



Von KI-Service "Midjourney" erzeugt

Sonderdruck aus
JavaSPEKTRUM 3/2023

Das AI-Glossary als Weg aus Babylon

Ein Werkzeug für eine gemeinsame KI-Terminologie

Gerhard Runze, Martin Haimerl, Marc Hauer, Taras Holoyad, Otto Obert, Henrich Pöhls, Rustam Tagiew, Jens Ziehn

Am 9. Dezember 2022 wurde zeitgleich mit dem Digital-Gipfel der Bundesregierung die bereits zweite Ausgabe der „Deutschen Normungsroadmap Künstliche Intelligenz“ (NRM KI) veröffentlicht [DIN22]. Das federführende Deutsche Institut für Normung (DIN) stand vor der Herausforderung, mehr als 570 mitwirkende Fachleute aus den verschiedensten Bereichen von Wissenschaft, Wirtschaft, Zivilgesellschaft und der öffentlichen Hand zu koordinieren.

Während der Arbeit an der NRM KI haben die Beteiligten früh festgestellt, dass es immer wieder eine gewisse Verwirrung bezüglich der verwendeten Begriffe unter den Mitwirkenden gab. Aus diesem Grund entstand eine Glossar-Gruppe (der die Autoren dieses Artikels angehörten), deren zentrales Anliegen die Bewältigung

dieses Sprachgewirrs war, das heißt, die Vereinheitlichung der Begriffe inkl. der zugehörigen Koordination der Teilnehmenden. Unter Leitung der Glossar-Gruppe entstand ein gemeinsames Glossar für die knapp 450 Seiten starke NRM KI, das einerseits die Schwerpunktthemen hinsichtlich der Anwendungen (z. B. Medizin, Mobilität, Energie & Umwelt, Finanzdienstleistungen, Industrielle Automation) und grundlegenden Fragen (z. B. KI-Klassifizierung, Sicherheit, Zertifizierbarkeit, Soziotechnische Systeme, Ethik) abdeckt. Andererseits verschafft es quer durch verschiedenste Interessensgruppen und Informationsquellen einen Überblick über die zentralen Begriffe im Bereich von KI und dessen Umfeld.

Eine Roadmap für KI-Normen

Künstliche Intelligenz (KI) ist inzwischen, und mit den aktuellen Entwicklungen immer stärker Beförderer von exponentiellen Technologien, die unterschiedlichste Branchen und Disziplinen enger denn je miteinander verbinden. General Purpose KI-Modelle, basierend auf maschinellem Lernen (ML), lösen bereits heute Probleme aus sehr unterschiedlich sensiblen Bereichen, von personalisierter Werbung bis zu medizinischer Diagnostik und autonomem Fahren. Sie können Sprache oder Bilder nicht nur analysieren, sondern auch künstlich erzeugen, und betreffen dabei die Spitzenforschung ebenso wie mittelständische Unternehmen oder Privatangehörige.

Einige KI-Anwendungen sind dem Menschen in Teilbereichen bereits überlegen, beispielsweise erstmals 2012 in der Bildauswertung bei der Erkennung von Straßenschildern [Cir12] oder im

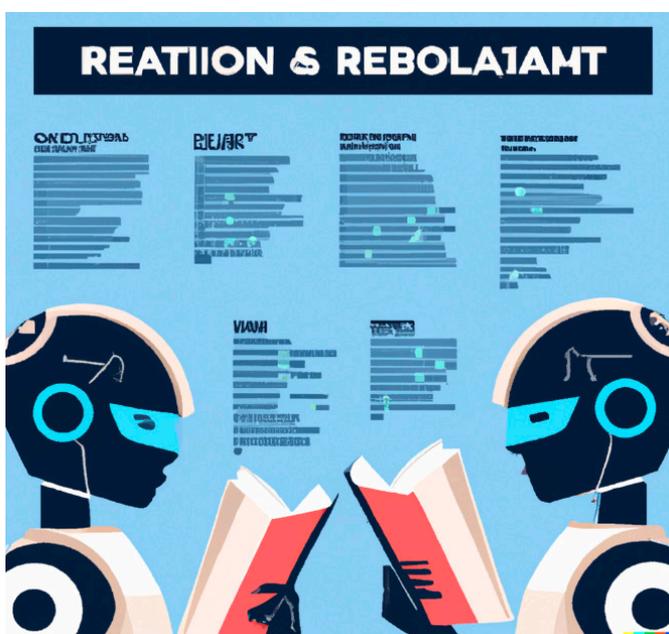


Abb. 1: „Humanoide Roboter, die Wörterbücher lesen, als Infografik“. Ein von der KI „DALL-E“ (OpenAI [Ope23b]) erzeugtes Bild für diesen Beitrag. Selbst für Experten ist schwer zu beschreiben und zu verstehen, wie dieses Bild zustande gekommen ist. Umso wichtiger ist bei Expertengesprächen, Missverständnisse selbst über elementare Begriffe zu vermeiden - nicht nur unter Robotern

