

工业智能每日观察：美国七州供水设施遭网络攻击，OT 安全防线告急

中国高技术产业发展促进会新质生产力工作委员会

博雅云创 & 中科创新驱动

2026 年 8 月 5 日星期三

摘要

最新产业信息显示，工业智能正在同时面对关键基础设施安全、机器人供应链重构、低空交通基础设施和制造业基础模型投资四类问题。美国多州供水设施遭受网络攻击，部分系统被迫转入人工操作，暴露小型公用事业在 PLC、远程接入和身份管理方面的薄弱环节；印度 Ati Robotics 通过本地电动车零部件供应链和自研驱动系统，构建低中国依赖的工业移动机器人，并计划扩大美国组装；Joby Aviation 与 Atoms 合作建设连接电动垂直起降飞行器和无人驾驶汽车的交通枢纽；风险投资机构 Felicis 则增设硬科技合伙人，把制造基础模型、工业机器人和硬件开发工具列为重点。工业 AI 竞争正在由单机能力延伸到安全、供应链、基础设施和工程软件。

目录

一、美国供水设施遭攻击，OT 安全再次暴露薄弱环节	3
二、Ati Robotics 以低中国依赖供应链切入美国工厂	3
三、Joby 与 Atoms 合作建设空中交通枢纽	4
四、Felicis 增设硬科技合伙人，制造基础模型进入投资视野	5

趋势观察	5
-------------	----------

参考资料	6
-------------	----------

一、美国供水设施遭攻击，OT 安全再次暴露薄弱环节

《卫报》8 月 4 日报道，美国至少七个州的供水和污水处理设施近期遭受网络攻击，其中明尼苏达州约 30 个系统受到影响，部分单位转入人工操作。路透社此前援引美国网络安全与基础设施安全局警告称，攻击者正在加强对供水设施、远程控制设备和工业控制系统的探测。

供水系统通常使用 PLC、SCADA、远程维护终端和第三方通信设备。许多中小型公用事业单位预算有限，设备运行周期长，默认口令、暴露端口、共享账号和未及时更新的软件仍然存在。攻击者未必需要掌握复杂工业工艺，只要获得远程访问权限，就可能干扰泵站、阀门、报警或监控界面。

这类事件提醒工业企业，OT 安全不能只依赖外围防火墙。首先要建立完整资产清单，识别哪些控制器和工程站能够从外部访问；其次应分离生产网络与办公网络，对远程维护采用多因素认证和一次性授权；再次要保留离线备份、人工操作流程和异常工况演练。

工业 AI 和智能体进入控制环境后，风险还会增加。用于诊断和运维的智能体可能拥有读取设备状态、修改参数或生成控制指令的能力，因此必须设置只读模式、命令白名单、双人审批和可回放日志。自动化水平越高，故障时回到安全状态的能力越重要。

二、Ati Robotics 以低中国依赖供应链切入美国工厂

《连线》8 月 4 日报道，印度机器人公司 Ati Robotics 通过印度电动车零部件供应链、自研感应电机和执行器系统，构建了中国零部件占比较低的自主移动机器人。公司产品包括托盘搬运机器人和可牵引约 1 万磅载荷的工业牵引车，并计划扩大美国密歇根州的组装能力。

Ati 并非只销售移动底盘。公司官网显示，其平台连接 ERP、MES、

实时车间数据和机器人调度，通过 AI 代理协调物料流动。目前已进入 70 多座工厂，累计完成约 200 万次任务，任务成功率达到 99%。

这条新闻的价值在于，机器人供应链正在从“整机国产化”转向“关键功能模块可替代”。工业机器人涉及电机、减速器、电池、传感器、控制器、计算平台和安全认证，完全摆脱单一国家供应链并不现实，但企业可以优先掌握影响性能和交付的核心部件。

对制造企业而言，供应链来源只是采购判断的一部分。还需要考察机器人能否与现有 MES 和仓储系统连接、故障后是否容易维修、备件能否长期供应，以及在多品牌车队中能否统一调度。Ati 强调与其他厂商机器人协同，说明工业移动机器人竞争正从硬件参数转向车间级物料编排。

三、Joby 与 Atoms 合作建设空中交通枢纽

Axios 8 月 4 日报道，电动垂直起降飞行器企业 Joby Aviation 与 Travis Kalanick 领导的机器人和工业自动化公司 Atoms 建立合作，计划开发面向空中出租车的交通枢纽。相关设施将承担起降、充电、乘客换乘和地面交通连接，并优先考虑佛罗里达、纽约、得克萨斯和加利福尼亚等市场。

低空交通商业化不只取决于飞行器性能，还需要地面工程体系。枢纽必须解决高功率充电、消防、噪声、航班调度、气象监测、乘客安检和与无人驾驶汽车的衔接。任何一个环节不足，都可能限制飞行器利用率。

Atoms 此前完成 17 亿美元融资，并将业务延伸到运输、采矿、建筑和食品生产等“重物理世界”行业。与 Joby 合作显示，它正在把机器人、软件调度和基础设施运营能力组合起来，而不是只开发单一机器人产品。

