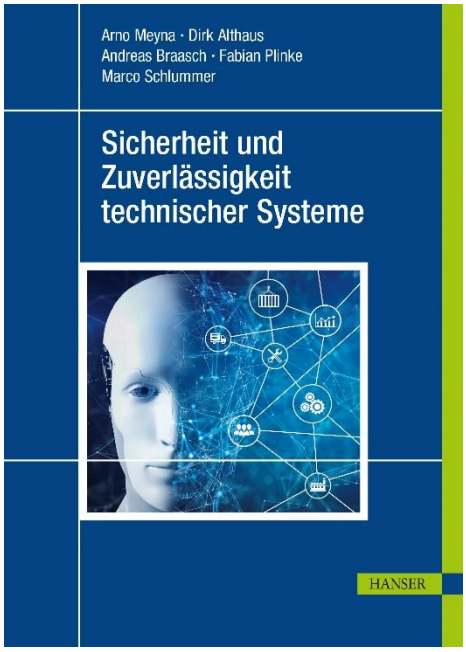
HANSER



Leseprobe

zu

Sicherheit und Zuverlässigkeit technischer Systeme

von Arno Meyna, Dirk Althaus, Andreas Braasch, Fabian Plinke und Marco Schlummer

Print-ISBN: 978-3-446-46003-4
E-Book-ISBN: 978-3-446-46808-5

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446460034
sowie im Buchhandel

Inhalt

Der Verlag und die Autoren haben sich mit der Problematik einer gendergerechten Sprache intensiv beschäftigt. Um eine optimale Lesbarkeit und Verständlichkeit sicherzustellen, wird in diesem Werk auf Gendersternchen und sonstige Varianten verzichtet; diese Entscheidung basiert auf der Empfehlung des Rates für deutsche Rechtschreibung. Grundsätzlich respektieren der Verlag und die Autoren alle Menschen unabhängig von ihrem Geschlecht, ihrer Sexualität, ihrer Hautfarbe, ihrer Herkunft und ihrer nationalen Zugehörigkeit.

Vorwort

Sicherheit und Zuverlässigkeit zählen zu den wichtigsten Anforderungen, die heute an ein technisches System gestellt werden. Das vorliegende Werk zu dieser vielseitigen Thematik wurde durch ein Autorenteam des Instituts für Qualitäts- und Zuverlässigkeitsmanagement GmbH (IQZ) erstellt, das seit vielen Jahren auf dem Gebiet der Sicherheit und Zuverlässigkeit tätig ist und daher über ein breit gefächertes und fundiertes Spezialwissen verfügt.

Das Werk basiert einerseits auf Vorlesungs- und Seminarunterlagen sowie Abschlussarbeiten einschließlich Dissertationen, wobei Teilbereiche davon auch im Lehrbuch von Meyna/Pauli (siehe Lit.) enthalten sind, das ebenfalls im Carl Hanser Verlag publiziert wurde, und andererseits auf Erkenntnissen der vielfältigen industriellen Projekte und dem damit verbundenen Erfahrungsschatz der Autoren.

Die Implementierung, die Erstellung der Bilder, Tabellen etc. sowie die umfangreiche Korrespondenz mit den Autoren und dem Verlag erfolgte durch Frau Xenia Rein, die mit Verve und vielen Anregungen am Gelingen des Werks einen erheblichen Anteil hatte. Dafür möchten sich die Autoren ganz herzlich bei Frau Rein bedanken.

Dem Lektor des Carl Hanser Verlags, Herrn Dipl.-Ing. Volker Herzberg, möchten die Autoren für seine vielen Anregungen und, insbesondere aufgrund der Covid-19-Pandemie, für das entgegengebrachte Verständnis und Vertrauen ihren Dank aussprechen.

Möge das Werk dazu dienen, die dargelegten Erkenntnisse der hochinteressanten Fachdisziplin *Zuverlässigkeits- und Sicherheitstechnik* in Forschung und Lehre sowie insbesondere in der Praxis zu nutzen, weiterzuentwickeln und damit zur Verbesserung der Qualität technischer Produkte einen Beitrag zu leisten.

Wuppertal/Hamburg im Dezember 2022

Arno Meyna
Dirk Althaus
Andreas Braasch
Fabian Plinke
Marco Schlummer

Das Institut für Qualitäts- und Zuverlässigkeits-management (IQZ)

Alle Autoren dieses Buches sind Geschäftsführer bzw. leitende Mitarbeiter des Instituts für Qualitäts- und Zuverlässigkeitsmanagement GmbH (IQZ).

IQZ

Ihr Qualitäts-Zulieferer.

Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH

www.iqz-wuppertal.de

Das IQZ wurde als innovatives Beratungsunternehmen aus der Bergischen Universität Wuppertal heraus gegründet und hat seine Geschäftstätigkeit im Juni 2012 aufgenommen. Das IQZ bietet seinen Kunden wissenschaftsnahe, lösungsorientierte und ganzheitliche Beratungsdienstleistungen, welche den Stand von Wissenschaft und Technik widerspiegeln, unter anderem in folgenden Bereichen:

Durch die enge Kooperation mit der Bergischen Universität Wuppertal und der Hochschule Ruhr West kann das IQZ nicht nur auf innovative Methoden nach Stand von Wissenschaft und Technik zurückgreifen, sondern deckt, durch jahrelange Projekterfahrung im Kontext namhafter Unternehmen, auch mehrere Jahrzehnte Facherfahrung im Sicherheits- und Zuverlässigkeitsmanagement ab. Daher können selbst komplexe Beratungs- und Forschungs-

aufträge durch das IQZ erbracht werden, immer mit dem Fokus, maßgeschneiderte Konzepte für die Kunden zu entwickeln und diese Konzepte pragmatisch in die Praxis umzusetzen.

Neben den Forschungs- und Entwicklungsprojekten im Rahmen des Produktentstehungs- und Produktbeobachtungsprozesses von der Planung, Entwicklung, Produktion, Nutzung bis zur Entsorgung in vielen industriellen Bereichen ist das IQZ seit vielen Jahren auch im Haftungs- und Versicherungsbereich mit Tätigkeiten betraut. Dies beinhaltet z. B. die Haftungsabwehr und Verhandlungsunterstützung im Regressfall oder Gutachtertätigkeiten für Versicherungskonzerne. Namhafte, weltweit agierende Versicherer sowie führende Anwaltskanzleien im Bereich Produkthaftung gehören hier zu unseren langjährigen Partnern.

Das Kundenspektrum des IQZ reicht vom Kleinstunternehmen, kleinen und mittleren Unternehmen (KMU) bis zum DAX-30-Unternehmen z. B. in der Automobil- und Luftfahrtindustrie.

Kontakt

Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH

Heinz-Fangman-Str. 4

42287 Wuppertal

Tel.: +49(0)202/515616 90

Fax: +49(0)202/515616 89

Mail: info@iqz-wuppertal.de

Teil I:

Essenzielle Anforderungen an die Sicherheits- und Zuverlässigkeitstechnik

„Der Mangel an Gewissheit ist die wichtigste Quelle unseres Wissens.“

Carlo Rovelli (1956)*

1 Herausforderungen für Staat, Gesellschaft und Unternehmen

1.1 Fragmente der Explikation der Sicherheits- und Zuverlässigkeitstechnik

Ein kurzer kulturhistorischer Rückblick

Sicherheits- und Zuverlässigkeitstechnik als interdisziplinäres Wissenschaftsgebiet ist eng mit der Entwicklung der Naturwissenschaft und Technik, aber auch mit der Gesellschaft und dem einzelnen Menschen selbst verbunden.

