DEKRA

DEKRA DIGITAL

Künstliche Intelligenz:
Was ist es, was kann es, und wie wird es reguliert?

Dr. Tarek R. Besold

(07.09.2021)

Was ist KI?

*„**KI ist jene Wissenschaft, die sich der Erforschung und dem Bau intelligenter Maschinen widmet**, und Intelligenz ist jene Eigenschaft, welche es einer Entität ermöglicht, angemessen und vorausschauend in ihrer Umgebung zu funktionieren.“*

(Nach: Nilsson, *The Quest for Artificial Intelligence*, 2009)

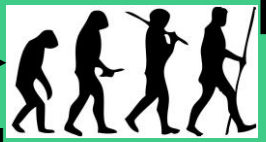
HEUTE

SCIENCE FICTION

Niedrig-stufige technologische Systeme

Große Lücke!

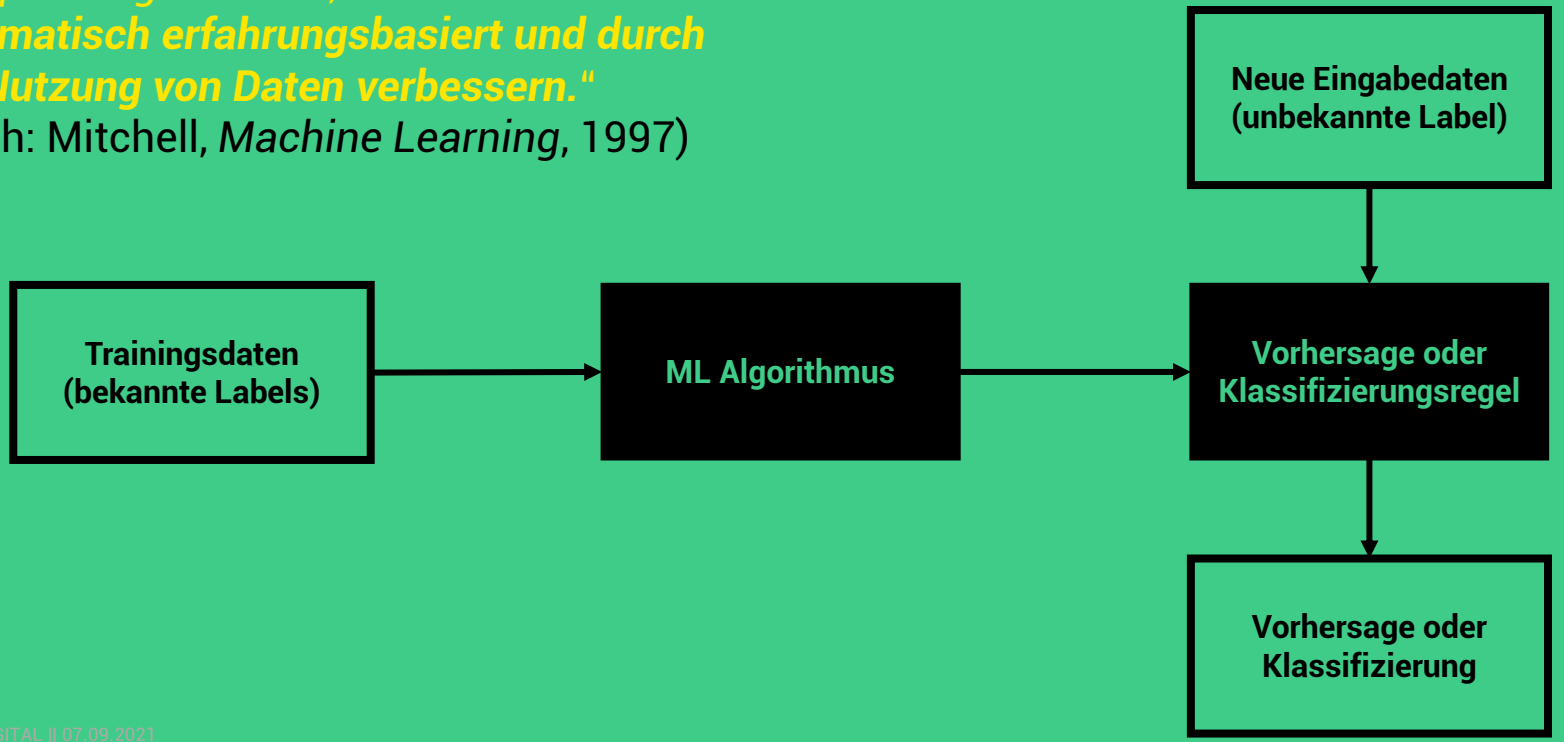
Noch eine große Lücke!



?

Was ist Maschinelles Lernen?

