记录成功样例，会错过工业融合最重要的机制：技术何时无法维持、为何不能复制、以及失败成本落在谁身上。失败并非单一的模型错误，可能来自感知与控制、工程接口、数据治理、组织服务、合同责任或投资选择。将这些情况区分开，能避免把所有未达目标都归因于“算法还不够好”。

IndustReal 的已观察实机失败包括夹爪内滑脱和插头楔紧；弹性线缆绕滑轮则被列为更复杂任务的仿真精度与效率限制，不是该研究已经测试失败的柔性物体任务。[7] 前两者可用于讨论接触、摩擦与几何配合；后者只限定外推范围。工业分析须分别记录已观察故障、尚未测试的对象与拟议补救，不能把未来工作当成实机故障证据。

研究任务的成功率异质性也反映任务难度差异。ACT 作者项目页的四项任务在相同示范数设置下仍报告不同成功率，范围为 64%至 96%；RSS 论文摘要另描述不同任务和示范条件下的结果。[6][1] 这种变异提醒研究者避免用最佳任务代表整个技术能力。生产线需按任务类别和变化包络设定验收，而不能把一个精细操作演示转换为“通用制造能力”。

从实验到现场的迁移还可能失败在环境分布偏移：相机安装、照明、夹具磨损、零件批次或运动速度改变输入条件。模型对已知样本的高分表现不等于对未来异常的稳健性。更有效的验证是列出关键变化因素，设计边界样本并记录误差和恢复；再将失败与特定变因关联，而不是仅在总体测试集中汇总成功率。

仿真方案的失败可能不在策略，而在虚拟环境精度。若接触、摩擦、刚度或传感器噪声建模错误，策略会学习到现实中不存在的可行路径。IndustReal 通过仿真到现实的特定基准展示方法，也将仿真真实性与变形物体复杂性列为限制。[7] 工业项目需区分“算法未能泛化”与“仿真标定不准确”，并记录实机数据是否用于感知微调、控制器配置或策略适配，避免把无策略微调误述为无需现场工程。

SVSAC | sv-sac.org

数字规划也会因模型误差和变更治理失效。布局模型可能遗漏设备更新、现场障碍或维修空间；即便碰撞检查正确，如果工程变更未传回三维资产，后续仿真也会基于过期条件。BMW Lydia 的公告描述虚实规划与协同，不能据此证明所有模型持续同步；其建设时间句子的因果指代也有歧义，需避免把六个月数字当作确定效果。[9] 此处的失败风险在于数据维护流程，而非 3D 引擎必然无效。

数字孪生或开放资产接口的另一个断点是运营数据连接并未自动转换为控制闭环。FODT 案例描述 Omniverse/OpenUSD、MES/SFC 及运营数据的连接，但数据可视化、工程规划、生产监控和机器自主控制是不同功能。[8] 如果分析把接口连通当作 AI 决策或过程优化，便会高估技术成熟度；反之，即使没有 AI 控制，数据互联仍可能改善工程协同，评价时应识别实际功能而非用“AI 工厂”标签替代。

合作公告还会出现“计划–交付–持续使用”的流失。BYD—NVIDIA 公告把工厂规划作为合作方向，没有公开具体落地基地；美的中报把 KUKA 与 NVIDIA 合作发布和中国客户交付并列，但未把客户设备连接到 AMP。[12][13] 后续若项目未上线，可能是预算、供应链、工艺不匹配或商业合同导致，不应将其自动归为技术失败；同样，宣布合作本身也不能计为成功部署。

企业披露与供应商案例的积极选择会带来幸存者偏差。成功发布的试点和旗舰工厂较容易公开，取消、延后或转回传统设备的项目可能只留在内部资料。若研究只从公开新闻取样，能看到的通常是企业愿意展示的技术环节。改善办法包括建立项目阶段时间线、寻找招标和许可记录、追踪设备后续版本及客户公开报告，并将“未发现公开信息”与“项目失败”严格区分。

