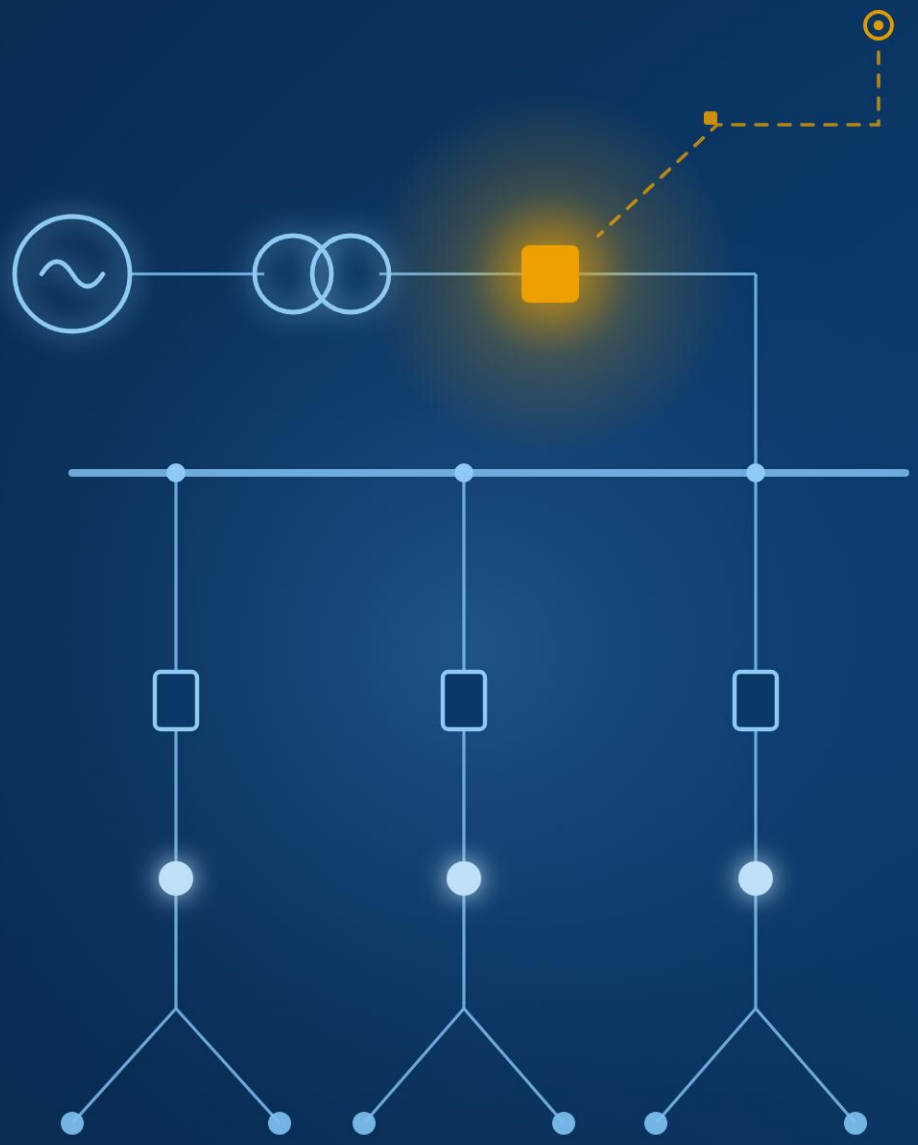

EAOS

Enterprise AI Operating System

پلتفرم رِنجِ سایبری صنعتی و دوقلوی دیجیتالِ فرایند

FORGE-OT

شبیه‌سازی فرایند فیزیکی و دوقلوی دیجیتال

شبیه‌سازی حریف بر پایهٔ ATT&CK for ICS

اعتبارسنجی فایروال، جداسازی و تشخیص

شواهد ممیزی‌پذیرِ IEC 62443 و NERC CIP

سکوی بومی، تمام برون‌خط

Air-Gap — بدون هیچ وابستگی به سرویس ابری خارجی

معرفی اجمالی محصول ۰۱

سه موتور، یک دوقلوی دیجیتال — در قالبِ یک محصول

پلتفرمِ رنجِ سایبری صنعتی و دوقلوی دیجیتال

مجموعه‌ای از قابلیت‌های به‌هم‌پیوستهٔ امنیتِ حوزهٔ عملیاتی (OT) که به‌جای شش ابزارِ جدا، در یک محصولِ واحد و بومی عرضه می‌شوند:

۱ — شبیه‌سازی محیط صنعتی: توپولوژیِ آگاه از مدلِ Purdue، دستگاه‌های مجازی (vPLC · vRTU · vIED · vSCADA · vHMI) و هشت موتورِ پروتکلِ صنعتیِ واقعی

۲ — دوقلوی دیجیتالِ فرایندِ فیزیکی: دینامیکِ ژنراتور، ترانسفورماتور، بریکر، پمپ، مخزن و خطِ لوله — تا موفقیتِ حمله با «پیامدِ فیزیکی» سنجیده شود، نه با عبورِ بسته

۳ — موتورِ حملهٔ سایبری: ۷۹ تکنیکِ MITRE ATT&CK for ICS، فازینگِ پروتکل، بازپخشِ فرمان، مردمیانی و تزریقِ دادهٔ نادرست

۴ — موتورِ اعتبارسنجیِ امنیت: فایروال، ناحیه‌بندی و کاندوئیت، IDS/IPS و دیودِ داده — با سنجشِ پوشش، MTTD و MTTR

۵ — آزمونِ نفوذِ مرحله‌ای و کاتالوگِ آزمونِ ICS: ۱۹ روش در ۵ فازِ CEH و ۲۴ آزمونِ استاندارد در ۸ دسته

۶ — تحلیل‌گرِ هوشمندِ محلی و گزارشِ امضاشده: تحلیلِ لاگ و PCAP، پیشنهادِ قاعده، و بستهٔ شواهدِ تغییرناپذیرِ نگاشته به IEC 62443 و NERC CIP

چرا این پلتفرم وجود دارد؟

فاصلهٔ میان کنترلی که خریده‌ایم و کنترلی که در روزِ حمله نگه می‌دارد

اثربخشیِ دفاع امروز با «فرض» سنجیده می‌شود، نه با «شاهد»

چهار شکاف، یک ریشه: نبودِ جایی امن برای اثباتِ اینکه کنترل‌ها واقعاً نگه می‌دارند

با FORGE-OT	وضعیت امروز
اعتبارسنجیِ مستقل و تکرارپذیر با seed ثابت و هشِ محیط — نتیجه بازتولیدپذیر است	**ادعای فروشنده و دیتاشیت** نتیجه‌ای که مختصِ محیط شما نیست
قضاوت در سطحِ پیامدِ فیزیکی تریپِ بریکر، سرریزِ مخزن، اضافه‌فشارِ خط لوله	**آزمون در سطحِ بسته** بدون هیچ سنجشی از پیامدِ فیزیکی
محیطِ ایزوله، ایمن‌به‌طورِ پیش‌فرض صفر ریسک برای دارایی زندهٔ صنعتی	**تست در محیطِ تولید ممکن نیست** پستِ برق و پالایشگاه محیطِ آزمایش ندارند
بومی و کاملاً برون‌خط بدون هیچ اتصال به اینترنت یا سرویس ابری	**ابزارِ خارجی و ابری** تحریم‌پذیر، غیرقابلِ استقرار در محیطِ ایزوله

اثباتِ اثربخشی	پیامدِ فیزیکی	کتابخانهٔ تهدیدِ ICS	شواهدِ ممیزی‌پذیر
با شاهد، نه با ادعا	معیارِ قبولی و ردی	ATT&CK تکنیکِ ۷۹	IEC 62443 · NERC CIP

ویژگی متمایزکننده

این پلتفرم از روزِ نخست برای محیطِ ایزوله و بدونِ اتصال به اینترنت (Air-Gap) طراحی شده است. هیچ وابستگی به سرویسِ ابریِ خارجی، هیچ بارگذاریِ امضا یا محتوا از اینترنت، و هیچ به‌روزرسانیِ کنترل‌نشده‌ای وجود ندارد؛ به‌روزرسانیِ کتابخانهٔ تهدید و استانداردها از رسانهٔ آفلاین انجام می‌شود. این یک تصمیمِ معماری در روزِ اول است، نه وصله‌ای بعدی.

