

*KI IN KRITIS
WHITE-PAPER-SERIE
KÜNSTLICHE INTELLIGENZ IN
KRITIS-UNTERNEHMEN*

TEIL 1 – EINFÜHRUNG

Kompetenzzentrum Kritische Infrastrukturen e.V.



KKI

KOMPETENZZENTRUM
KRITISCHE
INFRASTRUKTUREN E. V.

INHALT

1. Einführung	3
2. Theoretischer und regulatorischer Rahmen	4
2.1 Theoretischer Rahmen	4
2.2 Einsatz von KI im KRITIS-Sektor	6
2.3 KI im Kontext europäischer Regulierung – KI-Verordnung (AI Act)	7
2.4 Harmonisierte europäische KI-Standards zur KI-Verordnung	8
2.5 Weiteres gesetzliches und normatives Umfeld zur KI-VO	8
3. Herausforderungen von KI in kritischen Infrastrukturen	9
3.1 Beispiele für Kernprozesse der kritischen Infrastruktur	10
3.2 Herausforderungen für die Integration in bestehende Systeme	10
3.2.1 Skalierbarkeit und Leistung	10
3.2.2 Vertrauenswürdigkeit und Fehleranfälligkeit	10
3.2.3 Bias und ethische Herausforderungen	10
3.2.4 Sicherheitsrisiken und Datenschutz beachten	11
3.2.5 Kosten und Ressourcen planen	11
3.2.6 Veränderung der Unternehmenskultur organisieren	11
3.2.7 Langfristige Auswirkungen auf Geschäftsmodelle	11
3.3 Zusammenfassung	11
4. Anhang	12
Rollen gemäß KI-VO Artikel 3	12
Teilnehmende / Anmerkungen	12
Glossar	13
Literaturverzeichnis	14

1. EINFÜHRUNG

Die rasante Entwicklung der Künstlichen Intelligenz (KI) macht ihren Einsatz in Unternehmen der kritischen Infrastruktur unvermeidlich. Während KI früher in Software eingebettet war und durch feste Rahmenbedingungen reguliert wurde, nutzen Menschen heute generative KI-Modelle wie ChatGPT direkt. Diese direkte Interaktion verändert die Kontrolle über KI-Systeme grundlegend und birgt neue Herausforderungen für Sicherheit und Governance.

Gerade in kritischen Infrastrukturen führt der Einsatz von KI zu komplexen sicherheitstechnischen Fragen: Wie lässt sich verhindern, dass KI-Systeme fehlerhafte oder manipulierbare Entscheidungen treffen? Wie können Angriffe durch adversarielle Methoden oder Datenmanipulation erkannt und abgewehrt werden? Und wie lässt es sich sicherstellen, dass die Hoheit über sicherheitsrelevante Prozesse bei menschlichen Entscheidungsträgern verbleibt? Neben diesen technischen Herausforderungen fordert die KI-Verordnung einen verantwortungsvollen Umgang mit KI, insbesondere hinsichtlich Sicherheit, Gesundheit und Grundrechten. Dies umfasst auch den Schutz personenbezogener Daten gemäß der Datenschutz-Grundverordnung (DSGVO). Institutionen der kritischen Infrastruktur müssen daher nicht nur die Potenziale von KI nutzen, sondern auch robuste Strategien für Governance, Risikomanagement und Sicherheitsmechanismen entwickeln, um ihre Systeme

und damit die Gesellschaft vor unbeabsichtigten oder missbräuchlichen KI-Einflüssen zu schützen.

In Abbildung 1 wird ein Überblick über die zu berücksichtigenden Themenbereiche für mögliche Einsatzbereiche von KI in kritischen Infrastrukturen gegeben. Dies soll helfen, den KI-Einsatz in kritischen Infrastrukturen systematisch zu analysieren, Richtlinien zum Umgang mit KI-Systemen zu entwickeln und sicherheitsrelevante Herausforderungen frühzeitig zu adressieren.

In der White-Paper-Serie des KKI e. V. findet keine umfassende Betrachtung aller mit KI verbundenen Herausforderungen und Vorschriften statt. Vielmehr wird der Schwerpunkt auf die spezifischen Aspekte des KI-Einsatzes im Rahmen kritischer Infrastrukturen gelegt.

Die Entscheidung über den Einsatz von KI-Systemen oder die Freigabe der Nutzung von unspezifischen KI-Funktionen wie natürliche Sprachverarbeitung oder generische KI-Chatbots muss stärker unter der Betrachtung einer Risiko-Nutzen-Abwägung erfolgen als der bei Software sonst oft dominanten Kosten-Nutzen-Abwägung. Die unterschiedlichen Themenbereiche werden im Rahmen dieser Schriftreihe jeweils in einem eigenen White Paper behandelt und im Folgenden kurz vorgestellt:



Abbildung 1: Überblick White-Paper-Serie KI in KRITIS-Unternehmen, Prof. Thimm, DFKI, Feb. 2025

► Awareness

Für die Bewertung des Nutzens und Risikos sowie die Entscheidung über den Einsatz von KI in der kritischen Infrastruktur ist es notwendig, ein Bewusstsein (Awareness) für die Risiken, die mit den unterschiedlichen Möglichkeiten der KI verbunden sind, zu schaffen. Institutionen der kritischen Infrastruktur müssen verstehen, welche Potenziale, aber auch welche Risiken mit KI verbunden sind. Dies umfasst insbesondere sicherheitskritische Aspekte und die Notwendigkeit eines kontrollierten Einsatzes.

► Operative Anwendungen

Hier werden konkrete Anwendungsfälle von KI betrachtet, die sich mit operativen Anwendungen wie Leitstellen, Lagebilder, Gebäudeautomatisierung und Videoüberwachung befassen. Diese Systeme unterstützen Entscheidungsprozesse und Sicherheitsmechanismen, sind jedoch zugleich potenzielle Angriffsziele und erfordern eine robuste Absicherung.

► Technische Automatisierung & Entscheidungsunterstützung

Diese Themen beinhalten fortgeschrittene KI-Anwendungen wie Decision Support, Robotic Process Automation (RPA) und autonome Agenten. Diese Technologien ermöglichen eine höhere Automatisierung und Effizienz, erfordern jedoch klare Governance-Strukturen, um unbeabsichtigte oder missbräuchliche Nutzung zu verhindern.

