KI-FACHKONFERENZ

Workshop: Risikomanagement und -kontrolle

Sebastian Steinbach
TÜV-Verband

Berlin, 22.11.2021

Künstliche Intelligenz & TÜV

Über mich

- Sebastian Steinbach
- Head of AI & Education
- M.Sc. Empirische Sozialforschung, MBA Public Affairs

TÜV-Verband

- Gegründet 1884
- Berlin & Brüssel
- Mitglieder: TÜV-Unternehmen & Industrie

Unser Auftrag

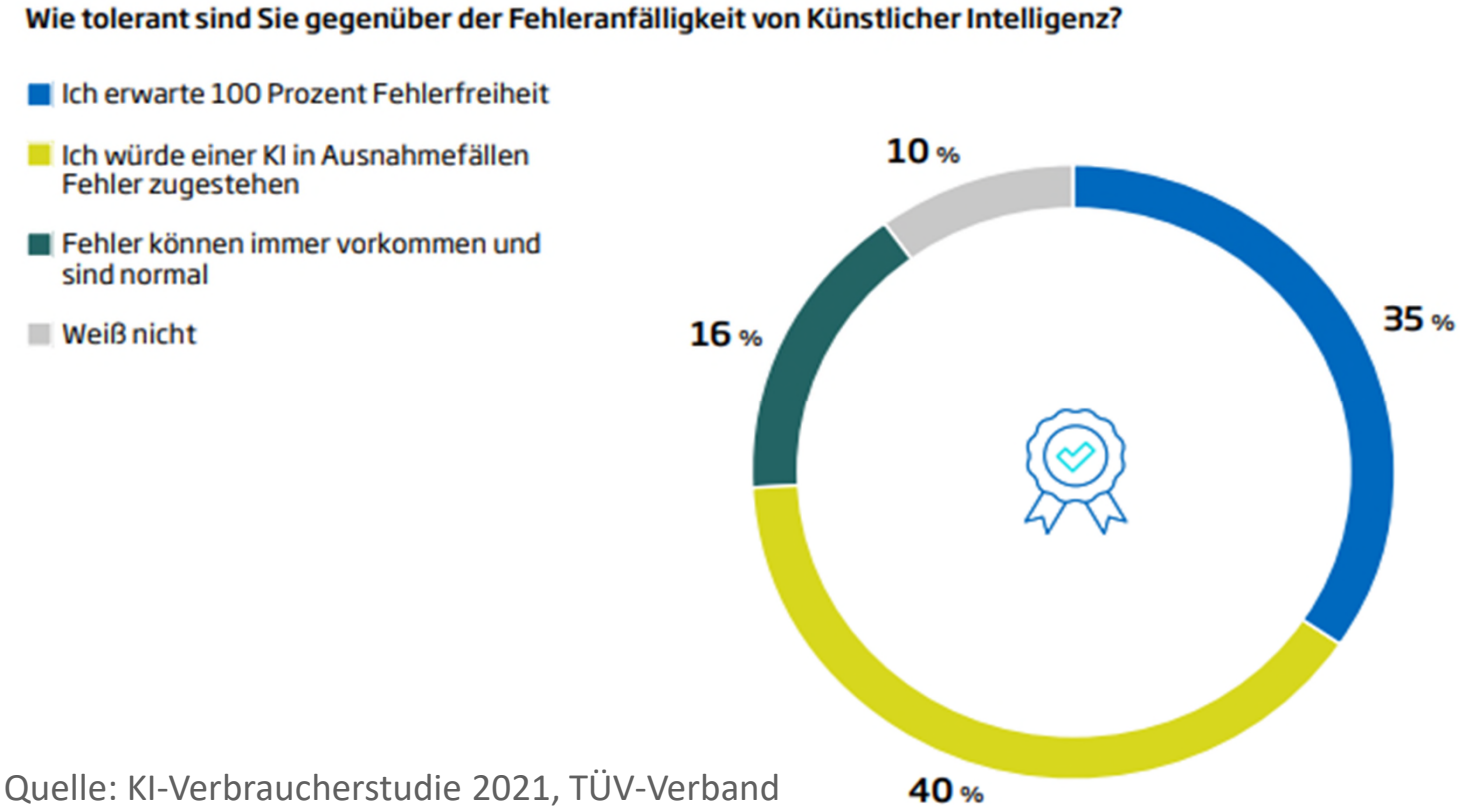
- Sicherheit gewährleisten
- Vertrauen in Digitales schaffen

