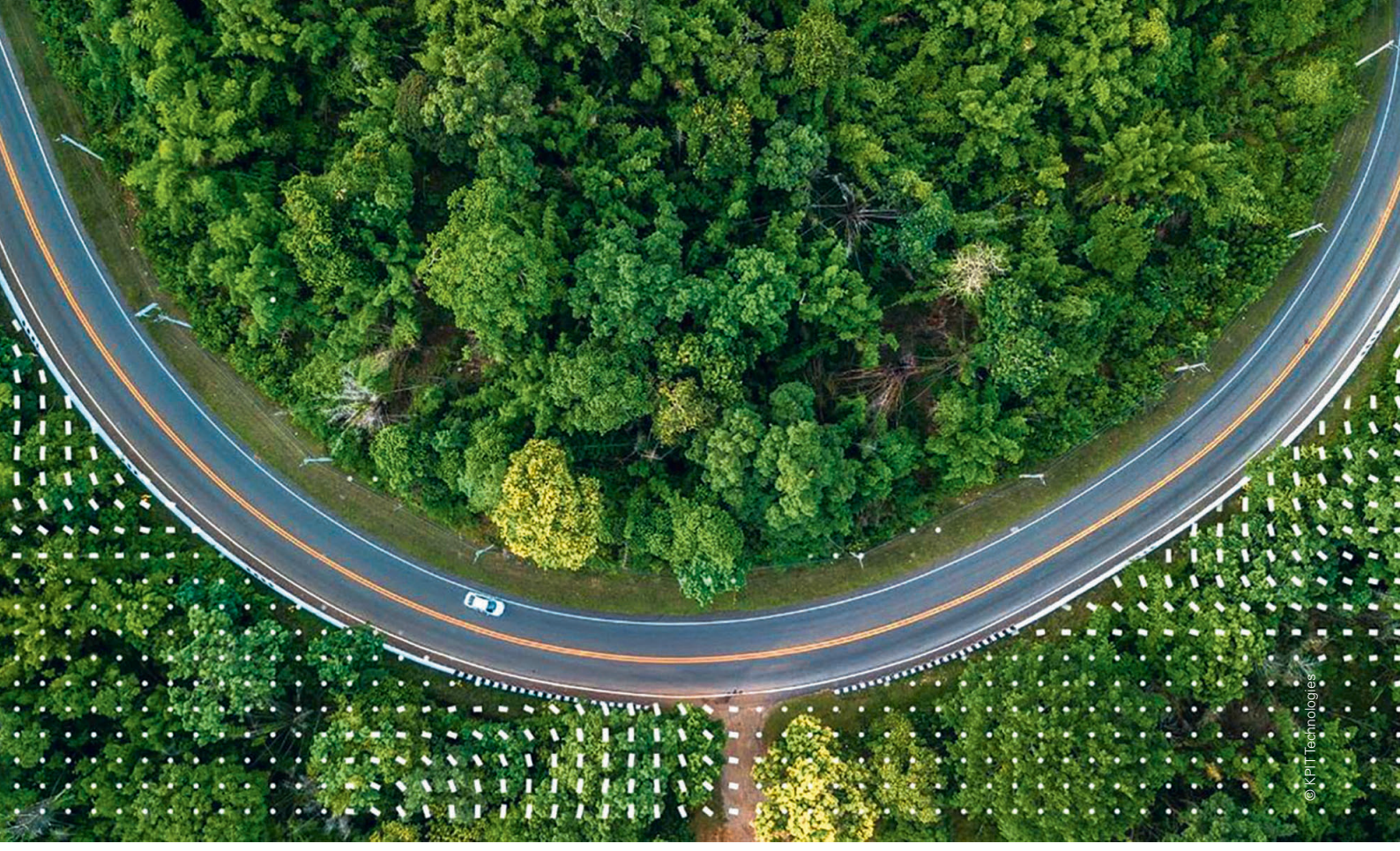

AUTOMATISIERTE FAHRFUNKTIONEN

Betriebssichere Architektur als **Sekundärkanal**

Angesichts der beabsichtigten Serienfertigung autonomer Fahrzeuge tritt die Komplexität sicherheitsorientierter autonomer Software immer deutlicher zu Tage. In diesem Fachbeitrag von KPIT Technologies wird ein systematischer Ansatz zur Ableitung einer betriebssicheren Architektur am Beispiel einer autonomen Autobahnpilot-Funktion diskutiert. Dazu werden detaillierte Systementwicklungstätigkeiten und Funktionssicherheitsanalysen durchgeführt.

