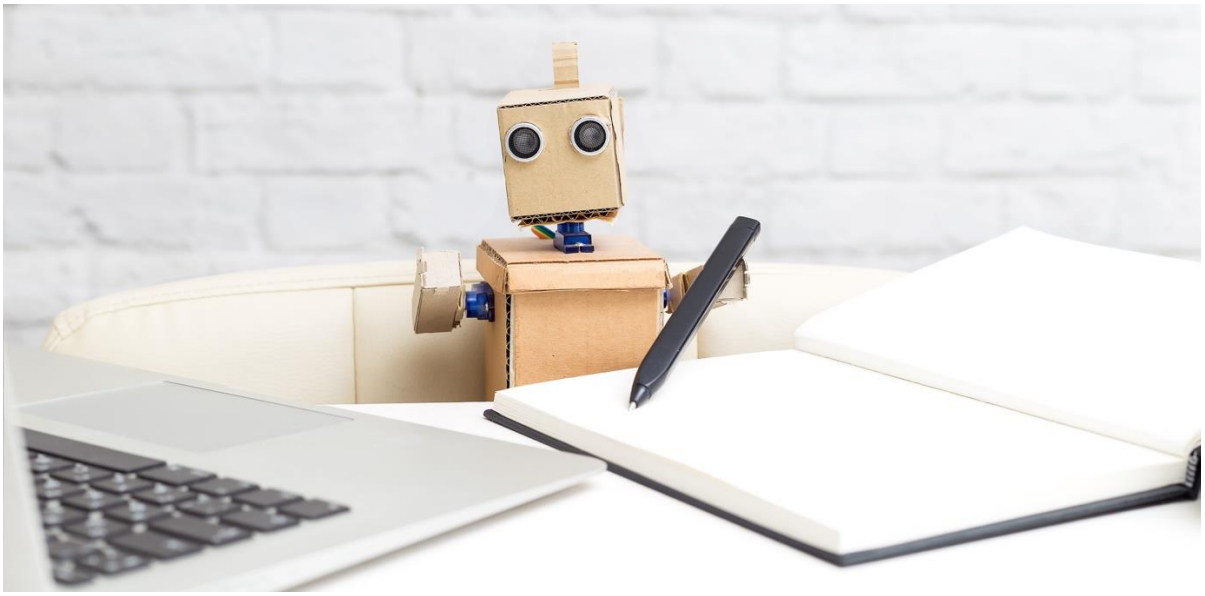
Verband der TÜV e.V.



POSITIONSPAPIER KÜNSTLICHE INTELLIGENZ

Vertrauen in KI-basierte Systeme schaffen

Künstliche Intelligenz (KI) ist zwar keine neue Technologie, sie gewinnt aber durch den technischen Fortschritt und leistungsfähigere Rechner- und Datenübertragungskapazitäten immer größere Bedeutung. Künstliche Intelligenz dringt in immer mehr Lebens- und Wirtschaftsbereiche vor, von Smart Homes über hochassistiertes und automatisiertes Fahren bis hin zu softwaregestützter Endoskopie in der Medizintechnik. Oft in Kombination mit Big Data und Big Data Analytics, deckt KI ein breites Spektrum ab und verspricht große Chancen für Wirtschaft und Gesellschaft. Es gibt dabei aber auch zahlreiche sicherheitstechnische und ethische Herausforderungen.

Einleitung

Der Deutsche Bundestag hat die Tragweite des Zukunftsthemas mit der Einrichtung einer Enquete-Kommission für KI gewürdigt. Die Bundesregierung veröffentlichte im November 2018 ihre KI-Strategie und identifizierte die Standardisierung als zentrales Handlungsfeld. KI-basierte Systeme dringen in nahezu alle Wirtschaftsbereiche vor und werden für die Zukunft große Fortschritte erzielen, beispielsweise in den Bereichen Mobilität, Gesundheit, öffentliche Dienstleistungen und Ressourcenmanagement. Die Bundesregierung begleitet und unterstützt diese Entwicklungen.

Die EU-Kommission hat im April 2018 ihre Strategie „Künstliche Intelligenz für Europa“ vorgelegt. Darin heißt es: Weil KI ein Klima des Vertrauens erfordert, muss ein geeigneter ethischer und rechtlicher Rahmen geschaffen werden. Angesichts der breit gestreuten Einsatzmöglichkeiten von KI erwägt die EU-Kommission sowohl horizontale als auch sektorspezifische Vorschriften zu überprüfen. Regulative Anforderungen sind mit Blick auf den freien Waren- und Dienstleistungsverkehr auf europäischer Ebene festzulegen. Erste ethische Leitlinien für KI hat die EU-Kommission bereits im April 2019 verabschiedet. Im Juli 2019 wurden diese noch einmal durch die einberufene Expertengruppe um 33 Anforderungen an KI ergänzt.

