Programm

Sicherheit trotz KI

KI für Sicherheit – Sicherheit von KI

1. Juni 2023, Hochschule Karlsruhe

Thematik

Verfahren der Künstlichen Intelligenz und des Maschinellen Lernens finden immer stärker Anwendung in der Praxis. Autonome Fahrzeuge, das Smart Grid, industrielle Regelungen und Überwachungen, Robotik, Scoring Systeme etc. basieren massiv auf diesen KI Verfahren. Dabei stellt sich die Frage inwieweit diese Verfahren und Anwendungen den Anforderungen nach Zuverlässigkeit, Sicherheit und Nicht-Angreifbarkeit bzw. Nicht-Manipulierbarkeit in der Praxis genügen.

Der Workshop dient insbesondere als Forum für eine intensive Diskussion, um die Verfahren und Systeme sicher zu gestalten. Es werden die Chancen und Herausforderungen der KI Verfahren im realen Einsatz sowohl aus Sicht der industriellen Praxis und der Anwender, als auch aus der Sicht der Wissenschaft und Forschung diskutiert.

Ausgewiesene Experten zu adressierten Workshop-Themen führen als Hauptredner in die Thematik ein. Nachwuchswissenschaftler, junge Ingenieure/Ingenieurinnen bzw. Informatiker/Informatikerinnen stellen ihre aktuellen Arbeiten vor.

Eingeladene Hauptredner

Prof. Dr. Christian Wressnegger

Karlsruhe Institute of Technology, Institute of Information Security and Dependability:
Sicherheit von XAI

Christian Wressnegger ist Assistenzprofessor für Informatik am Karlsruher Institut für Technologie (KIT) und leitet die Forschungsgruppe "Sicherheit intelligenter Systeme" (intellisec).

Seine Forschung dreht sich um die Kombination der Bereiche maschinelles Lernen und Computersicherheit. Er entwickelt Methoden im Bereich der Anwendungs- und Systemsicherheit, z.B. Ansätze zur Angriffserkennung oder zur Entdeckung von Schwachstellen in Software und eingebetteten Geräten. Auch die Robustheit, Sicherheit und Interpretierbarkeit des maschinellen Lernens stehen im Mittelpunkt seiner Forschung.

Prof. Dr. Simon Burton

Research Division Director, Fraunhofer-Institut für Kognitive Systeme IKS:
Addressing uncertainty in the safety assurance of machine learning

Simon Burton erwarb seinen Abschluss in Computerwissenschaften an der Universität von York, wo er zur Verifikation von sicherheitskritischer Software im Jahr 2001 auch promovierte. Er konzentrierte sich auf Forschungs- und Entwicklungsprojekte sowie Beratung, Entwicklung und Produkt-Organisationen im Automotive-Bereich. Zuletzt hatte er

die Rolle des Direktors für Sichere Fahrzeugsysteme bei der Robert Bosch GmbH inne. In dieser Funktion konzentrierte er sich unter anderem auf Strategieentwicklung für sichere automatisierte Fahrsysteme.

Seit September 2020 ist Simon Burton als Research Division Director für den Bereich Safety Mitglied des Direktoriums des Fraunhofer IKS und zeichnet für die Forschungsstrategie mit dem Fokus »Safe Intelligence« verantwortlich.

Seine persönlichen Forschungsbereiche umfassen dabei die Sicherheit komplexer, autonomer Systeme sowie die Sicherheit maschinellen Lernens. Zusätzlich zu seiner Rolle am Fraunhofer IKS ist Simon Burton Honorar-Gastprofessor an der Universität von York, wo er verschiedene Forschungsaktivitäten und interdisziplinäre Kollaborationen unterstützt.

Dr. Peter Deussen

National Standards Officer Germany, Corporate Standards Group, Microsoft Deutschland GmbH:
Standardisierungstrends im Zusammenhang mit Sicherheit

Peter Deussen ist National Standards Officer Germany in der Corporate Standards Group der Microsoft Deutschland GmbH. Er ist ein versierter Standardisierungsexperte mit langjähriger Erfahrung und Mitglied in ISO/IEC JTC 1 und DIN.

- ISO/IEC JTC 1ISO/IEC JTC 1 Standardization Professional: German Delegate in SC 27 - IT Security Techniques, German Delegate in SC 38 - Cloud Computing and Distributed Applications, German Delegate and Head of Delegation in SC 42 - Artificial Intelligence.
- Deutsches Institut für Normung Standards Professional: Co-Chair of NA 043-01-42 AA "Artificial Intelligence", Member of NA 043-01-38 AA "Distributed application platforms and services", Member of NA 043-01-27 AA "IT Security Techniques".