Der moderne Mensch (Homo sapiens, lat. „der weise, kluge Mensch“) wird gegenwärtig auf ein Alter von ca. 233 000 Jahren datiert, bezogen auf Knochen und Schädelfragmente des „Kibish Oma I“ in Ägypten (neue Erkenntnisse von Celine Vidal et al., publiziert in der englischsprachigen renommierten Fachzeitschrift „nature“), und breitete sich vom afrikanischen Kontinent ausgehend nach Europa aus. Nachgewiesen sind der Homo sapiens und der Neandertaler in Vorderasien vor etwa 40 000 Jahren und in Mitteleuropa vor ca. 10 000 Jahren. Die Begleitfunde, wie Pfeilspitzen, Faustkeile, Steinbeile etc., zeigen die enge Verbundenheit des modernen Menschen mit der Technik. Demnach war der Mensch bei seinem Erscheinen auf der Erde sogleich Techniker. Technik ist also menschliche Uranlage (sinngemäß nach Spengler).

Oswald Spengler schreibt weiter (siehe Lit.):

„Um das Wesen des Technischen zu verstehen, darf man nicht von der Maschinentechnik ausgehen, am wenigsten von dem verführerischen Gedanken, daß die Herstellung von Maschinen und Werkzeugen der Zweck der Technik sei.“

Mit der Entwicklung der menschlichen Sprache und der Hochkulturen in Ägypten und Mesopotamien entstand eine neue Qualität der Naturwissenschaft, Technik und Gesellschaft. Es entstanden technische Glanzleistungen, die heute noch bewundert werden, wie z. B. die Pyramiden von Gizeh oder die Megalithbauten in Spanien, deren Errichtung nur durch die systematische Nutzung der damaligen Naturwissenschaft und Technik, verbunden mit einem großen Einsatz von Mensch, Tier und Organisation, ermöglicht wurde.

Im Gegensatz zur „*Techne*“ als Inbegriff allen Könnens, das auf Wissen begründet ist, z. B. Malen und Musizieren als persönliche Fertigkeit, ist die Technik durch Ziele, z. B. Totenkult, und Zwecke, z. B. Bau einer Pyramide, charakterisiert. Nach Dessauer (siehe Lit.) sind technische Objekte durch Raumformen (räumliche Gebilde, ein Gerät, eine Maschine) und Zeit-

formen (eine Methode, ein Verfahren) gekennzeichnet, die aufgrund ihrer Finalität über den technischen Bereich hinausweisen können.

„Technik kann also mit Recht ein Real-Sein und Real-Werden aus Ideen genannt werden, ein dauerndes Hinüberschreiten von Zweckformen aus der Immanenz in die Erfahrungswelt, die hierdurch im Zeitverlauf bereichert wird“ (Dessauer).

Nach Bringmann ist Technik mehr als eine Maschine, ein Produktionsprozess; Technik ist selbst Wissenschaft. Donald Bringmann schreibt hierzu im Werk von Dessauer mit dem Titel „Streit um Technik“ (siehe Lit.):

„Wer in der Technik nur eine angewandte Wissenschaft sieht, lässt das Wesentliche unbetrachtet, das in den technischen Erfindungen und Konstruktionen steckt: jene irrationale seelische Triebkraft, die sich in allen noch so zweckrationalen technischen Gebilden zugleich verbirgt und kundgibt.“

Betrachtet man nun die Entwicklung der Sicherheits- und Zuverlässigkeitstechnik als wissenschaftliche Teildisziplin der Technik, so war und ist diese zunächst final mit der technologischen Entwicklung selbst verbunden. Die frühen Menschen kannten den Nutzen ihrer Waffen und Gerätschaften, aber auch die Gefahren, die mit einer unsachgemäßen Benutzung verbunden waren. Durch die Weiterentwicklung der Technik gelang es den Menschen jedoch, den vielfältigen Urgefahren der Natur und Tierwelt entgegenzutreten und ihre Lebensgrundlage zu sichern.

Nachgewiesen ist auch, dass es zur Zeit der ersten Hochkulturen bereits ein – wie wir heute sagen würden – sicherheitstechnisches Recht gab. Bekannt ist in diesem Zusammenhang der Codex, der unter der Herrschaft des Hammurapi (auch Hammurabi), 6. König der ersten Dynastie (1792 bis 1750 v. Chr.), im altbabylonischen Reich (Babylon wurde 1894/1830 v. Chr. vom semitischen Stamm der Amoriter unter Sumu-abum gegründet) entstand, als älteste bekannte Gesetzessammlung – mit 270 Rechtsgrundsätzen für das tägliche Leben – der Welt, aufgezeichnet auf einer ca. 2,25 m hohen Stele, die 1902 bei Ausgrabungen in Susa gefunden wurde und sich heute im Louvre in Paris befindet (Wikipedia).

Für den Sicherheitstechniker interessant ist in diesem Zusammenhang der Codex der Haftung, welcher in den §§ 228 bis 233 (DIN Mitteilungen, 10/78) beschrieben ist:

- *„Wenn ein Baumeister ein Haus für einen Mann baut und es für ihn vollendet, so soll dieser ihm als Lohn zwei Sekel Silber geben für je ein Sar Haus: (Anm.: 1 Sekel = 360 Weizenkörner = 9,1 Gramm, 1 Sar = 14,88 m²).“*
- *„Wenn ein Baumeister ein Haus baut für einen Mann und macht seine Konstruktion nicht stark, so dass es einstürzt und verursacht Tod des Bauherrn: dieser Baumeister soll getötet werden.“*
- *„Wenn der Einsturz den Tod eines Sohnes des Bauherrn verursacht, so sollen sie einen Sohn des Baumeisters töten.“*
- *„Kommt ein Knecht des Bauherrn dabei um, so gebe der Baumeister einen Knecht von gleichem Wert.“*
- *„Wird beim Einsturz Eigentum zerstört, so stelle der Baumeister wieder her, was immer zerstört wurde; weil er das Haus nicht fest genug baute, baut er es auf eigene Kosten wieder auf.“*
- *„Wenn ein Baumeister ein Haus baut und macht die Konstruktion nicht stark genug, so dass eine Wand einstürzt, dann soll er sie auf eigene Kosten verstärkt wieder aufbauen.“*

Weiter findet sich in der Bibel der Juden (600 bis 200 v. Chr.) (5. Buch Moses, 22/8):

„Wenn du ein neues Haus baust, sollst Du um die Dachterrasse eine Brüstung ziehen. Du sollst nicht dafür, dass jemand herunterfällt, Blutschuld auf Dein Haus laden."