Die Autoren des Artikels sind Mitautoren der Deutschen Normungsroadmap KI Ausgabe 2 und haben zum Teil auch schon an der Version 1 mitgewirkt.



Dr. Gerhard Runze arbeitet bei der imbus AG als Senior Berater für den Test eingebetteter Systeme, KI und agile Softwareentwicklung. Als Product Owner KI ist er für die Qualitätssicherung in KI-Projekten zuständig.
E-Mail: gerhard.runze@imbus.de

Prof. Dr. Martin Haimerl ist Professor für Medizintechnik und wissenschaftlicher Direktor des Innovations- und Forschungszentrums Tuttlingen an der Hochschule Furtwangen (HFU). Insbesondere beschäftigt er sich mit regulatorischen Fragestellungen im Bereich KI-basierter Medizinprodukte. E-Mail: martin.haimerl@hs-furtwangen.de

Marc P. Hauer ist forschender Doktorand am Algorithm Accountability Lab der TU Kaiserslautern und promoviert zu der Frage, wie man Softwareentwicklungsprozesse und Softwaresysteme, vornehmlich KI, verantwortungsvoll gestalten kann.
E-Mail: hauer@cs.uni-kl.de

Taras Holoyad standardisiert Qualitätskriterien sowie eine weltweit homogen anwendbare Taxonomie für KI-Systeme im Auftrag der Bundesnetzagentur. Aus Forschungsperspektive befasst er sich u. a. mit multimodaler Identifikation semantischer Ähnlichkeiten zwischen

Texten und Bildern.
E-Mail: taras.holoyad@bnetza.de

Otto Obert ist diplomierter Informatiker, Gründer und Inhaber des Start-ups Main DigitalEthiker GmbH, welches besonders für eine wertebasierte und nachhaltige Umsetzung der Digitalisierung und Digitalen Transformation steht.
E-Mail: otto.obert@digitaethiker.de

Dr. Henrich C. Pöhls ist Post-Doc und Projektleiter am IT-Sicherheitszentrum der Universität Passau und forscht und lehrt zu IT-Sicherheit von komplexen Systemen; und geht daher der Frage nach, wie man die Sicherheit von KI-Systemen zunächst eindeutig beschreiben und dann auch sicherstellen kann.
E-Mail: henrich@poehls.com

Dr. Rustam Tagiew forscht als wissenschaftlicher Referent am Deutschen Zentrum für Schienenverkehrsforschung (DZSF) zu Verfahren der Inbetriebnahmege-nehmigung für fahrerlose Schienenfahrzeuge und zu Methoden der zukunftsorientierten Technologieanalyse.
E-Mail: tagiewR@dzsf.bund.de

Jens Ziehn leitet die Forschungsgruppe „Automotive und Simulation“ am Fraunhofer IOSB in Karlsruhe, die sich mit Lösungen für Entwicklung und Absicherung autonomer Mobilitätssysteme beschäftigt.
E-Mail: jens.ziehn@iosb.fraunhofer.de

Rahmen der Erkennung von Hautkrebs in der Medizin [EST17]. Was die Zukunft bereithält, erahnen wir gerade erst an aktuellen Entwicklungen wie ChatGPT [Ope23a] oder DALL-E 2 [Ope23b]. Um den Mehrwert dieser Technologien zu maximieren, und gleichzeitig Risiken zu minimieren, wird schon heute für übermorgen geplant: Die NRM KI von DIN und DKE hat das Ziel, zu identifizieren, wo Normen und Standards nötig sind, um KI verlässlich entwickeln, betreiben und insbesondere verstehen zu können. Im vergangenen Jahr haben sich dazu Experten aus Wirtschaft, Gesellschaft und Forschung zusammengetan, um gemeinsam diese „Roadmap“ zu einer zweiten Ausgabe weiterzuentwickeln.

