VicOne Turns DEF CON 34 Robot Hacking Research into Free NVIDIA Isaac Sim Extension

The VicOne Radeis Extension for NVIDIA Isaac Sim™ helps robotics teams test how cyberattacks could change robot behavior before deployment.

The VicOne Radeis Extension for NVIDIA Isaac Sim™ helps robotics teams test how cyberattacks could change robot behavior before deployment.

DETROIT, MI, UNITED STATES, August 9, 2026 /EINPresswire.com/ -- VicOne, a Physical AI cybersecurity solutions leader, today released the free VicOne Radeis Extension for NVIDIA Isaac Sim™, enabling robotics developers to test how selected cyber-safety attack scenarios could affect the behavior of their own robot models in simulation.

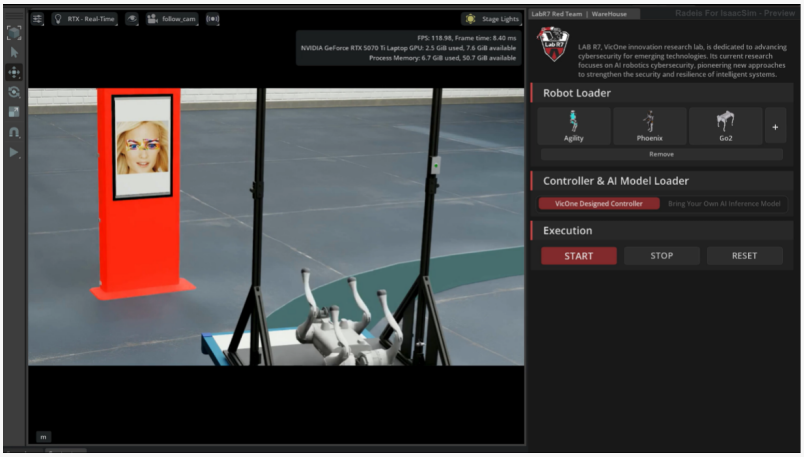
Available now, the extension allows teams to introduce robot cyber-safety attack scenarios into their simulation workflows. Developers can then observe whether the robot deviates from its intended task, operating boundaries, or expected response before exposing physical robots or real operating environments to unnecessary risk.

> Cyber-safety validation should be standard in robotics development. VicOne turns DEF CON research into repeatable simulations to address risks earlier and strengthen Physical AI at scale."
>
> *Max Cheng, Chief Executive Officer of VicOne*

The extension was shaped by findings from VicOne's Physical AI Safety Stress Test CTF at DEF CON 34's Robotic Hacking Community, where security researchers tested how digital compromise could alter robot behavior under controlled conditions. The challenge examined attack paths across AI models, perception, cloud and API services, robotics communications, and embedded systems.

At DEF CON 34, 16 teams recorded 25 successful solves. Nearly every core AI and robotics cyber-safety challenge was solved at least once, with only one advanced embedded systems challenge involving cryptography and firmware vulnerabilities remaining unsolved. The results showed that behavior-changing risks can emerge across multiple layers of the robot stack, reinforcing the need to evaluate cybersecurity at the system level rather than

assess vulnerabilities only in isolation.



The free VicOne Radeis Extension for NVIDIA Isaac Sim gives robotics teams a practical starting point for exploring cyber-to-physical risk

Robot makers invest heavily in functional testing, safety engineering, and simulation, but cyber-induced conditions can still fall outside conventional test plans. VicOne is using findings from the DEF CON challenge, including unsuccessful attempts and newly observed attack assumptions, to refine scenarios involving manipulated visual inputs, hijacked commands, poisoned AI policies, and exploited connected interfaces. By testing these conditions at the system level, teams can determine whether vulnerabilities in individual components could ultimately alter the behavior of the complete robot.

The VicOne Radeis Extension helps bring that question into development earlier. Instead of testing only within a generic demonstration environment, developers can use their own robot models, intended tasks, and operating assumptions within NVIDIA Isaac Sim.

“Robotics companies are moving from proving individual use cases to deploying robots at scale in real-world environments. As that shift accelerates, the industry must validate not only whether robots function as designed, but whether they remain reliable when the digital systems they depend on are compromised,” said Max Cheng, Chief Executive Officer of VicOne. “Cyber-safety validation must become a standard part of robotics development. By turning DEF CON research into repeatable simulation scenarios, we are helping developers address these risks earlier and build more resilient Physical AI at scale.”

From Robot Hacking Research to Repeatable Testing

Every attack attempt can contribute to stronger protection. A successful attempt may reveal a path from digital compromise to changed robot behavior. An unsuccessful attempt can still expose attacker assumptions, unexplored control paths, or safeguards that require further validation.

VicOne translates these findings into structured scenarios that developers can repeat as robot software, sensors, AI models, communications, and control architectures evolve.

Using the free extension, developers can:

- Bring their robot model and intended task into NVIDIA Isaac Sim.

- Apply curated scenarios informed by VicOne's Physical AI security research and DEF CON findings.
- Validate whether the VLM (Vision-Language Model) remains resilient against adversarial visual prompts, malicious inputs, and sensor manipulation attempts that could lead to incorrect interpretations or unsafe decision-making.
- Repeat tests as models, software, sensors, communications, and control paths change.

NVIDIA Isaac Sim provides a physically based environment for designing, simulating, testing, and validating AI-driven robots. The VicOne Radeis Extension adds cyber-safety scenarios and behavioral-impact observation to existing simulation workflows, helping teams examine security-related edge cases before moving into physical testing or deployment.

A Free Starting Point for Broader Cyber-Safety Validation

The free VicOne Radeis Extension for NVIDIA Isaac Sim gives robotics teams a practical starting point for exploring cyber-to-physical risk. It also helps engineering, safety, and security teams discuss risk through visible robot outcomes rather than treating vulnerabilities only as abstract software findings.

For organizations requiring broader assessment, VicOne Radeis is a pre-deployment cyber-safety validation solution that assesses component, system, and AI model risks, then evaluates how vulnerabilities and attack scenarios could affect the behavior of the integrated robot. The complete Radeis solution supports deeper investigation, remediation planning, release decisions, and compliance readiness.

The VicOne Radeis Extension for NVIDIA Isaac Sim is available now as a free download for developers using supported versions of NVIDIA Isaac Sim.

Download the free extension: https://github.com/VicOne-OSS-TW/labr7-radeis-InSimPhysicalAI
Watch the extension demo: https://youtu.be/SJH5PFiqQQ8
Learn more about VicOne Radeis: https://vicone.com/products/radeis/

About VicOne
VicOne is a cybersecurity leader for Physical AI, built on proven automotive cybersecurity expertise. Its software and services protect the digital systems that shape how vehicles and robots see, decide, and act. VicOne helps OEMs, Tier 1 suppliers, robot makers, and operators identify cyber risks early, assess their potential safety impact, and protect systems in operation, helping maintain safe, reliable behavior across real-world deployments. With 180+ zero-days uncovered across automotive and robotics, 100M+ new threat intelligence signals added monthly, and 30 U.S. patent applications pending in AIDV and AI security, VicOne combines specialized Physical AI security research with global threat intelligence. As a Trend Micro subsidiary, VicOne is backed by decades of global cybersecurity expertise. For more information,

visit vicone.com.

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