

Aufruf zur Einreichung von Beiträgen zum Workshop

Sicherheit trotz KI

KI für Sicherheit – Sicherheit von KI

1. Juni 2023, Hochschule Karlsruhe

„Sicherheit trotz KI“

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 realen Praxis genügen.

Hierzu ist ein Workshop am 1.6.2023 an der HS Karlsruhe geplant. Unter dem Titel „Sicherheit trotz KI“ sollen 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 werden.

Hauptredner sind:

- **PD Dr. Michael Mock, IAIS:** Ergebnisse aus dem Projekt "KI-Absicherung: Safe AI for Automated Driving"
- **Marc Fliehe, TÜV e.V.:** Sicherheit im KI-Kontext aus Sicht der TÜV-Prüfung und Wechselwirkungen zwischen Safety und Security
- **Prof. Dr. Simon Burton, IKS:** Addressing uncertainty in the safety assurance of machine learning
- **Prof. Dr. Christian Wressnegger, KIT KASTEL:** Sicherheit von XAI
- **Dr. Peter Deussen, National Standards Officer, Microsoft Deutschland:** Standardisierungstrends im Zusammenhang mit Sicherheit

Hiermit rufen wir zur Einreichung von Beiträgen aus Industrie, Forschung und Wissenschaft auf. Der Workshop soll insbesondere ein Forum für eine intensive Diskussion bieten. Arbeiten von Nachwuchswissenschaftler und junge Ingenieure bzw. Informatiker sind willkommen.

Beitragseinreichung

Es gelten die [Publikationsrichtlinien der SWT-Trends](#) (Bitte hinterlegtem Link folgen).

Beitragseinreichung bitte über

safe_ki@safeware-engineering.org

Die Länge eines eingereichten Beitrags sollte mindestens 2-3 Seiten umfassen.

Termine

06.02.2023 Einreichung Abstract

27.03.2023 Benachrichtigung über Annahme

08.05.2023 Eingang Druckvorlage

Programmkomitee

Hubert B. Keller, ci-tec GmbH Karlsruhe

Erhard Plödereder, Universität Stuttgart

(gemeinsamer Vorsitz)

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 Rannenber, Goethe-Universität Frankfurt

Detlef Streitferdt, TU Ilmenau

Workshopleitung

Hubert B. Keller, ci-tec GmbH Karlsruhe

Erhard Plödereder, Universität Stuttgart

Philipp Nenninger, Hochschule Karlsruhe

Organisationsleitung

Peter Dencker (Ausstellung),

Tobias Philipp (Finanzen)

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

Hochschule Karlsruhe, Fakultät Elektro- und Informationstechnik

Ansprechpartner

Hubert B. Keller, h.keller@ci-tec.de

Tatjana Nuss, t.nuss@ci-tec.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