Die Nutzung KI-basierter Systeme kann Auswirkungen auf die Privatsphäre haben, spezifische haftungsrelevante Fragestellungen aufwerfen, und die Autonomie der Nutzer einschränken. Der aktuelle nationale sowie europäische Rechtsrahmen berücksichtigt diese Technologie und ihre Auswirkungen bislang nur unzureichend. Hinsichtlich funktionaler Sicherheit (Safety), IT-Security und Privacy müssen die rechtlichen Rahmenbedingungen für die Entwicklung und Nutzung KI-basierter Systeme daher sorgfältig überprüft und gegebenenfalls angepasst werden. Damit KI-basierte Systeme sicher und beherrschbar sind, braucht es die Einordnung in verschiedene Risikolevel, um so die jeweiligen Sicherheitsanforderungen definieren zu können.

So ist beispielsweise beim hochassistierten und automatisierten Fahren zu erwarten, dass diese Fahrfunktionen nicht mehr wie bisher alleine mit regelbasierter Software gelöst werden können. Hier werden Techniken aus dem Bereich der künstlichen Intelligenz wie zum Beispiel Machine Learning zum Einsatzkommen müssen. Die Handhabung dieser selbstlernenden Systeme stellt ein neues Paradigma in der Funktionsentwicklung dar, dessen Anforderungen und Auswirkungen neu gedacht werden müssen. Beispiele hierfür sind die technische Umsetzung und Einhaltung ethischer Rahmenbedingungen, der Datenschutz sowie die Qualität der großen Menge an Realdaten für Trainings- und Testzwecke. Nicht zuletzt ist ein Zugang zu diesen Daten notwendig. Erst einer Analyse dieser Daten ermöglicht es, die Entscheidungen der lernenden Algorithmen zu verstehen und nachzuvollziehen.

Der VdTÜV setzt sich für die (Weiter)Entwicklung von Qualitäts- und Sicherheitsstandards zum kontrollierten Betrieb KI-basierter Systeme ein. Um die gesellschaftliche Akzeptanz dieser Technologie zu fördern, muss durch den Einsatz unabhängiger Prüforganisationen auf Basis verbindlicher Vorschriften das Vertrauen der Menschen in die Sicherheit KI-basierter Systeme gestärkt werden. Der VdTÜV unterstützt den Einsatz von KI-basierten Systemen zum Nutzen der Gesellschaft und bringt sich mit seinen Experten in eine konstruktive und faktenbasierte Diskussion ein. Erst durch die sichere Anwendung KI-basierter Systeme wird die notwendige gesellschaftliche Akzeptanz für ihren Einsatz geschaffen.

Verband der TÜV e.V.

Forderungen des VdTÜV

1. Verschiedene Risikolevel für KI-basierte Systeme definieren und anwenden

Zur Ermittlung unterschiedlicher Sicherheitsanforderungen regt der VdTÜV die Entwicklung eines Stufenmodells an, beispielsweise analog zu den in der SAE-Norm festgelegten Stufen beim automatisierten Fahren. Je nach Level sind hier unterschiedliche Sicherheits- und Prüfanforderungen für die eingesetzten Algorithmen denkbar. Sie reichen von einfachen industriellen Anwendungen (Automatisierung), über Bild- und Sprachverarbeitung bis hin zu hochkomplexen selbstlernenden autonomen Systemen, wie etwa hochassistierte bis autonome Fahrzeuge. Durch diese Risikolevel können Produkt- und Prüfanforderungen beschrieben werden, um Aussagen über die Sicherheit der Systeme zu machen. Die Prüfanforderungen sind vom Gesetzgeber festzulegen. Dieser muss auf Grundlage des Vorsorgeprinzips seinem Schutz- und Fürsorgeauftrag gegenüber der Gesellschaft auch bei KI-basierten Systemen in vollem Umfang gerecht werden.