*„**Maschinelles Lernen (ML)** bezeichnet das Studium und den Bau von Computeralgorithmen, welche sich selbst **automatisch erfahrungsbasiert und durch die Nutzung von Daten verbessern.**“*
(Nach: Mitchell, *Machine Learning*, 1997)

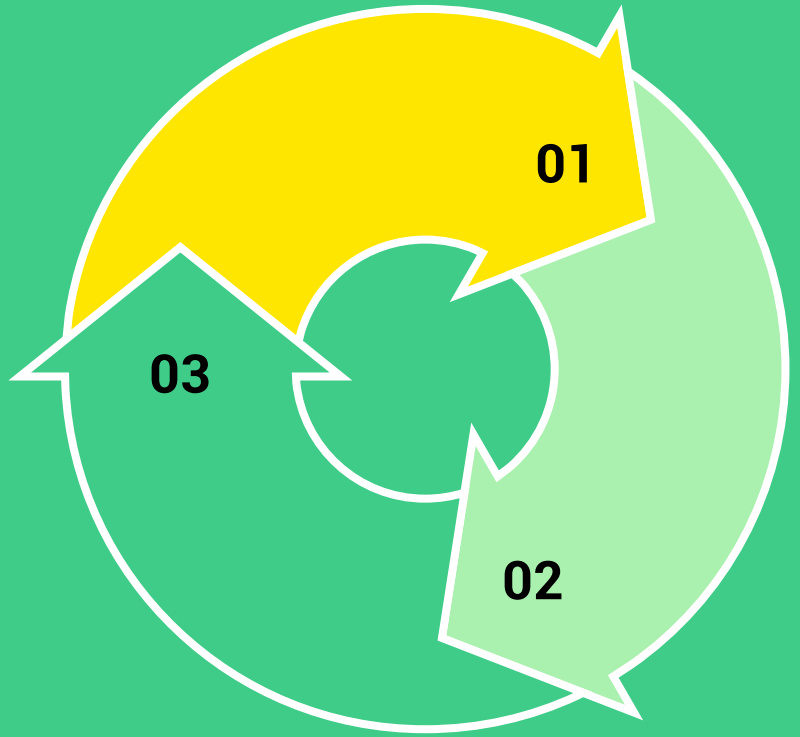


3 Schritte der KI-Lösungsentwicklung

	Datenvorbereitung	KI-Entwicklung	
Prozess	▪ Problembeschreibung und KPI-Definition ▪ Datenverfügbarkeit prüfen ▪ Datenzugriff und Vorbereitung des Datensets	▪ Datenverarbeitung ▪ KI-Modelltraining und -optimierung ▪ KI-Modelltest(s)	▪ Systemintegration ▪ Nutzerakzeptanztest(s) ▪ Roll-out und Nutzertraining
Schlüssel-rollen	Nutzer und Domänenexperten IT - Data Platform	KI-Ingenieure	SW & Big Data Ingenieure Nutzer und Domänenexperten

Projektlebenszyklus

Kontinuierliche Verbesserung



Vorbereitung

Problem, Daten und KPIs hinterfragen.

