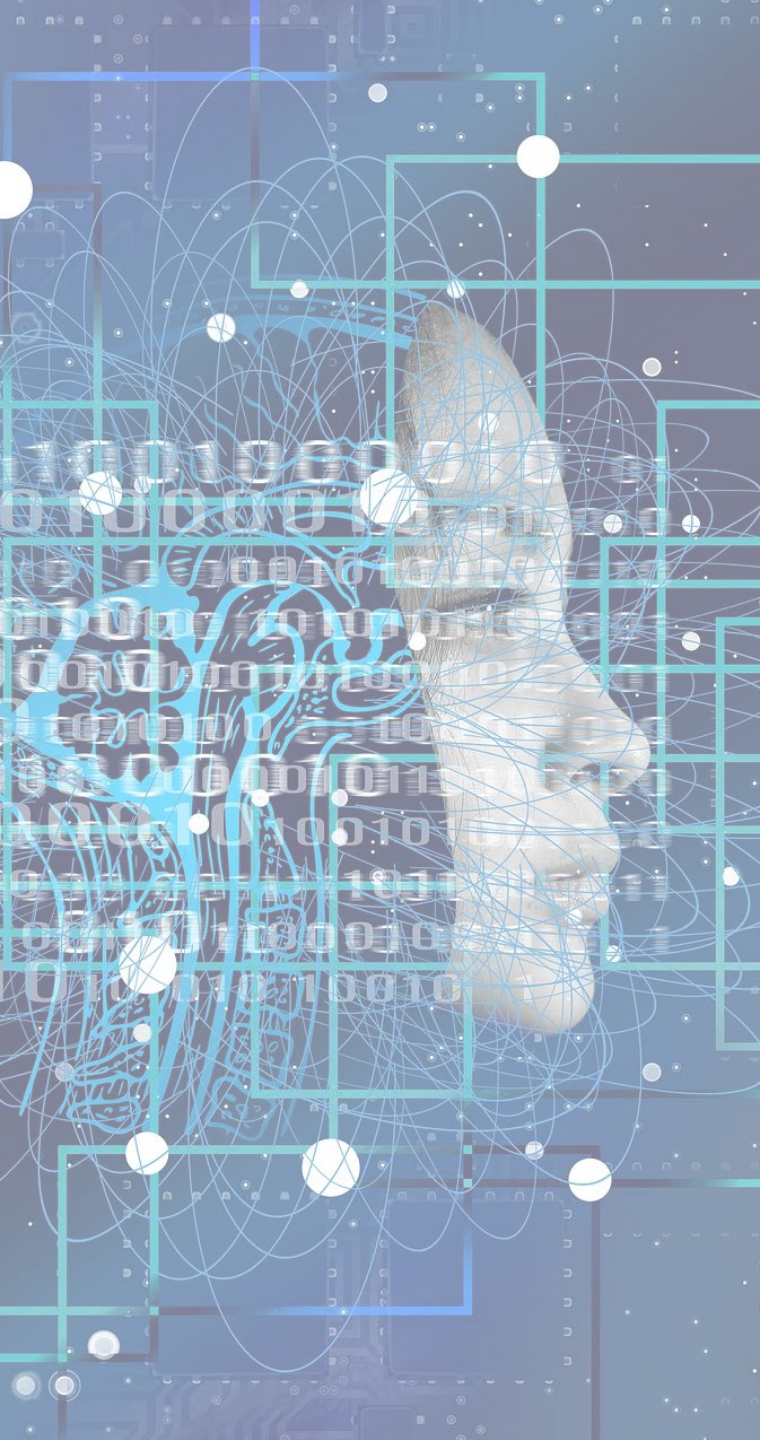
Vortrag für die Gesellschaft für Informatik

Die Weichen stellen für Künstliche Intelligenz: Ohne Normen und Standards geht es nicht

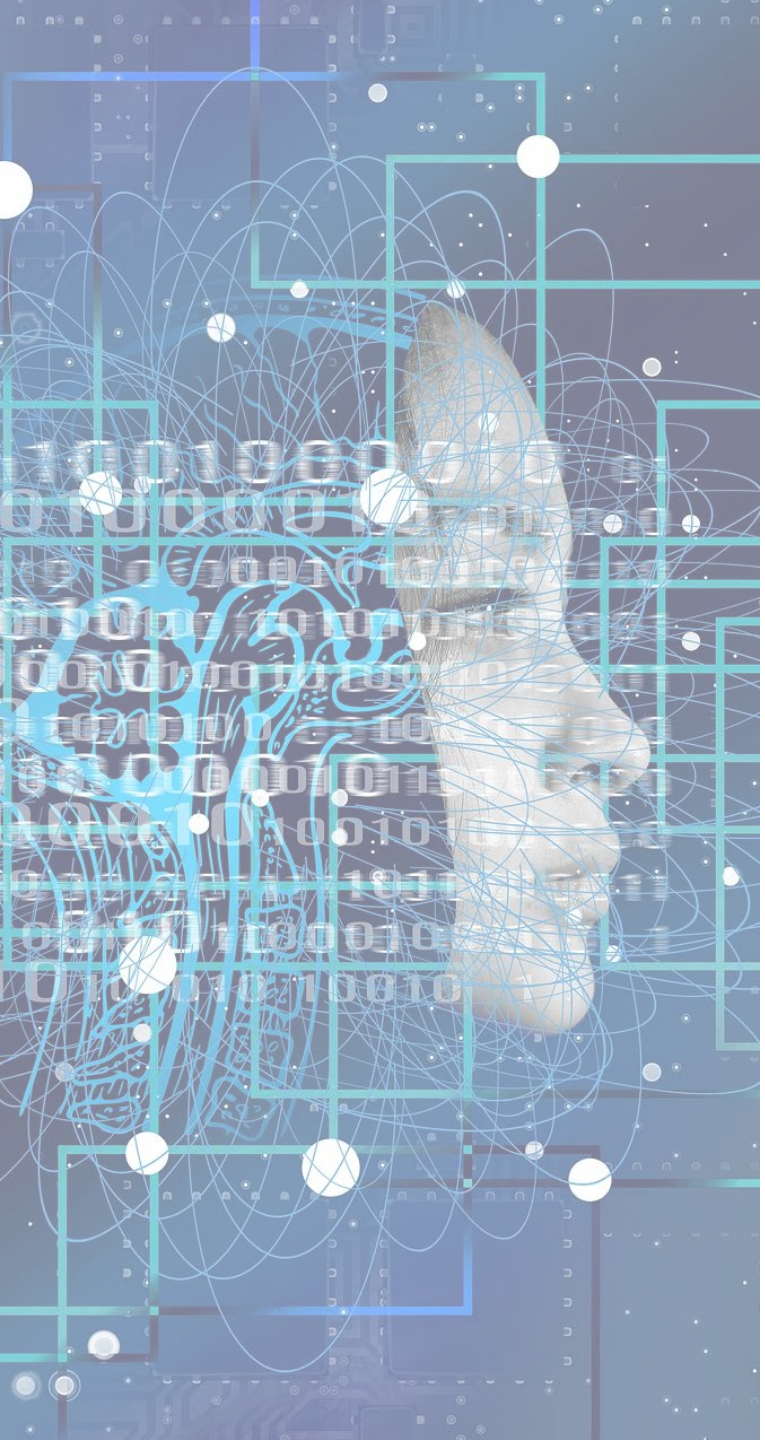
Filiz Elmas

27. Mai 2021



Agenda

1. Einführung
2. Normungsroadmap KI
3. Aktivitäten
4. Ausblick



Agenda

1. Einführung
2. Normungsroadmap KI
3. Aktivitäten
4. Ausblick

Über DIN

- **Neutrale Plattform** für Normung und Standardisierung in Deutschland und weltweit
- Privatwirtschaftlich organisiert
- Gegründet **1917**
- **P**ublic-**P**rivate **P**artnership seit **1975**
- Mitarbeiter **> 500**
- DIN-Mitglieder **> 3.200**
- Experten **≈ 36.000**
- DIN-Normen **> 34.000**
- DIN-Normenausschüsse **69**

KI braucht Normen und Standards

Wesentliche Herausforderungen / Hemmnisfaktoren für den Einsatz von KI

- Datenverfügbarkeit
- Kompatibilität
- Interoperabilität
- Vertrauen
- Transparenz
- Robustheit
- Sicherheit

- Standardisierte **Datenformate** schaffen Kompatibilität
- Definition von **Datenreferenzmodellen** sorgen für Interoperabilität
- Normen und Standards als Basis für **KI-Zertifizierung** sorgen für Verlässlichkeit, Robustheit, funktionale Sicherheit
- Normen und Standards unterstützen **technische Souveränität** und **Transparenz**

→ **Vertrauen in und Akzeptanz von KI-Systemen in Gesellschaft und Wirtschaft wird gestärkt**

KI-Strategie der Bundesregierung

November 2018: Veröffentlichung der KI-Strategie

- Übergeordnete Ziele
  - Deutschland zu einem führenden KI-Standort machen und Wettbewerbsfähigkeit sichern
  - Verantwortungsvolle und gemeinwohlorientierte Entwicklung und Nutzung von KI
  - KI ethisch, rechtlich, kulturell und institutionell in die Gesellschaft einbetten
- 12 Handlungsfelder, davon adressiert eines „Standards setzen“, eine Maßnahme: Erarbeitung Normungsroadmap KI

Dezember 2020: Fortschreibung der KI-Strategie

- Erhöhung der KI-Mittel bis 2025 von drei auf fünf Milliarden €
- Weiterentwicklung der Strategie mit Fokus auf Pandemiebekämpfung, Nachhaltigkeit, Umwelt- und Klimaschutz sowie internationale Vernetzung

Die Bundesregierung

KI Nationale Strategie für Künstliche Intelligenz
AI Made in Germany

Einführung

Normungsroadmap KI

„Gerade für lernende Systeme sind **maschinenlesbare und von Maschinen interpretierbare Normen** von erheblicher Bedeutung."

„Die **Überprüfung bestehender Standards und Normen** auf **„KI-Tauglichkeit"** ist dabei zu berücksichtigen."

Standards setzen

„Die BReg prüft, die **Teilnahme von Expertinnen und Experten**, insbesondere von **KMU** und **Start-ups**, an **internationalen Standardisierungsverfahren** zu unterstützen."

„Die BReg unterstützt die **Standardisierung von Begriffen und Klassifizierungen von KI** (z. B. Dimensionen der Selbständigkeit, Selbständigkeit des Lernens, mit KI verbundene Risiken)."

