fotomek / stock.adobe.com

04.03.2019 | Kurzinformation

Künstliche Intelligenz in Sicherheitssystemen

Am 26. und 27. März 2019 dreht sich in Erfurt alles um Funktionale Sicherheit. Dr. Henrik Putzer ist Experte bei Fragen rund um Künstliche Intelligenz im Kontext von Sicherheitssystemen und wird bei den Erfurter Tagen 2019 eine Keynote zu diesem Thema halten. Darüber hinaus engagiert er sich seit Jahren aktiv in der Normung. Wir haben mit Dr. Putzer im Vorfeld zu der Veranstaltung gesprochen: über Branchen mit Potenzial für KI-Anwendungen, sich selbst kontrollierende Algorithmen und ethische Herausforderungen.

Interview mit Dr. Henrik Putzer

Dr. Henrik Putzer I H. Putzer

Lange: *Häufig taucht auch der Begriff „maschinelles Lernen“ auf. Handelt es sich nur um einen anderen Begriff für KI oder ist das eine Unterdisziplin?*

Putzer: Tatsächlich existiert keine allgemein anerkannte Taxonomie für den Bereich der KI. Was ist KI? Ist ein Schachcomputer bereits KI? Vor 50 Jahren wäre ein solches Gerät eindeutig Magie gewesen – oder eben KI. Heute sehen wir das anders: Der Schachcomputer wiederholt letztendlich nur erfolgreiche Zugfolgen aus einer Datenbank und berechnet die Züge im Voraus. Aus dem Bauch heraus wird die Entscheidung „KI oder nicht KI?“ oft abhängig vom Verständnis der Prozesse in der Maschine getroffen. Hofstadter formuliert dazu: „KI ist alles, was noch nicht getan wurde“.

Wissenschaftlich nutzt man den Begriff KI weniger und zielt eher auf die funktionale Leistung ab. So kann „**maschinelles Lernen** (https://de.wikipedia.org/wiki/Maschinelles_Lernen) “ als eine Teildisziplin von KI eingeordnet werden. Das maschinelle Lernen selbst kann dabei sowohl auf symbolischen Grundsätzen beruhen (Wissen liegt explizit vor, z. B. Regelsysteme) oder auch subsymbolisch repräsentiert sein (Wissen wird implizit repräsentiert). Letzteres umfasst wiederum das maschinelle Lernen mit neuronalen Netzen und Deep Learning. Die umgangssprachliche Gleichsetzung von maschinellem Lernen oder gar KI mit neuronalen Netzen ist nicht korrekt.

Lange: *Mit dem Begriff „Künstliche Intelligenz“ werden oftmals auch autonome Fahrzeuge erwähnt. Wie lässt sich KI aus Ihrer Sicht am besten beschreiben?*

Putzer: „Autonome Fahrzeuge“ beinhaltet interessante Aspekte: „Autonom“ ist die umgangssprachliche Beschreibung selbstfahrender Autos, was wissenschaftlich korrekt als „voll automatisiert“ bezeichnet wird. Und so ist KI im engeren Sinne auch zu verstehen: als eine (relativ neue) Methodik, Automation zu implementieren. Flapsig gesprochen könnte man die aktuelle Form der KI-Nutzung als „Beschleunigung des Entwicklungsprozesses“ verstehen. Im Entwicklungsprozess werden klassische Anforderungen an Eingänge, Verarbeitung und Ausgabe zunächst spezifiziert und anschließend implementiert.

Insbesondere mit neuronalen Netzen ändert sich das: Neuronale Netze „lernen“ die Verarbeitung, also die Verbindung von Eingängen zu Ausgängen, anhand von Beispieldate. Dafür passt ein Algorithmus die internen Parameter des neuronalen Netzwerks solange an, bis der Zusammenhang der Eingänge und Ausgaben hinreichend dargestellt wird. Neue und ähnliche Eingänge kann das Netz interpolieren und findet

auf diese Weise Lösungen zu bis dahin unbekannten Eingängen. Parameter anpassen und interpolieren klappt manchmal gut, manchmal nicht und nur in seltenen Fällen verstehen wir genau, warum.

Schließlich entzieht sich dieser subsymbolische Entwurf einem geordneten Prozess und einer von Menschen verstehbaren, symbolischen Repräsentationen (bei symbolischer KI ist das anders). Dies ist auch ein Grund, weshalb es schwer ist, KI-Methoden für einen sicherheitsrelevanten Einsatz zu qualifizieren. Unbestritten ist, dass durch diese neue Entwurfsmethodik der KI höhere Komplexitäten erreicht werden können. Ebenso unbestritten in Fachkreisen ist, dass sich KI – in der aktuell genutzten Form – keine eigenen Ziele setzen, keine neuen Domänen erschließen und auch nicht die Weltherrschaft übernehmen kann – es sei denn, man automatisiert genau das.