► Governance & Management der KI

Als Querschnittsfunktion sind die Governance und das Management von KI zu betrachten. Innerhalb der Institutionen müssen Rahmenempfehlungen, Vorschriften, Prozesse, Kennzahlen und rechtliche Rahmenbedingungen für den KI-Einsatz entwickelt werden.

Ziel der KI-Verordnung:

Verantwortungsvoller Umgang mit KI im Sinne der KI-Verordnung und dem darin geforderten Schutz der Sicherheit, Gesundheit und Grundrechte inklusive des Schutzes der personenbezogenen Daten aus der DSGVO.

2. THEORETISCHER UND REGULATORISCHER RAHMEN

2.1 Theoretischer Rahmen

Künstliche Intelligenz

Künstliche Intelligenz bezeichnet die Fähigkeit von Anwendungen, menschenähnliche Intelligenzleistungen zu erbringen – wie z. B. Lernen, Problemlösen, Sprachverstehen, Planen oder sogar Kreativität. Dabei werden Algorithmen, insbesondere aus dem Bereich des Maschinellen Lernens, eingesetzt, um Muster in Daten zu erkennen und daraus Entscheidungen oder Vorhersagen abzuleiten.

KI-Systeme funktionieren im Kern durch das Training mit großen Datenmengen. Modelle – häufig sogenannte neuronale Netzwerke – analysieren diese Daten, um Regeln oder Zusammenhänge zu erkennen. Aktuelle KIs, wie ChatGPT oder Bildgeneratoren, beruhen auf sogenannten tiefen neuronalen Netzwerken (Deep Learning), die beson-

ders leistungsfähig im Erkennen komplexer Muster sind. Der aktuelle Stand der Technik ermöglicht Anwendungen wie Sprachassistenten, medizinische Diagnostik, autonome Fahrzeuge oder kreative Werkzeuge in Kunst und Design.

Zukünftig wird KI nicht nur präziser und schneller, sondern auch vielseitiger – mit Fortschritten in Richtung „Allgemeiner KI“ (General Purpose Artificial Intelligence), die flexibler „denken“ und sich besser an neue Situationen anpassen kann. Dabei werden auch ethische und gesellschaftliche Fragen eine entscheidende Rolle spielen, etwa beim Umgang mit Verantwortung, Datenschutz und Kontrolle. Eine Herausforderung besteht beispielsweise darin, die für das Training verwendete Datenmenge daraufhin zu prüfen und ggf. anzupassen, dass sie Sachverhalte repräsentativ und frei von ungewollter Diskriminierung aufzeigt.

Definition eines KI-System (OECD)

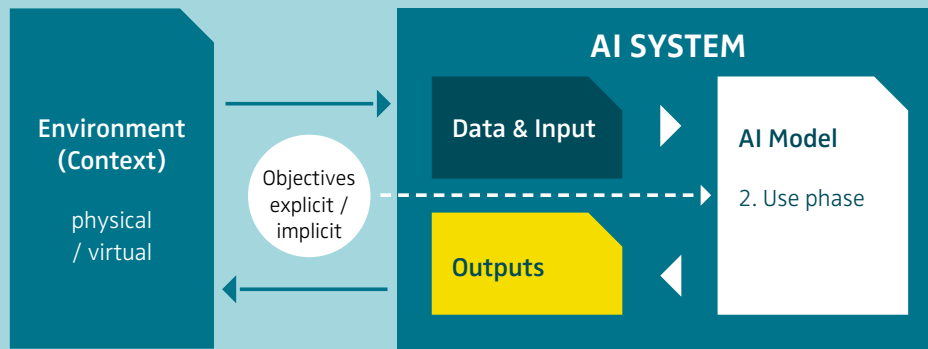


Abbildung 2: OECD AI system model (use phase) (Quelle: OECD)

Definition eines KI-Systems (KI-VO Artikel 3)

Ein KI-System ist ein maschinengestütztes System, das für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und aus den erhaltenen Eingaben explizite oder implizite Ziele ableitet, auf welche Weise Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

„An AI system is a machine-based system, that

- ▶ for explicit or implicit objectives
- ▶ infers, from the input it receives,
- ▶ how to generate outputs such as predictions, content, recommendations, or decisions
- ▶ that (can) influence physical or virtual environments.

Different AI systems vary in their levels of autonomy and adaptiveness after deployment.“

(Quelle: OECD)

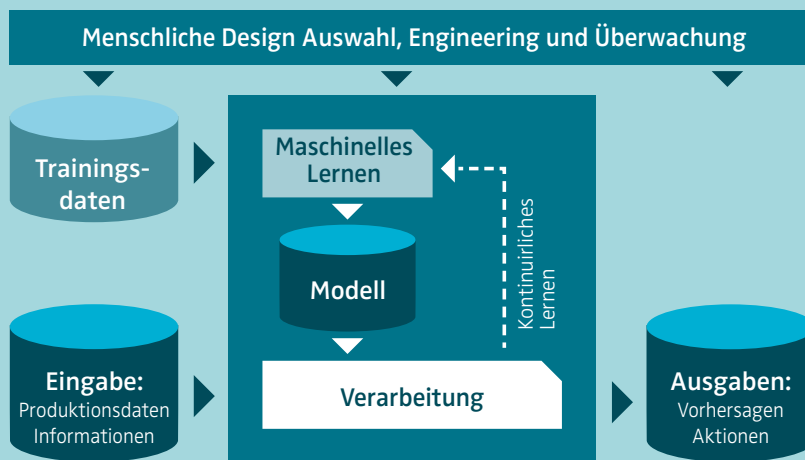


Abbildung 3: Darstellung basierend auf der Definition eines AI-Systems der ISO/IEC 22989 und der Definition der KI-VO eines AI-Systems als Produkt (Quelle: ISO/IEC)

Unterschiedliche Fähigkeiten von Künstlicher Intelligenz

Für Künstliche Intelligenz kann eine Unterscheidung in wissensbasierte KI und Maschinelles Lernen verwendet werden, wie in folgender Darstellung vorgeschlagen.