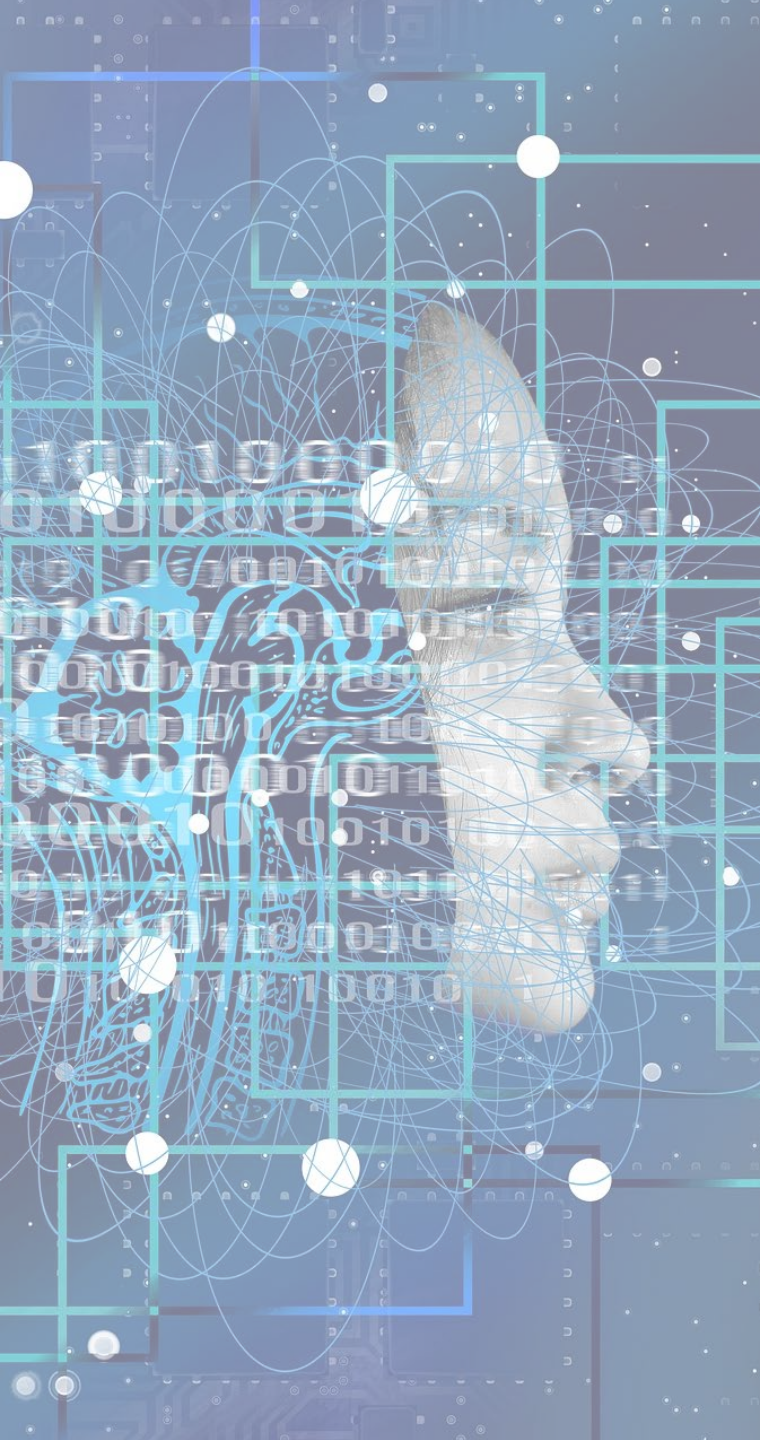
„Die BReg wird in einem gemeinsamen Projekt mit dem DIN eine **Roadmap zu Normen und Standards** im Bereich KI entwickeln."

Normungsroadmap KI setzt eine wesentliche Maßnahme der KI-Strategie

Ziele:

- Umfeld der KI-Standardisierung beschreiben
- Normungs- und Standardisierungsbedarfe aufzeigen
- Handlungsempfehlungen aussprechen

Download: www.din.de/go/normungsroadmapki



Agenda

1. Einführung
2. Normungsroadmap KI
3. Aktivitäten
4. Ausblick

Normungsroadmap Künstliche Intelligenz

Prozess der Normungsroadmap KI

2020

Basis schaffen

Erarbeitung der Normungsroadmap KI

- Einrichtung Steuerungsgruppe
- Kommunikationsmaßnahmen
- Festlegung Projektstruktur
- Aufbau DIN.ONE & KI-Themenseite
- Bildung von Arbeitsgruppen
- Erarbeitung der NRM KI
- Veröffentlichung der NRM KI auf Digitalgipfel

2021

Verstetigen

Umsetzung der Ergebnisse der Normungsroadmap KI

- Analyse Handlungsempfehlung
- Fachworkshops
- Eingliederung Themen in NAs
- Initiierung von N+S-Projekten
- Adressierung Empfehlungen an Forschung und Politik
- Gründung Koordinierungsgruppe
- Initiierung von Leuchtturmprojekten
- Initiierung der NRM KI V2

2022

Weiterentwickeln

Fortschreibung der Normungsroadmap KI

- Verstetigung und Nachhalten Ergebnisse der NRM (V1)
- Systematisches Ausbauen der Aktivitäten (CEN, ISO, national)
- Erarbeitung & Veröffentlichung der NRM KI (V2)
- Initiierung weiterer Leuchtturm-projekte
- Weitere Forschungs- und Normungsprojekte zu KI

Normungsroadmap Künstliche Intelligenz: Basis schaffen

Prozess der Normungsroadmap KI

2020

Basis schaffen

Erarbeitung der Normungsroadmap KI

- Einrichtung Steuerungsgruppe
- Kommunikationsmaßnahmen
- Festlegung Projektstruktur
- Aufbau DIN.ONE & KI-Themenseite
- Bildung von Arbeitsgruppen
- Erarbeitung der NRM KI
- Veröffentlichung der NRM KI auf Digitalgipfel

2021

Verstetigen

Umsetzung der Ergebnisse der Normungsroadmap KI

- Analyse Handlungsempfehlung
- Fachworkshops
- Eingliederung Themen in NAs
- Initiierung von N+S-Projekten
- Adressierung Empfehlungen an Forschung und Politik
- Gründung Koordinierungsgruppe
- Initiierung von Leuchtturmprojekten
- Initiierung der NRM KI V2

2022

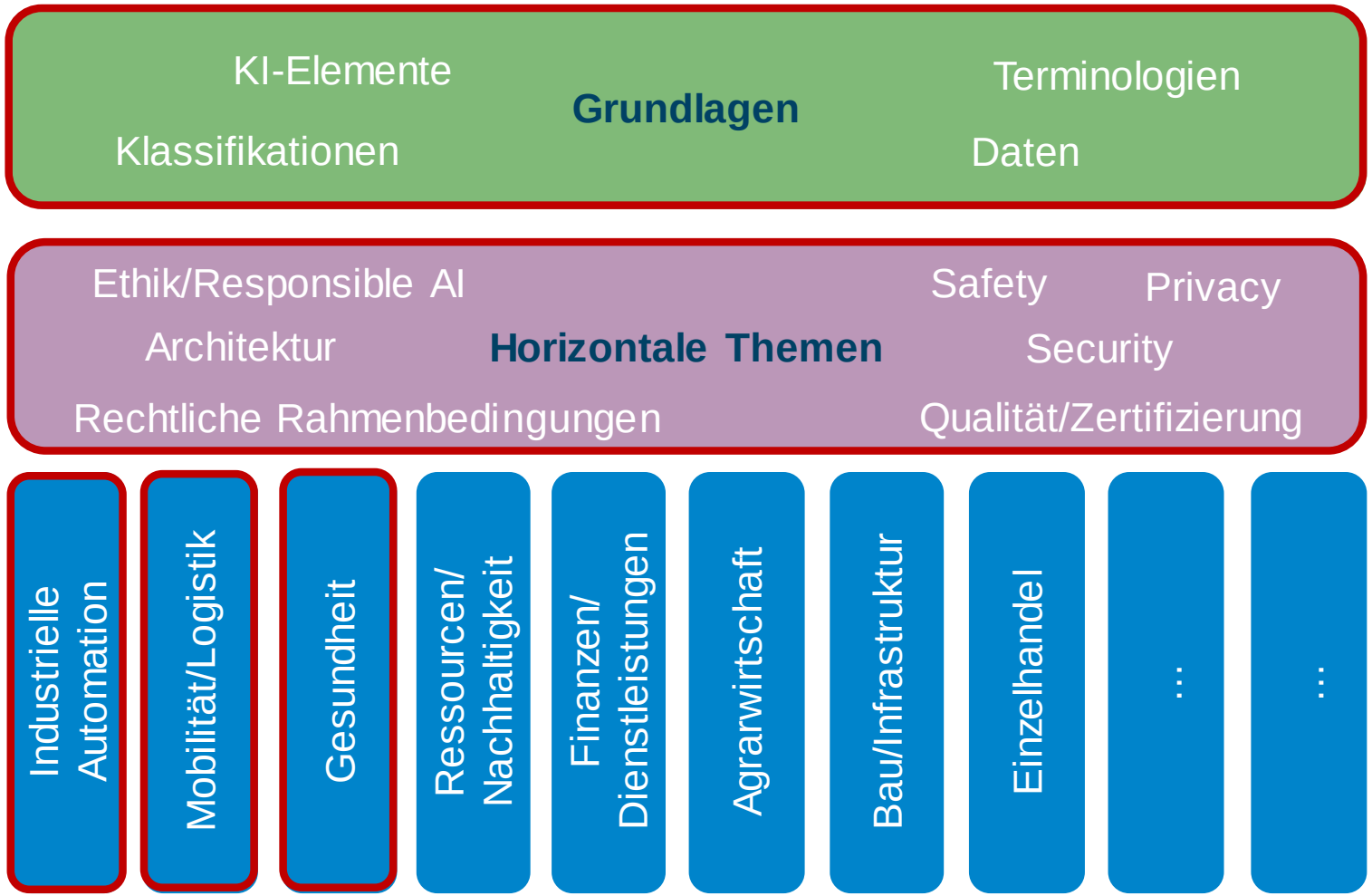
Weiterentwickeln

Fortschreibung der Normungsroadmap KI

- Verstetigung und Nachhalten Ergebnisse der NRM (V1)
- Systematisches Ausbauen der Aktivitäten (CEN, ISO, national)
- Erarbeitung & Veröffentlichung der NRM KI (V2)
- Initiierung weiterer Leuchtturm-projekte
- Weitere Forschungs- und Normungsprojekte zu KI