KI-Aktivitäten

- Prüfung von KI-Anwendungen
- Lösungsentwicklung im TÜV AI Lab
- AI Quality & Testing Hub

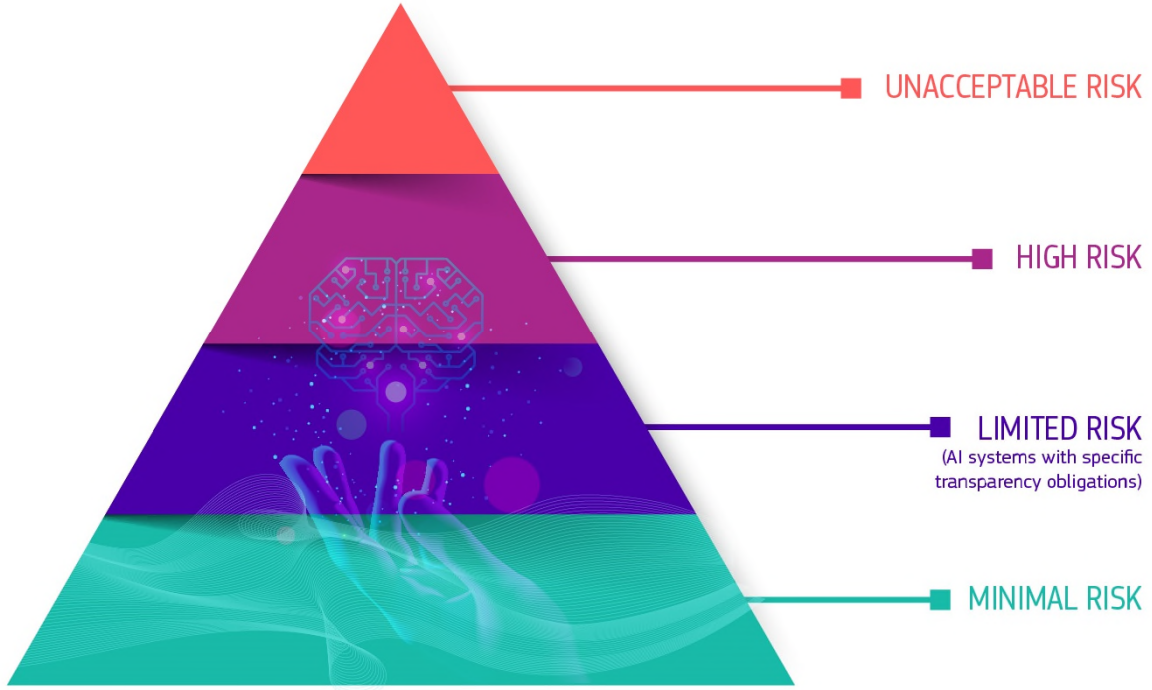
KI-Risikomanagement: Warum relevant?

- Erkennung, Analyse, Bewertung, Kommunikation, Überwachung und Steuerung von Risiken
  - > Unabhängig von Regulierung sinnvoll: Wunsch nach Kennzeichnung und Prüfung



Quelle: KI-Verbraucherstudie 2021, TÜV-Verband

AI Act: Regulierung abhängig vom Risiko



AI Act: Vorschriften für Anbieter von KI-Systemen mit hohem Risiko

Schritt 1	Schritt 2	Schritt 3	Schritt 4
			
Ein KI-System mit hohem Risiko wird entwickelt.	Es muss der **Konformitätsbewertung** unterzogen werden und den KI-Anforderungen genügen. Bei einigen Systemen wird eine notifizierte Stelle einbezogen.	Registrierung eigenständiger KI-Systeme in einer EU-Datenbank	Eine **Konformitätserklärung** ist notwendig. Das KI-System muss die CE-Kennzeichnung tragen. Das System kann in Verkehr gebracht werden.	*Bei wesentlichen Änderungen im Lebenszyklus des KI-Systems greift Schritt 2.*

KI-Risikomanagement im AI Act

- AI Act:
  - > Artikel 9:
    - (1) „Für Hochrisiko-KI-Systeme wird ein **Risikomanagementsystem** eingerichtet, angewandt, dokumentiert und aufrechterhalten.“
    - (2) „Das Risikomanagementsystem versteht sich als ein **kontinuierlicher iterativer Prozess** während des **gesamten Lebenszyklus eines KI-Systems**, der eine regelmäßige systematische Aktualisierung erfordert.“
    - > Ermittlung/Analyse der bekannten und vorhersehbaren Risiken
    - > Abschätzung/Bewertung der Risiken wenn KI-System zweckgemäß verwendet wird
    - > Abschätzung weiterer Risiken nach Inverkehrbringen

