(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. August 2020 (20.08.2020)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2020/165058 A1

(51) Internationale Patentklassifikation:
G05D 1/00 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2020/053236

(22) Internationales Anmeldedatum:
10. Februar 2020 (10.02.2020)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2019 202 025.9
15. Februar 2019 (15.02.2019) DE

(71) Anmelder: **ZF FRIEDRICHSHAFEN AG** [DE/DE]; Löwentaler Straße 20, 88046 Friedrichshafen (DE).

(72) Erfinder: **HIEMER, Marcus**; Sammletshofer Str. 25, 88074 Meckenbeuren (DE). **HEINRICHS-BARTSCHER, Sascha**; Austinstraße 72, 56075 Koblenz (DE). **MOHR, Mark**; Dr. Alex-Frick-Weg 8, 88069 Tettnang (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) **Title:** SYSTEM AND METHOD FOR THE SAFE OPERATION OF AN AUTOMATED VEHICLE

(54) **Bezeichnung:** SYSTEM UND VERFAHREN ZUM SICHEREN BETREIBEN EINES AUTOMATISIERTEN FAHRZEUGS

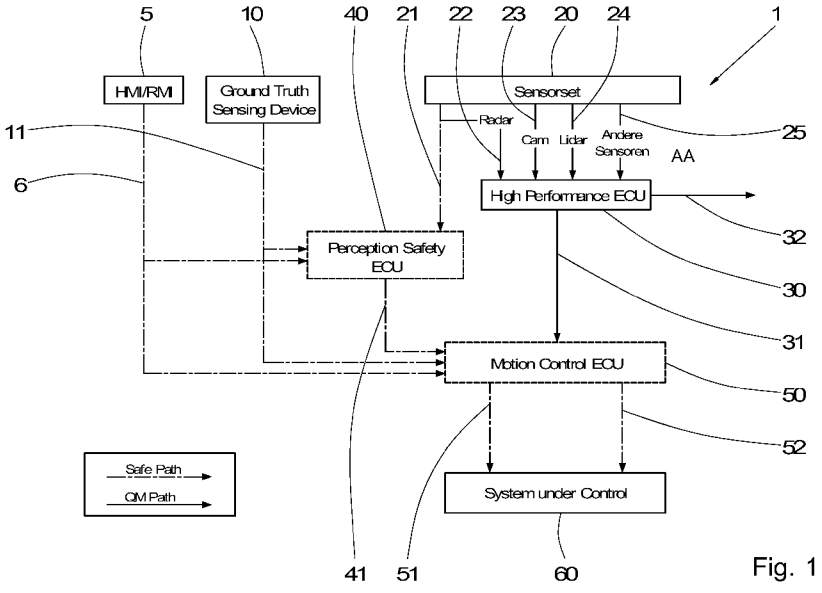

Fig. 1

20 Sensor Set
AA Other Sensors

(57) **Abstract:** The invention relates to a system for the safe operation of an automated vehicle, comprising a first network having a high performance ECU (30) which processes signals from a plurality of sensors (76-82) for orientation, control and collision avoidance in order to enable environmental and object detection and classification such that complex motion control is enabled. The high performance ECU (30) is coupled to a safe motion controller, motion control ECU (50), which is coupled to at least one drive element (90, 92, 94, 96) by means of at least two control signals (51, 52) redundantly for controlling the vehicle (70). In addition, a second, hierarchical, redundant network is provided for safe operation of the vehicle, which second network comprises an HMI/RMI (5) having at least one emergency switch-off device, a ground truth sensing device (10) for determining the position of objects in relation to the vehicle and a

WO 2020/165058 A1

[Fortsetzung auf der nächsten Seite]

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

perception safety ECU (40) in the form of a control unit which is coupled to the HMI/RMI (5), to the ground truth sensing device (10) and to at least one radar sensor by means of reliable connections in order to derive, from the transmitted signals, a reliable collision notification signal (41) which is fed to the motion control ECU (50) by means of a reliable connection such that the signals of the HMI/RMI (5), of the ground truth sensing device (10) and of the perception safety ECU (40) are reliably evaluated to detect an emergency state, in order to redundantly control the vehicle (70) into a safe state by means of at least two control signals (51, 52) if an emergency state is detected.

(57) Zusammenfassung: Es wird ein System zum sicheren Betreiben eines automatisierten Fahrzeugs offenhart, mit einem ersten Netzwerk, mit einer High Performance ECU (30) die Signale von einer Mehrzahl von Sensoren (76-82) zur Orientierung, Steuerung und Kollisionsvermeidung verarbeitet, um eine Umgebungs- und Objekterkennung und Klassifizierung zu ermöglichen, um eine komplexe Bewegungssteuerung zu ermöglichen. Die High Performance ECU (30) ist mit einer sicheren Bewegungssteuerung Motion Control ECU (50) gekoppelt, die mit mindestens einem Antriebselement (90, 92, 94, 96) über mindestens zwei Steuersignale (51, 52) redundant zur Steuerung des Fahrzeugs (70) gekoppelt ist. Zusätzlich ist ein zweites, hierarchisches, redundantes Netzwerk zum sicheren Betreiben des Fahrzeugs vorgesehen, das ein HMI/RM (5) mit zumindest einer Not-Aus-Schalteinrichtung, ein Ground Truth Sensing Device (10) zur Positionsbestimmung von Objekten relativ zum Fahrzeug, und eine Perception Safety ECU (40) aufweist, in Form eines Steuergerätes, das über sichere Verbindungen mit dem HMI/RMI (5), dem Ground Truth Sensing Device (10), und mindestens einem Radarsensor gekoppelt ist, um aus den übertragenen Signalen ein sicheres Kollisionsmeldesignal (41) abzuleiten, das der Motion Control ECU (50) über eine sichere Verbindung zugeführt ist, um die Signale der HMI/RMI (5), des Ground Truth Sensing Device (10) und der Perception Safety ECU (40) zur Erkennung eines Notzustands sicher auszuwerten, um das Fahrzeug (70) im Falle der Erkennung eines Notzustands über mindestens zwei Steuersignale (51, 52) redundant in einen sicheren Zustand zu steuern.

System und Verfahren zum sicheren Betreiben eines automatisierten Fahrzeugs

Die Erfindung betrifft ein System und ein Verfahren zum sicheren Betreiben eines automatisierten Fahrzeugs.

Hochautomatisierte, fahrerlose Arbeitsmaschinen werden dazu eingesetzt, einen komplexen Prozess effizient abarbeiten zu können. Neben der Prozessaufgabe muss sich das Fahrzeug automatisiert beispielsweise über Felder, auf Baustellen oder in Betriebshöfen bewegen und sich dabei häufig selbst orientieren. Für diese Orientierungsaufgabe und für die Erkennung der Umwelt zur Kollisionsvermeidung werden eine Vielzahl von Sensoren eingesetzt und verarbeitet. Die Verarbeitung dieser Daten erfolgt in immer rechenstärkeren, sog. High Performance ECUs. Häufig kommen dafür Maschinenlernverfahren wie Deep Neural Networks (DNN) zum Einsatz. Die verschiedenen Sensoren, ECUs und sonstigen Bestandteile sind über ein Fahrzeugnetzwerk gekoppelt, in dem Signale in nur mit Qualitätsmaßnahmen entwickelten Signalzweigen (QM) übertragen werden. Dies bedeutet, dass die Signale auf diesem Pfad zwar mit hoher Qualität ermittelt und übertragen werden, jedoch genügen diese Signale keinem Sicherheitsstandard und werden auch nicht mit Zusatzmaßnahmen besonders sicher über das Fahrzeugnetzwerk übermittelt.

Neben der Bewegung des Fahrzeugs zur Erfüllung einer Prozessaufgabe ist jedoch auch die Sicherheit des Fahrzeugs bei Bewegungen zu gewährleisten. Zusätzlich zum Fahrzeugnetzwerk mit QM-Wegen muss daher ein sicheres, mehrfach redundantes System geschaffen werden, um das Fahrzeug in einer Notsituation oder im Falle eines Ausfalls des QM-Netzwerks gefahrlos in einen sicheren Zustand zu überführen.

Im Stand der Technik sind zwar elektrische Netzwerkarchitekturen bekannt (vgl. DE 10 2012 102 173 A1), bei denen eine Vielzahl von Sensoren und Aktuatoren mit zwei oder mehr elektronischen Kontrolleinheiten (ECUs) zum Verarbeiten von Daten von den Sensoren und zum Erlassen von Befehlen an die Aktuatoren und mit zwei oder mehr Interface-Geräten zum Verbinden der Sensoren und Aktuatoren an die ECUs und mit einem Kommunikations-Bus vorgesehen sind, wobei die Interface-Gerätesoftware rekonfigurierbar sind, um die Konnektivität zu modifizieren.

Durch derartige Maßnahmen wird eine bessere und flexiblere Nutzung der Sensoren und Aktuatoren ermöglicht und im Falle eines Interface-Geräteausfalls eine gewisse Fehlertoleranz gewährleistet.

Ein derartiges System ist jedoch nicht ausreichend, um in einer Notfallsituation oder im Falle eines Ausfalls des Bordnetzes oder wichtiger Gerätekomponenten eine gefahrlose Überführung des Fahrzeugs in einen sicheren Zustand zu ermöglichen.