某些供应商量化声明需要进一步拆分。Foxconn 案例的 150 倍指标针对特定热分析仿真任务，50%时间缩短是负责人对营收周期、工厂建设和规划的预期，并非公开的跨厂对照结果。[8] 即使数字准确描述该案例，也不能直接外推到普通工序或全体工厂。研究中应记录指标定义、比较基准、观察期、样本及是否经第三方核验；缺少其中关键字段时，数字只能作为来源方主张。

合作成功还可能由非 AI 因素驱动。资本更新可以替换老旧设备，精益改善可以重排物料流，新增工程师可缩短调试，质量体系可提高异常发现率。若这些改变与 AI 同时发生，单一前后比较会错误归因。评估应以工艺变更清单和产品组合为基础，比较相似未改造工位，或使用分阶段上线来检验变化出现的时间点。

另外，项目选择自身就是结果的替代解释。管理能力强、设备标准化和产线数据完整的工厂更容易获批试点，也更可能获得好结果。试点表现不能代表平均

SVSAC | sv-sac.org

工厂，尤其不能证明政策或平台对资源较弱的中小企业同样有效。抽样研究需要记录试点资格、参与前能力、供应商投入和退出原因，区分技术效应与“准备就绪企业”效应。

失败也可能是收益定义不一致。供应商认为按合同接入系统即完成，集成商以接口验收计费，客户却预期降低全线成本；当系统达到技术性能但没有形成经营回报，各方会把项目描述成不同状态。项目审查应将合同验收、工位功能、产线运营和财务结果分别记录，并把未兑现预期对应到责任条款与工艺假设。这样才能区分技术可行但商业价值不足，与技术未达合同承诺。

锁定是另一个可能的负面结果：工具链依赖单一供应商、配置难以导出、诊断数据不完整，导致迁移成本上升。若平台在多厂扩张后需持续驻场，客户也可能由机器依赖转为服务依赖。锁定并非仅由专有代码造成，知识不可移交、停机时依赖总部审批、更新路径不透明也会增加退出成本。采购阶段需对迁移资产、版本保留、故障日志和替代服务商进行测试。

本地团队被长期排除在复杂故障处理之外，技术使用可能稳定但能力转移有限。这样的情形不应以“本地化成功”或“自主化失败”二分，而需判断客户是否以可接受成本获得了可靠服务、是否保有审计和退出能力，以及该安排能否满足长期运营。对于低使用频次、安全关键的设备，原厂维护可能经济上合理；对于高频变更工序，持续依赖外部专家则可能约束迭代速度。

跨境规则与安全约束也会改变实施方案，但不能预设其必然阻碍部署。《促进和规范数据跨境流动规定》对若干数据类别和条件规定了不同处理路径；技术架构可以通过本地推理、数据脱敏和受控远程支持应对部分需求。[17] 实际影响要根据数据字段、用途、参与方角色和具体适用条款确定。若企业改变架构，测量其对延迟、运维成本和模型效果的影响，不能仅从规则文本推断商业阻碍程度。

风险报告还应区分发生概率、后果严重性和可探测性。罕见故障若可快速发现并安全回退，和同样罕见但导致工伤、批量报废或长时间停线的故障，不应等价处理。FMEA 式分析可帮助识别传感失效、策略外推、网络中断和错误更新的后果，但风险分值本身不是实测事故率，必须由现场观察和工程评审校准。

跨案例的反证机会包括：同一平台在相似工艺上未扩张；低技术含量的传统改善带来相同运营结果；不同供应商通过不同路径达到相似功能；或本地集成能力强的工厂在较少 AI 使用下获得更好性能。遇到这些情况，研究应修订“平台带来收益”的因果解释，改为比较工艺适配、人员能力和管理投入。反例不是装饰，而是机制主张能否成立的检验。

SVSAC | sv-sac.org

公开资料无法解决的关键问题包括：项目合同是否达产、长期停机与维修账目、未公开试点的退出原因、模型更新权限、客户是否得到数据副本、AI 功能上线后是否保留人工兜底。这些缺口限制对当前部署规模和净收益的估计，但仍可通过有边界的案例研究、技术文件和企业访谈补足。若缺少这些材料，作者应明示不确定性而不以行业常识填空。