چرا ابزارهای موجود کافی نیستند

شبیه‌سازهای شبکه بسته را جابه‌جا می‌کنند اما فیزیکی ندارند؛ دوقلوهای مهندسیِ سازندگان فیزیک را دقیق مدل می‌کنند اما نه حریفی دارند نه اعتبارسنجیِ امنیتی؛ ابزارهای پایشِ تولید خودشان موضوعِ آزمون‌اند، نه جای امنی برای آزمون. مسئله نبودِ ابزار نیست — مسئله این است که هیچ‌کدام «آیا دفاعِ ما پیش از آسیبِ فیزیکی نگه می‌دارد؟» را پاسخ نمی‌دهند.

پنج ستونِ قابلیت، نُه ماژول — یک زنجیرهٔ پیوسته

هر ماژول مالکِ گروهِ نیازمندیِ خودش است؛ خروجیِ هر ستون، ورودیِ ستونِ بعدی می‌شود

شبیه‌سازی
MOD-SIMENG · MOD-PROC

- توپولوژیِ آگاه از Purdue با ناحیه و کاندوئیت
- دستگاهِ مجازی: vPLC · vRTU · vIED · vHMI · vSCADA
- هشت موتورِ پروتکلِ OT با پاسخِ واقعی
- دینامیکِ فرایند: ژنراتور، ترانس، بریکر، پمپ، مخزن

حمله
MOD-ATKENG

- ۷۹ تکنیکِ ATT&CK for ICS در ۱۲ تاکتیک
- فازینگِ پروتکل، بازپخشِ فرمان، مردمیانی
- تزریقِ دادهٔ نادرست به سیگنالِ فرایند
- آزمونِ نفوذِ مرحله‌ای: ۱۹ روش در ۵ فازِ CEH

اعتبارسنجی
MOD-VALENG

- فایروال و اثربخشیِ جداسازیِ ناحیه/کاندوئیت
- پوشش و تأخیرِ تشخیصِ IDS/IPS
- یک‌طرفه‌بودنِ دیودِ داده
- سنجشِ MTTD/MTTR در برابرِ زمانِ‌تاپیامد

تحلیل
MOD-AISA

- تحلیلِ لاگ و PCAP و بازسازیِ زنجیرهٔ حمله
- کشفِ شکافِ تشخیص در پوششِ فعلی
- پیشنهادِ قاعدهٔ تشخیص و قاعدهٔ فایروال
- استنتاجِ کاملاً محلی — بدون خروجِ داده

اثبات
MOD-RPT

- بستهٔ شواهدِ تغییرناپذیر و امضاشده
- نگاشت به IEC 62443 · NERC CIP · NIST
- گزارشِ ساخت‌یافتهٔ «قبل از رفع ← بعد از رفع»
- بازتولیدپذیر از هشِ محیط و seed ثابت

DP-11 **قلبِ محصول: دوقلوی دیجیتالِ فرایندِ فیزیکی**

حمله زمانی «موفق» شمرده می‌شود که پیامدِ فیزیکی بسازد — نه زمانی که بسته‌ای از فایروال عبور کند. همین معیار است که نتیجهٔ آزمون را به کارخانهٔ واقعی قابلِ‌انتقال می‌کند.

- **ایمنیِ پیش‌فرض:** هیچ حالتی از محصول توانِ کنش روی شبکهٔ تولید را ندارد. تنها مسیرِ دستگاهِ واقعی، بنچِ ایزولهٔ سخت‌افزار-در-حلقه است که نقش‌محور اجرا و در دفترِ ممیزی ثبت می‌شود.
- **گیتِ دومنظوره:** محتوای تهاجمی صرفاً برای اعتبارسنجیِ دفاعی در دسترس است؛ اجرای آن نیازمندِ نقشِ صریح، تأیید و ثبتِ ممیزی است و دستورالعملِ حمله به زیرساختِ زنده منتشر نمی‌شود.
- **خودکارسازیِ کامل از راهِ API:** هر کاری که در رابطِ کاربری ممکن است از راهِ API هم ممکن است — تا اعتبارسنجی به‌جای یک رویدادِ سالانه، به گامی در چرخهٔ مهندسی تبدیل شود.