Vor diesem Hintergrund liegt der Erfindung die Aufgabe zugrunde, ein System und ein Verfahren zum sicheren Betreiben eines automatisierten Fahrzeugs anzugeben, bei dem im Falle des Auftretens eines Notzustands etwa durch eine Kollisionsgefahr oder im Falle eines Ausfalls des Bordnetzes oder einzelner Komponenten davon eine gefahrlose Überführung des Fahrzeugs in einen sicheren Zustand gewährleistet ist.

Die vorliegende Erfindung beschreibt hierzu ein hierarchisches, mehrfach redundantes E/E-Netzwerk (elektrisch/elektronisches Netzwerk) zum sicheren Betreiben eines automatisierten Fahrzeugs.

Die Aufgabe der Erfindung wird gelöst durch ein System zum Betreiben eines automatisierten Fahrzeugs, mit:

(a) einem ersten Netzwerk, mit

- einem Sensorset mit einer Mehrzahl von Sensoren zur Erfassung der Umgebung des Fahrzeugs, der mit einer High Performance ECU gekoppelt ist, welche die Signale der Sensoren zur Orientierung, Steuerung und Kollisionsvermeidung verarbeitet; und

- einer sicheren Bewegungssteuerung Motion Control ECU, die mit mindestens einem Aktuator über mindestens zwei Steuersignale redundant zur Steuerung des Fahrzeugs gekoppelt ist;

- wobei die High Performance ECU ein Object Recognition Indicator Signal zur Orientierung, Steuerung und Kollisionsvermeidung an die Motion Control ECU ausgibt;

(b) einem zweiten, hierarchischen, redundantem Netzwerk zum sicheren Betreiben des Fahrzeugs, mit:

- einem HMI/RMI (Human/Remote Machine Interface) mit zumindest einer Not-Aus-Schalteinrichtung;

- einem Ground Truth Sensing Device zur Positionsbestimmung von Objekten relativ zum Fahrzeug;

- einer Perception Safety ECU, in Form eines Steuergerätes, das über sichere Verbindungen mit dem HMI/RMI, dem Ground Truth Sensing Device und mindestens einem Radarsensor gekoppelt ist, um aus den übertragenen Signalen ein sicheres Kollisionsmeldesignal abzuleiten, das der Motion Control ECU über eine sichere Verbindung zugeführt ist;

- wobei die Motion Control ECU dazu ausgebildet ist, die Signale der HMI/RMI, des Ground Truth Sensing Device und der Perception Safety ECU zur Erkennung eines Notzustands sicher auszuwerten, um das Fahrzeug im Falle der Erkennung eines Notzustands über mindestens zwei Steuersignale redundant in einen sicheren Zustand zu steuern.

Gemäß einem weiteren Aspekt der Erfindung wird ein Verfahren zum sicheren Betreiben eines automatisierten Fahrzeugs offenbart, bei dem

(a) in einem ersten Netzwerk

- ein Sensorset mit einer Mehrzahl von Sensoren zur Erfassung der Umgebung des Fahrzeugs, mit einer High Performance ECU gekoppelt wird und die Signale der Sensoren zur Orientierung, Steuerung und Kollisionsver-

meidung verarbeitet werden, um ein Object Recognition Indicator Signal zur Orientierung, Steuerung und Kollisionsvermeidung zu erzeugen, das

- an eine sichere Bewegungssteuerung Motion Control ECU übertragen wird, die mindestens einen Aktuator zur Steuerung des Fahrzeugs über mindestens zwei Steuersignale redundant sicher steuert;

(b) in einem zweiten, hierarchischen, redundantem Netzwerk zum sicheren Betreiben des Fahrzeugs

- ein HMI/RMI mit mindestens einer Not-Aus-Schalteinrichtung; und

- ein Ground Truth Sensing Device zur Positionsbestimmung von Objekten relativ zum Fahrzeug;

- mit einer Perception Safety ECU in Form eines Steuergerätes über sichere Verbindungen gekoppelt werden, und der Perception Safety ECU ferner das Signal mindestens eines Radarsensors zugeführt wird, um aus den übertragenen Signalen ein sicheres Kollisionsmeldesignal abzuleiten, das der Motion Control ECU über eine sichere Verbindung zugeführt wird;

- wobei die Motion Control ECU die Signale der HMI/RMI, des Ground Truth Sensing Device und der Perception Safety ECU auswertet, um einen Notzustand sicher zu erkennen, in dem das Fahrzeug über mindestens zwei Steuersignale redundant in einen sicheren Zustand gesteuert wird.

Erfindungsgemäß wird durch das zweite, hierarchische, redundante E/E-Netzwerk im Falle der Erkennung eines Notzustands eine sichere Überführung des Fahrzeugs in einen sicheren Zustand gewährleistet, indem die Motion Control ECU das Fahrzeug über mindestens zwei Steuersignale redundant steuert.

Hierzu ist ein vom ersten Fahrzeugnetzwerk getrenntes, zweites, hierarchisches, redundantes E/E-Netzwerk vorgesehen, in dem die Motion Control ECU über eine sichere Verbindung eingebunden ist.

Die Motion Control ECU wertet die sicheren Abschaltsignalindikatoren aus, die vom HMI/RMI, vom Ground Truth Sensing Device und von der Perception Safety ECU kommen.

Die Perception Safety ECU wertet die sicheren Signale der HMI/RMI und des Ground Truth Sensing Device aus, um eine sichere Positionsinformation höherer Güte aus den Eingangssignalen zu bestimmen. Wenn z.B. vom HMI/RMI ein Not-Aus-Signal ausgegeben wird, so schaltet die Perception Safety ECU das Ausgangssignal in jedem Fall auf "Not-Aus", so dass die Motion Control ECU das Fahrzeug in jedem Fall über mindestens zwei Steuersignale redundant in einem sicheren Zustand steuert.

Wird z.B. ein Objekt im Umfeld des Fahrzeugs mittels einer oder mehrerer Radarsignale erkannt und diese Information durch das Ground Truth Sensing Device mit Hilfe einer "Time of Flight-Kamera" bestätigt, so führt dies zu einem zuverlässigen Ausgangssignal der Perception Safety ECU über die Relativposition des potenziellen Objektes. Das Ausgangssignal der Perception Safety ECU beinhaltet hierbei bereits eine vorverarbeitete, sichere Objekterkennung der verschiedenen Sensorsysteme.

Die Motion Control ECU berechnet aus dem Kollisionsmeldesignal der Perception Safety ECU und ggf. aus den Abschaltsignalen der HMI/RMI und des Ground Truth Sensing Device ein Notfahrsignal, das zwei redundante Signale ansteuert, mit denen mindestens ein Aktuator über mindestens zwei Steuersignale redundant zum Stoppen oder Ausweichen angesteuert wird. Es kann sich hierbei um ein Brems- oder Lenksystem handeln, wobei auch gleichzeitig eine kombinierte Brems- und Lenkbewegung mit Ausweichen erzielt werden kann.

Gemäß einem weiteren Merkmal der Erfindung ist die Motion Control ECU ferner jeweils über eine sichere Verbindung mit dem HMI/RMI und mit dem Ground Truth Sensing Device gekoppelt.

Auf diese Weise kann die Motion Control ECU zusätzlich zum Kollisionsmeldesignal der Perception Safety ECU auch unmittelbar die sicheren Ausgangssignale der HMI/RMI und des Ground Truth Sensing Device verarbeiten, um die Sicherheit zur Erkennung eines Notzustandes weiter zu erhöhen. Beispielsweise wird auf diese Weise ein Not-Aus-Signal vom HMI/RMI unmittelbar zur Motion Control ECU übertragen, so dass die Motion Control ECU die Überführung des Fahrzeugs in einen sicheren Zustand unmittelbar einleiten kann.

Gemäß einer weiteren Ausgestaltung der Erfindung weist die HMI/RMI zumindest einen am Fahrzeug vorgesehenen Not-Aus-Schalter auf, sowie zumindest eine ferngesteuerte Not-Aus-Schalteinrichtung.

Auf diese Weise kann eine Not-Aus-Abschaltung sowohl menschengesteuert durch Betätigung eines Not-Aus-Schalters am Fahrzeug als auch ferngesteuert gewährleistet werden.

Gemäß einer weiteren Ausgestaltung der Erfindung ist die High Performance ECU dazu ausgebildet, aus den Signalen der Sensoren eines oder mehrerer Objekte in der Umgebung des Fahrzeugs zu erkennen, zu klassifizieren, Positionen und Bewegungsinformationen der Objekte zu bestimmen und an die Motion Control ECU als unsicheres Object Recognition Indicator Signal zu übertragen, wobei die Motion Control ECU ferner dazu ausgebildet ist, das Object Recognition Indicator Signal auszuwerten und mit dem sicheren Signal der Perception Safety ECU, und ggf. der HMI/RMI und des Ground Truth Sensing Device abzugleichen, um das Fahrzeug für den Fall, dass kein Notzustand erkannt wird, über die mindestens zwei Steuersignale gemäß einer vorgegebenen Fahraufgabe zu steuern.

