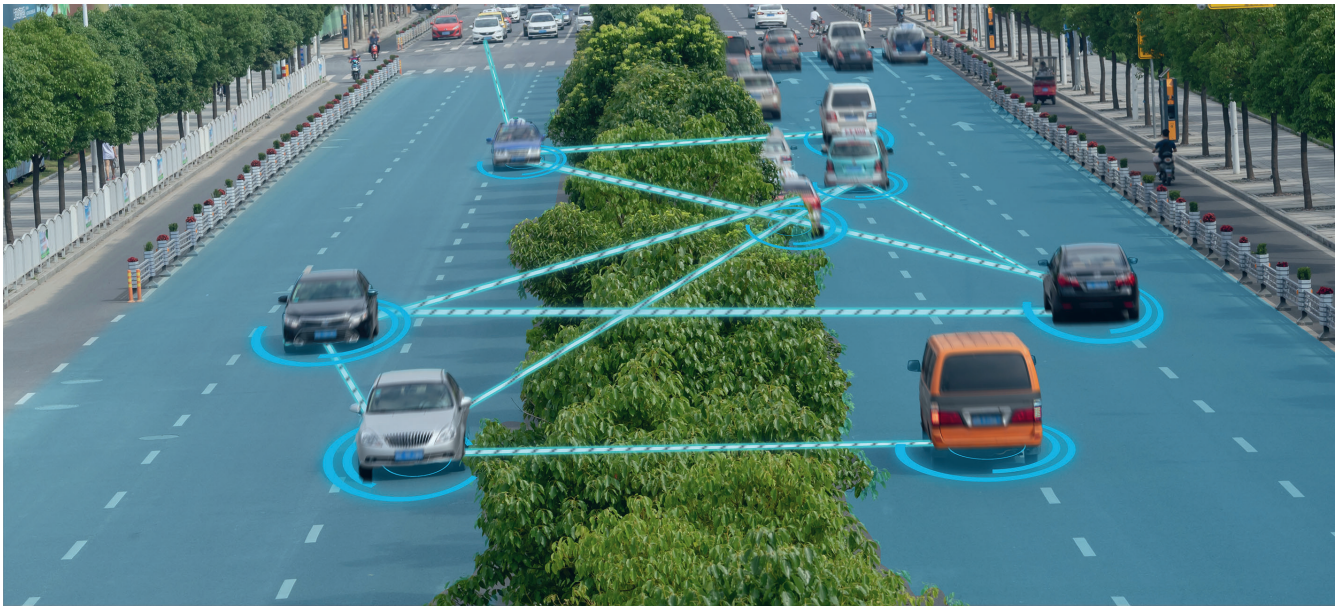

>>> AUTONOMES FAHREN UND KÜNSTLICHE INTELLIGENZ

FuSi für Künstliche Intelligenz

KI ist beim hochautomatisierten Fahren an mehreren Verarbeitungsstufen beteiligt, von der Wahrnehmung bis zur Situationsanalyse und Streckenplanung. Trotz der Schwierigkeit, ihre interne Verarbeitung zu verstehen, kann eine KI-Komponente in Bezug auf Funktionale Sicherheit und SOTIF wie beliebige Hardware- oder Software-Komponenten behandelt werden, wie in diesem Artikel gezeigt wird.

Um immer komplexere Automated Driving (AD)-Aufgaben zu erfassen, muss die Anwendung durch eine zunehmende Vielfalt von Sensoren in Anzahl und Typ eine komplexere und genauere Darstellung der Verkehrssituation erstellen (siehe Bild 1). In der Folge wird das AD-System immer komplexer und unterliegt daher zunehmend verschiedenen Fehlerarten. Ein unerkannter Fehler in einer der Komponenten dieses AD-Systems kann schwerwiegende Folgen haben. Ziel eines sicheren Systems ist es, sicherzustellen, dass Fehler erkannt werden und dass das System genügend Sicherheitsmechanismen implementiert, um das gesamte System in einen sicheren Zustand zu versetzen.

Dennoch zwingt die Komplexität der AD-Komponenten die Anwendungen dazu, die Algorithmen von modellbasierten Techniken auf die der Künstlichen Intelligenz (KI) wie Machine Learning (ML) oder Deep Learning (DL) umzustellen. Solche Verfahren werden zwar immer besser, tendieren aber zur Instabilität, deren Ursprung nur schwer nachzuvollziehen ist.