Der vorangehend aufgeführte Codex der Haftung zeigt, dass der Baumeister eines Hauses bereits vor 4000 Jahren die Sicherheit implementierte, d. h. nach heutigem Verständnis „in ein Produkt/einen Produktionsprozess hineinentwickelte". Neben den Gefahren durch die Technik war der Mensch seit jeher einer Vielzahl natürlicher Gefahren einschließlich gesellschaftsbedingten und politischen Gefahren – wie die vielen Kriege und die damit verbundenen schrecklichen Auswirkungen zeigen – ausgesetzt. Nach Heidegger[1] ist die menschliche Existenz ein *„Sein zum Tode"*. Unbestritten ist jedoch, dass die stetig fortschreitende technische Zivilisation umfassende ökonomische, medizinische und soziale Vorteile mit sich brachte, ein „menschenwürdiges Leben" ermöglichte und zu einer erheblichen Verlängerung des menschlichen Lebens führte. Diese Kohärenz von Mensch und Technik als Grundpfeiler von Lebensqualität, Freiheit und Entfaltung wurde mit der Entwicklung großtechnischer Systeme und deren möglichen negativen Auswirkungen für Mensch und Umwelt, die sich aufgrund neuer naturwissenschaftlicher und technischer Erkenntnisse feststellen ließen, zu Beginn des 20. Jahrhunderts zur Inkohärenz und ist heute Gegenstand kontroverser Diskussionen über das „Für und Wider der Technik".

Ratzinger schrieb hierzu (siehe Lit.):

„Wenn es zutrifft, daß der innere Ausgangspunkt der Technik in der Erringung von Freiheit durch Gewähren von Sicherheit lag, so muß es von da aus auch die innere Forderung jeder technischen Entwicklung und ihr eigenes Leitmaß sein, sie so zu gestalten, daß daraus nicht größere Unsicherheit und in der Steigerung von Abhängigkeiten größere Unfreiheit entsteht. Sie wird dabei erkennen müssen, daß nicht (wie es anfangs aussah) technisches Tun als solches schon befreiendes und damit sittliches Tun ist, daß aber technisches Tun von sittlichen Maximen geleitet sein muß, um seinem eigenen Ursprung zu genügen, der in einer sittlichen Idee lag."

Die systematische Analyse von Gefahrenpotenzialen gleich welcher Art, denen der Mensch in seinem Dasein ausgesetzt ist, deren Risiken er bewusst oder unbewusst eingeht, und die Entwicklung von entsprechenden Schutz- und Verhaltensmaßnahmen zu deren Bewältigung sind seit jeher Aufgabe der entsprechenden wissenschaftlichen Fachdisziplinen der Naturwissenschaft, Ingenieurswissenschaft, Mathematik, Geistes- und Gesellschaftswissenschaft, Medizin und Psychologie sowie deren Spezialisierungen, da nur in diesen das entsprechende Fachwissen vorhanden ist.

Allerdings zeigte es sich, dass die methodische und inhaltliche Fokussierung auf eine oder mehrere Fachdisziplinen der Bedeutung der Sicherheit für den einzelnen Menschen, aber auch die Gesellschaft mit ihrem ethischen, humanen, wirtschaftlichen und politischen Grundverständnis nicht gerecht wird. Hierzu schrieben Peters und Meyna im Vorwort (siehe Lit.):

„Die Sicherheitstechnik ist eine interdisziplinäre Wissenschaft, deren Schwerpunkt traditionell die Ingenieurswissenschaften bilden. Aber auch die Human- und Sozialwissenschaften, Recht, Ökonomie, Management, Personen- und Objektschutz, Rettungswesen, Umweltschutz, Datenschutz u. a., leisten heute einen nicht unerheblichen Beitrag zur Reduzierung und Bewertung des Risikos und der sicheren Nutzung eines Mensch-Maschine-Umwelt-Systems."

[1] Martin Heidegger (1889 – 1976)

Risiko in der modernen globalen Industriegesellschaft

Wie bereits dargelegt, sind der Mensch in seinem Dasein und die Gesellschaft vielfältigen natürlichen und zivilisationsbedingten Risiken ausgesetzt. Die Herkunft des Begriffs Risiko ist nicht eindeutig geklärt. Vielfach wird von einem arabischen Ursprung mit dem Ausdruck „risqu“ (von Gottes Gnaden abhängiger Lebensunterhalt) bzw. vom im Mittelalter ins Italienische übernommenen „risico“ (Wagnis, Gefahr bei einer Schiffsreise oder militärischen Unternehmen) ausgegangen.

Mit Risiko wird heute in der Regel das Produkt aus der Eintrittswahrscheinlichkeit eines bestimmten Ereignisses und dem Schadensausmaß (Ereignisschwere) bezeichnet (siehe Abschnitt 9.4).

Durch Logarithmierung und Darstellung als Geradengleichung erhält man eine Gerade gleichen Risikos (Bild 9.5). Das heißt, ein formal gleiches Risiko tritt bei geringer Eintrittswahrscheinlichkeit und großen Auswirkungen (z. B. bei einem Flugzeugabsturz), aber auch bei einer großen Eintrittswahrscheinlichkeit und geringeren Auswirkungen (z. B. im Straßenverkehr) ein.

Interessant ist in diesem Zusammenhang, dass in der Bevölkerung bezüglich des Erstgenannten eine Risikoaversion besteht. Es wurde deshalb vorgeschlagen, einen Risikoaversionsfaktor in die Risikobeurteilung einzufügen. Allerdings fehlt hierfür die wissenschaftliche Grundlage. Problematisch ist jedoch, dass vielfach von „punktförmigen“ Risiken, z. B. Toten/Jahr und Einwohnern, ausgegangen wird und entsprechende Vergleiche z. B. für tödliche Arbeitsunfälle nach Wirtschaftszweigen oder Vergleiche von statistisch abgesicherten natürlichen Risiken mit probabilistisch ermittelten technischen Risiken (z. B. Kernkraftwerke) erfolgen, um so eine gewisse Akzeptanz zu ermöglichen (siehe deutsche Risikostudie, „Kernkraftwerke“, siehe Lit.).Geht man davon aus, dass die Eintrittshäufigkeit (Wahrscheinlichkeit) durch eine entsprechende Verteilungsfunktion und die Ereignisschwere durch eine weitere entsprechende Funktion gegeben ist, so ist auch das Risiko durch eine entsprechende Zeit-Orts-Funktion gegeben.

Das zivilisationsbezogene Risiko ist immer mit einer menschlichen Handlung verbunden, deren Folgen nicht absehbar sind. Es müssen vielfach Entscheidungen getroffen werden, auch dann, wenn nicht alle Fakten und Sachverhalte überprüfbar und bekannt sind. Als weiterer Faktor ist die Kontrollierbarkeit der möglichen Folgen (z. B. von Atomkraft, Gentechnik, neuen Technologien → Technikfolgenabschätzung) von großer Bedeutung. Problematisch ist aber auch die Bewertung der zukünftigen Eintrittswahrscheinlichkeit eines Ereignisses aus den bisher ermittelten, zumal sich die Randbedingungen ständig ändern können. Ferner ist die Freiwilligkeit, mit der der Einzelne oder bestimmte gesellschaftliche Gruppierungen ein Risiko eingehen, von Bedeutung. So gesehen stellt das Risiko eine mehrdimensionale Größe dar.

Der Begriff des Risikos wird oft synonym zum Begriff der Gefahr (gevare, mittelhochdeutsch „Hinterhalt“, „Betrug“) verwendet. Die Gefahr als Möglichkeit eines zukünftigen Schadens oder Nachteils ist im Gegensatz zum vordefinierten objektiven Risiko eine qualitative Größe für die Kennzeichnung einer natürlichen oder zivilisationsbedingten Gefahrenquelle. Diese sind nicht immer latent vorhanden und können unbekannt sein.