Auf diese Weise wird die High Performance ECU genutzt, um aus den Sensorsignalen ein detaillierteres Bild der Umgebung des Fahrzeugs zu bestimmen und um Objekte zu erkennen oder diese einer Klasse zuzuordnen. Dies kann beispielsweise erreicht werden durch Zuhilfenahme von Algorithmen der künstlichen Intelligenz (Deep Learning), wie z.B. Segmentic Segmentation. Die Berechnungen der High Performance ECU, die

sehr komplex sein können und ein vielschichtiges Bild der unmittelbaren Fahrzeugumgebung liefern können, werden somit von der Motion Control ECU mit dem sicheren Kollisionsmeldesignal der Perception Safety ECU abgeglichen, um für den Fall, dass kein Notzustand erkannt wird, eine Steuerung des Fahrzeugs gemäß einer vorgegebenen Fahrzeugaufgabe nach den Vorgaben der High Performance ECU zu bewirken.

Gemäß einer weiteren Ausgestaltung der Erfindung weist die High Performance ECU eine Schnittstelle zur Ausgabe eines Ausgangssignals auf, insbesondere an ein Human Machine Interface, etwa in Form eines Displays.

Auf diese Weise können die berechneten Signale der High Performance ECU mit hohem Informationsgehalt nicht nur zur Fahrzeugbewegungssteuerung, sondern auch für andere Aufgaben genutzt werden, etwa um einen Benutzer über die Umgebung unmittelbar zu informieren.

Gemäß einer weiteren Ausgestaltung der Erfindung handelt es sich bei dem Sensorset um ein Surround Sensing Sensorset, mit mehreren Sensoren, vorzugsweise mit unterschiedlichem Messprinzip, insbesondere mit mindestens einem Radarsensor, mit mindestens einem Kamerasensor, mit mindestens einem Lidarsensor, und vorzugsweise einem oder mehreren anderen Sensoren, insbesondere einem Ultraschallsensor und/oder einem Infrarotsensor.

Auf diese Weise können umfangreiche Sensordaten genutzt werden, um eine möglichst präzise Erfassung der Fahrzeugumgebung auch mit mehreren Messprinzipien zu gewährleisten, so dass eine besonders hochwertige und sichere Abtastung der Fahrzeugumgebung ermöglicht wird.

Gemäß einer weiteren Ausgestaltung der Erfindung weist das Ground Truth Sensing Device eine Time of Flight-Kamera und/oder ein Lidarsystem, insbesondere zur Fußgängererkennung, und/oder einen Bumper auf, der bei Kontakt mit einem Gegenstand ein Signal auslöst.

Time of Flight-Kameras sind 3D-Kamerasysteme, die mit dem Laufzeitverfahren Distanzen messen. Sie werden nach dem verwendeten PMD-Sensor auch PMD-Kameras genannt und können im Entfernungsbereich von einigen Dezimetern bis ca. 40 m eingesetzt werden.

Lidarverfahren sind dem Radar verwandte Verfahren zur optischen Abstands- und Geschwindigkeitsmessung, wobei statt Radarstrahlen Laserstrahlen verwendet werden. Lidar-Systeme sind im Bereich von fahrerlosen Fahrzeugen zur Hinderniserkennung bekannt und auch teilweise genormt, um Unfälle mit Personen, die die automatischen Fahrwege kreuzen könnten, zu vermeiden.

Ein Bumper (Stoßfänger), der bei Kontakt mit einem Gegenstand ein Signal auslöst, ermöglicht eine unmittelbare Kollisionserkennung.

Gemäß einer weiteren Ausgestaltung der Erfindung wird das Signal des Ground Truth Sensing Device und/oder der Perception Safety ECU und/oder der HMI/RMI und/oder der Motion Control ECU drahtgebunden redundant oder mittels eines Bussystems abgesichert (insbesondere mit Alife Count oder Cyclic Redundancy Check) übertragen.

Eine sichere Signalübertragung ist einerseits drahtgebunden redundant ermöglicht, andererseits auch mittels eines Bussystems, das entsprechend abgesichert ist. Dies ermöglicht eine einfache und flexible Verbindung.

Gemäß einer weiteren Ausgestaltung der Erfindung ist die Perception Safety ECU als Steuergerät ausgebildet, das mit Software gesteuert ist, welche regelbasiert, ohne eine Verwendung von KI-Algorithmen, die Eingangssignale auswertet, um daraus ein sicheres Signal höherer Güte mit einer sicheren Positionsinformation zu bestimmen.

Um eine sichere Verarbeitung zu gewährleisten, erfolgt die Softwaresteuerung regelbasiert, ohne dass KI-Algorithmen verwendet werden. Es wird ein sicheres Kollisionsmeldungssignal ausgegeben, dessen Information aus Eingangssignalen berechnet wird, die ihrerseits alle sicher sind.

Gemäß einer weiteren Ausgestaltung der Erfindung weist das System eine Human Control Branch, eine Level 2 Driver Assistance Perception Branch und eine Level 4 Autonomous Driving Perception Branch auf,

- wobei die Human Control Branch die HMI/RMI aufweist, die zumindest mit der Perception Safety ECU über eine sichere Verbindung gekoppelt ist;

- wobei die Level 2 Driver Assistance Perception Branch die Perception Safety ECU aufweist, sowie mindestens einen Radarsensor und mindestens eine Kamera, wobei die Signale des Radarsensors und die Signale der Kamera über eine sichere Verbindung einer sicheren Fusionseinheit zugeführt sind, die ein sicheres fusioniertes Signal ausgibt;

- wobei die Signale der HMI/RMI, die Signale der Fusionseinheit der Perception Safety ECU und der Motion Control ECU über sichere Verbindungen zugeführt sind, um daraus in der Perception Safety ECU ein sicheres Kollisionsmeldungssignal abzuleiten, welches der Motion Control ECU über eine sichere Verbindung zugeführt ist;

- wobei die Level 4 Autonomous Driving Perception Branch die High Performance ECU aufweist, die mit dem Sensorset gekoppelt ist und dazu ausgebildet ist, aus den Signalen der Sensoren ein Object Recognition Indicator Signal abzuleiten, das der Motion Control ECU zugeführt ist;

- und wobei die Level 2 Driver Assistance Perception Branch dazu ausgebildet ist, das Fahrzeug über die Motion Control ECU im Falle der Erkennung eines Notzustands oder eines Ausfalls der Level 4 Autonomous Driving Perception Branch mittels des sicheren, fusionierten Signals in einen sicheren Zustand zu steuern.

In diesem Fall dient die Level 4 Autonomous Driving Perception Branch mit der High Performance ECU als neuer Systemanteil zum autonomen Fahren. Als Rückfallebene für diesen Zweig wird die heute z.B. in Lkws standardmäßig eingesetzte Level 2 Driving Assistance Perception Branch verwendet. Diese besteht typischerweise aus einem

nach vorne gerichteten Radarsensor, dessen Signale mit den Daten einer Kamera fusioniert werden. Diese Signale werden bereits heute mit sehr hoher Qualität sicher berechnet und mit einem Signal bereitgestellt, das ein Umgebungsbild liefert, so dass die Motion Control ECU das Fahrzeug im Falle der Erkennung eines Notzustandes noch in einen sicheren Zustand überführen kann.

Vorteilhaft bei dieser Ausgestaltung ist der modulare Ansatz: Ein bestehendes und lauffähiges Level 2 System kann um ein "Level 4 System Upgrade" erweitert werden. Als Rückfallebene im Fehlerfall ist das Level 2 System kurzzeitig imstande, ein Umgebungsbild mittels des fusionierten Radar/Kamerasignals bereitzustellen, so dass die Motion Control ECU das Fahrzeug in einen sicheren Zustand überführen kann.

Es versteht sich, dass die vorstehend genannten und die nachstehend noch zu erläuternden Merkmale der Erfindung nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind, ohne den Rahmen der Erfindung zu verlassen.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung bevorzugter Ausführungsbeispiele unter Bezugnahme auf die Zeichnung. Es zeigen:

Fig. 1 ein Blockschaltbild einer ersten Ausführung eines erfindungsgemäßen Systems zum sicheren Betreiben eines automatisierten Fahrzeugs;

Fig. 2 ein Blockschaltbild eines weiteren erfindungsgemäßen Systems mit einer Level 2 Driving Assistance Perception Branch und einer Level 4 Autonomous Driving Perception Branch und

Fig. 3 eine vereinfachte Darstellung eines erfindungsgemäßen Fahrzeugs mit einem in der Nähe zu detektierenden Objekt.

In Fig. 1 ist eine erste Ausführung eines erfindungsgemäßen Systems 1 zum Betreiben eines automatisierten Fahrzeugs dargestellt.

Das System 1 weist ein erstes Netzwerk auf, das eine High Performance ECU 30 aufweist, die mit einem Sensorset 20 und einer Motion Control ECU 50 gekoppelt ist. Die Verbindungen innerhalb dieses Netzwerks erfolgen über Wege, die nur mit Qualitätsmaßnahmen gesichert sind, bei denen es sich jedoch nicht um "sichere" oder "fehlersichere" Verbindungen handelt, wie sie für sicherheitskritische Aufgaben erforderlich sind. Derartige "unsichere" Verbindungen oder Wege werden im Folgenden sowie in den Figuren als "QM Path" oder "QM-Weg" bezeichnet und in den Figuren durch durchgezogene Verbindungen gekennzeichnet. Dagegen werden "sichere" bzw. "fehlersichere" Verbindungen, welche für sicherheitskritische Aufgaben erforderlich sind, in der Anmeldung und in den Figuren allgemein als "Safe Path" oder "sichere Verbindung" bezeichnet und in den Figuren durch strichpunktierte Linien gekennzeichnet.