Vertrauen in die Daten

Die grundlegende Aufgabe einer AD-Anwendung besteht darin, die Daten der Sensoren zu erfassen, die Verkehrssituation auszuwerten, eine sichere Trajektorie zu berechnen und diese zur Ausführung an die Aktoren zu senden. Durch Fehler und Toleranzen der Sensoren leidet das System unter einer gewissen Unsicherheit und beeinflusst damit das Vertrauen, das man in die Detektionen setzen kann. Das Vertrauen kann durch den Einsatz von Sensorfusionstechniken im räumlichen Bereich und Zielverfolgungsmethoden im zeitlichen Bereich erhöht werden. Der Kalman-Filter wird häufig für diesen Zweck verwendet, insbesondere bei Radar.

Die Berücksichtigung des Vertrauensniveaus der Detektionen im Entscheidungsprozess ist bei AD-Anwendungen von entscheidender Bedeutung. Das Vertrauen muss sich durch die Verarbeitungskette ausbreiten. Softwarekomponenten, die auf KI basieren, können Teil der Verarbeitungskette sein und sollten daher nicht anders behandelt werden. Wenn man das Konzept auf das Gesamtsystem, vom Sensor bis zum Stellglied, überträgt, wird es möglich, das Gesamtsystem und die Sicherheit der beabsichtigten Funktion (SOTIF) zu bewerten.

NN-Komponenten einfach halten

Eine Möglichkeit, Fehlprognosen aus einem Neuronalen Netz (NN) erkennen zu können, besteht darin, die Komplexität so gering wie möglich zu halten, es mit Merkmalen (z. B. Geschwindigkeit und Lage von Objekten) zu versorgen und

die Plausibilität der Ein- und Ausgänge zu überprüfen.

Um die NNs jedoch einfach und klein zu halten, muss eine Sammlung von NNs implementiert werden, die jeweils einer bestimmten Aufgabe zugeordnet sind. Dieser Ansatz unterliegt Abweichungen, wenn die Vorverarbeitungsschritte in Bezug auf die Entwicklungsreife nicht stabil genug sind. Es hat auch den Nachteil, dass kaskadierende NNs eine zunehmende Ungenauigkeit verursachen und sich somit auf das SOTIF auswirken können. Die Verwendung eines End-to-End-Ansatzes kann dieses Problem beheben. Deep Convolutional NNs wie das VGG16 haben eine hervorragende Leistung bei der Objekterkennung gezeigt. Aufgrund seiner Komplexität ist es aber auch wesentlich schwieriger, die Ursache von Fehleinschätzungen zu verstehen und damit Sicherheitsmechanismen zu entwickeln, um sie zu verhindern.

Die Situation wird noch komplizierter, wenn die Anwendung Objekte verfolgen muss. Bewegte Objekte wie z. B. Fußgänger oder Fahrzeuge müssen sehr präzise lokalisiert werden, um eine sichere Trajektorie zu berechnen. Damit ein NN auch eine präzise Lokalisierung der erfassten Objekte ermöglicht, wurden Netzwerkdesigns wie das U-Net [2] entwickelt. Das U-Net fügt ein weiteres Level in der Komplexität des NN hinzu. Es macht die Aufgabe, Fehlprognosen zu erkennen, noch komplizierter. Andererseits, wenn die Information über die Position der Objekte verfügbar ist, kann die zeitliche Verfolgung nicht nur mithilfe der Art des Objekts wie beim VGG16, sondern auch mit der Position dieser Objekte erfolgen.

Eine Möglichkeit, die Größe eines NNs auf der Grundlage von Rohbildern zu reduzieren, besteht darin, eine Sammlung von spezialisierten NNs zu verwenden, die der Erkennung sehr spezifischer Objekte, wie z. B. Verkehrszeichen, dienen (siehe Bild 1). Mit einfachen NNs erleichtert es die Gestaltung funktionaler Sicherheitsmechanismen zur Fehlererkennung. Da sie kleiner sind und sehr spezifischen Aufgaben gewidmet sind, sind diese NN in der Regel einfacher zu trainieren.