Als komplementäre Größe wird vielfach der Begriff der Sicherheit verwendet. Im Sinne der Sicherheitstheorie ist die additive Verknüpfung von Sicherheitswahrscheinlichkeit und Gefährdungswahrscheinlichkeit durch eins gegeben (siehe Abschnitt 9.4). Das heißt, wenn

keine Gefährdung vorliegt, z. B. keine Lawinengefahr im Mittelgebirge im Sommer, so ist die Sicherheit durch 100 % (d. h. eine absolute Sicherheit) gegeben.

Mit dem Begriff der Gefahr werden häufig zeitliche Abstände, z. B. eine konkrete Gefahr, eine aktuelle Gefahr, eine Gefahr im Verzug, und Wahrscheinlichkeiten, wie z. B. eine abstrakte Gefahr, miteinander verknüpft. In diesen Fällen ist die Quantifizierung über das objektive Risiko aussagefähiger. Dabei ist zu beachten, dass ein Risiko nur dann vorhanden ist, wenn eine Gefahr und eine Exposition gegenüber derselben gegeben sind. So sind beispielsweise die Gefahren des Straßenverkehrs für den Nichtteilnehmer irrelevant, für die Gesellschaft aber sehr bedeutend. Das heißt, eine Gefahr ist in der Regel immer durch einen örtlich und zeitlich begrenzten Gefahrenwirkungskreis charakterisiert, wobei dieser jedoch fließend und global wirkend sein kann (z. B. Atomkatastrophen von Tschernobyl, 1986, Fukushima, 2011, Giftgasunfälle in Seveso, 1976, und Bophal, 1984).

Die örtlichen und zeitlichen Auswirkungen können auch den Lebensraum für nachfolgende Generationen stark einschränken. Das bedeutet aber auch, dass zu den global wirkenden natürlichen Katastrophen (Klima, Krankheiten, Seuchen und andere) und den durch die Gesellschaft selbst verursachten Katastrophen (z. B. Krieg, Terrorismus) eine neue Qualität des Risikos, begründet durch den naturwissenschaftlichen und technischen Fortschritt, hinzugekommen ist.

Nach Bieri ist Risiko ein Bestandteil des menschlichen Daseins, eine risikofreie Lebensform ist nicht denkbar und gleichbedeutend mit dem Tod. Ernst Bieri (siehe Lit.) schreibt hierzu treffend:

„Kein Leben und damit auch keine Technik ohne Risiko: Man kann und soll das Risiko durch den Einsatz des verfügbaren Wissens und Könnens auf ein Minimum herabdrücken, und diese Marschrichtung ist von der Technik eingeschlagen worden, von der Verbesserung der Maschinen in den Fabriken über die Verkehrsmittel aller Art, bis zu den Anlagen für Energiegewinnung und den Umweltschutz. Aber jedes Risiko vollständig und für alle Zukunft ausschalten zu wollen, das wäre Hybris, wäre die Anmaßung der Allmacht durch den Menschen. Das Ende der von uns überblickbaren Risiken tritt mit dem Tod ein. Wer also jedes Risiko ausschalten will, beendet das menschliche Leben, das ohne Risiko, ohne Angst, aber auch ohne den dauernden und über weite Strecken erfolgreichen Kampf dagegen nicht möglich ist.“

Die Ermittlung von Gefahrenpotenzialen und Risiken bis zu einem gewissen Grad beherrschbar zu machen, ist eine interdisziplinäre Aufgabe der Sicherheits- und Zuverlässigkeitstechnik. Allerdings tritt in diesem Zusammenhang sofort die Frage nach der Akzeptanz eines verbleibenden Risikos auf, d. h. das Abwägen zwischen dem Nutzen (z. B. einer neuen Technologie, eines neuen Medikamentes) und den möglichen Schäden für den Menschen und seinen Lebensraum (Arbeitswelt, Umwelt, Gesundheit und anderes). Als Beispiel hierzu sei die kontrovers geführte Diskussion über das Für und Wider der Kernenergie aufgeführt. Das Beispiel zeigt auch die zeitliche Veränderbarkeit der Bewertung von Risiken durch die Gesellschaft und insbesondere durch bestimmte Gruppierungen der Gesellschaft, unabhängig von neuen wissenschaftlichen Erkenntnissen. Karl Steinbuch schreibt hierzu (siehe Lit.):

„Die Akzeptanz technischer Risiken hat drei Dimensionen:

Erstens die technische Dimension: Die Verminderung technischer Risiken durch Menschen, Methoden oder Material.

Zweitens die pädagogische Dimension: Die Aufklärung über die Zwangsläufigkeit mancher Risiken.

Drittens die ethische Dimension: Die Erzeugung von Verantwortung und Vertrauen.

Auf diesem Gebiet wurde in den letzten Jahren vieles versäumt – wir alle werden hierunter leiden: Das Vertrauenspotential entscheidet über den erreichbaren Wohlstand – die Zerstörung des Vertrauenspotentials (z. B. durch Konfliktideologie oder Skandalpublizistik) führt zwangsläufig zur Verminderung unseres Wohlstandes."

Das Erkennen einer Gefahr und die Beurteilung des Risikos mit seiner Eintrittswahrscheinlichkeit und den möglichen Schadensauswirkungen ist a priori immer mit mehr oder weniger großen Unsicherheiten verbunden, da besonders bei seltenen Ereignissen eine statistische Verifizierung nicht möglich ist. Folglich gibt es kein sogenanntes „Restrisiko" und „Sicherheitsrisiko". Dies gilt auch für die Schadensauswirkungen.

Thomas A. Jäger schreibt hierzu (siehe Lit.):

„Die lange Inkubationszeit der physischen Schädigung des Menschen durch schleichend akkumulierende Umwelteinflüsse, wie Wasser- und Luftverschmutzung oder durch in Nahrungsmitteln enthaltene Schadstoffe, macht das Erkennen der Zusammenhänge schwierig. Das gleiche gilt für die physische und psychische Schädigung durch Lärm. Der Nachweis gesundheitlicher Schädigungen ist umso schwieriger, als die Symptome schleichend und nicht eindeutig und ihre Quellen überaus vielfältig sind. Wenn jemand durch schädigende Umwelteinflüsse in seiner Vitalität herabgesetzt oder gar krank ist, so fällt dies lange Zeit nicht weiter auf und die Ursachen bleiben im Nebel."

Ungeachtet dessen zeigen die in diesem Zusammenhang vielfältig eingesetzten wissenschaftlichen Methoden, Verfahren, Simulationen und anderes zur Sicherheit, Zuverlässigkeit, Gesundheit, Umweltverträglichkeit, Schutz, dass Risiken objektiviert und minimiert werden können. Das Grundgesetz der Bundesrepublik Deutschland sagt hierzu in Artikel 1 unmissverständlich:

„(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

Zum Paradigma der Sicherheits- und Zuverlässigkeitstechnik

Aufgrund der zuvor erläuterten engen Verknüpfung der Sicherheits- und Zuverlässigkeitstechnik mit den Natur- und Technikwissenschaften und deren deterministischem Weltbild (jeder Vorgang hat eine Ursache, die Wirkung kann sich höchstens mit der endlichen Lichtgeschwindigkeit ausbreiten) ist dieser Kausalnexus des klassischen Determinismus auch Paradigma der Sicherheits- und Zuverlässigkeitstechnik.