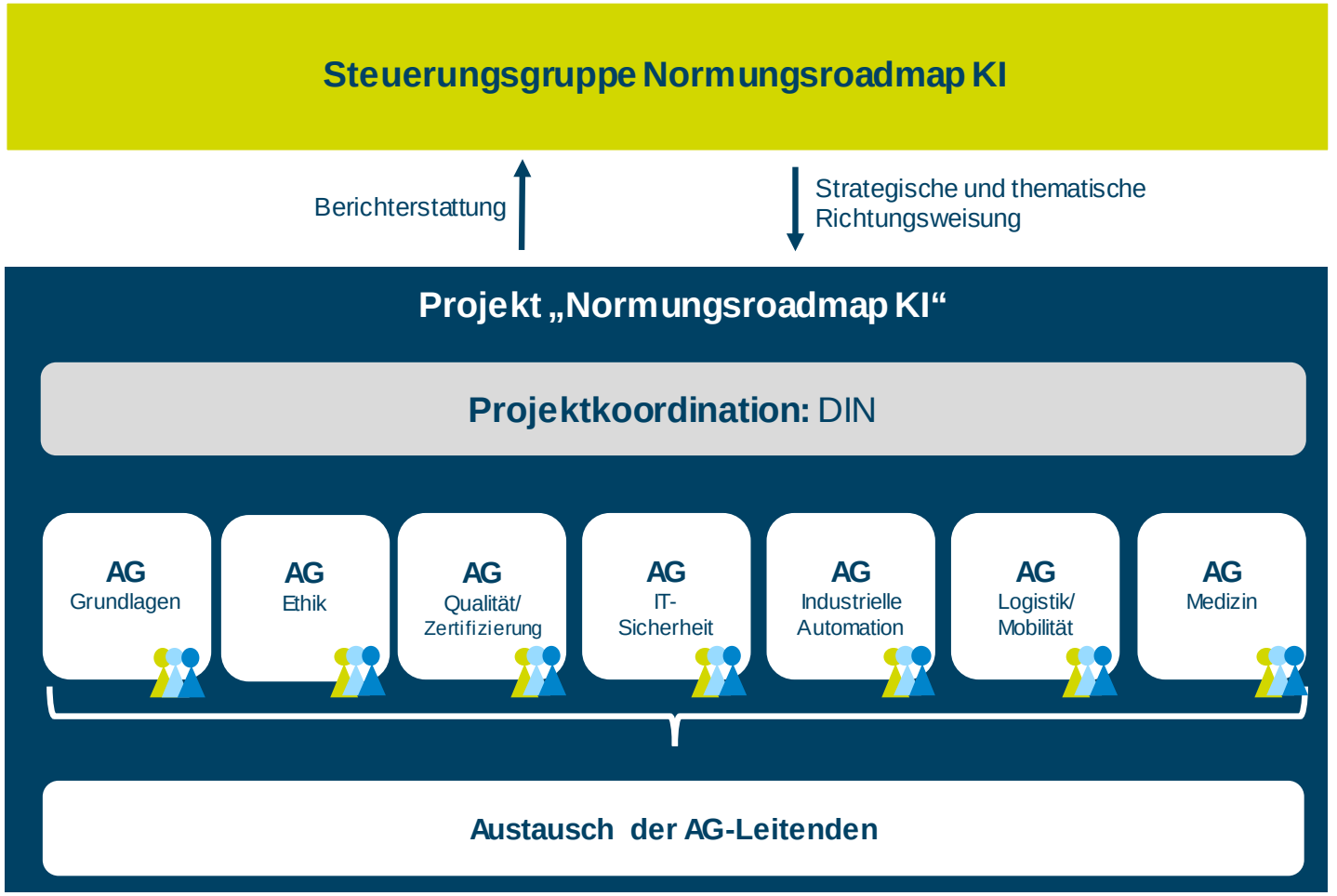
Normungsroadmap Künstliche Intelligenz: Basis schaffen

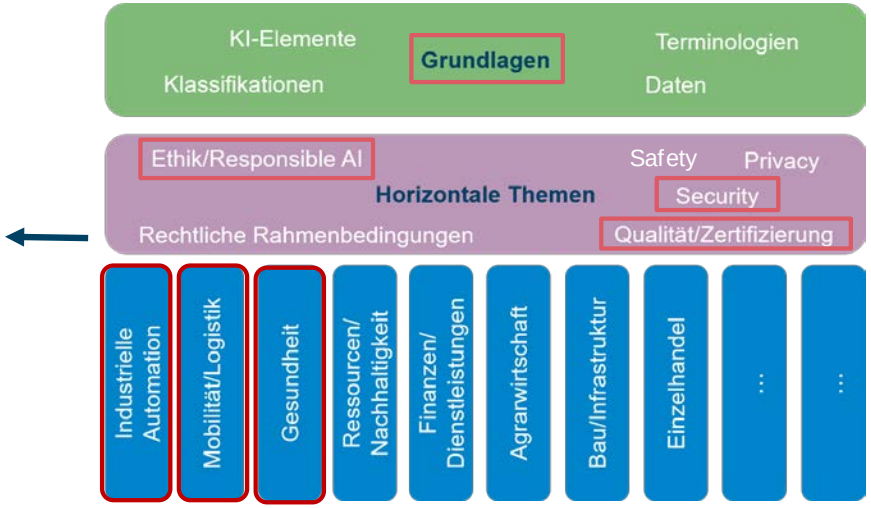
Themenfelder KI



Normungsroadmap Künstliche Intelligenz: Basis schaffen

Struktur des Projekts NRM KI





Normungsroadmap Künstliche Intelligenz: Basis schaffen

Mitglieder Steuerungsgruppe

Dr. Tarek R. Besold
neurocat GmbH

Jörg Bienert
KI-Bundesverband

Dr. Julia Borggräfe
BMAS

Dr. Joachim Bühler
Verband der TÜV e. V.

Susanne Dehmel
Bitkom e. V.

Dr. Dirk Hecker
Fraunhofer IAIS

Thorsten Herrmann
Microsoft Deutschland

Stefan Heumann
Stiftung Neue Verant-
w ortung

Dr. Wolfgang Hildesheim
IBM Deutschland

Prof. Jana Koehler
DFKI

Prof. Ina Schieferdecker
BMBF

Stefan Schnorr
BMWi

Prof. Klaus Mainzer
TU München

Dr. Christoph Peylo
Robert Bosch GmbH

Alexander Rabe
eco Verband

Andreas Steier
Mitglied des Deutschen
Bundestages

Dr. Volker Treier
DIHK

Prof. Wolfgang Wahlster
Plattform Lernende
Systeme

Prof. Dieter Wegener
Siemens AG

Christoph Winterhalter
DIN

Normungsroadmap Künstliche Intelligenz: Basis schaffen

Meilensteine der Normungsroadmap KI

August 2019

Konstituierung Steuerungsgruppe NRM KI

Oktober 2019

Auftaktveranstaltung im BMWi mit > 300 TN

Januar 2020

Kick-Off Arbeitsgruppen

Erarbeitung der Normungsroadmap KI

Erarbeitungszeit: 7 Monate
Anzahl der Sitzungen > 60

Juli 2020

Fertigstellung Manuskript

Lektorat

November 2020

Veröffentlichung

Normungsroadmap Künstliche Intelligenz: Basis schaffen

Zahlen zur Normungsroadmap KI

300
Fachleute

7
Arbeits-gruppen und Schwer-punkte

20
Mitglieder in der Steuerungs-gruppe

180
AutorInnen

>70
Standardi-sierungs-bedarfe

236
Seiten

Normungsroadmap Künstliche Intelligenz

Schwerpunktthemen

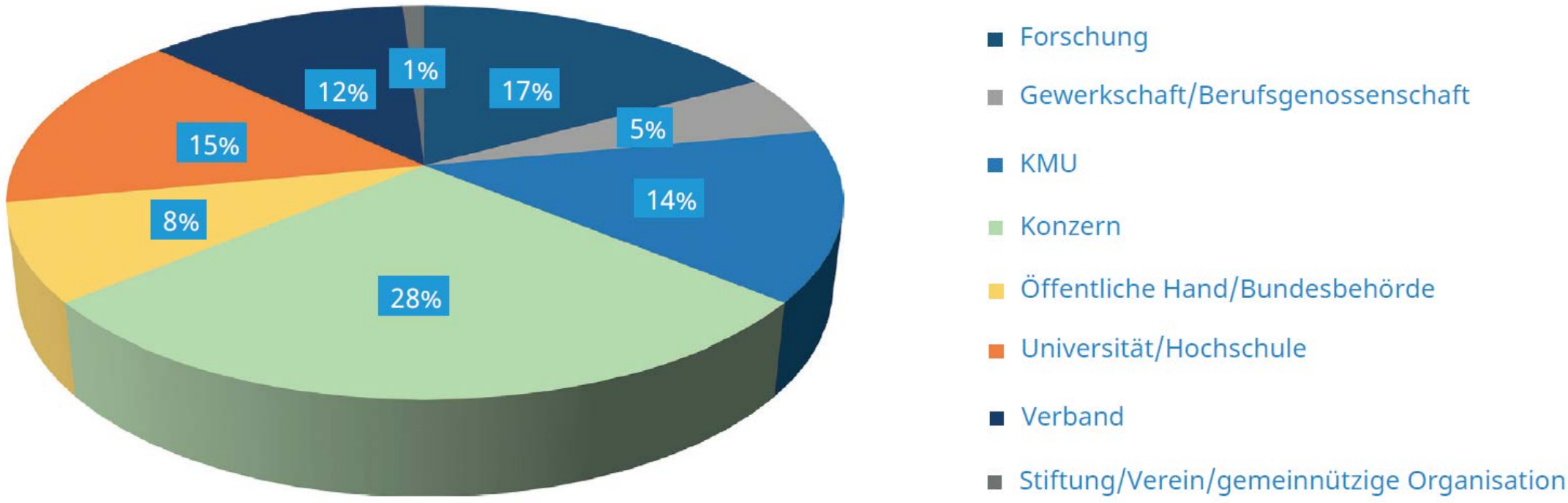
Arbeitsgruppen

- Grundlagen
- Ethik/Responsible AI
- Qualität, Konformitäts-bewertung und Zertifizierung
- IT-Sicherheit bei KI-Systemen
- Industrielle Automation
- Mobilität und Logistik
- KI in der Medizin

