KI-FACHKONFERENZ

Artificial Intelligence Act

Industrie 4.0 und Industrielle Automation

Jürgen Heiles

Frankfurt,
22.11.2021

Ziele des Workshops

Erstellung einer Übersicht für die Themenkomplexe:

- Welche Normen gibt es bereits in dem Bereich, die als mögliche harmonisierte Norm vorgeschlagen werden könnten?
- Welche Normen befinden sich in dem Bereich derzeit im Entwicklungsprozess, die als mögliche harmonisierte Norm vorgeschlagen werden könnten?
- Welche harmonisierten Normen müssen in diesem Bereich entwickelt werden, um die Anforderungen zukünftig erfüllbar zu machen?

Agenda

- Einführung in den Vorschlag zur Regulierung von AI in der EU mit dem Fokus auf High-Risk AI Anwendungen
- Zusammenhang zwischen AI und Maschinen Regulierung
- Übersicht zu relevanten Standardisierungsaktivitäten
- Sammlung von Themen für harmonisierte Normen für die EU AI Regulierung

Zur Beantwortung der im Workshop gestellten Fragen gehen sie bitte zu https://pingo.coactum.de/422101 oder scannen sie den QR Code

Frage 1 – Wie gut kennen sie den Vorschlag für eine Regulierung von AI in der EU?

- Ich habe mich schon detailliert mit der Vorschlag für eine AI Regulierung in der EU beschäftigt
- Ich kenne den Vorschlag für eine AI Regulierung in der EU, habe mich aber damit noch nicht detailliert beschäftigt
- Ich kenne den Vorschlag für eine AI Regulierung in der EU nicht

Nur eine Antwort möglich!

Zur Beantwortung der im Workshop gestellten Fragen gehen sie bitte zu https://pingo.coactum.de/422101 oder scannen sie den QR Code

Antworten zur Frage 1

Wie gut kennen sie den Vorschlag für eine Regulierung von AI in der EU?

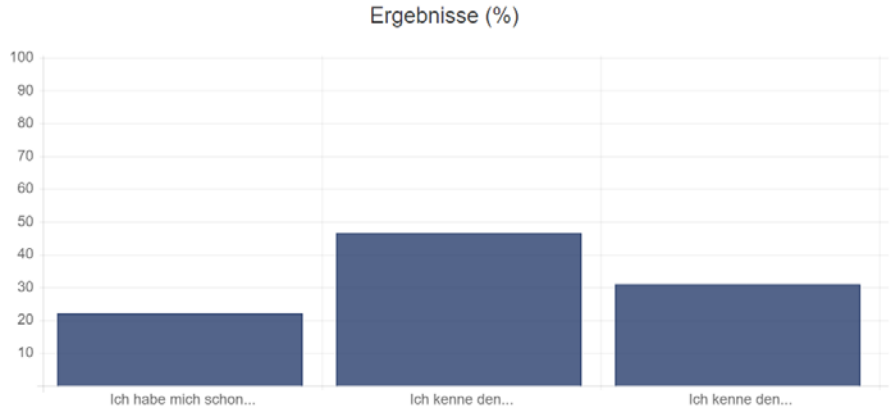
Teilnehmer: **45**

Antwortmöglichkeiten:

10 22% Ich habe mich schon detailliert mit der Vorschlag für eine AI Regulierung in der EU beschäftigt

21 47% Ich kenne den Vorschlag für eine AI Regulierung in der EU, habe mich aber damit noch nicht detailliert beschäftigt

14 31% Ich kenne den Vorschlag für eine AI Regulierung in der EU nicht



Frage 2 – Sind sie bei relevanten Standardisierungsaktivitäten beteiligt?

- Ich beteilige mich an AI Standardisierungsaktivitäten
- Ich beteilige mich an Industrial Automation/I4.0 Standardisierungsaktivitäten
- Ich beteilige mich an anderen Standardisierungsaktivitäten
- Ich beteilige mich nicht an Standardisierungsaktivitäten

Mehrere Antworten möglich!