Wer aber zusammen reden und arbeiten will, sollte sicher sein, auch dieselbe Sprache zu sprechen. Und gerade das ist bei KI alles andere als einfach: Schon der Begriff „KI“ selbst ist auf unterschiedlichste Arten definiert worden (die Uneinigkeit beginnt spätestens beim Begriff „Intelligenz“). Zudem verbindet er so unterschiedliche Branchen, dass sich sogar branchenspezifische Standards in ihren Begriffsdefinitionen widersprechen können. Das führt zu der kuriosen Situation, dass zwei Experten aus unterschiedlichen Branchen völlig aneinander vorbeireden können, obwohl beide standardisierte Begriffe verwenden – wie wir an Beispielen in diesem Beitrag sehen und diskutieren werden, und wie auch in Abbildung 2 und 3 sichtbar wird.

Gerade im technisch-wissenschaftlichen Bereich ist ein wesentlicher Erfolgsfaktor, dass die Beteiligten einheitliche Begriffe verwenden. Das kennen wir beispielsweise in technischen Systemen: Wenn Softwaresysteme nicht dieselbe „Sprache“ verstehen, wenn sie Daten und deren Inhalte nicht einheitlich interpretieren, dann kommt es mit großer Wahrscheinlichkeit früher oder später zu

Schwierigkeiten. Ein Beispiel dafür aus dem technischen Umfeld ist der Absturz der NASA-Sonde „Mars Climate Orbiter“, die im Rahmen des Discovery-Programms zur Untersuchung des Marsklimas zum Einsatz kam. Im Zuge der Untersuchungen wurde der Absturz auf Berechnungen in unterschiedlichen Maßeinheiten seitens der involvierten Teams aus Europa und den Vereinigten Staaten zurückgeführt [Mer99]. Davon ausgehend sind Übereinkünfte nicht nur auf der Ebene technischer Systeme wichtig, sondern auch für die Zusammenarbeit verschiedener Partner, zum Beispiel von unterschiedlichen Unternehmen oder organisatorischer Ebenen.

Wie wirksam man mit sprachlicher Verwirrung technische Entwicklungen zum Erliegen bringen kann, hat schon die Bibel (Genesis 11, 1-9) erzählt: Als die Babylonier den Bau eines Turms beginnen, der bis in den Himmel reichen soll, gibt Gott ihnen unterschiedliche Sprachen – das allein genügt, um das Vorhaben scheitern zu lassen.

Ziele der Arbeitsgruppe Glossar

Um die genannten Mehrdeutigkeiten bestmöglich einzudämmen, zumindest aber klar zu benennen und für die Arbeit eine verbindende Sprache zu schaffen, hat das DIN in der NRM KI eine Arbeitsgruppe für ein gemeinsames, branchen- und bereichsübergreifendes Glossar eingesetzt. Im Rahmen dieser Tätigkeit haben wir, die Mitglieder dieser Arbeitsgruppe und Autoren dieses Artikels, uns die Aufgabe gestellt, für die gängigsten Fachbegriffe im Umfeld von KI und maschinellem Lernen (ML) prägnante, kurze Definitionen aufzustellen: mit Verweis auf bereits bestehende Normen oder Definitionen, insbesondere dort, wo diese zu Missverständnissen und Bedeutungsunterschieden führen können.

Dass dies nicht nur einem akademischen Zweck dient, haben wir in unseren Diskussionen um manche Begriffe hautnah erlebt. Einige davon greifen wir im Folgenden als Beispiele auf, geben einen Einblick in die Arbeiten und ihre Besonderheiten im Vergleich zu sonst üblichen Glossaren und zeigen, wie Anwender auch zukünftig von diesem Mehrwert profitieren.

Normen und Gesetze – nicht immer in Harmonie

Eine grundlegende Eigenschaft von Dokumenten aus Normung und Gesetzgebung ist, die Terminologie für die jeweils im Dokument beschriebenen Sachverhalte festzulegen. Das allein verschafft aber noch keine breite Anwendung der festgelegten Terminologien: Normungsdokumente müssen oft erst teuer erworben werden. Zudem können Normen auf nationaler, europäischer oder internationaler Ebene in der Definition identischer Begriffe stark voneinander abweichen. Zum Beispiel existiert für Begriffe in ISO-Normen eine Suchmaschine namens *Online Browsing Platform (ISO OBP)* [ISO23], die bei der Suche zum Beispiel nach dem Begriff „Metadaten“ mindestens 96 Normen mit 46 unterschiedlichen Definitionen ergibt [Fur20].