失败机制的综合判断是，工业融合不是模型能力单变量问题，而是技术、工艺、服务、数据、合同和组织选择的联合结果。学术实验识别局部技术边界，供应商公告揭示产品定位和路线，企业报告可能说明交付或流程参照；它们各自留下不同的失败信息。[7][12][8][13][9][11] 只有将正面案例、未扩展结果和替代解释纳入同一分析框架，才能避免把公开亮点误当成系统性产业转型。

第十七章　可证伪命题与案例设计：怎样识别技术融合的条件

前述案例比较支持的是机制假说而非总体因果结论。下一步研究应把观察单位限定为“技术组件–工艺任务–具体工厂–部署阶段”，并保留时间。仅以企业或行业为单位会把不同模型、工位、地理位置和成熟阶段合并，使所谓“AI 采用”既不可重复编码，也无法与结果对应。

每个案例至少应有一张技术–流程图：算法或软件功能是什么，传感与设备从哪里提供输入，输出如何进入控制器或决策流程，人工在哪些环节确认，故障如何回退。数字规划应用另标为相邻数字化功能，除非有明确 AI 组件。该图能防止把品牌、仿真引擎、数据接口、生成式 AI 和机器人控制混称一个系统。

命题一：任务输入越可观测、工艺变化越能参数化、失败越容易检测并安全回退，学习型策略越可能从实验转入稳定工位。解释变量可由传感覆盖、异常可分类比例、复位方式和损伤严重度描述；结果变量应包括跨批次首过合格、恢复时间、人工介入和持续班次运行。IndustReal 和 ACT 提供受控任务基准，但不覆盖上述工厂结果，需要现场数据检验。[6][7]

命题二：跨厂模板越能把共性接口与场地差异显式分离，新站新增工程工时越低。可测量代码/配置复用比例、重新采集和校准次数、接口重写工时、验收脚本复用率及现场驻场时间。若复用比例高却故障或返工增加，则表明标准化遗漏了重要差异；若工时不降但质量和恢复显著改善，则复制价值不应只按费用判断。

SVSAC | sv-sac.org

命题三：客户本地工程师获准访问必要诊断数据和参与联合维护的权限越充分，客户本地工程师独立关闭故障的比例越可能提高。需记录权限范围、升级层级、首次响应与恢复、修复主体、复发和跨班组复用。观察到更多本地工单关闭不一定代表知识吸收，也可能是简单故障被转给本地；必须按复杂度分层，并判断客户能否解释根因及控制更新。

命题四：数据模型治理越成熟，模型或仿真更新引起的回归问题越少。具体特征包括设备与工件版本关联、模型变更审批、传感器校准时间、日志时间同步、回滚流程和变更后的再验证。Sculley 等讨论的机器学习系统依赖与反馈耦合可以支撑该机制分析，但不提供制造项目回归率数据。[15] 需要通过多版本运行记录验证。

命题五：平台连接越开放，客户迁移成本越低，但开放协议本身不够。研究需测试资产能否完整导出、替代设备能否读取语义、授权是否允许本地运行、调试历史是否随系统交接，以及服务商替换后是否能完成安全验证。一个接口符合通用标准仍可能缺少安全状态和异常含义；迁移测试比产品说明更能检验开放性。

命题六：跨企业或集团服务网络越能反复处理共同工程问题，知识越可能沉淀成可复用规范。可观测指标包括跨企业共享测试或培训的活跃用户、重复故障处理时间、工程师流动、通用适配模块和多企业采购复用。对集团内流程迁移与独立供应商生态分别编码，避免把同一集团的管理复制误作开放集群外溢。[11][14]

这些命题要求区分投入、过程和结果。训练数据量、服务器数量、设备交付和平台用户属于投入或活动；工位成功、维修和接口适配属于过程；整线交付、质量、劳动和成本属于结果。若公告只报告前两类，不应直接推断第三类。多层指标还可定位效果为何中断：模型准确但维护不可用，或系统可用但经济收益不足。

时间指标需按制造术语分层：需求 takt、实测工序 cycle、订单 lead time、换型、停机和恢复分别记录。[16] 单台设备延迟不能代替整线交付；若对比前后数据，须固定或控制可用生产时间、客户需求、产品组合、缓冲和返工。物料流与信息流可帮助定位瓶颈是否从 AI 工位转移到相邻环节，而非消失。