Sie kann aber auch in Schwache und Starke KI unterschieden werden. Schwache KI (Narrow AI) ist auf spezifische Aufgaben spezialisiert. Sie kann keine kontextübergrei-

fenden Entscheidungen treffen oder lernen, da sie kein Bewusstsein oder Verständnis besitzt, sondern nur aufgrund erlernter Muster reagiert. Beispiele sind Sprachassistenten wie Siri, Übersetzungsprogramme oder Chatbots.

Eine Starke KI (General AI) bezeichnet ein hypothetisches System, die ein menschenähnliches Bewusstsein simuliert. Sie kann nicht nur Aufgaben ausführen, sondern auch

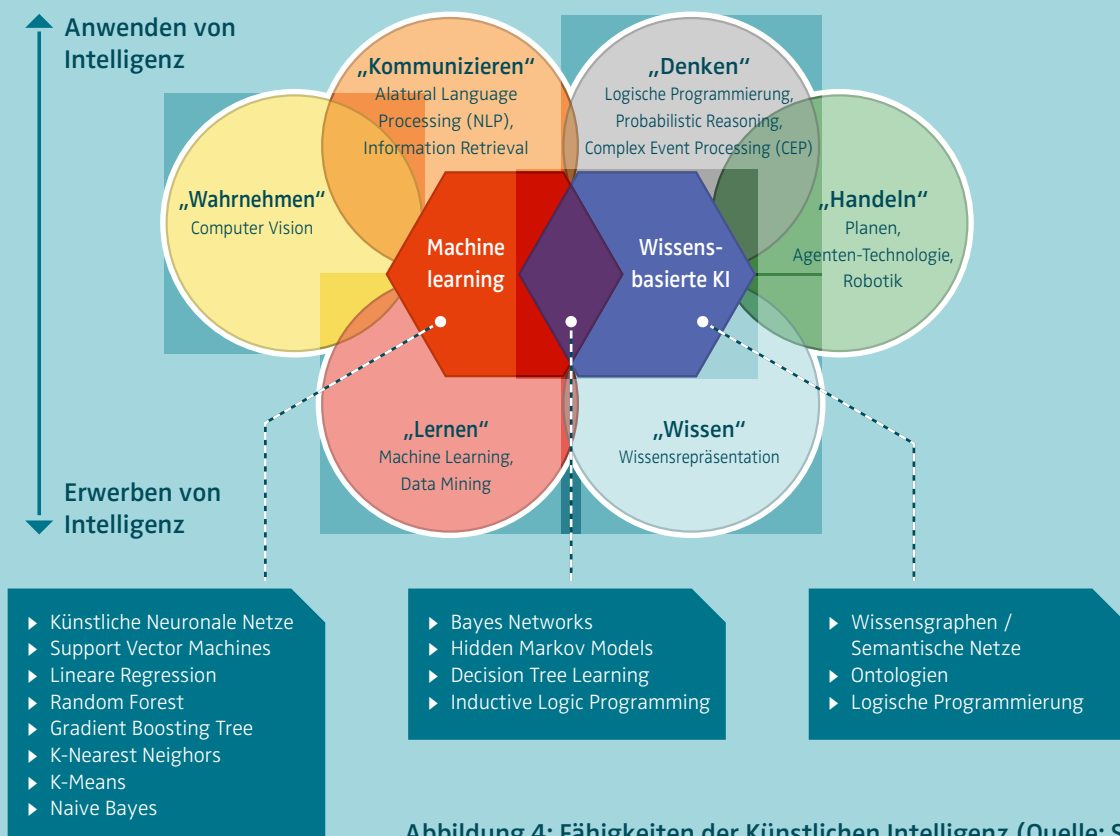


Abbildung 4: Fähigkeiten der Künstlichen Intelligenz (Quelle: Springer)

wirklich „verstehen“, „denken“ und eigenständig Schlüsse ziehen – also echte kognitive Fähigkeiten zeigen. Eine Starke KI wäre in der Lage, flexibel in neuen Situationen zu handeln, ähnlich wie ein Mensch. Bis heute existiert eine solche KI nicht; sie ist Gegenstand intensiver Forschung und ethischer Debatten

2.2 Einsatz von KI im KRITIS-Sektor

Kritische Infrastrukturen (KRITIS) bilden das Rückgrat moderner Gesellschaften. Sie umfassen essenzielle Bereiche wie Energieversorgung, Wasserwirtschaft, Gesundheitswesen, Transport und Informationstechnologie, deren Funktionsfähigkeit grundlegend für das Gemeinwohl, die öffentliche Sicherheit und die wirtschaftliche Stabilität ist. Für Unternehmen im KRITIS-Sektor (kritische Infrastrukturen) gelten beim Einsatz von Künstlicher Intelligenz besondere Anforderungen. Diese ergeben sich aus der sicherheitskritischen Bedeutung dieser Sektoren für die Gesellschaft und aus rechtlichen Vorgaben. Einsatzfelder sind zum Beispiel Prognosen, Steuerungen und Überwachungen.

Im Energiesektor spielt der Einsatz von Künstlicher Intelligenz in einigen wichtigen Anwendungsbereichen wie im Energiehandel eine wichtige Rolle. Zum Beispiel in intelligenten Stromnetzen (Smart Grids) kann KI die Energiever-

teilung und das Netzwerkmanagement optimieren, indem die KI Angebot und Nachfrage in Echtzeit analysiert. Für Lastprognosen kann die KI den Energieverbrauch vorhersagen und Schwankungen ausgleichen, um Überlastungen zu vermeiden. Eine Optimierung von Solar- und Windkraftanlagen ist durch KI möglich, indem z. B. Wetterdaten analysiert und die Stromerzeugung angepasst werden können.

In der Wasserbranche kann der Einsatz von KI-Technologien beispielsweise bei der Überwachung von Wasserqualität, der Steuerung von Wasserinfrastrukturen sowie der Reaktion auf Störungen eingesetzt werden. Einige Unternehmen in der Wasser- und Abwasserbranche setzen bereits verschiedene KI-basierte Anwendungen und -systeme zur Überwachung und Optimierung des Betriebs ein.