Zur Beantwortung der im Workshop gestellten Fragen gehen sie bitte zu https://pingo.coactum.de/422101 oder scannen sie den QR Code

Antworten zur Frage 2

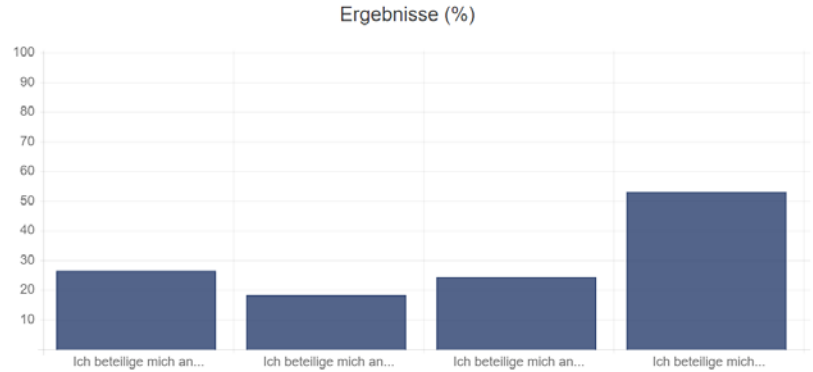
Sind sie bei relevanten Standardisierungsaktivitäten beteiligt?

Dies ist eine Multiple-Choice-Umfrage.

Teilnehmer: **49**

Antwortmöglichkeiten:

- 13 27% Ich beteilige mich an AI Standardisierungsaktivitäten
- 9 18% Ich beteilige mich an Industrial Automation/I4.0 Standardisierungsaktivitäten
- 12 24% Ich beteilige mich an anderen Standardisierungsaktivitäten
- 26 53% Ich beteilige mich nicht an Standardisierungsaktivitäten



EU AI and Machinery regulation

Disclaimer:
Both regulations are proposals and under consideration by the European Parliament and Council. Various aspects are under discussion and may change until final approval .

EU AI regulation COM(2021) 206 and Machinery regulation COM(2021) 202 proposals jointly published on April 21st 2021. The latter shall replace the existing Machinery Directive and considers AI with a reference to the former.

Principal policy Objectives

- Ensure that **AI systems on EU market are safe and respect EU laws and values**
- **Create legal certainty** to facilitate investment and innovation in AI
- **Enhance the governance and enforcement** of existing legal requirements
- Facilitate the development of a single market for **safe, lawful and ethical AI applications**

The regulation covers in addition to placing products onto the market also the use of AI systems

The regulations are now handled by the European Parliament and Council.
Approval of both is expected in Q3/2022. **They should to come into force 24 to 48 month later.**

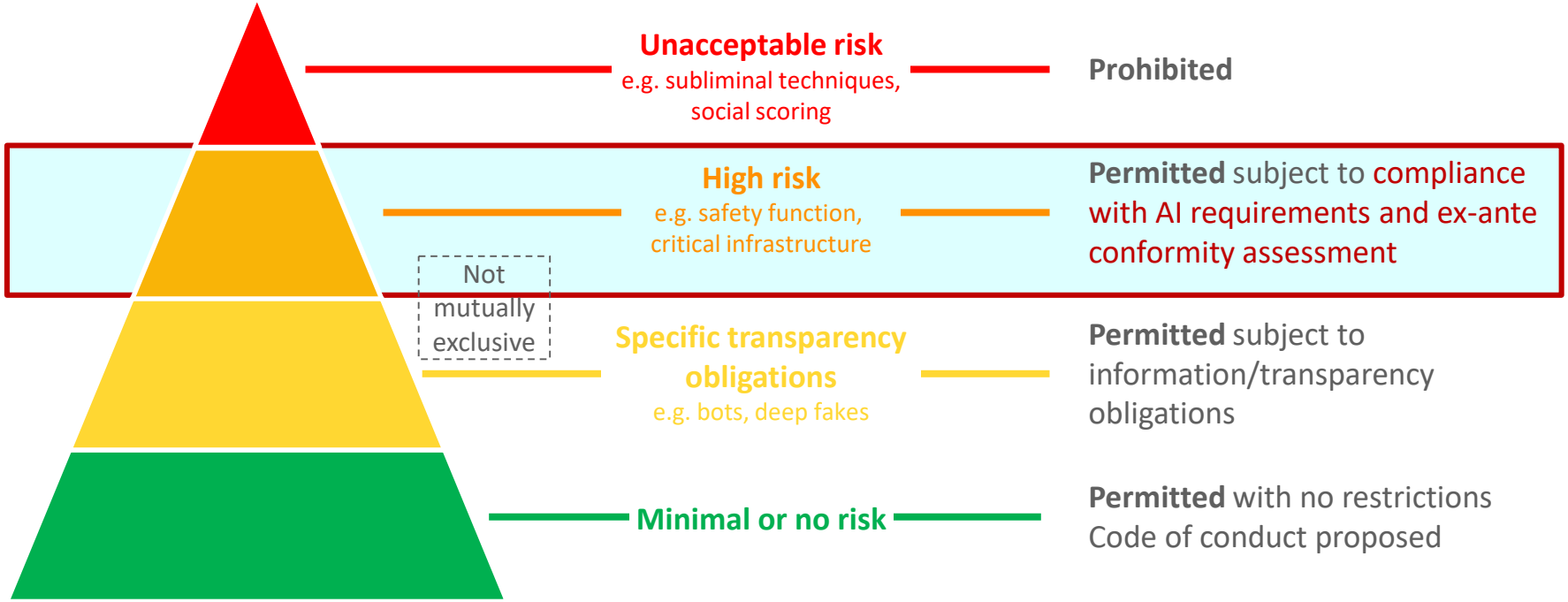
AI definition (from the AI regulation)