Doz. Dr.rer. nat. habil. Hendrik Schäbe

Principal Assessor RAMS / Teamleiter Funktonale Sicherheit, TÜV Rheinland InterTraffic GmbH:
Anwendung der KI in der Bahntechnik - mögliche Sicherheitsstrategien

Hendrik Schäbe ist Principal Assessor RAMS / Teamleiter Funktonale Sicherheit beim TÜV Rheinland InterTraffic GmbH. Sein Diplom und seine Promotion waren in der theoretischen Physik, seine Habilitation in der mathematischen Statistik.

Seine Tätigkeiten liegen auf dem Gebiet der Zuverlässigkeit und Sicherheit in der Automobilindustrie, Luft- und Raumfahrt, Kerntechnik sowie der Bahntechnik. Er arbeitet auf dem Gebiet der Funktionalen Sicherheit einschließlich dem Einsatz von Künstlicher Intelligenz.

Sicherheit trotz KI

PD Dr. Michael Mock

Fraunhofer-Institut für Intelligente Analyse und Informationssysteme (IAIS):
Ergebnisse aus dem Projekt "KI-Absicherung: Safe AI for Automated Driving“

Technologisch ist autonomes Fahren bereits in greifbarer Nähe – doch ohne nachgewiesene Sicherheit für alle Verkehrsteilnehmenden wird diese Vision nicht umgesetzt werden können.

Michael Mock ist Senior Data Scientist am Fraunhofer IAIS und Privatdozent an der Universität Magdeburg. Im Zentrum seiner Forschungsarbeiten stehen die Entwicklung von verteilten Systemen und Algorithmen zur Verarbeitung großer Datenmengen insbesondere in massiven Datenströmen. Zurzeit leitet und koordiniert er das von der EU geförderte Forschungsprojekt FERARI, in dem eine hochskalierbare verteilte Architektur zur zeitnahen Verarbeitung massiver Datenströme entwickelt wird.

Programm

31.05.2023		**Mittwoch**
17.00		**MV Versammlung FV Ada/FG Ada**
19.00		**Get Together**
01.06.2023		**Donnerstag**
09.00		**Beginn Workshop / Begrüßung**
		Session 1 (Hubert B. Keller)
09.15 - 09.50		**Prof. Dr. Christian Wressnegger**, Karlsruhe Institute of Technology, Institute of Information Security and Dependability: **Sicherheit von XAI**
09.50 - 10.15		**Lukas Schulth** (University of Konstanz**), Christian Berghoff, Matthias Neu** (BSI): **Detecting Backdoor Poisoning Attacks on Deep Neural Networks by Heatmap Clustering**
10.15 - 10.40		**Leo Wilms** (University of Bonn)**, Arndt von Twickel, Matthias Neu, Christian Berghof** (BSI)**:** **Quantifying Attribution-based Explainable Artificial Intelligence for Robustness Evaluations**
10.40 - 11.00		**Pause**

Gesellschaft für Informatik e.V.
Fachgruppe Ada
FB Sicherheit
FB Softwaretechnik

Hochschule Karlsruhe
University of
Applied Sciences

HKA

safeware engineering
safe and secure software

		Session 2 (Peter Dencker)
11.00 - 11.35		**Prof. Dr. Simon Burton**, Research Division Director, Fraunhofer-Institut für Kognitive Systeme IKS: **Addressing uncertainty in the safety assurance of machine learning**
11.35 - 12.00		**Philipp Jass, Hamzih Abukhashab, Carsten Thomas** (HTW Berlin)**, Mirko Conrad, Ines Fey, Harald Schülzke** (samoconsult GmbH)**, Peter Woltersdorf, Michael Weber** (DResearch Fahrzeugtechnik GmbH): **CertML: Initial steps towards using N-version neural networks for improving AI safety**
12.00 - 12.25		**André Dietrich** (HTW Dresden)**, Nico Enghardt** (FU Berlin, secunet)**, Tobias Philipp** (secunet)**, Christopher Schmidt** (secunet, Ruhr-Universität Bochum): **Towards an Efficient and Lazily-Verifiable SAT Proof Checker in SPARK 2014**
12.25 - 13.15		**Mittagspause**
		Session 3 (Philipp Nenninger)
13.15 - 13.50		**Dr. Peter Deussen**, National Standards Officer Germany, Corporate Standards Group, Microsoft Deutschland GmbH: **Standardisierungstrends von KI im Zusammenhang mit Sicherheit**
13.50 - 14.15		**Samuel Kopmann** (KIT Institute of Telematics)**, Hauke Heseding, Martina Zitterbart** (KIT KASTEL Security Research Labs): **Toward Joining DDoS Mitigation and Image Segmentation**
14.15 - 14.40		**Stephan Kleber, Patrick Wachter** (Mercedes-Benz Tech Innovation GmbH): **A Strategy to Evaluate Test Time Evasion Attack Feasibility**
14.40 - 15.15		**Pause**
		Session 4 (Detlef Streitferdt)
15.15 - 15.50		**Doz. Dr.rer. nat. habil. Hendrik Schäbe**, Principal Assessor RAMS / Teamleiter Funktonale Sicherheit, TÜV Rheinland InterTraffic GmbH: **Anwendung der KI in der Bahntechnik - mögliche Sicherheitsstrategien**
15.50 - 16.25		**PD Dr. Michael Mock**, Fraunhofer-Institut für Intelligente Analyse und Informationssysteme (IAIS): **Ergebnisse aus dem Projekt "KI-Absicherung: Safe AI for Automated Driving“**
16.25		**Abschluss**

