Ergebnisse der Normungsroadmap KI A2

und Bedarfe aus Prüfung/Zertifizierung

Jan Rösler

Veröffentlichung der Normungsroadmap KI (Ausgabe 2)

- Fortschreibung der ersten Ausgabe (2020)
- Veröffentlicht am 9. Dezember 2022
- Fokus: AI Act
- Maßnahme der KI Strategie der Bundesregierung
- Kostenfreier Download: www.din.de/go/normungsroadmapki

Filiz Elmas, Leiterin Strategische Entwicklung Künstliche Intelligenz bei DIN, Christoph Winterhalter, Vorsitzender des Vorstandes von DIN, Robert Habeck, Vizekanzler und Bundesminister für Wirtschaft und Klimaschutz, Prof. Dr. Wolfgang Wahlster, CEA des DFKI und Michael Teigeler, Geschäftsführer DKE (v.l.n.r.) © Stefan Zeitz

Schwerpunktthemen der Normungsroadmap KI

HORIZONTALE THEMEN

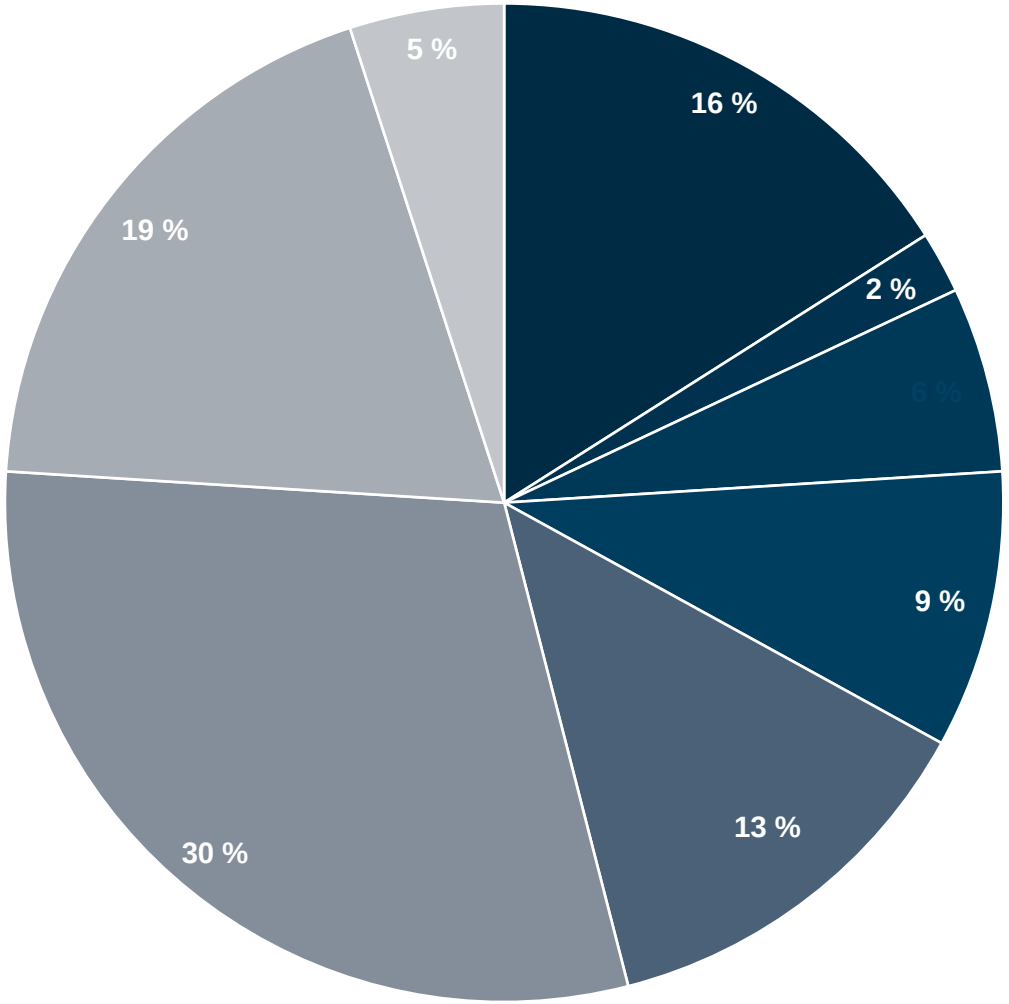
- Grundlagen
- Prüfung und Zertifizierung
- Sicherheit Safety & Security
- Soziotechnische System