KI-Entwicklung

Optimierung des Modells mit neuen Daten oder Erkenntnissen

Produktisierung

Roll-out neuer Lösung mit optimiertem Modell

Bandbreite an KI-Lösungen

Computer Vision

Computer Audition

Computer Linguistics

Robotics and Control

Forecasting

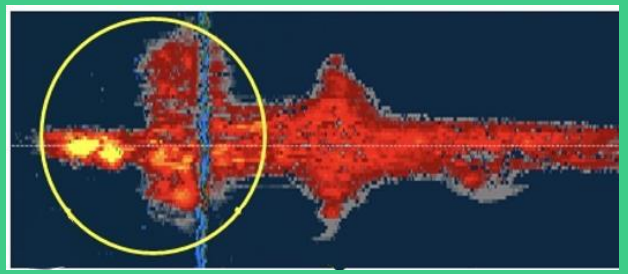
Discovery

Planning

Creation

KI in der zerstörungsfreien Prüfung

Fotoaufnahme



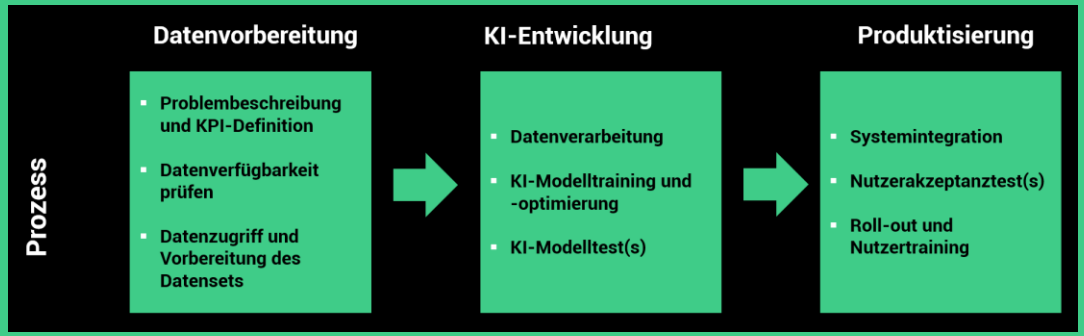
Messdaten

Datenanalyse zur Identifikation von Pipelineanomalien

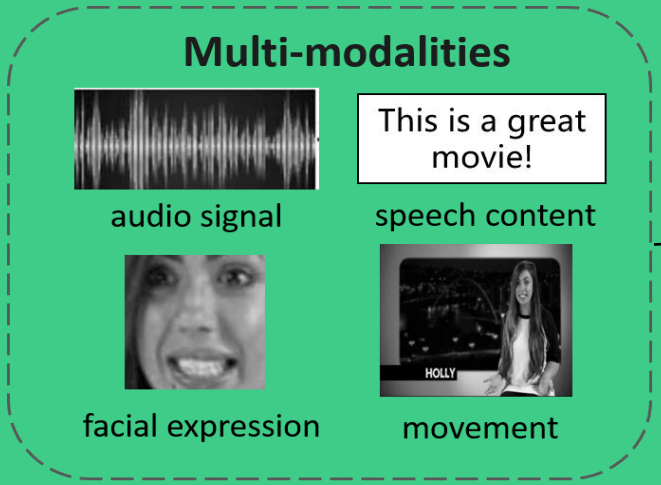
→ Manueller, teurer Prozess

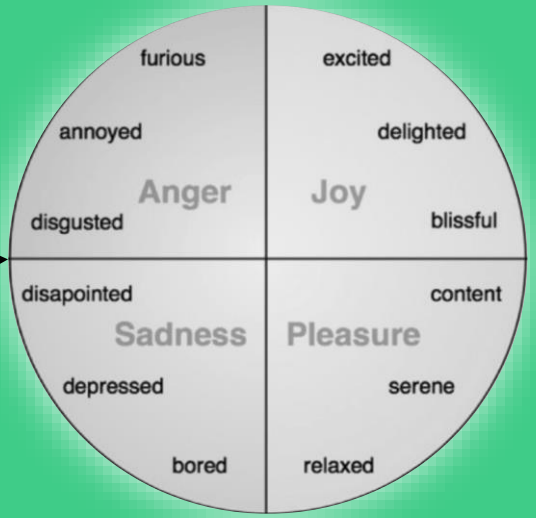
KI-Einsatz zur Automatisierung des Analyseprozesses

→ 20% Kostenreduktion



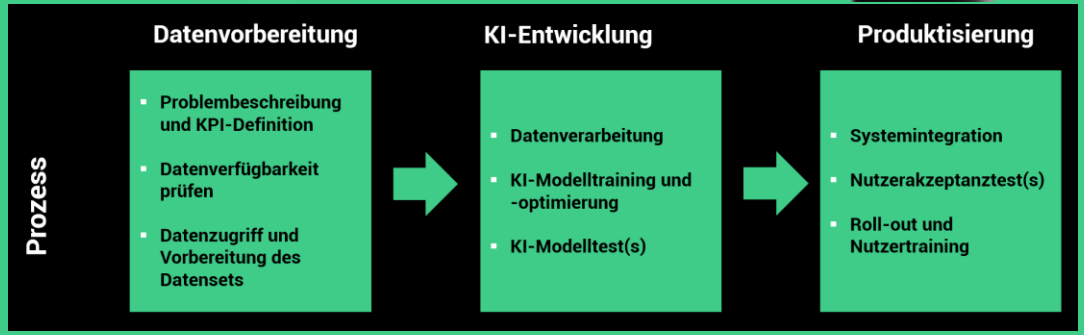
KI in multimodaler Emotionsanalyse





Datenanalyse zur Identifikation und zum Monitoring des emotionalen Zustands der Nutzer

Angewandt in smartphone-basierter digitaler Gesundheitsanwendung zur Überwachung der Wirksamkeit verhaltensbasierter Interventionen



KI ist kein Selbstläufer

Die Anwendung von ML in Automatisierungsszenarien kann durch verschiedene Faktoren erschwert werden, wie etwa der Qualität und/oder Menge der verfügbaren Trainingsdaten (die GIGO-Regel: „*garbage in, garbage out*“) und der Opakheit des entstehenden ML Modells:

Falls zu wenige Eingabebeispiele vorliegen, kann der ML Algorithmus keine ausreichend generellen Regeln extrahieren.

Datenmenge

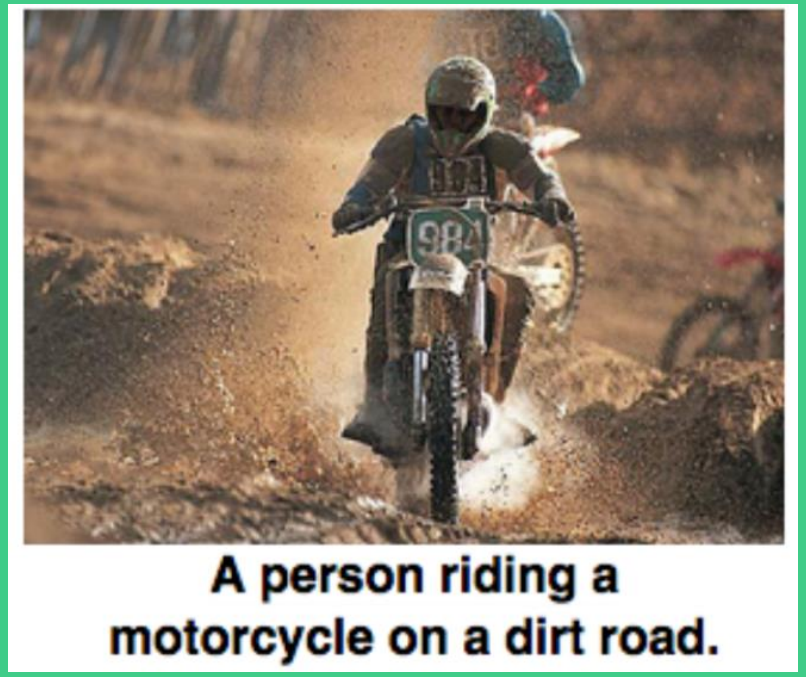
Falls die verfügbaren Eingabebeispiele nicht alle relevanten Beispielfälle beinhalten, oder zu stark in ihrer Qualität schwanken, kann der ML Algorithmus keine verlässlichen Regeln extrahieren.