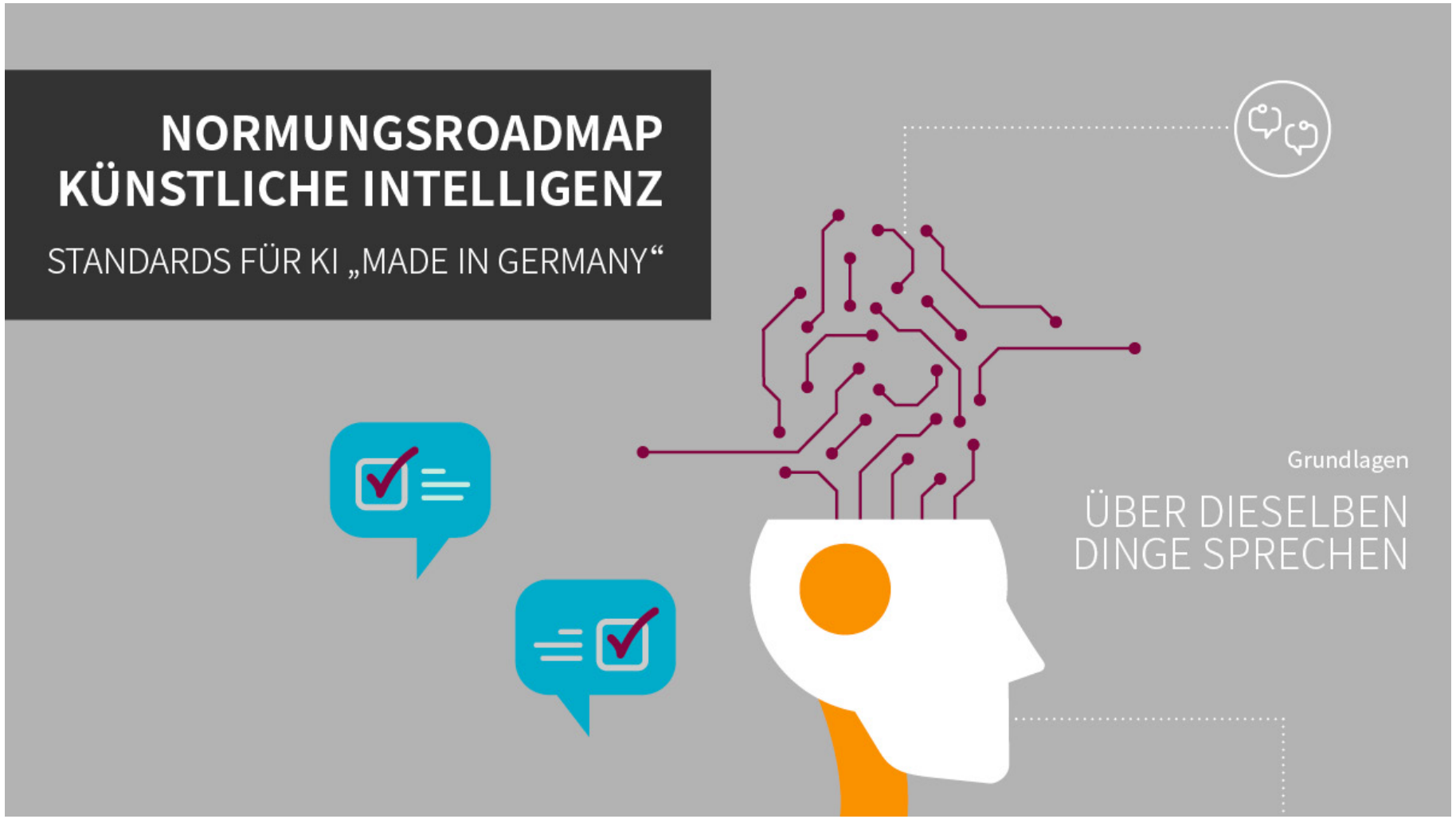
Normungsroadmap Künstliche Intelligenz: Basis schaffen