Das "unsichere" erste Netzwerk, welches die High Performance ECU 30, das zugehörige Sensorset 20 und die Motion Control ECU 50 enthält, ist zusätzlich noch um ein zweites, hierarchisches, redundantes E/E-Netzwerk mit sicheren Komponenten und sicheren Verbindungen ergänzt. Durch das zweite, redundante Netzwerk wird unabhängig vom ersten Netzwerk mit QM-Wegen eine gefahrlose Überführung des Fahrzeugs in einen sicheren Zustand gewährleistet, selbst also, wenn das erste Netzwerk ausfallen oder mit Fehlerzuständen behaftet sein sollte.

Die sicheren Verbindungen im zweiten, hierarchischen, redundanten Netzwerk sind entweder mittels elektrischer Leitungen redundant ausgeführt oder über ein Bussystem abgesichert ausgeführt, das etwa mittels Alive Count oder Cyclic Redundancy Check sicher ausgestaltet ist.

Ein Fahrzeug 70, das mit einem derartigen System 1 betrieben werden kann, ist beispielhaft in Fig. 3 dargestellt. Es handelt sich hierbei um ein automatisiertes Fahrzeug, das mit zwei angetriebenen Rädern 90, 92 und mit zwei gelenkten Rädern 94, 96 versehen ist. Das Fahrzeug 70 wird mittels des Systems 1 betrieben. Das Fahrzeug 70 kann beispielsweise als landwirtschaftliches Nutzfahrzeug ausgebildet sein.

Das Sensorset 20 gemäß Fig. 1 bzw. Fig. 3 ist als Surround Sensing Sensorset ausgeführt, mit mehreren Sensoren mit unterschiedlichem Messprinzip. Hierzu sind beispielhaft in Fig. 3 zwei Kamerasensoren 76, 77 dargestellt, ein Lidarsensor 82, zwei Radarsensoren 80, 81 und zwei andere Sensoren 78, 79, wobei es sich insbesondere um Ultraschallsensoren und/oder Infrarotsensoren handeln kann.

In Fig. 1 sind die Signale der Sensoren bezeichnet. Hierbei handelt es sich um ein Radarsignal 22, ein Kamerasignal 23, ein Lidarsignal 24 und Signale 25 von anderen Sensoren. Diese Signale 22-25 sind der High Performance ECU 30 zugeführt. Die High Performance ECU 30 berechnet aus den Signalen 22, 23, 24, 25 ein Bild der Umgebung des Fahrzeugs 70 und kann Objekte (vgl. 72 gemäß Fig. 3) zum einen erkennen, sie zum anderen aber auch einer Klasse zuordnen. Dies kann erreicht werden durch Zuhilfenahme von Algorithmen der künstlichen Intelligenz KI (Deep Learning), wie z.B. Segmentic Segmentation. Die High Performance ECU 30 enthält in der Regel noch Hilfsrechner, wie beispielsweise graphische Prozessoren usw. Die High Performance ECU 30 kann infolge des hohen Datenumfangs der Eingangssignale und der Rechenkapazität sehr komplexe Berechnungen durchführen, die zur Auswertung der Umgebung des Fahrzeugs 70 dienen, mit Hilfe derer Objekte 72 erkannt und klassifiziert werden können. Das Ausgangssignal der High Performance ECU 30 wird der Motion Control ECU 50 als unsicheres Object Recognition Indicator Signal 31 zugeführt.

Die Ausgangssignale der High Performance ECU 30 können nicht nur zur Fahrzeugbewegungssteuerung über die Motion Control ECU 50 verwendet werden, sondern können auch anderen Empfängern zur Verfügung gestellt werden, wie beispielsweise in Fig. 1 anhand des Pfades 32 dargestellt ist. Es könnte sich hierbei etwa um ein Human Machine Interface 84, etwa in Form eines Displays, handeln, wie beispielhaft in Fig. 3 dargestellt ist.

Die Motion Control ECU 50 setzt das Object Recognition Indicator Signal der High Performance ECU 30 um und berechnet hieraus redundante Steuersignale 51, 52, die zugeordneten Aktoren redundant zugeführt werden, um so das Fahrzeug 70 gemäß einer vorgegebenen Fahraufgabe zu steuern, wie beispielhaft bei 60 gezeigt ist.

Erfindungsgemäß ist das erste Netzwerk, zu dem die High Performance ECU 30, das Sensorset 20, die Motion Control ECU 50 und die zugehörigen Steuersignale 51, 52, mit dem das System 60 kontrolliert wird, gehören, noch um das hierarchische, mehrfach redundante E/E-Netzwerk ergänzt, das in Fig. 1 über sichere Verbindungen (Safe Path) gemäß dem strichpunktierten Weg angekoppelt ist (die Motion Control ECU 50 mit den zugehörigen Steuersignalen 51, 52 ist hierbei beiden Netzwerken zuzuordnen).

Hierzu ist eine HMI/RMI (Human/Remote Machine Interface) 5 vorgesehen. Hierbei handelt es sich um mindestens einen Not-Aus-Schalter (vgl. Fig. 3, Ziffer 87) der unmittelbar am Fahrzeug 70 aufgenommen ist und von einem Benutzer betätigt werden kann. Zusätzlich weist die HMI/RMI 5 einen ferngesteuerten Remote-Aus-Schalter 88 auf. Dieser kann von einem menschlichen Anwender oder von einem übergeordneten System ferngesteuert über eine sichere Verbindung übertragen werden. Es versteht sich, dass sowohl der Not-Aus-Schalter 87 als auch der ferngesteuerte Remote-Aus-Schalter 88 mit der HMI/RMI über sichere Verbindungen gekoppelt sind. Das HMI/RMI 5 gibt ein externes Steuersignal 6 aus, das der Motion Control ECU 50 über eine sichere Verbindung, z.B. über eine redundante Kabelverbindung etwa unter Nutzung eines Digitaleingangs der Motion Control ECU 50 zugeführt ist. Ferner ist das externe Steuersignal 6 der HMI/RMI 5 einer Perception Safety ECU 40 gleichfalls über eine sichere Verbindung zugeführt.

Das redundante sichere Netzwerk enthält ferner ein Ground Truth Sensing Device 10, das ein Ground Truth Sensing Indicator Signal 11 ausgibt, das der Motion Control ECU 50 und der Perception Safety ECU 40 jeweils über eine sichere Verbindung zugeführt ist.

Bei dem Ground Truth Sensing Device 10 handelt es sich um ein Messgerät, mit dem sich unter normalen Bedingungen die Position eines Objektes 72 relativ zum Fahrzeug 70 sicher bestimmen lässt. Es kann sich hierbei etwa um eine Time of Flight-Kamera (TOF-Kamera) handeln. Eine TOF-Kamera ist ein 3D-Kamerasystem, das mit dem Laufzeitverfahren (Time of Flight, TOF) Distanzen messen kann.

Alternativ oder zusätzlich kann das Ground Truth Sensing Device 10 ein Lidarsystem aufweisen. Lidarsysteme sind teilweise schon zertifiziert erhältlich, z.B. für eine Fußgängererkennung. Zusätzlich kann das Ground Truth Sensing Device etwa einen Bumper (Stoßfänger) aufweisen, der bei Kontakt mit einem Gegenstand ein Signal auslöst.

Das Ground Truth Sensing Device 10 liefert als Ausgangssignal 11 ein Ground Truth Indicator Signal 11, mit dem die Position eines Objektes 72 relativ zum Fahrzeug 70 sicher bestimmt werden kann. Das Signal 11 wird entweder drahtgebunden redundant oder über ein abgesichertes Bussystem zur Motion Control ECU 50 und zur Perception Safety ECU 40 übertragen.

Der Perception Safety ECU 40 sind neben dem externen Steuersignal 6 der HMI/RMI 5 und neben dem Ground Truth Indicator Signal 11 des Ground Truth Sensing Device 10 ferner noch das Signal 21 mindestens eines Radarsensors zugeführt, das redundant oder abgesichert übertragen wird. Der mindestens eine Radarsensor oder die mehreren Radarsensoren, die Teil des Sensorsets 20 sein können, können durch Software-Programme im Sensorsteuergerät bereits vorverarbeitet sein und fertige "Radarobjekte" enthalten. Sie können jedoch auch Rohdaten enthalten, die erst in der Perception Safety ECU 40 verarbeitet werden. Während das Signal des mindestens einen Radarsensors 21 an die Perception Safety ECU 40 sicher übertragen wird, müssen die Signale der Radarsensoren des Sensorsets 20, die der High Performance ECU 30 zugeführt werden, nicht sicher bzw. redundant übertragen werden. Bei diesen Radarsignalen 22 kann es sich um Obermengen, Teilmengen oder disjunkte Mengen der Radarsignale 21 handeln, die der Perception Safety ECU 40 zugeführt sind.

Bei der Perception Safety ECU handelt es sich um ein Steuergerät, das mittels eines Software-Programms regelbasiert ohne die Zuhilfenahme von KI-Algorithmen die von der HMI/RMI 5, dem Ground Truth Sensing Device 10 und dem mindestens einen Radarsensor übertragenen Signale zusammenführt und daraus ein sicheres Kollisionsmeldungssignal 41 berechnet, das an die Motion Control ECU 50 sicher übertragen wird. Die Perception Safety ECU 40 ist dazu vorgesehen, aus den sicheren Eingangssignalen 6, 11, 21 eine sichere Positionsinformation höherer Güte zu bestimmen:

Wenn z.B. mehrere Radarsignale 21 ein Objekt 72 in der Umgebung erkennen und das Ground Truth Sensing Device etwa mittels der TOF-Kamera oder mittels eines Lidars diese Information bestätigt, so enthält das Kollisionsmeldungssignal 41 ein zuverlässiges Signal über die Position des potenziellen Objektes 72.