定量比较至少应有明确的基线和处理边界。可在同一工厂选择工艺和设备相近的工位，记录改造前后并匹配产品、班次和设备年龄；若分期上线，可观察未上线工位作为临时参照。方案仍受管理者优先选择准备充分工位的偏差影响。分析应报告不平衡变量与敏感性，而不是将匹配或时间序列设计称作随机实验。

SVSAC | sv-sac.org

对跨企业平台，应补充合同和流程追踪。访谈客户、集成商、设备商与平台供应商，核对试点如何选定、数据如何授权、模型如何更新、故障如何升级、验收标准是否改变。研究团队应获取受访者授权、区分可公开与保密材料并采用交叉核验。访谈能揭示责任和未公开失败，却不能单独验证绩效数字，需与运营日志或文件互证。

案例选样要纳入未扩展和失败项目。先根据公开资料建立计划、试点、交付、运行、复制、终止的项目清单，再对不同结果类型抽样，记录每类材料可得性。若终止项目缺少公开信息，应明确样本对失败机制的覆盖不足，避免由新闻稿统计部署率。监管披露、采购文件、设备售后资料或劳动安全记录可能提供反向证据，但各自覆盖范围不同。

比较来源时应记录来源方的利益和观察位置。企业报告通常更了解交付与战略，但可能强调旗舰案例；供应商案例能说明产品组件和客户流程，却往往选择性披露；同行评议论文能细化方法，但任务和场景受实验控制限制；政府文件界定制度或行业背景，不证明企业采用。来源偏差不是将证据全部否定，而是决定每条材料能支持何种推断。

项目评价应在观察前约定工况、有限观察窗及故障暴露，而非等出现故障才结束。单件、连续批次、跨班次及维护后复测支持不同范围的结论；窗口内无维修事件时，可单列受控维护演练并明确它不证明自然故障恢复。退出、未发生事件和观察不足分别登记，不将无记录当成功或失败，也不以最好运行片段替代全窗结果。

法律与数据治理应嵌入研究设计。记录者需明确哪些日志含个人信息、哪些材料受客户商业秘密约束、跨境访问是否有合法基础以及数据留存期限；最小必要字段与受控权限能降低收集风险。研究报告需说明无法获取的字段及其对结论影响，不可用合成数据或行业假设冒充现场证据。涉及具体出境流程的判断应由适格法律专业人士结合个案复核。

研究者还应区分 AI 的边际作用与更广泛的数字工程贡献。对 Lydia、FODT 和 BYD 规划等材料，可分别记录虚拟规划、数据接口和明确 AI 方向；如果未显示 AI 组件，则不纳入“AI 控制效果”结果。对 KUKA AMP 或 AI 机器人，应单独核实产品功能、客户站点和运行时权限。概念边界清晰才能避免把一般数字化成熟度归因于 AI。[12][8][13][9]

机制检验须先规定方向、可比对象与反证条件。在任务、设备与新增范围可比并控制初次学习后，接口复用仍不降低工程工时，才构成对其降本机制的不利证据；结果未测量或观察不足不是反证。本地维护权提高而恢复未改善，需要区

SVSAC | sv-sac.org

分复杂度和故障转交变化；高任务成功率未改善良率或停机，则限制从技术表现推到经营收益。个别反例可约束适用范围，不能不经比较便否定所有条件下的机制。

适合公开发表的结果不应只有一个“融合指数”。可以形成结构化案例数据表，以技术组件、任务、产地/工厂位置、组织角色、阶段、指标定义、来源类型、观察期、对照和缺失项编码。定量部分只汇总真正可比的任务或运营指标；机制部分用过程证据解释差异。指数会压缩合同、服务和失败这类异质因素，除非透明定义权重和敏感性，不能作为简单排名。

第 17 章把前述机制转成可比较而可被推翻的命题，不预设国家或平台领先。观察窗、未扩展项目、来源位置与概念边界按本章规则处理；现有公开材料只能支持机制综述、案例筛选和条件预测，尚无中国工厂层面的因果估计。