SEKTOR-SPEZIFISCHE THEMEN

- Industrielle Automation
- Mobilität
- Medizin
- Finanzdienst-leistungen
- Energie/Umwelt

Zusammensetzung der Arbeitsgruppen

Anzahl: 570 Fachleute



Zahlen zur Normungsroadmap KI

570 Fachleute

9 Arbeits-gruppen/ Schwer-punkte

18 Mitglieder Koordinie-rungsgruppe

318 Autor*innen

116 Handlungs-bedarfe

6 Übergreifende Empfehlungen

448 Seiten

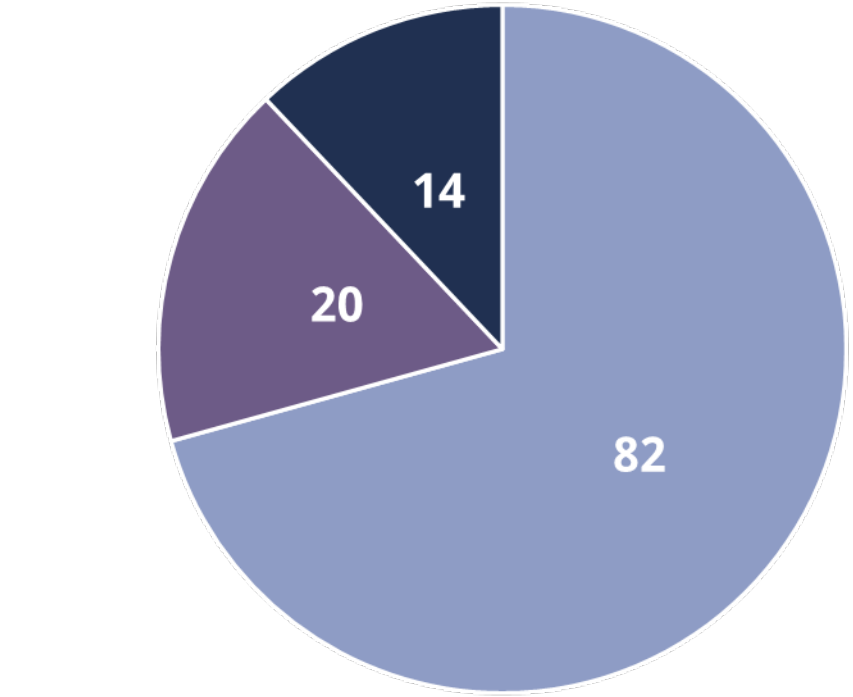
Ergebnisse der NRM KI (Ausgabe 2)

Insgesamt 116 Handlungsbedarfe identifiziert, unterteilt in 3 Kategorien:

KATEGORIE 1:
Bedarf adressiert Normung und Standardisierung

KATEGORIE 2:
Bedarf adressiert Forschung

KATEGORIE 3:
Bedarf adressiert Politik/Gesetzgeber



Stand: Mai 2023

Bedarf 03-… aus Prüfung und Zertifizierung

- 03-01 Spezifikation von formalen Anforderungen an „explainable“ AI („XAI“)-Methoden
- 03-02 Operationalisierung der „Erklärgüte“ von XAI-Methoden
- 03-03 Entwicklung eines Standards mit Guidance-Dokumenten für die Abbildung von Risiken eines Systems in die Funktionalität von KI-Komponenten
- 03-04 Entwicklung von Funktionalitätsklassen für KI-Technologien
- 03-05 Entwicklung von Werkzeugkriterien für die Prüfung von KI-Systemen
- 03-06 Entwicklung von ineinandergreifenden Standards für KI-Systeme und notwendiger Konformitätsbewertungsverfahren
- 03-07 Entwicklung von Qualifikationskriterien für Prüfer und Zertifizierter zu Cybersecurity und Privacy für KI (In Bearbeitung: ISO/IEC 42006)
- 03-08 Vernetzung aller Akteur*innen
- 03-09 Definition von Kontrollpunkten

Bedarf 03-01 (Forschungsbedarf)

Spezifikation von formalen Anforderungen an „explainable“ AI („XAI“)-Methoden

Formulierung konkreter operationalisierbarer/prüfbarer Anforderungen an XAI-Methoden. Welche formalen Aussagen sollen anhand der Ergebnisse einer XAI-Methode möglich sein?