Im Bereich der Wartung kann KI in Windturbinen, Solarmodulen, Rohrleitungen oder Schienennetzen frühzeitig Fehler oder Verschleiß prognostizieren sowie erkennen und so Ausfälle reduzieren (Predictive Maintenance).

KI ermöglicht zudem Effizienzverbesserung und Optimierung im Verbrauch zum Beispiel von Energie oder Wasser in Industrie und Gebäuden, indem Beleuchtung, Heizung und Kühlung basierend auf Nutzungsverhalten und Wetterdaten gesteuert werden (Smart Building).

Auch die Optimierung von Energiespeicherung, beispielsweise von Batterieladung und -entladung für Elektrofahrzeuge, kann effizienter verwaltet und gesteuert werden, um die Netzstabilität zu gewährleisten. Im Handel und in der Preisgestaltung im Energiemarkt mit seiner dynamischen Preissetzung kann KI Markttrends analysieren und Strompreise optimieren. Im automatisierten Handel handeln KI-gesteuerte Algorithmen mit Energie an Börsen für eine effizientere Marktregulierung.

Insgesamt müssen bei der Entwicklung und Nutzung von KI-Technologien daher höhere Sicherheits- und Datenschutzanforderungen eingehalten werden. Unternehmen und Organisationen der kritischen Infrastruktur prüfen ihre KI-Systeme bereits genauer und dokumentieren die Berichte, um sicherzustellen, dass diese zuverlässig sind. Hier soll insbesondere der AI Act dazu beitragen, das Vertrauen in KI-Anwendungen auch bei kleineren und mittleren Betrieben zu stärken und mögliche Risiken zu minimieren, was letztlich auch den im Bereich KRITIS angesiedelten Branchen zugutekommt, da sie damit KI-Systeme als vertrauenswürdige und effizientere Technologien einsetzen können.

2.3 KI im Kontext europäischer Regulierung – KI-Verordnung (AI Act)

Mit Veröffentlichung der europäischen KI-Verordnung (KI-VO) (EU) 2024/1689 (auch AI Act genannt) im August 2024 bestehen europaweit harmonisierte Vorschriften für den Einsatz von Produkten, die Künstliche Intelligenz verwenden, insbesondere in Bereichen, die die KI-Verordnung mit Risiko und Hochrisiko definiert. Die KI-VO hat die Ziele, einerseits das Vertrauen in KI zu stärken durch die Regulierung der Sicherheit von KI-Systemen, andererseits auch die Förderung von Innovation zu unterstützen. Die Übergangsfrist zur Umsetzung der Anforderungen aus dem AI Act endet im August 2026.

Die einheitlichen Regeln der KI-VO verbieten gewisse Praktiken im Bereich KI, stellen besondere Anforderungen an

sog. Hochrisiko-KI-Systeme, definieren für bestimmte KI-Systeme einheitliche Transparenzvorschriften und haben Vorgaben für KI-Modelle mit allgemeinem Verwendungszweck.

Die KI-Verordnung ist eingebettet in das EU New Legislative Framework (EU NLF) für Produktsicherheit und ergänzt die europäische Verordnung zur Maschinensicherheit für Produkte, die Verfahren der Künstlichen Intelligenz verwenden.

Für Produkte mit KI gelten bereits bestehende EU-Verordnungen wie die DSGVO, der Cybersecurity Act (CSA) und der Cyber Resilience Act (CRA), die Radio Equipment Directive (RED) ebenso wie der Data Act und ggf. weitere. Dabei sind CRA und AI Act in besonderer Weise für Cybersecurity und deren Konformität direkt verbunden.

Die zuständige Marktaufsicht zur KI-Verordnung und deren Umsetzung erfolgt in Deutschland durch ein Umsetzungsgesetz, vergleichbar der Datenschutz-Grundverordnung. Die Behörde zur Marktaufsicht in Deutschland ist aktuell in Planung.

Harmonisierte EU-Standards für die Konformität zur KI-VO

Das New Legislative Framework (NLF) beinhaltet die Einbindung der Wirtschaft für die Beschreibung der technischen und organisatorischen Umsetzung für die Compliance mit dem Gesetz. Dies erfolgt durch die Verwendung von sogenannten harmonisierten europäischen Normen (hENs). Diese Standards wurden bei der europäischen Standardisierungsorganisation CEN CENELEC mit dem sog. Standardisation Request durch die Europäische Kommission in Auftrag gegeben. Im Rahmen des Standardisierungsprozesses werden diese neuen hENs auf Compliance mit dem Gesetz geprüft und abschließend im Europäischen Amtsblatt veröffentlicht. Die Verwendung dieser hENs ist freiwillig und ermöglicht ein Self-Assessment, d. h. die Anwendung einer hEN beinhaltet eine Konformitätsvermutung mit der hEN und damit eine Compliance-Vermutung mit dem Gesetz.

2.4 Harmonisierte europäische KI-Standards zur KI-Verordnung

Die EU-Kommission hat CEN CENELEC über einen Standardisation Request zur KI-VO mit der Entwicklung von hENS zu 10 Themenbereichen beauftragt, die Unternehmen bei der

Einhaltung der Compliance durch Konformität zur Verfügung stehen sollen.

Die 10 Themen der zukünftigen harmonisierten Standards zur KI-VO umfassen die Inhalte der Artikel 9–15 und 17 und sollen Ende 2026 veröffentlicht werden.