Die Determiniertheit der Welt und des Menschen im Kontext von „Willensfreiheit und bedingtem freien Willen" ist bis in unsere heutige Zeit Gegenstand philosophischer, psychologischer, neurophysiologischer und anderer Betrachtungen.

Ungeachtet dessen ist der naturwissenschaftliche und technische Fortschritt seit Newton[2] und Laplace[3] durch den Determinismus geprägt. Nach Laplace ist die Zukunft durch die Gegenwart (Anfangsbedingung z. B. einer Differenzialgleichung) eindeutig bestimmt (siehe

[2] Isaac Newton (1643 – 1727)

[3] Pierre-Simon Laplace (1749–1827)

auch das Gedankenkonstrukt des „Laplaceschen Dämons“ als einer „Intelligenz“, die befähigt ist, alle Determinationen und Faktoren in Vergangenheit und Zukunft genauestens zu kennen). Dem gegenüber steht das indeterministische Weltbild der Quantenmechanik (Heisenberg[4], Born[5], Schrödinger[6] und andere), d. h. die Nichtbestimmtheit der Ursachen bei physikalischen Vorgängen – Zukunft ist nur durch stochastische Modellbildung (Zufalls-Prozess) bestimmbar –, welches in Widerspruch zum Laplaceschen Weltbild steht (siehe auch 2. Hauptsatz der Thermodynamik). Man beachte in diesem Zusammenhang aber auch die streng deterministische Position von Albert Einstein[7] „Gott würfelt nicht“ (sinngemäß aus dem Briefwechsel mit Max Born (siehe Lit.)), die heute jedoch für den Mikrokosmos als widerlegt angesehen wird.

Ähnlich wie in der Physik fand unter anderem durch die Arbeiten von Wöhler, Weibull (siehe Lit.) und weiteren Autoren im Bereich der Werkstoffermüdung und insbesondere in den 40er- und 50er-Jahren durch Pieruschka und Lusser die Stochastik als „Systemdenken“ Einzug in die Ingenieurswissenschaften. So schreibt Pieruschka, der sein Buch Robert Lusser widmete, im Vorwort (siehe Lit.):

„In the year 1943, the author became, for the first time, aware of the reliability problem during flight testing of the German V-1 missile. Intensive studies of this subject were started in 1954 upon coming to the United States. In the subsequent eight years, the author has completed a great amount of study in the field of reliability theory as research scientist with the Army Rocket and Guided Missile Agency, Redstone Arsenal, Alabama, and with the Lockheed Missile and Space Company, Sunnyvale, California.“

Weiter heißt es auf Seite 47:

„The Swiss mathematician Jakob Bernoulli developed the rule which published 1713. Robert Lusser has been stressing the serious consequence of the product rule in the achievement of reliability in complex equipments since the year 1950, and by this insistence has brought into being reliability as a serious profession. Therefore, Formula (siehe Formel 13.1) is called Robert Lusser's reliability formula.“

Die zweite Auflage des 1962 erschienenen Buches von Igor Bazovsky (siehe Lit.) stellt ebenfalls die Pionierleistungen von Lusser (Seite 275) und Pieruschka (Seiten 60 und 71) heraus.

„Another historical development in the same direction took place in Germany during the Second World War. Robert Lusser, one of the reliability pioneers, narrates how he and his colleagues, while working with Wernher von Braun on the V1 missile, met with the reliability problem. The first approach they took towards V1 reliability was that a chain cannot be stronger than its weakest link. Thus, the missile will be as reliable as the weakest link can made, or as strong.“

Nicht unerwähnt sei, dass bereits 1954 (danach jährlich) in den USA das 1. National Symposium on Reliability and Quality Control der IEEE und in Deutschland 1961 (danach alle zwei Jahre) die erste Tagung über Zuverlässigkeit stattfand. Auf Anregung von Ludwig Bölkow, einem der großen Förderer der Deutschen Zuverlässigkeit (siehe Lit.), wurde bereits

4) Werner Heisenberg (1901–1976)

5) Max Born (1882–1970)

6) Erwin Schrödinger (1887–1961)

7) Albert Einstein (1879–1955)

1964 der Fachausschuss „Zuverlässigkeit und Qualitätskontrolle“ beim VDI gegründet. Es entwickelte sich die Zuverlässigkeitstheorie als stochastische Theorie zur Bewertung komplexer Mensch-Maschine-Umweltsysteme. Das Paradigma der Zuverlässigkeitstheorie ist das stochastische Ausfall- bzw. Lebensdauerverhalten von Komponenten und Systemen. Das heißt, die Lebensdauer einer Komponente – wie die des Menschen – ist eine Zufallsvariable. Die Zuverlässigkeitstheorie verfügt wie in diesem Buch dargestellt über ein theoretisches Konzept, einschließlich Methoden, Verfahren und Kenngrößen zur qualitativen und quantitativen Bewertung technischer Systeme gleich welcher Art. Da die Sicherheit als Teilmenge der Ausfall- und Betriebszustände eines Systems angesehen werden kann, ist diese isomorph; das bedeutet, das theoretische mathematische Gebäude der Zuverlässigkeitstheorie bildet auch das theoretische Gebäude der stochastischen Sicherheitstechnik. Die stochastische Modellbildung kann allerdings eine deterministisch orientierte Sicherheits- und Zuverlässigkeitstechnik nicht ersetzen, sondern ermöglicht a priori eine Bewertung im frühen Entwicklungsstadium und im Rahmen des Produktentstehungsprozesses (siehe Kapitel 4) und der Test- und Prüfplanung (siehe Kapitel 27). Die vorangegangenen Betrachtungen zeigen, dass die Paradigmen der Sicherheits- und Zuverlässigkeitstechnik durch den Nexus von Determinismus und Indeterminismus geprägt sind. Allerdings fehlt in diesen Paradigmen eine Unbekannte, und dies ist der Mensch als Individuum und Mittelpunkt des Seins, eingebunden in Gesellschaft, Umwelt, Technik mit all ihren kulturellen und traditionellen Unterschieden. Albert Kuhlmann schlägt deshalb einen „kybernetischen“ Ansatz der Sicherheitswissenschaft vor (siehe Lit.):

„Die Verknüpfung zwischen Kybernetik und Sicherheitswissenschaft ergibt sich daraus, dass technische Einrichtungen von Menschen bedient und kontrolliert werden, die sich selbst im Wirkungsbereich dieser technischen Einrichtung befinden. Sie nutzen die Maschine, sind aber auch ihren Gefahren für Leib, Leben und Sachen ausgesetzt. Das menschliche Verhalten sowie das Verhalten der Maschine sind wiederum von den Bedingungen der Umwelt abhängig. Die Umwelt technischer Einrichtungen wird ihrerseits oft von ihnen vielfältig beeinflusst, z. B. durch die Abgabe von Abfällen, Abwässern, Lärm und luftfremden Stoffen. Der Mensch wiederum kann Einfluss nehmen auf derartige Umweltfaktoren. Jede technische Einrichtung ist deshalb eingebettet in ein durch Wechselwirkungen gekennzeichnetes Mensch-Maschine-Umwelt-System.“

Laut Kuhlmann befasst sich die Sicherheitswissenschaft mit der Sicherheit vor möglichen Gefahren bei der Nutzung der Technik, nicht aber mit militärischer und sozialer Sicherheit oder mit der Sicherheit vor Krankheit, die nicht von der Technik verursacht wird.