Die Komplexitäten sicherheitsorientierter autonomer Software ergeben sich aus mehreren Faktoren wie Sicherheitskonformität, datengestützter Sicherheitsarchitektur, Integration, Testabdeckung, virtueller Simulation, Laufleistungsabdeckung und Homologation. Dementsprechend kommt es bei den meisten Produktionsprogrammen für die Autonomiestufe L3 und höher zu Verzögerungen. Des Weiteren ist die Erfüllung der ISO 26262 im kompletten Software-Stack für das autonome Fahren ein kritischer Aspekt um die Anforderungen von L3 und höherer Autonomiestufen zu erfüllen.

Eine „betriebssichere" redundante Softwareschicht als Sekundärkanal sorgt für Redundanz im Software-Stack für das autonome Fahren, um die ASIL D-Anforderungen zu erfüllen. Auch wenn jede Funktion und jedes Leistungsmerkmal im Primärkanal dem Sicherheitskonzept entsprechen muss, ist ein Sekundärkanal zur Erfüllung der ASIL D-Anforderungen ebenfalls unerlässlich, da dessen „betriebssichere" Funktion bei einem Ausfall des Primärkanals die dynamische Fahraufgabe übernimmt, um die Fahrsicherheit des autonomen Fahrzeugs zu gewährleisten.

Sekundärkanal

Wenn Störungen im Primärkanal erkannt werden und der Fahrer nicht rechtzeitig die Kontrolle übernimmt, übernimmt die Sekundärkanalfunktion den gestörten Betrieb, der zum sicheren

Stopp des autonomen Fahrzeugs führt. Dies wird durch eine voll funktionsfähige betriebssichere Software erreicht, die Erkennung, Wahrnehmung, Lokalisierung, Planung und Bewegungssteuerung umfasst. Zur Definition der Architektur der Sekundärkanalsoftware wurde eine detaillierte Systementwicklungs- und Sicherheitsanalyse gemäß ISO 26262-Prozess durchgeführt, die später beschrieben wird. Eine L3-Funktion im System wird erwogen zur Ableitung der Elementdefinitionen, Betriebsbedingungen und Gefahrenanalyse und Risikobewertung (HARA). Diese Störungen werden dann als Teil von HARA analysiert und minimale Risikoanteile (MRC) definiert. Um das System während eines Ausfalls in einen sicheren Zustand zu bringen, werden MRCs die Grundlage zur Definition von MRMs. Die betriebssichere Architektur für einen Sekundärkanal wird anhand der MRMs definiert.

Ein hochautomatisiertes Fahrsystem oder L3+ System stützt sich bei allen dynamischen Fahraufgaben hauptsächlich auf das System selbst. Dazu gehören Längs- und Querregelung, Objekterfassung und -erkennung und Fallback bei dynamischen Fahraufgaben. Beim hochautomatisierten Fahrsystem wird davon ausgegangen, dass der auf einen Fallback vorbereitete Benutzer kurzfristig wieder die Kontrolle übernimmt, wenn das System ihn dazu auffordert. Diese Systeme können nicht erwarten, dass der Fahrer angesichts der begrenzten Reaktionszeit auf die Aufforderung reagiert. Der Schlüssel zur Lösung dieses Problems liegt in einem höheren Grad an Autonomie und Verfügbarkeit und einer Verbesserung des Systems. Eine betriebssichere Architektur für das autonome Fahrsystem ist erforderlich, um ein akzeptables Sicherheitsniveau zu erreichen, und sie muss das minimale Risikomanöver ausführen, um das System in einen sicheren Zustand zu bringen, wenn irgendwelche Komponenten oder Unterfunktionen ausfallen. Das betriebssichere System muss von Störungen verursachte Fehler erfassen, den Schaden beurteilen, den Fehler in fehlertoleranter Zeit beheben und die Störung isolieren. Das System gewährleistet die Integrität der zur Steuerung der Fahr-