Wenn in einem anderen Beispiel ein anderes Ground Truth Indicator Signal 11, wie z.B. das Ansprechen eines Schließschalters in einem "Bumper" sowie eine Abstandsinformation aus einem Radarsignal 21 gleichzeitig ein sehr nahes Objekt messen, so wird dadurch die Information bestätigt und ist damit zuverlässiger. Damit kann ausgeschlossen werden, dass etwa der Bumper-Schließkontakt z.B. durch eine Vibration versehentlich kurzzeitig geschlossen hat.

Wenn etwa in einem dritten Beispiel ein Not-Aus-Signal 6 über das HMI/RMI 5 ferngesteuert erzeugt wird, so schaltet die Perception Safety ECU auf jeden Fall das Kollisionsmeldungssignal 41 auf "Not-Aus", welches von der Motion Control ECU 50 in ein entsprechendes Notfahrsignal umgesetzt wird.

Die Motion Control ECU 50 wertet die sicheren "Abschaltsignalindikatoren" 6, 11, 41 aus, die vom HMI/RMI 5, vom Ground Truth Sensing Device 10 und von der Perception Safety ECU 40 sicher übertragen werden. Dabei beinhaltet das sichere Kollisionsmeldungssignal 41 von der Perception Safety ECU eine bereits vorverarbeitete, sichere Objekterkennung verschiedener Sensorsysteme. Aus den Abschaltsignalen 6, 11, 41 wird im Falle der Erkennung einer Notsituation ein Notfahrsignal berechnet, das zwei redundante Signale 51, 52 ansteuert, mit denen zugeordnete Aktuatoren redundant zum Stoppen und/oder Ausweichen des Fahrzeugs 70 angesteuert werden.

In Fig. 3 sind zugeordnete Antriebsräder 90, 92 und zugeordnete gelenkte Räder 94, 96 beispielhaft dargestellt, welche über redundante, drahtgebundene Verbindungen von der Motion Control ECU 50 angesteuert werden, um im Falle eines Notfahrsignals einen Stopp- und/oder Ausweichvorgang einzuleiten. Je nach Fahrsituation und Notfahrsignal kann also etwa ein Bremssystem redundant angesteuert werden oder ein Lenksystem redundant zum Ausweichen angesteuert werden. Es können auch gleichzeitig hierbei

ein Brems- und ein Lenksystem redundant angesteuert werden, so dass eine Bremsung kombiniert mit Ausweichen erzielt wird.

Darüber hinaus wertet die Motion Control ECU 50 das unsichere Object Recognition Indicator Signal 31 der High Performance ECU 30 mit hohem Informationsgehalt aus und steuert die zumindest zwei redundanten Ausgangssignale 51, 52 derart, dass das Fahrzeug 70 für den Fall, dass kein Notzustand erkannt wird, gemäß einer vorgegebenen Fahraufgabe nach den Vorgaben der High Performance ECU 30 gesteuert wird.

Eine komplexe, vorgegebene Fahraufgabe ohne Notzustand könnte z.B. das Folgen eines Schwads auf einer Wiese sein. Die Erkennung eines Schwads erfolgt dann z.B. mittels zweier Kameras, deren Signale 23 mittels eines Deep Learning Algorithmus in der High Performance ECU 30 verarbeitet werden. Die High Performance ECU 30 berechnet daraus eine komplexe Umgebungsinformation und sendet diese im Signal 31 an die Motion Control ECU 50. Diese steuert die Lenkung über eines der Signale 51 und/oder 52 so an, dass das Fahrzeug 70 dem erkannten Schwad folgt.

In Fig. 3 ist das zuvor anhand von Fig. 1 beschriebene System 1 beispielhaft auf einem automatisierten Fahrzeug 70 vereinfacht dargestellt, das sich entlang eines Weges 74 bewegt. Hierbei ist zusätzlich ein Display 84 dargestellt, das von der High Performance ECU 30 über einen zugeordneten Ausgang 32 angesteuert wird, um einem etwaigen Benutzer des Fahrzeugs diverse Steuerinformationen und ggf. ein berechnetes Bild der Fahrzeugumgebung anzuzeigen. Beispielhaft ist hierbei ein sicheres Bussystem 98 dargestellt, das eine abgesicherte Übertragung etwa mittels Alive Count oder Cyclic Redundancy Check ermöglicht. Das HMI/RMI 5, die Performance Safety ECU 40, das Ground Truth Sensing Device 10, die High Performance ECU 30 und die Motion Control ECU 50 können über dieses sichere Bussystem 98 gekoppelt sein. Alternativ kann natürlich auch jeweils eine redundante drahtgebundene Verbindung vorgesehen sein.

Anhand von Fig. 2 wird im Folgenden eine bevorzugte Abwandlung des Systems erläutert, die insgesamt mit der Ziffer 1a bezeichnet ist. Hierbei werden für entsprechende Teile entsprechende Bezugsziffern verwendet.

Das System 1a weist eine Level 4 Autonomous Driving Perception Branch 80 auf, welche das Sensorset 20 und die High Performance ECU 30 umfasst. Als Rückfallebene für diesen Zweig ist eine Level 2 Driving Assistance Perception Branch 75 vorgesehen.

Derartige L2-Systeme werden bereits heute z.B. in Lkws standardmäßig eingesetzt. Eine solche Level 2 Driving Assistance Perception Branch 75 weist typischerweise einen nach vorne gerichteten Radarsensor auf, sowie mindestens eine Kamera. Die Ausgangssignale 21b des Radarsensors und der Kamera werden in einer Fusionseinheit 10b fusioniert. Hieraus wird mit sehr hoher Qualität ein L2 Obstacle Indicator Signal 11b berechnet und bereitgestellt. Wiederum sind die sicheren Signale 6 von der HMI/RMI 5, das L2 Obstacle Indicator Signal 11b von der Fusionseinheit 10b und das sichere Kollisionsmeldungssignal 41 von der Perception Safety ECU 40 der Motion Control ECU 50 über sichere Verbindungen zugeführt.

Vorteilhaft bei diesem System ist der modulare Ansatz: Ein bestehendes und lauffähiges L2-System kann um ein "L4-Upgrade" erweitert werden. Als Rückfallebene im Fehlerfall ist das L2-System kurzzeitig imstande, mittels der Fusionseinheit 10b ein L2 Obstacle Indicator Signal mit einem Umgebungsbild bereitzustellen, so dass die Motion Control ECU 50 das Fahrzeug 70 in einen sicheren Zustand überführen kann.

Bezugszeichen

1	System
5	HMI/RMI
6	externes Steuersignal
10	Ground Truth Sensing Device
10b	Fusionseinheit
11	Ground Truth Sensing Indicator Signal
11b	L2 Obstacle Indicator Signal
20	Sensorset
21	Radarsignal abgesichert
21b	Radarsignal abgesichert
22	Radarsignal nicht gesichert
23	Kamerasignal
24	Lidarsignal
25	Signal anderen Sensors
30	High Performance ECU
31	Object Recognition Indicator Signal
32	Ausgangssignal Human Machine Interface
40	Perception Safety ECU
41	Kollisionsmeldungssignal
50	Motion Control ECU
51	redundantes Steuersignal
52	redundantes Steuersignal
60	gesteuertes System
70	Fahrzeug
72	Objekt
74	Bewegungsweg
76	Kamera
77	Kamera
78	anderer Sensor
79	anderer Sensor
80	Radarsensor

81 Radarsensor
82 Lidarsensor
84 Display
87 Not-Aus-Schalter
88 Remote Not-Aus-Schalter
90 Antriebsrad/Bremse
92 Antriebsrad/Bremse
94 gelenktes Rad
96 gelenktes Rad
98 sicheres Bussystem

Patentansprüche

1. System zum sicheren Betreiben eines automatisierten Fahrzeugs (70), mit:
   (a) einem ersten Netzwerk, mit
      - einem Sensorset (20) mit einer Mehrzahl von Sensoren (76, 77, 78, 79, 80, 81, 82) zur Erfassung der Umgebung des Fahrzeugs (70), der mit einer High Performance ECU (30) gekoppelt ist, welche die Signale (22, 23, 24, 25) der Sensoren (76-82) zur Orientierung, Steuerung und Kollisionsvermeidung verarbeitet; und
      - einer sicheren Bewegungssteuerung Motion Control ECU (50), die mit mindestens einem Antriebselement (90, 92, 94, 96) über mindestens zwei Steuersignale (51, 52) redundant zur Steuerung des Fahrzeugs (70) gekoppelt ist;
      - wobei die High Performance ECU (30) ein Object Recognition Indicator Signal (31) zur Orientierung, Steuerung und Kollisionsvermeidung an die Motion Control ECU (50) ausgibt;
   (b) einem zweiten, hierarchischen, redundantem Netzwerk zum sicheren Betreiben des Fahrzeugs (70), mit:
      - einem HMI/RMI (Human/Remote Machine Interface) (5) mit zumindest einer Not-Aus-Schalteinrichtung (87, 88);
      - einem Ground Truth Sensing Device (10) zur Positionsbestimmung von Objekten relativ zum Fahrzeug (70);
      - einer Perception Safety ECU (40), in Form eines Steuergerätes, das über sichere Verbindungen mit dem HMI/RMI (5), dem Ground Truth Sensing Device (10), und mindestens einem Radarsensor (80, 81) gekoppelt ist, um aus den übertragenen Signalen ein sicheres Kollisionsmeldesignal (41) abzuleiten, das der Motion Control ECU (50) über eine sichere Verbindung zugeführt ist; und
      - wobei die Motion Control ECU (50) dazu ausgebildet ist, die Signale der HMI/RMI (5), des Ground Truth Sensing Device (10) und der Perception Safety ECU (40) zur Erkennung eines Notzu-

stands sicher auszuwerten, um das Fahrzeug (70) im Falle der Erkennung eines Notzustands über mindestens zwei Steuersignale (51, 52) redundant in einen sicheren Zustand zu steuern.