第十八章　综合讨论、决策建议与研究边界

本次分析的中心判断不是“硅谷技术进入中国工厂”这一单向扩散叙事，而是前沿技术、设备与软件接口、工艺知识和组织能力在具体生产任务中的重新组合。所谓融合，至少包含三种不同层次：算法或模型被嵌入既有生产流程；数字规划、仿真或数据接口改变工程决策；以及跨地团队把一处积累的工艺知识转化为另一处可运行的流程。三者可能同时存在，却不能彼此代证。特别是，使用数字孪生或三维引擎并不自动意味着使用了 AI，集团内流程迁移也不等同于模型迁移。核心问题也受到公开议题的启发：截至 2026 年 10 月 23 日，高交会官网仅预告论坛拟于 11 月 26 日举行，并将具身智能、Sim2Real 和场景落地列为议程方向；这只是未来议题背景，不是活动实录或产业采用证据。[13][9][11][18]

从工程机制看，融合的瓶颈往往位于模型与生产对象之间的转换链。传感器、执行器、工装、控制器、制造执行系统、质量记录和异常处置共同界定模型可观察、可作用的边界。研究原型能够在设定任务上完成闭环，并不意味着它已处理设备漂移、材料批次变化、工件定位误差、连续轮班和人工接管。工业 AI 的评价单位因此不应只是模型，而应是包含接口与责任人的任务系统；但这项判断是本篇的分析框架，并非现有公开案例已经验证的普遍规律。[6][7][15]

第 11–12 章已说明研究任务、公司方案与交付陈述回答不同问题。由此，开放代码不能代证中国量产，企业宣布采用也不能倒证某算法有效；证据只能在相应任务和阶段上互补，不能组成统一成熟度排序。[6][7][12][13]

SVSAC | sv-sac.org

综合判断保留四个字段即可明确推论边界：主张要说明改变何种结果，观察单位区分任务、设备、班次、工厂与集团，时段标明基准及持续期，反事实说明未采用时的可比状态。材料能填写哪些字段就支持哪些判断，不能把技术可行、实施与经营价值合成一个“落地”标签。

地理维度同样需要拆开。总部所在地、技术研发地、模型训练地、设备生产地、工厂所在地和客户交付地可能跨越多个法域，且公开案例经常只明确其中一两项。将“美国前沿技术”和“中国制造”当成两个内部同质的实体，会遮蔽跨国集团、供应商网络和地方工艺团队之间的真实连接。研究具体项目时，应记录技术来源、接口控制者、数据处理安排、设备与备件服务地点，以及工艺知识由谁维护；未披露的地理链路应保持未知，而不由企业国籍推断。[8][9][11]

这些差异改变实际判断所需的对照。若问题是动作在指定系统中能否完成，ACT 与 IndustReal 提供比平台愿景更贴近任务的实验依据；若问题是中国生产现场的流程是否被异地新厂借鉴，Lydia—德布勒森的具名布局参照比机器人基准更贴近对象，却仍受公司披露和多来源共同设计限制。若问题是车端研发或工厂规划的合作方向，BYD 公告才是对应材料；它不能替代某一工厂的应用与效果记录。比较由待解释问题决定，不能把“实验更细”或“企业已宣布”单独当作整体产业化更强的排序。[6][7][12][9][11]

并行投入按第 16 章的机制分别归因：布局、设备、培训和质量制度与 AI 同步变化时，前后改善只能先归于技术组合；接入、工装或维护不足也可能阻断作用。不能把缺少互补条件和模型本身失效混为同一解释。

第 16 章还区分了准备充分项目先入选与成功案例先公开两种选择。若未扩展、停用和替换项目不能进入观察范围，多篇正面公告仍只能证明这些路径存在；单个失败也不能否定全部适用条件。

时间判断沿用第 16 章的计划–交付–使用区分与第 17 章观察窗：宣布日不替代部署日，安装量不替代活跃任务，示范不替代持续量产。只披露初始阶段的材料不补写后续；阶段日期、停止与回退状态分别保留。

第 9 章已区分可交接文档与依赖现场判断的知识。退出或迁移时，拥有图纸、参数表和规程并不证明能处理磨损、材料替代和班组异常。知识黏性与隐性知识在此仍只是技术转移研究的概念参照，不是原文对 AI 工厂的直接实证。[14]