Zusammensetzung der Arbeitsgruppen

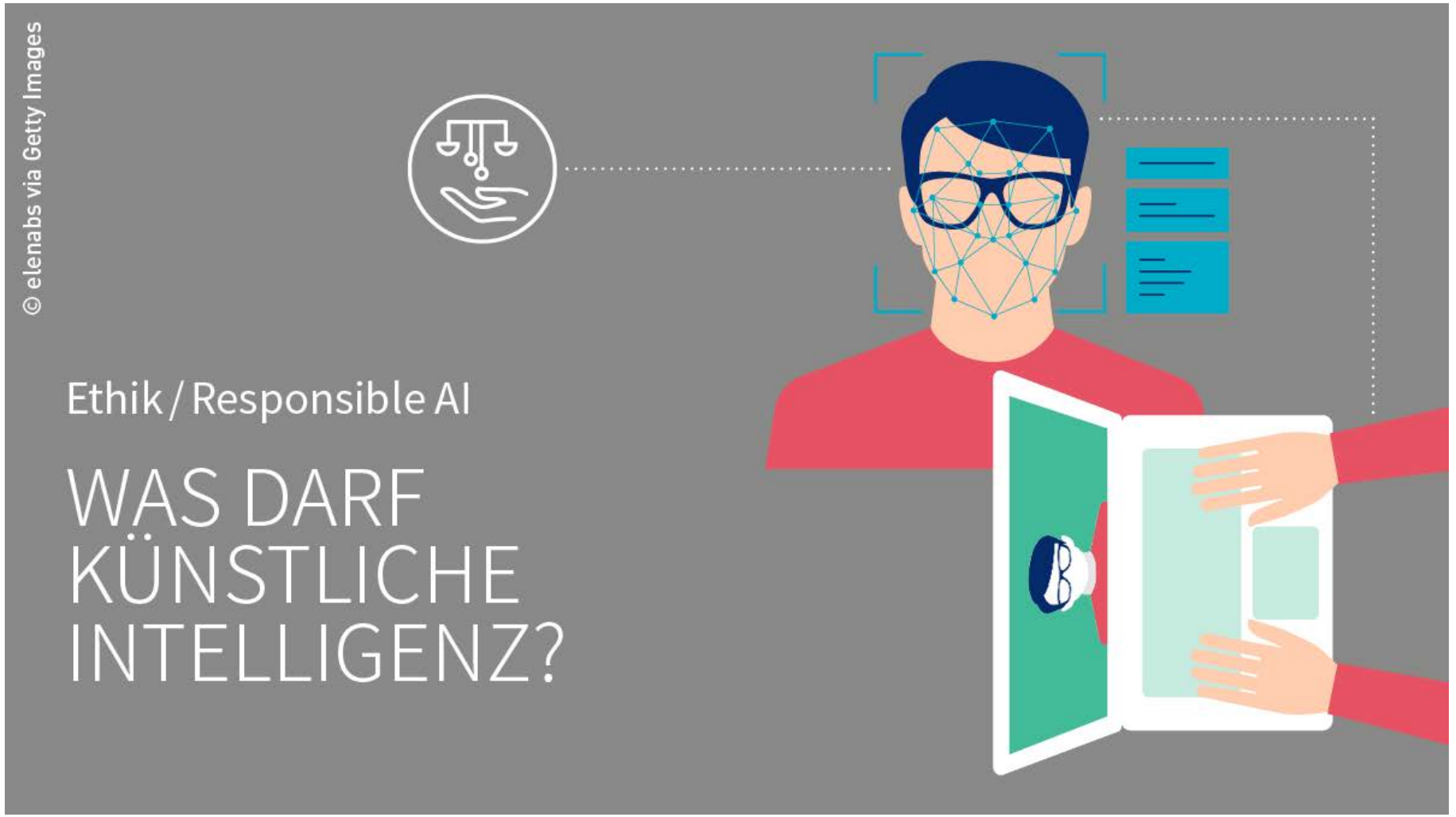
Anzahl: ca. 300



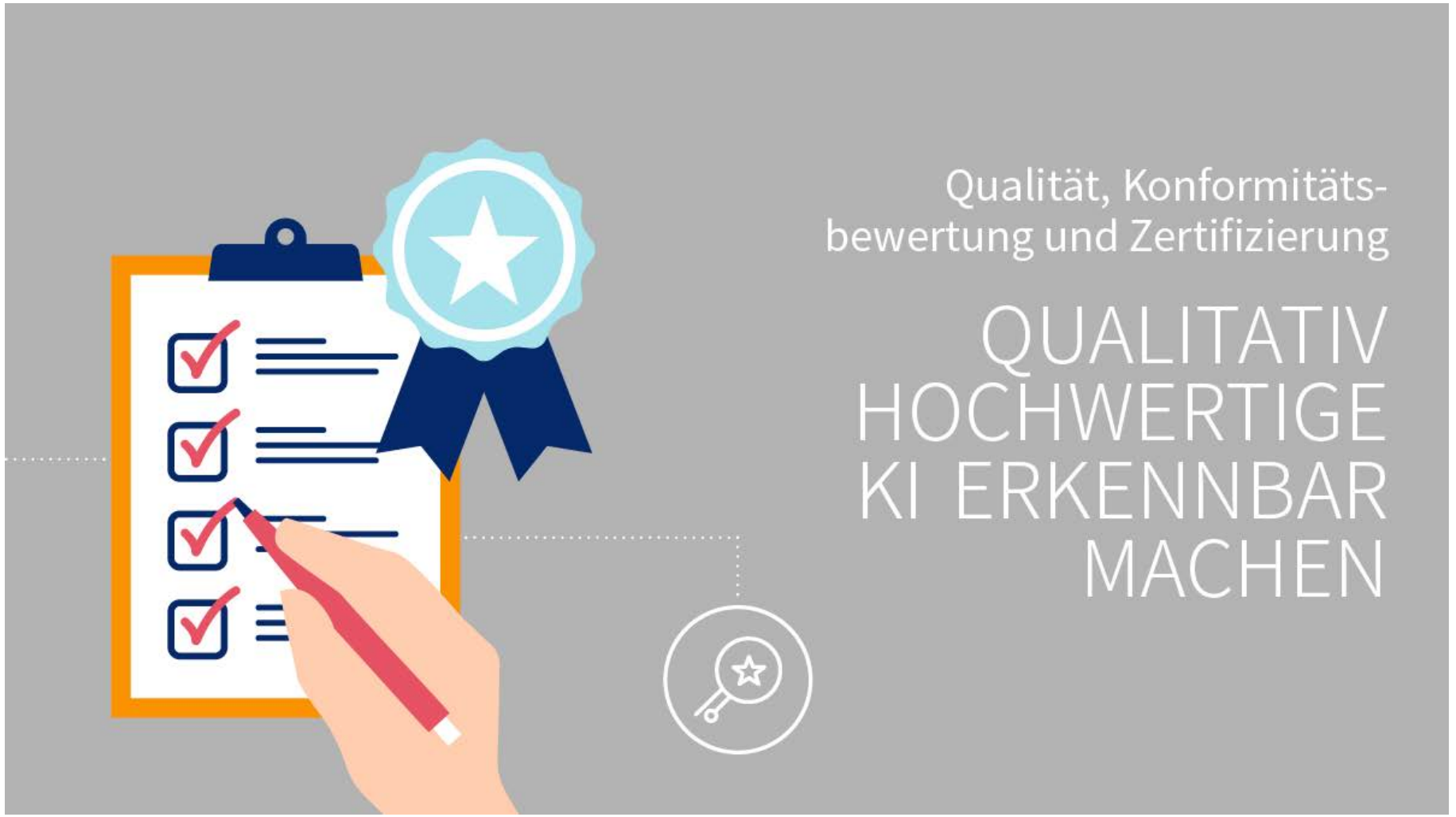
Schwerpunktthema: Grundlagen



Schwerpunktthema: Ethik

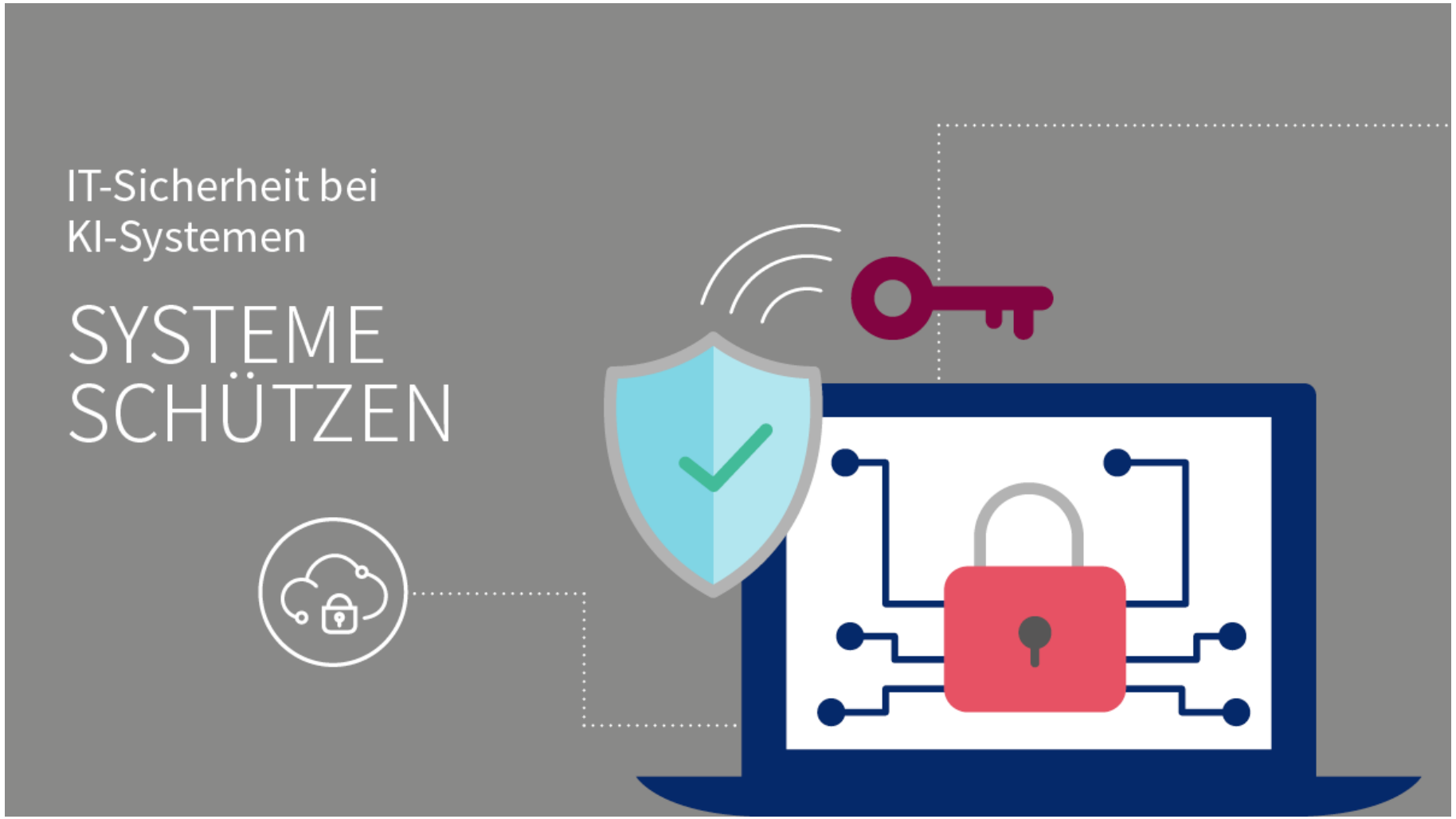


Schwerpunktthema: Qualität & Zertifizierung

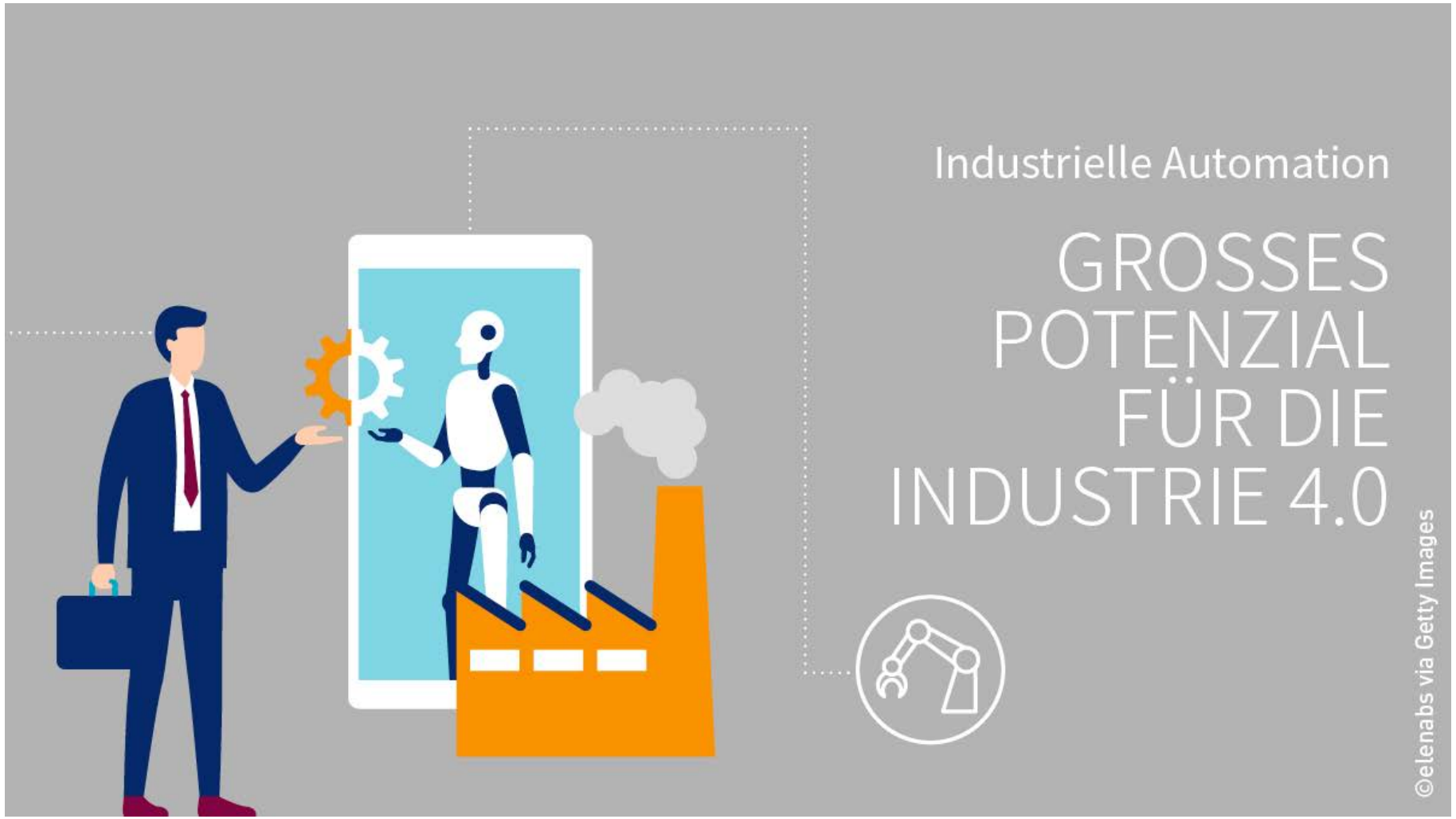


Normungsroadmap Künstliche Intelligenz

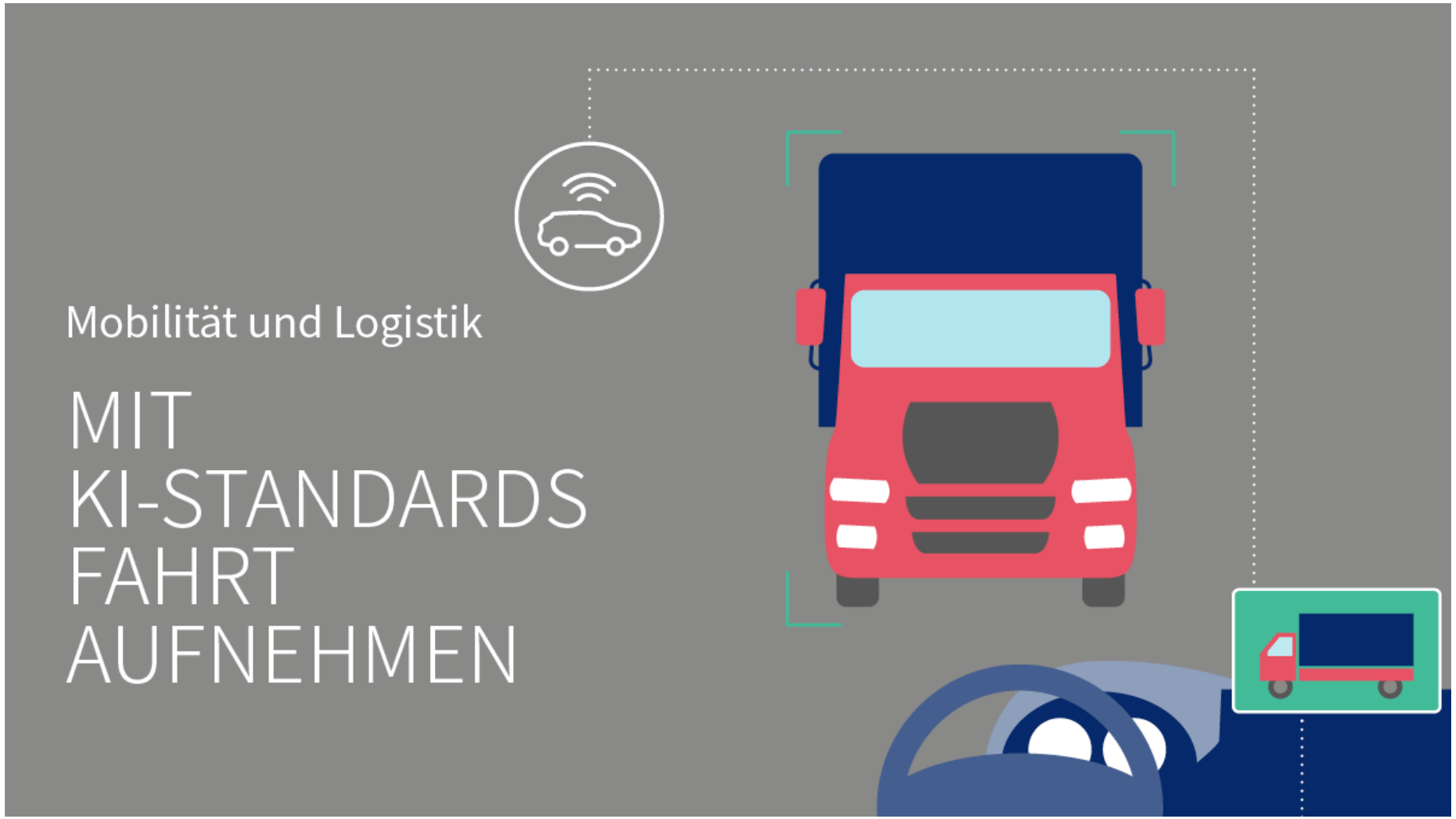
Schwerpunktthema: IT-Sicherheit



Schwerpunktthema: Industrielle Automation

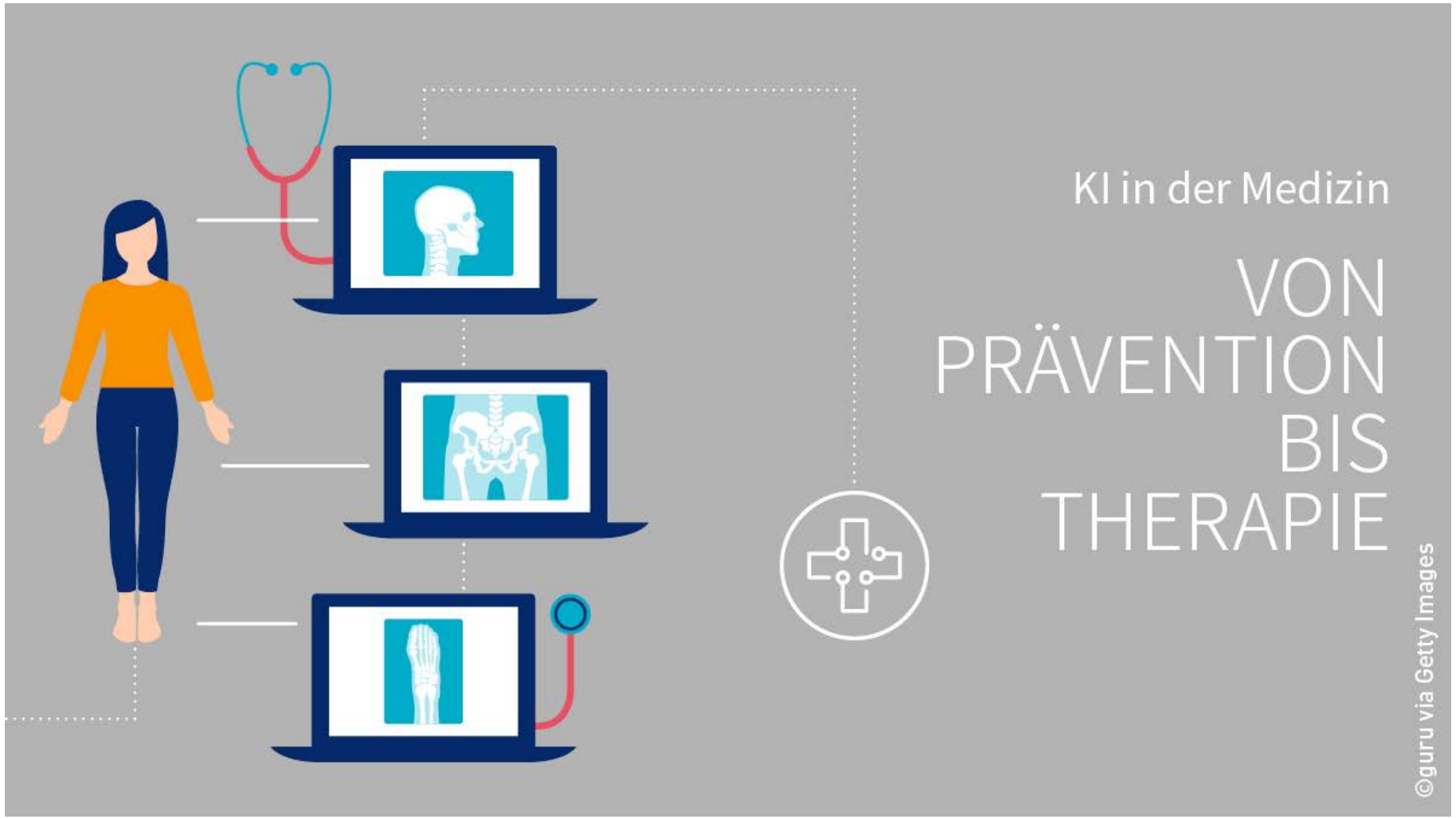


Schwerpunktthema: Mobilität & Logistik



Normungsroadmap Künstliche Intelligenz

Schwerpunktthema: KI in der Medizin



Normungsroadmap Künstliche Intelligenz

Handlungsempfehlungen der NRM KI

Handlungs-empfehlung 1	Handlungs-empfehlung 2	Handlungs-empfehlung 3	Handlungs-empfehlung 4	Handlungs-empfehlung 5
Initiierung und Durchführung eines Umsetzungs-programms für die Standardisierung von Datenreferenz-modellen für die Interoperabilität von KI-Systemen	Erstellung einer horizontalen KI-Basis-Sicherheitsnorm	Erarbeitung einer praxisgerechten, risikoadaptiven Kritikalitätsprüfung