(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 638 941**

(51) Int. CI.:

H04L 1/20 (2006.01)
B60T 8/88 (2006.01)
H04L 1/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.08.2013 PCT/EP2013/067823**

(87) Fecha y número de publicación internacional: **06.03.2014 WO14033172**

(96) Fecha de presentación y número de la solicitud europea: **28.08.2013 E 13753195 (0)**

(97) Fecha y número de publicación de la concesión europea: **31.05.2017 EP 2891264**

(54) Título: **Método para ejecutar una función de seguridad de un vehículo y sistema para ponerlo en práctica**

(30) Prioridad:

29.08.2012 DE 102012215343

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.10.2017

(73) Titular/es:

CONTINENTAL AUTOMOTIVE GMBH (100.0%)
Vahrenwalder Strasse 9
30165 Hannover, DE

(72) Inventor/es:

ERDEM, BETTINA y
ROSS, HANS-LEO

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método para ejecutar una función de seguridad de un vehículo y sistema para ponerlo en práctica.

La presente invención se refiere, en general, a un método para la ejecución de una función de seguridad en un vehículo y, en particular, a un sistema general para la ejecución de este método de acuerdo con las reivindicaciones.

Los vehículos modernos vienen equipados cada vez más con dispositivos de protección activos y pasivos. Los dispositivos de protección son en general unidades funcionales instaladas en el vehículo que desempeñan funciones de seguridad especiales de forma total o parcialmente automática. En general, una función de seguridad sirve para después de haber reconocido o determinado un incidente predefinido como peligroso restablecer una condición de seguridad, como por ejemplo, restablecer o mantener el funcionamiento del vehículo evitando o, por lo menos, minimizando de esta manera riesgos para las personas o los bienes, así como lesiones personales o daños materiales. Son funciones de seguridad conocidas y ampliamente utilizadas, por ejemplo, la activación de airbags mediante un sistema de airbags y el frenado de una o más ruedas del vehículo mediante un sistema de control electrónico de estabilidad.

Purnendu Sinha describe en “Architectural design and reliability analysis of a fail-operational brake-by- wire system from ISO 26262 perspectives", Reliability Engineering And System Safety, Elsevier Applied Science, GB, Bd. 96, Nr. 10, 15 de marzo de 2011, páginas 1349-1359, ISSN: 0951-8320, un análisis de fiabilidad de un sistema de freno del tipo Brak-by-wire. En este análisis se representó un árbol de averías de un sistema de freno mediante un diagrama de bloques asignándole a cada bloque una probabilidad de error.

Para la ejecución de las funciones de seguridad es fundamental contar con los datos necesarios, aquellos que contienen la información necesaria para la ejecución de la función de seguridad, por ejemplo, aquellos relacionados con el funcionamiento o el movimiento del vehículo.

Estos datos podrían ser, por ejemplo, datos enviados por una unidad sensora del vehículo, por ejemplo, una unidad sensora que detecte la cantidad de revoluciones de las ruedas o la posible colisión del vehículo. En la actualidad están en desarrollo ciertas funciones de seguridad que controlan de forma total o parcial el movimiento del vehículo en tránsito y que modifican, por ejemplo, la velocidad o la dirección del vehículo, para evitar un accidente o esquivar un obstáculo.

En general y en particular, en el caso de estas últimas funciones de seguridad existe cierta incertidumbre si al momento de la ejecución de la función de seguridad correspondiente los datos disponibles (y la información que contienen) son seguros y confiables para la ejecución de la función de seguridad. En particular existe la incertidumbre respecto de la calidad, la disponibilidad y la fiabilidad del sistema de comunicación empleado para la transmisión de los datos y, en particular, la incertidumbre respecto de la calidad de los datos enviados y sobre la posible pérdida de calidad durante la recepción de los datos. Así, por ejemplo, la pérdida o corrupción de los datos, que podría ocurrir como consecuencia de un desperfecto en el sistema de comunicación durante la transferencia de los datos, podría afectar a la ejecución de la función de seguridad. Ese efecto adverso a la función de seguridad podría, por ejemplo, provocar que la función de seguridad se ejecute en el momento equivocado o mediante un parámetro incorrectamente calculado.

La presente invención tiene por finalidad, proporcionar tanto un método como un sistema que permitan la ejecución segura y confiable de las funciones de seguridad de un vehículo.

Dicha finalidad de acuerdo con la presente invención se resolverá mediante un método de acuerdo con el objeto principal y mediante un sistema general según el objeto accesorio. El perfeccionamiento y formas de realización especiales del método y del sistema general se pueden se obtener con las reivindicaciones adjuntas.

Por lo tanto, en la presente se proporcionan métodos para realizar una función de seguridad en un vehículo mediante, al menos, unos datos de un sistema de comunicación, necesarios para la ejecución de la función de seguridad, en una unidad de control del vehículo. Mediante una unidad de control se generarán señales de control en función de los datos recibidos que serán transmitidas por una unidad funcional del vehículo. La función de seguridad se ejecutará a través de la unidad funcional en función de las señales control.

Asimismo, se repetirán pruebas de diagnóstico a intervalos para determinar si hubo una falla en uno o más de los sistemas eléctricos, electrónicos o programables o si se produjo un error que impidió la ejecución de la función de seguridad o que pudiera afectar a los datos relacionados con la seguridad. Estas pruebas de diagnóstico se ejecutarán en cada uno de estos sistemas.

Respecto del método propuesto es asimismo esencial que se transmitan mediante el sistema de comunicación los metadatos de los datos a través de la unidad funcional, de modo que la información de los metadatos se refiera al menos uno de los sistemas eléctricos, electrónicos y/o programables empleados para realizar el método. Preferiblemente, estos metadatos incluyen al menos información sobre el sistema de comunicación. Por medio de la unidad de control se determinará en función de esta información al menos la fiabilidad de los datos respecto de

–la probabilidad de que se produzca un error o una avería que podría afectar a la ejecución de la función de seguridad y

la probabilidad de que la existencia de estas fallas o avería sea detectada por las pruebas de diagnóstico y/o por un conductor del vehículo (2) oportunamente antes de que la función de seguridad resulte adversamente afectada, en donde la unidad de control (4) verifica, como una función de al menos un valor de fiabilidad, si los datos transmitidos son confiables para realizar la función de seguridad. Además, se puede verificar mediante la unidad de control si están disponibles los datos necesarios para ejecutar la función de seguridad correspondiente (y para el adecuado control de la unidad de función) están completos (incluida la información de diagnóstico necesaria).

El sistema general que aquí se propone para la ejecución de la función de seguridad de un vehículo, comprende el vehículo y un sistema de comunicación que está configurado para transmitir los datos necesarios para la ejecución de la función de seguridad por la unidad funcional del vehículo. La unidad funcional está configurada para crear, en función de los datos trasmitidos, señales de control y transmitirlas mediante una unidad funcional del vehículo. La función de seguridad está configurada para ejecutar la función de seguridad en función de las señales de control.

El sistema general está configurado además para realizar repetidamente a intervalos pruebas de diagnóstico para verificar si hay una falla en uno o más sistemas eléctricos, electrónicos y/o programables del sistema general, como por ejemplo, si existe una falla que podría afectar adversamente la ejecución de la función de seguridad.

Según el procedimiento propuesto es esencial para el sistema general que el sistema de comunicación esté configurado además para transmitir los metadatos de los datos mediante la unidad funcional en donde los metadatos contienen información de al menos uno de dichos sistemas del sistema general. Preferiblemente estos metadatos contienen información, al menos, sobre el sistema de comunicación. La unidad funcional está configurada además, en función de dicha información, para determinar al menos un valor de fiabilidad de los datos respecto de

la probabilidad de que se produzca un error o una avería que podría afectar la ejecución de la función de seguridad y

la probabilidad de que la existencia de estas fallas o averías sea detectada por las pruebas de diagnóstico y/o por un conductor del vehículo oportunamente antes de que la función de seguridad resulte adversamente afectada, y en función de al menos un valor de fiabilidad para verificar si los datos transmitidos son confiables para realizar la función de seguridad. Asimismo, se puede configurar la unidad funcional para verificar si los datos necesarios para ejecutar la función de seguridad están disponibles.

Para realizar de forma eficaz la función de seguridad es igualmente necesario además, que el uso de los datos transmitidos y la información que estos contienen permita reconocer cierta situación de riesgo o suceso peligroso, como se describirá más adelante con los ejemplos correspondientes.

La siguiente explicación se refiere tanto al método como al sistema general propuestos. Esto significa en particular, que ciertos nuevos desarrollos y diseños ejemplificativos, que se describen únicamente en relación con el método o únicamente en relación con el sistema en general, se pueden usar tanto en el sistema general o como en el método. El término “estar configurado” significa que la función de seguridad o el sistema (eléctrico, electrónico y/o programable) en cuestión está diseñado y programado de manera tal que las funciones siguientes se pueden realizar mediante la unidad funcional, por ejemplo, ejecutar en el sistema. Por ejemplo, la unidad funcional, como por ejemplo el sistema, puede comprender componentes eléctricos, electrónicos y/o programables, tales como, circuitos, controladores, microchips, sensores, almacenamiento de datos, interfaces, líneas de datos, receptores, transmisores, etc. En particular, el sistema de comunicación puede comprender una WLAN y/o una red móvil y/o un sistema de transmisión de datos por cable o inalámbrico y la unidad funcional puede estar provista, por ejemplo, de receptores e interfaces de datos compatibles con ellos.

Él método y el sistema propuestos se distinguen por una “seguridad funcional” particularmente elevada, en la cual la verificación de la fiabilidad y disponibilidad de los datos necesarios para la realización están integrados directamente en el método o en el sistema general. Por lo tanto, es posible por ejemplo que, como se describe más adelante, la función de seguridad se ejecute en consideración de los resultados de la verificación, por ejemplo, solo cuando el resultado de la verificación sea positivo, es decir cuando los datos disponibles sean suficientemente confiables y (completos) para ejecutar la función de seguridad.

Bajo la seguridad funcional mencionada, en el caso en cuestión se describe parte de la seguridad general del sistema general de la que depende el correcto funcionamiento de los sistemas eléctricos, electrónicos y/o programables (en adelante, sistemas E/E/PE) en relación con la seguridad del sistema general y, dado el caso, en relación con servicios externos. En el caso en cuestión, todos los sistemas E/E/EP del sistema general propuesto se especificarán como importantes para la seguridad o importantes para ella, aquellos que se utilizan para la ejecución del método propuesto y aquellos que en caso de que sufran una falla o avería, dicha falla o avería podría afectar adversamente la ejecución de la función de seguridad. Por consiguiente de aquí en adelante, se debe interpretar como falla o avería de uno de los sistemas E/E/EP toda condición anormal de los sistemas E/E/EP respectivos, como consecuencia de la cual, el sistema en cuestión ya no puede desempeñar su función o solo puede hacerlo de forma limitada. La falla o avería de los sistemas E/E/EP, que individualmente o en combinación con otras fallas o averías, impidan ejecutar la función de seguridad, siempre y cuando no sean reconocidas oportunamente, se considerarán también en adelante como fallas funcionales, fallas relacionadas con la seguridad o fallas con un efecto importante para la seguridad.

