

25.11.2020 11:25

Research results, Transfer of Science or Research

fortiss and DKE develop first security standard for AI-systems



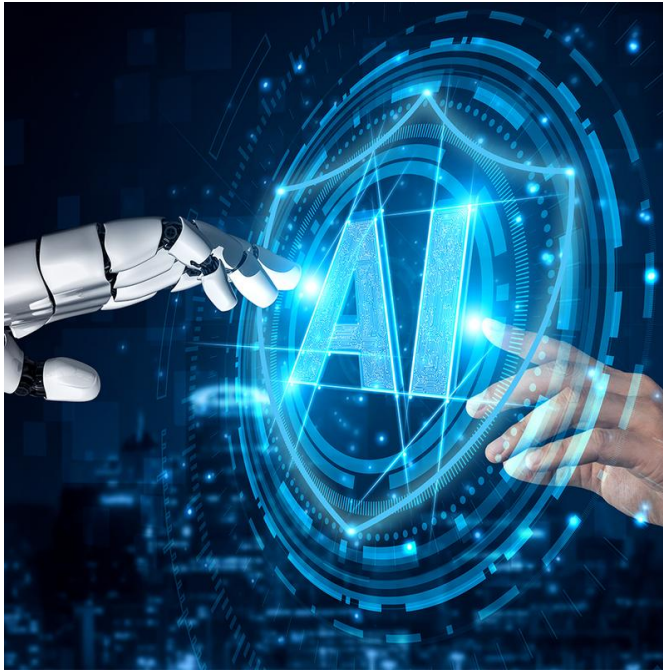
In Pocket speichern

fortiss

Dies ist eine Pressemitteilung von:
**fortiss - Landesforschungsinstitut
 des Freistaats Bayern für softwareintensive Systeme**

Silvia Hervé

Weitere Pressemitteilungen dieser
 Einrichtung



International breakthrough in the field of artificial intelligence: fortiss develops the world's first security standard for AI-based systems with the DKE. | [Download](#)

A milestone toward the future. The DKE (German Commission on Electronics and Information Technologies) sets new standards for safety, compatibility and verifiability in the field of artificial intelligence with the first, detailed framework for the development of trustworthy AI-based systems. The standard (implementation guideline), which was developed under the leadership of the fortiss research institute, is drawing international attention.

Air taxis, fully automated vehicles, smart homes. While artificial intelligence is considered the technology of the future, at present it is subject to hardly any clear definitions or binding guidelines. That makes verifiable safety and dependable standards important conditions for ensuring trustworthiness among industry and consumers in the immense potential of AI systems over the long term.

The DKE standards institute has managed a breakthrough with internatio-

Diese Website verwendet Cookies, um die Bereitstellung unserer Dienste zu optimieren.

[Cookie-Einstellungen...](#)

[Alle Cookies akzeptieren](#)

of fortiss, is already receiving international attention. Japan has expressed a desire to adopt the standard without changes.

Dependable framework for the potential of artificial intelligence

As the third and most recent E/E technology, apart from software and hardware, AI offers tremendous potential for innovations, including in areas such as mobility, medicine and resource protection. When it comes to establishing and adhering to universally-valid safety standards however, AI is still facing major challenges. To cite one example, the development and approval of autonomous/cognitive systems, such as in the automobile sector, can help to drastically reduce traffic volumes and lower the risk of accidents. The issue is that there is currently no method for testing and verifying the safety of such systems in line with dependable standards. In concrete terms, this means that although developers are currently in a position to build a fully automated vehicle, they are still unable to verify that the vehicle is safe in all driving situations. The result is that in many cases the process, from research and development to approval, is bogged down or impeded from the start.

So far what has been missing is a structured development approach, as well as a binding method for monitoring, analyzing and verifying safety in AI-based systems. Furthermore, an interface is lacking that equally meets AI development and standardization criteria and which can verify that a neural network is functional and safe.

Clear standards for creative innovations

This gap has finally been filled by the DKE with the VDE-AR-E 2842-61 implementation guideline by establishing a dependable safety standard that takes into account the current state of research and development. The six-volume publication (plus guiding principles of implementation) thus paves the international way for the structured and verifiable safe development of AI-based systems and represents a reference standard that can lead to an AI seal of quality.

Once such a standard is published, it can be further improved through practical application and experience and also to ensure efficient use by small-to-medium enterprises. The goal is to enable the development of safe AI technologies that meet binding safety standards, thus ensuring that industry and consumers possess the same level of trustworthiness in AI-based systems as they do in hardware and software solutions. The DKE standard is already a significant and visionary step in this direction.

Wissenschaftlicher Ansprechpartner:

Dr. Henrik Putzer

Competence field manager Trustworthy Autonomous Systems

Diese Website verwendet Cookies, um die Bereitstellung unserer Dienste zu optimieren.

[Cookie-Einstellungen...](#)