für KI-Systeme	Initiierung und Durchführung eines nationalen Umsetzungs-programms „Trusted AI“ zur Ertüchtigung der europäischen Qualitätsinfra-struktur	Analyse der Standardisierungs-bedarfe und agile Entwicklung marktreifer Normen und Standards mit Pilotprojekten (entlang von Use Cases) im Bereich der Künstlichen Intelligenz

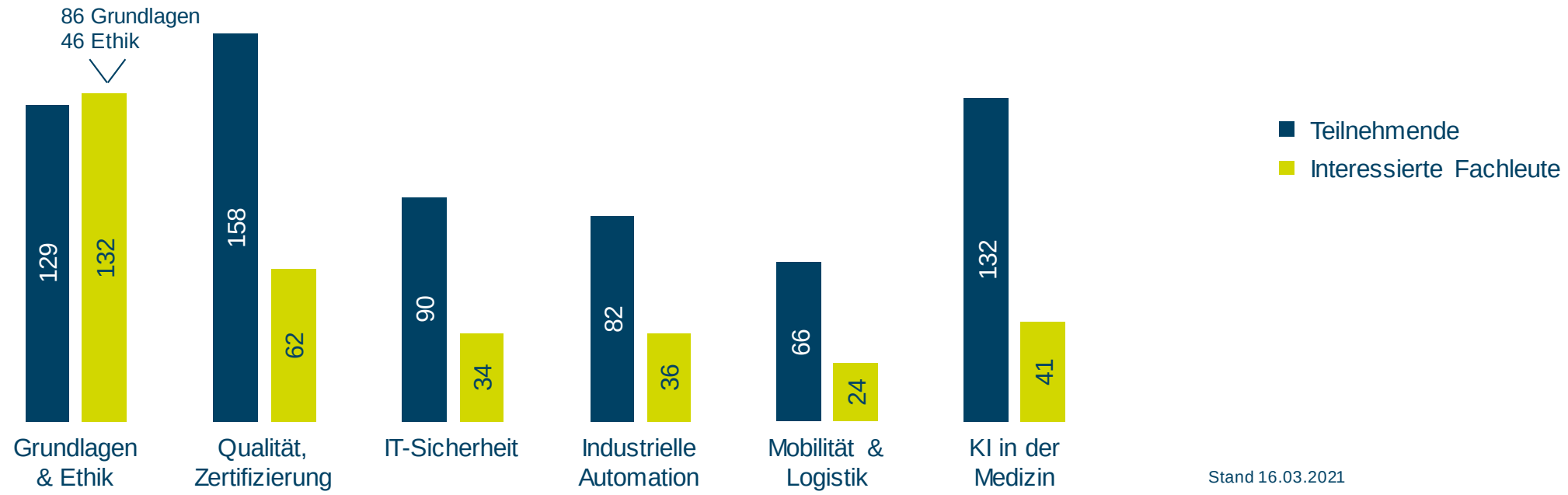
Normungsroadmap Künstliche Intelligenz

Prozess der Normungsroadmap KI

Normungsroadmap Künstliche Intelligenz: Verstetigen

Übersicht Fachworkshop

In Q1 2021 fanden sechs Workshops statt, in denen die Handlungsbedarfe der NRM KI diskutiert und priorisiert wurden. Hierzu haben sich insgesamt rund 500 Teilnehmende angemeldet.

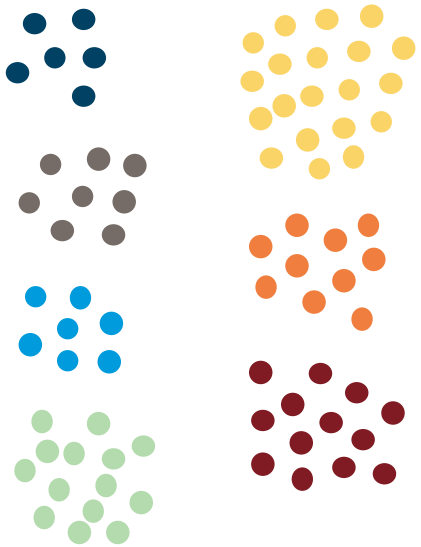


Stand 16.03.2021

Normungsroadmap Künstliche Intelligenz: Verstetigen

Analyse der Handlungsempfehlungen

Handlungsempfehlungen der NRM KI



Anreicherung der Handlungs-empfehlungen

- Thematische Verortung (betroffener Normen-ausschuss bzw. Arbeitsausschuss)
- Ansprechpartner bei DIN (zuständiger Projektmanager/ Gruppenleiter)
- Potentielle neue Experten