Datenqualität

Die meisten ML-Systeme repräsentieren die gelernten Regeln nicht explizit, was die Überprüfung der Korrektheit und der Vollständigkeit der gelernten Programme erschwert.

Opakheit

KI ist kein Selbstläufer



Google, 2014

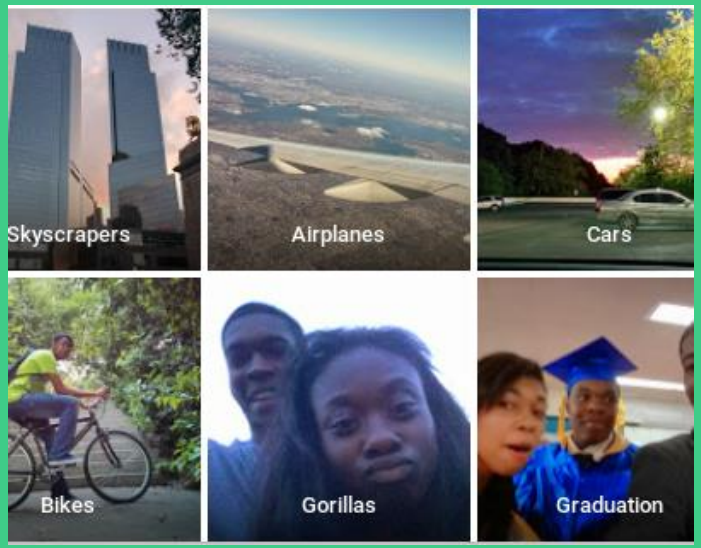
Google, 2014

KI ist kein Selbstläufer

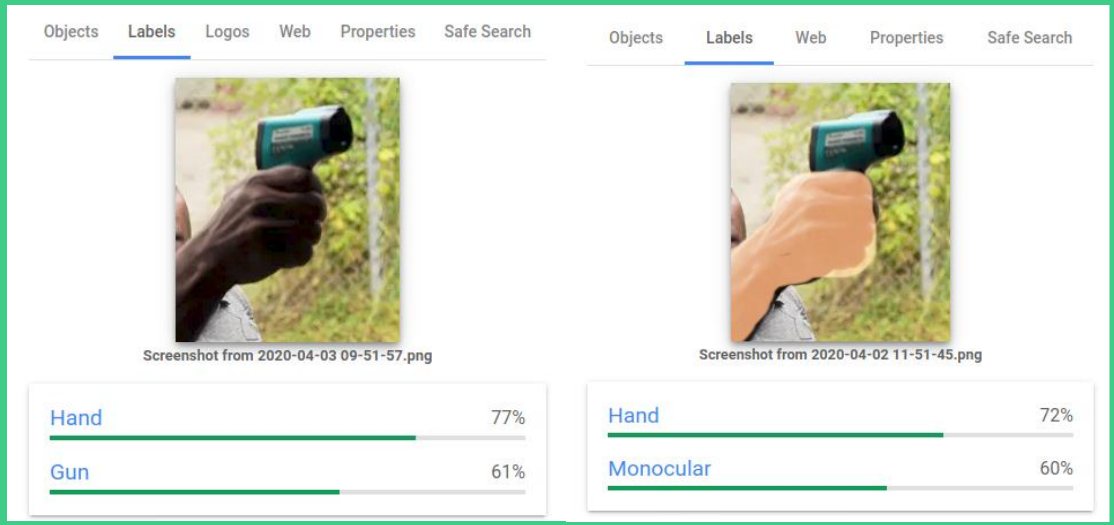
Google, 2014

Person + Hund + Grüne Wiese ≠ Frisbee fangen

KI ist kein Selbstläufer



Google, 2015



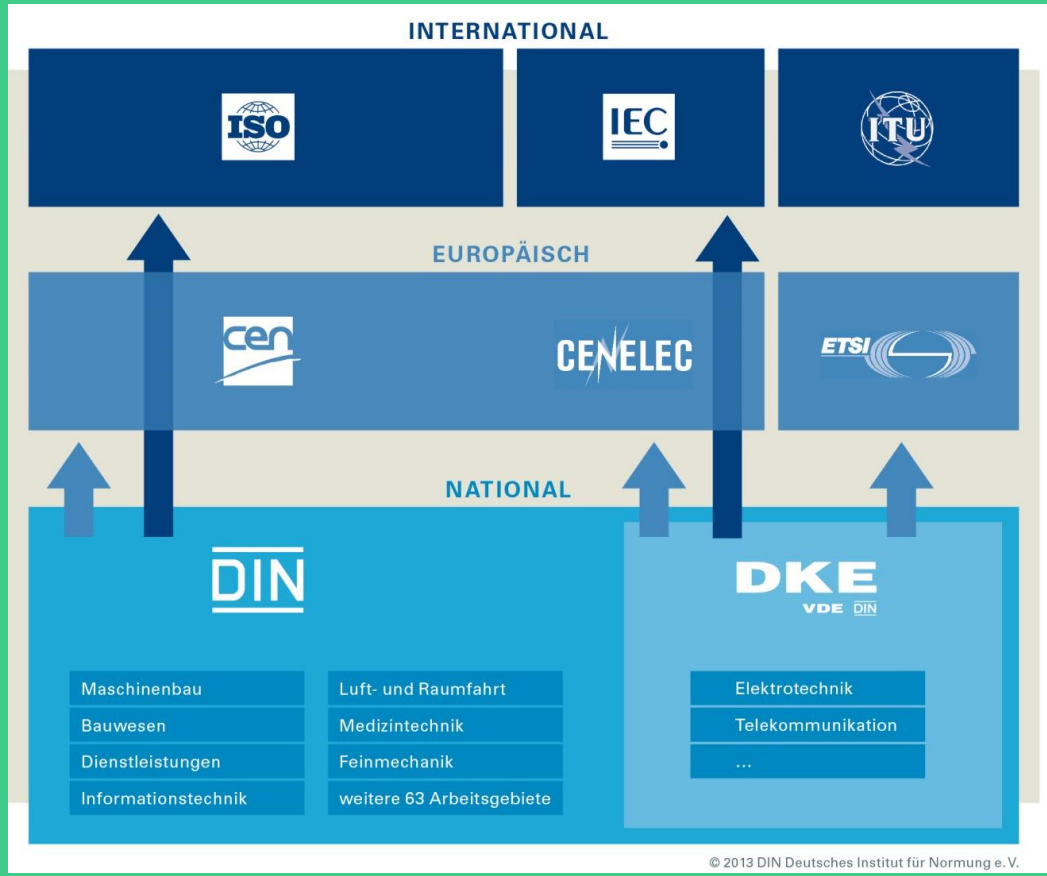
Google, 2020

Auch KI muss getestet und zertifiziert werden!

Standards und Normen

- **Norm:**
  - Dokument, das Anforderungen an Produkte, Dienstleistungen oder Verfahren festlegt.
  - Schafft Klarheit über Eigenschaften, erleichtert freien Warenverkehr, fördert Export.