Software that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with, and that is developed with one or more of the following techniques and approaches:

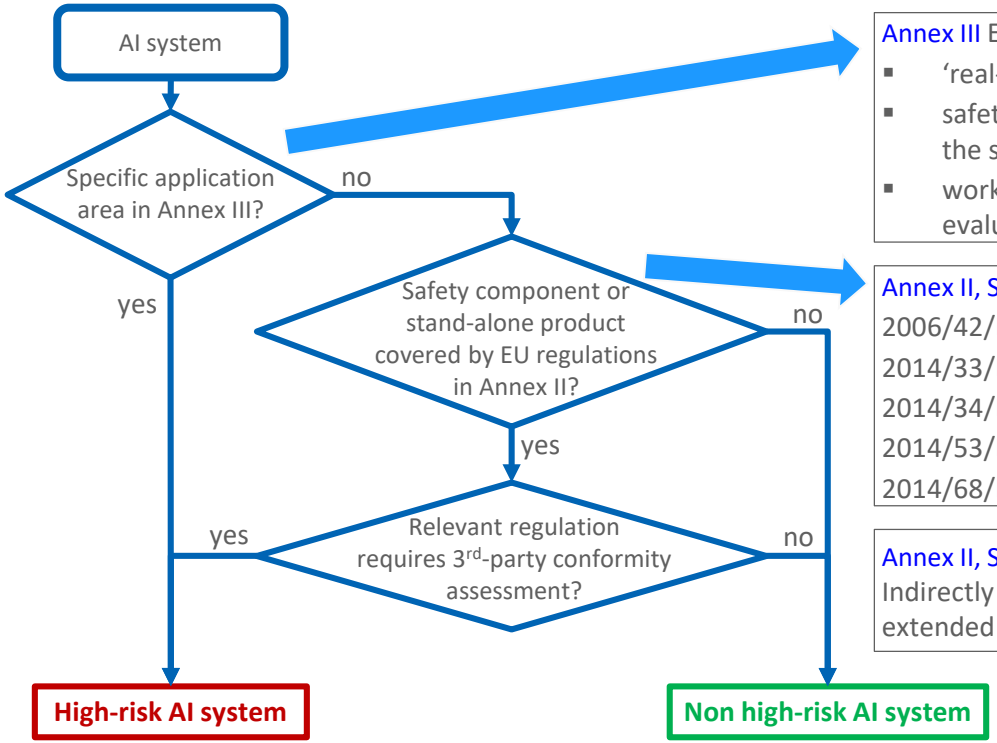
- ❑ Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- ❑ Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- ❑ Statistical approaches, Bayesian estimation, search and optimization methods..

This definition has received a lot of comments that state that it is too broad and would include various traditional software solutions like PLC programs which are already sufficiently cover by existing regulation.

Risk-based approach of AI regulation



High-risk AI Systems



Annex III Examples

- 'real-time' and 'post' remote biometric identification of natural persons
- safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity
- workforce management (e.g. recruitment, promotion, performance evaluation, termination)

Annex II, Section A (NLF based) Examples

2006/42/EC	Machinery
2014/33/EU	Lifts
2014/34/EU	ATEX
2014/53/EU	Radio equipment
2014/68/EU	Pressure equipment

The proposed new Machinery Regulation adds Software, including AI, ensuring safety functions and Machinery embedding AI systems ensuring safety functions to the list of high-risk machinery products

Annex II, Section B (e.g. motor vehicles, railway, aviation)
Indirectly affected by the AI regulation as these regulations will be extended to cover the requirements of this regulation for AI systems