2. Gesetze, Normen und Standards überprüfen, anpassen und ergänzen

Es fehlt derzeit an Prüfszenarien, Methoden und Standards, um die Sicherheit der eingesetzten Algorithmen und selbstlernenden Systeme über den gesamten Produktlebenszyklus hinweg sicherzustellen: beginnend bei der Entwicklung über die Genehmigung, die Nutzung bzw. den Betrieb bis hin zum Recycling. Aus Sicht des VdTÜV bedarf es einer unabhängigen und neutralen Kontrolle der Einhaltung noch zu schaffender sicherheitstechnischer Normen und Standards – sowie ethischer und datenschutzrechtlicher Anforderungen.

3. Zugang zu Daten ermöglichen

Die Voraussetzung für die Anwendung KI-basierter Systeme sind Daten, mit denen die Systeme angelernt werden. Ein Grundproblem ist, dass diese so genannten Trainingsdaten immer nur die Vergangenheit abbilden. Aber auch während der Betriebsphase spielen die während der Nutzung generierten Daten eine große Rolle, denn sie verändern das System fortlaufend. Dabei wird nicht überprüft, ob diese Daten ausgewogen und korrekt sind. Der VdTÜV setzt sich dafür ein, dass entsprechend des Risikolevels der Zugang zu den relevanten Daten für berechtigte Stellen ermöglicht wird. Datenvielfalt, Datensouveränität, Verfügbarkeit von Daten, aber auch der Datenschutz gewinnen durch KI eine noch wichtigere Bedeutung.

4. Gesetzliche Verankerung der Überprüfung KI-basierter Systeme durch unabhängige Dritte

Die Einhaltung definierter Produktanforderungen muss insbesondere für sicherheitsrelevante KI-basierte Systeme gesetzlich festgeschrieben werden. Die Prüfung der KI-basierten Systeme, insbesondere die Bewertung der erforderlichen Selbstdiagnosemechanismen, muss durch von Anbietern und Nutzern unabhängige Prüforganisationen („unabhängige Dritte“) erfolgen. Hierfür ist sicherzustellen, dass die berechtigten Stellen Zugang zu den für die Sicherheit des Systems relevanten Algorithmen und Daten haben.

5. Funktionsweise und Entscheidungsfindung von KI-basierten Systemen verstehen, entwicklungsbegleitend prüfen und lebenslang begleiten

Die Herausforderungen für die Sicherheit im gesamten Lebenszyklus eines KI-basierten Systems machen deutlich, dass eine einmalige Prüfung vor dem Inverkehrbringen nicht ausreicht. In Abhängigkeit vom Risikolevel des Systems ist die Formulierung unterschiedlicher Produkt- und Prüfanforderungen erforderlich. Sie müssen sowohl die zugrundeliegenden Algorithmen und die Methode, mit der das System trainiert wurde, als auch die Daten (Qualität, Auswahl, Menge) umfassen. In der Überprüfung dieser Anforderungen sind insbesondere die Prüfungsintervalle entsprechend flexibel anzupassen. Daher setzt sich der VdTÜV für entwicklungsbegleitendes Prüfen ein, da insbesondere für Produkte mit höheren Risikolevel (zum Beispiel autonomes Fahren) die notwendige sicherheitsrelevante Integrität bereits im Produktentwicklungsprozess entsteht. Eine sicherheitstechnische Prüfung erst am Bandende wird in Zukunft nicht mehr ausreichend sein. Es stellt sich dabei die Herausforderung, nicht nur zu wissen, ob komplexe automatisierte Systeme reagieren, sondern auch, warum sie reagieren. Die lebenslange Begleitung und Beobachtung eines KI-basierten Systems sowohl durch den Hersteller als auch durch unabhängige Dritte ist daher erforderlich.

6. Durch Ethikstandards Vertrauen in KI-basierte Systeme schaffen

KI-basierte Systeme und deren Entwicklungsrahmen müssen auch unter ethischen Gesichtspunkten betrachtet und geprüft werden, um Diskriminierung und gesellschaftliche Schäden zu vermeiden. Selbstlernende Systeme müssen jederzeit sicher und beherrschbar bleiben. Um Vertrauen in KI-basierte Systeme zu schaffen, braucht es Ethikstandards, zu denen sich Hersteller bekennen und die sie nachvollziehbar einhalten müssen. Diese Standards bedürfen eines gesamtgesellschaftlichen Konsenses. Der VdTÜV setzt sich dafür ein, dass diese Ethikstandards in ihrer Umsetzung transparent und, wo notwendig, durch Dritte überprüfbar sind.

Kontakt

Leitstelle Digitales
Ansprechpartnerin: Elisa Brummel
E-Mail: elisa.brummel@vdtuev.de
Tel. +49 30 760095 360
www.vdtuev.de