  - Unterstützt Rationalisierung und Qualitätssicherung in Wirtschaft, Technik, Wissenschaft und Verwaltung.
  - Dient unter anderem Sicherheit von Menschen und Sachen sowie der Qualitätsverbesserung.
  - Unterschied zu Standard: Normen werden von Normungsorganisationen „offiziell“ erstellt und veröffentlicht.

Die Standardisierungslandschaft aus deutscher Sicht



ISO: Internationale Organisation für Normung

IEC: Internationale Elektro-technische Kommission

ITU: Internationale Fernmeldeunion

CEN: Europäisches Komitee für Normung

CENELEC: Europäisches Komitee für Elektrotechnische Normung

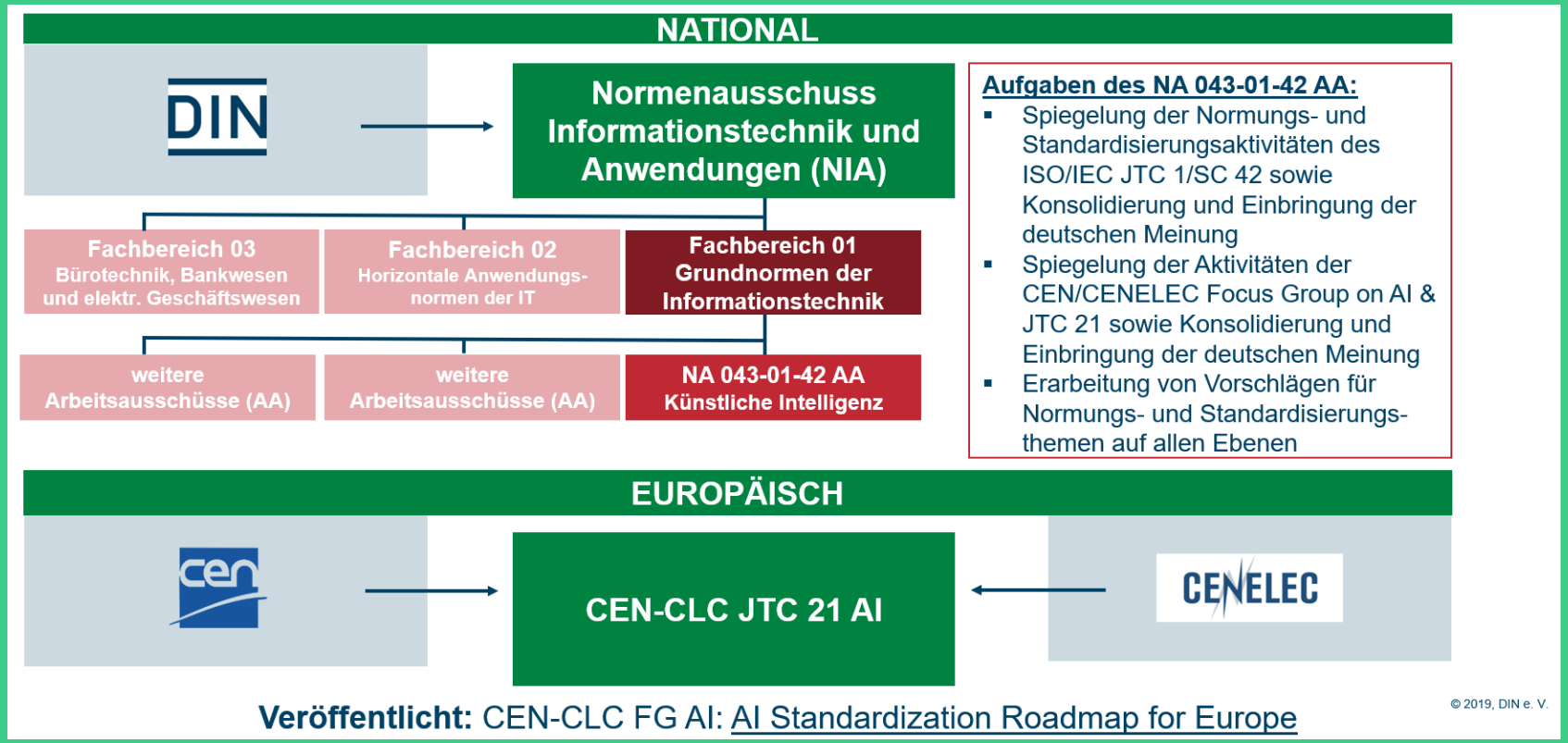
ETSI: Europäisches Institut für Telekommunikationsnormen

