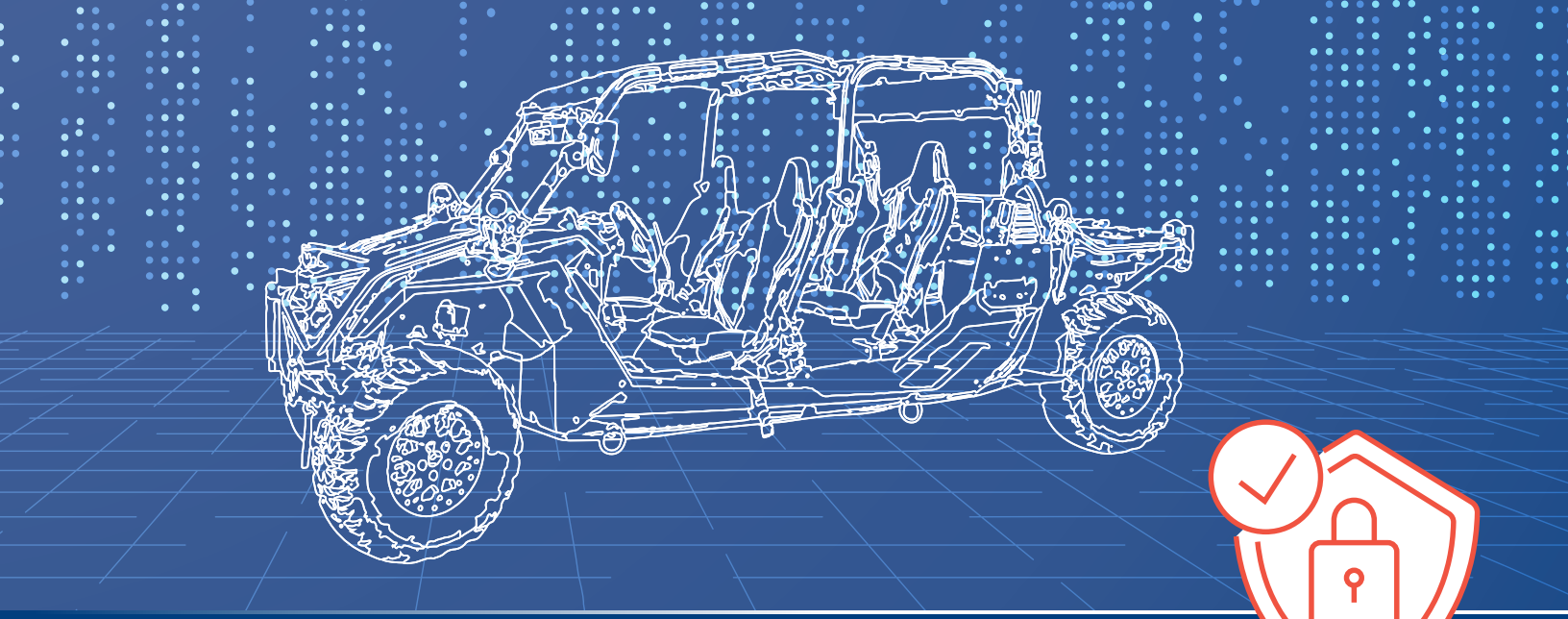

Off-Road Autonomous Ground Vehicles, Secured

Adapt to Changing Threats with Autonomous, Intelligent Cyber Autonomy

Autonomous ground vehicles rely heavily on software, sensors, and communication systems to operate. As with any connected device, hackers can exploit the vulnerabilities present within a vehicle's software or systems, leading to unauthorized access, data theft, remote manipulation – or even a complete takeover of the vehicle's functions.

Developed, trained and tested using Neya's **Virtual Integration and Simulation Environment (VISE)**, Neya's cybersecurity program applies the new Department of Defense **Zero Trust** cybersecurity architecture to enhance the protection, mitigation, recovery and adaptability of autonomous ground vehicles—making Neya's vehicles more secure than ever before.

Key Program Features:

- Built on DoD Zero Trust cybersecurity architecture
- Managed using the Autonomous Intelligent Cyber Agent (AICA)
- Supports the complete autonomous cyber mission plan/lifecycle
- Able to autonomously identify threats and risks to autonomous vehicle missions
- Undetectable by malware and resistant to compromise

Neya Systems believes Zero Trust architecture is the leading solution for protecting autonomous ground vehicles from evolving threats. The development of Zero Trust cybersecurity strategies, complete with autonomous cyber detection, protection, response, and recovery, is critical to the safety and security of autonomous ground vehicles.

Neya's cybersecurity software is designed to be a completely self-contained cyber defender, capable of autonomously hunting, reporting, and defending threats that can exploit or disrupt vehicle missions.

NEYA
A SUBSIDIARY OF ARA

neyarobotics.com | info@neyarobotics.com | 724-799-8078
Neya Headquarters
555 Keystone Drive, Warrendale PA 15086