Mediante el método y el sistema general propuestos todos los riesgos relacionados con fallas funcionales que se reconozcan y analicen durante la fase conceptual de la función de seguridad correspondiente y que se tengan en cuenta de forma automática o automatizada podrán ser controlados y minimizados de forma automática o automatizada. Por ejemplo, el valor de fiabilidad de los datos se puede definir como criterio de verificación durante la fase conceptual. Durante la fase de uso o de puesta en marcha de la función de seguridad se utiliza este valor de fiabilidad para comprobar de forma automática o automatizada la disponibilidad y seguridad de los datos. El valor de fiabilidad se utiliza como “calificador” electrónico, que representa la disponibilidad e integridad de la información que se puede utilizar electrónicamente. Con el método y el sistema general que se proponen en la presente también se puede realizar un análisis en línea de la disponibilidad, integridad y calidad (es decir, la integridad de la seguridad) mediante los datos y la información transmitidos por el sistema de comunicación.

Los datos necesarios para la ejecución de la función de seguridad pueden ser, por ejemplo, datos o señales de medición aportados por un sensor o una unidad de medición del sistema general o por información derivada de tales datos o señales de medición. La unidad de medición puede estar integrada a otro vehículo o infraestructura (fija). Por consiguiente, estos componentes del vehículo o de la infraestructura son parte del sistema general propuesto. Los datos, por lo tanto, también pueden provenir o ser transmitidos por un socio de comunicaciones externo al vehículo, como por ejemplo, otro vehículo (comunicación car2car, C2C) u otra infraestructura (fija) (comunicación car2infrastructure, C2X). Los datos pueden ser transmitidos mediante una cadena de diversos socios de comunicación (vehículo, infraestructura) a través de la unidad funcional del vehículo. Dicha cadena de socios de comunicación es, por consiguiente, parte del sistema de comunicación y, por lo tanto, también un componente del sistema general aquí propuesto. La comunicación puede ser tanto cableada o como inalámbrica. A continuación se presentarán otros ejemplos.

De los datos necesarios para la ejecución de la función de seguridad puede resultar que por el momento no constituyan un motivo para ejecutar la función de seguridad. Es decir que aun cuando los datos necesarios para ejecutar la función de seguridad sean completos y confiables, es posible que no se ejecute realmente dicha función. Por lo general, se prevé que la función de seguridad, como se describe a continuación, sólo se ejecute con la condición indispensable (pero no suficiente) de que los datos indispensables para ello estén totalmente disponibles y sean suficientemente confiables.

Las pruebas de diagnóstico mencionadas para detectar las fallas o averías mencionadas se pueden ejecutar por ejemplo mediante los correspondientes sistemas E/E/EP del sistema general automáticamente (autopruebas de este sistema). Aunque también es posible que se utilicen los sistemas de diagnóstico configurados para la ejecución de las pruebas de diagnóstico. De este modo, se pueden ejecutar pruebas de diagnóstico que abarquen todo el sistema general. Se entiende que una falla ha sido detectada oportunamente cuando se cuenta con el tiempo suficiente para tomar las medidas correctivas correspondientes para impedir los riesgos o daños causados o relacionados con la falla o minimizarlos al menos a un nivel aceptable.

Los mencionados metadatos pueden contener, por ejemplo, el valor de la anteriormente mencionada probabilidad o el valor de una o varias magnitudes de la que aquella depende, como la tasa de falla, la cobertura de diagnóstico, la métrica o las mediciones que se tratarán más adelante. Los metadatos pueden contener asimismo de forma adicional o alternativa la identificación de dispositivo de uno o varios de los sistemas E/E/EP importantes para la seguridad del sistema general. En este último caso sobre la base a los identificadores de dispositivo se pueden leer los valores de dicha probabilidad y de la tasa de error, de la cobertura de diagnóstico, la métrica y/o las mediciones de las que aquella depende pertenecientes al sistema E/E/EP correspondiente mediante, por ejemplo, la unidad de control de un dispositivo de almacenamiento o de una base de datos, para luego usarlos, como se describe, para determinar el valor mínimo de fiabilidad de los datos. Mediante dichos sistemas E/E/EP se pueden accionar en particular a través una unidad sensora o de medición, una unidad de transmisión del sistema de comunicación, un canal de comunicación del sistema de comunicación (al igual que, por ejemplo, un sistema WLAN o un sistema móvil

como UMTS, LTE, GPS, GPRS o EDGE) así como también una unidad de control de recepción. Además, la unidad de control y la unidad funcional son lógicamente sistemas E/E/EP importantes para la seguridad.

Mediante la mencionada verificación se puede prever, por ejemplo, si los datos transmitidos necesarios para la ejecución de la función de seguridad serán suficientemente fiables en comparación con el valor de fiabilidad de los datos con un umbral determinado. Por ejemplo, se puede prever que los datos clasificados como suficientemente seguros son mayores (o como alternativa, menores) que dicho umbral. El umbral se puede determinar según el potencial de riesgo (por ejemplo, definido teniendo en cuenta la probabilidad de que ocurra el siniestro y la magnitud del daño asociado a la función de seguridad) de la función de seguridad respectiva, o sea, cuanto mayor el potencial de riesgo de la función de seguridad, más alto será lógicamente el valor elegido para umbral correspondiente. Dado el caso que se puedan proporcionar varios valores de fiabilidad, se podrían comparar cada uno de los valores de fiabilidad con un umbral predefinido y, por ejemplo, solo se evaluarían como suficientemente seguros cada uno de los valores de fiabilidad que fuera mayor (o como alternativa, menor) que el umbral correspondiente.

Se consideran valores de fiabilidad en general los valores de mediciones de fiabilidad de los datos en cuestión. Estas mediciones en general dependen de las probabilidades mencionadas y de la probabilidad de que se produzca la falla o avería que podría afectar adversamente a la ejecución de la función de seguridad y de la probabilidad de que gracias a las pruebas de diagnóstico y/o a la intervención del conductor del vehículo no se produzca la falla o avería que podría afectar adversamente a la ejecución de la medida de seguridad. También es posible que uno o varios de al menos un valor de fiabilidad se obtenga a través del valor de una de estas probabilidades. Se consideran valores de fiabilidad de los datos, en particular, la tasa de error, el nivel de cobertura de diagnóstico y la métrica en cuestión.

Si de la verificación se desprende que los datos necesarios para la ejecución de la función de seguridad no están totalmente disponibles o no son suficientemente fiables, se puede prever que los datos transmitidos por la unidad de control no sean utilizados para disparar la función de seguridad y/o

que se envíe a través de la unidad de control una señal de desactivación de la función de seguridad, por lo cual principalmente la unidad funcional después de recibir dicha señal de desactivación entre automáticamente en un modo de seguridad en el cual no se pueda ejecutar la función de seguridad. De este modo se puede estar seguro de que la función de seguridad solo se ejecutará si la verificación determina que los datos necesarios para ello son suficientemente seguros y fiables.

Asimismo el método de esta manera determinará que para este caso los datos no están totalmente disponibles o no son suficientemente seguros. De forma adicional o alternativa es posible controlar mediante la unidad de control un emisor de señal del vehículo que informe al conductor el resultado de la verificación y si los datos necesarios para la ejecución de la función de seguridad están totalmente disponibles y son suficientemente fiables o no. De forma adicional o alternativa se puede prever para ello que, en caso de que la verificación indique que los datos necesarios para la ejecución de la función de seguridad no están completamente disponibles o son suficientemente fiables, se controle mediante la unidad de control un emisor de señal que informe al conductor que la función de seguridad no está disponible por el momento.

De este modo, el conductor siempre está informado de la disponibilidad de la función de seguridad.

De este modo el conductor puede ser asistido en su conducta en el tránsito personalizando el uso u omisión de la o las funciones de seguridad y si fuera necesario ajustando la respuesta respectiva. En caso de que, por ejemplo, el conductor fuera advertido oportunamente de que no hay datos suficientemente seguros y necesarios para ejecutar automáticamente la maniobra de frenado o de evasión automática u otros procedimientos total o parcialmente automatizados del funcionamiento del vehículo, el conductor podrá adoptar la actitud apropiada y conducir con la debida precaución. De esta manera también se puede asegurar que el conductor del vehículo pueda conducir siempre de forma responsable y confiar entonces en la ejecución automática de la función de seguridad, como la intervención autónoma, total o parcialmente automatizada en la conducción del vehículo cuando se le advierte que los datos necesarios están completamente disponibles y son suficientemente fiables. Esto cumple con los requisitos de la “Convención de Viena sobre tránsito”, que establecen que se debe garantizar que el conductor ejerza el control sobre el vehículo.

Es posible que se calcule al menos un valor de fiabilidad en función de al menos de una de las tasas de error siguientes: l_{SPF}, l_{RF}, l_{MPF}, $_{MP}$Fi_, l_{MP}FD, l_{MPFP}, l_S. Estas tasas de error (errores por unidad de tiempo) son valores estadísticos y se refieren a cierto tipo de falla. A continuación, se indican las definiciones de los distintos tipos de falla. Asimismo cinco de estas tasas de error suelen referirse únicamente a uno de los sistemas E/E/EP importantes para la seguridad, que se utilizan para la ejecución del método y que son parte del sistema general propuesto, y también para cierto tipo de fallas que pueden ocurrir en estos sistemas de E/E/EP. Es posible que para cada uno de estos sistemas E/E/EP solo se pueda definir cierto tipo de tasa de error.

Cada una de las tasas de error mencionadas de un sistema E/E/EP dado importante para la seguridad indica el número promedio de fallas para un tipo de error determinado, que se producen en una unidad de tiempo en el sistema E/E/EP respectivo. Una unidad típica a tal fin es 10^{-9} fallas por hora. El valor devuelto por estas tasas de error es el tiempo promedio entre fallas (MTBF o MTTF, por sus siglas en inglés), así como también el intervalo entre dos fallas. Las tasas de error se definirán típicamente para el tiempo de funcionamiento de cada sistema E/E/EP y, por consiguiente, son respectivamente una medición de que en el sistema E/E/EP considerado se produjo cierta falla según Art. 25 durante el período de funcionamiento del sistema E/E/EP. Individualmente son posibles las siguientes definiciones de los distintos tipos de fallas, a las que hacen referencia las respectivas tasas de error: l_{SPF}: fallas que, aun cuando se produzcan individualmente, son funcionales y tienen un efecto importante para la seguridad y cuya existencia no es verificada por las pruebas de diagnóstico y, por consiguiente, tampoco pueden ser detectadas oportunamente por las pruebas de diagnóstico antes de que la función de seguridad sea adversamente afectada; l_{RF}: fallas que, aun cuando se produzcan individualmente, son funcionales y tienen un efecto importante para la seguridad y cuya existencia es verificada por las pruebas de diagnóstico pero no son detectadas oportunamente antes de que tengan un efecto adverso sobre la función de seguridad (las pruebas de diagnóstico tiene también una así denominado demora respecto de este tipo de fallas); l_{RF}: fallas que, cuando se producen o existen junto con otras fallas, son funcionales y tienen además un efecto importante para la seguridad, siempre y cuando no se detecten oportunamente pueden producir un efecto adverso en la función de seguridad.

$l_{MPF\ L}$: fallas, que cuando se producen o existen junto con otras fallas, tienen un efecto importante para la seguridad y son funcionales, y cuya existencia no es verificada por las pruebas de diagnóstico así como tampoco pueden ser detectadas oportunamente por ellas. Estas fallas también se pueden describir como fallas latentes; l_{MPFD}: fallas, que cuando se producen o existen junto con otras fallas, tienen un efecto importante para la seguridad, son funcionales y su existencia no es verificada por las pruebas de diagnóstico así como tampoco pueden ser detectadas oportunamente por ellas; $l_{MPF\ P}$: Fallas, que cuando existen u ocurren junto con otras fallas tienen un efecto importante para la seguridad, son funcionales y su existencia puede ser detectada oportunamente por el conductor de un vehículo; l_S: fallas, que aun cuando no sea detectadas, no tienen efectos importantes para la seguridad y no son funcionales.