这类枢纽适合采用数字孪生进行容量和流程验证。运营方可以在建设前模拟飞行器到达、充电排队、乘客换乘和异常天气，投运后再把真实数据回流模型，优化站点布局和设备维护。低空经济的工业软件入口，正在从飞控扩展到站场和网络运营。

四、Felicis 增设硬科技合伙人，制造基础模型进入投资视野

Business Insider 8 月 3 日报道，风险投资机构 Felicis 聘请 Graham Littlehale 担任合伙人，专注航空航天、国防、能源、制造和机器人。Felicis 此前投资 CoreWeave、Crusoe 和 Skild AI，新岗位将进一步加强其在“物理世界软件化”方向的布局。

Littlehale 明确提到“制造基础模型”，即帮助产品从概念、设计走向生产的 AI 系统；同时关注加速硬件开发的数字工具，以及面向建筑等行业的任务型机器人。这一投资逻辑与消费级通用智能体不同，更重视 CAD/CAE、工艺知识、供应链和现场数据。

制造基础模型短期内很难像语言模型一样直接通用。不同工厂的设备、材料和质量标准差异较大，模型需要与规则、机理、仿真和确定性控制结合。更现实的产品路径，是先在设计检查、工艺规划、机器人编程和异常诊断中形成可验证能力。

资本进入有助于扩大研发投入，但工业项目最终要接受交付周期、可靠性和投资回报检验。能够把模型能力转化为标准化工程流程的公司，才可能从项目制服务走向平台化收入。

趋势观察

当天四条动态说明，工业智能正在进入系统竞争：供水攻击要求 OT 系统具备隔离和恢复能力，Ati Robotics 展示供应链与物料编排的重要性，Joby 与 Atoms 把 Physical AI 延伸到交通基础设施，Felicis 则把制造基础模型纳入资本配置。未来工业 AI 的价值不只来自更聪明的算法，而来自安全可控、供应稳定、流程可验证和工程可复制。

参考资料

1. The Guardian: 《US water facilities targeted by cyberattacks in at least seven states》, 2026-08-04。用途: 核验多州供水设施受攻击及部分系统转入人工操作。<https://www.theguardian.com/technology/2026/aug/04/us-cyber-attacks-water-minnesota-iran>
2. Reuters: 《US cyber defense agency warns of increased hacker targeting of water utilities》, 2026-07-30。用途: 补充美国官方对供水和工业控制系统风险的预警。<https://www.reuters.com/world/us-cyber-defense-agency-warns-increased-hacker-targeting-water-utilities-2026-07-30/>
3. Wired: 《How One Startup Built a (Mostly) China-Free Robot》, 2026-08-04。用途: 核验 Ati Robotics 供应链、自研部件、产品和美国扩产计划。<https://www.wired.com/story/how-one-startup-built-a-mostly-china-free-robot>
4. Ati Robotics: 《The Material Orchestration System for Today' s Factory》, 持续更新。用途: 补充工厂数量、任务成功率、ERP/MES 连接和物料编排能力。<https://www.atirobotics.ai/>
5. Ati Robotics: 《Ati Motors Becomes Ati Robotics》, 2026-04-22。用途: 补充公司从移动机器人向全栈物料编排平台转型。<https://www.atirobotics.ai/resources/educational-content/ati-motors-becomes-ati-robotics/>
6. Axios: 《Future mobility hubs link air taxis, robotaxis》, 2026-08-04。用途: 核验 Joby 与 Atoms 合作及交通枢纽规划。<https://>

www.axios.com/2026/08/04/mobility-hubs-air-taxis-robotaxis-joby-atoms-kalanick

7. Financial Times: 《Uber founder Travis Kalanick raises \$1.7bn for new start-up》, 2026-07-22。用途: 补充 Atoms 融资、工业自动化范围和资本结构。<https://www.ft.com/content/149b3a6e-b004-4e27-a9de-52e41b47404e>
8. Business Insider: 《The VC firm behind Shopify is doubling down on robotics and defense》, 2026-08-03。用途: 核验 Felicis 聘任、制造基础模型和硬科技投资方向。<https://www.businessinsider.com/felicis-hires-graham-littlehale-to-lead-hard-tech-startup-focus-2026-8>
9. FCC: 《FCC Adds Foreign-Produced Power Inverters and Robots to Covered List》, 2026-07-28。用途: 补充机器人供应链安全 and 市场准入背景。<https://www.fcc.gov/document/fcc-adds-foreign-produced-power-inverters-and-robots-covered-list-0>
10. arXiv: 《2026 Roadmap on Artificial Intelligence and Machine Learning for Smart Manufacturing》, 2026-04-05。用途: 补充工业 AI 在数据、数字孪生、机器人、可靠性和基础模型方面的技术路线。<https://arxiv.org/abs/2605.00839>

联系我们，请扫描二维码



新质生产力工作委员会
官方公众号



工业智能算网
gyznsw.cn

新质生产力工作委员会：

中国高技术产业发展促进会新质生产力工作委员会，专注于推动工业人工智能、智能制造、数字化转型等前沿技术发展，为企业提供政策解读、技术咨询和产业对接服务。

工业智能算网：

专注于工业人工智能、新质生产力、工业软件 CAE、智能制造等前沿技术。提供每日动态分析、技术趋势解读、解决方案分享，推动工业智能化转型。

网站地址：<https://gyznsw.cn>