第 10 章的版本时序冲突也界定了本地化成本：接口可接入却赶不上现场验证与停线窗口时，更新可能增加再确认工作。语言或界面适配不能消除设备兼容、技能和备件约束；成本须由版本、工时与故障记录核算，不能从合作公告推算。

SVSAC | sv-sac.org

采用者可沿第 17 章已定义的节拍、周期、换型、恢复及质量指标检查收益是否传到整线。单机提速若只把等待转移到相邻工序，或减少漏检却显著增加复检负荷，都不能直接称交付改善。制造术语帮助保持比较口径，不能替代项目数据。[16]

供应方的责任判断回到第 10 章的变更治理：谁更新、验证、回滚并交接配置，决定维护工作由谁承担。数据依赖、配置耦合和反馈回路的技术债概念提示持续成本，却不是已测行业指标；不能用实验模型改善抵销尚未计量的现场维护负担。[15]

公共政策的分析也应从“支持 AI”转向支持可验证的扩散条件。共用测试设施、设备协议与数据格式标准、技能培训、第三方验证和中小企业可负担的集成服务，可能降低进入门槛；但公共投入是否改善生产率，仍需有受益企业、对照对象、时间窗口和额外性评估。对跨境数据规则的讨论则必须精确到数据类型、处理角色、适用法域和具体程序，不能把一项程序性豁免扩写成普遍许可，也不能以法规文本推断企业已完成合规。[17]

因此，第 17 章的机制检验在证据链中止处也须停止外推：可说明方案或组织路径存在，不等于已说明量产成效。保留本章的主张、单位、时段与反事实，可以指出尚缺哪一连接；这里收束的是既有命题的判断规则，不是新增实测结果。

前文关于任务变化、工艺节拍、接口、当地授权和知识吸收的命题，应理解为条件性比较而非普遍排序。学习型控制、专用自动化和人工操作各自可能适合不同的变化范围、风险容忍度和验证成本；将某条路线称为“先进”不能预先决定哪种方案更合适。尤其当质量后果严重或回退困难时，验证强度本身会改变技术方案的相对价值。

前文的跨厂迁移命题同样强调复制边界：可复用的工程资产降低重复开发，却不消除材料、工装、班组和制度差异。集团内部网络较易形成共同标准，但其知识外溢通常有组织边界；独立区域集群可能覆盖更多企业，却承担更高的信息治理和商业协调成本。比较这两种路径时，核心是哪些知识可以共享、谁有权修改、谁承担再验证，而不是简单判定集权或本地化更优。

前文关于供应商集中、本地服务和退出能力的命题，则提示部署后的控制权不可由初始采购决策代替。平台集中可能减少早期接口摩擦，也可能增加切换成本；多供应商方案可能降低单点依赖，也可能加重协调。只有在更新、故障、续约和迁移等真实事件中观察责任履行，才可判断风险是否兑现。本篇未取得这类客户合同和长期运维记录，因此这些仍是比较机制，而非对具体厂商的定性。

SVSAC | sv-sac.org

研究边界仍然明确。所用材料来自公开论文、企业公告、监管与政策文件及术语资料，来源的可见性与完整性不均；部分论文仅取得摘要，企业披露存在选择性，未公开的商业合同、生产数据和失败项目无法纳入。本篇没有开展工厂实地调查、访谈或计量因果识别，也不是穷尽性系统综述。因此，结论是机制解释与可检验问题的归纳，不能作为行业渗透率、平均收益、就业影响或某一工厂当前能力的估计。对法律义务的说明也仅用于标示研究边界，不替代针对具体主体和数据流程的法律判断。

归纳而言，硅谷前沿技术与中国制造的融合并非技术移植的终点，而是围绕工艺任务、系统接口、组织知识和现场服务不断协商的过程。真正需要验证的不是“是否采用 AI”这一标签，而是何种技术组件在何种生产条件下，经由谁控制的接口，改变了哪项结果，收益与风险由谁承担，以及当条件变化时能否诊断、修复或退出。把这些问题落实到可观察的工序和时间线上，才可能将宏观叙事转化为可比较、可反驳、可积累的制造研究。