Se definirán además $l_{MPF,DP} = l_{MPF,D} + l_{MPF,P}$. También se aplica $l_{MPF} = l_{MPF,L} + l_{MPF,DP}$. También se aplica $l = l_{SPF} + l_{RF} + l_{MPF,L} + l_{MPF,DP} + l_S$, en donde l es la tasa de error del sistema E/E/EP considerado del sistemas general y una medición de la probabilidad de que cualquier falla (funcional o no) se produzca en estos sistemas E/E/EP, en donde l es la tasa de error general del sistema E/E/EP considerado del sistema general y una medición de la probabilidad, de que se produzca cualquier falla (funcional o no) en ese sistema E/E/EP.

Las tasas de error así definidas del sistema E/E/EP junto con la norma ISO 26262 se indican con los mismos símbolos y dimensiones, tal como se establece en el Capítulo 5, Anexo C, Sección C1 de la norma ISO 26262.

Por lo tanto en caso de que al menos uno de dicho valores de fiabilidad de los datos, por ejemplo, se calculen en función de una o varias de las magnitudes de l_{SPF}, l_{RF}, l_{MPF}, $l_{MPF\ L}$, l_{MPFP}, L_{MPFD} de los sistemas E/E/EP, se garantiza entonces que el valor de fiabilidad de la probabilidad de existencia de errores o averías que pueden afectar adversamente a la ejecución de la función de seguridad, así como también en función de la probabilidad de que la existencia de una falla o avería sea detectada por las pruebas de diagnóstico y/o por un conductor del vehículo oportunamente antes de que la ejecución de la función de seguridad sea adversamente afectada. En particular es posible que uno o varios o cada uno de al menos uno de los valores de fiabilidad se definan como una de las tasas de error I_{SPF}, I_{RF}, I_{MPF}, $I_{MPF\ L}$, $I_{MPF\ P}$ de uno de los sistemas E/E/EP importantes para la velocidad o en función de estas tasas de error.

Por ejemplo, al menos un valor de fiabilidad de al menos uno de los valores de fiabilidad de los datos sea calculado en función de al menos un valor de un nivel de cobertura de diagnóstico de al menos uno de los sistemas E/E/EP importantes para la seguridad del sistema utilizado para la ejecución del procedimiento.

$$DC_{RF} = \left(1 - \frac{\lambda_{RF}}{\lambda}\right) \times 100$$

El nivel de cobertura de diagnóstico es en particular una medición significativa para la fiabilidad de uno de los sistemas E/E/EP importantes para la seguridad. Esta medición corresponde a la definición mediciones $K_{DC,\ RF}$ de la norma ISO 26262, Capítulo 5, Anexo C.3. También es posible que para varios o cada uno de los sistemas E/E/EP importantes para la seguridad del sistema general se calcule le valor de se calculen los niveles de cobertura $DC_{rf.}$ Por último, estos valores se pueden utilizar como valores de fiabilidad de los datos. Es posible, de forma alternativa o

adicional, determinar uno de los valores de fiabilidad o el valor de fiabilidad como producto del valor de este nivel de cobertura de diagnóstico, por consiguiente como $DC_{RF,1}$ x$DC_{RF,2}$ x $DC_{RF,3}$ x ... x $DC_{RF,n}$, es el número de sistemas E/E/EP importantes para la seguridad del sistema general. Este producto se corresponde con la así llamada “Ley de Lusser” y es en particular una medición significativa para la fiabilidad del sistema general y, por lo tanto, también para los datos, en particular entonces cuando se conocer para cada uno de los sistemas E/E/EP del sistema general el nivel de cubertura de diagnóstico correspondiente (y se incluyen en el producto como uno de los factores) y en cada uno de los sistemas E/E/EP en que dichas pruebas de diagnóstico se ejecutan.

En otra forma de realización, mediante la cual para la ejecución del método son utilizados asimismo más sistemas E/E/EP relacionados para la seguridad, se prevé que al menos se use un valor de fiabilidad de al menos uno de los valores de fiabilidad de los datos que depende del valor de la métrica (M_{SPFRF})

$$M_{SPF,RF} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{SPF} + \lambda_{RF})}{\sum_{\text{safety-related HW elements}} \lambda}$$

La sumatoria incluye varios, preferentemente todos, los sistemas E/E/EP importantes para la seguridad del sistema general que también se usan para la ejecución del método. La frase “safety-related HW elements” se refiere en la presente a los sistemas E/E/EP importantes para la seguridad. Esta métrica corresponde a la Norma ISO 26262, Capítulo 5, Anexo C, Sección C.2 que se define como “métrica para falla de un solo punto”. La métrica $M_{SPF\ RF}$ también es significativa, cuando dichas pruebas de diagnóstico no se ejecutan en todos los sistemas E/E/EP o cuando no se ejecuta ninguna prueba de diagnóstico que incluya el sistema general.

En una forma de realización del método (que comprende además el sistema general) se prevé que en caso de que los datos necesarios para la ejecución de la función de seguridad no estén completamente disponibles o no sean suficientemente confiables,

los datos se transmitirán nuevamente a través de la unidad de control transcurrido un tiempo de espera predefinido, en donde los datos se transmiten de esta manera frecuentemente a la unidad control hasta que estén totalmente disponibles y sean suficientemente confiables. Esta es una posibilidad, en que por ejemplo, se puede utilizar información repetida de forma temporal. Por ejemplo, se puede alcanzar en caso de que aparezca un obstáculo ante el vehículo y sea captado primero con una calidad por ejemplo del 10% de la calidad total del sensor y más tarde se confirma con una calidad del 50%, en cumplimiento de la ley de fiabilidad para este tipo de información redundante una fiabilidad total del 90% de la fiabilidad básica.

En una forma de realización se prevé que los metadatos durante la puesta en marcha del vehículo, en particular antes de que comience a circular, se transmitan a través de la unidad de control, en donde se utilizará al menos un valor de fiabilidad de al menos uno de los valores de fiabilidad de los datos en función del valor de la cobertura del diagnóstico (DC_{MPFL}).

$$DC_{MPF,L} = \left(1 - \frac{\lambda_{MPF,L}}{\lambda}\right) \times 100$$

de al menos uno de los sistemas E/E/EP del sistema general, en donde la función de seguridad solo se ejecuta con la condición adicional de que este valor de fiabilidad utilizado en la puesta en marcha sea superior a un valor de umbral predeterminado. Este nivel de cobertura de diagnóstico corresponde a la definición mediciones K_{DCMPFL} de la norma ISO 26262, Capítulo 5, Anexo C, Ecuación C.4. De la misma manera, se calcularán los riesgos correspondientes que se basan en fallas o averías ya existentes o desconocidas, que solo en combinación con otras fallas o averías afectan adversamente a la función de seguridad. El nivel de cobertura de diagnóstico $DC_{MPF,L}$ es por lo tanto una medición particularmente significativa para la fiabilidad correspondiente a una falla latente del sistema general (y, por consiguiente, para los datos), véase más arriba la definición de este tipo de tasa de error. Asimismo

también es posible la formación de producto DC_{RF} descrito más arriba, donde deben cumplirse las condiciones correspondientes.

En una forma de realización se prevé que los metadatos durante la puesta en marcha del vehículo, en particular antes de que comience a circular, se transmitan a través de la unidad de control, en donde se determinará al menos un valor de fiabilidad de al menos uno de los valores de fiabilidad de los datos en función del valor de la métrica (M_{mpfl})

$$M_{MPF,L} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{MPF,L})}{\sum_{\text{safety-related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

en donde la sumatoria incluirá varios, preferiblemente todos, los sistemas E/E/EP importantes para la seguridad del sistema general 1, en donde la función de seguridad se ejecutará únicamente con la condición adicional de que este valor de fiabilidad supere un umbral dado. Esta métrica corresponde a la Norma ISO 26262, Capítulo 5, Anexo C, Sección C0.3 que se define como “métrica para falla latente”. De la misma manera se calcularán los riesgos correspondientes que se basan en fallas o averías ya existentes o desconocidas, que solo en combinación con otras fallas o averías afectan adversamente a la función de seguridad. La métrica M_{MPFL} es también una medición de fiabilidad de la fiabilidad de los datos, en caso de que las pruebas de diagnósticos no cubran el sistema general y, por ejemplo, solo verifiquen algunos de los sistemas E/E/EP del sistema general relacionados con la seguridad.

En una forma de realización del método o del sistema general se prevé que la función de seguridad sea un dispositivo de protección del vehículo activo o pasivo. Por ejemplo, se puede prever que

la unidad funcional sea un sistema de freno electrónico y la función de seguridad, un potenciador de freno automático y/o que

la unidad funcional sea un asistente de freno de emergencia y la función de seguridad, una operación de freno total o parcial del vehículo que se acciona automáticamente y/o que

la unidad funcional sea un asistente de evasión y la función de seguridad permita eludir automáticamente un obstáculo y/o

la unidad funcional sea una unidad ESC y la función de seguridad un estabilizador automático del vehículo, en particular, mediante el frenado de una o varias ruedas del vehículo y/o la limitación de la potencia del motor del vehículo y/o que

la unidad función sea un sistema de airbag y la función de seguridad, la activación del airbag.

Mediante el sistema general también se pueden conectar varios vehículos mediante un dispositivo de carga eléctrico en donde se establezca la comunicación y la transferencia de datos entre dicho dispositivo y el vehículo. Aquí por ejemplo, se puede prever que la función de seguridad se interrumpa el suministro de corriente al dispositivo de carga o que se interrumpa el proceso de carga antes de que produzca la sobrecarga de la batería.

A continuación el método y el sistema general aquí propuestos se representarán de forma esquemática en las Figuras 1 a 5 y se explicarán en detalle formas especiales de realización. Se muestra:

en la Figura 1 una manera de ejecutar una función de seguridad de un vehículo según el sistema general de la presente; en la Figura 2 un ejemplo de un diagrama de los principios del sistema;

en la Figura 3 un sistema de bus para la transmisión de “mensajes relacionados con la seguridad”;

en la Figura 4 un diagrama de bloques y en la Figura 5 las etapas del control primario.

La Figura 1 muestra una manera, según el sistema general de la presente, de ejecutar un ejemplo especial del método de la presente mediante la ejecución de una función de seguridad de un primer vehículo 2. El sistema general incluye el primer vehículo 2 y un sistema de comunicación 3, que está configurado para transmitir los datos necesarios para la ejecución de la función de seguridad a través de una unidad de control 4 del vehículo. La unidad

de control 4 está configurada para generar, en función de los datos trasmitidos, señales de control y transmitirlas por una unidad funcional del vehículo 2. La unidad funcional está configurada para ejecutar la función de seguridad en función de las señales de control.

Mediante la unidad funcional 5 se acciona un sistema de frenos electrónico del vehículo 2 en la forma de un asistente de frenado de emergencia y mediante una función de seguridad se accione automáticamente el frenado total o parcial del vehículo 2. Del mismo también podría preverse que la unidad funcional sea un asistente de evasión y la función de seguridad consista en eludir automáticamente un obstáculo y/o la unidad funcional sea una sistema ESC y la función de seguridad consista en estabilizar automáticamente el vehículo, en particular mediante el frenado de una o más ruedas del vehículo y/o mediante la limitación de la potencia del motor del vehículo y/o la unidad funcional sea un sistema de airbag y la función de seguridad el accionamiento de los airbags.