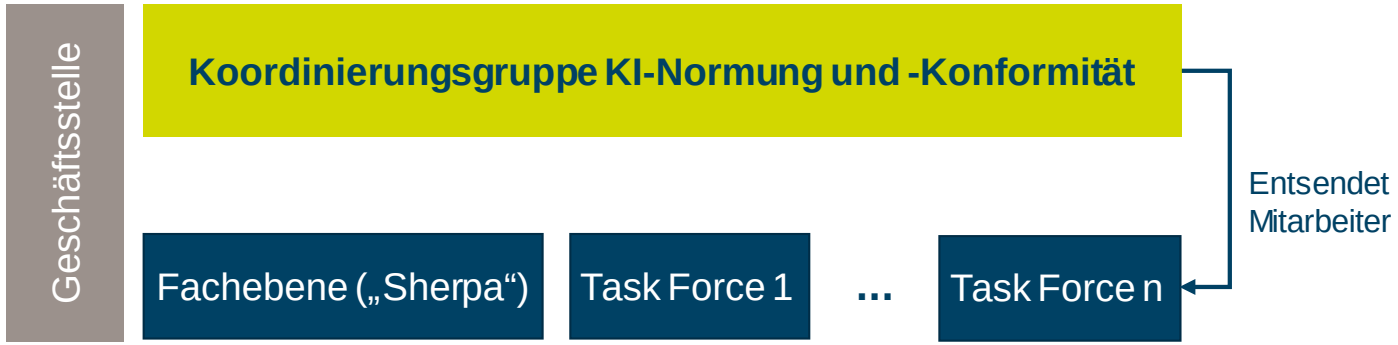
Kriterien zur Bewertung des weiteren Vorgehens

- Diskussionspunkte aus Fachworkshops
- Dringlichkeit der Umsetzung (Umfrage in Fachworkshops)
- Reifegrad des Bedarfs (wie explizit ist er formuliert oder besteht Notwendigkeit zur Konkretisierung)
- Abstimmung der Bedarfe mit Geschäftsführern der Normenausschüsse

Grundlagen
Ethik
Qualität, Zertifizierung
IT-Sicherheit
Industrielle Automation
Mobilität & Logistik
KI in der Medizin

Normungsroadmap Künstliche Intelligenz: Weiterentwickeln

Koordinierungsgruppe



Mandat

Die Bundesregierung, vertreten durch BMWi, BMBF und BMAS, beauftragt die Koordinierungsgruppe KI-Normung und -Konformität, alle zur Umsetzung der KI-Normungsroadmap notwendigen Aktivitäten durchzuführen.

Themenschwerpunkte

- Ganzheitliche Umsetzung der Normungsroadmap KI (Umsetzungsaktivitäten, Leuchtturmprojekte)
- Mitgestaltung des europäischen Ordnungsrahmens zu KI
- Impulse zur agilen Entwicklung von N.&.S. mit KI-Pilotprojekten, Überprüfung bestehender Normen auf KI-Tauglichkeit
- Fortschreibung der Normungsroadmap
- Kompetenzaufbau und (Weiter-) Bildung
- Strategische Kommunikation der Rolle der Normung am Beispiel von KI
- Empfehlungen zu wichtigen innovationspolitischen Entwicklungen und zur Gestaltung des Standorts Deutschland

Normungsroadmap Künstliche Intelligenz: Weiterentwickeln

Mitglieder der Koordinierungsgruppe

Politisch verantwortliche Ressorts

- Bundesministerium für Wirtschaft und Technologie – Stefan Schnorr
- Bundesministerium für Arbeit und Soziales – Dr. Julia Borggräfe
- Bundesministerium für Bildung und Forschung – Prof. Ina Schieferdecker

Technologische KI-Forschung

- DFKI – Prof. Jana Koehler
- Fraunhofer – Prof. Stefan Wrobel
- Lernende Systeme – Prof. Wolfgang Wahlster

Gesellschaft und Ethik

- verbraucherzentrale Bundesverband – Jutta Gurkmann
- IG Metall – Detlef Gerst
- Open Knowledge Foundation – Julia Kloiber

Normungsorganisationen

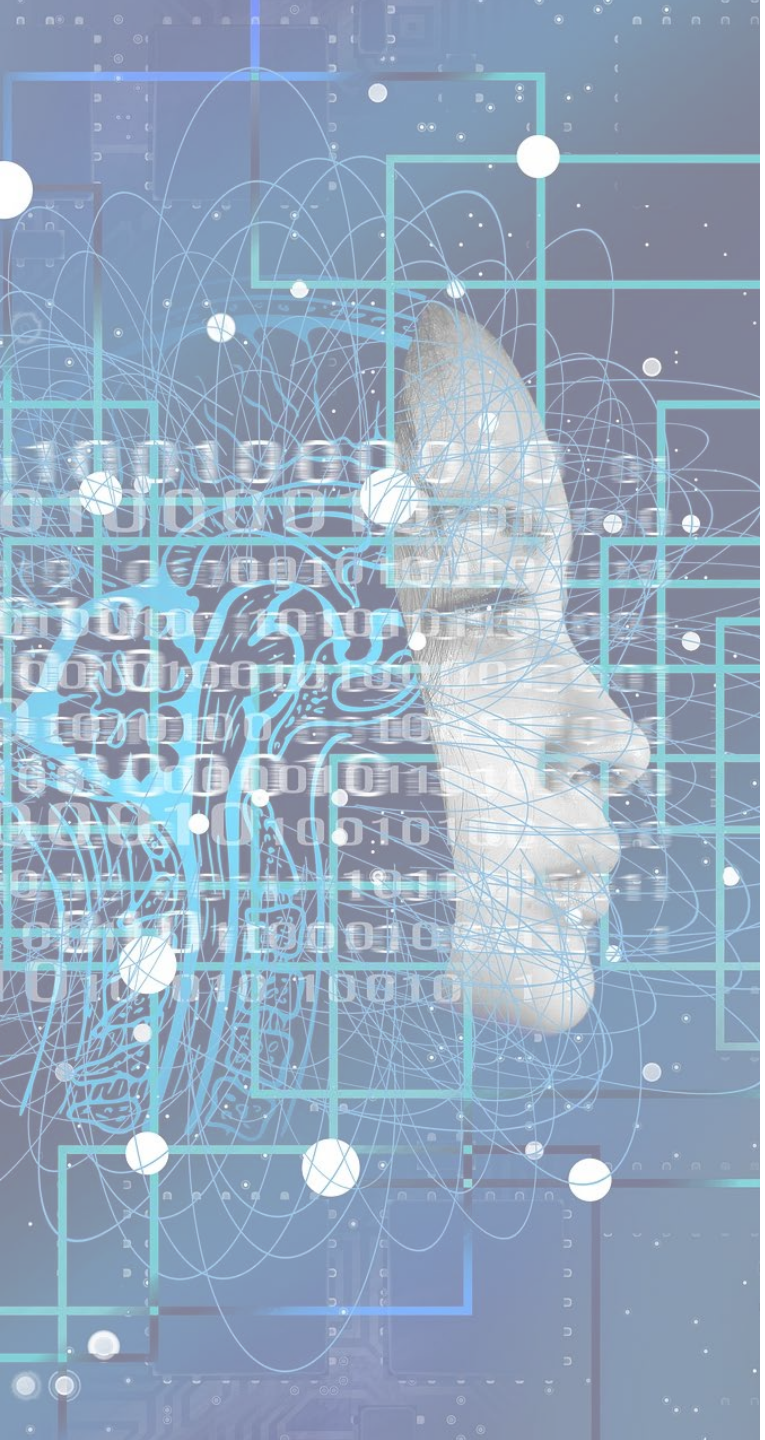
- DIN – Christoph Winterhalter
- DKE – Prof. Dieter Wegener

Industrie und Wirtschaftsverbände

- bitkom / IBM – Dr. Wolfgang Hildesheim
- ZVEI: Die Elektroindustrie – N.N.
- VdTÜV – Dr. Joachim Bühler
- eco – Alexander Rabe
- VDMA / VDA / BOSCH – Dr. Christoph Peylo
- DIHK – Dr. Volker Treier
- KI Bundesverband – Dr. Tina Klüwer

Ständige Gäste

- Lernende Systeme – Dr. Johannes Winter

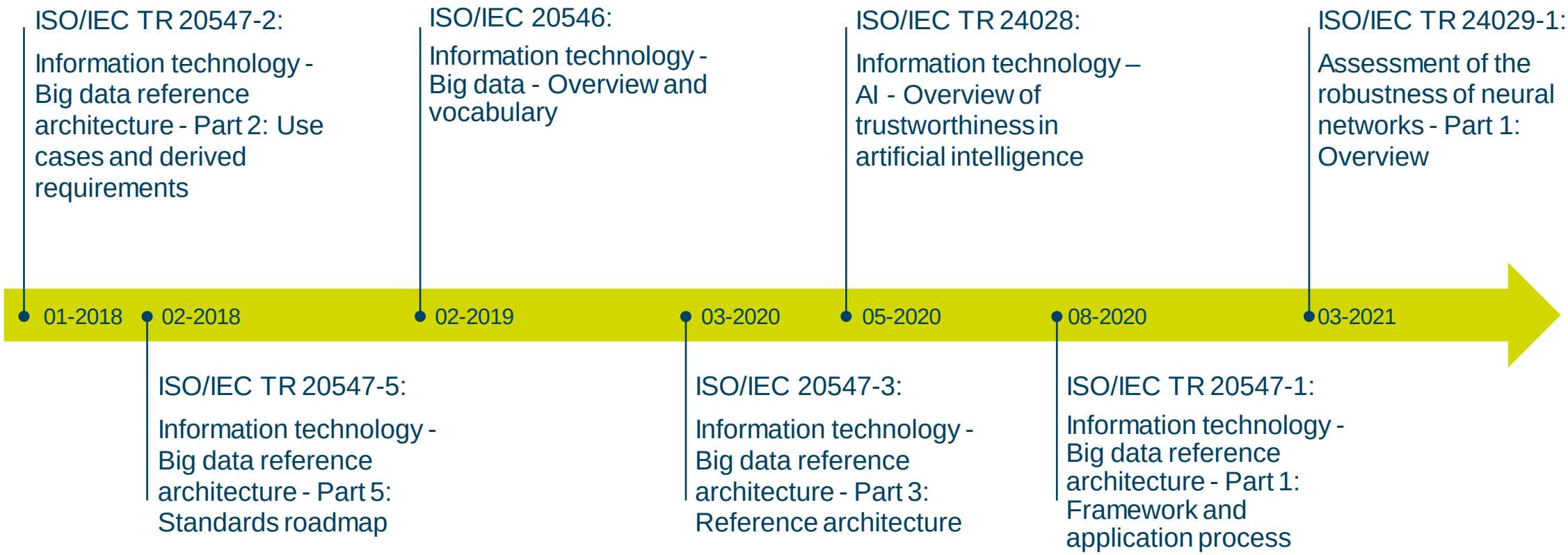


Agenda

1. Einführung
2. Normungsroadmap KI
3. Aktivitäten
4. Ausblick

Aktivitäten

Veröffentlichte internationale Standards



Aktivitäten

Veröffentlichte DIN SPECs

Aktivitäten

Laufende Normungsprojekte (1/3)

WG 1 Foundational Standards

ISO/IEC CD 22989: AI - Concepts and terminology

ISO/IEC CD 23053: Framework for AI(AI) Systems Using Machine Learning (ML)