High-risk AI Systems - Requirements

Establish and implement **risk management system** in light of the **intended purpose** of the AI system

- Use high-quality **training, validation and testing data** (relevant, representative, …)
- Draw up **technical documentation** & setup **logging capabilities** (traceability & auditability)
- Ensure appropriate degree of **transparency** and provide users with **information** on capabilities and limitations of the system & how to use it
- Ensure **human oversight** (measures built into the system and/or implemented by the users)
- Ensure **robustness**, **accuracy** and **cybersecurity**

High-risk AI Systems – Providing conformity

High-risk AI systems which are in conformity **with harmonized standards** (or common specifications) shall be **presumed to be in conformity** with the **high-risk AI requirements**.

For high-risk AI systems that fall under a legislation in **Annex II, section A (e.g. machinery directive)** , conformity assessment shall part of the assessment according to that legislation.
The high-risk AI requirements shall be part of that assessment
-> no dedicated high-risk AI conformity assessment, but integrated into existing assessment

High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified.
For high-risk AI systems that **continue to learn** after being placed on the market, changes to the high-risk AI system and its performance that have been **pre-determined** by the provider at the moment of the **initial conformity assessment** and are **part of** the information contained in the **technical documentation**, are **not substantial modifications**.

Frage 3 – Ist die AI Regulierung relevant für ihr Geschäft oder Arbeitsgebiet?

- Ja
- Eventuell, es ist aber noch eine genauere Analyse notwendig
- Nein

Nur eine Antwort möglich!

Zur Beantwortung der im Workshop gestellten Fragen gehen sie bitte zu https://pingo.coactum.de/422101 oder scannen sie den QR Code

Antworten zur Frage 3

Ist die AI Regulierung relevant für ihr Geschäft oder Arbeitsgebiet?

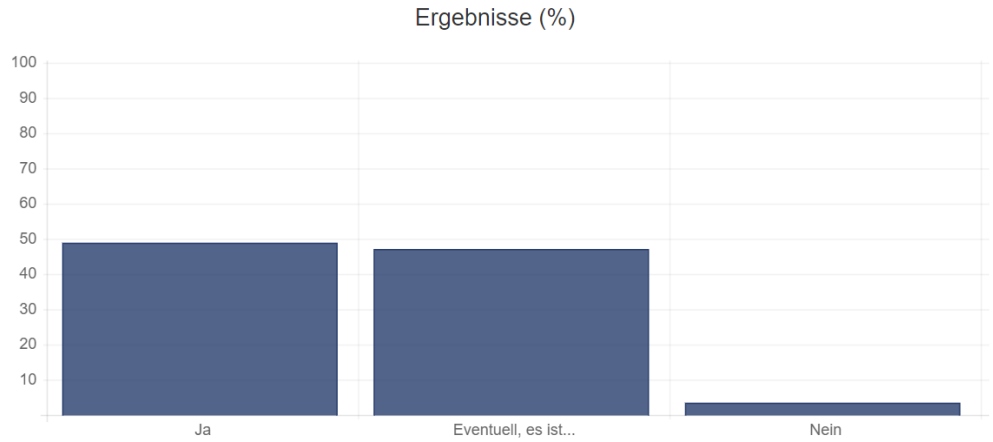
Teilnehmer: **55**

Antwortmöglichkeiten:

27 49% Ja

26 47% Eventuell, es ist aber noch eine genauere Analyse notwendig

2 4% Nein



Frage 4 – Gibt es in ihrem Arbeitsgebiet AI Use Cases, die in die High-Risk Kategorie fallen?

- Ja, einige
- Ja, wenige
- Nein

Nur eine Antwort möglich!

Zur Beantwortung der im Workshop gestellten Fragen gehen sie bitte zu https://pingo.coactum.de/422101 oder scannen sie den QR Code

Antworten zur Frage 4

Gibt es in ihrem Arbeitsgebiet AI Use Cases, die in die High-Risk Kategorie fallen?

