工业智能每日观察：多 Agent 进入核电 OT，非只读动作仍需人工授权

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 10 日星期一

摘要

工业智能当天最值得关注的增量，集中在一个非常具体的问题：AI 怎样真正进入 OT 环境。DEF CON 34 的 ICS Village 刚刚收官，多项项目把多 Agent、数字孪生和工业协议直接放进可验证测试环境。NICSSIM 以小型模块化反应堆为对象，设置监督 Agent、只读漏洞分析 Agent、修复 Agent 和独立安全审计 Agent；mrhOTshOT 则把工业协议动作封装成 LLM 可调用工具，让 Agent 根据实时过程状态动态组合攻击序列；ICSForge 提供 500 多个安全验证场景，覆盖 10 种工业协议和 68 项 MITRE ATT&CK for ICS 技术。与此同时，Forterro–Orderwise 产品负责人 8 月 9 日提出，AI 正在推动 ERP 从“记录系统”转向参与生产计划、仓储和供应链决策的智能运营层。

目录

一、NICSSIM：多 Agent 进入核电 OT，但最终控制权仍交给人

ICS Village 展示的 NICSSIM 是一套完全软件化的小型模块化反应堆 ICS 测试环境，可建模、部署、监测和分析 1—3 个 SMR 组成的虚拟机组，让安全研究在不接触真实核设施的条件下进行。

它最值得关注的不是“核电用了 AI”,而是 Agent 架构本身:监督 Agent 作为唯一协调入口，只读漏洞分析 Agent 负责发现问题，修复 Agent 负责提出处置动作，独立安全审计 Agent 检查结果；分析环境和目标 ICS 环境严格分离，非只读动作必须经过人类授权。

项目团队报告称，在 7 种模型、4 家模型提供商的测试中，单 SMR 环境最高响应成功率达到 0.96，三反应堆场景约 0.91，并同步比较延迟、Token 与成本。其设计还把 ISA/IEC 62443 合规映射放进流程。

这比“让大模型直接控制工厂”现实得多：Agent 首先在数字孪生环境内分析和验证，安全审计 Agent 与人类再对高风险动作把关。对于油气、电力、化工等行业，这种“仿真—分析—审计—人工批准—执行”的链条，比完全自主控制更可能成为近期工业 AI 落地形态。

二、mrhOTshOT：工业协议开始被封装成 Agent 工具

ICS Village 另一项演示 mrhOTshOT 走向了相反方向。它将历史重大 ICS 攻击重新构造成完整攻击链，覆盖 Windows 初始访问、横向移动、工程站进入、工业协议原生过程操纵以及物理影响。更关键的是，其 Agentic Attack Emulation Framework 把每一个工业协议动作都暴露为可调用工具，由 LLM Agent 读取实时过程状态并动态组合攻击序列，而不是执行固定脚本。

项目现场演示涉及 10 个分布式 PLC 以及 Modbus、TriStation、S7comm

等真实工业协议场景。研究者明确指出，这种方法展示了“AI 辅助 ICS 攻击编排”可能是什么样子。

这并不意味着 Agent 已经可以自动攻破所有工厂，但它降低了复杂攻击链的编排门槛。过去攻击者需要同时理解工业协议、PLC 行为和工艺逻辑；Agent 工具化后，一部分协议操作和攻击步骤可以通过统一接口组织。

三、IRONMAP：互联网暴露的 OT 设备规模值得重新审视

8 月 9 日的 IRONMAP 议题披露，项目团队在其持续扫描研究中编目了超过 550 万个面向公网的 ICS/OT 资产，其中超过 225 万个被标记为高风险。团队还报告识别超过 24.2 万个 EtherNet/IP 设备、约 50 万个 Modbus 设备，以及 149 套直接暴露互联网的自动油罐液位系统。需要强调的是，这些数字属于项目方研究结果，并非政府或行业官方统计。

对于制造企业而言，真正的问题不是“全世界到底暴露了多少设备”，而是自己的 PLC、工业网关、远程维护接口、楼宇系统和能源控制设备中，还有多少历史遗留资产可以直接从互联网访问。

四、ICSForge 把 OT 安全从“采购了什么”变成“到底测出了什么”

ICSForge 提供 500 多个真实 OT 流量场景，覆盖 Modbus/TCP、DNP3、S7comm、IEC-104、OPC UA、EtherNet/IP、BACnet/IP、MQTT、GOOSE、PROFINET DCP 等 10 种协议，并映射 MITRE ATT&CK for ICS v18 中的 68 项技术，占其列举 83 项技术的 82%。

其设计并不攻击真实生产设备，而是在指定 Sender—Receiver 架构中生成真实协议流量和 PCAP，用来验证 IDS、OT 网络监测、安全分区、防火墙和 ACL 究竟能不能看到和阻断预期攻击。

随着 AI 安全产品进入工厂，“覆盖率证明”会越来越重要。企业不能只采购一个宣称具备 AI 分析能力的产品，而需要反复确认：设备升级、网络改造、规则变化之后，检测和防护能力是否仍然成立。

五、ERP 正在从记录系统走向主动运营层

Forterro 旗下 Orderwise 高级产品经理 Carrie Tallett 在 8 月 9 日发表的行业文章中指出，AI 正推动 ERP 从记录交易的后台系统，转向生产计划、仓储管理和供应链决策的主动参与者。文章认为，AI 可以连接 ERP、仓储系统和生产数据，在需求、库存或设备可用性变化时辅助调整生产与物流。

真正困难的环节仍然是闭环。物料编码、BOM、库存、工艺和设备数据如果不一致，模型产生的“智能建议”很难进入实际执行。工业 AI 价值因此越来越依赖统一数据底座、系统接口、审批和可追溯机制。

趋势观察

DEF CON 的 OT 项目展示了 AI 在工业系统中的双向效应：多 Agent 可以辅助防御，也可能降低攻击编排门槛；ICSForge 则把安全能力拉回到可测量覆盖率；ERP 的变化进一步说明 AI 正在进入核心业务决策链。下一阶段工业 AI 最关键的词不会是“自主”，而更可能是可验证、可审计、可回退。

参考资料

1. ICS Village / DEF CON 34 | 《NICSSIM —Multi-Agent Cyber Defense Framework for Distributed Nuclear OT Systems》 | 2026-08-08

2. ICS Village ｜《Give an AI Industrial Protocol Tools and Watch What It Destroys》 ｜ 2026-08-08

3. ICS Village ｜ 《Five Million Industrial Control Systems Walk Into a Bar: What IRONMAP Found》 ｜ 2026-08-09

4. ICS Village ｜ 《ICSForge: Open-Source OT/ICS Security Coverage Validation Platform》 ｜ 2026-08-07

5. ICS Village ｜ DEF CON 34 完整议程 ｜ 2026-08-06 至 08-09

6. Automation News ｜ Carrie Tallett，《Beyond ERP: how AI is connecting the smart factory》 ｜ 2026-08-09

7. Digital Twin Consortium ｜ Multi-Agent Front-Running Simulation 相关资料 ｜ 2026-08

8. ISA ｜ ISA/IEC 62443 系列标准 ｜ 持续更新

9. Cisco ｜ 《2026 State of Industrial AI Report》 ｜ 2026 年

10. arXiv ｜《2026 Roadmap on Artificial Intelligence and Machine Learning for Smart Manufacturing》 ｜ 2026 年

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