„Das Ziel der Sicherheitswissenschaft besteht darin, Schadwirkungen bei der Nutzung der Technik so klein wie möglich oder wenigstens in vorgegebenen Grenzen zu halten. Unter Schadwirkungen sollen dabei sowohl unfallartige als auch solche Schäden verstanden werden, die z. B. infolge von Umweltbelastungen durch technische Anlagen entstehen können.“

Der Begriff der Sicherheitswissenschaft ist bei Kuhlmann technikbezogen. Das heißt, ein Schutz vor Gefahren, die nicht durch die Technik verursacht sind, ist nicht Gegenstand der Sicherheitswissenschaft. Hierzu ist anzumerken, dass eine klare Trennung zwischen den einzelnen zivilisationsbedingten und den natürlichen Risiken nicht immer möglich ist (zum Beispiel beim Klimawandel). Die Verwendung des Terminus Sicherheitswissenschaft statt Sicherheitstechnik ist strittig. Wie zuvor erläutert, ist die Technik allgemein und damit auch die Sicherheitstechnik eine Wissenschaftsdisziplin, die allerdings als eine interdisziplinäre multifakultative Disziplin anzusehen ist. Unstrittig ist jedoch, wie bereits erwähnt,

dass der Mensch eine besondere Herausforderung für die sicherheits- und zuverlässigkeitstechnische Gestaltung und Nutzung eines Mensch-Maschine-Umwelt-Systems darstellt. Neben den Paradigmen Determinismus und Indeterminismus sei hier von einem **Humankompatibilismus** als drittes Paradigma ausgegangen. Im Gegensatz zum sogenannten „human factor" – gekennzeichnet durch die Anpassung „Mensch/Maschine", geprägt durch psychologische, medizinische und andere Erkenntnisse – soll das hier neu eingeführte Paradigma „Humankompatibilismus" auch die Anpassung „Maschine/Mensch" (human engineering) durch das Wissensgebiet der Ergonomie und Anthropotechnik mitberücksichtigen. Des Weiteren sollen die Wissenschaftsdisziplinen, die sich mit den Gefahrenpotenzialen und deren Reduzierung bei der Herstellung und Nutzung technischer Systeme gleich welcher Art auseinandersetzen, Bestandteil des Humankompatibilismus sein. Hierzu zählen insbesondere die Verkehrssicherheit, Arbeitssicherheit, Arbeitsmedizin, Arbeitsphysiologie, Pädagogik und andere Disziplinen. Dieses hier neu eingeführte Paradigma „Humankompatibilismus" berücksichtigt die physischen, psychischen, geistigen und anderen Eigenschaften des Menschen im Sinne einer teleologischen Interaktion mit der Technik und der damit verbundenen Umwelt. Alle drei Paradigmen zusammen charakterisieren aber auch die Bereiche Umweltschutz, Personen- und Objektschutz, Rettungswesen (Sicherungswesen, Brand- und Explosionsschutz, Unfallrettungswesen, persönliche Schutzausrüstung, Katastrophen- und Zivilschutz, Evakuierung und anderes), Qualitätssicherung, Risk-Management, Datenschutz und das sicherheitstechnische Recht als sich stetig verändernde Festschreibung sicherheitstechnischer Erkenntnisse.

1.2 Aktuelle Herausforderungen

Die aktuellen Herausforderungen im Kontext Sicherheit und Zuverlässigkeit sind durch die medienwirksamen Schlagwörter „Digitalisierung", „Industrialisierung 4.0 und Robotik" und in diesen eingebettet „Künstliche Intelligenz" (KI) geprägt. Die industriellen Entwicklungen und Innovationen in diesen Bereichen bilden ein großes Potenzial zur Verbesserung der Lebensqualität in allen Bereichen des menschlichen Daseins. Damit eng verbunden sind jedoch auch vielfältige Fragestellungen im Sinne von Safety und Security.

Aufgabe von Staat, Gesellschaft, Industrie, Wissenschaft ist es, diese zu konstatieren und die mit jeder neuen technologischen Entwicklung verbundenen Gefahren, Risiken für den Einzelnen und die Gesellschaft zu bewerten, zu minimieren und in diesem Zusammenhang entsprechende gesetzliche Rahmenbedingungen zu schaffen.

Mit diesen Herausforderungen sind insbesondere die in Forschung und Entwicklung tätigen Wissenschaftler und Ingenieure konfrontiert. Hier gilt es neue Ansätze und Verfahren zur Bewertung, Validierung und Verifizierung der Sicherheit, Zuverlässigkeit, Verfügbarkeit und anderer Kategorien bereitzustellen.

Dabei bildet die sogenannte „Künstliche Intelligenz" (KI) einen zentralen Baustein, der durch ständig wachsende Entwicklungen und Anwendungen im Kontext des maschinellen Lernens, bei Perzeption, Entscheiden, Handeln, Kommunikation etc. als „schwache KI" geprägt ist.

Hierzu gehören aktuell unter anderem die Themenkomplexe

- Robotik, Steuerung, Regelung, Expertensysteme,
- autonomes Fahren,
- Sprach- und Textverarbeitung,
- Bild- und Spracherkennung,
- Mustererkennung
- etc.

Für den Bereich der Technischen Zuverlässigkeit gehören hierzu die Themen

- Zuverlässigkeitsplanung und -prüfung (allgemein),
- Predictive Maintenance,
- Fehlerdetektion,
- Ausfallratenbestimmung, Schwachstellenanalyse,
- Struktur- und Systemanalyse
- etc.

Heute wird KI bereits in vielen Branchen wie

- Industrie (Produktion, Fertigung, Qualitätssicherung, Steuerungs- und Regelungstechnik, Robotik und Vernetzung),
- Verkehrsträger (Schiene-, Luft-, Straßenverkehr und autonomes Fahren sowie deren Vernetzung),
- Energiewirtschaft (Steuerung und Optimierung, Netzbetrieb, Kraftwerksteuerung, prädiktive Wartung und Instandhaltung, Vertrieb etc.),
- Wirtschaft und Finanzwelt,
- Medien und Bildungsbereich (Textanalyse, digitale Assistenten, Crawling und Indexierung, Blockchain-Technologie, Video Content Marketing etc.),
- Medizin (Bildgebung, Diagnose, CT, Telemedizin, Neuroprothetik, Exoskelett etc.),
- Militär (autonome Waffensysteme, Strategieentwicklung, Entscheidungsfindung etc.),
- Jurisprudenz (Vertragsgestaltung und -prüfung, Recherche, Prozessvorbereitung, Handlungs- und Entscheidungsempfehlungen)
- etc.

erfolgreich eingesetzt.

Für das multi-fakultative Fachgebiet *Künstliche Intelligenz (KI)* gibt es, aufgrund des nicht fassbaren Begriffs der natürlichen Intelligenz im etymologischen Sinne, zahlreiche Definitionen. Prinzipiell verfolgt KI das Ziel die Attribute der kognitiven analogen Eigenschaften des Menschen durch eine digitale lernfähige Maschine nachzubilden.