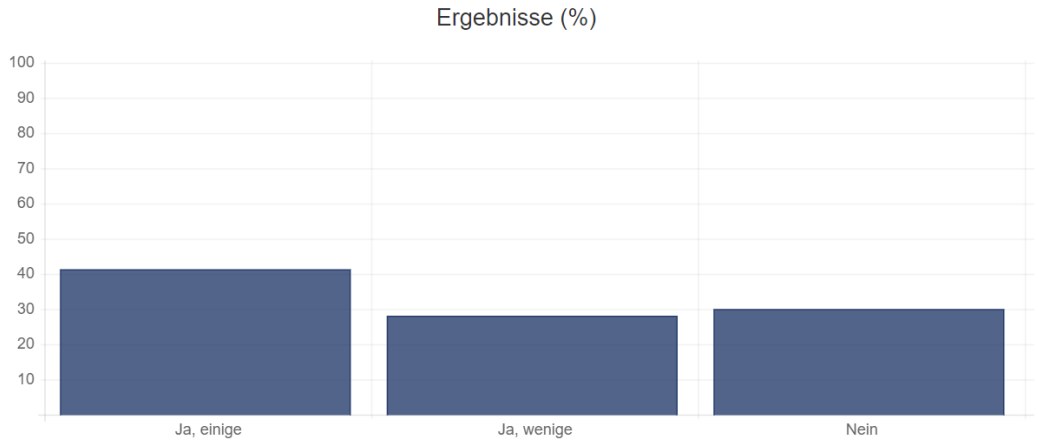
Teilnehmer: **53**

Antwortmöglichkeiten:

22 42% Ja, einige

15 28% Ja, wenige

16 30% Nein



Machinery Directive – Harmonized Standards

Ergänzung aus Workshop:
ISO 13849 Safety of machinery –
Safety-related parts of control systems

Type-A – Basic safety standards

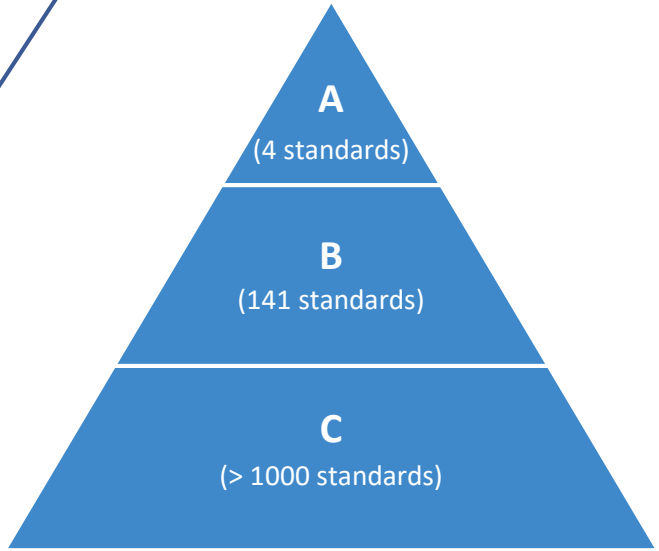
giving basic concepts, principles for design, and general aspects that can be applied to machinery
i.e. EN ISO 12100: Safety of machinery — General principles for design — Risk assessment and risk reduction

Type-B – Generic safety standards

dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery
i.e. EN (IEC) 62061: Safety of machinery - Functional safety of safety-related control systems*

Type-C – Machine safety standards

dealing with detailed safety requirements for a particular machine or group of machines
(e.g. machine tools, cranes, food processing, garden equipment)

