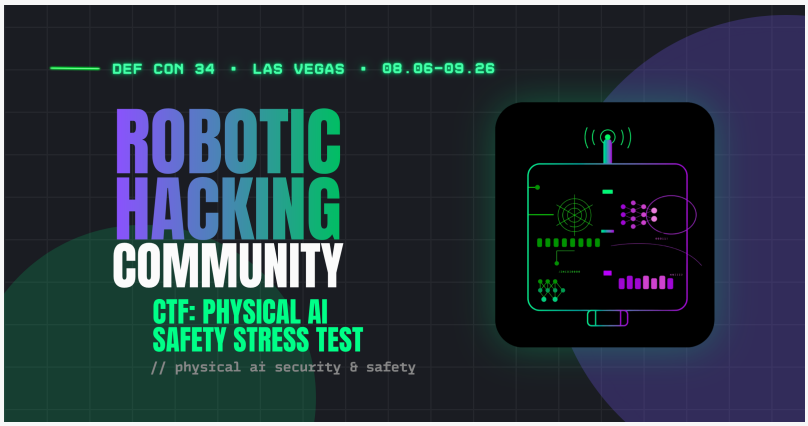
VicOne Brings Physical AI Safety Stress Test to DEF CON 34 to Test How Cyber Risk Can Change Robot Behavior

Digital twin CTF challenge helps robotics makers and operators identify cyber-to-safety risks through Physical AI security scenarios before deployment.



Digital twin CTF challenge helps robotics makers and operators identify cyber-to-safety risks through Physical AI security scenarios before deployment.

DETROIT, MI, UNITED STATES, July 7, 2026 /EINPresswire.com/ -- VicOne, a Physical AI and automotive cybersecurity solutions leader, today announced it will bring the Physical AI Safety Stress Test to the DEF CON 34 Robotic Hacking Community (RHC). The Physical AI Safety Stress Test is a digital-twin capture the flag (CTF) challenge designed to show how cyber risk can affect what AI-driven robots perceive, decide, and do before those systems operate around people, infrastructure, and mission-critical environments.

As robots move from controlled demonstrations into factories, warehouses, public spaces, and field operations, safety validation is becoming more complex. AI-driven robots no longer rely only on mechanical design and deterministic control logic. They increasingly depend on sensors, APIs, firmware, middleware, AI models, cloud-connected services, and embodied reasoning systems.

> “Robot safety cannot stop at mechanical reliability. As Physical AI systems begin to perceive, reason, and act in the real world, cybersecurity becomes part of the safety case.”
>
> *Max Cheng, Chief Executive Officer of VicOne*

That shift changes the safety question for robotics makers and operators. A robot does not need a broken motor to become unsafe. It may become unsafe if it receives the wrong signal, follows the wrong instruction, trusts the compromised model, exposes an unprotected wrong interface, or executes an unintended control path.

VicOne LAB R7 has tracked more than 20 public Physical AI security incidents and vulnerability disclosures over the past 18 months, showing how quickly the robot attack surface is expanding as robots become more autonomous, connected, and AI-driven.

The Physical AI Safety Stress Test brings that challenge into a controlled digital twin environment. Built like a virtual escape room for AI robots, the hands-on CTF translates real-world Physical AI security scenarios into repeatable missions that test and demonstrate how cyberattacks can move from digital compromise to physical behavior risk.

“When large language and vision-language models move into the robot brain, prompt injection is no longer just an AI-output problem. It can become a physical-action problem,” said Max Cheng, Chief Executive Officer of VicOne. “That is why robot safety cannot stop at mechanical reliability. As Physical AI systems begin to perceive, reason, and act in the real world, cybersecurity becomes part of the safety case.”

The challenge includes hands-on missions across six safety-relevant areas:

- prompt injection targeting robot AI reasoning;
- poisoned AI policy models that alter task behavior;
- adversarial visual inputs targeting embodied perception;
- cloud and API security weaknesses;
- security weaknesses in robotics communication protocols, including ROS 2 and DDS; and
- embedded firmware trust-chain weaknesses.

Each mission demonstrates how a cyber condition can influence robot perception, decision-making, task execution, operational boundaries, or trust assumptions. The goal is not only to challenge security researchers, but also to help robotics makers and operators identify where safety validation must expand as robots become more autonomous, connected, and AI-driven.

For manufacturers, cyber-to-safety validation affects product safety cases, pre-deployment testing, customer trust, and post-market monitoring. For operators, it affects site safety, restricted-area control, uptime, incident response, and confidence in autonomous systems operating near workers, equipment, and critical assets.

The Physical AI Safety Stress Test uses a Real2Sim digital twin built in a physics-based robotics simulator. The environment models the Reachy Mini Lite and LeKiwi mobile manipulator, both of which will also be featured in the RHC show-floor environment. Each team receives an isolated environment accessible through the challenge API, enabling participants to explore Physical AI attack paths without exposing live robots to unsafe conditions.

By turning emerging attack scenarios into repeatable digital twin validation, VicOne is helping define Physical AI cybersecurity as a foundation for real-world robot safety. Drawing on its

automotive cybersecurity, vulnerability research, and cyber-physical risk validation expertise, VicOne is extending its security approach to AI-driven machines, helping robotics manufacturers and operators evaluate cyber-to-safety risk across design, pre-deployment validation, and real-world operations.

The Physical AI Safety Stress Test will be featured at the Robotic Hacking Community (RHC) in West Hall 4, Level 1, Room 1309 during DEF CON 34, Aug. 6–9, 2026, at the Las Vegas Convention Center in Las Vegas. The hands-on CTF is limited to a maximum of 80 teams.

About VicOne
VicOne delivers cybersecurity software and services for the automotive industry, with a vision to secure the vehicles of tomorrow. Purpose-built for automotive manufacturers and suppliers, VicOne helps secure connected and software-defined vehicles across the specialized demands of modern mobility. As a Trend Micro subsidiary, VicOne is powered by more than 30 years of cybersecurity expertise and deep automotive threat intelligence. Through LAB R7, its innovation research lab, VicOne is extending its automotive cybersecurity expertise to Physical AI, with research focused on AI robotics cybersecurity and the security of intelligent systems.For more information, visitvicone.com/lab_r7.

Ling Cheng
VicOne
344002265 ext.
email us here
Visit us on social media:
LinkedIn
X
Other