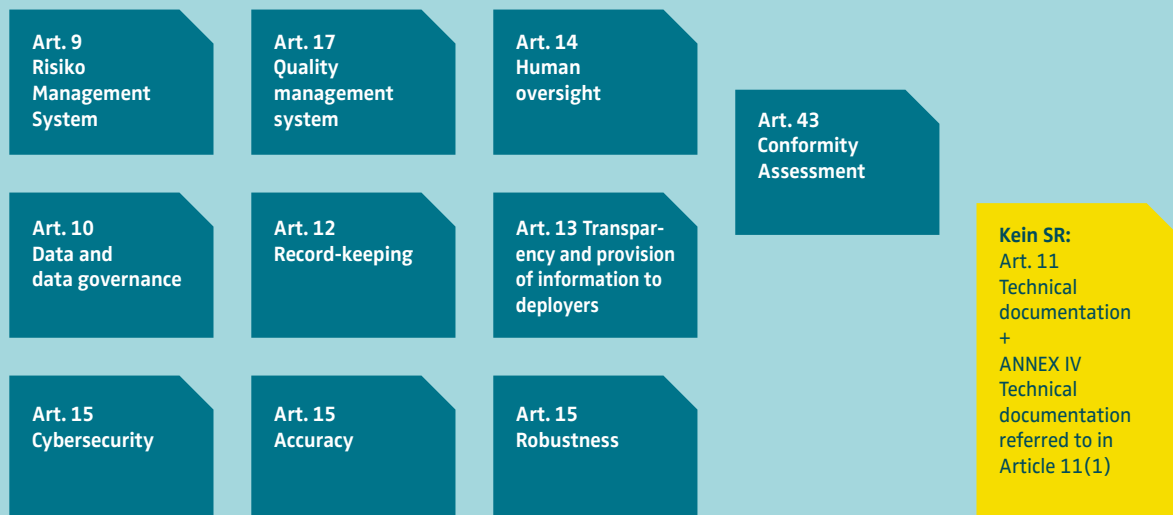


Abbildung 5: Die 10 Themen der zukünftigen harmonisierten Standards zur KI-Verordnung

Ausgangspunkt für die Entscheidung über passende Sicherheitsmaßnahmen ist eine Risikoanalyse und ein Risikomanagement. Das Qualitätsmanagementsystem organisiert die Umsetzung der technischen und organisatorischen Maßnahmen 1–8 und das Conformity Assessment dokumentiert die Einhaltung der gesetzlichen Anforderungen durch Einhaltung der Anforderungen aus den hENS.

Die geplanten hENS verwenden oder basieren auf, soweit möglich, international bereits verfügbare Standards zu KI. Da es Besonderheiten aus der KI-VO in Europa gibt, wie z. B. die Einhaltung der Charta der Grundrechte der EU (Fundamental Rights inkl. Safety und Health) in der Risikobetrachtung, erwartet die EU-Kommission spezifische hENS.

KI-VO; Artikel 4 „KI-Kompetenz“

Dieser Artikel gilt ab Februar 2025 für alle Unternehmen, die KI entwickeln und in Verkehr bringen oder betreiben.

„Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz ver-

fügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.“

2.5 Weiteres gesetzliches und normatives Umfeld zur KI-VO

In den kritischen Infrastrukturen wie Wasser/Abwasser oder Energie müssen neben dem AI Act auch andere Gesetze und Regelungen beachtet werden, die den Einsatz von Technologien und Daten betreffen.

Nachfolgend einige wichtige Gesetze beispielhaft aus dem Strom, Wasser- und Abwasserbereich, die zusätzlich relevant sein könnten:

1. Datenschutz-Grundverordnung (DSGVO):

Da bei der Überwachung und Steuerung von Energie- oder Wasserinfrastrukturen oft personenbezogene Daten verarbeitet werden, muss die Branche die DSGVO einhalten, um den Schutz der Daten sicherzustellen.

2. Umweltschutzgesetze:

Gesetze wie das Wasserhaushaltsgesetz (WHG) und die Wasserrahmenrichtlinie in Deutschland regeln den Schutz von Wasserressourcen und Umweltstandards, die bei der Nutzung von KI-Technologien berücksichtigt werden müssen.

3. Gesetze zur IT-Sicherheit:

Gesetze wie die EU-NIS-2-Verordnung, das IT Sicherheitsgesetz, der EU Cybersecurity Act und der Cyber Resilience Act sowie der Critical Entity Resilience Act. Vorschriften wie das IT-Sicherheitsgesetz fordern, dass kritische Infrastrukturen, zu denen auch Energie, Wasser- und Abwasseranlagen gehören, besonders geschützt werden.

4. Energiegesetze:

Die Energiebranche selbst ist durch das Energiewirtschaftsgesetz zusätzlich reguliert. Da viele Wasserinfrastrukturen energieintensiv sind, müssen auch energiebezogene Vorgaben beachtet werden, etwa im Rahmen der Energiewende.

5. Branchen- und Normenregelungen:

Es gibt spezifische technische Standards und Normen, die bei der Implementierung von KI-Systemen in der Energie- und Wasserbranche beachtet werden sollten, z. B. DIN-, EN- und ISO/IEC-Normen mit bestehenden Regelwerken und Vorgehensmodellen, wie u. a. die ISO 27001/27002 und der BSI-Standard 200-4 umfassend einbezogen und auf ihre Anwendbarkeit im Kontext von KI in KRITIS-Unternehmen untersucht werden sollten.

3. HERAUSFORDERUNGEN VON KI IN KRITISCHEN INFRASTRUKTUREN

In kritischen Infrastrukturen wie Wasser, Wärme-, Strom- und Gasnetzen gibt es verschiedene Prozesse, die für die Sicherheit, Effizienz und Zuverlässigkeit der Versorgung von entscheidender Bedeutung sind.

Diese Infrastrukturen müssen rund um die Uhr funktionieren und jede Störung kann weitreichende Folgen haben – sowohl für die Bevölkerung als auch für die Wirtschaft. Die grundlegenden Prozesse werden in Führungs-, Kern- und Unterstützungsprozesse unterteilt und haben eine Vielzahl von Aktivitäten, die miteinander verknüpft sind und eine stabile Versorgung gewährleisten.

Unternehmen in kritischen Infrastrukturen sind insbesondere dem ständigen Wandel unterzogen, da diese mit

der Aufrechterhaltung der Leistungserbringung und den gesetzlichen Vorgaben konform sein müssen. Um für die zukünftigen Konformität gerüstet zu sein, besteht eine Herausforderung für die Unternehmen darin, in ihren Prozessen den Einsatz von Künstlicher Intelligenz zu eruieren.

Der Einsatz von Künstlicher Intelligenz in Führungs-, Kern- und Unterstützungsprozessen – also in den zentralen Geschäftsbereichen eines Unternehmens – bringt sowohl Chancen als auch tiefgreifende Herausforderungen mit sich.

Nachfolgend soll ein Beispiel der generellen Prozesslandschaft eines Unternehmens der kritischen Infrastrukturen abgebildet werden.