ISO/IEC WD 42001: Management system

WG 2 Data

ISO/IEC WD 5259-1: Data quality for analytics and ML - Part 1: Overview, terminology, and examples

ISO/IEC AWI 5259-2: Data quality for analytics and ML - Part 2: Part 2: Data quality measures

ISO/IEC WD 5259-3: Data quality for analytics and ML - Part 3: Data quality management requirements and guidelines

ISO/IEC WD 5259-4: Data quality for analytics and ML - Part 4: Data quality process framework

ISO/IEC CD 24668: Process management framework for Big data analytics

Aktivitäten

Laufende Normungsprojekte (2/3)

WG 3 Trustworthiness

- ISO/IEC AWI TR 5469: Functional safety and AI systems
- ISO/IEC CD 23894:Risk Management
- ISO/IEC AWI TR 24027:Bias in AI systems and AI aided decision making
- ISO/IEC AWI 24029-2: Assessment of the robustness of neural networks - Part 2: Methodology for the use of formal methods
- ISO/IEC AWI TR 24368: Overview of ethical and societal concerns
- ISO/IEC AWI 25059: Software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Quality model for AI-based systems
- ISO/IEC AWI TS 6254: Objectives and methods for explainability of ML models and AI systems

WG 4 Use Cases

- ISO/IEC WD 5338: AI system life cycle processes
- ISO/IEC WD 5339: Guidelines for AI applications
- ISO/IEC CD TR 24030: Artificial Intelligence (AI) - Use cases

Aktivitäten

Laufende Normungsprojekte (3/3)

WG 5 Computational approaches and characteristics

ISO/IEC WD TS 4213: Assessment of machine learning classification performance

ISO/IEC WD 5392: Reference architecture of knowledge engineering

ISO/IEC AWI DTR 24372: Overview of computational approaches for AI systems

Joint Working Governance implications of AI

ISO/IEC CD 38507: Governance of IT - Governance implications of the use of artificial intelligence by organizations

Forschungsprojekt Zertifizierte KI

Projektübersicht

März 2021 bis Februar 2026

Gesamtvolumen ~ 10,8 Mio. Eur

Zertifizierung von Standard-KI-Anwendungen (ZERTIFIZIERTE KI)

Fraunhofer IAIS

UNIVERSITÄT BONN

Universität zu Köln

RWTH AACHEN UNIVERSITY

DIN

Bundesamt für Sicherheit in der Informationstechnik

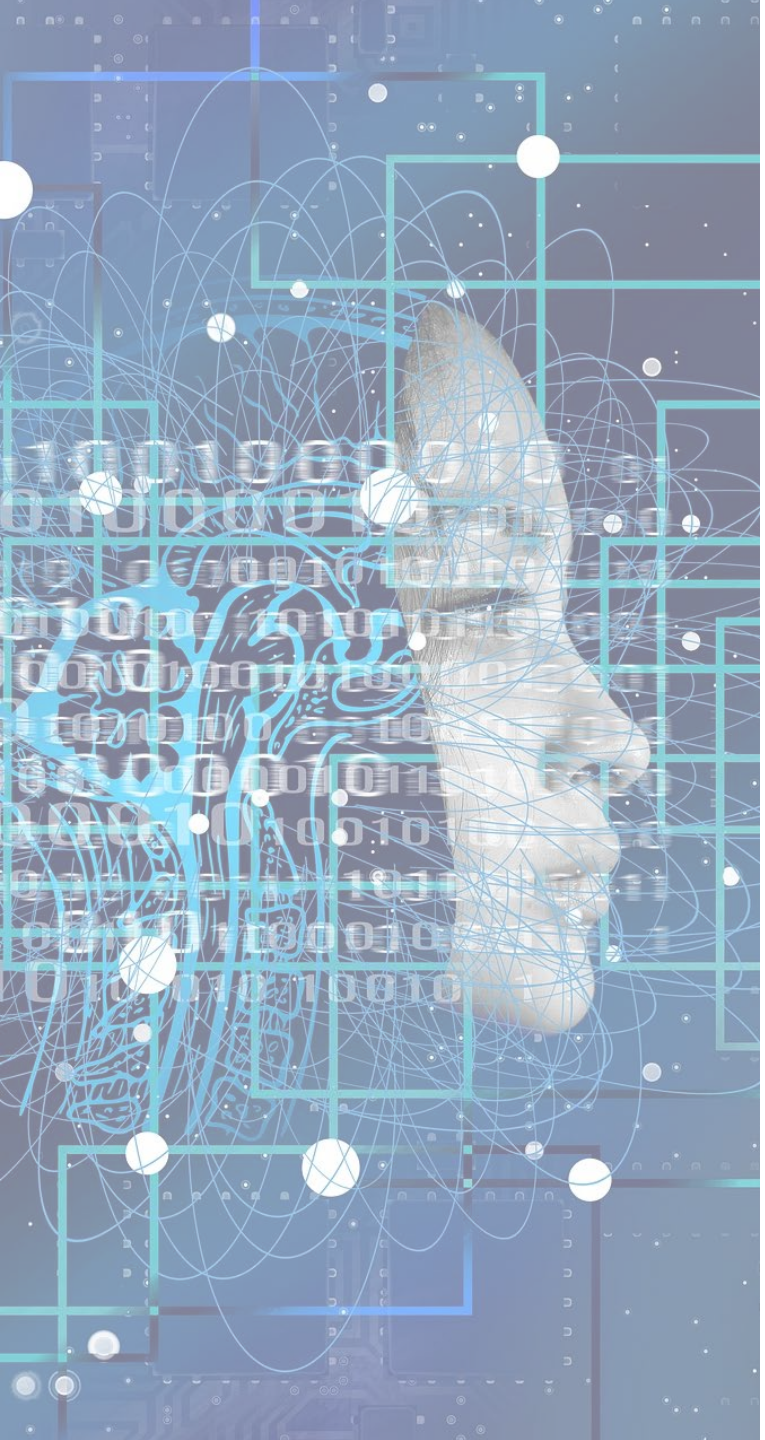
Projektziel:

- **Erarbeitung von standardisierungsreifen Prüfkriterien und Prüfmethoden für KI-Systeme**
- Entwicklung von Absicherungsmethoden und Prüfwerkzeugen für KI-Systeme
- Ergebnistransfer in konkrete Wirtschaftsangebote

Gefördert durch:

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

PtJ Projektträger Jülich Forschungszentrum Jülich



Agenda

1. Einführung
2. Normungsroadmap KI
3. Aktivitäten
4. Ausblick

Ausblick: weitere Sektoren

Sektorenbetrachtung

Schwerpunktthemen NRM KI
Abfrage in Fachworkshops

Ausblick: KI-Regulierung

EU-Regulierung

Ziel

- Schaffung eines einheitlichen europäischen Regelungsrahmens für das Inverkehrbringen, den Einsatz und die Nutzung von KI

Limitationen

- Waffensysteme werden explizit ausgeschlossen

Risikobasierter Ansatz

- Verbot gefährlicher KI-Anwendungen (u.a. Social Scoring, willkürliche Überwachung, unterschwellige Einflussnahme auf die/den Nutzer*in)
- Hochrisiko KI („high risk AI“) soll nach Prinzip des New Legislative Framework (NLF) auf Basis harmonisierter Europäischer Normen (hEN) mit Vermutungswirkung und mit Anbringung der CE-Kennzeichnung in Verkehr gebracht werden
  - Dokumentationspflichten für Hersteller
  - Anbringung der CE-Kennzeichnung
  - Hinzuziehung einer benannten dritten Stelle für Anwendungen
- KI-Systeme und -Anwendungen mit geringem Risiko (z.B. Chatbots) müssen Transparenzanforderungen erfüllen
- Risikofreie KI-Systeme werden nicht reguliert

Ausblick: KI-Regulierung

EU-Regulierung

Kernaussagen

- Regulierung soll robust und doch flexibel sein mit einem freiwilligen „codes of conduct“, der über die Regulierung hinausgeht, mit klaren KPIs
- Entwicklung von Ethischen Leitlinien für die Entwicklung und Verwendung von KI
- Datenbank für „high-risk“ KI-Systeme, eingerichtet und überwacht durch die Kommission, öffentlich einsehbar
- Innovationskomponente: Experimentierräume („Sandboxing schemes“) werden eingerichtet als Testumgebungen für neue KI-Entwicklungen
- Einrichtung des „European Artificial Intelligence Board“
- Jeder Mitgliedsstaat benennt eine nationale Behörden (in DE vrsl. die DAkkS), die Überwachung der Konformitätsbewertung nach der Regulierung übernimmt
- Biometrische Systeme im öffentlichen Raum (z.B. zur Einreisekontrolle) werden explizit erwähnt

Kritisch

- Mit dem Artikel 41 „common specifications“ wird durch Kommission, wie auch z.B bei der Batterieverordnung, eine Hintertür zum NLF eingebaut
  - Wo keine harmonisierten Normen existieren oder wo relevante harmonisierte Normen nicht ausreichen: Recht per Durchsetzungsrechtsakt „common specifications“ zur Umsetzung der technischen Anforderungen aus Titel III
  - Nicht beschrieben, was der Grund dafür sein muss, dass es keine hEN gibt und „common specifications“ erlassen werden dürfen

Nächste Schritte

- Aufnahme in AUWP der Europäischen Kommission
- Erarbeitung DIN/DKE-Stellungnahme
- Einbringen Konsultationsphase
- Dialog mit polit. Stakeholdern und Schattenberichterstattern
- Implikation für laufende Projekte berücksichtigen

Informationen und Links

Weitere Informationen

KI-Themenseite www.din.de/go/ki mit Informationen rund um das Thema KI.
Dort finden Sie u.a.:

- **Normungsroadmap KI**: steht sowohl in dt. als auch in engl. Sprachfassung zum kostenlosen Download bereit (www.din.de/normungsroadmapki).
- **KI-Flyer**: fasst die wesentlichen Ergebnisse und Handlungsempfehlungen der Normungsroadmap KI zusammen
- **KI-Film**: erklärt am Beispiel Medizin, wie KI funktioniert und welchen Nutzen Normen und Standards haben
- **Übersicht** über veröffentlichte Normen und Standards sowie laufende Normungs- und Standardisierungsaktivitäten

DIN.ONE Kollaborationsplattform www.din.one/site/ki werden weitergehende Informationen und Möglichkeiten der Mitwirkung geboten. Interessierte können sich kostenfrei registrieren und sich in den weiteren Prozess der Umsetzung der Normungsroadmap KI aktiv einbringen.

Filiz Elmas

Leiterin Geschäftsfeldentwicklung Künstliche Intelligenz

Filiz.Elmas@din.de

+49 (0) 30 2601-2464

www.din.one/site/ki

DIN
Deutsches Institut für Normung e. V.
Saatwinkler Damm 42/43
13627 Berlin

www.din.de