DIN: Deutsches Institut für Normung e. V.

DKE: Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

DIN und DKE vertreten die nationalen Interessen in der europäischen und internationalen Normung.

KI-Normung auf deutscher und europäischer Ebene



Harmonisierte Normen auf EU-Ebene

- Als **harmonisierte Normen** im Sinne des New Legislative Frameworks werden die europäischen Normen angesehen, die die europäische Normenorganisationen (CEN; CENELEC; ETSI) der EC formell vorlegen und die in deren Auftrag erarbeitet wurden (sog. *mandatierte Norm*) und deren Fundstelle im EU-Amtsblatt veröffentlicht wurde.

- **Konformitätsvermutung**: Wenn bei Entwurf und Fertigung eines Produkts harmonisierte Normen angewandt werden, geht der Gesetzgeber automatisch davon aus, dass das Produkt mit jenen grundlegenden Sicherheits- und Gesundheitsschutzanforderungen der Harmonisierungsrechtsvorschrift, welche die Norm abdeckt, konform ist.

Harmonisierte Normen: Beispiel Maschinenrichtlinie

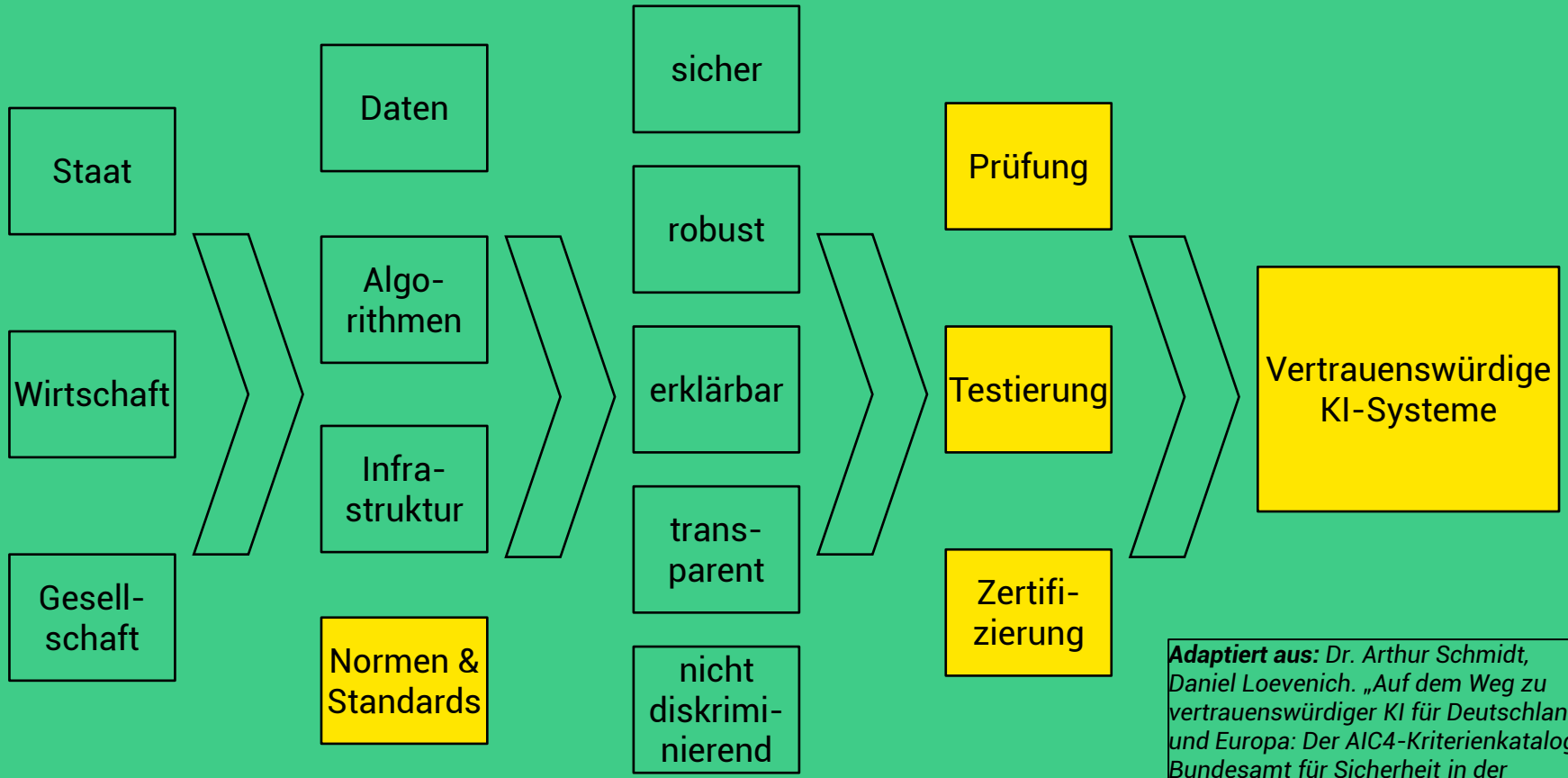
- **Konkretisierung der wesentlichen Anforderungen der Maschinenrichtlinie**: Viele harmonisierte Normen decken nur einen Aspekt bzw. mehrere Aspekte der wesentlichen Anforderungen des Anhangs I der Maschinenrichtlinie 2006/42/EG ab, ganz oder auch nur unvollständig. Harmonisierte Normen haben deshalb formal einen informativen Anhang Z (bzw. ZZ bei CENELEC), in dem meist in Form einer Tabelle angegeben wird, welche Abschnitte der jeweiligen Norm welche wesentlichen Anforderungen der EG-Richtlinie z. B. Anhang I der Maschinenrichtlinie 2006/42/EG erfüllen.
- **Konformitätsvermutung**: Bei Maschinen, die mit harmonisierten Normen oder Teilen davon übereinstimmen wird eine Konformität mit den Anforderungen der Maschinenrichtlinie 2006/42/EG vermutet.