کاربردها

یک زنجیرهٔ واقعی، و آنچه هر ذی‌نفع از آن به دست می‌آورد

از نفوذ تا پیامدِ فیزیکی — و اینکه کدام کنترل واقعاً جلویش را گرفت

هر سناریو تا انتهای زنجیره اجرا می‌شود؛ حکمِ قبولی وقتی صادر می‌شود که کنترل، حمله را **پیش از** آسیبِ فیزیکی متوقف کند

- **برق — تولید و انتقال**
  جعلِ GOOSE/SV یا دستکاریِ تنظیماتِ رله ← **تریپِ نابه‌جای بریکر و خاموشیِ آبشاری**
- **آب و فاضلاب**
  تغییرِ نقطهٔ تنظیمِ تزریقِ مواد یا جعلِ سطحِ مخزن ← **آلودگیِ شیمیایی یا سرریزِ مخزن**
- **نفت و گاز**
  سرکوبِ آلارم به‌همراهِ دستکاریِ کنترلِ فشار ← **اضافه‌فشار، نشتی و دورزدنِ ESD**
- **تولید و صنایع**
  فرمانِ حرکتیِ مخرب به درایو و روبات ← **توقفِ خط، آسیبِ تجهیز و افتِ کیفیت**

ذی‌نفع	آنچه به دست می‌آورد	ذی‌نفع	آنچه به دست می‌آورد
مدیرعامل و هیئت‌مدیره	تصویرِ مدیریتی از ریسکِ فرایند، قابلِ دفاع در برابرِ نهادِ ناظر	تیمِ قرمز	شبیه‌سازیِ حریفِ ICS با پیامدِ فیزیکی، بدون هیچ خطری برای کارخانه
مدیرِ امنیت **(CISO)**	اتصالِ مستقیمِ حمله، اعتبارسنجی، یافته و اقدامِ اصلاحی در یک پرونده	تیمِ آبی و **SOC**	سنجشِ پوششِ تشخیص و MTTD روی ترافیکِ واقعیِ پروتکل‌های صنعتی
مهندسِ **SCADA** و **ICS**	تضمینِ معماری: هیچ آزمونِ خودکاری روی تجهیزِ زنده نمی‌نویسد	واحدِ خرید و تدارکات	مقایسهٔ بی‌طرفانهٔ محصولات تحتِ شرایطِ یکسان و تکرارپذیر
ممیز و واحدِ انطباق	شواهدِ نگاشته‌شده به IEC 62443 و NERC CIP، بازتولیدپذیر در سالِ بعد	سازندهٔ تجهیز و آزمایشگاه	هارنسِ خنثی برای آزمون و صحه‌گذاریِ محصول، همراه با HIL

پوششِ فنی: هشت موتورِ پروتکلِ واقعی، نه یک شبیه‌سازِ ظاهری

اعداد زیر از ممیزیِ داخلیِ ماژول‌ها آمده‌اند — نه از خوداظهاری

۸	۷۹	۲۴	۱۹	۱۲۷
موتورِ پروتکلِ OT	**تکنیکِ ATT&CK for ICS**	**آزمونِ استانداردِ ICS**	**روشِ آزمونِ نفوذ**	**نیازمندیِ کارکردی**
با پاسخِ واقعی و فازینگِ موتور-محور	در ۱۲ تاکتیک، با امکانِ واردکردنِ ماتریسِ بیرونی	در ۸ دسته، نگاشته به IEC 62443 و NIST 800-82	در ۵ فازِ CEH، نگاشته به ICS Cyber Kill Chain	هرکدام با ماژولِ مالک و آزمونِ متناظر

پروتکل‌های صنعتی موتورِ واقعی — ساخت، تجزیه، اعتبارسنجی، فازینگ

Modbus/TCP · Modbus RTU · DNP3 · IEC 60870-5-104 · IEC 61850 GOOSE · OPC UA · EtherNet/IP · PROFINET