Prozesslandkarte Netzbetreiber			
Führungsprozesse Steuerung: Strategie, Forschung und Führung)			
Strategie-entwicklung/ Forschung & Innovation	Unternehmensplanung und Controlling	Disziplinarische und fachliche Führung	Integrierte Managementsysteme (wie ISMS, BCMS, etc.)
Kernprozesse (Leistungserbringung: Produktion und/oder Dienstleistung)			
Erzeugung/Förderung	Transport	Verteilung oder Speicherung	Überwachung und Systemführung
Beschaffung für den Kernprozess			
Unterstützungsprozesse (Befähigung: Administration)			
IT-Management	Personal	Buchhaltung	TQM-Systemmanagement
Gebäudemanagement/physische Sicherheit			

3.1 Beispiele für Kernprozesse der kritischen Infrastruktur

Kernprozesse beinhalten oft kritische Entscheidungen, die für den Erfolg eines Unternehmens entscheidend sind. KI-Systeme, insbesondere komplexe Modelle wie Deep Learning, sind jedoch häufig schwer nachvollziehbar. Diese „Black Box“-Natur von KI-Modellen bedeutet, dass es schwierig ist, die genauen Ursachen für eine Entscheidung nachzuvollziehen. Wenn beispielsweise ein KI-Modell eine wichtige Produktionsentscheidung trifft, könnte es für das Unternehmen problematisch sein, die genaue Logik zu verstehen, die zu dieser Entscheidung geführt hat. Das Fehlen einer nachvollziehbaren Entscheidungsfindung kann zu Vertrauenseinbußen und rechtlichen Problemen führen, insbesondere, wenn Fehler auftreten. Im Folgenden werden beispielhaft Kernprozesse der kritischen Infrastruktur vorgestellt.

Stromverteilung:

Die elektrische Energieverteilung erfolgt von den Erzeugerquellen (z. B. Kraftwerken) über sogenannte Transport- und Verteilungsnetze bis zu den Endverbrauchern (z. B. Haushalts- oder Gewerbekunden). Hierbei wird die Energie über unterschiedliche Spannungsebenen von der Höchstspannung (380 kV) über Hoch- und Mittelspannung (110 kV, 10 kV) bis zur Niederspannung (230/400 V) bedarfsgerecht transformiert und übertragen. Von der Systemführung der jeweiligen Netzbetreiber werden Systemdienstleistungen wie Spannungs- und Frequenzhaltung, Engpassmanagement und Wiederversorgung erbracht, um Stabilität und Qualität der Stromversorgung sicherzustellen.

Gastransport und -verteilung:

Gas wird über Pipelines transportiert und in verschiedenen Stationen reduziert und in die entsprechenden Verteilernetze eingespeist. Dieser Prozess umfasst auch die Verwaltung von Druck, Temperatur und die Sicherstellung eines sicheren Transports.

Wasserwirtschaft

Die Wasserwirtschaft in Deutschland ist stark dezentralisiert und es gibt etwa 1.200 Wasserversorgungs- und 10.000 Abwasserentsorgungsbetriebe. Es gibt die Wasserentnahme aus Talsperren, Seen, Flüssen oder dem Grundwasser, eine technische Anlage zur Aufbereitung und das Druckverteilnetz teilweise mit Hochbehältern bis zum Verbraucher. Für die Abwasserableitung werden kilometerlange Kanäle und Abwasserdruckleitungen mit Pumpstationen genutzt und für die Abwasserreinigung kommen mehrstufige Klärwerke zum Einsatz.

3.2 Herausforderungen für die Integration in bestehende Systeme

Die Integration von KI in bestehende Kernprozesse ist technisch sehr anspruchsvoll. Viele Unternehmen arbeiten mit Altsystemen, die möglicherweise nicht mit modernen KI-Technologien kompatibel sind. Die Umstellung auf KI-basierte Prozesse erfordert oft umfangreiche Änderungen an bestehenden IT-Infrastrukturen, was hohe Kosten und Zeitaufwand mit sich bringen kann. Zudem muss die KI in der Lage sein, mit unterschiedlichen Datenquellen zu interagieren und komplexe, oft unstrukturierte Daten zu verarbeiten.

3.2.1 Skalierbarkeit und Leistung

In vielen Kernprozessen ist die Verarbeitung von großen Datenmengen erforderlich, um fundierte Entscheidungen zu treffen – beispielsweise in der Produktion oder im Vertrieb. KI muss in der Lage sein, mit diesen großen Mengen effizient zu arbeiten. Skalierbarkeit und Leistungsfähigkeit sind daher große Herausforderungen, insbesondere, wenn die KI in Echtzeit agieren soll, wie es etwa im Bereich des Energietrading oder der Echtzeitsteuerung notwendig ist. Wenn KI-Modelle zu langsam sind oder nicht ausreichend skalieren, können sie den gesamten Prozess verlangsamen oder ineffizient machen.

3.2.2 Vertrauenswürdigkeit und Fehleranfälligkeit

In kritischen Kernprozessen können Fehler oder falsche Entscheidungen katastrophale Folgen haben. Ein KI-System, das Fehler macht, kann erhebliche finanzielle Verluste verursachen, die Qualität eines Produkts beeinträchtigen oder die Sicherheit gefährden. In Bereichen wie der Automatisierung der Produktion oder der Finanzbuchhaltung ist die Minimierung von Fehlern entscheidend. KI-Systeme müssen daher besonders robust und zuverlässig sein. Zudem erfordert der Umgang mit solchen Fehlern, etwa durch ein funktionierendes Monitoring-System, eine detaillierte Überprüfung und ein kontinuierliches Testen der KI-Modelle.

3.2.3 Bias und ethische Herausforderungen

Ein besonders schwieriges Thema in Kernprozessen ist der Bias (Vorurteile) in den KI-Modellen. Wenn KI mit historischen Daten trainiert wird, die Verzerrungen oder Diskriminierungen enthalten, kann die KI diese Vorurteile verstärken und fehlerhafte Entscheidungen treffen. In kritischen Prozessen wie der Personalrekrutierung, der Prognosen oder der Monitoringanalyse kann dies schwerwiegende Auswirkungen haben, insbesondere wenn solche Verzerrungen unbemerkt bleiben. Es ist daher erforderlich, KI-Systeme regelmäßig auf Bias zu überprüfen und sicherzustellen, dass die Modelle auf fairen und repräsentativen Daten basieren.