2. System nach Anspruch 1, bei dem die Motion Control ECU (50) ferner jeweils über eine sichere Verbindung mit dem HMI/RMI (5) und mit dem Ground Truth Sensing Device (10) gekoppelt ist.

3. System nach Anspruch 1 oder 2, bei dem die HMI/RMI (5) zumindest einen am Fahrzeug (70) vorgesehenen Not-Aus-Schalter (87) und zumindest eine ferngesteuerte Not-Aus-Schalteinrichtung (88) aufweist.

4. System nach Anspruch 1, 2 oder 3, bei dem die High Performance ECU (30) dazu ausgebildet ist, aus den Signalen (22, 23, 24, 25) der Sensoren (76-82) eines oder mehrere Objekte (72) in der Umgebung des Fahrzeugs (70) zu erkennen, zu klassifizieren, Positionen und Bewegungsinformationen der Objekte (72) zu bestimmen und an die Motion Control ECU (50) als unsicheres Object Recognition Indicator Signal (31) zu übertragen, und wobei die Motion Control ECU (50) dazu ausgebildet ist, das Object Recognition Indicator Signal (31) auszuwerten und mit den sicheren Signalen der HMI/RMI (5), des Ground Truth Sensing Device (10) und der Perception Safety ECU abzugleichen, um das Fahrzeug (70) für den Fall, dass kein Notzustand erkannt wird, gemäß einer vorgegebenen Fahraufgabe zu steuern.

5. System nach Anspruch 4, bei dem die High Performance ECU (30) eine Schnittstelle (32) zur Ausgabe eines Ausgangssignals, insbesondere an ein Human Machine Interface, etwa in Form eines Displays (84), aufweist.

6. System nach einem der Ansprüche 1 bis 5, bei dem das Sensorset (20) ein Surround Sensing Sensorset ist, mit mehreren Sensoren (76-82) vorzugsweise mit unterschiedlichem Messprinzip, insbesondere mit mindestens einem Radarsensor (80, 81), mindestens einem Kamerasensor (76,77), mindestens einem Lidarsensor (82), und vorzugsweise einem oder mehreren anderen

Sensoren (78,79), insbesondere einem Ultraschallsensor und/oder einem Infrarotsensor.

7. System nach einem der vorhergehenden Ansprüche, bei dem das Ground Truth Sensing Device (10) eine Time of Flight Kamera, und/oder ein Lidarsystem, insbesondere zur Fußgängererkennung, und/oder einen Bumper aufweist, der bei Kontakt mit einem Gegenstand ein Signal auslöst.

8. System nach einem der vorhergehenden Ansprüche, bei dem das Signal des Ground Truth Sensing Device (10), und/oder der Perception Safety ECU (40), und/oder der HMI/RMI (5), und/oder der Motion Control ECU (50) drahtgebunden redundant oder mittels eines Bussystems (98) abgesichert (insbesondere mit Alive Count oder Cyclic Redundancy Check) übertragen wird.

9. System nach einem der vorhergehenden Ansprüche, bei dem die Perception Safety ECU (40) als Steuergerät ausgebildet ist, das mit Software gesteuert ist, welche regelbasiert, ohne eine Verwendung von KI-Algorithmen, die Eingangssignale (6, 11, 21) auswertet, um daraus ein sicheres Signal (41) höherer Güte mit einer sicheren Positionsinformation zu bestimmen.

10. System nach einem der vorhergehenden Ansprüche, mit einer Human Control Branch (70), mit einer Level 2 Driver Assistance Perception Branch (75) und mit einer Level 4 Autonomous Driving Perception Branch (80),
    - wobei die Human Control Branch (70) die HMI/RMI (5) aufweist, die mit der Perception Safety ECU (40) und der Motion Control ECU (50) über eine sichere Verbindung gekoppelt ist;
    - wobei die Level 2 Driver Assistance Perception Branch (75) die Perception Safety ECU (40) aufweist, sowie mindestens einen Radarsensor (21b) und mindestens eine Kamera, wobei das Signal des Radarsensors (21b) und das Signal der Kamera über eine sichere Verbindung einer sicheren Fusionseinheit (10b) zugeführt sind, die ein sicheres fusioniertes Signal (11b) ausgibt, das der Perception Safety ECU (40) über eine sichere Verbindung zugeführt ist, um daraus in der Percepti-

on Safety ECU (40) ein sicheres Kollisionsmeldungssignal (41) abzuleiten, welches der Motion Control ECU (50) über eine sichere Verbindung zugeführt ist;

- wobei die Level 4 Autonomous Driving Perception Branch (80) die High Performance ECU (30) aufweist, die mit dem Sensorset (20) gekoppelt ist und dazu ausgebildet ist, aus den Signalen der Sensoren (22, 23, 24, 25) ein Object Recognition Indicator Signal (31) abzuleiten, das der Motion Control ECU (50) zugeführt ist;
- und wobei die Level 2 Driver Assistance Perception Branch (75) dazu ausgebildet ist, das Fahrzeug (70) über die Motion Control ECU (50) im Falle der Erkennung eines Notzustands oder eines Ausfalls der Level 4 Autonomous Driving Perception Branch (80) mittels des sicheren, fusionierten Signals (11b) in einen sicheren Zustand zu steuern.

11. System nach Anspruch 10, bei dem der Motion Control ECU (50) zusätzlich zum Signal (41) der Perception Safety ECU (40) auch das Signal (6) der HMI/RMI (5) und das Signal (11b) der Fusionseinheit (10b) über sichere Verbindungen zugeführt sind.

12. Verfahren zum sicheren Betreiben eines automatisierten Fahrzeugs, bei dem
    (a) in einem ersten Netzwerk
        - ein Sensorset (20) mit einer Mehrzahl von Sensoren (76-82) zur Erfassung der Umgebung des Fahrzeugs (70) mit einer High Performance ECU (30) gekoppelt wird und die Signale der Sensoren (76-82) zur Orientierung, Steuerung und Kollisionsvermeidung verarbeitet werden, um ein Object Recognition Indicator Signal (31) zur Orientierung, Steuerung und Kollisionsvermeidung zu erzeugen, das
        - an eine sichere Bewegungssteuerung Motion Control ECU (50) übertragen wird, die mindestens einen Aktuator (90, 92, 94, 96) zur Steuerung des Fahrzeugs (70) über mindestens zwei Steuersignale (51, 52) redundant sicher steuert;

(b) in einem zweiten, hierarchischen, redundantem Netzwerk zum sicheren Betreiben des Fahrzeugs

- ein HMI/RMI (Human/Remote Machine Interface) (5) mit mindestens einer Not-Aus-Schalteinrichtung (87, 88); und
- ein Ground Truth Sensing Device (10) zur Positionsbestimmung von Objekten relativ zum Fahrzeug;
- mit einer Perception Safety ECU (40) in Form eines Steuergerätes über sichere Verbindungen gekoppelt werden, und der Perception Safety ECU (40) ferner das Signal (21) mindestens eines Radarsensors (80, 81) zugeführt wird, um aus den übertragenen Signalen ein sicheres Kollisionsmeldesignal (41) abzuleiten, das der Motion Control ECU (50) über eine sichere Verbindung zugeführt wird;
- wobei die Motion Control ECU (50) ferner jeweils über eine sichere Verbindung mit dem HMI/RMI (5) und mit dem Ground Truth Sensing Device (10) gekoppelt wird; und
- wobei die Motion Control ECU (50) die Signale (6, 11, 41) der HMI/RMI (5), des Ground Truth Sensing Device (10) und der Perception Safety ECU (40) auswertet, um einen Notzustand sicher zu erkennen, in dem das Fahrzeug (70) über mindestens zwei Steuersignale (51, 52) redundant in einen sicheren Zustand gesteuert wird.

13. Verfahren nach Anspruch 12, bei dem die Motion Control ECU (50) ferner jeweils über eine sichere Verbindung mit dem HMI/RMI (5) und mit dem Ground Truth Sensing Device (10) gekoppelt wird.