پروتکلِ کنتورِ هوشمند از مسیرِ تعریفِ داده‌محورِ پروتکل

DLMS/COSEM · IEC 62056-21 · ANSI C12.18 · ANSI C12.22

تاکتیک‌های ATT&CK for ICS ۱۲ تاکتیک با سنجشِ پوشش

دسترسیِ اولیه · اجرا · پایداری · فرار از دفاع · کشف · حرکتِ جانبی · گردآوری · فرماندهی و کنترل · مهارِ پاسخ · مهارِ کنترل · اثرگذاری بر فرایند · آسیب

دسته‌های آزمونِ ICS ۲۴ آزمون با حکمِ قبول/رد/هشدار

استحکام · احراز هویت · کنترلِ دسترسی · جداسازی · سخت‌سازی · میان‌افزار · پایش · ایمنی

چرا این اعداد اهمیت دارند

یک شبیه‌سازِ ظاهری فقط وانمود می‌کند که پروتکل را می‌فهمد؛ چنین چیزی نه فازینگِ معنادار می‌دهد نه قاعدهٔ تشخیصِ قابلِ‌اتکا. در این پلتفرم هر هشت پروتکل موتورِ واقعی دارند: فریم ساخته، تجزیه، اعتبارسنجی و با آگاهی از ساختار خراب می‌شود. به همین دلیل قاعده‌ای که اینجا آزموده می‌شود، در محیطِ واقعی هم همان رفتار را دارد.

آنچه ادعا نمی‌کنیم

لنگرگاه‌های R1 و بخشِ عمدهٔ R2 امروز کار می‌کنند و با دروازهٔ خودکارِ پذیرش سنجیده می‌شوند. اما کاراییِ بلادرنگِ دیتاپلین روی کارتِ شبکهٔ واقعی و اتصالِ سخت‌افزارِ واقعی روی بنچ، ذاتاً به تجهیزِ فیزیکی نیاز دارند و با نرم‌افزار به‌تنهایی اثبات نمی‌شوند. این‌ها را جزوِ «انجام‌شده» نمی‌شماریم و در بخشِ ۰۸ صریح فهرست کرده‌ایم.

معماری

سه موتورِ مستقل‌اماترکیب‌پذیر، زیرِ یک هستهٔ حاکمیتیِ واحد

دو صفحهٔ استقرار

کنترل‌پلین	رابطِ وبِ سروشدهٔ محلی، هماهنگ‌سازی، RBAC و گزارش — بدون هیچ وابستگیِ ابری
دیتاپلین	مؤلفهٔ بومیِ محلی: پلِ L2/L3، اتصالِ کارتِ شبکه، تایمینگِ بلادرنگ، ورودی‌وخروجیِ HIL
شبکهٔ تولید	هرگز — تنها مسیرِ دستگاهِ واقعی، بنچِ ایزولهٔ HIL با نقشِ کنترل‌شده و ثبتِ ممیزی است

نُه ماژول، هرکدام با مرزِ مشخص

- **MOD-SIMENG · MOD-PROC** — محیطِ صنعتی و فیزیکِ فرایند — موتور ۱
- **MOD-ATKENG** — شبیه‌سازیِ حریف و کتابخانهٔ تهدیدِ ICS — موتور ۲
- **MOD-VALENG** — سنجشِ اثربخشیِ کنترل‌ها در سطحِ بسته و فرایند — موتور ۳
- **MOD-DT** — بستنِ مدلِ فرایند به توپولوژیِ واقعیِ مشتری و هشِ محیط
- **MOD-HIL** — سخت‌افزارِ واقعی در حلقه، تنها روی بنچِ ایزوله
- **MOD-AISA** — تحلیل و پیشنهادِ قاعده، با استنتاجِ کاملاً محلی
- **MOD-RPT** — شواهدِ تغییرناپذیر و گزارشِ چندمخاطبه
- **MOD-PLAT** — کنترلِ دسترسی، ممیزی، API و قفلِ ایمنی برای همهٔ ماژول‌ها

قاعدهٔ مرزبندی

هیچ ماژولی حقِ نوشتنِ مستقیم در پایگاه‌دادهٔ ماژولِ دیگر را ندارد، و هیچ حالتی از سامانه — از جمله حالتِ پیش‌فرض — مسیری برای کنش روی شبکهٔ تولید نمی‌سازد. تنها استثنای دستگاهِ واقعی، بنچِ ایزولهٔ HIL است که انتخابی، نقش‌محور، برون‌خط و کاملاً ثبت‌شده کار می‌کند.

