IFIP WG MEETING · 2026

Security analysis in real-world OT scenarios: the HASE approach

Domenico Cotroneo (d.cotroneo@charlotte.edu)

Meera Sridhar (msridhar@charlotte.edu)

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Made with GAMMA

THE PROBLEM

The Research Problem

OT is insecure by design

Modbus, DNP3, S7, and EtherNet/IP use cleartext communication, weak or no authentication, and implicit trust. AI is now automating exploitation of these protocols.

What the literature shows

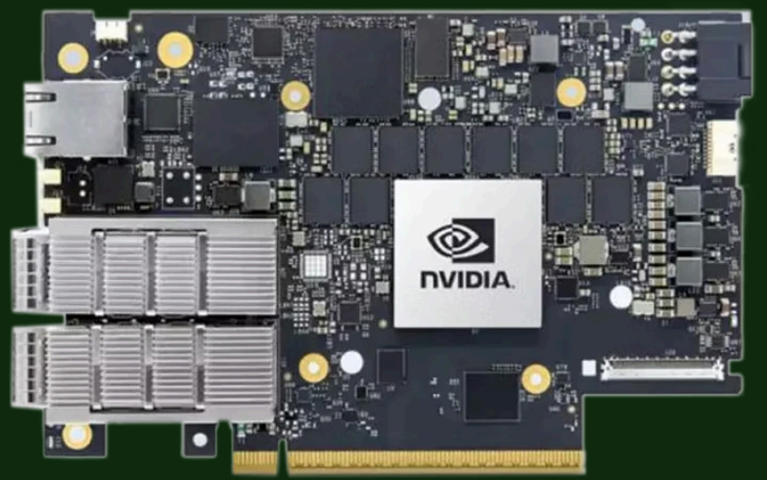
- State-of-the-art IDS evaluations are predominantly benchmark-driven, leading to near-perfect detection results.
- However, benchmark accuracy does not translate into resilience under adaptive attack conditions.
- Performance deteriorates substantially in evolving operational environments, with a 15–22% F1 loss.

Nowadays, the problem is not detecting attacks, but engineering AI defenses that remain effective against continuously learning adversaries.

Made with GAMMA

HASE PROJECT: HARDWARE ACCELERATED CYBER SECURITY AT THE EDGE

Hardware-accelerated AI defense



DPU NVIDIA BlueField

A server inside the NIC, with ARM cores, memory, and accelerators.

It is responsible for:

- Inspecting line-rate traffic transparently, without affecting the control loop or adding latency.

NVIDIA Morpheus

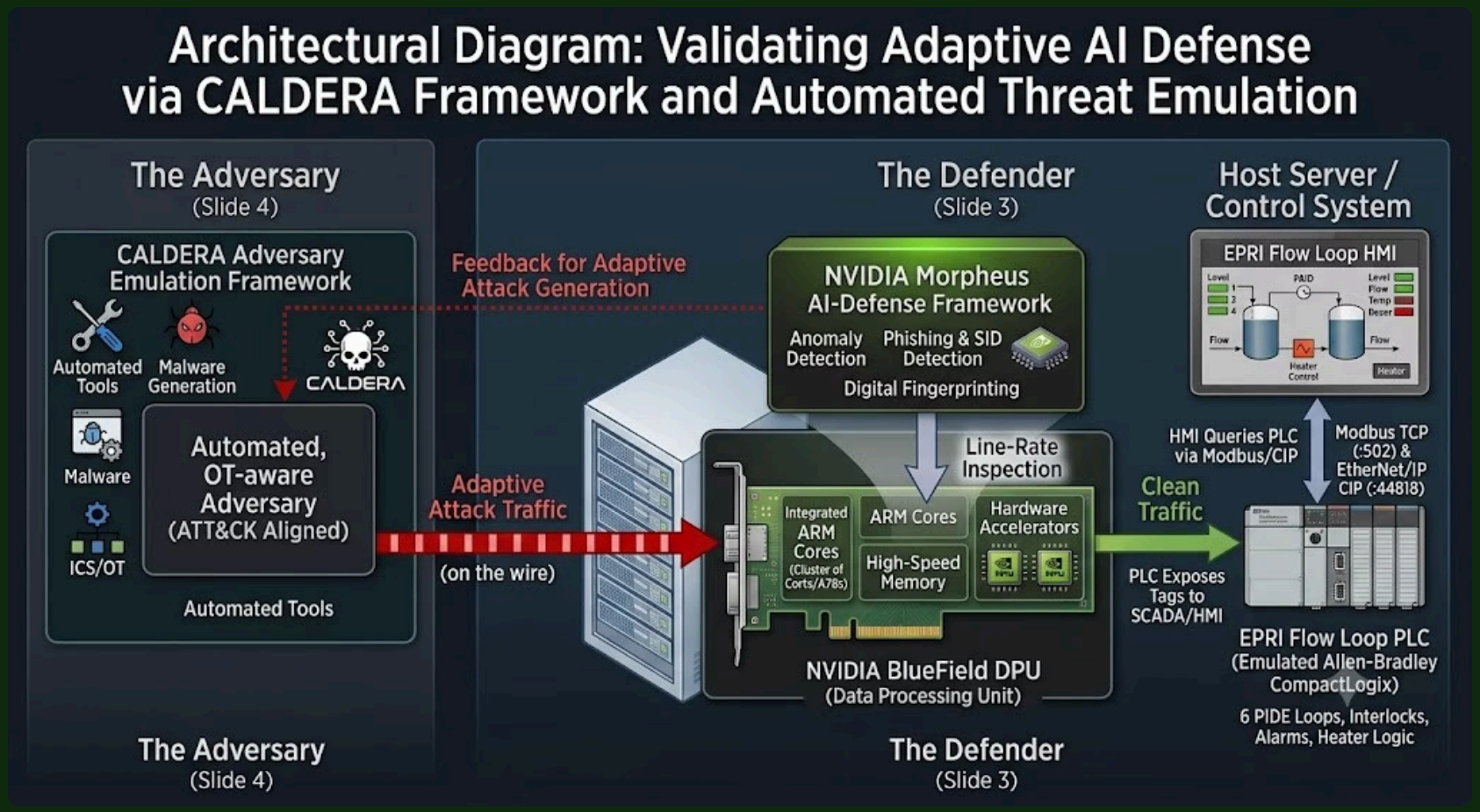
A GPU-accelerated, streaming AI defense framework built on RAPIDS (cuDF, cuML, Triton). Its pipelines include digital fingerprinting, anomaly and ransomware detection, sensitive-data detection, and phishing detection.