El sistema general 1 está configurado además para repetir a intervalos de tiempo las pruebas de diagnóstico para verificar si en uno o más de los sistemas eléctricos, electrónicos y/o programables, como así también en un sistema E/E/EP importante para la seguridad del sistema general 1 existe una falla o ha ocurrido una avería que podría haber afectado adversamente la ejecución de la función de seguridad. En este ejemplo se propone que se ejecuten autopruebas automáticamente por medio de los sistemas E/E/EP del sistema general 1 (autopruebas del sistema). Aunque también es posible que se configuren para la ejecución de las pruebas de diagnóstico los sistemas de diagnóstico correspondientes. A los sistemas E/E/EP importantes para la seguridad pertenecen en particular la unidad de control 4, la unidad funcional 5 y el sistema de comunicaciones 3, que en este ejemplo una primera unidad de comunicación 6 de la unidad de control 4 comprende una segunda unidad de comunicación 7 y una tercera unidad de comunicación 8. Las unidades de comunicación 6, 7, 8 están configuradas para la transmisión inalámbrica recíproca de datos por los canales de comunicación de base móvil 9, 10, 11 (como UMTS, LTE, GPS, GPRS o EDGE) Como alternativa se podrían utilizar otras unidades y canales de comunicación (como por ejemplo, un sistema WLAN).

Respecto de los datos necesarios para la ejecución de la función de seguridad se utilizan mediciones y señales de medición de una primera y una segunda unidad de medición 12, 13 del sistema general 1. Las unidades de medición 12, 13 de este ejemplo, pueden estar integradas respectivamente en un segundo o tercer vehículo 14, 15 aunque también pueden estarlo en una estructura fija. Los vehículos 14, 15, son, por lo tanto, también parte del sistema general 1. Los datos se pueden transmitir por comunicación car2car (C2C) aunque también se pueden transmitir por comunicación car2infastructure (C2X) en caso de que se utilice dicha estructura. Los datos se pueden transmitir al primer vehículo 2 través de una cadena compuesta por el segundo y tercer vehículo 14, 15.

El sistema de comunicación 3 está configurado además, para transmitir además de los datos, los metadatos de los datos a través de la unidad de control 4, los cuales incluyen información de los metadatos sobre los siguientes sistemas E/E/EP del sistema general 1: la primera unidad de comunicación 6, la segunda unidad de comunicación 7, la tercera unidad de comunicación, los canales de comunicación 9, 10, 11 y la primera y la segunda unidad de medición 12, 13.

Respecto de estos metadatos se utiliza para cada uno de estos sistemas E/E/EP el valor de las siguientes tasas de error, que corresponden cada una a un tipo de falla que se puede presentar en los sistemas E/E/EP correspondientes: Ispf, Irf, Impf, Impf,l, Impf,d, $l_{MPF\ P}$, l_S donde las tasas de error son las definidas anteriormente. (Por tal motivo no se repiten las definiciones especificadas con anterioridad.) [45]

Dichos datos se pueden usar además o en lugar de los valores de estas tasas de error aunque también se pueden usar los valores del nivel de cobertura de diagnóstico o las métricas, por ejemplo, las métricas y niveles de diagnóstico de cobertura tal como se indica a continuación. Los metadatos se pueden usar además o en lugar de los identificadores de uno o varios de dichos o todos los sistemas E/E/EP importantes para la seguridad del sistema general 1. En el último caso sobre la base de estos identificadores de dispositivo se pueden leer de un almacenamiento 16 o base de datos y seguir utilizando los valores de tasa de error, nivel de cobertura de diagnóstico o métricas que corresponde a los sistemas E/E/EP mediante la unidad de control 4.

Las tasas de error especificadas más arriba tanto de la unidad de control 4 como las de la unidad funcional, que son asimismo sistemas E/E/EP del sistema general 1, se guardan en el almacenamiento 16 de la unidad de control y no se trasmiten como metadatos.

La unidad de control está configurada, en función de dicha información, y de la tasa de error, para calcular el valor de fiabilidad de los datos. Entonces estas tasas de error dependen de la probabilidad de que la existencia de fallas o averías que podrían afectar adversamente a la ejecución de la función de seguridad y de la probabilidad de que la existencia de estas fallas o averías sea reconocida por las pruebas de diagnóstico y/o por el conductor del vehículo oportunamente antes de que afecte adversamente a la ejecución de la función de seguridad; los valores de fiabilidad también dependen de dichas probabilidades.

Se calcularán mediante la unidad de control 4 los valores del nivel de cobertura de diagnóstico (DCRF) de

$$DC_{RF} = \left(1 - \frac{\lambda_{RF}}{\lambda}\right) \times 100$$

de la primera unidad de comunicación 6, de la segunda unidad de comunicación 7, de la tercera unidad de comunicación 8, de los canales de comunicación 9, 10, 11, la primera y la segunda unidad de medición 12, 13 así como también de la unidad de control 4 y de la unidad funcional 5. Por último se determinará uno de los valores de fiabilidad como producto del valor de estos niveles de cobertura de diagnóstico $DC_{RF,1}$ x $DC_{RF,2}$ x $DC_{RF,3}$ x ... x $DC_{RF,n}$, donde n representa la cantidad de sistemas E/E/EP importantes para la seguridad del sistema general 1. En caso de que se puedan utilizar indistintamente los datos de medición de ambas unidades de medición 12, 13 para controlar la unidad funcional, los niveles de ambas unidades de medición 12, 13, todas las unidades de comunicación 6, 7, 8 y todos los canales de comunicación 9, 10, 11 van al producto y, por lo tanto, al valor de probabilidad. De no ser así, solo el nivel de cobertura de diagnóstico de esa unidad de medición se incluirá en el producto, y por consiguiente, en el valor de fiabilidad uno de cuyos valores de medición se utilizó realmente en el control de la unidad función y solo el nivel de cobertura de diagnóstico de aquellos canales de comunicación y unidades de comunicación que participaron realmente en la transmisión de dicho valor de medición. En este caso es posible por ejemplo, como se describe más adelante, que se elija el valor de medición de aquella unidad de medición con la cual se pueden alcanzar un mayor valor de fiabilidad de los datos. También es posible de manera análoga, determinar un valor de fiabilidad alternativo (o adicional) de los datos como valor de la métrica ($M_{SPF,RF}$)

$$M_{SPF,RF} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{SPF} + \lambda_{RF})}{\sum_{\text{safety-related HW elements}} \lambda}$$

Por medio de la unidad de control 4 se confirma en función del valor de fiabilidad de los datos dados como producto del valor de estos DCRF si la transmisión de datos necesarios para la ejecución de la función de seguridad son suficientemente confiables, en tanto se compara el valor de fiabilidad de los datos con un umbral dado. Los datos se considerarán entonces suficientemente seguros si el valor de fiabilidad es mayor (o como alternativa, menor) que dicho umbral. El umbral se fija en función del potencial de riesgo de la función de seguridad. Cuanto mayor el potencial de riesgo de la función de seguridad, mayor será el umbral correspondiente.

Asimismo, se puede configurar la unidad funcional para verificar si los datos necesarios para realizar la función de seguridad están totalmente disponibles.

Si de la verificación se desprende que los datos necesarios para la ejecución de la función de seguridad no están completamente disponibles o no son suficientemente confiables, se puede prever que los datos transmitidos por la unidad funcional no sean utilizados para activar la función de seguridad 5. Además, en este caso se envía una señal de desactivación desde la unidad de control 4 a la unidad funcional 5, y por consiguiente, la unidad funcional 5 después de recibir la señal de desactivación entra automáticamente en un modo de seguridad en el cual no se puede ejecutar la función de seguridad. De este modo se garantiza que la función de seguridad se ejecutará solo si la verificación determina que los datos necesarios para ello son suficientemente seguros y confiables. Asimismo de esta manera el método determinará que para este caso los datos no están totalmente disponibles o no son suficientemente seguros.

Se prevé además que es posible controlar mediante la unidad de control 4 un emisor de señal 17 del primer vehículo 2 que informe al conductor el resultado de la verificación y además si los datos necesarios para la ejecución de la función de seguridad están totalmente disponibles y son suficientemente fiables o no. Se prevé además que en caso de que la verificación indique que los datos necesarios para la ejecución de la función de seguridad no están completamente disponibles o no son suficientemente confiables, se controle mediante la unidad de control 4 el emisor de señal que informe al conductor que la función de seguridad no está disponible por el momento.

De la transmisión de los datos se puede determinar, en particular, que por el momento no hay motivo para la ejecución de la función de seguridad. Esto también se puede comunicar al conductor mediante el emisor de señal 17, en caso de que estos datos sean suficientemente confiables. Es decir que aun cuando los datos necesarios para

ejecutar la función de seguridad este completamente disponibles y sean confiables, es posible que no se ejecute realmente dicha función.

Se puede prever además que los metadatos de los datos ya se hayan transmitido mediante la unidad de control 4 durante la puesta en marcha del vehículo 2 antes de iniciar el un viaje. Naturalmente esto solo es posible cuando la transmisión de los datos y los metadatos se puede realizar durante la puesta en marcha. Esto se puede lograr fácilmente en algunos casos en los que las unidades de medición 12, 13 al igual que el sistema de comunicación 3 están integrados al primer vehículo 2. Esto suele ser así cuando la unidad funcional 5 es una unidad ESC y la función de seguridad consiste en estabilizar el vehículo 2 automáticamente como por ejemplo, mediante el frenado de una o varias ruedas del vehículo o mediante la reducción de la potencia del motor del vehículo.

Durante la puesta en marcha del vehículo se activan estos sistemas y se transmiten los metadatos a través de la unidad de control 4. Luego se pueden calcular los valores del nivel de cobertura del diagnóstico ($D_{CMPF,L}$)

$$DC_{MPF,L} = \left(1 - \frac{\lambda_{MPF,L}}{\lambda}\right) \times 100$$

de la primera unidad de comunicación 6, de la segunda unidad de comunicación 7, de la tercera unidad de comunicación 8, de los canales de comunicación 9, 10, 11, la primera y la segunda unidad de medición 12, 13 así como también de la unidad de control 4 y de la unidad funcional 5. Entonces, se determinará como valor de fiabilidad adicional de los datos el producto de los valores de este nivel de cobertura de diagnóstico así como también el valor de $DC_{MPF,L,1}$ $DC_{MPF,L,2}$ x $DC_{MPF,L,3}$ x ... x $DC_{MPF,L,n}$

$$M_{MPF,L} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{MPF,L})}{\sum_{\text{safety-related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

También es posible, que según corresponda se determine un valor de fiabilidad alternativo (o adicional) de los datos como un valor de la métrica ($M_{MPF,L}$), donde se realice preferentemente la sumatoria de todos los sistemas E/E/EP importantes para la seguridad del sistema general 1. La función de seguridad se ejecutará entonces solo con la condición adicional de que el valor de fiabilidad obtenido de $DC_{MPF,L}$ (o como alternativa de $M_{MPF,L}$) supere un umbral prestablecido. En esta forma de realización de ejemplo además se volverán a transmitir los datos, en caso de que los datos necesarios la ejecución de la función de seguridad en la unidad de control 4 no estén completamente disponibles o no sean suficientemente confiables, después de que haya transcurrido un tiempo de espera dado a través de la unidad de control 4; los datos se volverán a transmitir de esta manera a través de una unidad de control 4 a intervalos hasta que los datos estén completamente disponibles y sean suficientemente confiables. De esta manera en caso de que la primera unidad de medición detecte un obstáculo para el vehículo primero con una calidad de, por ejemplo, del 10% de la calidad máxima de la unidad de medición 12 y sea detectado más tarde con una calidad del 50% por la segunda unidad de medición 13, en cumplimiento de la ley de fiabilidad para este tipo de información redundante se alcanzará una fiabilidad general respecto de fiabilidad básica superior al 90%. Mediante esta confirmación mutua de los metadatos de la primera unidad de medición 12 y de los metadatos de la segunda unidad de medición 13 puede de esta manera se pueden obtener un valor de fiabilidad de estos datos, suficientemente alto para la ejecución de la función de seguridad, si bien los datos medidos por las unidades de medición 12, 13 transmitidos por separado no hayan sido suficientemente fiables.