Im Gegensatz zu kostenpflichtigen Normen sind Gesetzesdokumente staatlicher Organe üblicherweise kostenfrei vollständig einsehbar, können aber identische Begriffe wiederum anders als Normungsdokumente definieren. Ein Beispiel dafür sind die unterschiedlichen terminologischen Formulierungen zwischen dem europäischen Gesetzesvorschlag zu KI („AI Act“) [Eur21] und der

internationalen Norm zu KI-Konzepten und Terminologie „ISO/IEC 22989“. Unternehmen, die sich auf Gesetzesdokumente stützen, stehen möglicherweise schneller vor einem schwer nachvollziehbaren Geflecht ineinandergreifender Begriffe und Querbezüge zu unterschiedlichen Dokumententeilen. Allerdings können auch terminologische Beschreibungen erst nach einer Analyse miteinander verknüpfter Normen und Gesetze nachvollzogen werden.

Das AI-Glossary als neuer Ansatz

Selten orientiert sich (auch aus den genannten Gründen) der Sprachgebrauch innerhalb von Zivilgesellschaft, Wirtschaft und Wissenschaft direkt an terminologischen Beschreibungen in Normungs- und Gesetzesdokumenten. Wir haben uns in der Glossar-Gruppe der Aufgabe gestellt, für jeden wichtigen Begriff im Kontext der KI-Thematik eine Liste der Definitionen aus den wichtigsten Normungsdokumenten zusammenzustellen und neben der NRM KI in vollem Umfang zugänglich als „AI-Glossary“ zu veröffentlichen [AIG23].

Neben den häufig genutzten KI-Begriffen mit ihrer Bedeutung und definierenden Normen, wie in Abbildung 2 gezeigt, haben wir zudem grundlegende Fachbegriffe aus den Bereichen bestehender und absehbarer KI-Anwendungen aufgenommen. Dies war für das von der NRM KI abgedeckte breite Spektrum an Fachdisziplinen oft eine sinnvolle Ergänzung. Zusätzlich enthält es aber auch Begriffe aus verschiedenen Fachdisziplinen, die besonders von KI-Entwicklungen betroffen sind oder bald sein werden (wie Informatik, Recht, Soziologie ...), um die interdisziplinäre Kommunikation zu erleichtern.

The image shows two side-by-side entries from the AI-Glossary. The left entry is for 'künstliche Intelligenz' (artificial intelligence) and the right entry is for 'validierung' (validation). Both entries provide multiple definitions from different standards and contexts.

künstliche Intelligenz

künstliche Intelligenz (KI) • artificial intelligence (AI)

Der Begriff **künstliche Intelligenz** wird in verschiedenen Disziplinen aus unterschiedlichen Perspektiven diskutiert. Aufgrund des KI-Effekts entwickelt sich der Begriff stetig weiter. Folgend sind drei Definitionen ausgewiesen:

- Definition 1: Fähigkeit eines technischen Systems, Wissen und Kompetenzen zu erwerben, zu verarbeiten und anzuwenden (ISO/IEC 29119-11)¹.
- Definition 2: Ein computergestütztes System, das kognitiv arbeitet, um Informationen zu verstehen und Probleme zu lösen (ISO/IEC 22989).
- Definition 3: Künstliche Intelligenz bezeichnet eine Reihe von Technologien, [...] die im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen können, die das Umfeld beeinflussen, mir dem sie interagieren (Europäisches KI-Gesetz im Entwurf, EC2021).