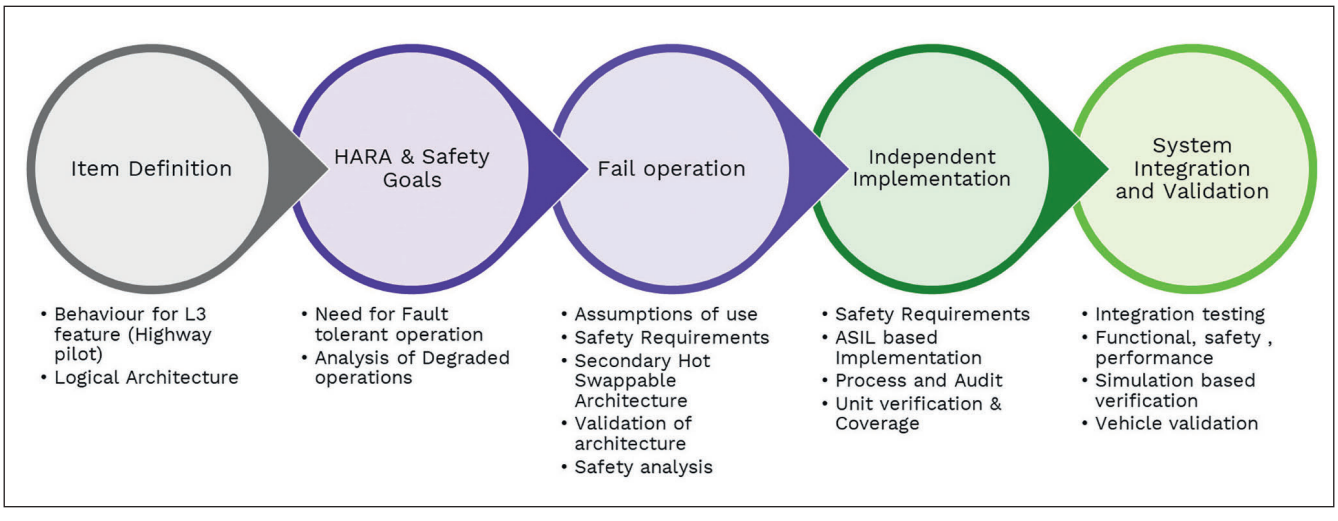

Bild 1: Sicherheitsprozess zur Definition der betriebssicheren Architektur. © KPIT Technologies