Los componentes que se muestran en las Figuras 2 a 5 corresponden a un vehículo normal, según las políticas vigentes pertinentes. En conjunto el sistema básico aquí descrito, que incluye frenos, dirección, etc. se corresponde con los sistemas aprobados. La función aquí descrita debe controlar un vehículo en tránsito a fin de que circule de forma segura (mediante un sistema parcial o totalmente automático) asistiendo al conductor (en el sentido de los sistemas de asistencia al conductor actuales) de modo que pueda conducir de manera independiente o bien bajo el control de otros sistemas o complementos. De modo que la intervención externa solo pueda frenar o acelerar el vehículo. En otras especificaciones esto se describirá mediante el control de la velocidad del vehículo, en donde el rango de velocidad entre la desaceleración hasta la detención y aceleración es de hasta 130 km/h.

Según principios similares es posible que vehículo sea objeto de interferencias transversales (p.ej., por la conducción o por frenado lateral, como ESC) o verticales (sistema dinámico de amortiguación por resortes), sin embargo para ello se incluyen otros sensores y actuadores.

El diseño del dispositivo de control, cuyo así llamado calificador lleva el sistema de la invención, debe cumplir con la norma ISO 26262 una vez aplicado el ASIL máximo.

En la Figura 2, el diagrama de bloques principios debe interpretarse como un ejemplo. La información externa al vehículo proviene en este ejemplo de un portal de tránsito y se puede transmitir mediante comunicaciones V2I y TTS-G5. La información interna del vehículo de los sensores a bordo en la Figura 2 proviene de las cámaras o de otros sensores del vehículo (como por ejemplo, el sistema ESC).

Los elementos más importantes son:

E1- un portal en una autopista equipado con un sistema de comunicación V2X capaz de entregar información relacionada con la seguridad. - límite de velocidad permitido para los próximos tramos de carretera, información sobre el tiempo o sobre problemas de tránsito que podrían afectar a la conducción del vehículo por parte del conductor. (Niebla, contaminación, embotellamientos, etc.)

E2 – Sistema de transmisión de datos a una central de control de tránsito

E3 – Procesamiento de datos en la central de control de tránsito

E4 – Sistema de transmisión de datos que pone a disposición de los vehículos en las áreas pertinentes los datos de la central de control de tránsito por medio de la telefonía móvil. En el sentido estricto de la conexión móvil de la central de tránsito con el vehículo respectivo.

E5 – Sistema de cámaras que permite el reconocimiento de señales de tránsito, condición de manejo del vehículo que va delante, de personas y señalización de autopistas, etc.

E6 – Sistema de comunicación del dispositivo de control central del vehículo

E9 – Dispositivo de control central del vehículo

El vehículo cuenta además con una pantalla que puede mostrar el estado de los indicadores de seguridad en forma de semáforos.

El dispositivo de control central del vehículo puede influir a través de la interfaz de comunicación del vehículo en la gestión del motor y del dispositivo de control de freno en un intervalo de 0 a 100% del margen de regulación de los respectivos dispositivos de control.

Todos los sistemas E1 a E9 generan cada uno un calificador de diagnóstico único para cada sistema que indica la calidad del diagnóstico disponible al momento de la transferencia de los datos.

DCSPF = 0 - 60 % diagnóstico débil

DCSPF = 60 - 90 % error de sistema estático que dominará.

DCSPF = 90 - 99 % error de sistema dinámico que dominará.

Dependiendo de la interpretación, cada sistema E1 a E9 proporciona un valor de fiabilidad (tasa de error en -9FIT (error en función del tiempo) por hora) que se determinará a partir de la calificación de seguridad del sistema en el proceso de desarrollo.

Los sensores reducirán el porcentaje del valor de fiabilidad en función de la calidad de la captura de información correspondiente a la calidad máxima de reconocimiento.

Los calificadores son evaluados como información por el conductor según se indica a continuación:

Verde: según información segura no se prevén riesgos estacionarios en los próximos tramos.

Amarillo: el sistema no puede proporcionar información segura, de modo la conducción del vehículo depende únicamente del conductor.

Rojo: se ha detectado con certeza un riesgo en el próximo tramo, en caso de que el conductor no realice ninguna maniobra para evitarlo (como por ejemplo, accionar el acelerador o los frenos) el vehículo será frenado en un lapso determinado.

El sistema está definido de modo que el conductor circule bajo su responsabilidad en el área controlada, por ejemplo, un tramo de autopista vigilado y que además será advertido que debe retomar el control de la conducción cuando el sistema se lo advierta oportunamente. 1. Conducir a una velocidad fija. Un sistema externo (en este caso la central de control de tránsito) determina la velocidad.

2. El vehículo será acelerado hasta un máximo de 130 km/h por la central de control de tránsito cuando esta información segura esté disponible para el próximo tramo de autopista.

3. El vehículo será frenado como máximo hasta su detención por la central de control de tránsito en función de cierta información de la central de control de tránsito disponible.

Durante la conducción del vehículo a través de la central de control de tránsito, los sensores internos del vehículo sirven para vigilar el espacio en que se transita. En caso de que estos sensores detecten resultados inesperados (caída de una carga del vehículo que circula delante), objetos (presencia de personas o animales en la carretera), defectos estructurales de la carretera o relacionados con la posición (el vehículo sale de la carretera), entonces la gestión de la velocidad será controlada por la información segura a través de dichos sensores. El conductor podrá mediante el accionamiento intenso del freno o del acelerador, de todos los sistemas internos y externos recuperar activamente la gestión de la velocidad.

En la Figura 3 se muestra un sistema de bus para la transmisión de información conceptual relacionada con la seguridad. Todos los calificadores de diagnóstico se deben definir durante el desarrollo del sistema. Para todos los sistemas de comunicación se deben instrumentar las siguientes medidas. De este modo, las imágenes de error estándar necesarias para el diagnóstico estarán disponibles tanto para las comunicaciones por cable como para las inalámbricas.

Sobre la base del análisis de la seguridad de los datos para el sistema de bus interno del vehículo se deben definir más medidas referidas a la integridad de los datos (medidas de seguridad). En caso de que las medidas definidas anteriormente no sean suficientes como datos externos de la central de control de tránsito entonces se podrán integrar todos los calificadores de seguridad o los identificadores de los emisores a la formación del calificador de cobertura de diagnóstico. Es decir que el calificador de cobertura de diagnóstico solo se podrá generar cuando los sistemas de comunicación de las medidas necesarias para la seguridad de los datos también estén activos.

Una aclaración al respecto: Cuando sea necesario verificar los datos antes de iniciar una acción como por ejemplo, conducir, frenar, será difícil manipular los datos intencionalmente, porque se los debe manipular de dos maneras independiente, para que el efecto pase la prueba de plausibilidad.

Tan pronto esto se demore, podrá ser detectado por el calificador.

Una ventaja particular del sistema es que, solo el sistema que lleva el identificador decide respecto de la degradación relacionada con la seguridad y, por consiguiente, se pueden desactivar o incluso eliminar las vías de desconexión en los demás sistemas participantes. En la actualidad los sistemas subordinados se conectan sobre la base de sus propios diagnósticos. Mediante la desconexión o la simple omisión de la información de seguridad aumenta la disponibilidad del sistema general. Asimismo los sistemas autorreparables pueden, según su condición, reactivarse sin intervención del mecánico para las funciones de seguridad.

En la Figura 4 se muestra un diagrama de bloques del sistema. Las funciones del dispositivo de seguridad (ECU) comprenden por ejemplo:

recibir las señales de los sensores internos y externos que incluye sus calificadores de datos (datos de fiabilidad, calidad de señal y datos de diagnóstico específicos).

recepción de peticiones del conductor (que incluyen datos de diagnóstico pertinentes respecto de sistemas o componentes)

Control de los actuadores (MM, gestión del motor y BR frenos) a través de una entrada de control remoto definida de los respectivos actuadores.

Formación de los calificadores y vigilancia e iniciación del cambio del control primario (conducción del vehículo)

Registro del estado de calidad en una secuencia y registro de eventos por cada solicitud o transferencia del control primario.

Los componentes o sistemas externos deben suministrar los siguientes datos u otra información además de los datos de rendimiento:

Calidad cuantificada de la información de rendimiento relacionada con la seguridad (por ejemplo, la calidad de detección de los sensores expresada, por ejemplo, como porcentaje del rendimiento máximo)

La fiabilidad (tasa de error) específica de los sistemas o componentes sobre la base de la calificación de la seguridad durante el desarrollo. Como alternativa esta información puede estar almacenada en el dispositivo de control central (ECU). En razón de la integridad de los datos esta información también puede estar cifrada para evitar la manipulación de los datos externos.

El estado de diagnóstico actual, para el cual los valores pueden ser digitales (diagnóstico activo o positivo) también se pueden transferir como valor de la cobertura del diagnóstico. El nivel de cobertura de diagnóstico también se basa en los datos de calificación de seguridad durante el desarrollo del producto. También por razones de seguridad de los datos, estos datos se pueden cifrar o transferir firmados, para evitar la manipulación externa.

Los datos sobre calidad de señal, fiabilidad y cobertura de diagnóstico, se pueden cifrar o firmar individualmente o en bloque. Según el grado de interacción se pueden encapsular de 1 a 3 conjuntos de datos, de modo haya una interacción múltiple. La múltiple interacción de datos, que pueden estar almacenados o examinados en distintos lugares dificultará la manipulación voluntaria o involuntaria de los datos. Mediante la encapsulación se puede evitar la manipulación de los calificadores de seguridad o la adulteración de los datos y, por consiguiente, el sistema puede tomar decisiones más seguras.

En la Figura 5 se muestran las fases del dominio del vehículo (control primario). Por cada función automatizada del vehículo, el sistema debe asumir el dominio del (control primario).

Para ello se deben considerar las siguientes fases: - El conductor conduce el vehículo bajo su responsabilidad, los sistemas de asistencia le brindan apoyo, sin embargo no asumen nunca el control del vehículo.

Cambio del conductor al sistema: el conductor cede claramente el dominio del vehículo y el sistema está listo para asumir el control.

El sistema conduce el vehículo, el conductor vigila el sistema con reserva.

-Cambio del sistema al conductor: el sistema cede el dominio y el conductor lo recibe del sistema. En este caso podría ser que el conductor asuma directamente el dominio o por solicitud del sistema.