Erstellung eines ausfallsicheren Systems

Neben der Implementierung von Sicherheitsmechanismen ist es auch möglich, redundante KI-Komponenten einzusetzen. Diese Technik ist ähnlich wie jede Hardware- oder Software-Redundanz. Die Idee ist, mehrere Implementierungen zu verwenden, die auf den gleichen Anforderungen basieren, von verschiedenen Teams implementiert und auf verschiedenen Datensätzen trainiert werden, um systematische Fehler zu vermeiden. Die Ergebnisse der verschiedenen Versionen von NNs werden zusammen mit dem Vertrauen auf ihre Vorhersagen an ein Abstimmungssystem gesendet (siehe Bild 1). Dieses System kann dann die tatsächliche Leistung des NN-Sets ermitteln.

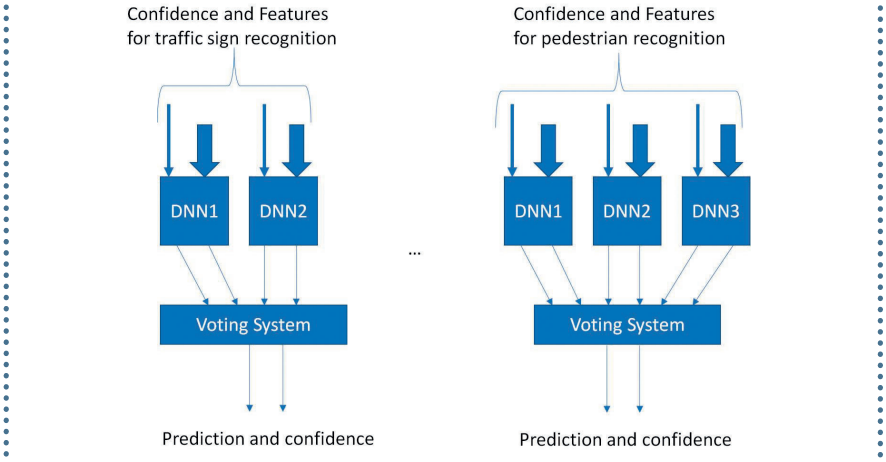

Bild 1: Ein Beispiel für einfache redundante neuronale Netze. Alle sind für eine sehr spezifische Aufgabe vorgesehen. Sie werden in Gruppen unterschiedlicher Größe kombiniert. Ihr Ausgang wird an das Wahlsystem geleitet, das die Prognosen zusammen mit dem Vertrauensniveau bereitstellt. (© KPIT)

Fazit

Autonomes Fahren wird immer komplexer, je höher der Grad der Autonomie ist. Die Anzahl und Vielfalt der Sensoren nimmt zu und die AD-Anwendung erfordert immer ausgefeiltere Algorithmen zur Erfassung der Verkehrssituation und der Umgebung des Fahrzeugs.

Die KI ist an einer wachsenden Anzahl von Verarbeitungsstufen beteiligt, von der Wahrnehmung über die Situationsanalyse bis hin zur Trajektorienplanung. Trotz der Schwierigkeit, ihre interne Verarbeitung zu verstehen, kann die KI-Komponente in Bezug auf Funktionale Sicherheit und SOTIF wie jede andere Hard- und Softwarekomponente behandelt werden. Um die KI-Komponenten herum können funktionale Sicherheitsmechanismen aufgebaut werden. Sie können die Konsistenz der Vorhersagen sowohl im räumlichen als auch im zeitlichen Bereich überprüfen. Die zeitliche Domäne muss mit Vorsicht behandelt werden, wenn es darum geht, zeitliche Beschränkungen in den Sicherheitsanforderungen festzulegen.

Auf der anderen Seite bietet die Norm ISO 26262 Werkzeuge zur Zuordnung von Fehlerwahrscheinlichkeiten und zur Analyse des Gesamtsystems mit KI. Sicherheitsmechanismen können für das Gesamtsystem einschließlich der KI-Komponenten konzipiert werden. Die Normen Für Funktionale Sicherheit und SOTIF sind eine große Hilfe bei der Weiterentwicklung der gesamten Softwarearchitektur, sodass alle Sicherheitsanforderungen erfüllt und die Sicherheitsziele erreicht werden können. ■ (oe)

» **www.kpit.com**

Quellenverzeichnis

[1] *Very Deep Large Convolutional Networks for Large-Scale Image Recognition*, K. Simonyan und A. Zisserman, 10–04–2015, Veröffentlicht ICLR 2015,

[2] *Convolutional Networks for Biomedical Image Segmentation*, O. Ronneberger, P. Fischer und T. Brox, 18–05–2015

Oliver Bockenbach ist Subject Matter Expert Autonomous Driving bei KPIT.