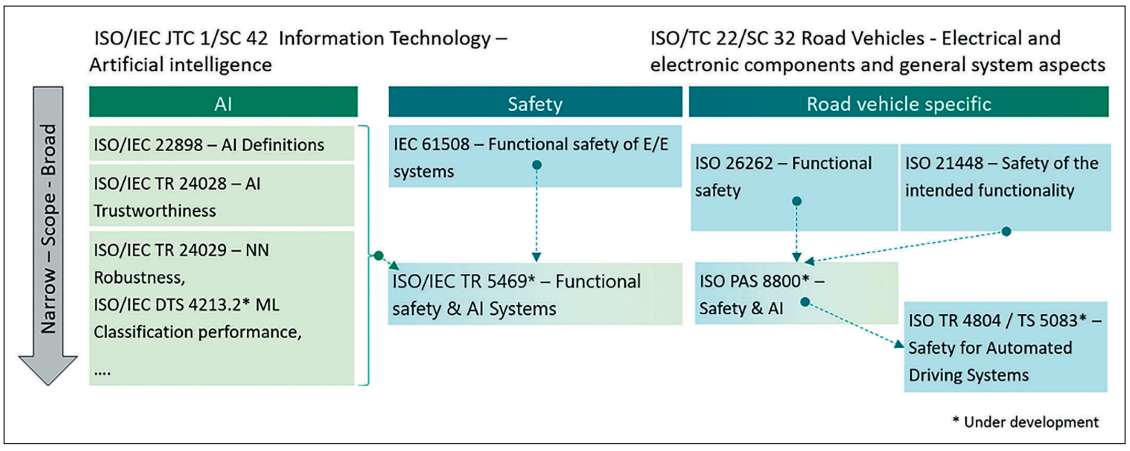

Hierarchie der Normen für künstliche Intelligenz, funktionale Sicherheit und Safety, die insbesondere für Straßenfahrzeuge ausgelegt ist.

Standards

Auf dem Weg zu sicheren KI

Das Fraunhofer-Institut für Kognitive Systeme diskutierte am 15.02.2022 welche Rolle Standards und Normen bei der Nutzung von künstlicher Intelligenz und vor allem maschinellem Lernen in sicherheitskritischen Systemen, zum Beispiel beim automatisierten Fahren, einnehmen.

Autonomes Fahren und künstliche Intelligenz (KI) sind eng miteinander verknüpft. Kein Wunder, denn KI-Systeme können diverse Daten parallel und in Echtzeit verarbeiten, wie den Straßenverlauf, die Straßenschilder und Ampeln oder die Bewegungen anderer Verkehrsteilnehmer. Dafür muss das System lernen, diese Daten zu interpretieren, Situationen zu beurteilen und darauf reagieren zu können.

Damit KI-Systeme in sicherheitskritischen Anwendungen verlässlich arbeiten, bedarf es Normen und Standards. Das von Simon Burton und Karsten Roscher geführte Webinar des Fraunhofer-Instituts für Kognitive Systeme (IKS), beschäftigte sich zunächst mit den Fragestellungen: Wofür sind Normen da und welche Arten von Normen gibt es? Normen formulieren Anforderungen an Produkte, Technologien oder Dienstleistungen und schaffen somit zum einen Klarheit über Eigenschaften. Zum anderen sollen sie Sicherheit und Qualität gewährleisten. Für KI, funktionale Sicherheit und Safety speziell für Straßenfahrzeuge wurden spezifische Normen und Standards definiert (**Bild**), die nicht immer Hand in Hand gehen. Denn bestehende Normen zur Gewährleistung der funktionalen Sicherheit wie die ISO 26262 gehen von einem vollständigen Verständnis eines Systems und dessen Umgebung aus. Ein KI-System erfüllt diese Grundannahme nicht.

Erwartungen relativieren

Man sollte sich vor Augen führen, dass internationale Normen nur einen Konsens über den Stand der Technik und bewährte Verfahren dokumentieren können. Es dauert Zeit, bis der Stand der Technik erreicht ist und Normen festgelegt werden. Agilere Normungsansätze wie technische Berichte und öffentlich verfügbare Spezifikationen können eine schnellere Reaktion ermöglichen, unterliegen aber ähnlichen Einschränkungen. Es besteht immer noch große Unsicherheit darüber, ob und wie künstliche Intelligenz und maschinelles Lernen (ML) sicher gemacht werden kann. Zudem entwickelt sich dieser Bereich sehr schnell. Von daher sind detaillierte und stabile Anforderungen an spezifische Techniken und Anwendungen in nächster Zeit nicht zu erwarten, was sich auf die Sicherheitsbewertung und Zertifizierung der KI-Systeme auswirken wird. Stellt sich nun die Frage, wie lässt sich dennoch eine sichere KI erzielen? Das Fraunhofer IKS schlug folgende Wege vor:

- Argumentieren, dass Unzulänglichkeiten nicht zu sicherheitskritischen Systemausfällen führen, oder
- abwarten, bis eine Reihe geeigneter Methoden zur Gewährleistung der Sicherheit entwickelt wurde oder sich als wirksam erwiesen hat, oder
- Kriterien für wirksame Sicherheitsargumente und entsprechende Nachweise für eine Reihe von Techniken mit Schwerpunkt auf bestimmten Eigenschaften von ML definieren.
- Danach: Definition von Best-Practice-Methoden und Metriken für spezifische Techniken und Anwendungen, wenn sich Best Practice etabliert hat.

Anforderungen

Wenn man den sicheren Einsatz von KI vorantreiben möchte, sollten folgende Anforderungen an Sicherheitsstandards für KI- und ML-basierte cyberphysische Systeme erfüllt sein: Eine Definition eines akzeptablen Sicherheitslevels, eine Definition der sicherheitsrelevanten Eigenschaften von KI und ML und die Identifizierung wirksamer Methoden zur Sammlung von Beweisen. Auch ein strukturierter und iterativer Sicherheitslebenszyklus zur Gewährleistung einer systematischen Anwendung geeigneter Methoden während und nach der Entwicklung ist erforderlich. „KI ist keine Magie", schloss Simon Burton das Webinar. ■ (eck)

www.iks.fraunhofer.de

Stefanie Eckardt ist Chefredakteurin der HANSER automotive.