(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
13 octobre 2016 (13.10.2016)

WIPO | PCT

(10) Numéro de publication internationale
WO 2016/162624 A1

(51) Classification internationale des brevets :
B60W 50/02 (2012.01) *B60W 50/00* (2006.01)
B60W 50/029 (2012.01)

(21) Numéro de la demande internationale :
PCT/FR2016/050768

(22) Date de dépôt international :
5 avril 2016 (05.04.2016)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1552961 7 avril 2015 (07.04.2015) FR

(71) Déposant : **VALEO EQUIPEMENTS ELECTRIQUES MOTEUR** [FR/FR]; 2 rue André Boulle, 94046 Creteil Cedex (FR).

(72) Inventeurs : **DEGOUL, Paul**; 5 rue Victor Considérant, 75014 Paris (FR). **LEEMAN, Michel**; 10 rue Laurence Savart, 75020 Paris (FR).

(74) Mandataire : **MARTIN, Joaquim**; Valeo Equipements Electriques Moteur, 2 rue André Boulle, 94046 Creteil Cedex (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : 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, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (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).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

(54) **Title** : METHOD FOR IMPLEMENTING A MOTOR VEHICLE FUNCTION IN ACCORDANCE WITH STANDARD ASIL LEVELS, CORRESPONDING SYSTEM, AND MOTOR VEHICLE INCLUDING SUCH A SYSTEM

(54) **Titre** : PROCÉDÉ D'IMPLÉMENTATION D'UNE FONCTION D'UN VÉHICULE AUTOMOBILE CONFORME A DES NIVEAUX ASIL STANDARDS, SYSTÈME CORRESPONDANT ET VÉHICULE AUTOMOBILE COMPRENANT UN TEL SYSTÈME

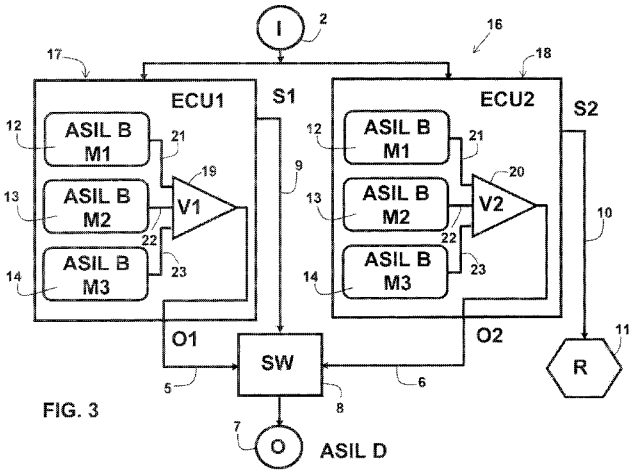

FIG. 3

(57) **Abstract** : The invention relates to a method which makes it possible to implement a motor vehicle function in accordance with standard ASIL levels corresponding to increasing safety requirement levels QM, A, B, C, and D, such as those defined by the ISO 26262 standard. The method implements said function using a first safety requirement level by at least means (12, 13, 14) having a second safety requirement level that is lower than said first safety requirement level. In accordance with the invention, for a design variant with less than four means (12, 13, 14), the first safety requirement level is rated D or C and the second safety requirement level is rated B, A or QM.

(57) **Abrégé** :

[Suite sur la page suivante]

WO 2016/162624 A1

Le procédé selon l'invention autorise l'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards correspondant à des niveaux d'exigence en termes de sécurité croissants QM, A, B, C, D tels que ceux définis par la norme ISO 26262. Le procédé est du type de ceux implémentant cette fonction avec un premier niveau d'exigence en termes de sécurité par au moins des moyens (12, 13, 14) présentant un second niveau d'exigence en termes de sécurité inférieur audit premier niveau d'exigence en termes de sécurité. Conformément à l'invention, le premier niveau d'exigence en termes de sécurité est coté D ou C et le second niveau d'exigence en termes de sécurité est coté B, A ou QM pour une diversité de conception des moyens (12, 13, 14) inférieure à quatre.

PROCEDE D'IMPLEMENTATION D'UNE FONCTION D'UN VEHICULE AUTOMOBILE CONFORME A DES NIVEAUX ASIL STANDARDS, SYSTEME CORRESPONDANT ET VEHICULE AUTOMOBILE COMPRENANT UN TEL SYSTEME

DOMAINE TECHNIQUE DE L'INVENTION.

La présente invention concerne un procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards ("Automotive Security Integrity Level" en terminologie anglaise, c'est-à-dire "Niveau d'exigence en termes de Sécurité en Automobile").