Web-Seminare schaffen Wissen: Funktionale Sicherheit und IT-Sicherheit

Grundsätze (nicht nur) in der Eisenbahn-Automatisierung

Der Schwerpunkt des Web-Seminars wird die Beziehung zwischen Funktionaler Sicherheit und IT-Sicherheit für kritische Systeme sein. Diese erfährt gegenwärtig große Aufmerksamkeit und führt zu verschiedenen und widersprüchlichen Empfehlungen.

In seinem Web-Seminar erläutert **Prof. Jens Braband** (https://de.wikipedia.org/wiki/Jens_Braband) die Ableitung und Rechtfertigung von Grundprinzipien, die den Ausgangspunkt für die erforderliche weiterführende Diskussion bilden.

Lange: *In welchen Bereichen wird Künstliche Intelligenz aktuell schon eingesetzt?*

Putzer: Aktuell wird KI in Bereichen eingesetzt, die nicht sicherheitsrelevant sind. Es geht primär um Unterstützungsfunktionen, bei denen der Mensch immer die finale Entscheidung trifft. Dies kann z. B. in der medizinischen Diagnose – auch bei seltenen Krankheiten – der Fall sein, wo eine Computer-KI Diagnose- und Therapievorschläge macht, der behandelnde Arzt aber die letzte Entscheidung trifft. Weitere, erfolgreiche Beispiele sind die Überwachung von IT-Netzen auf Anomalien, also Angriffe, die Vorsortierung großer Datenmengen wie in Recruiting-Prozessen, aber auch Bildverbesserungsalgorithmen für Handyaufnahmen.

Technisch analysiert könnte man sagen, dass – insbesondere neuronale Netze – sehr erfolgreich zur Mustererkennung eingesetzt werden. Beispiele gibt es aktuell genug: Die Sortierung von Suchergebnissen im Internet wie bei Google, die Erkennung von gesprochener Sprache in Tonaufnahmen wie im Fall von Alexa, Siri etc. und die Erkennung sowie Verfolgung von Objekten in Bildsequenzen wie die Erkennung anderer Verkehrsteilnehmer in einem selbstfahrenden Fahrzeug. Seit einiger Zeit werden auch Erfolge beim Einsatz von KI in der Planung von Verhalten erzielt wie beispielsweise künstliche GO-Spieler oder das Fahrverhalten von selbstfahrenden Autos. Ein recht junges Beispiel kommt von DeepMind: Es konnte eine KI trainiert werden, die selbst die besten Spieler von Starcraft 2, einem Echtzeit-Strategiespiel, chancenlos lässt.

Lange: *Wann begegnet uns Künstliche Intelligenz schon heute im Alltag?*

Putzer: Zumeist wenig offensichtlich und nicht direkt, denn KI treibt einige Funktionalitäten in Geräten, die wir nutzen. Gute Computergrafik kann daran gemessen werden, dass man es nicht als Computergrafik erkennt, sondern als „natürlich“ wahrnimmt. Genau das gleich gilt für KI-getriebene Funktionen: Funktionen nehmen wir nicht als auffällig oder störend wahr und merken erst auf den zweiten Blick, welche Leistung dahintersteht.

Lange: *Wie kann künstliche Intelligenz dabei unterstützen, Sicherheitssysteme (im Sinne von Safety) zu verbessern und welche Vorteile bietet Künstliche Intelligenz in Sicherheitssystemen?*

Putzer: Der Einsatz von KI für die Sicherheit im Sinne von Security zeigt bereits Erfolge, z. B. bei der Erkennung von Anomalien wie ein verlassener Koffer am Flughafen. Die Vorteile der KI sind u. a. fehlende Ermüdung im Vergleich zu Menschen, die Verarbeitung von massiven Eingangsdatenmengen und die vergleichsweise einfache Vervielfältigung der Systeme. Allerdings gelten hier die bereits erwähnten Einschränkungen: Die Systeme erkennen zwar Anomalien, aber Menschen übernehmen die finale Beurteilung und Entscheidung.