Als Begründer der KI wird allgemein der Informatiker John McCarthy[8] angesehen, der 1956 am Dartmouth College in Hanover (New Hampshire, USA) einen Workshop mit dem Titel „Dartmouth Summer Research Project on Artificial Intelligence“ organisierte. McCarthy verweist allerdings selbst auf Alan Turing[9], einen der Gründungsväter der modernen Computertechnologie, der Informatik und damit der KI (Turing-Maschine, Turing-Test). Im deutschsprachigen Raum wird allgemein Karl Steinbuch[10] als einer der Pioniere der Kybernetik (Begründer Norbert Wiener[11]) und Künstlichen Intelligenz (maschinelles Lernen) und Namensgeber der Informatik als neue akademische Fachdisziplin, hervorgegangen aus der Kybernetik, angesehen (zur Geschichte der Entwicklung siehe Erhard Konrad, siehe Lit.).

Auch wenn die besonders in den letzten Jahren aufgrund verbesserter Rechentechnologien erzielten KI-Erfolge beeindruckend sind, ist der Weg zur sogenannten *„starken KI“,* d. h. der Adaption der gesamten kognitiven Fähigkeiten des Menschen im Sinne des Analogon Mensch-Maschine, noch durch viele Meilensteine gekennzeichnet. So schreibt Bernd Vowinkel in seinem Buch *Maschinen mit Bewusstsein* (siehe Lit.), Kapitel 1, Natürliche Intelligenz:

„Bei Fragen der Leistungsfähigkeit und der Eigenschaft von künstlicher Intelligenz wird in der Regel der Mensch als Maß aller Dinge zum Vergleich herangezogen. Das trifft insbesondere auf die Eigenschaften zu, die es bei der künstlichen Intelligenz noch nicht gibt, nämlich Bewusstsein, Vernunft und freier Wille.“

Ob es jemals eine *„starke KI“* geben wird, ist strittig, obwohl ernst zu nehmende Wissenschaftler sich bereits mit dem nächsten Schritt einer *„super KI“* und dessen Auswirkungen auf die Menschheit gedanklich auseinandersetzen. Das Gleiche gilt für neurobiologische Forschungen und die Prämissen zur Entwicklung einer *„humanen Überintelligenz“* aufgrund von Quantenvorgängen im Gehirn. Unstrittig ist jedoch die Weiterentwicklung von KI und deren Verknüpfung mit der menschlichen Willenskraft (Nervensystem und Gehirnaktivität) zu einer gewissen *„hybriden Intelligenz“*, die es bereits heute ermöglicht, Schwerstbehinderten eine gewisse Beweglichkeit zurückzugeben, z. B. als Exoskelett-Hand (Neuroprothetik, neuronal gesteuerte Robotik). In diesem Kontext zeigt Bild 1.1 eine mögliche Illustration.

Auch sind sich Wissenschaftler darin einig, dass die Weiterentwicklung und Nutzung von Quantencomputern die KI stark beeinflussen wird (siehe Förderprogramm des BMBF zur Quantentechnologie).

[8] John McCarthy (1927 – 2011)

[9] Alan Turing (1912–1954)

[10] Karl Steinbuch (1917–2005)

[11] Norbert Wiener (1894–1964)

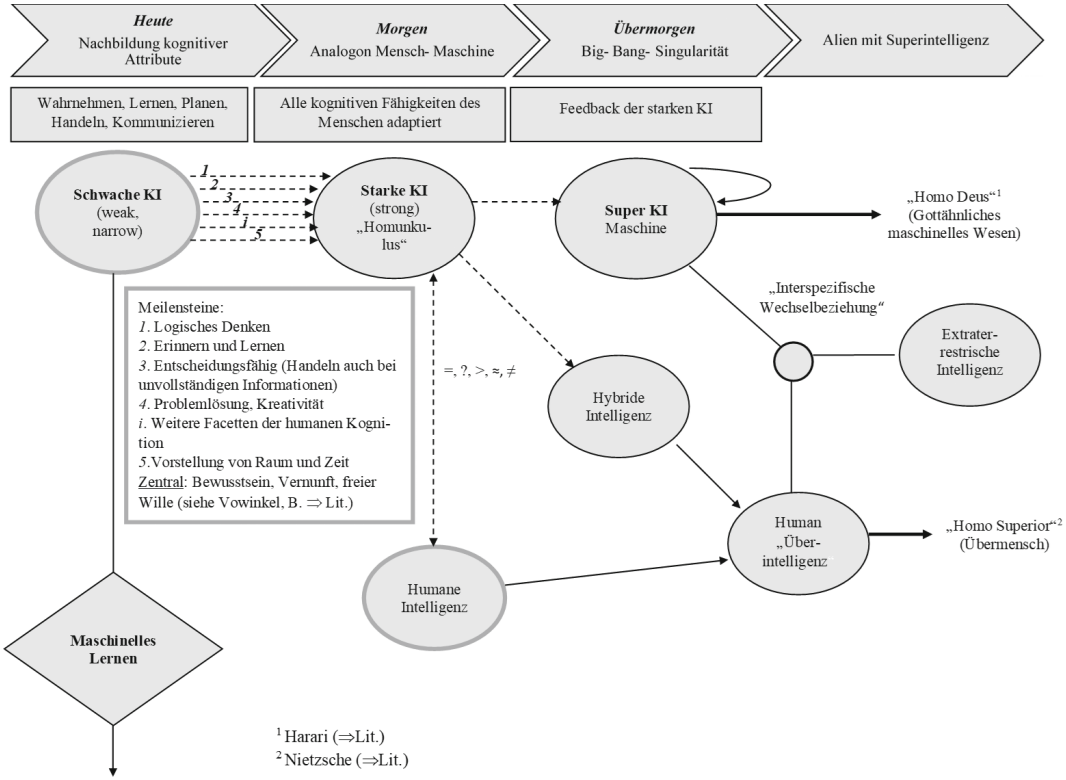


Bild 1.1 Evolution der Künstlichen Intelligenz

Dass digitale lernfähige Maschinen in vielen speziellen, determinierten Bereichen den intellektuellen Fähigkeiten eines Menschen überlegen sind, ist unstrittig. So gewann der IBM Computer Deep Blue 1997 gegen den damaligen Schachweltmeister Garry Kasparov mit 3,5 zu 2,5 Punkten (d. h., von sechs Partien hat Kasparov zwei verloren, eine gewonnen, drei endeten mit Remis).

Doch zurück zur „schwachen KI“: Der Kernbereich der *„schwachen KI“* ist durch das *maschinelle Lernen* geprägt. Hier wurden in den letzten Jahren aufgrund der immensen Weiterentwicklung der Computertechnologie, verbunden mit einer enormen Steigerung der Rechenleistung durch entsprechende Prozessoren und Vernetzung, mit der Möglichkeit sehr große Datenmengen auch in Echtzeit sehr schnell zu verarbeiten, enorme Fortschritte erzielt. *Machine Learning* ist durch lernfähige Algorithmen wie *neuronale Netze* und *Deep Learning* gekennzeichnet. Im Gegensatz hierzu nutzt *Data Mining* statistische Verfahren mit dem Ziel aus den Daten (auch bei einer geringen Anzahl) allgemeine Zusammenhänge und Wissen zu generieren. Bild 1.2 zeigt hierzu einen groben Überblick hinsichtlich *Machine Learning* und *Deep Learning* als inklusive Ausprägung sowie *Data Mining* und die hierzu genutzten algorithmischen Verfahren.