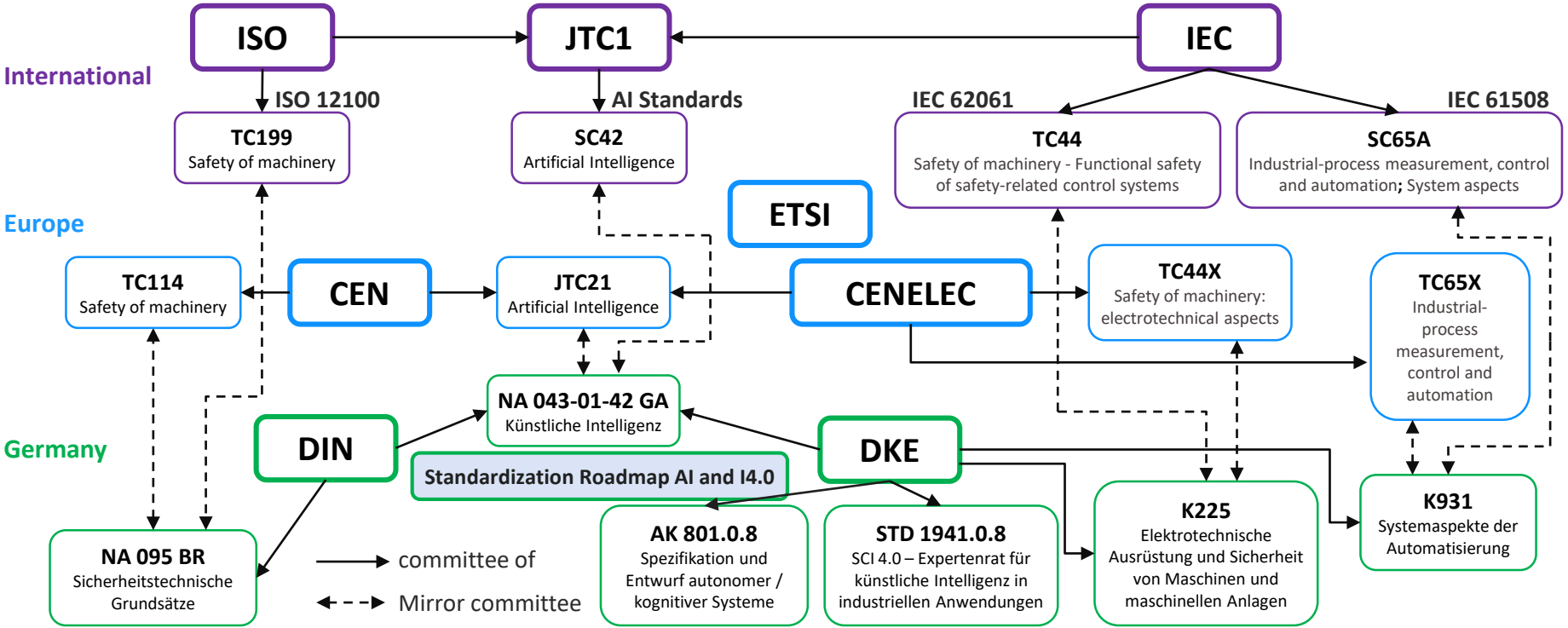


On the Machinery Directive website of the European Commission a summary list of all harmonized standards is available.
Note, that formally the summary list does not provide legal effect; only the publications in the Official Journal and the Commission Implementing Decisions themselves are legally binding

*based on IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

Relevant standardization bodies for harmonized standards

This figure is not complete, for specific topics like security also other committees are involved. In addition also other bodies like IEEE and ITU work on AI standards



AI Standards in ISO/IEC JTC1 SC42 with relation to the EU AI regulation

ISO/IEC has some approved documents and many ongoing work items that have some relation to the EU AI regulation. Only some are listed below. Detailed analysis is required how far they fit to the regulation requirements.

General:

- ISO/IEC 22989 Artificial Intelligence Concepts and Terminology

Risk management:

- ISO/IEC 23894 AI Risk management

Data Quality:

- ISO/IEC IS 5259 series Data quality for analytics and machine learning (ML)

Transparency:

- ISO/IEC TS 6254 Objectives and approaches for explainability of ML models and AI systems
- New work item proposed Transparency taxonomy of AI systems

Human oversight:

- ISO/IEC TS 8200 Controllability of automated artificial intelligence systems

Robustness, accuracy and cybersecurity:

- ISO/IEC 24029 series Assessment of the Robustness of Neural Networks
- ISO/IEC TS 4213 Assessment of machine learning classification performance
- New work item proposal on Bias mitigation

Quality management:

- ISO/IEC 42001 AI management system

Functional safety:

- ISO/IEC TR 5469 Functional Safety and AI systems

In cooperation with IEC SC65A

See the AI Watch: AI Standardisation Landscape report from the JRC of the European Commission for a detailed overview and analysis.

Other related standardization activities

Ergänzung aus Workshop:
IEC 62998-3 „Safety of Machinery - Safety-related sensors used for the protection of persons Part 3: Sensor technologies and algorithms" beschäftigt sich ebenfalls mit den Anforderungen an AI für Sensorik

Safety of machinery and AI:

- ISO TC199:
  ISO TR 22100-5 Safety of machinery — Relationship with ISO 12100 — Part 5: Implications of artificial intelligence machine learning

Functional safety and AI:

- IEC SC65A is considering AI in the context of functional safety of electrical and electronic control systems (IEC 61508)

Automotive safety and AI:

- ISO TC22 SC32:
  ISO 21448 Road vehicles — Safety of the intended functionality

Security/Privacy and AI:

- ISO/IEC JTC1 SC27:
  new work items on AI and security and privacy
- ETSI ISG SAI Industry Specification Group Securing AI

Conformity Assessment:

- CEN/CENELEC JTC21 AHG 2 Conformity Assessment

Development of Autonomous Systems:

- DKE AK 801.0.8 Spezifikation und Entwurf autonomer / kognitiver Systeme

Analysis of relevant standards for the EU AI Regulation:

- ISO/IEC JTC1 SC42
- CEN/CENELEC JTC21 WG1
- DIN/DKE

Bitte schreiben sie Standardisierungsaktivitäten, die sie als relevant ansehen und die hier nicht aufgelistet sind, in den Chat!