En la fase "El conductor conduce", el conductor es responsable del sistema. El sistema se encuentra en disponibilidad y comunica al conductor mediante diagnósticos adecuados su disposición para asumir el dominio del vehículo.

En la fase "Cambio del conductor al sistema" el conductor le hace saber al sistema que desea ceder el control primario. Él se ha cerciorado de que se encuentra en una situación de manejo en que esto es posible y de que no es peligroso ceder el dominio del vehículo al sistema. El sistema inicializa los sistemas pertinentes para asumir el dominio del vehículo y activa las funciones correspondientes. Una vez que el sistema asume completamente el control primario, comunica la situación al conductor.

En la fase "El sistema conduce" el sistema tiene el control primario de la función definida. El conductor debe vigilar el vehículo, las condiciones de manejo y el sistema; el conductor puede en cualquier momento en un intervalo adecuado recuperar el dominio sobre el vehículo. En la fase "Cambio del sistema al conductor" el sistema puede comunicar la intención del ceder el control primario, o bien, el conductor puede retirar el control primario del sistema.

Aquí se produce nuevamente la división entre la fase "El sistema cede el control primario" y la fase "El conductor retira el control primario al sistema“.

En la fase "El sistema cederá el control primario" el sistema reconoce a una distancia segura que el control primario ya no será seguro (por ejemplo, fin de la autopista). El sistema está diseñado de modo que esta información sea recibida por el conductor con suficiente antelación (por ejemplo, 30 segundos). El escenario debe aplicarse en consecuencia cuando el diagnóstico del sistema detecta una falla, que la seguridad del sistema del control no puede

manejar de forma segura. En caso que el período de advertencia se defina en 30 segundos, entonces el sistema se debe configurar de modo que pueda conservar el dominio del vehículo de forma suficientemente segura en ese lapso. Esto se puede garantizar mediante un adecuado diseño de tolerancia a las fallas del sistema.

Para ejecutar la fase "El conductor retira el control primario al sistema", el sistema está configurado de modo que el conductor pueda recuperar el control primario intuitivamente en cualquier momento. El sistema debe pasar de inmediato al modo de supervisión cuando el conductor recupera claramente el control primario.

El sistema reconoce a una distancia suficiente que el control primario ya no será seguro (por ejemplo, fin de la autopista). El sistema está diseñado de modo que esta información sea recibida por el conductor con suficiente antelación, por ejemplo, 30 segundos. El escenario debe aplicarse en consecuencia cuando el diagnóstico del sistema detecta una falla, que la seguridad del sistema del control no puede manejar de forma segura. En caso que el período de advertencia se defina en 30 segundos, entonces el sistema se debe configurar de modo que pueda conservar el dominio del vehículo de forma suficientemente segura en ese lapso. Esto se puede garantizar mediante un adecuado diseño de tolerancia a las fallas del sistema.

El sistema ha configurado el control primario para la función definida. El conductor debe vigilar el vehículo, las condiciones de manejo y el sistema; el conductor puede en cualquier momento en un intervalo adecuado recuperar el dominio sobre el vehículo. Así funciona el calificador de seguridad como documentación archivada en línea y queda documentado el cambio de control primario. Lista de referencia

Sistema general

Primer vehículo

Sistema de comunicación

Unidad de control (ECU)

Unidad funcional

Primera unidad de comunicación

Segunda unidad de comunicación

Tercera unidad de comunicación

Canal de comunicación

Canal de comunicación

Canal de comunicación

Primera unidad de medición

Segunda unidad de medición

Segundo vehículo

Tercer vehículo

Almacenamiento

Emisor de señal

DC Nivel de cobertura de diagnóstico SPFM Métrica de error único LFM Métrica de error latente

PMHF Tasa de error para evento principal

ASIL Nivel de integridad de la seguridad automotriz

REIVINDICACIONES

1. Un método para realizar una función de seguridad en un vehículo (2), en donde los datos necesarios para ejecutar la función de seguridad se transmiten a una unidad de control (4) de un vehículo (2) mediante al menos un sistema de comunicación (3) en donde las señales de control son generadas por la unidad de control (4) como una función de los datos transmitidos y se transmiten a una unidad funcional (5) del vehículo (2) en donde la función de seguridad es ejecutadas por la unidad funcional (5) como una función de las señales de control, en donde las pruebas de diagnóstico son ejecutadas repetidamente a intervalos de tiempo, en donde las pruebas de diagnóstico comprueban la existencia de una falla o avería que podría afectar adversamente a la ejecución de la función de seguridad en uno o más de los sistemas eléctricos, electrónicos y/o programables (3-13) utilizados para ejecutar el método, caracterizado porque los metadatos de los datos transmitidos contienen información sobre los sistemas empleados para ejecutar el método, en donde al menos un valor de fiabilidad de los datos es determinado por la unidad de control (4) utilizando esta información cuyo valor depende

de la probabilidad de que ocurran fallas o averías que afecten adversamente a la ejecución de la función de seguridad y

de la probabilidad de que la existencia de estas fallas o averías sea detectada por las pruebas de diagnóstico y/o por un conductor del vehículo (2) oportunamente antes de que la función de seguridad resulte adversamente afectada, en donde la unidad de control (4) verifica, como una función de al menos un valor de fiabilidad, si los datos transmitidos son confiables para ejecutar la función de seguridad.

2. El método de acuerdo con la reivindicación 1, caracterizado porque si los datos necesarios para ejecutar la función de seguridad no están totalmente disponibles o no son confiables,

los datos transmitidos a la unidad de control (4) no se usan para accionar la unidad funcional (5) y/o

se envía una señal de desactivación a la unidad funcional (5) por medio de la unidad de control (4) en donde, una vez recibida esta señal de desactivación, la unidad funcional ingresa automáticamente en un modo de seguridad en donde no se puede ejecutar la función de seguridad y/o

los datos se transmiten a la unidad de control (4) nuevamente después de un tiempo de espera predefinido, en donde los datos se transmiten de esta manera frecuentemente a la unidad de control (4) hasta que los datos estén totalmente disponibles y sean suficientemente confiables.

3. El método de acuerdo de una de las reivindicaciones precedentes caracterizado porque mediante la unidad de control (4) un generador de señales del vehículo (2) se acciona para indicar al conductor si los datos necesarios para ejecutar la función de seguridad están totalmente disponibles y son confiables.

4. El método de acuerdo con una de las reivindicaciones precedentes, caracterizado porque si los datos necesarios para ejecutar la función de seguridad no están totalmente disponibles o son confiables, se acciona mediante la unidad de control (4) el generador de señales (17) para indicar al conductor la falta de disponibilidad momentánea de la función de seguridad.

5. Método de acuerdo con una de las reivindicaciones precedentes caracterizado porque los datos se producen como una función de las señales de medición de al menos una unidad de medición (12, 13).

6. Un Método de acuerdo con una de las reivindicaciones precedentes caracterizado porque al menos un valor de fiabilidad se determina como una función de al menos una de las tasas de error l_{SPF}, l_{RF}, l_{MPF}, $l_{MPF,L}$, $l_{MPF,P}$, $l_{MPF,D}$, en donde cada una de estas tasas de error especifica la cantidad de fallas que ocurren en una unidad de tiempo en un sistema eléctrico, electrónico y/o programable (3-13) que se usa para ejecutar el método en donde las tasas de error respectivas se relacionan cada una exclusivamente con los siguientes tipos de fallas:

l_{SPF}:fallas que, aun cuando se produzcan individualmente, pueden afectar adversamente a la ejecución de la función de seguridad y cuya existencia no es verificada por las pruebas de diagnóstico y, por consiguiente, tampoco puede ser detectada oportunamente por las pruebas de diagnóstico antes de que la función de seguridad sea negativamente afectada;

l_{PF}: fallas que, aun cuando se produzcan individualmente, pueden afectar adversamente a la ejecución de la función de seguridad y cuya existencia es verificada por las pruebas de diagnóstico pero no es detectada por las pruebas de diagnóstico oportunamente antes de que la función de seguridad sea negativamente afectada;

$l_{MPF,L}$: fallas que, cuando se producen o existen al mismo tiempo que otras fallas, pueden afectar adversamente a la ejecución de la función de seguridad y cuya existencia no es verificada por las pruebas de diagnóstico;

$l_{MPF,D}$: fallas que, cuando se producen o existen al mismo tiempo que otras fallas, pueden afectar negativamente la ejecución de la función de seguridad y cuya existencia es verificada y detectada por las pruebas de diagnóstico oportunamente antes de que la función de seguridad sea adversamente afectada;

$l_{MPF,P}$: fallas que cuando se producen o existen al mismo tiempo que otras fallas, pueden afectar adversamente a la ejecución de la función de seguridad y cuya existencia es detectada oportunamente por el conductor del vehículo (2).

7. El método de acuerdo con la reivindicación 6 caracterizado porque al menos un valor de fiabilidad de al menos un valor de fiabilidad de los datos se determina como una función de al menos un valor de DCRF de cobertura de diagnóstico de acuerdo con la norma ISO 26262.

$$DC_{RF} = \left(1 - \frac{\lambda_{RF}}{\lambda}\right) \times 100$$

de al menos uno de los sistemas eléctricos, electrónicos y/o programables utilizado para realizar el método en donde 1 es especificado para este sistema (3-13) por l_{SPF}+ l_{RF} + $l_{MPF,L}$ + $l_{MPF,D}$ + $l_{MPF,P}$, e l_S es la tasa de error para la existencia de cualquier falla en este sistema (3-13).

8. El método de acuerdo con la reivindicación 6 o 7 caracterizado porque al menos un valor de fiabilidad de al menos un valor de fiabilidad de los datos se determina como una función de al menos un valor de la métrica $M_{SPF,RF}$ de acuerdo con la norma ISO 26262.

$$M_{SPF,RF} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{SPF} + \lambda_{RF})}{\sum_{\text{safety-related HW elements}} \lambda}$$

en donde la sumatoria está compuesta por una pluralidad de sistemas eléctricos, eléctricos y programables (3-13) que se usan durante el método y en donde pueden producirse fallas que, por sí solas o combinadas entre sí, pueden afectar adversamente a la ejecución de la función de seguridad, en donde 1 está especificado por este sistema (3-13) por l_{SPF} + l_{RF} + $l_{MPF,L}$ + $l_{MPF,D}$ + $l_{MPF,P}$ e l_S es la tasa de error para la existencia de cualquier falla en este sistema (3-13).

9. El método de acuerdo con una de las reivindicaciones 6 a 8 caracterizado porque los metadatos ya fueron transmitidos a la unidad de control (4) durante la puesta en marcha del vehículo (2), en particular antes de iniciar un viaje, en donde al menos un valor de fiabilidad de al menos uno de los valores de fiabilidad de los datos se determina como una función del valor de la cobertura de diagnóstico $DC_{MPF,L}$ de acuerdo con la norma ISO 26262

$$DC_{MPF,L} = \left(1 - \frac{\lambda_{MPF,L}}{\lambda}\right) \times 100$$

de al menos de uno de los sistemas eléctricos, electrónicos y/o programables que se usa para ejecutar el método, en donde la función de seguridad se ejecuta únicamente con la condición adicional de que este valor de fiabilidad que se determina durante el proceso sea mayor que un valor de umbral predefinido, donde 1 es especificado para el sistema (3-13) por l_{SPF} + l_{RF} + $l_{MPF,L}$ + $l_{MPF,D}$ + $l_{MPF,P}$ e l_S es la tasa de error para la existencia de cualquier falla en este sistema (3-13).