KI-Risikomanagement im AI Act

- AI Act:
  - > Artikel 9:

    (Forts.)
    - > Maßnahmen nach „Stand der Technik“ anwenden (harmonisierte Normen/Spezifikationen)
    - > Restrisiko muss „vertretbar“ sein und Nutzer:innen kommuniziert werden
    - > Hochrisiko-KI-Systeme müssen „zu jedem geeigneten Zeitpunkt während des gesamten Entwicklungsprozesses“ getestet werden

KI-Risikomanagement: Wie mit AI Act umgehen?

- Empfehlung des TÜV AI Labs (Whitepaper des TÜV AI LAB zur Risikoklassifizierung von KI-Systemen)
  - > Bestehende Regeln und Normen so weit wie möglich nutzen
  - > Für Risikomanagementsystem z.B. ISO/IEC 23894
- Forderung Bitkom
  - > ISO/IEC 23894 in Katalog ergänzen, zusätzlich zur Nutzung „harmonisierter europäischer Standards“

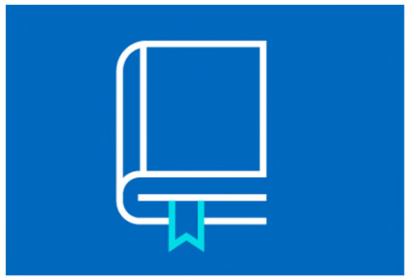
> Für Entwickler von KI-Anwendungen: Risikomanagementsystem implementieren (insb. „Hochrisikosysteme“, aber nicht ausschließlich)

KI-Risikomanagement: Herausforderungen und Lösungen

- Implementierung eines Risikomanagementsystems und kontinuierliche Tests insbesondere für KMUs und Startups anspruchsvoll
- Mögliche Unterstützung: AI Quality & Testing Hub
  - > Initiative von TÜV-Verband und VDE
  - > Anlaufstelle für Qualität und Zertifizierung von KI-Systemen
  - > Aushängeschild für KI „Made in Germany“ schaffen
  - > Aufbau und Vermittlung von Qualitäts-Kompetenz / Schaffung technischer und rechtlicher Experimentierräume
  - > Geplante Standorte: Berlin, Hessen, NRW

AI Quality & Testing Hub

KI ganzheitlich denken: 4 Säulen des AI Quality & Testing Hub



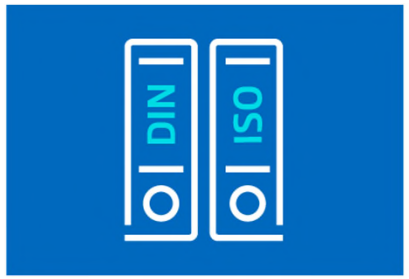
Qualität & Regulatorik

Qualitätskriterien

Ethik & Werte

Experimentierräume, inkl. rechtlicher Experimentierfelder

„Sandboxes“

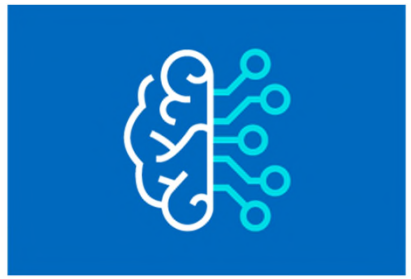


Testen & Prüfen

Prüfschemata

Neue Prüfmethoden und -tools

Testumgebungen & Prüflabore



Kompetenzaufbau

Weiterbildung

Qualifizierung – auch für KMU, Behörden

Expert:innen-Netzwerk

Stipendienprogramme

Transformation

Kommunikation

Changemanagement

Events

Showrooms und Demonstrationen

Weitere Informationen: www.tuev-verband.de/digitalisierung/kuenstliche-intelligenz oder bit.ly/tüv-ki

Vielen Dank für Ihre Aufmerksamkeit!

Sebastian Steinbach

TÜV-Verband e.V.
Head of Artificial Intelligence & Education

Tel.: +49 30 760095-360
E-Mail: sebastian.steinbach@tuev-verband.de