3.2.4 Sicherheitsrisiken und Datenschutz beachten

Kernprozesse beinhalten oft vertrauliche und sensible Daten, etwa im Finanzwesen, in der Produktion oder im Personalwesen. KI-Systeme müssen diesen Datenschutzanforderungen gerecht werden und gleichzeitig vor Cyberangriffen geschützt sein. Ein KI-System, das in einem kritischen Prozess wie der Leitungssteuerung eingesetzt wird, könnte potenziellen Hackerangriffen ausgesetzt sein. Angreifer könnten versuchen, das System zu manipulieren oder unbefugten Zugriff auf Daten zu erlangen. Der Schutz dieser Systeme vor solchen Bedrohungen ist eine zentrale Herausforderung.

3.2.5 Kosten und Ressourcen planen

Die Implementierung von KI in Kernprozessen erfordert in der Regel erhebliche Investitionen, sowohl in Bezug auf die Technologie selbst als auch auf das erforderliche Fachwissen. Viele Unternehmen müssen spezielle KI-Ingenieure und Data Scientists einstellen oder externe Berater hinzuziehen, um die Systeme zu entwickeln und zu implementieren. Zudem erzeugt Aufrechterhaltung der KI-Infrastruktur Kosten, da regelmäßige Wartung und Anpassungen notwendig sind, um mit den Veränderungen in den Geschäftsprozessen und Datenquellen Schritt zu halten.

3.2.6 Veränderung der Unternehmenskultur organisieren

Die Einführung von KI in Kernprozessen hat Auswirkungen auf die Unternehmenskultur. Mitarbeiter müssen nicht nur die neuen Systeme lernen, sondern auch mit den Veränderungen umgehen, die durch die Automatisierung und die Entscheidungsfindung durch KI entstehen. Dies kann Widerstand und Unsicherheit hervorrufen. Insbesondere Mitarbeiter, die bisher zentrale Entscheidungen getroffen

haben, könnten sich durch die KI in ihrer Autorität bedroht fühlen. Eine klare Kommunikation und Schulung der Mitarbeiter sind erforderlich, um eine erfolgreiche Akzeptanz von KI-Technologien zu gewährleisten.

3.2.7 Langfristige Auswirkungen auf Geschäftsmodelle

Die Implementierung von KI in Kernprozessen kann nicht nur die Art und Weise verändern, wie Unternehmen arbeiten, sondern auch ihr gesamtes Geschäftsmodell. KI kann neue Geschäftsmodelle ermöglichen, bestehende Modelle jedoch auch obsolet machen. Unternehmen müssen daher die langfristigen Auswirkungen von KI auf ihre Geschäftsfelder bedenken und Strategien entwickeln, um sich kontinuierlich anzupassen.

3.3 Zusammenfassung

Künstliche Intelligenz (KI) hat in den letzten Jahren stark an Bedeutung gewonnen und beeinflusst nahezu alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens. KI revolutioniert einige Bereiche und hält Einzug in die Prozesse (Führungs-, Kern- und Unterstützungsprozesse) von Unternehmen. Zusammengefasst lässt sich sagen, dass die Implementierung von KI in den Kernprozessen eines Unternehmens in der Zukunft neue Möglichkeiten schafft, aber auch zahlreiche neue Herausforderungen mit sich bringt. Diese reichen von technologischen Aspekten wie der Integration und Skalierbarkeit in die Unternehmen bis hin zu organisatorischen Fragen der Akzeptanz und der ethischen Verantwortung. Der Erfolg hängt daher nicht nur von der Qualität der Technologie ab, sondern auch von einer sorgfältigen Planung, kontinuierlichen Anpassung und der Fähigkeit, die KI im Einklang mit den Unternehmenswerten und -zielen zu nutzen.

4. ANHANG

Rollen gemäß KI-VO Artikel 3

3. „Anbieter“: eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;

4. „Betreiber“: eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

5. „Bevollmächtigter“: eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;

6. „Einführer“: eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt;

7. „Händler“: eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem EU-Markt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;

8. „Akteur“: ein Anbieter, Produkthersteller, Betreiber, Bevollmächtigter, Einführer oder Händler;

9. „Inverkehrbringen“: die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem EU-Markt ;

10. „Bereitstellung auf dem Markt“: die entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem EU-Markt im Rahmen einer Geschäftstätigkeit;

11. „Inbetriebnahme“: die Bereitstellung eines KI-Systems in der EU zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung.

DIN EN ISO 9000:2015-11

3.2.4 Kunde

Person oder Organisation (3.2.1), die ein Produkt (3.7.6) oder eine Dienstleistung (3.7.7) empfängt oder empfangen könnte, welches oder welche für diese Person oder Organisation vorgesehen ist oder von ihr gefordert wird.

BEISPIEL: Verbraucher, Klient, Endanwender, Einzelhändler, Empfänger eines Produkts oder einer Dienstleistung aus einem internen Prozess (3.4.1), Nutznießer und Käufer.

Anmerkung zum Begriff: Ein Kunde kann der Organisation angehören oder ein Außenstehender sein.

Teilnehmende / Anmerkungen

Regina Gnirss	Berliner Wasserbetriebe
Lorenz Müller	NBB Netzgesellschaft
	Berlin-Brandenburg mbH & Co. KG
Andrea Pieper	KKI-Kompetenzzentrum
	Kritische Infrastrukturen GmbH
Dr. Henrich C. Pöhls	IT-Sicherheitszentrum
	der Universität Passau
Felix Schmalenbach	Berliner Wasserbetriebe
Marco Schwarz	Stromnetz Berlin GmbH
Mathias Schröder	Berlin Energie Netz und
	Service GmbH
Georg Seemann	ENLITE Management &
	Engineering GmbH
Annegrit Seyerlein-Klug	Technische Hochschule
	Brandenburg
Prof. Ingo Timm	Universität Trier

Dieses White Paper wurde von mehreren Expertinnen und Experten aus verschiedenen Organisationen, Einrichtungen und Unternehmen unter der Koordination des KKI e.V. erstellt. Die Inhalte dieses Dokuments wurden nach bestem Wissen und Gewissen sowie mit größtmöglicher Sorgfalt zusammengestellt. Der KKI e.V. und die an diesem White Paper beteiligten Personen und Organisationen, Einrichtungen und Unternehmen übernehmen jedoch keine Gewähr für die Vollständigkeit, Richtigkeit, Aktualität oder Eignung der bereitgestellten Informationen für spezifische Anwendungsfälle.