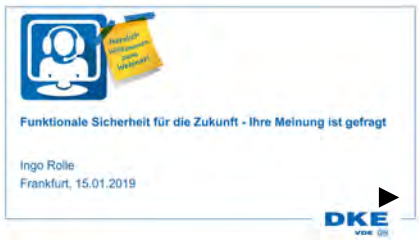
Im Kontext von Safety stellt KI eine Herausforderung dar, an deren Lösung wir arbeiten, Stichwort „Dependable AI“ oder „Trustworthy AI“. Aktuell sind Komfortsysteme oder unterstützende Anwendungen realisierbar, bei denen ein Mensch letztendlich die Sicherheitsverantwortung trägt. Hierzu ein Beispiel: Bei einem Fahrspur-Assistenten erhält der Fahrer beim Überfahren der Spurmarkierung einen leichten Lenkimpuls als Hinweis, den er aber jederzeit ignorieren kann, wenn er die Situation anders beurteilt.

Zunehmend sollen KI-Lösungen auch sicherheitsrelevante Aufgaben übernehmen, die ein Mensch wegen der Komplexität oder hohen Geschwindigkeits- bzw. Präzisionsanforderungen nicht mehr selbst beurteilen und überwachen kann. Die KI muss also korrekt arbeiten oder zumindest kein zusätzliches Sicherheitsrisiko in die Lösung einbringen. Genau an diesem Ziel arbeiten wir: Eine KI als Kern von Automation übernimmt nachweislich sicherheitsrelevante Aufgaben und ebenso die Sicherheitsverantwortung. Der Vorteil einer solchen Lösung liegt im einfacheren Systemansatz: Es ist keine Redundanz mit schwer zu realisierenden, klassischen Ansätzen mehr notwendig. Gleichzeitig ergibt sich ein höherer Nutzen, weil die Überwachung durch den Menschen ebenfalls nicht mehr notwendig ist. Ein nachweislich sicherer KI-Abstandstempomat im Fahrzeug würde beispielsweise selbst keine Auffahrunfälle verursachen, aber auch nicht mehr durch Freiraumerkennung eingeschränkt sein. Zudem würde ein sicherer KI-Abstandsautomat niemals den Menschen um die Übernahme bitten.

Für Lösungen auf der Basis komplexer, KI-basierter Technologie sind jedoch neue Ansätze erforderlich, die zu robuster, sicherer und verlässlicher – „Dependable“ bzw. „Trustworthy“ KI – führen, welche die Automation an sich sicher macht. Ein Baustein wird hierbei ein genormter Ansatz zur Entwicklung solcher Systeme sein.

Web-Seminare schaffen Wissen: Funktionale Sicherheit für die Zukunft

In diesem Web-Seminar wird der Lebenszyklus nach DIN EN 61508 (VDE 0803) anhand eines konkreten Anwendungsbeispielsl veranschaulicht. Zudem werden die Kernanforderungen der Norm erläutert.



- 00:01:34 – Der allgemeine Sicherheitsbegriff nach ISO/IEC Guide 51
- 00:06:39 – "Elektrische Sicherheit" aus Sicht der elektrotechnischen Normung
- 00:13:39 – Funktionale Sicherheit aus Sicht der Normenreihe IEC 61508
- 00:40:07 – Eine Anwendung mit elektrischer und funktionaler Sicherheit
- 00:55:10 – Ausblick: Informationssicherheit aus Sicht der Normenreihe IEC 62443

Lange: *Im Webinar von Hr. Rolle wurde die Bedeutung der Risikobewertung hervorgehoben. In seinem Interview beschrieb Hr. Kieviet folgendes Szenario: „Man stelle sich einen Verbund kollaborierender, mobiler Mehrfachroboter vor. Wenn jetzt diese ihr Verhalten durch KI lernen, haben sie keine Chance mehr, alles in einer Analyse vorherzubestimmen.“ Gibt es hier bereits erste Lösungsansätze?*

Putzer: Ja, hierzu gibt es bereits Ansätze. Der einfachste ist in der IEC-Normenreihe 61508 zu finden, die den Einsatz von KI an bestimmten Stellen, z. B. bei der Fehlerkorrektur, nicht empfiehlt. Jedoch ist man vor allem in komplexen Szenarien ggfs. gezwungen, KI-Technologien einsetzen, um überhaupt eine Lösung für das Problem zu finden, da klassische Entwicklungsmethoden an dieser Stelle versagen. In der Vergangenheit wurde in solchen Fällen eine Risikoanalyse durchgeführt und dann, neben der KI-Funktionalität, redundante Kanäle als „Sicherheitsbarriere“ implementiert.

