DIN SPEC 92001-2

Künstliche Intelligenz - Life Cycle Prozesse und Qualitätsanforderungen - Teil 2: Robustheit

DIN SPEC 92001-2 PRAXISBEISPIEL

Widerstandsfähige KI

Der Hintergrund

Der Begriff Künstliche Intelligenz (KI) umfasst eine Reihe verschiedener Ansätze, um IT-Systeme so zu optimieren, dass sie in der Regel sehr spezialisierte Probleme lösen können. Die meisten KI-Algorithmen basieren dabei auf neuronalen Netzen, die von den riesigen Datenmengen profitieren, die heutzutage verfügbar sind. Diese neuronalen Netze sind lose den Gehirnen lebender Organismen nachempfunden: Sie können Informationen eigenständig verarbeiten, darauf reagieren und lernen, Probleme selbst zu lösen. Anders als beispielsweise das menschliche Gehirn sind sie jedoch anfällig für schon geringfügige Störungen bei der Eingabe und Aufnahme von Daten. Dadurch kann es passieren, dass das maschinelle Lernen ein betreffendes Problem nicht mehr hinreichend robust lösen kann, also nicht stabil ist. Weil KI-Module jedoch zunehmend in hochsensiblen Industriezweigen und Geschäftsbereichen eingesetzt werden, sind Robustheit und Qualitätssicherung über ihren gesamten Lebenszyklus notwendig.

Die DIN SPEC

Die DIN SPEC 92001-2 baut auf der DIN SPEC 92001-1 auf. Letztere beschreibt ein Qualitätsmetamodell für KI-Module, das verschiedene Phasen in deren Lebenszyklus einführt und als grundlegende Qualitätspfeiler Robustheit, Funktionalität und Leistung sowie Nachvollziehbarkeit definiert. Teil 2 betrachtet den Aspekt der Robustheit unter zwei spezifischen Blinkwinkeln nun genauer. Zum einen geht es um die Robustheit gegenüber mathematisch optimierten Störungen, mit denen bei einem gezielten Angriff Fehlfunktionen in KI erzeugt werden sollen. Zum anderen ist auch Robustheit gegenüber natürlich auftretenden Signalstörungen oder anderen Beeinträchtigungen der Datenqualität notwendig, die bei der Anwendung von KI häufig vorkommen. Die DIN SPEC 92001-2 strukturiert dazu umfangreiche Anforderungen entlang eines systematischen Risikomanagementprozesses. Im ersten Schritt, „Scope, Context, Criteria“ (Umfang, Kontext, Kriterien), müssen Organisationen allgemeine Anforderungen für ihre konkreten KI-Risiken ausarbeiten. Darauf folgt eine umfangreiche KI-Risikobewertung, bestehend aus den Schritten „Threat Model Analysis“ (Bedrohungsmodellanalyse), „Impact Analysis“ (Einflussanalyse), und „Robustness Evaluation“ (Auswertung der Robustheit). Basierend auf der empirischen Auswertung der Robustheit erfolgt dann eine gezielte Risikominderung – beispielweise durch Maßnahmen zur Verteidigung gegen Angriffe oder zur Stärkung der Robustheit. Je nach realem Entwicklungs- und Einsatzkontext der KI, sollen diese Schritte in digitalen, simulierten, und/oder physikalischen KI-Umgebungen stattfinden. Die DIN SPEC schlägt Entwicklern und Betreibern zudem vor, ihre KI-Module in unterschiedliche Risikobereiche einzuteilen, um deren Robustheit risikoorientiert aufzubauen. Sie umfasst 53 technische Anforderungen, die in Prioritätskategorien eingestuft sind.

Der Nutzen

Die DIN SPEC 92001-2 strukturiert das sehr lebendige Forschungsfeld zur Robustheit von KI-Modulen und schafft eine detaillierte technische Grundlage für robuste und vertrauenswürdige KI-Anwendungen. Sie ermöglicht sowohl Entwicklern als auch Anwendern von KI ein zeitgemäßes Risikomanagement durch klar formulierte und pragmatisch ausbalancierte

„Die DIN SPEC 92001-2 schafft eine detaillierte technische Grundlage für robuste und vertrauenswürdige KI-Anwendungen."