> *„Niemand formuliert es so, aber für mich ist KI fast eine Geisteswissenschaft. Es ist wirklich der Versuch, menschliche Intelligenz und Kognition zu verstehen.“*
>
> *Sebastian Thrun (CEO bei Kitty Hawk Coporation and Innovation)*

Für weitere Ausführungen hierzu siehe Kapitel 22.

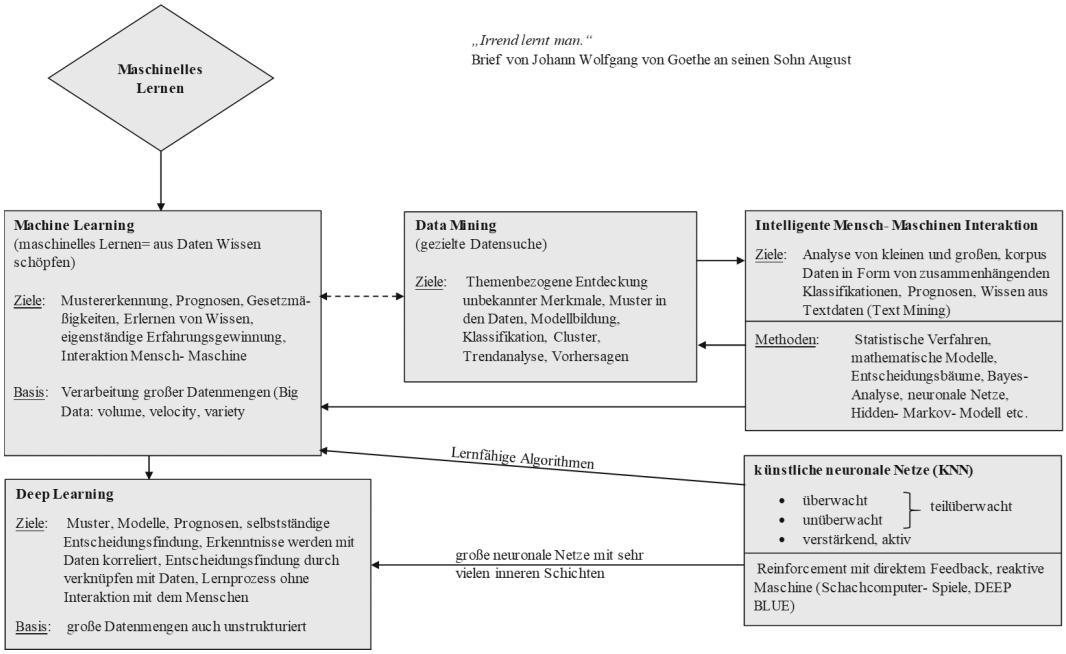


Bild 1.2 Gegenwärtige Praxis der Künstlichen Intelligenz

Bei aller Euphorie bezüglich der Weiterentwicklung und stetig wachsenden Einsatzbereiche von KI bleibt ein zentrales Thema die Absicherung, d. h. die qualitative und quantitative Bewertung hinsichtlich Sicherheit, Zuverlässigkeit, Verfügbarkeit der durch das maschinelle Lernen geprägten sicherheitskritischen Anwendungsbereiche, wie z. B. Mensch-Roboter-Interaktion, autonomes Fahren, aufgrund der nicht mehr nachvollziehbaren Output-Ergebnisse der zugrunde gelegten und implementierten neuronalen Netze allgemein und insbesondere von *Deep Neural Networks*. Ein Ziel ist es deshalb, neuronale Netze erklärbar zu gestalten. Unter dem Terminus „*Explainable Artificial Intelligence*", kurz *Explainable AI,* werden hierzu gegenwärtig weltweit Förderprojekte und Forschungen durchgeführt (siehe hierzu unter anderem das Fraunhofer-Institut für Kognitive Systeme, IKS).

Des Weiteren spielt die Qualität der zugrunde gelegten Input-Daten eine entscheidende Rolle. Eine sorgfältige Dateninterpretation und -verarbeitung gelernter Trainingsdaten, aber auch ungelernter Daten als Modellinput ist deshalb unerlässlich für die Robustheit der Modellierung. Diesbezügliche Fehler, insbesondere bei sicherheitskritischen Anwendungen, können naturgemäß mit weitreichenden Auswirkungen und Folgen verbunden sein. Für weitere Ausführungen hierzu siehe Kapitel 6.

Es liegt auf der Hand, dass der Einsatz von KI insbesondere für automatisierte Systeme wie z. B. in automatisierten Prozessen und bei der Nutzung von Robotern sowie bei deren Vernetzung in der Produktion (Industrie 4.0) oder beim autonomen Fahren, aber auch im medizinischen Bereich (Medizintechnik), mit einem stringenten Sicherheitsnachweis verbunden ist. So sind beispielsweise die prinzipiellen Dilemmata beim autonomen Fahren zwar weitgehend bekannt (Meyna/Heinrich, siehe Lit.), allerdings ab Level 3 (Hochautoma-

tisiert) aufgrund der erforderlichen Absicherungen allgemein – von Forschungsfahrzeugen bis Level 5 abgesehen – noch nicht verfügbar. Es ist deshalb äußerst anspruchsvoll, geeignete Strategien wie Fail-Operational Systems für die Behandlung von komplexen Fehlerzuständen wie z. B. bei der Perzeption, der Fahrzeugregelung, der implementierten Hard- und Software, ungewollter oder gewollter Manipulation im Kontext des dynamischen, adaptiven Fehlermanagements inklusive einer Rückfallebene zur Degradation zu entwickeln und diese qualitativ und quantitativ zu bewerten. Nicht zuletzt gilt es, eine systembezogene Resilienz und Verfügbarkeit in Echtzeitanforderungen umzusetzen und zu gewährleisten (Forschungen hierzu siehe unter anderem Fraunhofer IKS und IQZ).

Nach wie vor ungeklärt sind auch die rechtlichen Fragestellungen und Probleme bei den Lern- und Trainingsprozessen der Software im Kontext der damit verbundenen „autonomen" Handlungs- und Entscheidungsprozesse (Ambivalenz Hersteller vs. Anwender), siehe hierzu unter anderem die juristische Dissertation von Justin Grapentin (siehe Lit.).

Mit dem zunehmenden Einsatz von KI und deren Weiterentwicklung in vielen Bereichen der humanen Existenz spielen auch die damit verbundenen ethischen Fragestellungen eine immer größere Rolle. In diesem Zusammenhang sei auf die in jeder Hinsicht lesenswerte kleine Monographie von Christoph Bartneck et al. des Carl Hanser Verlags (siehe Lit.) verwiesen. Empfehlenswert ist außerdem das Buch „Maschinelles Lernen – Grundlagen und Algorithmen in Python" von Jörg Frochte (2. Auflage 2019, Carl Hanser Verlag, München).

„KI ist wahrscheinlich das Beste oder das Schlimmste, was der Menschheit passieren kann."

Stephen Hawking (1942 – 2018)

Index

Symbole

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z