L'invention concerne également un système apte à la mise en œuvre de ce procédé, ainsi que le véhicule automobile comprenant ce système.

ARRIERE PLAN TECHNOLOGIQUE DE L'INVENTION.

Le développement récent des véhicules autonomes (niveaux d'automatisation 4 et 5 tels que définis par la Société des Ingénieurs de l'Automobile (SAE, acronyme de "Society of Automotive Engineers") requiert des systèmes opérationnels après défaillance ("fail operational") au lieu des systèmes classiques dans les applications critiques en termes de sécurité dans l'automobile qui ne requièrent que des systèmes passifs après défaillance ("fail silent").

Un système opérationnel après défaillance maintient sa fonctionnalité ou au moins une fonctionnalité réduite dans le cas d'une défaillance simple quelconque.

Un système opérationnel après défaillance nécessite un bus de données et des alimentations redondants ainsi qu'une unité de calcul électronique (ECU ou "Electronique Computing Unit" en terminologie anglaise) redondante.

Une architecture matérielle possible pour réaliser une unité de calcul électronique opérationnelle après défaillance est connue en tant qu'architecture Duplex - Double, et son utilisation est courante en avionique.

Une architecture Duplex- Double peut être constituée par deux ECU passives après défaillance classiques en automobile et un commutateur, comme le montre la **Figure 1**.

Les deux ECUs peuvent être basées par exemple sur l'utilisation d'un microcontrôleur à double cœur synchrone dit LSDC (acronyme de "Lock Step Dual Core" en terminologie anglaise). Quand un statut de la première unité de calcul électronique est fonctionnel, les données de sortie sont celles fournies par la

première unité de calcul électronique. Quand le statut de la première unité de calcul électronique est non-fonctionnel, c'est-à-dire qu'elle est en défaillance, les données de sortie sont celles fournies par la seconde unité de calcul électronique. Le statut de la seconde unité de calcul électronique est utilisé pour rapporter les erreurs cachées, quand elle n'est pas opérationnelle, et qu'elle n'est plus capable de prendre le relais en .cas de défaillance de la première unité de calcul électronique. Dans le cas de données de sortie multiples, le commutateur est un réseau de commutateurs.

En ce qui concerne le logiciel, le standard ISO 26262 établit un cadre formel pour la sécurité fonctionnelle des modules dans l'automobile. La norme ISO 26262 stipule que la sécurité (« safety » en anglais) du logiciel doit être prise en compte de manière systématique pendant tout le cycle de développement du logiciel.

Un ASIL est attribué sur la base du risque de l'occurrence d'un évènement dangereux en prenant en compte la périodicité de la situation, l'impact d'un dommage éventuel, et dans quelle mesure cette situation peut être contrôlée et gérée.

La norme ISO 26262 définit quatre ASIL indiqués par des lettres de A à D, cette dernière correspondant au risque le plus faible et au niveau d'exigence en termes de sécurité le plus élevé. Un niveau d'exigence en termes de sécurité indiqué par QM ("Qualité Management" c'est-à-dire "Gestion de la Qualité") est assigné aux fonctions non- critiques.

Beaucoup de fonctions de véhicules autonomes auront au moins deux contraintes de sécurité ASIL D contradictoires. D'une part, une décision erronée sera ASIL D, et, d'autre part, la perte de la fonction sera aussi ASIL D.

Pour satisfaire une décision correcte au niveau ASIL D, l'implémentation de la fonction dans les deux ECUs requerra soit que le logiciel soit développé au niveau ASIL D, soit requerra une décomposition ASIL, telle que définie dans la norme ISO 26262. Dans le cas d'une décomposition ASIL, deux modules redondants développés à un niveau inférieur de criticité peuvent être implémentés dans les deux ECUs. Développer un logiciel d'application complexe au niveau ASIL D n'est pas la stratégie généralement retenue dans un développement industriel automobile, pour des raisons de coût et de durée de développement. Par conséquent, une décomposition ASIL conduisant à des ASILs inférieurs sera préférée au moins pour les logiciels d'applications. Cependant, une décomposition ASIL nécessite une implémentation redondante et diversifiée. Dans ces conditions,

quelle que soit l'architecture matérielle choisie pour réaliser les unités de calcul électroniques passives après défaillance, deux algorithmes différents seront nécessaires de façon à assurer l'indépendance entre les deux modules redondants implémentés dans chaque ECU, sinon la décomposition ASIL pour réduire l'ASIL n'est pas autorisée par la norme ISO 26262.