Frage 5 – Welche Themen sind für harmonisierte Standards für die EU AI Regulierung relevant?

Offen Frage, sie können mehrere Themen angeben!

Zur Beantwortung der im Workshop gestellten Fragen gehen sie bitte zu https://pingo.coactum.de/422101 oder scannen sie den QR Code

Antworten zur Frage 5

Welche Themen sind für harmonisierte Standards für die EU AI Regulierung relevant?

Dies ist eine Freitext-Frage.

Teilnehmer: **4**

Ansicht ändern

Themen aus dem Chat:
- Vorgehensmodell beim Einsatz von KI in technischen Systemen
- KI-Building Blocks
- Selbstbeschreibungen von KI Datenprodukten
- Schädigungspotential
- Erklärbarkeit

Antwort	Häufigkeit
Schnittstellendefinition bei feldüberwachung	1
Validierung von ai-systemen	1
Predictive maintenance	1
Safety	1

Frage 6 – Möchten sie sich an der Erstellung von harmonisierten Standards für die EU AI Regulierung beteiligen?

- Ja, ich bin schon an der AI Standardisierung beteiligt
- Ja, ich bin bisher noch nicht an der AI Standardisierung beteiligt
- Nein, das Thema ist für mich relevant aber ich habe nicht die Ressourcen für eine Mitarbeit
- Nein, das Thema ist für mich nicht relevant

Nur eine Antwort möglich!

Zur Beantwortung der im Workshop gestellten Fragen gehen sie bitte zu https://pingo.coactum.de/422101 oder scannen sie den QR Code

Mitarbeit in relevanten Standardisierungsaktivitäten in Deutschland

Eine Mitarbeit bei ISO, IEC, CEN and CENELEC erfordert eine Mitarbeit in den jeweiligen deutschen Spiegelgremien bei DIN und DKE

DIN/DKE Deutsche Normungsroadmap Künstliche Intelligenz
Die Arbeiten an Version 2 werden Anfang 2022 gestartet
Kontakt: Filiz Elmas, DIN; filiz.elmas@din.de

DIN/DKE NA 043-01-42 GA Künstliche Intelligenz
Spiegelgremium von ISO/IEC JTC1 SC42 und CEN/CENELEC JTC21
Kontakt: Katharina Sehnert, DIN; Katharina.sehnert@din.de

DKE STD 1941.0.8 SCI 4.0 – Expertenrat für künstliche Intelligenz in industriellen Anwendungen
UAG Sichere, vertrauenswürdige KI
Trägt zu den Normungsroadmaps KI und I4.0 bei
Kontakt: Yves Leboucher, DKE; yves.leboucher@vde.com

DKE K931 Systemaspekte der Automatisierung
Spiegelgremium von IEC SC65A und CENELEC TC65X
Kontakt: Dr. Jens Gayko, DKE; jens.gayko@vde.com

DKE K225 Elektrotechnische Ausrüstung und Sicherheit von Maschinen und maschinellen Anlagen
Spiegelgremium von IEC TC44 und CENELEC TC44X
Kontakt: Peter Täubl, DKE; peter.taeubl@vde.com

DKE AK 801.0.8 Spezifikation und Entwurf autonomer / kognitiver Systeme
Kontakt: Johannes Koch, DKE; johannes.koch@vde.com

DIN NA 095 Sicherheit von Maschinen und Geräten
Spiegelgremium von ISO TC199 und CEN TC114
Kontakt: Reiner Hager, DIN; reiner.hager@din.de

Relevanter Chatverlauf des Workshops mit nachträglichen Antworten I

Zum Testen benötigt es Anforderungen - ansonsten ist es "Ausprobieren": wie werden Anforderungen an ein AI System abgebildet?

➔ Anforderungen sollten in Standards definiert werden. Teilweise entstehen dies schon z.B. in ISO/IEC JTC1 SC42. Teileweise gibt es aber aus meiner Sicht auch noch Forschungsbedarf.