حلقهٔ شاهد

از حمله تا پیامد، تا رفع، تا اطمینان از رفع — و جایگاه دقیقِ هوش مصنوعی

۱ اجرای کمپینِ حمله با seed ثابت
سناریو روی توپولوژی و دوقلوی فرایند اجرا می‌شود — قطعی و تکرارپذیر

▼

۲ سنجشِ پیامد در مدلِ فیزیکی
آیا حمله به تریپ، سرریز یا اضافه‌فشار رسید؟ زمانِ‌تاپیامد ثبت می‌شود

▼

۳ یافته و حکمِ پایه
هر یافته با شدت، نگاشتِ چارچوب و کنترلِ مسئولش ثبت می‌شود

▼

۴ رفعِ مرحله‌ای — کمینه‌ترینِ توالیِ مؤثر
کنترل‌ها یکی‌یکی اعمال می‌شوند تا مشخص شود کدام رفع، به چه ترتیبی، و کدام غیرضروری بود

▼

۵ اجرای دوبارهٔ همان کمپین
با همان seed، تا تفاوت واقعاً به رفع نسبت داده شود نه به تصادف

↻ حلقه تا رسیدن به «مهارشده» یا توقف در فلات تکرار می‌شود

گزارشِ امضاشدهٔ «قبل از رفع ← بعد از رفع»
بستهٔ تغییرناپذیر با هشِ محتوا و امضا — بازتولیدپذیر از هشِ محیط، نگاشته به IEC 62443 و NERC CIP

انطباق با چارچوب‌های مرجع

- **IEC 62443-3-3** و **62443-4-2** — خط‌پایهٔ امنیتِ سامانه و مؤلفه در محیطِ صنعتی
- **NERC CIP** — محیطِ امنیتِ الکترونیکی، پاسخ به حادثه، مدیریتِ تغییر
- **MITRE ATT&CK for ICS** — طراحیِ تکنیک‌ها و سنجشِ پوششِ تاکتیکی
- **NIST SP 800-82** — کنترل‌های امنیتیِ حوزهٔ عملیاتی
- **NIST CSF** — پیوندِ حاکمیت با شناسایی، حفاظت، تشخیص و پاسخ
- **Purdue · ISA-95** — سطح‌بندیِ مرجع و جای‌گذاریِ درستِ دارایی
- **ICS Cyber Kill Chain** — مرحله‌بندیِ زنجیرهٔ نفوذ تا اثرِ فیزیکی
- **CEH** — فازبندیِ روش‌شناسیِ آزمونِ نفوذ

جایگاه هوش مصنوعی

تحلیل‌گرِ هوشمند در این پلتفرم دستیار است، نه تصمیم‌گیرنده. استنتاج کاملاً محلی و برون‌خط انجام می‌شود؛ خروجیِ آن همیشه جدا از نتیجهٔ قطعیِ موتورِ اعتبارسنجی و همراه با درجهٔ اطمینان نمایش داده می‌شود؛ و هیچ قاعده یا تغییری بدون تأییدِ صریحِ انسان اعمال نمی‌شود. خودگردانیِ کامل به لنگرگاهِ R10 موکول شده است.

نردبانِ انتشار: پنج لنگرگاهِ تعریف‌شده، نه یک صفِ ده‌تایی

هر لنگرگاه، مجموعهٔ مشخصی از ماژول‌ها را باز می‌کند؛ مرزِ ایمنی در هیچ‌کدام سست نمی‌شود

ساخته شده
هستهٔ حلقهٔ امن
R1 · MVP
شبیه‌سازی ← حمله ← اعتبارسنجی ← گزارش، با بستهٔ فیزیکِ برق و هستهٔ پلتفرم

در دستِ کار
حرفه‌ای
R2 · Professional
تحلیل‌گرِ هوشمندِ مشورتی، کالیبراسیونِ دوقلو، پهنای کاملِ پروتکل، بستهٔ آب