Redundante Kanäle sorgen durch Absperrungen oder Abschalteinrichtungen für die Sicherheit und haben sozusagen einen „safe envelope“ für die KI-Funktionalität geschaffen. Werden Funktionalitäten und Szenarien aber noch komplexer, ist das leider nicht mehr möglich, da man für den „safe envelope“ selbst KI benötigen würde. Aus diesem Grund arbeiten Industrie und Wissenschaft aktuell gemeinsam daran, die KI-Funktionalität selbst sicher zu gestalten. In diesen Ansätzen wird die Ermittlung und Bewertung von Risiken nach wie vor eine grundlegende Bedeutung haben.

Lange: *Gibt es noch andere Herausforderungen?*

Putzer: Die aktuellen Anstrengungen in Forschung und Industrie versuchen der KI immer neue Funktionen – „Kunststückchen“ – beizubringen. Beim Einsatz der KI im großen Stil ist die Herausforderung sicherlich die gleiche wie bei herkömmlicher Automation: soziale Konsequenzen abschätzen und mit Verstand hinsichtlich der Technologielimitierung vorgehen.

Safety gehört, wie zuvor bereits erwähnt, noch nicht zu den Stärken von KI. Auch ein Weltverständnis ist noch in weiter Ferne. So ist die KI in Form neuronaler Netze derzeit nur in der Lage, eine klar abgegrenzte Aufgabe zu lösen. Diese abgegrenzte Aufgabe erledigt die KI bisweilen besser als der Mensch. Die wissenschaftliche Herausforderung ist es, diese Beschränkungen mit neuen Ansätzen zu durchbrechen.

Hingegen ist die ethische Herausforderung hierbei, der Einsatzweise dieser neuen Technologien klare Regeln zu geben. Gibt es diese Regeln, so liefert die Wissenschaft die Möglichkeit, ethische Regeln nachweisbar in der KI-Lösung zu verankern. Allerdings hat die Geschichte gezeigt, dass

rein beschränkende Regeln auf Dauer keine Wirkung zeigen, sondern dass das Neue aus sich heraus die Zukunft wird. KI als neues Gedankengut wird durch seine Erfolge zu einer neuen, akzeptierten Technologie vor der wir – zumindest in der jetzigen Form – keine Angst haben müssen.

LIGHTFIELD STUDIOS / stock.adobe.com

Die Deutsche Normungsroadmap Künstliche Intelligenz

verfolgt das Ziel, Handlungsempfehlungen rund um KI für die Normung zu geben.

Künstliche Intelligenz gilt weltweit und in zahlreichen Branchen als eine der Schlüsseltechnologien für künftige Wettbewerbsfähigkeit. Umso wichtiger sind die Empfehlungen der Normungsroadmap, die die deutsche Wirtschaft und Wissenschaft im internationalen KI-Wettbewerb stärken, innovationsfreundliche Bedingungen schaffen und Vertrauen in die Technologie aufbauen sollen.

Lange: *Viele verstehen unter dem Begriff „Künstliche Intelligenz" ein System, das sich im Laufe der Zeit verändert. Sicherheitssysteme werden vor Inbetriebnahme, also am Anfang ihres Lebenszyklus, abgenommen. Jede Veränderung am System führt zumindest zu einer erneuten Teilabnahme der Sicherheitsfunktion. Wie kann man ein sich selbst veränderndes Sicherheitssystem abnehmen?*

Putzer: Sich selbst verändernde KI bedeutet, dass eine Funktion im laufenden Betrieb angepasst wird. Das ist keine notwendige Voraussetzung für KI, aber eine durchaus interessante Funktionalität: Sie ermöglicht einer sich selbst weiter entwickelnden KI alle neuen Situationen während der Nutzung – und nicht nur zum Zeitpunkt der Entwicklung – in das Lernen einzubeziehen. Es geht letztendlich um eine Funktionsänderung im Betrieb. Hierzu gibt es Beispiele von Standards, die das u. a. in der Luftfahrt (sicherheitsrelevant!) erlauben.

