



Seminarort

Das Webinar wird mit der MS Teams durchgeführt.
Die Zugangsdaten werden 14 Tage vor der Veranstaltung
per E-Mail an die Teilnehmer versandt.

Gebühr

EUR 790,--
Die CCG ist ein gemeinnütziger Verein und in Deutschland von der Um-
satzsteuer befreit. Für Veranstaltungen an ausländischen Standorten
gelten die dortigen Steuerregelungen.
Mitglieder der CCG erhalten 10% Rabatt. Studentenrabatte sind auf
Nachfrage verfügbar. Die Rabatte sind nicht miteinander kombinierbar.
Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte melden Sie sich möglichst bis 14 Tage vor Seminarbeginn an:
Carl-Cranz-Gesellschaft e.V., Argelsrieder Feld 22, D-82234 Weßling
Tel. +49 (0) 8153 / 88 11 98 -12
E-Mail: anmelden@ccg-ev.de
Internet: www.ccg-ev.de

Die Anmeldungen werden schriftlich bestätigt.

Weitere Informationen zum Inhalt

Dr. Ing. Nadia Burkart
Fraunhofer IOSB, Karlsruhe
E-Mail: nadia.burkart@iosb.fraunhofer.de

Stornierung

Bei Stornierungen, die später als 14 Tage vor Seminarbeginn eingehen,
werden 25% der Gebühr, bei Nichterscheinen die volle Gebühr in Rech-
nung gestellt. Die Vertretung eines angemeldeten Teilnehmers ist selbst-
verständlich möglich.

Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus ande-
ren triftigen Gründen ein Seminar bis 14 Tage vor Beginn abzusagen.
Sie behält sich weiter vor, entgegen der Ankündigung im Programm auch
kurzfristig einen Dozenten und evtl. auch dessen Thema zu ersetzen. Ein
Schadensersatzanspruch bleibt ausgeschlossen.

Teilnehmer

Mitarbeiter aus Industrie, Behörden und Organisationen mit Sicherheitsauf-
gaben, Streitkräften, (z.B. Cyber Innovation Hub) sowie Forschung und Ent-
wicklung, die sich einen Überblick über heutige und zukünftige Möglichkei-
ten von KI für Führung, Aufklärung, Verteidigung und Sicherheit verschaffen
wollen.

Seminarinhalte

Modelle der Künstlichen Intelligenz halten in vielen Lebensbereichen Ein-
zug. Auch im Bereich Verteidigung und Sicherheit ist davon auszugehen,
dass KI in Teilbereichen zu einer Effizienzsteigerung führen wird. Um KI in
sicherheitskritischen Umgebungen einzusetzen, ist ein Vertrauens-, Risiko-
und Sicherheitsmanagement erforderlich. In diesem Zusammenhang wurde
der Begriff AI TRISM (AI-Trust, Risk and Security Management) geprägt.
Das Seminar führt in das Thema ein und beleuchtet die Aspekte Erklärbar-
keit, ModelOps, Detektion & Widerstandsfähigkeit bzgl. gegnerischen An-
griffen und Datenschutz. Ergänzend adressiert es die Chancen und Risiken
Generativer KI, die durch die Verfügbarkeit von z.B. ChatGPT in den Fokus
gerückt ist.

Vortragende

Dr.-Ing. Nadia Burkart Dr.-Ing. Arne Schumann Dr. Andreas Jedlitschka	Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB), Karlsruhe
Dr. Almuth Müller	Fraunhofer Institut für Experimentelles Software-Engineering (IESE), Kaiserslautern

Unterlagen

Jeder Teilnehmer erhält die Vortragsunterlagen.
Die Kosten dafür sind in der Gebühr enthalten.

Seminar FA 1.28

KI - Vertrauens-, Risiko- und Sicherheitsmanagement (AI TRISM)

**03. Juli 2025
Webinar**

Wissenschaftliche Leitung

Dr. Ing. Nadia Burkart
Fraunhofer IOSB, Karlsruhe

Seminarprogramm

Donnerstag, 03.07.2025
09:00 – 16.15 Uhr

Teil 1

09:00 – 09:30
N. Burkart

Begrüßung, Organisation

09:30 – 11:00
A. Jedlitschka

Sicherheit mit und von KI

- Motivation (u.a. Regularien, Herausforderungen)
- KI für Security Engineering (inkl. Cybersecurity)
- Sichere KI (Security für KI)
- Unsicherheitsbewertung der KI
- Ausblick

11:00 – 12:30
N. Burkart

Erklärbare KI

- Einführung zur Erklärbarkeit im Kontext maschineller Lernverfahren
- grundlegende Prinzipien zur Erzeugung von Erklärungen
- mit beispielhafter Demonstration anhand relevanter Anwendungsdomänen wie bei der Erkennung von Deep Fakes

Teil 2

13:15 – 14:45
A. Schumann

Adversial Attacks

- Einführung in Adversarial AI
- Arten von Angriffen - Beispiele und zu resultierendes Fehlverhalten
- Erkennung von Angriffen
- Verteidigungen & Robustifizierung
- Herausforderungen & Trends

14:45 – 16:15
A. Müller

LLMs:

Herausforderungen im Umgang mit Generativer KI

- Was ist generative KI?
- Einordnung in die KI-Landschaft, grundlegende Aspekte, Chancen und Herausforderungen, generativer KI
- Anwendungskontext: Informationen in Textform