- Die Trainingsdaten betreffend?
- Das Testdatum betreffend?
- Das Modell betreffend?
- Den Zusammenhang zwischen Ein- und Ausgabedaten (Prädiktionen) betreffend?
- Den Zusammenhang zwischen Modell, Ein- und Ausgabedaten betreffend?

Welche praktischen Konsequenzen sollen sich sicher aus diesen Aussagen ableiten lassen? Welcher Mehrwert an „Verlässlichkeit“ soll wirklich geschaffen werden, und wie kann er nachgewiesen werden?

Eine sektorübergreifende und auch im Entwurf AI Act verankerte Forderung ist die nach „Erklärbarkeit“, „Interpretierbarkeit“ etc. […] Dementsprechend ist die Validierung/Verifikation dieser Methoden tendenziell oft eher qualitativ, subjektiv und zirkulär. Formale Kriterien sind notwendig, um zu spezifizieren, welche Aussagen / praktischen Konsequenzen auf Basis des Ergebnisses einer gegebenen XAI-Methode korrekt und zulässig sind. Die Einhaltung dieser Kriterien muss formal oder empirisch verifiziert werden. Nur so können Fehlinterpretationen vermieden werden.

Bedarf 03-03 (politischer Bedarf)

Entwicklung eines Standards mit Guidance-Dokumenten für die Abbildung von Risiken eines Systems in die Funktionalität von KI-Komponenten

KI-Systeme sind:

- möglicherweise hybrid,
- möglicherweise Komponenten eines technischen Systems,
- möglicherweise Teil einer verteilten Architektur auf verschiedenen Plattformen und in verschiedenen Infrastrukturen.

Die Risikoanalyse für das KI-System erfolgt mit Blick auf das gesamte technische System. Daraus müssen Safety-, Security-, …-Anforderungen an die Teile und Komponenten des KI-Systems abgeleitet werden. Dies wird unter Berücksichtigung des Einsatzzweckes und vorhandener Prüfvorschriften und Rahmenbedingungen erfolgen müssen (ISO-26262-Reihe [455], Maschinenrichtlinie etc.). Man bildet also Risiken ganz oder teilweise auf Prüfanforderungen an das ganze KI-System oder auf Teile davon ab. Diese Abbildung bildet den Anker für die Einbettung der Prüfergebnisse in bestehende Prüfverfahren und ihre Bewertung. Contributions CEN/CLC JTC 21 & ISO SC 42 WG 3 „TAISEC“ & „TAISEM“ Einbettung von KI-Prüfungen in die bestehende Prüfinfrastruktur.

Bedarf 03-06 (Forschungsbedarf)

Entwicklung von ineinandergreifenden Standards für KI-Systeme und notwendiger Konformitätsbewertungsverfahren

Damit Konformitätsbewertungsverfahren für KI-Systeme nutzbar sind, ist es wichtig, dass die geltenden Normen der Reihe DIN EN ISO/IEC 17000:2020 [147] (Level 3 Normen) beachtet werden. Für spezifische Anforderungen an bestimmte Evaluierungsaufgaben innerhalb der definierten Konformitätsbewertungs-aktivität auf Level 3 sind nach sektoralen oder technischen Anforderungen auf Level 4 differenzierte Normen für KI-Systeme zu entwickeln. Daneben besteht Normungsbedarf im Bereich der Grundlagen, insbesondere bezüglich Kalibrierung und Eignungsprüfungsanbieter (Ringversuche). Auch hier sind auf Level 4 Normen zu entwickeln, welche die technischen Besonderheiten und Risiken der KI-Systeme berücksichtigen. Besonders wichtig ist es, die Normungsvorhaben an den Gegenstand der Konformitätsbewertung (KI-System / Organisation i. S. v. Herstellenden oder Inverkehrbringer) (Level 5) von den Normungsvorhaben, die sich auf Konformitätsbewertung beziehen (Level 4 und 3), zu trennen. Nur so ist es möglich, die einzelnen Rollen und Verantwortlichkeiten im Hinblick auf Herstellende, Inverkehrbringer, Nutzer*innen und Konformitätsbewertungsstellen richtig zuzuschreiben. Nur durch klare Vorgaben an Qualifikationen und klare Anforderungen können Prüfverfahren, die sich durch Ringversuche in ihrer Bewertungsqualität messen müssen, entwickelt werden. Zuerst sind die Anforderungen an den Gegenstand zu kennen, bevor festgelegt werden kann, wie diese überprüft werden können.