Dieses Dokument dient ausschließlich zu Informationszwecken und stellt keine rechtliche, geschäftliche oder technische Beratung dar. Die Verwendung der Inhalte erfolgt auf eigenes Risiko. Der KKI e.V. und die Mitwirkenden haften nicht für direkte oder indirekte Schäden, die sich aus der Nutzung der in diesem Dokument enthaltenen Informationen ergeben.

Die in diesem White Paper geäußerten Meinungen und Interpretationen spiegeln die Ansichten der jeweiligen Autorinnen und Autoren wider und stellen nicht unbedingt die offizielle Position des KKI e.V. oder der beteiligten Organisationen, Einrichtungen und Unternehmen dar. Wir empfehlen, die Inhalte dieses White Papers mit eigenen Prüfungen zu ergänzen und, falls erforderlich, fachkundige Beratung einzuholen.

Glossar

KI-Projekte sind vorzugsweise mit interdisziplinär besetzten Teams durchzuführen. Zu den verschiedenen Fachdisziplinen (Softwareentwicklung, Betriebswirtschaft, KI-/Datenexperten, etc.) kommen Stakeholder auch aus „KI-fremden“ Gebieten. Hier ist es wichtig, die Kommunikation von Beginn an auf ein gemeinsames Verständnis von KI-relevanten Begriffen aufzubauen. Viele Begriffe sind erst in den letzten Jahren entstanden bzw. haben sich weiterentwickelt. Selbst Experten meinen möglicherweise subtil andere Dinge mit dem gleichen Begriff. Die Verwendung eines gemeinsamen Wortschatzes ist daher wichtig und die Bildung eines internen Glossars hilfreich. Dabei kann man auf bestehendes, bereits diskutiertes Vokabular zurückgreifen:

- ▶ ISO/IEC 22989 (kostenfrei zum Download verfügbar unter <https://www.iso.org/standard/74296.html>) liefert einen ersten Grundstock.
- ▶ Der europäische AI Act enthält ebenfalls Begriffe.
- ▶ Des Weiteren gibt es unter <https://ai-glossary.org/> eine erweiterte Fassung des Glossars, welches im Rahmen der 2. Ausgabe der Deutschen Normungsroadmap KI erarbeitet wurde und auf Basis verschiedener Quellen die technischen Begriffe definiert sowie bestehende Unterschiede aufzeigt.

Beispiel für Begriffsthemen

In der Begriffswelt des Maschinellen Lernens – also dem Ansatz, der heute möglicherweise oft einfach mit KI gleichgesetzt wird – bezieht sich der Begriff Validierung auf eine Auswahl beziehungsweise Optimierung eines geeigneten KI-Modells (siehe ISO/IEC 22989 – „Artificial intelligence concepts and terminology“ [ISO22]). Aber im Kontext der Produktentwicklung bezeichnet Validierung möglicherweise die Erbringung eines objektiven Nachweises, dass Produkthanforderungen für eine gegebene Anwendung ausreichend erfüllt worden sind (siehe ISO/IEC 17000 –

„Konformitätsbewertung – Begriffe und allgemeine Grundlagen“). In der Produktentwicklung ist dies also eher der finale Schritt, im Lebenszyklus eines KI-Systems ist er hingegen nur ein Zwischenschritt im Training des ML-Modells. [Vertiefend dazu siehe: G. Runze, M. Haimerl, M. Hauer, T. Holoyad, O. Obert, H. C. Pöhls, R. Tagiew und J. Ziehn. Ein Werkzeug für eine gemeinsame KI-Terminologie. In JavaSPEKTRUM 03/2023, SIGS DATACOM GmbH, May, 2023.]

Beispiele für Glossar-Einträge

KI-System: ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann und nach seiner Einführung Anpassungsfähigkeit zeigt und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können. [Quelle: KI-VO Artikel 3]

Modell (allg.): physikalische, mathematische oder anderweitig logische Darstellung eines Systems, einer Einheit, eines Phänomens, eines Prozesses oder von Daten, einschließlich ihrer Beziehungen und Abhängigkeiten, unter Verwendung eines festgelegten Satzes von Regeln und Konzepten. [Quelle: ai-glossary, <https://ai-glossary.org/index> | Zugriff 05.10.2025; ähnlich steht es auch in der ISO/IEC 22989.]

KI-Modell mit allgemeinem Verwendungszweck: ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden. [Quelle: KI-VO Artikel 3]

Maschinelles-Lernen (ML)-Modell: ein mathematisches Konstrukt, das auf der Grundlage von Eingangsdaten eine Schlussfolgerung oder Vorhersage trifft. [Quelle: ai-glossary, <https://ai-glossary.org/index>; Zugriff 05.10.2025, ähnlich steht es auch in der ISO/IEC 22989.]

Literaturverzeichnis

https://pm-wissen.com/wie-funktioniert-kuenstliche-intelligenz_27150
Zugriff 05.10.2025

Vgl. OECD:
<https://oecd.ai/en/wonk/ai-system-definition-update>
Zugriff 05.10.2025

Vgl.
https://link.springer.com/chapter/10.1007/978-3-662-63449-3_2/figures/1
Zugriff 13.1.26
SSN 1860-4803 ISSN 1860-4811 (electronic)
Ethics of Science and Technology Assessment Bd. 48
Künstliche Intelligenz in der Forschung; Neue Möglichkeiten und Herausforderungen für die Wissenschaft
Grundlagen und Anwendungen von KI, Autoren: Bernhard G. Humm, Peter Buxmann und Jan C. Schmidt, Springer © Der/die Herausgeber bzw. der/die Autor(en) 2022

Vgl. ISO/IEC 22989 Information technology – Artificial intelligence – Artificial intelligence concepts and terminology
<https://www.iso.org/standard/74296.html>
Zugriff 05.10.2025