给企业的下一步建议

硅谷技术与中国制造的结合，值得从具体产品和工程问题切入；合作价值最终要由可交付的成果体现。因此，我们建议把下一步工作收敛为一项有明确交付物的专项任务。

具体起点是：先把企业需求翻译为技术任务，再明确知识产权、接口、验证与商业分工，按项目寻找适配伙伴。在此基础上，管理层可以按证据充分程度、资源投入与业务影响确定优先级，先验证关键假设，再安排后续合作与投入。

要把上述判断用于实际经营，可以围绕具体产品或项目、目标市场、现有能力和决策难点，进一步形成技术需求定义、合作方向筛选、跨境协作与成果转化方案。这类工作需要把行业研究、企业诊断与合作条件核验衔接起来，让分析结果成为管理层可以使用的决策依据。

资料与分析范围

下列说明列明资料范围、分析依据与适用条件，便于读者辨别文中的事实、推演和建议。市场进入、交易安排及适用规则仍需结合具体项目核实。

本篇考察硅谷相关前沿技术与中国制造现场之间可能形成的连接机制，聚焦机器人学习、仿真与数字规划、工业软件和设备接口、跨厂流程知识转移及本地工程服务。研究采用定向公开证据综述与机制比较，分析同行评议论文、企业公告、监管文件和行业术语资料，区分实验室可行性、企业计划、项目部署、稳定

SVSAC | sv-sac.org

生产和可识别经营效果。公开材料显示，技术进入制造并非模型的单向移植，而是算法、设备、工艺数据、接口授权、工程团队与服务网络的组合；集团内部流程借鉴、独立区域集群扩散和模型迁移也属于不同过程。BMW Lydia 采用 Unreal 进行虚拟规划、Debrecen 披露参考中国沈阳与德国莱比锡流程，以及 BYD 关于车端计算、云端开发和虚拟工厂规划的公告，分别说明规划、集团知识流动与企业计划的不同证据边界。[12][9][11] 高交会官网截至 2026 年 10 月 23 日仅预告未来论坛拟讨论具身智能及 Sim2Real 等议题，本篇仅将其作为公共议程背景。[18] 文章进一步提出按任务、接口、版本、故障恢复、人员授权和时间阶段验证技术贡献的比较框架。现有证据无法估计中国工厂的普遍采用率、平均收益或长期可靠性；本篇未开展工厂实地调查、访谈或计量因果识别，也不是穷尽性系统综述。结论应理解为机制分析和可检验命题，而非对具体企业绩效或行业总体效果的实证估计。

SVSAC - sv-sac.org

SVSAC | sv-sac.org

参考文献

[1] Zhao T Z, Kumar V, Levine S, Finn C. ALOHA / ACT project page: Learning Fine-Grained Bimanual Manipulation with Low-Cost Hardware[EB/OL]. 2023. https://tonyzhaozh.github.io/aloha/.

[2] Robotics: Science and Systems 2023. Learning Fine-Grained Bimanual Manipulation with Low-Cost Hardware: conference program author page[EB/OL]. 2023. https://roboticsconference.org/2023/program/papers/016/.

[3] Braojos J, Benitez J, Llorens J, Ruiz L. Impact of IT integration on the firm's knowledge absorption and desorption[J]. Information & Management, 2020, 57(7): 103290. https://doi.org/10.1016/j.im.2020.103290.（仅核读元数据与摘要）

[4] U.S. Department of Commerce, Bureau of Industry and Security. Revision to License Review Policy for Advanced Computing Commodities[Z]. 2026-01-15. 91 FR 1684–1689. https://www.govinfo.gov/content/pkg/FR-2026-01-15/pdf/2026-00789.pdf.

[5] 中华人民共和国商务部新闻办公室. 2026 年 1-8 月全国吸收外资 4799.5 亿元人民币[EB/OL]. 2026-09-18. https://www.mofcom.gov.cn/xwfb/rcxwfb/art/2026/art_bd939b758a6243728e1f294973c5b2f2.html.

[6] Zhao T Z, Kumar V, Levine S, Finn C. Learning Fine-Grained Bimanual Manipulation with Low-Cost Hardware[C]//Robotics: Science and Systems XIX. 2023. https://doi.org/10.15607/RSS.2023.XIX.016.