Morpheus runs on the *same* BlueField DPU at the core of HASE, making it the natural defensive counterpart in an AI-vs-AI test.

Made with GAMMA

THE ADVERSARY

OT-aware adversary emulation



MITRE Caldera

Declarative adversary emulation with a C2 server and Sandcat agent. **Facts** make it adaptive rather than scripted, so the attack chain adjusts to what it finds on the target.

MITRE ATT&CK

A shared vocabulary for industrial control systems, with tactics.

Every ability is tagged with ATT&CK.

HASE CLI toolkit (haseplugin)

A protocol-agnostic CLI invoked by Caldera.

Add a protocol once, and every adversary inherits it.

Made with GAMMA

THE INNOVATION

Cratos integrates attacker and defender in one real hybrid simulation framework

A hybrid cyber-physical framework that seamlessly integrates real industrial controllers, AI pipelines, and virtualized OT environments.

Framework	Real OT protocol enforcement	Adaptive autonomous attacker	AI defender in the loop	Closed co-evolution loop
ARC [9]	□ abstract twin	◑ DRL paths	✓	◑ no protocol
Evo-Defender [10]	✓ real S7-1200	□ LSTM-scripted	◑ incremental	□ no feedback to attacker
L2M-AID [11]	◑ SWaT, offline	□ offline replay	✓ MARL	□ offline
MALF [12]	✓ multi-proto PLCs	✓ adaptive fuzz	□ no defender	□
Cratos	✓ EtherNet/IP + CIP + Modbus	Caldera-based, → adaptive payload	→Morpheus / IDS	by design

Cratos starts with the substrate the others miss, and builds the closed loop. (✓ = today, → = roadmap)

Made with GAMMA

FIRST RESULTS · HASE

A working pipeline that infers the EPRI demo plant

Faithful substrate (~70% fidelity vs. real CompactLogix)

Two coupled tanks held at setpoint, with real cross-tank transfer, mode-correct heating, latched/acknowledged alarms, and a real Logix identity plus L5X symbolic tag namespace.

Autonomous CIP recon, end to end (terminal block)

Discover, identify, enumerate tags and objects, then batch-read in one session to monitor EtherNet/IP traffic.

CIP write path is now functional → process-control impairment next.

Made with GAMMA

WHERE WE STAND

Ongoing research activities

WHAT WE HAVE (today)

- ✅ Faithful EPRI flow-loop digital twin, at approximately 70% fidelity to a real CompactLogix
- ✅ Autonomous CIP reconnaissance, end to end over EtherNet/IP
- ✅ Working end-to-end pipeline, from Caldera operator to OT process
- ✅ Functional CIP write path

WHAT COMES NEXT (roadmap)

- ➡️ Defender and IDS in the loop (Morpheus class)
- ➡️ AI-vs-AI experimental scenario

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Made with GAMMA