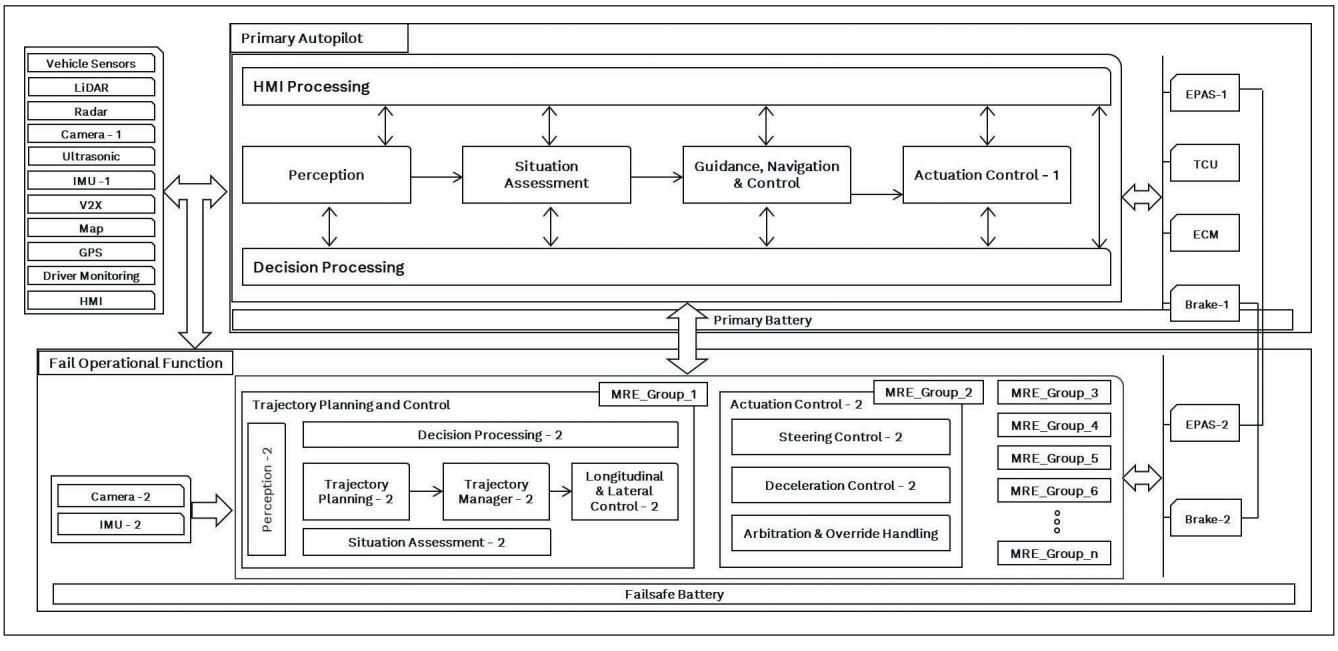

Bild 2: Betriebssichere Architektur für die Sekundärfunktionen. © KPIT Technologies