Die einfach übertragbaren Ansätze für im Betrieb weiterlernende KI sind ähnlich: Es muss dafür nachweislich gesorgt werden, dass die Freiheitsgrade der Änderung immer wieder in einem sicheren System münden. Neuere Ansätze der Forschung gehen den Weg der „Online-Zertifizierung", d. h. ein besonderes Teilsystem sorgt nach der Funktionsanpassung dafür, dass ein zugelassener sicherer Zustand erreicht wird. Letztendlich stehen dahinter entweder Monitorfunktionalitäten, Redundanzen oder Metafunktionen, die auf der Grundlage von redundantem Wissen die Beurteilung für die „Online-Zertifizierung" realisieren. Funktionieren wird das aber immer nur mit spezifischen Funktionseinschränkungen der KI und/oder der Selbständerung. Sollen alle möglichen Freiheitsgrade genutzt werden, so muss die Frage gestellt werden, wie man den allumfassenden Sicherheitsnachweis erbringen will. Denn hierfür müsste man einen Algorithmus erstellen (den Zertifizierer), der entscheidet, ob ein anderer Algorithmus (die sich selbst ändernde KI) sicher ist. Die theoretische Informatik hat jedoch schon nachgewiesen, dass nicht einmal ein Algorithmus definiert werden kann, der entscheidet, ob ein anderer Algorithmus überhaupt terminiert (Halteproblem). Wir kommen hier also mit spannenden Fragen an die Grundlage der Informatik.

Lange: *Bisher sind die bestehenden Normenreihen IEC 61508 und EN 50128 eindeutig: In beiden Normen wird Künstliche Intelligenz explizit als nicht zu empfehlende Technik benannt. Auch andere Normen wie DO178, DO254 oder ISO26262 verlangen nach einem deterministischen System. Ist eine Entwicklung von Normen bereits absehbar, die sich inhaltlich konkret mit Funktionaler Sicherheit im Kontext von Künstlicher Intelligenz auseinandersetzen?*

Putzer: Ja, die Normung steht der KI aktuell noch skeptisch gegenüber, auch wenn ein generelles Verbot von KI nicht gegeben ist. Diese Skepsis ist auch natürlich, da Normung den Stand der Technik abbildet und KI erst dabei ist, Stand der Technik zu werden. Es ist noch nicht so lange her, da wurde Software ähnlich skeptisch betrachtet. Software ist zunehmend der bestimmende und wertschöpfende Teil von vielen Produkten. Gleichzeitig wurden in der Vergangenheit viele funktionierende Normen in diesem Kontext entwickelt.

Und genau so muss sich die Normung auch mit dem Thema der KI befassen – je früher desto besser, denn Innovationszyklen werden immer kürzer und die Halbwertszeit von Normen wird sich damit verkürzen. Im Expertengremium DKE/AK 801.0.8 entsteht beispielsweise eine Anwendungsrichtlinie („Spezifikation und Entwurf autonomer/kognitiver Systeme") für Systeme, die im Kern ihrer Funktionalität auf Künstliche Intelligenz setzen können und Attribute der Trustworthiness , also Safety, Security, Usability etc., umsetzen. Parallel arbeitet ein ISO-Komitee, das SC42, daran, KI insgesamt zu standardisieren. Diese Tätigkeiten werden durch ein DIN-Gremium begleitet bzw. gestützt.

Lange: *Sollten hierfür bestehende Normen ergänzt oder neue Normen für spezifische Anwendungsbereiche / Anwendungsmöglichkeiten erarbeitet werden?*

Putzer: Je nach Zusammensetzung der Normungs-Komitees ist durchaus beides denkbar. Wichtig ist, dass die Normen möglichst an einem Strang ziehen und für die Anwender widerspruchsfreie und gut anwendbare Vorgaben erzeugen. Dafür ist es aber ebenso wichtig, dass sich Experten für KI und Experten für (Safety-) Normung abstimmen. Ein sehr gutes Forum – neben den Normungsgremien – sind Fachtagungen wie die VDE DKE-Tagung zum Thema „Funktionale Sicherheit für die Zukunft".

sdx15 / stock.adobe.com

Mit dem DKE Newsletter sind Sie immer am Puls der Zeit! Monatlich ...

- fassen wir die wichtigsten Entwicklungen in der Normung kurz zusammen
- berichten wir über aktuelle Arbeitsergebnisse, Publikationen und Entwürfe
- informieren wir Sie bereits frühzeitig über zukünftige Veranstaltungen

Lange: *Wie ist Deutschland im weltweiten Vergleich bei Funktionaler Sicherheit im Kontext Künstlicher Intelligenz aktuell aufgestellt?*