14. Verfahren nach Anspruch 12 oder 13, bei dem die High Performance ECU (30) aus den Signalen (22, 23, 24, 25) der Sensoren (76-82) eines oder mehrere Objekte (72) in der Umgebung des Fahrzeugs erkennt, klassifiziert, Positionen und Bewegungsinformationen der Objekt(e) (72) bestimmt und als unsicheres Object Recognition Indicator Signal (31) an die Motion Control ECU (50) überträgt, und bei dem die Motion Control ECU (50) das Object Recogni-

tion Indicator Signal (31) auswertet und mit den sicheren Signalen der HMI/RMI (5), des Ground Truth Sensing Device (10) und der Perception Safety ECU abzugleicht, um einen Notzustand zu erkennen, und um das Fahrzeug (70) für den Fall, dass kein Notzustand erkannt wird, gemäß einer vorgegebenen Fahraufgabe zu steuern.

15. Motion Control ECU (50), welche mit mindestens einem Aktuator über mindestens zwei Steuersignale (51, 52) redundant zur Steuerung eines Fahrzeugs (70) gekoppelt ist, wobei die Motion Control ECU (50) dazu ausgebildet ist, Signale (6, 11, 41) einer HMI/RMI (5), eines Ground Truth Sensing Device (10) und einer Perception Safety ECU (40) zu empfangen und zur Erkennung eines Notzustands sicher auszuwerten, um das Fahrzeug (70) im Falle der Erkennung eines Notzustands über die mindestens zwei Steuersignale (51, 52) redundant in einen sicheren Zustand zu steuern.

16. Fahrzeug (70) mit zumindest einer Motion Control ECU (50) nach Anspruch 15 oder einem System nach einem der Ansprüche 1 bis 11.

17. Fahrzeug (70) nach Anspruch 16, wobei das Fahrzeug (70) als landwirtschaftliches Nutzfahrzeug ausgebildet ist.

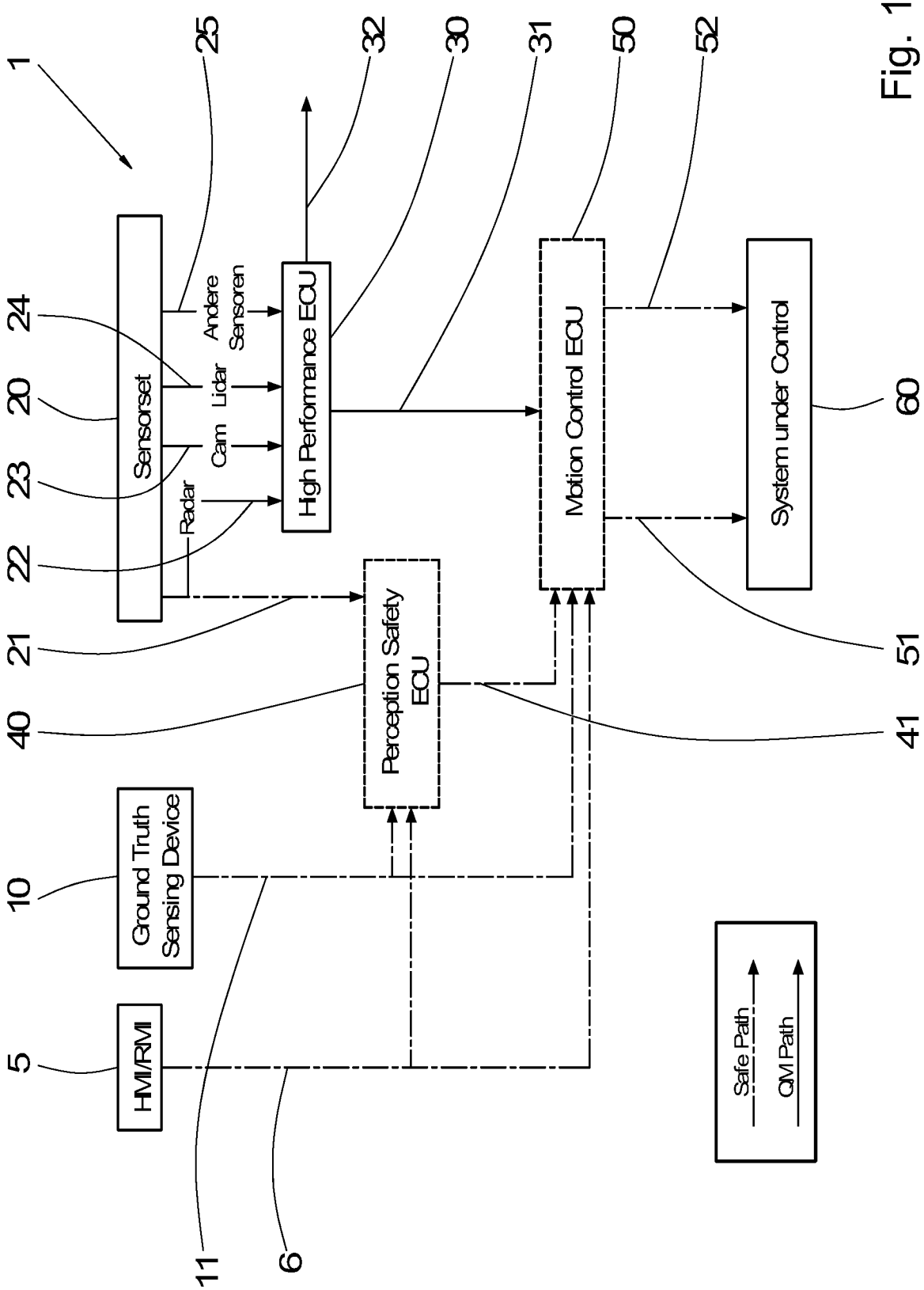
1
25
32
30
31
50
52
24
20
23
22
21
40
10
5
11
6
Sensorset
Andere Sensoren
Lidar
Cam
Radar
High Performance ECU
Motion Control ECU
System under Control
Perception Safety ECU
Ground Truth Sensing Device
HMI/RMI
60
51
41
Safe Path
QM Path

Fig. 1

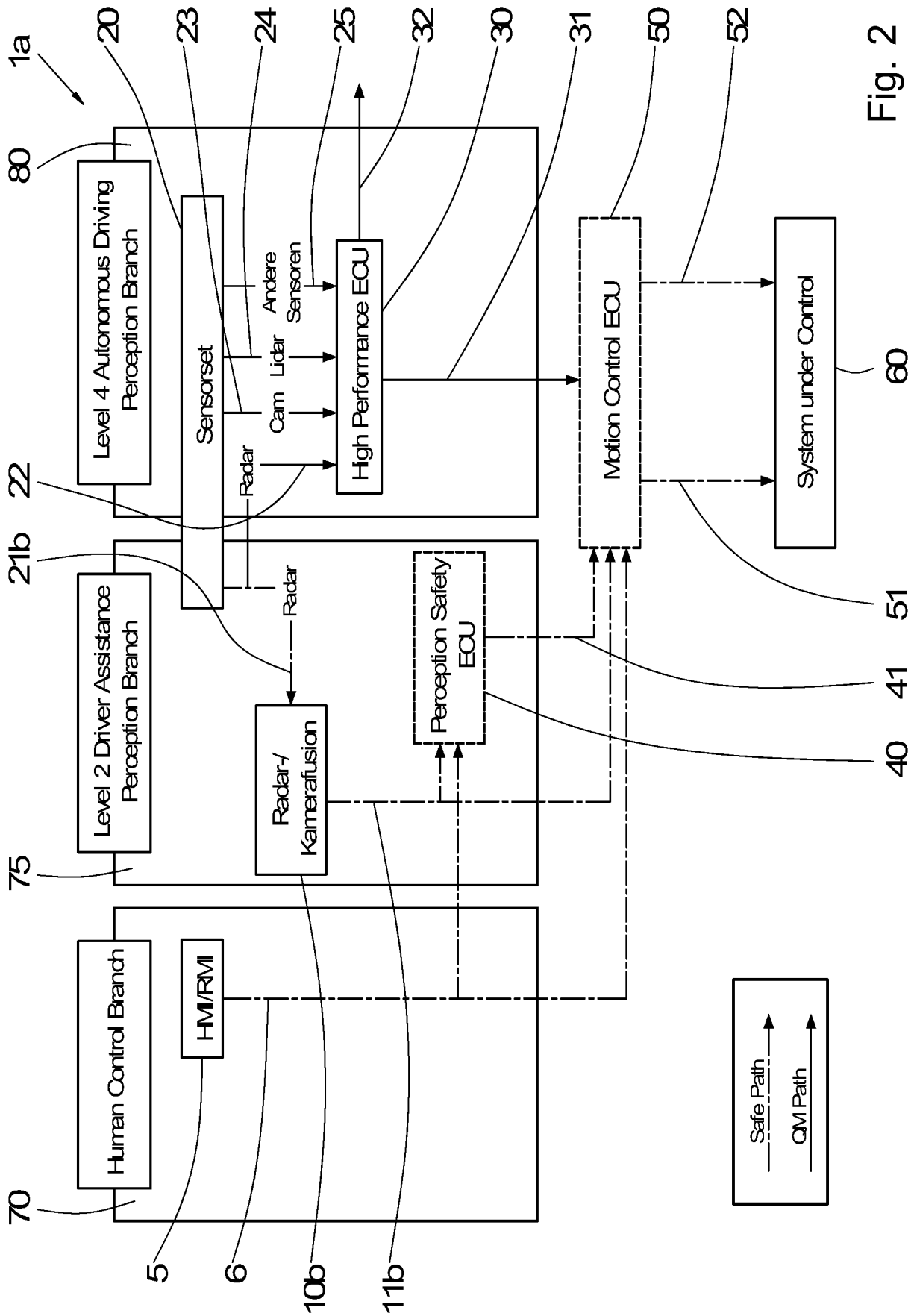
1a
20
23
24
25
32
30
31
50
52
80
Level 4 Autonomous Driving Perception Branch
Sensorset
Andere Sensoren
Lidar
Cam
Radar
High Performance ECU
Motion Control ECU
System under Control
60
22
21b
Level 2 Driver Assistance Perception Branch
Radar
Radar-/ Kamerafusion
Perception Safety ECU
51
41
40
75
Human Control Branch
HMI/RMI
70
5
6
10b
11b
Safe Path
QM Path