Sicherheit trotz KI

Termine

18.05.2023 Schluss online Anmeldung und Eingang Gebühr

31.05.2023 17.00 Uhr, Mitgliederversammlung Förderverein Ada/FG Ada

31.05.2023 19.00 Uhr, Get Together

01.06.2023 9.00 Uhr, Beginn Workshop

Anmeldung

Bitte melden Sie sich über die Webseite mit Ihren Daten an unter:
https://ada-deutschland.de/de/ada-in-deutschland/tagungen-workshops/sicherheit_trotz_ki/

Bei Fragen bitte Email an Kontaktpersonen oder an anmeldung@ada-deutschland.de.

Teilnehmergebühren

Die Teilnehmergebühren betragen inkl. Verpflegung und Get Together:

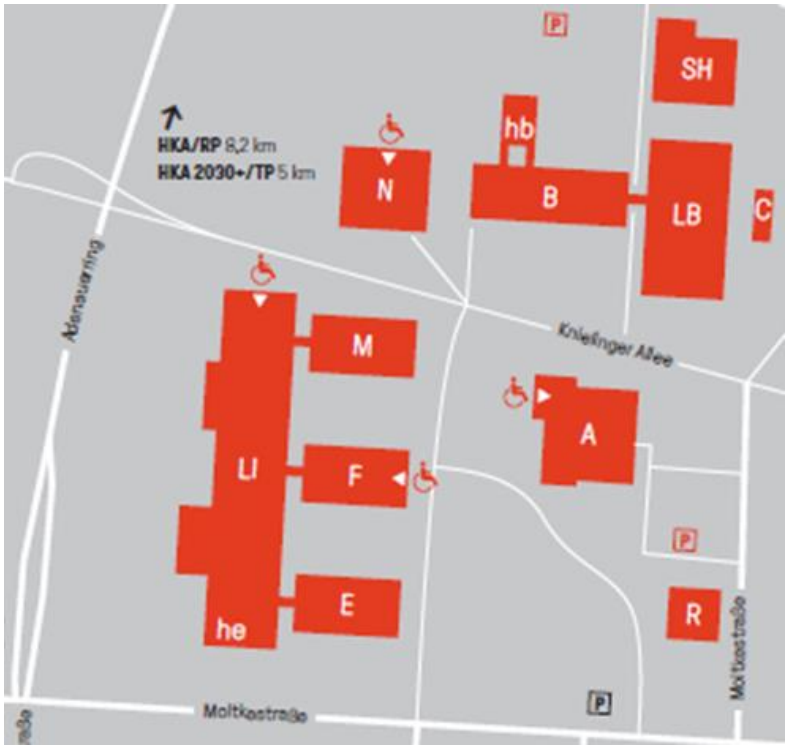
- Vortragende 50 EUR
- Teilnehmer Hochschulen 100 EUR
- Mitglieder FV Ada 100 EUR
- Teilnehmer Industrie 180 EUR
- Studenten 20 EUR
- Aussteller incl. einer Person 400 EUR
- Anmeldung vor Ort zzgl. 20 EUR

Veranstaltungsort

Der Workshop findet an der Hochschule Karlsruhe, Moltkestraße 30, 76133 Karlsruhe, statt (https://www.h-ka.de/standorte).

Zur Hochschule Karlsruhe (HKA-Campus) gelangen Sie vom Hauptbahnhof (Hbf) mit der Linie 2 (Knielingen Nord) oder Linie 3 (Rappenwörth/Daxlanden) bis Haltestelle „Europaplatz/Postgalerie“. Dort dem ausgeschilderten Fußweg in nördliche Richtung (ca. 10 Min.) folgen.

Oder vom Marktplatz mit der Linie 1 (Heide) bis Haltestelle „Kunstakademie/Hochschule“ und zu Fuß in östliche Richtung (Adenauerring, ca. 5 Min.) Der Workshop findet im Gebäude B bzw. hb statt. Parkmöglichkeiten gibt es in der Willy-Andreas-Allee nördlich des Gebäudes.