Zertifizierung

- **Zertifizierung:**
  - Sonderform der Konformitätsbewertung (d.h., Überprüfung der Erfüllung bzw. Einhaltung definierter Anforderungen an Produkt, System, Prozess oder Personen).
  - Definition in DIN EN ISO/IEC 17000:2004:

    „Maßnahme durch einen unparteiischen Dritten, die aufzeigt, dass ein angemessenes Vertrauen besteht, dass ein ordnungsgemäß bezeichnetes Erzeugnis, Verfahren oder eine ordnungsgemäß bezeichnete Dienstleistung in Übereinstimmung mit einer bestimmten Norm oder einem bestimmten anderen normativen Dokument ist.“

Von der Technischen Richtlinie zur Konformitätsprüfung/Zertifizierung



Adaptiert aus: *Dr. Arthur Schmidt, Daniel Loevenich. „Auf dem Weg zu vertrauenswürdiger KI für Deutschland und Europa: Der AIC4-Kriterienkatalog. Bundesamt für Sicherheit in der Informationstechnik. 06/07/2021.*

Technische Standards vs. Ethische/Gesellschaftliche Belange

- **Themen der technischen Standardisierung**: Qualitätskriterien, Daten, Good Engineering Practices, Sicherheit (*safety* und/oder security) von KI-Systemen, KI-Systemarchitekturen, KI-spezifische Interoperabilität und Portabilität, terminologische/technologische Grundlagen, etc.
- **Ethische/gesellschaftliche Belange**: Benutzerfreundlichkeit, Inklusivität, Zugänglichkeit (*accessibility*) von KI-Systemen, Nachhaltigkeit von KI-Systemen (z.B. bzgl. UN SDGs), etc.
- **Standardisierung ist häufig stärker auf technische Standardisierung denn auf ethische/gesellschaftliche Fragen fokussiert.**

Technische Herausforderungen der KI-Standardisierung/Zertifizierung

- **Technologie standardisieren während sie entwickelt wird**: KI ist ein aktives F&E-Feld, „technologie-spezifische“ Standardisierung veraltet schnell
- **Verifikation vs. Validierung**: ML-Technologie ist (häufig) statistisch, formale Korrektheitsbeweise sind praktisch nicht verfügbar
- **Cyberphysisches Setup**: KI-Standardisierung/Zertifizierung muss physische und digitale Aspekte abdecken – Organisationen, Prozesse, technische Artefakte, Software,…
- **Testen vs. Monitoring**: Cyberphysische KI-Systeme können sich entlang des Lebenszyklus verändern – punktuelles Testen muss vermutlich durch Monitoring komplementiert werden