1. ISO/IEC 29119-11

► Kopieren ► Exportieren

validierung

Validierung (im Kontext von ML) • validation (in the context of ML)

Validierung, auch bezeichnet als ML-Modelloptimierung oder Model-Tuning, bezeichnet im Kontext von ML die Prüfung trainierter ML-Modelle durch Validierungsdaten. Dadurch lässt sich die Güte der trainierten ML-Modelle erkennen, vergleichen und optimieren (→ siehe Hyperparameter). Insbesondere lässt sich meist erkennen, ob das ML-Modell auf unbekannte Daten generalisieren kann, oder auf die Trainingsdaten übertrainiert wurde (Überanpassung), vergleichbar mit einem "Auswendiglernen" aller Trainingsfragen samt korrekter Antworten. Dieser Schritt grenzt sich von der Definition der Validierung im Kontext der System- und Produktentwicklung ab, da es bei der Validierung im ML-Kontext lediglich um einen Zwischenschritt im Trainingsprozess und nicht um eine unmittelbare Überprüfung des final Modells bzw. der System- bzw. Produkthanforderung handelt (→ Validierung im Kontext System- und Produktentwicklung)

► Kopieren ► Exportieren

Validierung (im Kontext System- und Produktentwicklung) • validation (in the context of system or product development)

Validierung im Kontext von System- und Produktentwicklung ist die Bestätigung durch die Erbringung eines objektiven Nachweises, dass die Anforderungen an einen bestimmten Verwendungszweck oder eine bestimmte Anwendung erfüllt worden sind

Abb. 2: Selbst identische Begriffe aus der Welt der KI können unterschiedliche Definitionen in verschiedenen Standards haben. Hier zwei Beispiele aus dem AI-Glossary [AIG23] mit Verweisen auf verschiedene Quellen (links der Begriff „KI“) oder in unterschiedlichem Kontext (rechts der Begriff „Validierung“)

terschiede in der Begriffsbildung gezielt herausgearbeitet. Damit liefert das AI-Glossary die Möglichkeit, einen weitreichenden Überblick über die Begriffswelt im Bereich KI zu erhalten. Es bildet so eine Basis für einen Vergleich, eine konsistente Verwendung und auch eine weitere Vereinheitlichung der Begriffe. In der konkreten Anwendung kann das Glossar als eine einheitlich genutzte Referenz im Zuge gemeinsamer Arbeiten sowie der organisatorischen Abstimmung zwischen und innerhalb von Teams genutzt werden. Im Zuge organisatorischer Arbeiten bietet das Glossar eine Orientierung für umzusetzende Anforderungen an Produkte und Dienste sowie die damit zusammenhängenden operativen Schritte.

Es ist direkt als Webseite kostenfrei verfügbar, auf der man nach passenden Begriffen suchen kann. Somit ist ein sehr universeller Zugang zu der vollständigen Liste der Begriffe gesichert. Uns ist wichtig, dass das AI-Glossary in zitierfähiger Form vorliegt. Deshalb werden dedizierte Stände freigegeben werden, die als Version eindeutig referenziert werden können. Das AI-Glossary beinhaltet damit auch die Möglichkeit, den Stand der Entwicklungen in diesem sehr dynamischen Umfeld widerzuspiegeln. Zudem wollen wir die Funktionalität in weiteren Stufen ausbauen. Das betrifft insbesondere erweiterte Such- und Filterfunktionen, mit denen Begriffe aus einem bestimmten Unterbereich gezielt gesammelt werden können.

Unterschiedliche Verwendung des Begriffs Validierung

In der Entwicklung einer KI-basierten Anwendung (vgl. Abb. 3) mischen sich die Begriffswelten der klassischen System- und Produktentwicklung mit der des maschinellen Lernens (ML):

Im Bereich ML wird in der Regel ein vorhandener Entwicklungsdatensatz zufällig in drei unterschiedlich große, aber inhaltlich gleichartige Anteile aufgeteilt: den Trainings-, den Validierungs- und den Test-Datensatz. Auf dem Trainingsdatensatz werden Modelle trainiert, es werden also ihre Parameter „gelernt“. Im anschließenden Validierungsschritt wird auf anderen Daten geprüft, ob das Modell auch auf unbekanntem Daten gut genug arbeitet. Ist das nicht der Fall, ist das erst mal kein Problem: Man wählt im Zweifel ein neues Modell oder eine neue Trainingsmethode, oder verändert deren Struktur durch Parameter (Hyperparameter), und trainiert neu. Ist man zufrieden, wird das Ergebnis noch einmal auf dem letzten Teildatensatz, den Testdaten geprüft. Wenn hier die Leistung deutlich schlechter ist, sollte man seinen Ansatz grundsätzlich hinterfragen – aber auf keinen Fall einfach weitere neue Modelle trainieren.