Putzer: Deutschland hat brillante Köpfe mit großem Potential. Deutschland hat die ersten Programme und Institutionen, die hier Maßstäbe setzen können. Doch an der Spitze sehe ich Deutschland nicht. Hier sind noch freier denkende Nationen mit mehr Budget oder Nationen mit großem, politischem Druck vor uns einzuordnen. Zwei Dinge könnten Deutschland weiter nach vorne bringen: Die Abkehr von der „Deutschen Angst", ohne jedoch das Augenmaß, zu verlieren und eine Bereitstellung von Budgets mit weniger Bürokratie. Schließlich benötigen wir Freigeister, die hohe, kreative und innovative Leistungen erbringen. Das lässt sich aber nicht mit einengenden Vorgaben schaffen. Zielführend wäre es, den richtigen Nährboden zu erzeugen. Dafür muss die typische „Deutsche Angst" durch einen Dialog in der Gesellschaft abgebaut werden. Budgets müssten außerdem effizient eingesetzt werden: Nicht alles mit dem Gießkannenprinzip verteilen, aber auch nicht alles auf wenige, große Forschungsinstitute beschränken.

Lange: *Nehmen wir hierzulande evtl. sogar eine Vorreiterrolle in einem Bereich ein?*

Putzer: Ja, die Grundgedanken des Expertengremiums **DKE/AK 801.0.8** (https://www.dke.de/de/ueber-uns/dke-organisation-auftrag/dke-fachbereiche/dke-gremium?id=3006525&type=dke%7Cgremium) sind sehr innovativ. In einem ersten Mix aus angepassten Entwicklungslebenszyklus und einem Abschnitt zur Entwicklung von KI-Komponenten parallel zu Hardware- und Software-Komponenten ergibt sich großes Potenzial, das unter Experten bereits einiges an Beachtung findet. Dieses Potenzial kann und muss von dem gesammelten Wissen zum Thema leben – oder eben dem versammelten Wissen bei entsprechenden Treffen der Experten-Community als Basis des fachlichen Austauschs. Hier müssen auch (fachliche) Vorurteile abgebaut werden und Korridore für die Inhalte von Normen zur KI. Dieser Korridor muss nach und nach durch die Forschung und den Stand der Technik gefüllt werden. Pilotprojekte müssen mit den Normungsansätzen arbeiten und schrittweise verbessern. Die ersten Schritte unternimmt u. a. der Expertenkreis **DKE/AK 801.0.8** (https://www.dke.de/de/ueber-uns/dke-organisation-auftrag/dke-fachbereiche/dke-gremium?id=3006525&type=dke%7Cgremium) , aus dessen Arbeit später ggfs. völlig neue Entwicklungs- und Verifikations-Ansätze entstehen.

Lange: *Laufen wir – ohne die gleichzeitige Erarbeitung bzw. Ergänzung vorhandener Normen – zukünftig Gefahr, den Anschluss bei Innovationen zu verlieren?*

Putzer: Ja, das kann passieren. Der erste Stolperstein ist die Beibehaltung bestehender Normen: Bereits die Einschränkung der **IEC-Normenreihe 61508** (https://de.wikipedia.org/wiki/IEC_61508) hinsichtlich der nicht-Empfehlung von KI wird oft fehlinterpretiert. Dies führt dazu, dass in Projekten nicht mit KI gearbeitet wird, weil es nicht empfohlen wird. Das ist jedes Mal wieder eine verpasste Chance, Erfahrungen zu sammeln und Kompetenzen aufzubauen. Normen sollten klar sein und nur durch Ziele einschränken wie Ausfallraten oder andere Metriken. Methoden oder Technologien sollten a priori nicht ausgeschlossen werden. Und Normen dürfen kein Damoklesschwert der (nicht-)Zulassung von Produkten erzeugen, sondern müssen Erfahrungen dokumentieren und den Weg in die Zukunft freigeben.

Insbesondere im Bereich der KI ist ein Umdenken und eine neue Haltung in den Gremien wichtig: Nicht mehr sequenziell „forschen – anwenden – normieren", sondern alle Tätigkeiten vereinen. Bezüglich der KI sehen wir es in der Forschung bei **fortiss** (https://www.fortiss.org) und in Industrieprojekten bei der **cogitron** (http://www.cogitron.de/) : Grundlagenforschung und industrielle Forschung sind in praktischen Anwendungen beinahe gleichauf. Das liegt nicht zuletzt an den enormen finanziellen Mitteln der Industrie. Es entsteht ein Miteinander aus Forschung und Industrie. Es wäre gut, so früh wie möglich einen Dreiklang daraus zu machen: Forschung, Industrie und Normung.

Redaktioneller Hinweis:

Die im Text aufgeführten Normen und Standards können Sie beim VDE VERLAG erwerben.