Initiativen zur KI-Standardisierung/Normung/Zertifizierung

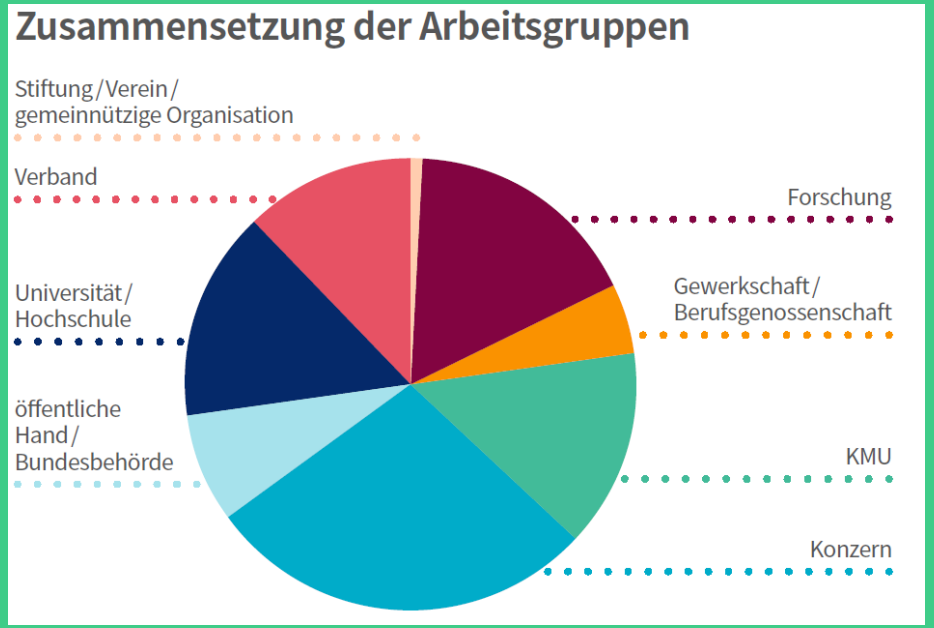
- **Zahlreiche Initiativen auf nationaler Ebene (Auswahl):**
  - Nationale Normungsroadmap KI: Umsetzungsprogramm “Trusted AI" (https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2020/11/20201130-ki-made-in-germany-etablieren.html)
  - KI.NRW Flagship KI-Zertifizierung “made in Germany" (https://www.ki.nrw/flagships/zertifizierung/)
  - Initiativen/Projekte der TIC-Industrie (DEKRA DIGITAL, VdTÜV, etc.)
- **Zahlreiche Initiativen auf europäischer Ebene (Auswahl):**
  - Frankreich: Grand Défi «Sécuriser, certifier et fiabiliser les systèmes fondés sur l'intelligence artificielle» (https://www.gouvernement.fr/grand-defi-securiser-certifier-et-fiabiliser-les-systemes-fondes-sur-l-intelligence-artificielle)
  - EU: Regulation on a European Approach for Artificial Intelligence (https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence)

„Regulation on a European Approach for Artificial Intelligence“

- **EU-weiter regulatorischer Rahmen:**
  - Entwurf am 21.04.2021 veröffentlicht, frühe Fassung bereits vorab “geleakt”.
  - Sieht Konformitätsbewertungen für “high-risk”-KI-Systeme vor, bspw.:
    - Biometrische Systeme im öffentlichen Raum
    - Kritische Infrastruktur
    - Bewerbungs- und Personalmanagement
    - Credit Scoring
  - Neubewertung nach “substantial modification” (bspw. online learning).

Deutsche Normungsroadmap Künstliche Intelligenz

- **Maßnahme zur Umsetzung der KI-Strategie der Bundesregierung**
  - 300 Expert*innen
  - 7 Arbeitsgruppen & Schwerpunktthemen:
    - Grundlagen von KI
    - Ethik / Responsible AI
    - Qualität, Konformitätsbewertung & Zertifizierung
    - IT-Sicherheit bei KI-Systemen
    - Industrielle Automation
    - Mobilität & Logistik
    - KI in der Medizin



Deutsche Normungsroadmap Künstliche Intelligenz

- **Über 70 identifizierte Normungs- und/oder Standardisierungsbedarfe, fünf zentrale Handlungsempfehlungen:**
  - Datenreferenzmodell für die Interoperabilität von KI-Systemen umsetzen
  - Horizontale KI-Basis-Sicherheitsnorm erstellen
  - Praxisgerechte initiale Kritikalitätsprüfung von KI-Systemen ausgestalten
  - Nationales Umsetzungsprogramm “Trusted AI” zur Ertüchtigung der europäischen Qualitätsinfrastruktur initiieren/durchführen
  - Use Cases auf Normungsbedarf analysieren

Siehe auch: https://www.din.de/de/forschung-und-innovation/themen/kuenstliche-intelligenz/fahrplan-festlegen

Koordinierungsgruppe „KI-Normung und Konformität“

- **Nachfolgegremium zur Steuerungsgruppe der Normungsroadmap:**
  - Initiative des BMWi, BMAS, und BMBF
  - Vertreter*innen aus Wirtschaft, Politik, Wissenschaft und Zivilgesellschaft
  - Praktischen Umsetzung der Empfehlungen aus der Normungsroadmap
  - Unter anderem “Nationales Umsetzungs-programm Trusted AI” (BSI & BfDI):
    “*Basis für reproduzierbare und standardisierte Prüfverfahren leg[en], mit denen Eigenschaften von KI-Systemen wie Verlässlichkeit, Robustheit, Leistungsfähigkeit und funktionale Sicherheit geprüft und Aussagen über die Vertrauenswürdigkeit getroffen werden können.*“
    (Quelle: https://bit.ly/3gjdDY6)

Zusammenfassung

- **Take Home Message:**
  - KI findet Eingang in mehr und mehr Bereiche des täglichen (Arbeits-)Lebens
  - KI ist kein Selbstläufer, sondern benötigt Regulierung, Testung und Zertifizierung
  - Normung und Standardisierung haben strategische Bedeutung für KI-Regulierung im EU-Raum
  - Normungsroadmap KI zeichnet wahrscheinliche KI-Normungs-/ Standardisierungsbedarfe und -vorhaben der kommenden Jahre vor

Let's innovate safety together, byte by byte:

Dr. Tarek R. Besold
DEKRA DIGITAL
tarek.besold@dekra.com