در دستِ کار
سازمانی
R3 · Enterprise
سخت‌افزار در حلقه روی بنچ ایزوله، هم‌خلبانِ هوشمند، عمقِ نگاشتِ انطباق

آینده
رِنجِ سایبری
R5 · Cyber Range
رزمایشِ تیمیِ سرخ/آبی/بنفش، بازارچهٔ محتوا، هم‌گام‌سازیِ محافظت‌شده از مسیرِ دیود

آینده
خودگردان
R10 · Autonomous
اعتبارسنجیِ پیوسته و حلقه‌بسته روی دوقلوی زنده؛ جداسازیِ خطوطِ محصولِ مستقل

آنچه امروز اثبات‌شده است

- **حلقهٔ کاملِ امن** — شبیه‌سازی، حمله، اعتبارسنجی و گزارش، سرتاسر اجرا می‌شود
- **هشت موتورِ پروتکل** — با پاسخِ واقعی و فازینگِ موتور-محور، نه پاسخِ ساختگی
- **حلقهٔ بستهٔ رفع** — رفعِ مرحله‌ای و گزارشِ امضاشدهٔ قبل→بعد
- **اتصالِ HIL** — فقط روی بنچ ایزوله؛ در حالتِ آزمایشگاهی رد می‌شود

۸۵۰	۱۱/۱۱	۹
آزمونِ خودکارِ سبز	بخشِ دروازهٔ پذیرش	ماژولِ تعریف‌شده

درصدها از ممیزیِ داخلیِ ماژول‌ها و دروازهٔ خودکارِ پذیرش آمده‌اند، نه از خوداظهاری. سامانه‌ای که مأموریتش سنجشِ آمادگی بر پایهٔ شواهد است، نمی‌تواند وضعیتِ خودش را بدون شاهد اعلام کند.

آنچه هنوز ادعا نمی‌شود

- کارایی بلادرنگِ دیتاپلین روی کارتِ شبکهٔ واقعی
- اتصالِ تجهیزِ فیزیکیِ واقعی روی بنچِ سخت‌افزار-در-حلقه
- کالیبراسیونِ دوقلو در برابرِ دادهٔ یک کارخانهٔ واقعی
- آزمونِ کارایی و نفوذِ سرتاسری در مقیاسِ عملیاتی
- تأییدِ نهاییِ تصمیم‌های معماری توسط کارفرما

گامِ بعدیِ پیشنهادی

یک استقرارِ آزمایشی روی توپولوژیِ واقعیِ یکی از سایت‌های شما، در محیطِ ایزوله و با بستهٔ فیزیکیِ برق: تعریفِ توپولوژی و ناحیه‌بندی، اجرای یک کمپینِ کاملِ حمله تا پیامدِ فیزیکی، و تحویلِ گزارشِ امضاشدهٔ «قبل از رفع ← بعد از رفع» به‌عنوانِ نمونهٔ ملموسِ شواهد. تمامِ این چرخه بدونِ هیچ اتصالی به اینترنت و بدونِ هیچ تماسی با شبکهٔ تولید اجرا می‌شود.

EAOS

Enterprise AI Operating System

آیا دفاعِ ما جلوی تهدیدِ امروز را
پیش از رسیدن به فرایندِ فیزیکی می‌گیرد؟

FORGE-OT برای پاسخ‌دادن به همین یک پرسش ساخته شده است — و برای اینکه پاسخ، به‌جای ادعا، یک بستهٔ شواهدِ امضاشده و بازتولیدپذیر باشد.

استقرارِ درون‌سازمانی
تک‌گره، روی سخت‌افزارِ خودتان

کاملاً برون‌خط
بدون هیچ اتصالِ خروجی

ایمن به‌طورِ پیش‌فرض
بدون مسیر به شبکهٔ تولید

این سند صرفاً جهتِ معرفی است و تعهدِ قراردادی ایجاد نمی‌کند.
قابلیت‌های نشان‌داده‌شده به لنگرگاهِ انتشارِ مربوطه مقیدند؛ آنچه هنوز ساخته نشده، به‌صراحت در بخشِ ۰۸ فهرست شده است.