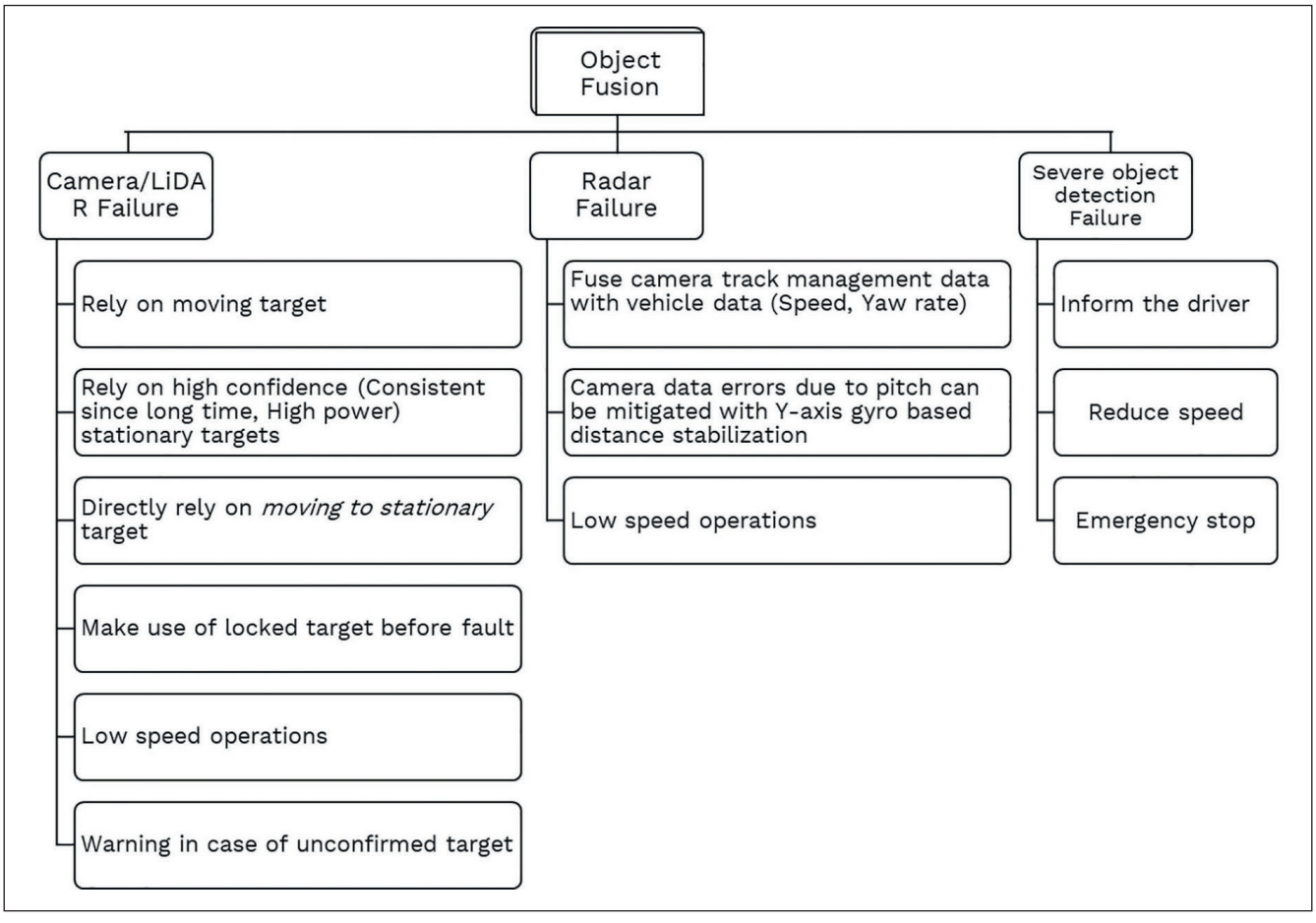

Bild 3: Abgeleitete mögliche MREs für Objektfusionsstörungen. © KPIT Technologies

zeugstellantriebe verwendeten Ausgangsdaten und sorgt bei Störungen für einen kontinuierlichen sicheren Betrieb. Eine Möglichkeit zur Erreichung von Betriebssicherheit ist die Erhöhung der Redundanz von Sensoren, Steuerungen, Stellgliedern usw., dies führt jedoch zu mehr Kosten, Gewicht und Raumbedarf, und dies sind einige der Sachzwänge in der Automobilindustrie. Die Lösung kann also nur im Software-Stack liegen. Der Prozess zur Definition, Entwicklung und Validierung einer Sicherheitsfunktion

Validierung der Sicherheitsfunktion

Bevor wir uns mit den Details der Architektur beschäftigen, ist es sehr wichtig, den vollständigen Prozess zu verstehen, der zur Definition, Entwicklung und Validierung solcher Sicherheitsfunktionen befolgt wird. In Bild 1 ist der Prozessablauf dargestellt.

Ein Prozess gewährleistet eine systematische Entwicklung sicherer Software. Im Allgemeinen wird der Detailprozess vor Realisierung des Prototyps nicht genau befolgt. Aber für das betriebssichere System ist es von entscheidender Bedeutung, den Prozess zur Definition der Architektur zu befolgen, der aus den Artefakten der Sicherheitsanalyse abzuleiten ist.

Die Architektur der Sekundärfunktion

Durch ein durchdachtes System und die Sicherheitsentwicklung wird die betriebssichere Architektur abgeleitet, um die ASIL D-Anforderungen auf der Ebene des autonomen Fahrsystems zu erfüllen. In Bild 2 ist die Systemarchitektur zur Sicherstellung einer sicheren Fahrt auf der Autobahn durch die Primär- und Sekundärfunktionen dargestellt. Sowohl die Primär- als auch die Sekundärfunktion sind mit einer unabhängigen Stromversorgung galvanisch getrennt, um Einzelpunktfehler zu vermeiden. Eine ungleiche Softwarearchitektur (primär und sekundär) würde mehr Robustheit und Neutralität durch verschiedene Technologie bieten, da es unterschiedliche Besitzer gibt.

Basierend auf dem Szenario in der Architektur wird jeder Komponentenausfall analysiert, und daraus werden mehrere mögliche MREs abgeleitet. Diese MREs werden dann in der Architektur (Abbildung 2) nach Komponentenschicht gruppiert. Das Ziel all dieser MREs ist die Erreichung der endgültigen MRC in Form von Sicherheit/Komfort/Not-Halt. Beispielsweise wird MRE_Gruppe1 zur Ableitung der internen MREs ausgearbeitet, um eine betriebssichere Bedingung im Fall irgendeines Komponentenversagens zu erreichen.