Gesellschaft für Informatik e.V.
Fachgruppe Ada
FB Sicherheit
FB Softwaretechnik

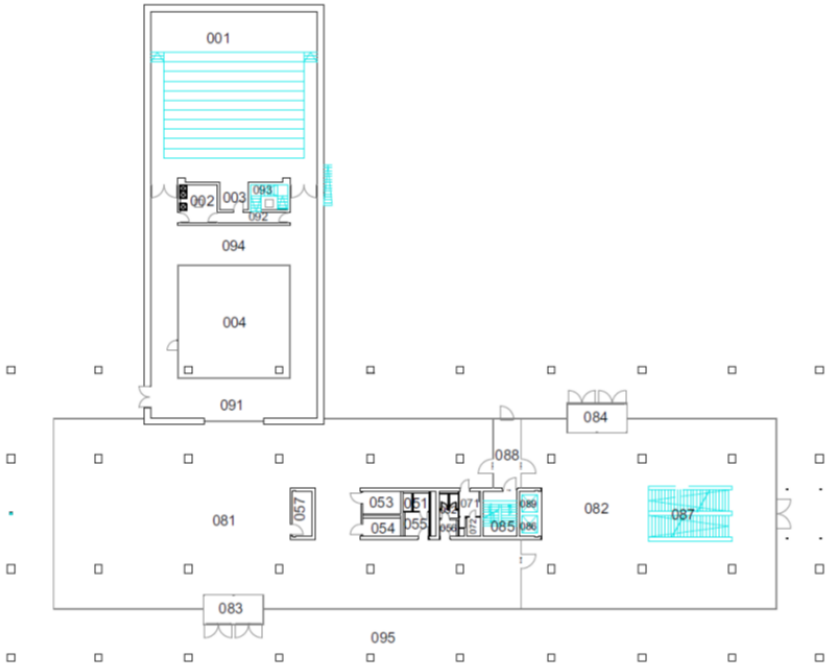
Hochschule Karlsruhe
University of
Applied Sciences

HKA

safeware engineering
safe and secure software

Sicherheit trotz KI

Die Vorträge finden im Hörsaal Bau hb statt (Bild oberer Teil). Pausen und Ausstellungen sind im Bau B (Bild unterer Querteil). Der Zugang zum Gebäude erfolgt von Süden in den Bau B.



Wissenschaftliche Leitung

Hubert B. Keller, ci-tec GmbH Karlsruhe und Erhard Plödereder, Universität Stuttgart

Workshopleitung

Hubert B. Keller, ci-tec GmbH Karlsruhe • Erhard Plödereder, Universität Stuttgart • Philipp Nenninger, Hochschule Karlsruhe

Organisationsleitung

Peter Dencker (Ausstellung), Tobias Philipp (Finanzen)

Programmkomitee

Hubert B. Keller, ci-tec GmbH Karlsruhe • Erhard Plödereder, Universität Stuttgart

Gerhard Beck, Ada Deutschland • Mirko Conrad, samoconsult GmbH • Peter Dencker, Hochschule Karlsruhe • Christof Ebert, Vector Consulting Services GmbH • Bernhard Fechner, FU Hagen, Christopher Gerking, KIT • Reiner Kriesten, Hochschule Karlsruhe • Ulrich Lefarth, GTS Deutschland • Juergen Mottok, OTH Regensburg • Philipp Nenninger, Hochschule Karlsruhe • Tobias Philipp, secunet Security Networks AG • Kai Rannenberg, Goethe-Universität Frankfurt • Detlef Streitferdt, TU Ilmenau

Veranstalter

Gesellschaft für Informatik, Fachbereiche „Sicherheit“ und „Softwaretechnik“, Fachgruppen Ada, ENCRESS, EZQN, FERS, FoMSESS, SIDAR
Förderverein Ada Deutschland e. V.
Hochschule Karlsruhe, Fakultät Elektro- und Informationstechnik

Ansprechpartner

Hubert B. Keller, h.keller@ci-tec.de
Tatjana Nuss, t.nuss@ci-tec.de
Tobias Philipp, tphilipp@gmail.com

Aussteller / Sponsoren

AdaCore (https://www.adacore.com/)

Details zum Workshop

https://ada-deutschland.de/de/ada-in-deutschland/tagungen-workshops/sicherheit_trotz_ki/

www.ada-deutschland.de

Gesellschaft für Informatik e.V.
Fachgruppe Ada
FB Sicherheit
FB Softwaretechnik

Hochschule Karlsruhe
University of
Applied Sciences

HKA

safeware engineering
safe and secure software