DIN SPEC 92001-2
PRAXISBEISPIEL

Richtlinien und Handlungsempfehlungen. Dazu werden die mit dem Einsatz von KI-Systemen verbundenen Risiken analysiert und betrachtet, wie sie in den verschiedenen Prozessen und Phasen im Lebenszyklus eines KI-Moduls auftreten. „Mithilfe der DIN SPEC 92001-2 können Unternehmen und andere Organisationen ihre KI-basierte Software resistenter machen gegen alle erdenklichen Störprozesse", erläutert Stephan Hinze, Geschäftsführer der neurocat GmbH und Initiator der DIN-SPEC 92001-2. „Sie ist ein notwendiger Baustein in der KI-Strategie jeder Organisation, weil sie KI-Qualitätssicherung transparent und nachvollziehbar macht."

Die Zusammenarbeit

Die DIN SPEC 92001-2 wurde im PAS-Verfahren (Publicly Available Specification) erarbeitet und erscheint auf Englisch. Am Projekt beteiligt waren die Acsioma GmbH, DFKI GmbH, EMEIA-GSA Automation, Ernst & Young AG, Fraunhofer – Institut für Offene Kommunikationssysteme FOKUS, Fraunhofer – Institut für Molekularbiologie und angewandte Ökologie (IME), GESTALT Robotics GmbH, Hochschule für Angewandte Wissenschaften (HAW), Hochschule für Technik und Wirtschaft Berlin (HTW) FB4 Wirtschaftswissenschaften, IABG mbH, Micropsi industries GmbH, Microsoft Deutschland GmbH, neurocat GmbH, Otto-von-Guericke-Universität Magdeburg, Institut III: Philosophie, Robert Bosch GmbH, Stiftung neue Verantwortung e.V., STILL GmbH, TÜV Süd Auto Service GmbH, Universität Osnabrück und die Universität Tübingen.

Die DIN SPEC 92001-2 ist kostenlos erhältlich unter **www.beuth.de**

Über DIN SPEC

Für den Erfolg einer Idee ist häufig entscheidend, wie schnell sie im Markt verbreitet wird. Mit der DIN SPEC setzen Unternehmen – vom Start-up über den Mittelstand bis zu Großunternehmen – innerhalb weniger Monate agil und unkompliziert Standards. Dabei ist die DIN SPEC fest mit den Namen der Innovatoren verbunden und so ein wirksames Marketinginstrument, das dank der anerkannten Marke DIN zu großer Akzeptanz bei Kunden und Partnern führt. DIN selbst sorgt dafür, dass die DIN SPEC nicht mit bestehenden Standards kollidiert und veröffentlicht sie international. Eine DIN SPEC kann auch die Basis für eine spätere DIN-Norm sein.

Fünf Gründe für DIN SPEC

- → Schnelles Tempo: DIN SPEC lassen sich innerhalb weniger Monate erstellen und veröffentlichen.
- → Weltweite Anerkennung: International bestens etabliert, sichert die Marke DIN maximales Vertrauen am Markt. Innovationen und Unternehmen genießen hohe Akzeptanz bei Anwendern und Investoren.
- → Agiles Netzwerk: Der DIN SPEC-Prozess fördert den Austausch mit relevanten Marktteilnehmern. Das erweitert das Netzwerk mit Key-Playern: Anforderungen von Herstellern und Kunden fließen ein.
- → Einfaches Handling: DIN organisiert das gesamte DIN SPEC-Projekt. Das spart Zeit, um sich auf die Inhalte und das Netzwerken zu konzentrieren.
- → Direktes Plug & Play: Durch den DIN SPEC-Prozess wird die Innovation mit dem aktuellen Stand der Technik abgestimmt. Anwender können sofort und ohne Hürden mit dem Standard arbeiten.

www.din.de/go/spec

DIN e. V. · Saatwinkler Damm 42/43 · 13627 Berlin
Telefon: +49 30 2601-2303 oder -2607 · Telefax: +49 30 2601-42303 oder -42607 · E-Mail: spec@din.de