Anschließend wird das Gesamtsystem „integriert“. Das heißt, das ML-Modell wird in das umgebende System, zum Beispiel den Roboter, eingefügt und in Hinblick auf seine Wirkung im Gesamtsystem bewertet. Die erste Prüfung, ob das zusammengesetzte System wie spezifiziert funktioniert, heißt ebenfalls „Test“ (oftmals auch als Verifizierung bezeichnet) – aber in der Welt der Systementwicklung. Hier wird das erfolgreich getestete System anschließend wiederum „validiert“ – um final, zum Beispiel in Wechselwirkung mit echten menschlichen Anwendern, zu prüfen, ob es die ursprünglichen Anforderungen erfüllt. Neben den mehrfachen Dopplungen der Begriffe kommt insbesondere verwirrend hinzu: Die „Validierung“ im Bereich ML geht dem „Test“ voraus. In der Systementwicklung hingegen ist es genau umgekehrt – hier findet der „Test“ zuerst statt, während die „Validierung“ die abschließende Bewertung darstellt (siehe auch [ISO22] und [ISTQB21]).

Konkret profitieren dadurch viele Rollen wie Anwender, Entwickler, Tester, Manager, Architekten oder Entscheider durch eine bessere Kommunikation mit weniger Missverständnissen selbst unter Experten unterschiedlicher Fachdisziplinen. Ergebnis sind typischerweise Produkte besserer Qualität und effizientere Prozesse.

Wir hoffen, dass dieses Glossar, das im Mai – also kurz vor Erscheinen dieses Hefts – verfügbar sein wird, vielen bei der Arbeit mit KI-Systemen hilfreich sein wird und dazu beiträgt, Klarheit in das etwas „babylonische“ Sprachgewirr im Bereich der KI-Terminologie zu bringen.

Literatur und Links

[AIG23] AI-Glossary, entstanden aus der Arbeit an der Deutschen Normungsroadmap KI, Ausgabe 2, s. [DIN22], <https://ai-glossary.org>

[BMW20] BMWK, Strategie Künstliche Intelligenz der Bundesregierung, Fortschreibung 2020, <https://www.bmwk.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-fortschreibung-2020.pdf>

[Cir12] D. Ciresan, U. Meier, J. Schmidhuber, Multi-column Deep Neural Networks for Image Classification, in: IEEE Conf. on Computer Vision and Pattern Recognition, p. 3642–3649, 2012

[DIN22] DIN und DKE, Deutsche Normungsroadmap KI, Version 2, 2022-12-09, <https://www.dke.de/de/arbeitsfelder/core-safety/normungsroadmap-ki>

[EST17] A. Esteva et al., Dermatologist-level classification of skin cancer with deep neural networks, in: Nature, 2017 Feb 2, 542(7639):115–118. doi: 10.1038/nature21056, Epub 2017 Jan 25

[ETSI21] ETSI GR ENI 004 - Experiential Networked Intelligence (ENI). Terminology for Main Concepts in ENI, Version 2.2.1, 2021

[Eur21] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts Com/2021/206 Final, 2021, verfügbar unter: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

[Fur20] J. Furner, Definitions of “metadata”: A brief survey of international standards, in: J. of the Association for Information Science and Technology 71.6 (2020): E33-E42

[ISO20] ISO/IEC TR 29119-11 - Software and systems engineering — Software testing — Part 11: Guidelines on the testing of AI-based systems, 2020

[ISO22] ISO/IEC 22989 - Information technology — Artificial intelligence — Artificial intelligence concepts and terminology, 2022

[ISO23] International Organization for Standardization's Online Browsing Platform, <https://www.iso.org/obp/ui#home>

[ISTQB21] International Software Testing Qualifications Board - Certified Tester AI Testing Syllabus, Version 1, 2021

[Koc01] P. Koch, Bedeutungswandel und Bezeichnungswandel, in: Zeitschrift für Literaturwissenschaft und Linguistik 31.1 (2001): 7–36

[Mea90] C. Mead, Neuromorphic Electronic Systems, in: Proc. of the IEEE 78 (10) (1990) 1629–1636

[Mer99] A. Merwarth et al., Mars Climate Orbiter Mishap Investigation Board Phase I Report, 10.11.1999, https://www.dcs.gla.ac.uk/~johnson/Mars/MCO_report.pdf

[Ope23a] Open AI Plattform, ChatGPT, openai.com/blog/chatgpt/

[Ope23b] Open AI Plattform, DALL•E 2, openai.com/dall-e-2