Fig. 2

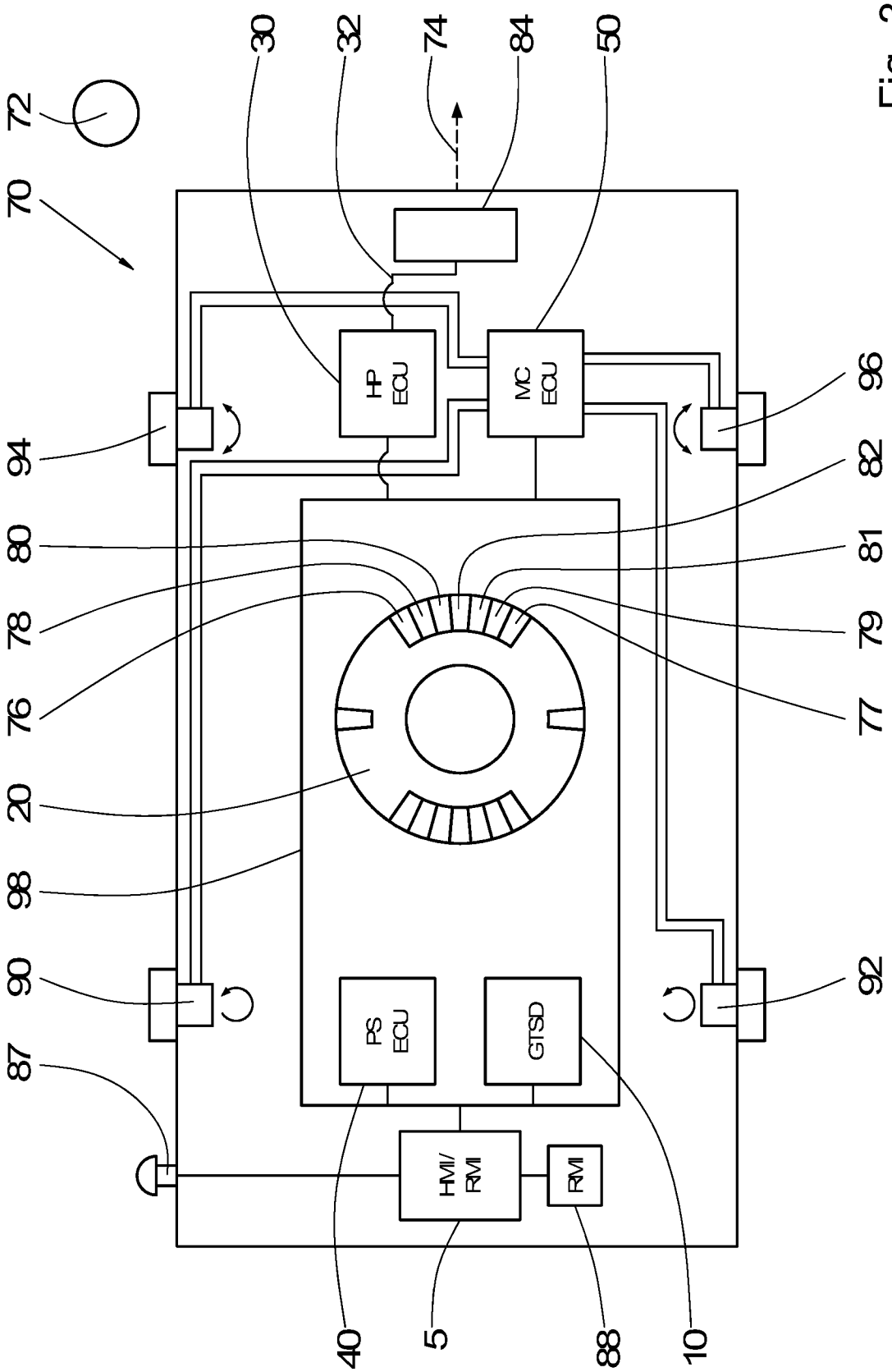
72
70
30
32
74
84
50
HP ECU
MC ECU
94
96
82
80
81
78
79
76
77
20
98
90
92
87
PS ECU
GTSD
HMI/ RMI
RMI
40
5
88
10

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2020/053236

A. CLASSIFICATION OF SUBJECT MATTER

G05D 1/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2017055563 A (TOYOTA MOTOR CORP) 16 March 2017 (2017-03-16) abstract	1-17
A	US 2017090476 A1 (LETWIN NICHOLAS [US] ET AL) 30 March 2017 (2017-03-30) paragraph [0011] - paragraph [0062]	1-17
A	US 8705527 B1 (ADDEPALLI SATEESH K [US] ET AL) 22 April 2014 (2014-04-22) column 4, line 20 - column 15, line 20 column 18, line 15 - column 29, line 16	1-17
A	WO 2018154859 A1 (HONDA MOTOR CO LTD [JP]) 30 August 2018 (2018-08-30) abstract	1-17

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 May 2020	**14 May 2020**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Coda, Ruggero** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2020/053236

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2017055563 A	16 March 2017	NONE	
US 2017090476 A1	30 March 2017	EP 3356899 A2	08 August 2018
		US 2017090476 A1	30 March 2017
		US 2018321677 A1	08 November 2018
		WO 2017058961 A2	06 April 2017
US 8705527 B1	22 April 2014	US 8514825 B1	20 August 2013
		US 8705527 B1	22 April 2014
		US 8718797 B1	06 May 2014
		US 8848608 B1	30 September 2014
		US 8863256 B1	14 October 2014
		US 8903593 B1	02 December 2014
		US 8989954 B1	24 March 2015
		US 9036509 B1	19 May 2015
		US 9083581 B1	14 July 2015
		US 9154900 B1	06 October 2015
		US 2013301584 A1	14 November 2013
		US 2014215491 A1	31 July 2014
		US 2014303807 A1	09 October 2014
		US 2014380442 A1	25 December 2014
		US 2015029987 A1	29 January 2015
		US 2015222708 A1	06 August 2015
		US 2015264554 A1	17 September 2015
		US 2017251339 A1	31 August 2017
		US 2019020985 A1	17 January 2019
WO 2018154859 A1	30 August 2018	CN 110290999 A	27 September 2019
		DE 112017007113 T5	31 October 2019
		JP WO2018154859 A1	12 December 2019
		US 2019359225 A1	28 November 2019
		WO 2018154859 A1	30 August 2018

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2020/053236

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G05D1/00
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G05D

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	JP 2017 055563 A (TOYOTA MOTOR CORP) 16. März 2017 (2017-03-16) Zusammenfassung	1-17
A	US 2017/090476 A1 (LETWIN NICHOLAS [US] ET AL) 30. März 2017 (2017-03-30) Absatz [0011] - Absatz [0062]	1-17
A	US 8 705 527 B1 (ADDEPALLI SATEESH K [US] ET AL) 22. April 2014 (2014-04-22) Spalte 4, Zeile 20 - Spalte 15, Zeile 20 Spalte 18, Zeile 15 - Spalte 29, Zeile 16	1-17
A	WO 2018/154859 A1 (HONDA MOTOR CO LTD [JP]) 30. August 2018 (2018-08-30) Zusammenfassung	1-17

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
4. Mai 2020	14/05/2020

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Coda, Ruggero

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2020/053236

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
JP 2017055563 A	16-03-2017	KEINE	
US 2017090476 A1	30-03-2017	EP 3356899 A2	08-08-2018
		US 2017090476 A1	30-03-2017
		US 2018321677 A1	08-11-2018
		WO 2017058961 A2	06-04-2017
US 8705527 B1	22-04-2014	US 8514825 B1	20-08-2013
		US 8705527 B1	22-04-2014
		US 8718797 B1	06-05-2014
		US 8848608 B1	30-09-2014
		US 8863256 B1	14-10-2014
		US 8903593 B1	02-12-2014
		US 8989954 B1	24-03-2015
		US 9036509 B1	19-05-2015
		US 9083581 B1	14-07-2015
		US 9154900 B1	06-10-2015
		US 2013301584 A1	14-11-2013
		US 2014215491 A1	31-07-2014
		US 2014303807 A1	09-10-2014
		US 2014380442 A1	25-12-2014
		US 2015029987 A1	29-01-2015
		US 2015222708 A1	06-08-2015
		US 2015264554 A1	17-09-2015
		US 2017251339 A1	31-08-2017
		US 2019020985 A1	17-01-2019
WO 2018154859 A1	30-08-2018	CN 110290999 A	27-09-2019
		DE 112017007113 T5	31-10-2019
		JP WO2018154859 A1	12-12-2019
		US 2019359225 A1	28-11-2019
		WO 2018154859 A1	30-08-2018