DIN SPEC 92001-2

Artificial Intelligence – Life Cycle Processes and Quality Requirements – Part 2: Robustness

DIN SPEC 92001-2 CASE STUDY

Robust AI

The background

The term Artificial Intelligence (AI) covers a number of different approaches to optimize IT systems so that they can solve very specialized problems. Most AI algorithms are based on neural networks that benefit from the huge amounts of data available today. These neural networks are loosely modeled on the brains of living organisms: They can process information independently, react to it and learn to solve problems themselves. However, unlike the human brain they are susceptible to even minor disturbances in the input data. As a result, machine learning may no longer be able to solve a problem in a sufficiently robust manner, i.e. it may not be stable. However, because AI modules are increasingly used in highly sensitive industries and business areas, robustness and quality assurance throughout their entire life cycle are necessary.

The DIN SPEC

The DIN SPEC 92001-2 is based on DIN SPEC 92001-1. The latter describes a quality metamodel for AI modules, which introduces different phases in their life cycle and defines robustness, functionality and performance as well as comprehensibility as fundamental quality pillars. Part 2 now takes a closer look at the aspect of robustness under two specific angles. On the one hand, it deals with the robustness against mathematically optimized disturbances, which are used to generate malfunctions of AI, for example in the case of a targeted attack. On the other hand, robustness against naturally occurring signal disturbances or other impairments of data quality is necessary, which often occur when using AI. The DIN SPEC 92001-2 structures extensive technical requirements along a systematic risk management process. In the first step, "Scope, Context, Criteria", organizations must develop general requirements for their specific AI risks. This is followed by a comprehensive AI risk assessment, consisting of the steps "Threat Model Analysis", "Impact Analysis", and "Robustness Evaluation". Based on the empirical evaluation of the robustness, a targeted risk reduction is then carried out - for example, through measures to defend against attacks or to strengthen the robustness. Depending on the real development and deployment context of the AI, these steps should take place in digital, simulated, and/or physical AI environments. The DIN SPEC also suggests that developers and operators divide their AI modules into different risk categories in order to build up their robustness in a risk-oriented way. DIN SPEC 92001-2 comprises 53 technical requirements, which are classified in priority categories.

The benefit

The DIN SPEC 92001-2 structures the very lively research field of AI robustness and creates a detailed technical basis for robust and trustworthy AI applications. It enables both developers and users of AI to manage AI risks in a modern way by means of clearly formulated and pragmatically balanced guidelines and recommendations for action. To this end, the risks associated with the use of AI systems are analyzed and considered as they occur in the various processes and phases in the life cycle of an AI module. "With the help of DIN SPEC 92001-2, companies and other organizations can make their AI-based software more resistant to all conceivable disruptive processes," explains Stephan Hinze, Managing Director of neurocat GmbH and initiator of DIN-SPEC 92001-2, "It is a necessary building block in the AI strategy of every organization because it makes AI quality assurance transparent and comprehensible."

DIN

"DIN SPEC 92001-2 creates a detailed technical basis for robust and trustworthy AI applications."

DIN SPEC 92001-2
CASE STUDY

The collaboration

DIN SPEC 92001-2 was developed within 18 months using the PAS (Publicly Available Specification) procedure and is published in English. The project involved Acsioma GmbH, DFKI GmbH, EMEIA-GSA Automation, Ernst & Young AG, Fraunhofer - Institute for Open Communication Systems FOKUS, Fraunhofer - Institute for Molecular Biology and Applied Ecology (IME), GESTALT Robotics GmbH, University of Applied Sciences (HAW), University of Applied Sciences Berlin (HTW) FB4 Economics, IABG mbH, Micropsi industries GmbH, Microsoft Deutschland GmbH, neurocat GmbH, Otto-von-Guericke University Magdeburg, Institute III: Philosophy, Robert Bosch GmbH, Stiftung neue Verantwortung e.V., STILL GmbH, TÜV Süd Auto Service GmbH, University of Osnabrück and the University of Tübingen.

The DIN SPEC 92001-2 is available for free download under **www.dinmedia.de**

About DIN SPEC

The success of an idea is often determined by how quickly it is spread in the market. With the DIN SPEC, companies - from start-ups to medium-sized and large enterprises - set standards within a few months in an agile and uncomplicated manner. The DIN SPEC is firmly linked to the names of the innovators, making it an effective marketing instrument that leads to great acceptance among customers and partners thanks to the recognized DIN brand. DIN itself ensures that the DIN SPEC does not collide with existing standards and publishes them internationally. A DIN SPEC can also be the basis for a future DIN standard.

Five reasons for DIN SPEC

- → Fast: DIN SPEC can be created and published within a few months.
- → Worldwide recognition: Well established internationally, the DIN brand ensures maximum trust in the market. Innovations and companies enjoy high acceptance among users and investors.
- → Agile network: The DIN SPEC process promotes exchange with relevant market participants. This expands the network with key players: Requirements of manufacturers and customers are incorporated.
- → Easy handling: DIN organizes the entire DIN SPEC project. This saves time, so you can concentrate on content and networking.
- → Direct plug & play: The DIN SPEC process ensures that the innovation is aligned with the current state of the art. Users can work with the standard immediately and without hurdles.

DIN e. V. · Am DIN-Platz · Burggrafenstraße 6 · 10787 Berlin
E-Mail: spec@din.de