sepp.med

WHITEPAPER

BOUNDED INTELLIGENCE

Wie funktionale Sicherheit, Cybersecurity und SOTIF KI im Fahrzeug nachweisbar machen

Wir machen **DIGITALISIERUNG** – aber **SICHER!**

www.seppmed.de

Inhalt

1. EXECUTIVE SUMMARY

Künstliche Intelligenz ist in der Fahrzeugentwicklung angekommen, und zwar quer durch alle Domänen. Machine Learning (ML) Modelle übernehmen Aufgaben in der Umfeldwahrnehmung, optimieren Energiemanagement-Strategien in elektrifizierten Antrieben, priorisieren Warnmeldungen im Human-Machine Interface (HMI) und steuern adaptive Fahrwerksfunktionen. Doch die klassischen Sicherheitsmethoden, die jahrzehntelang deterministische Systeme verlässlich abgesichert haben, stoßen bei probabilistischen ML-Komponenten an methodische Grenzen. Unabhängig davon, ob das Modell in einem ADAS (Advanced Driver Assistance Systems) Steuergerät, einem Batteriemanagementsystem oder einer Instrumentencluster-Software arbeitet.

Dieses Whitepaper zeigt, warum KI im Fahrzeug keine neue Safety-Disziplin erfordert, sondern eine konsequente Erweiterung des bestehenden Engineering-Instrumentariums. Im Zentrum steht ein integriertes Engineering-Modell, das funktionale Sicherheit (Functional Safety, FuSi), Cybersecurity und SOTIF (Safety of the Intended Functionality) in einem gemeinsamen Prozess zusammenführt:

Eine harmonisierte FMEA (Fehlermöglichkeits- und Einflussanalyse) bildet dabei das Bindeglied zwischen den Disziplinen.

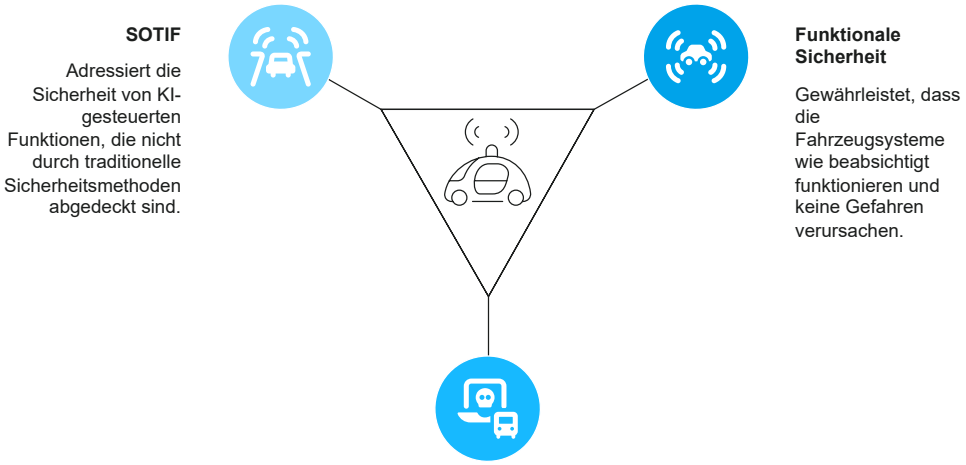
KI-spezifische Architekturmuster wie Shadow Mode und Confidence-Based Decisions machen nichtdeterministisches Verhalten beherrschbar.

Szenariobasierte Validierung ersetzt die unzureichende Code-Coverage-Logik für ML-Wahrnehmungsfunktionen.

Wer dieses Fundament heute legt, ist vorbereitet auf die regulatorische Welle ab 2027, statt sie unter Termindruck kurz vor Start of Production (SOP) nacharbeiten zu müssen.

Wo Ihr Programm heute steht und wo die größten Lücken liegen, zeigt der 30-Punkte-Reifegrad-Check: https://go.seppmed.de/reifegrad-check-automotive-ki

Integriertes Engineering-Modell



2. KERNAUSSAGEN AUF EINEN BLICK

- Eine **harmonisierte FMEA** verbindet Safety-FMEA, TARA (Threat Analysis and Risk Assessment) und SOTIF-Analyse unter einem gemeinsamen Vokabular und vermeidet so doppelte Risikoartefakte.

- **Bounded Intelligence** definiert nachweisbare Verhaltensgrenzen für ML-Modelle und macht nichtdeterministisches Verhalten in der Safety-Argumentation handhabbar, ob in der Umfeldwahrnehmung, im Antriebsstrang oder in der Fahrerinteraktion.

- **Szenariobasierte Validierung** in Simulation, SIL (Software in the Loop), MIL (Model in the Loop), HIL (Hardware in the Loop) und Track-Erprobung ersetzt die für ML-Funktionen ungeeignete klassische Code-Coverage.

- **Auditfähige Traceability** von der Anforderung bis zur Evidenzmappe gewährleistet Nachweissicherheit über die gesamte Lieferkette.

- **Frühzeitige methodische Integration** vermeidet kostspielige Late Findings: Die in der Qualitätssicherung etablierte Zehnerregel besagt, dass sich die Kosten zur Fehlerbehebung mit jeder späteren Prozessphase typischerweise verzehnfachen. Fehler, die erst nach SOP im Feld auftreten, sind damit um Größenordnungen teurer als solche, die in der Designphase erkannt werden [1].

- Die **regulatorische Welle ab 2027**, insbesondere der EU AI Act (Artificial Intelligence Act) mit Hochrisiko-Anforderungen für KI als Sicherheitskomponente, belohnt Organisationen, die ihr Engineering-Fundament heute schon auf Morgen vorbereiten.