Innovationswettbewerb „Sicherheit mit und für KI“ Baden-Württemberg (2023)

Projektsteckbrief

FLATARNE: Flexible and Autonomous Cybersecurity and Training Device for the Integration of AI-based Robotics and Networked Entities



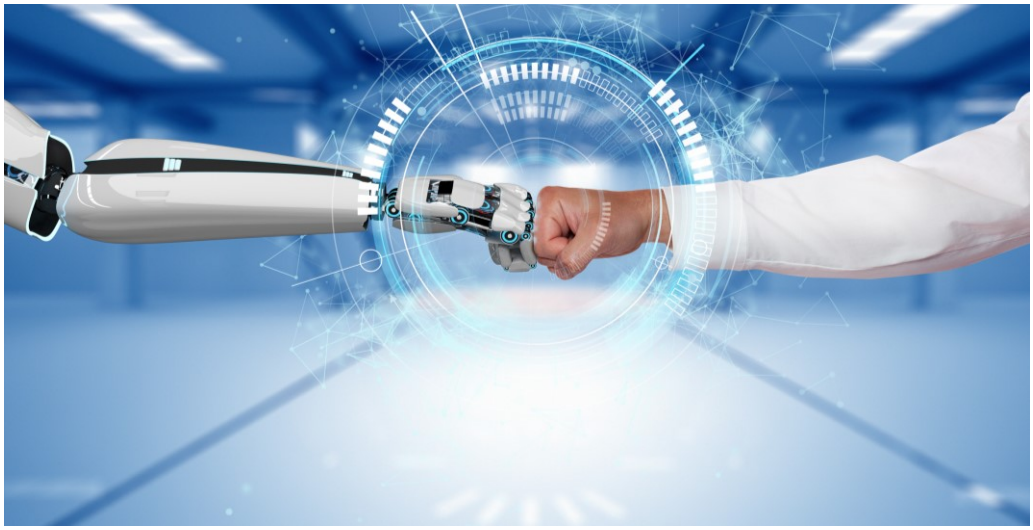
Baden-Württemberg
Ministerium für Wirtschaft,
Arbeit und Tourismus

Worum geht es: Im Rahmen des Projekts FLATARNE verbessert die Neura Robotics GmbH die Security, Safety und Privacy von KI-basierten Robotersystemen.

Dies wird erreich durch:

1. Security für KI: Verbesserte Bereitstellung von Security-Patches für KI-basierte Robotersysteme.
2. Privacy für KI: Ermöglichung einer sichereren und datenschutzkonformen Rücksendung anonymisierter Trainingsdaten.
3. Safety für KI: Erhöhte Robustheit von KI-basierten Systemen durch die Sammlung von variantenreichen Trainingsdaten für eine verbesserte Modellentwicklung.

Projektkonsortium: Neura Robotics GmbH



Innovationswettbewerb „Sicherheit mit und für KI“ Baden-Württemberg

In einer zunehmend digital vernetzten und von Künstlicher Intelligenz (KI) beeinflussten Welt wird die Sicherheit und die Vertrauenswürdigkeit von Produkten und Dienstleistungen immer wichtiger.

Um die Entwicklung sicherer und vertrauenswürdiger KI-Produkte und KI-Dienstleistungen zu forcieren, hat das Wirtschaftsministerium Baden-Württemberg den Innovationswettbewerb „Sicherheit mit und für KI“ ausgeschrieben. Mit dem Wettbewerb werden Unternehmen in Baden-Württemberg in der Entwicklung innovativer Sicherheitslösungen gefördert, bei der KI-Technologien zum Einsatz kommen oder die dazu dienen KI-Anwendungen sicherer zu machen. Sicherheit umfasst hierbei die drei Dimensionen Security (Cybersicherheit), Safety (Betriebssicherheit) und Privacy (Datenschutz).

Der Innovationswettbewerb „Sicherheit mit und für KI“ ist eine Maßnahme im Rahmen des Aktionsprogramms „KI für den Mittelstand“ des Ministeriums.