[7] Tang B, Lin M A, Akinola I, et al. IndustReal: Transferring Contact-Rich Assembly Tasks from Simulation to Reality[C]//Robotics: Science and Systems XIX. 2023. https://doi.org/10.15607/RSS.2023.XIX.039.

[8] NVIDIA Corporation. Foxconn develops physical-AI-enabled smart factories with digital twins[EB/OL]. 页面无明确发布日期，accessed 2026-10-23. https://www.nvidia.cn/case-studies/foxconn-develops-physical-ai-enabled-smart-factories-with-digital-twins/.

[9] BMW Group. BMW Brilliance Plant Lydia inaugurated: Digitalization empowered vehicle plant sets new standards for future-oriented vehicle production[EB/OL]. 2022-06-23. https://www.press.bmwgroup.com/global/article/detail/T0401453EN/bmw-brilliance-plant-lydia-inaugurated:-digitalization-empowered-vehicle-plant-sets-new-standards-for-future-oriented-vehicle-production?language=en.

[10] BMW Group. BMW Group and NVIDIA take virtual factory planning to the next level[EB/OL]. 2021-04-13. https://www.press.bmwgroup.com/global/article/detail/T0329569EN/bmw-group-and-nvidia-take-virtual-factory-planning-to-the-next-level?language=en.

[11] BMW Group. BMW Group Plant Debrecen enters the finish straight: Heartbeat of the plant comes to life with ramp-up of assembly[EB/OL]. 2025-03-27. https://www.press.bmwgroup.com/global/article/detail/T0449177EN/bmw-group-plant-

SVSAC | sv-sac.org

debrecen-enters-the-finish-straight:-heartbeat-of-the-plant-comes-to-life-with-ramp-up-of-assembly?language=en.

[12] NVIDIA Corporation. NVIDIA DRIVE Powers Next Generation of Transportation — From Cars and Trucks to Robotaxis and Autonomous Delivery Vehicles[EB/OL]. 2024-03-18. https://investor.nvidia.com/news/press-release-details/2024/NVIDIA-DRIVE-Powers-Next-Generation-of-Transportation--From-Cars-and-Trucks-to-Robotaxis-and-Autonomous-Delivery-Vehicles/default.aspx.

[13] Midea Group Co., Ltd. 2026 Interim Results Announcement and Interim Report[EB/OL]. 2026-08-28. https://www1.hkexnews.hk/listedco/listconews/sehk/2026/0828/2026082802074.pdf.（PDF 报告第 50–52 页；中期财务结果未经审计）

[14] Branstetter L, Maskus K E. Global Knowledge Flows, Absorptive Capacity and Capability Acquisition: Old Ideas, Recent Evidence and New Approaches[A]//Taubman A, Watal J, eds. Trade in Knowledge: Intellectual Property, Trade and Development in a Transformed Global Economy. Cambridge: Cambridge University Press, 2022: 405–430. https://doi.org/10.1017/9781108780919.017.可读副本：https://www.wto.org/english/tratop_e/trips_e/trip_30062023_e/chapter13_maskus_branstetter.pdf.

[15] Sculley D, Holt G, Golovin D, et al. Hidden Technical Debt in Machine Learning Systems[C]//Advances in Neural Information Processing Systems 28. 2015: 2503–2511. https://papers.neurips.cc/paper/5656-hidden-technical-debt-in-machine-learning-systems.pdf.

[16] Lean Enterprise Institute. Takt Time; Cycle Time; Value Stream Mapping[EB/OL]. https://www.lean.org/lexicon-terms/takt-time/; https://www.lean.org/lexicon-terms/cycle-time/; https://www.lean.org/lexicon-terms/value-stream-mapping/.（官方词典定义；非 AI 应用效果研究）

[17] 国家互联网信息办公室. 促进和规范数据跨境流动规定[Z]. 2024-03-22. https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm.

[18] 中国高新技术论坛官网. 中国高新技术论坛（2026）[EB/OL]. 页面访问于 2026-10-23；活动预告日期为 2026-11-26. https://www.chtf.com/luntanjihuodong/gaoxinluntan/.

SVSAC | sv-sac.org