Wie soll eine Aufnahme zur Nachverfolgbarkeit sichergestellt werden? Welcher detailierungsgrad ist notwendig? (Stichwort "Vorratsdatenspeicherung")

➔ Das ist noch offen. In einigen Anwendungsbereichen wie im Eisenbahnbereich gibt es schon Anforderungen zur Datenaufzeichnung (Juridical Recording) Das könnte man sich anschauen zur Erstellung von Standards. Je nach Anwendung können sich daraus auch Konflikte bzw. spezifisch Anforderungen bzgl. Privacy ergeben.

Jetzt sind wir erst am Anfang der Normierung, wie können jetzt schon Produkte auf dem Markt gebracht werden, die auch zukünftig die Anforderungen erfüllen? Was ist notwendig?

Momentan kann man High Risk noch gar nicht in Verkehr bringen, da keiner sagt wie die Validierung konkret aussehen soll.

➔ Ja, unabhängig von der AI Regulierung müssen ja heute schon die Anforderungen der Maschinen Direktive eingehalten werden. Da AI in den Harmonized Standards nicht berücksichtigt wird ist eine Nachweisführung basierend auf diesen Standards nicht möglich. Es ist auch eine Nachweisführung ohne Standards möglich, diese muss aber von einer anerkannten Drittstelle abgenommen werden.

Sicherheitskritische KI benötigt meines Erachtens auch zuverlässige Hardware (bspw. GPU oder FPGA), welche diese ausführt. Gibt es hierzu auch Regulierungsansätze?

➔ Die Regulierung ob für AI oder die Maschinen Direktive beziehen sich immer auf das gesamte Produkt/System. Dies beinhaltet auch die Hardware und Hardware Aspekte wie Ausfallrate müssen bei den Sicherheitsbetrachtungen mit einbezogen werden. Standards wie IEC 61508 und IEC 62061 behandelt Hardware and Software Safety Aspekte.

Relevanter Chatverlauf des Workshops mit nachträglichen Antworten II

Wie sind Robustness und Accuracy spezifiziert? Für beide existieren doch sehr viele Arten von Metriken und nur Spezifizierung und Quantifizierung dieser Metriken kann der Anforderung einen Sinn verleihen.

➔ **Zum Thema Robustness gibt es den veröffentlichten Technical Report ISO/IEC 24029-2 „Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 1: Overview" der generelle Aspekte betrachtet. Ein Technical Specification ISO/IEC 24029-2 "Artificial Intelligence – Assessment of the robustness of neural networks – Part 2: Methodology for the use of formal methods" ist im entstehen. Das heist aber nicht, das das Thema gelöst ist.**

Bei Safety ist die 61508 relevant oder soll mal wieder ein neuer Standard definiert werden?

Die IEC 61508 ist und bleibt relevant für FuSI sagt aber sagt nichts zu AI und wird dies vermutlich nicht in der kommenden Edition 3 machen. Dazu müssen neue Standards generiert werden.

➔ **Es könnte ein eigener Standard zu Funktionaler Sicherheit und AI entstehen oder eine Erweiterung der IEC 61508. Momentan wird an einem Technical Report. Momentan entsteht der Technical Report ISO/IEC TR 5469 "Artificial intelligence — Functional safety and AI systems" der den aktuellen Stand der Problematik betrachtet. Im Automotive Bereich gibt es Aktivitäten wie ISO 21448 "Road vehicles — Safety of the intended functionality"**

Wie offen zugänglich sind diese Standard Entwürfe?

➔ **Für alle diese Projekte gibt es im Rahmen der Erarbeitung eine öffentliche Entwurfskommentierung über die nationalen Normungsorganisationen DIN & DKE. In diesem Zeitraum können Sie die Entwürfe in unserem Normentwurfsportal einsehen und Kommentare einreichen. Diese werden dann im nationalen Spiegelgremium besprochen und ggf. international eingebracht.**

➔ **Den besten Zugriff und Einfluss hat man wenn man in dem relevanten Standardisierungsgremium (über das deutsche Spiegelgremium) mitarbeitet.**

Die Berufsgenossenschaften und DGUV, als Spitzenverband erarbeiten gerade diverse Stellungsnahmen und Grundlagen zu Automatisiert fahrende Fahrzeuge in betrieblichen Bereichen und Bedienungs-Assistenzsystemen.

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:

Jürgen Heiles
Siemens AG

Tel.: +49 173 7151668
E-Mail: juergen.heiles@siemens.com