→ Contributions CEN/CENELEC JTC 21 WG 2 „Conformity Assessment“

Bedarf 03-08 (generalistisch, politscher Bedarf)

Vernetzung aller Akteur*innen

[…] Normungsvorhaben, die Methoden, Verfahren oder Prozesse vorsehen, die z. B. eine Konformitätsbewertung (z. B. als Prüfung) von Anforderungen vorsehen, müssen mit einem breiten Expert*innenfeld aus dem Bereich der Konformitätsbewertungsstellen und Akkreditierungsstellen besetzt werden. Dabei gilt es, auch innerhalb der Normungsarbeit ein gemeinsames Verständnis des notwendigen Zusammenwirkens der verschiedenen Ebenen (Metrologie, Konformitätsbewertung, Akkreditierung, Herstellung, Inverkehrbringung und Anwendung) zu etablieren, um geeignete und ineinandergreifende Normen für den Gegenstand (z. B. KI-System) sowie für die Konformitätsbewertung (z. B. im Rahmen einer Prüfung) zu entwickeln.

In der Normung gibt es kein übergreifendes Verständnis, wie in der Praxis Normanforderungen an den Gegenstand und Normanforderungen an Prüfprozesse ineinandergreifen. Dies sollte zukünftig besser versucht werden, am Anfang eines Normungsvorhabens hervorzustellen, um besser abgestimmte Normungsvorhaben zu haben. Je besser das gegenseitige Verständnis ist, desto leichter wird die praktische Umsetzung. In Kapitel 4.3 wird deutlich, dass das Verständnis von „Prüfung und Zertifizierung“ je nach Anwendungsfeld und Berufskontext unterschiedlich aufgefasst wird. Dabei existiert ein gesetzlich geregeltes System in der EU, welches die Qualität von Produkten, Prozessen, Services und Dienstleistungen absichert: die Qualitätsinfrastruktur.

Bedarf 03-09 (Normungsbedarf)

Definition von Kontrollpunkten

Anhand des KI-Lebenszyklus sind einzelne Prüfpunkte, an denen eine Konformitätsbewertung (Level 4 und 3) stattfinden muss, mit einem Minimalset an Evaluationstätigkeiten zu definieren, um die Konformität mit den rechtlichen Anforderungen, die in Gesetzesvorhaben wie dem europäischen AI Act oder dem kanadischen Artificial Intelligence and Data Act [170] definiert werden, bewerten und bestätigen zu können. Dabei ist eine klare Rollendefinition auf der Ebene der KI-Entwickler*innen/Herstellenden/Inverkehrbringer als auch auf der Ebene der Konformitätsbewertungsstellen und Akkreditierungsstellen notwendig.

Nach einer klareren Rollenstruktur gilt es dann, herauszuarbeiten, welche Rolle (aus Level 5 oder Level 3) an welchem Punkt im KI-Lebenszyklus in die Entwicklung, Evaluierung, den Einsatz und die Stilllegung des KI-Systems integriert werden muss, um die gesetzlichen Anforderungen zu erfüllen.

Bessere Verzahnung von Unternehmen, die KI-Systeme entwickeln und/oder in Verkehr bringen, mit den Konformitätsbewertungsstellen (erster, zweiter und dritter Seite).

Bedarfs-Voting per WebEx-Umfrage

Welche/r der vorgestellten Bedarfe interessiert Sie? Bitten stimmen Sie jetzt ab, zu welchen der Bedarfen wir Sie auf dem Laufenden halten sollen.

- 03-01 Spezifikation von formalen Anforderungen an „explainable“ AI („XAI“)-Methoden (Forschungsbedarf)
- 03-03 Entwicklung eines Standards mit Guidance-Dokumenten für die Abbildung von Risiken eines Systems in die Funktionalität von KI-Komponenten (politischer Bedarf)
- 03-06 Entwicklung von ineinandergreifenden Standards für KI-Systeme und notwendiger Konformitätsbewertungsverfahren (Forschungsbedarf)
- 03-08 Vernetzung aller Akteur*innen (generalistisch, politscher Bedarf)
- 03-09 Definition von Kontrollpunkten (Normungsbedarf)

Jan Rösler

Senior Projektmanager
DIN – Abt. Strategische Themenentwicklung KI

Jan.Roesler@din.de

DIN
Deutsches Institut für Normung e. V.
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin

www.din.de