Die Architektur berücksichtigt geeignete Schnittstellen mit Primärkanalfunktionen wie zum Beispiel Sensor-, Anwendungs- und Middleware-Schnittstellen. Jede Schicht der Architektur wird in verschiedene MRE-Gruppen aufgeteilt (Wahrnehmung, Fahrstrecke, Fahrzeugbewegungskontrolle, usw.). Ein rei-

bungsloser Übergang von der Ausführung des Primärsystems zur betriebssicheren Funktion muss gewährleistet sein.

MRE_Gruppe1: Wahrnehmung

Die Wahrnehmungskomponente kann aufgrund eines oder mehrerer Komponentenausfälle auf den Ebenen der Objekt-, der Spur- und/oder der Sensorfusion fehlschlagen. Für jeden Komponentenausfall wird eine detaillierte Analyse durchgeführt, um interne MREs abzuleiten und einen eingeschränkten Betrieb zu erreichen.

Störungen in der Signalerfassung

Wie in Bild 3 gezeigt, kann die Objektfusion aus mehreren Gründen wie Kameraerfassungs- oder Radererfassungsstörungen oder beidem fehlschlagen, was schwerwiegende Objekterfassungsfehler zur Folge hat. Wenn zum Beispiel der Ausfall eines Kamerasensors festgestellt wird, kann sich das Wahrnehmungsmodul immer noch auf andere Sensoren stützen, wenn ein bewegliches Objekt per Radar erfasst wird. Einige andere Techniken wie die Sperre der Zielinformationen, wenn sie über mehr als einen bestimmten Zeitraum erfasst werden und die Verwendung dieser historischen Informationen vor dem Fehlerzustand kann helfen, den ausfallsicheren Betrieb durchzuführen. Ebenso lassen sich bei Ausfall der Radarerfassung Kameradatenfehler aufgrund von Pitch durch kreiselbasierte Abstandsstabilisierung abmildern.

Spurfusionsstörung

Wenn es eine Teilfahrspurerkennung oder Kameradaten mit geringer Zuverlässigkeit gibt, lässt sich die Ego-Spurgeometrie auf Basis anderer Verkehrsobjektpfade schätzen. Werden die Straßenränder oder die Leitplanke erfasst (Cluster in Radarreflexionen), können sie bei der Erstellung virtueller Spurinformationen helfen. Im ungünstigsten Fall, wenn keine Spurinformationen verfügbar sind, kann sie sich auf vordere oder seitliche Zielinformationen stützen und dem Zielobjekt in einem sicheren Abstand folgen.

Bei zeitweise auftretenden IMU-Störungen hilft die Verwendung dynamischer Modelle und Fahrzeugzustände (Fahrzeugsensor) und die Auslegung von linearen/erweiterten/Unscented Kalman-Filtern die Sensorgenauigkeit zu verbessern. Bei schwerwiegenden Fehlern empfiehlt sich jedoch ein redundanter Sensor für den Sekundärkanal in der Architektur.

Fazit

Der Bedarf an der sekundären Sicherheitsfunktion wurde im Systementwicklungsprozess erkannt. Ein systematisches Konzept zur Entwicklung einer betriebssicheren Sekundärfunktion gemäß ISO 26262 wurde anhand eines Beispiels besprochen.
Die unabhängige Entwicklung der Sicherheitsfunktion mit allen Systemen und Sicherheitsartefakten würde die Konzentration auf die Besitzer der Primärfunktion beseitigen. Die Architektur ist modular ausgelegt und lässt sich individuell anpassen und in die Primärfunktionen und Middleware integrieren, um den Software-Stack für das autonome Fahren kompatibel zu ASIL-Anforderungen zu machen.
Dies beschleunigt seinerseits die Entwicklung des autonomen Fahrens bei gleichzeitiger Erfüllung der gesetzlichen Anforderungen. ■ (oe)

www.kpit.com

Dr. Manaswini Rath ist Vice President and Global Head Autonomous Driving bei KPIT Technologies.

Reshma Sheerin ist Senior Solution Architect bei KPIT Technologies.