10. El método de acuerdo con una de las reivindicaciones 6 a 9 caracterizado porque los metadatos ya fueron transmitidos a la unidad de control (4) durante el proceso de puesta en marcha del vehículo (2), en particular antes de iniciar un viaje, en donde al menos un valor de fiabilidad de al menos uno de los valores de fiabilidad de los datos se determina como una función del valor de la métrica $M_{MPF,L}$ de acuerdo con la norma ISO 26262

$$M_{MPF,L} = 1 - \frac{\sum_{\text{safety-related HW elements}} (\lambda_{MPF,L})}{\sum_{\text{safety-related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

en donde la sumatoria se forma con una pluralidad de sistemas eléctricos, electrónicos y/o programables que se usa durante la realización del método y en donde puede ocurrir una falla que puede afectar negativamente a la ejecución de la función de seguridad, en donde la función de seguridad se ejecuta únicamente con la condición adicional de que este valor de fiabilidad sea mayor que un valor de umbral predefinido, donde 1 es especificado para este sistema (3-13) por $\lambda_{SPF} + \lambda_{RF} + \lambda_{MPF,L} + \lambda_{MPF,D} + \lambda_{MPF,P}$, e ls es la tasa de error para la existencia de cualquier falla en este sistema (3-13).

11. El método de acuerdo con una de las reivindicaciones precedentes caracterizado porque la unidad funcional (5) es un dispositivo de protección activo o pasivo del vehículo (2) caracterizado porque:

la unidad funcional (5) es un sistema de freno electrónico y la función de seguridad es un potenciador de freno automático y/o en donde la unidad funcional (5) es un asistente de freno de emergencia y la función de seguridad es una operación de freno total o parcial del vehículo (2) que se acciona automáticamente y/o en donde la unidad funcional (5) es un asistente de evasión y la función de seguridad es una acción de manejo automática para eludir un obstáculo y/o

la unidad funcional (5) es una unidad ESC y la función de seguridad consiste en estabilizar automáticamente del vehículo (2), en particular mediante el frenado de una o más ruedas del vehículo (2) y/o acelerando el motor del vehículo (2) y/o en donde

-la unidad funcional (5) es un sistema de airbag y la función de seguridad es la activación del airbag.

12. Un sistema general (1) para ejecutar una función de seguridad en un vehículo (2) que comprende el vehículo y un sistema de comunicación que está configurado para transmitir datos que son necesarios para ejecutar la función de seguridad a una unidad de control (4) del vehículo (2), en donde la unidad de control (4) está configurada para generar señales de control como una función de los datos transmitidos y para transmitir dichas señales de control a una unidad funcional (5) del vehículo (2) en donde la unidad funcional (5) está configurada para realizar pruebas de diagnóstico repetidamente a intervalos de tiempo para verificar la existencia de una falla o desperfecto que podría afectar adversamente a la ejecución de la función de seguridad en uno o más sistemas eléctricos, electrónicos y/o programables del sistema general caracterizado porque el sistema de comunicación también está configurado para transmitir metadatos de los datos a la unidad de control (4), en donde los metadatos contienen información de los sistemas especificado del sistema general, en donde la unidad control (4) está configurada para determinar al menos un valor de fiabilidad de los datos mediante la unidad de control (4) y como una función de esta información, dicho valor de fiabilidad depende de la probabilidad de la existencia de fallas que podrían afectar adversamente a la ejecución de la función y- de la probabilidad de que la existencia de estas fallas sea detectada por las pruebas de diagnóstico y/o por un conductor del vehículo (2) oportunamente antes de que la función de seguridad resulte negativamente afectada y para verificar como una función de al menos un valor de fiabilidad que los datos transmitidos son confiables para ejecutar la función de seguridad.

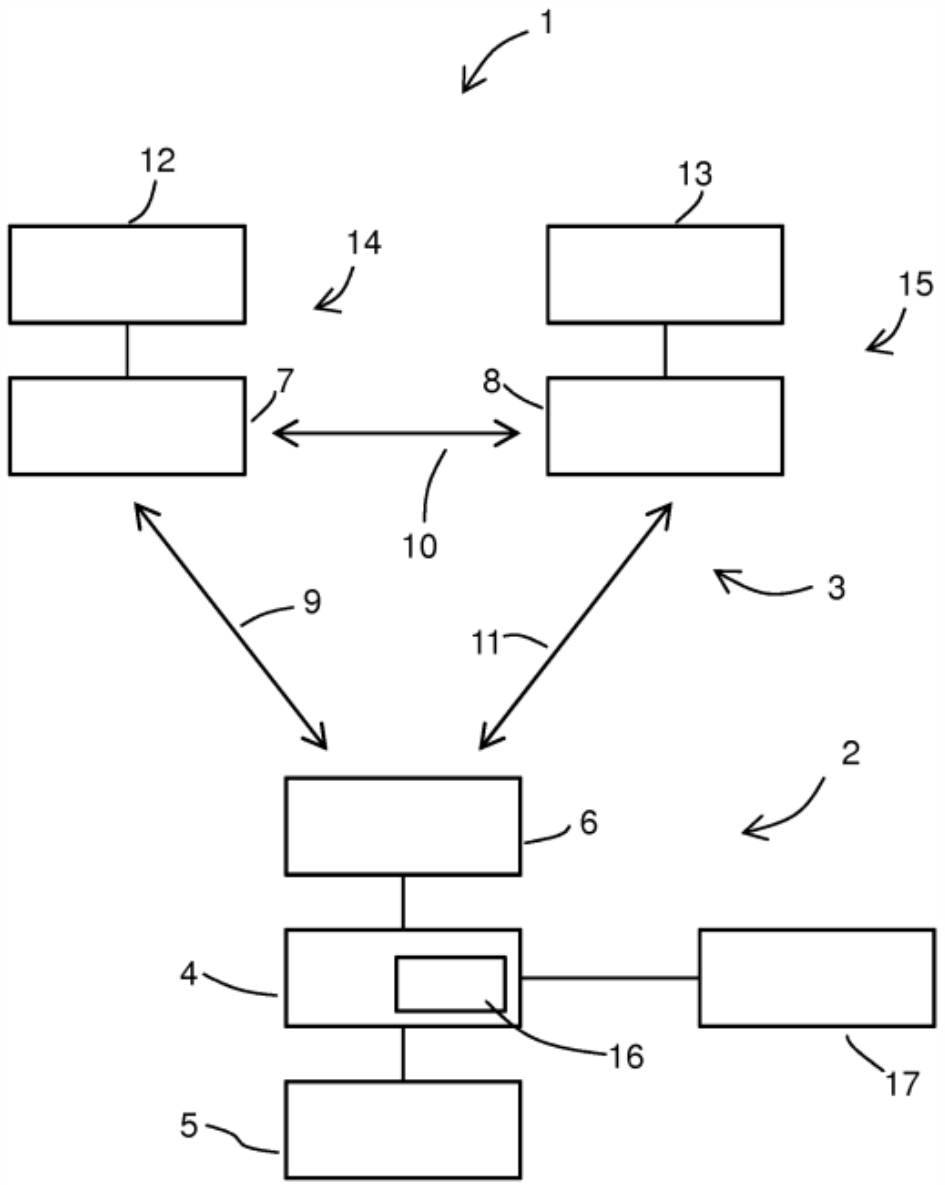


Fig. 1

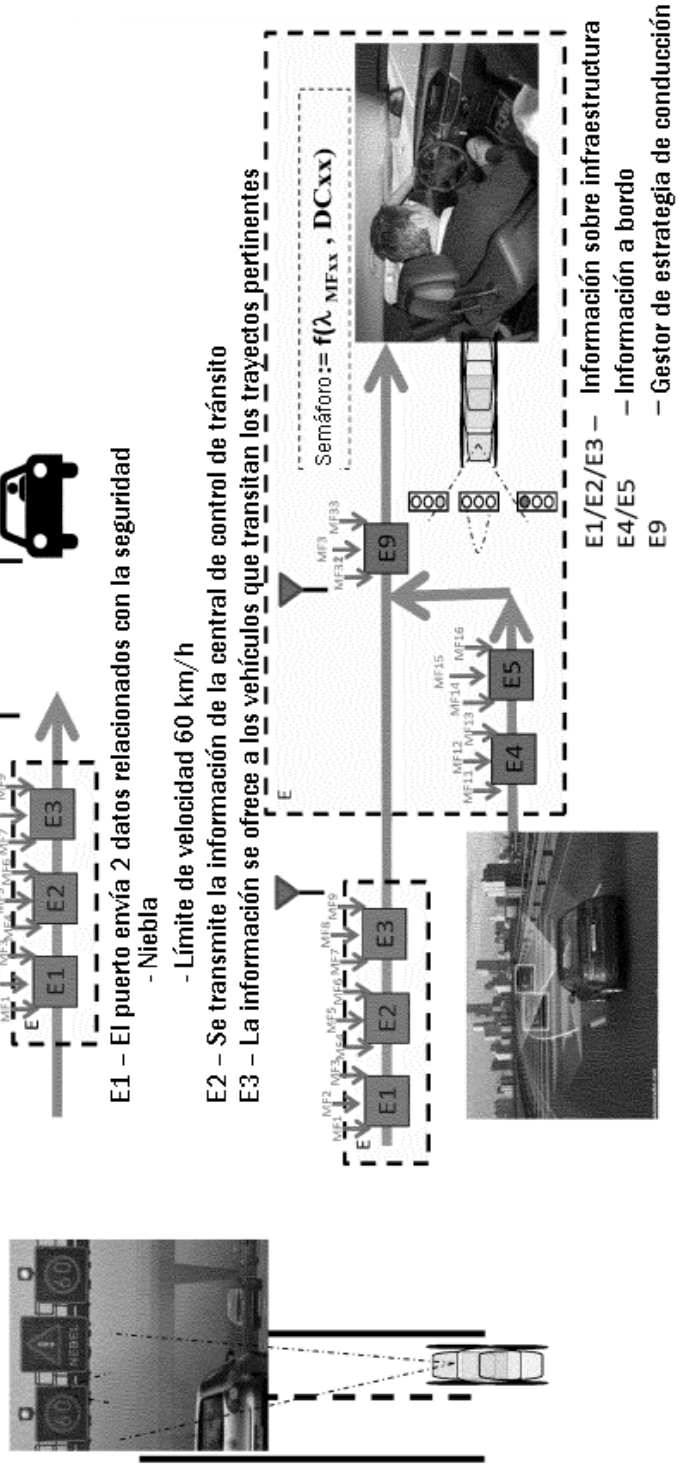
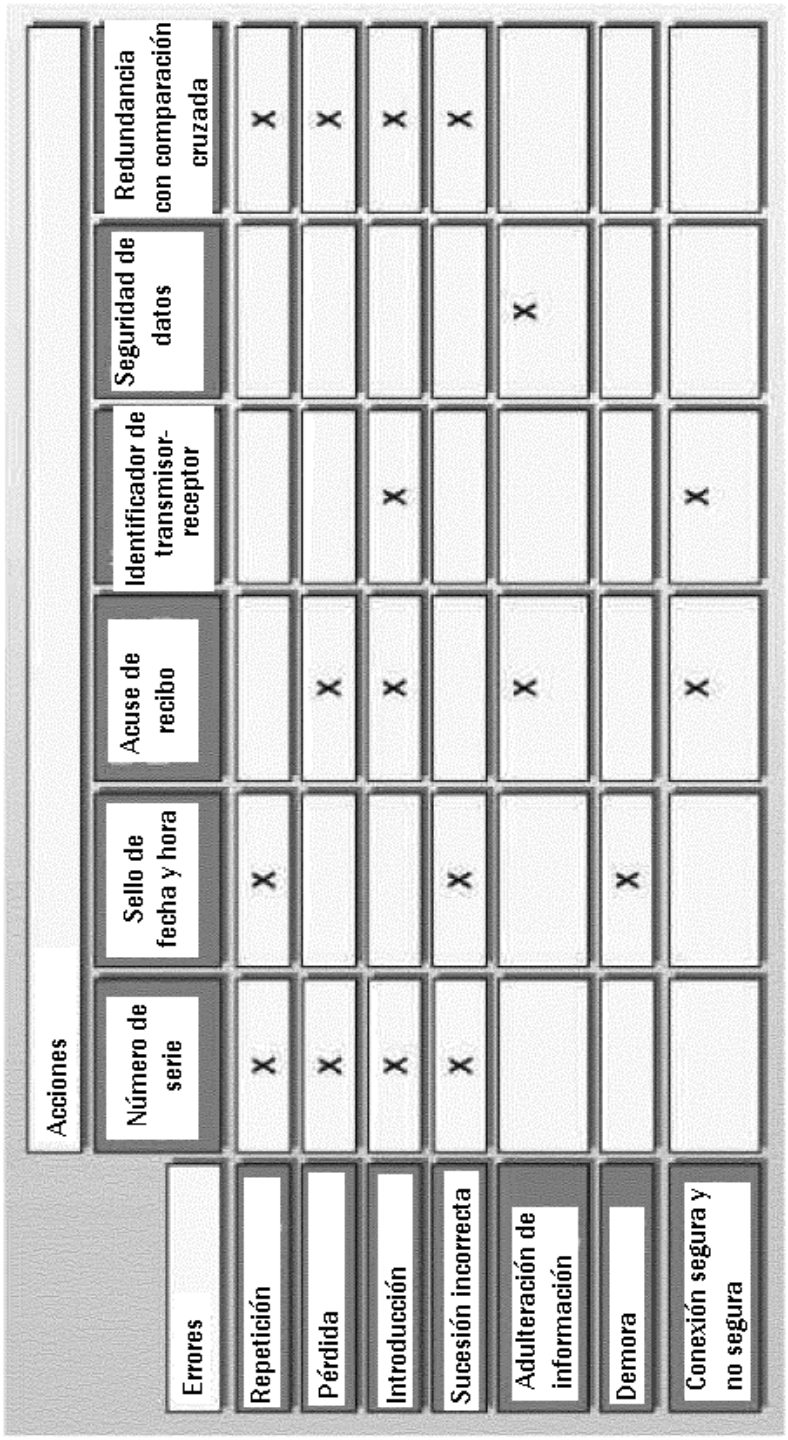