Offline-Bereitstellung von Security Patches für KI-basierte Robotersysteme

Die zunehmende Komplexität und das wachsende Datenvolumen von KI-basierten Systemen machen diese besonders anfällig für Cyberangriffe. Daher sind regelmäßige Updates von hoher Wichtigkeit. Insbesondere Security-Patches sind dabei von großer Bedeutung, da Assets ohne die entsprechenden Patches für Angreifer ein besonders attraktives Ziel darstellen.

Gerade bei KI-basierten Robotersystemen besteht hier jedoch eine große Herausforderung: Diese werden in der Regel offline betrieben und sind somit nur schwer zugänglich für Sicherheitsupdates. Pragmatische Workarounds wie etwa USB-Updates sind sowohl aufwändig als auch fehleranfällig, während bestehende Lösungen nicht die notwendige Integration moderner Machine Learning Operations (MLOps) – also die Automatisierung und Vereinfachung von Workflows und Bereitstellungen für das maschinelle Lernen - beinhalten.

Dieses Problem aufgreifend, zielt das Projekt FLATARNE darauf ab, ein innovatives Gateway zu entwickeln, das es ermöglicht, Security Patches offline auf KI-basierte Robotersysteme zu deployen. Darüber hinaus soll dieses Gateway ermöglichen, dass anonymisierte Trainingsdaten des Roboters sicher an den Anbieter zurückgeschickt werden. Diese sollen dann in KI-Trainingsprozesse integriert werden, wodurch die Performance und Zuverlässigkeit von KI-Modellen kontinuierlich verbessert wird.

Mehr Security, Privacy und Safety für KI-gestützte Robotersysteme

Mit der Arbeit im Projekt FLATARNE soll die Sicherheit von KI-gestützten Robotersystemen mittels eines innovativen Software-Gateways auf mehrfache Art und Weise verbessert:

1) Security: Durch die Offline-Bereitstellung von Security Patches via eines Gateways reduzieren sich der Aufwand und die Risiken, die mit der Aktualisierung von Robotersystemen bisher verbunden sind. Hierdurch wird zudem ein kontinuierlicher Update-Prozess vereinfacht, um jederzeit ein hohes Security-Level von KI-gestützten Robotersystemen zu wahren.
2) Privacy: Gleichzeitig müssen Unternehmen durch die Implementierung des Software-Gateways keine Kompromisse beim Datenschutz eingehen. Das Gateway bietet zudem die Möglichkeit einer sicheren und datenschutzkonformen Rücksendung anonymisierter Trainingsdaten des Robotersystems.
3) Safety: Die via des Gateways gesammelten anonymisierten Trainingsdaten können dann wiederum in KI-Trainingsprozesse für die Weiterentwicklung KI-basierter Robotersysteme integriert werden. Hierdurch kann die Performance und die Zuverlässigkeit von KI-Modellen kontinuierlich gesteigert werden und somit auch die Sicherheit im Einsatz von und der Arbeit mit KI-basierten Robotern verbessert werden.

Insgesamt soll es Unternehmen mit Hilfe des im Rahmen von FLATARNE entwickelten Software-Gateway ermöglicht werden, sich besser gegen Cybersicherheitsbedrohungen zu wappnen, während sie dabei gleichzeitig ihre Betriebssysteme effizienter gestalten.

Kontakt

Neura Robotics GmbH
Dr. Alexander Blass
Gutenbergstraße 44
72555 Metzingen

Gefördert durch

Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg
Postfach 10 01 41
Schlossplatz 4 (Neues Schloss)
70001 Stuttgart
Tel: 0711 123-2869
Fax: 0711 123-2871
pressestelle@wm.bwl.de
www.wm.baden-wuerttemberg.de

Weitere Informationen

https://neura-robotics.com/

Quellenhinweis

Weitere Informationen zum Innovationswettbewerb finden Sie unter:

www.wirtschaft-digital-bw.de

Baden-Württemberg
Ministerium für Wirtschaft,
Arbeit und Tourismus

Initiative Wirtschaft 4.0 BW