E1 – El puerto envía 2 datos relacionados con la seguridad
- Niebla
- Límite de velocidad 60 km/h
E2 – Se transmite la información de la central de control de tránsito
E3 – La información se ofrece a los vehículos que transitan los trayectos pertinentes
Semáforo := f(λ MFxx , DCxx)
E1/E2/E3 – Información sobre infraestructura
E4/E5 – Información a bordo
E9 – Gestor de estrategia de conducción

FIG. 2



Errores	Acciones						
	Número de serie	Sello de fecha y hora	Acuse de recibo	Identificador de transmisor-receptor	Seguridad de datos	Redundancia con comparación cruzada
Repetición	X	X				X
Pérdida	X		X			X
Introducción	X		X	X		X
Sucesión incorrecta	X	X				X
Adulteración de información			X		X	
Demora		X				
Conexión segura y no segura			X	X		

FIG. 3

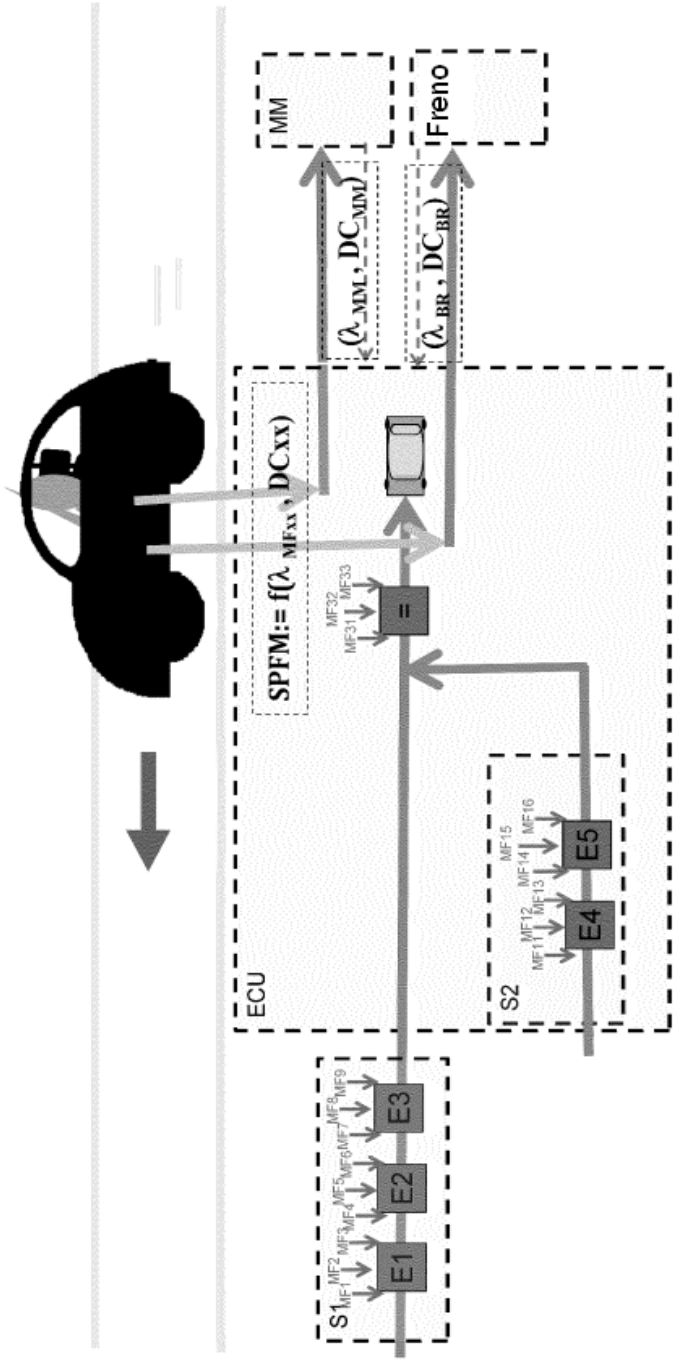

MM
Freno
(λ_{MM}, DC_{MM})
(λ_{BR}, DC_{BR})
SPFM:= $f(\lambda_{MFxx}, DCxx)$
ECU
=
MF32
MF31
MF33
S1
S2
E1
E2
E3
E4
E5
MF1
MF2
MF3
MF4
MF5
MF6
MF7
MF8
MF9
MF11
MF12
MF13
MF14
MF15
MF16

FIG. 4

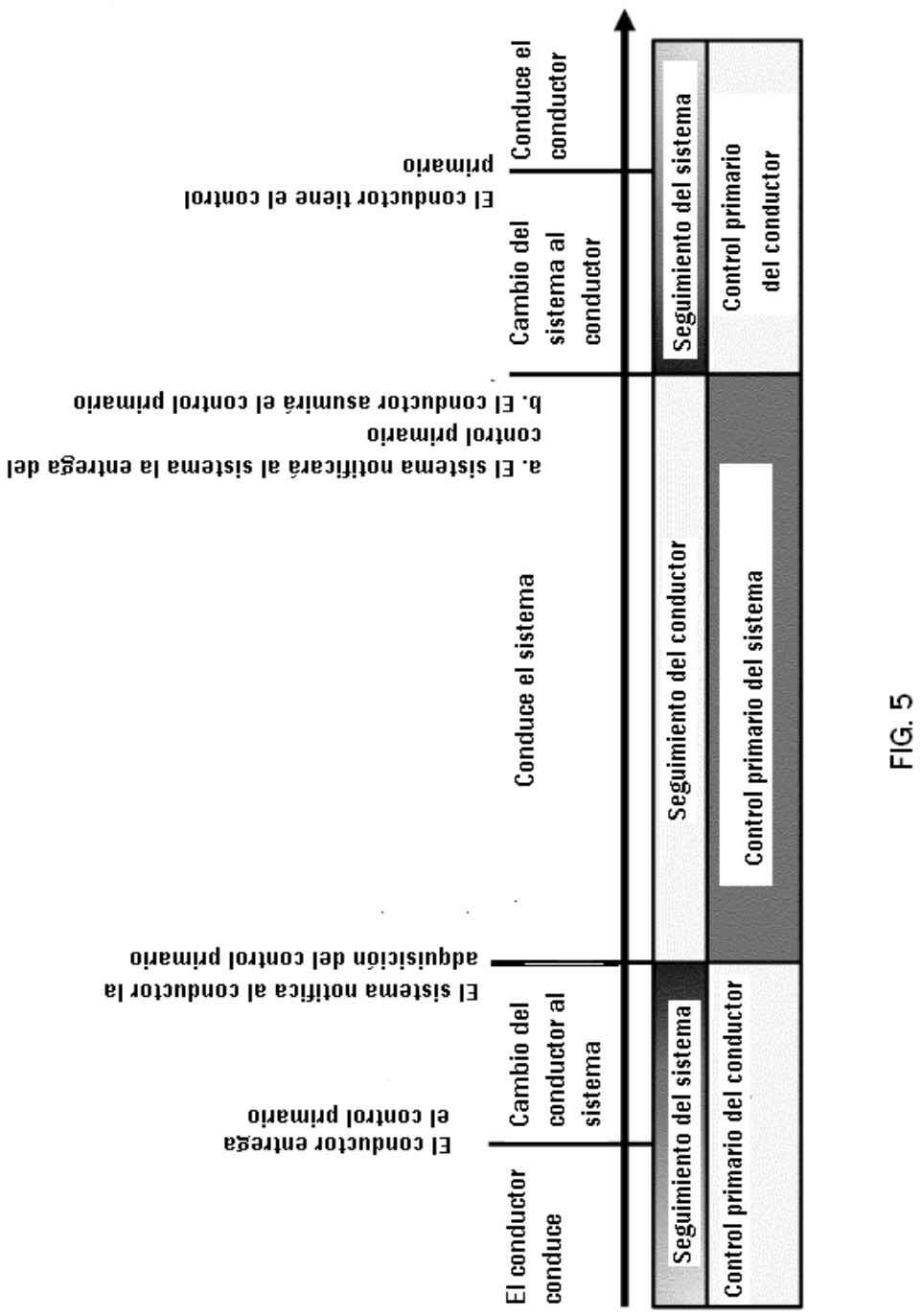

El conductor conduce
El conductor entrega el control primario
Cambio del conductor al sistema
El sistema notifica al conductor la adquisición del control primario
Conduce el sistema
a. El sistema notificará al sistema la entrega del control primario
b. El conductor asumirá el control primario
Cambio del sistema al conductor
El conductor tiene el control primario
Conduce el conductor
Seguimiento del sistema
Control primario del conductor
Seguimiento del conductor
Control primario del sistema
Seguimiento del sistema
Control primario del conductor

FIG. 5