En outre pour satisfaire à la contrainte de disponibilité en cas de défaillance simple, les modules logiciels implémentés dans chacune des unités de calcul électroniques d'une architecture Duplex-Double doivent aussi présenter une diversité.

Si ce n'était pas le cas, une erreur systématique affectant l'un des deux algorithmes redondants dans l'une des deux ECUs passives après défaillance affecterait aussi l'autre ECU. Si cette erreur était activée sur l'une des ECU, elle serait activée simultanément sur l'autre, car les données d'entrée des deux ECUs sont les mêmes, et par conséquent, les deux ECUs défailliraient simultanément, ne satisfaisant pas de ce fait la contrainte de disponibilité. Etant donné que la raison fondamentale de la défaillance est une erreur d'un logiciel de plus faible ASIL, cela n'est pas acceptable.

Cela signifie que pour une fonction soumise à deux contraintes de sécurité contradictoires ASIL D (ou C), l'une portant sur la validité des données de sortie, et l'autre sur la disponibilité de ces données de sortie, quand une architecture Duplex-Double est utilisée, quatre modules logiciels différents seront nécessaires comme le montre la **Figure 2**. Mais dans de nombreux cas, il n'est pas possible de satisfaire à la condition de diversité logicielle, c'est-à-dire qu'il n'est pas possible de trouver quatre algorithmes différents pour une même fonction.

Il est évidemment plus facile de développer un système, ou un sous-système, qualifié en tant qu'ASIL B plutôt qu'ASIL D.

Par conséquent, des incitations de coût et d'ordre pragmatique conduisent à situer tout ou partie d'un projet à un niveau le plus bas possible dans l'échelle des ASIL, tout en visant une qualification globale la plus haute possible.

Par exemple, la demande brevet US20150057908 décrit une unité de contrôle moteur remplissant des fonctions de sécurité qualifiée à un niveau ASIL B au moyen d'un microcontrôleur qualifié à un niveau ASIL B et d'un circuit intégré qualifié à un niveau QM.

La décomposition ASIL exposée dans cette demande, ne semble pas pouvoir être transposée à une architecture Duplex-Double, telle que décrite ci-dessus,

devant être qualifiée à un niveau ASIL D ou ASIL C.

Il existe donc un besoin pour une solution technique permettant de qualifier cette architecture à ces niveaux ASIL élevés en utilisant une implémentation qualifiée à un niveau inférieur, tout en limitant la diversité de conception.

DESCRIPTION GENERALE DE L'INVENTION.

La présente invention vise par conséquent à satisfaire ce besoin.

Elle a précisément pour objet un procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards correspondant à des niveaux d'exigence en termes de sécurité croissants QM, A, B, C, D tels que ceux définis par la norme ISO 26262.

Le procédé dont il s'agit est du type de ceux implémentant cette fonction avec un premier niveau d'exigence en termes de sécurité par au moins des moyens présentant un second niveau d'exigence en termes de sécurité inférieur au premier niveau d'exigence en termes de sécurité pour une diversité de conception de ces moyens inférieure à quatre.

Selon l'invention, ce premier niveau d'exigence en termes de sécurité est coté D ou C et le second niveau d'exigence en termes de sécurité est coté B, A ou QM,

Cette fonction est réalisée, selon l'invention, en parallèle à partir d'au moins une donnée d'entrée par des première et seconde unités électroniques de calcul passives après défaillance générant respectivement au moins des première et seconde données de sortie constituant alternativement au moins une donnée de sortie nominale de la fonction selon un état des première et seconde unités électroniques de calcul.

Dans un premier mode de réalisation de l'invention, les première et seconde unités électroniques de calcul exécutent chacune un ensemble identique de trois modules logiciels différents réalisant cette fonction et générant les première et seconde données de sortie par l'intermédiaire de premier et second voteurs majoritaires, le second niveau d'exigence en termes de sécurité d'au moins un des trois modules étant inférieur de deux degrés au premier niveau d'exigence en termes de sécurité.

Dans un deuxième mode de réalisation de l'invention, les première et seconde unités électroniques de calcul exécutent respectivement, d'une part, un premier et un deuxième modules, et, d'autre part, le deuxième et un troisième

modules parmi un ensemble de trois modules différents réalisant cette fonction et générant les première et seconde données de sortie par l'intermédiaire de premier et second voteurs majoritaires prenant en compte des première, deuxième et troisième sorties intermédiaires générées respectivement par les premier, deuxième et troisième modules, le second niveau d'exigence en termes de sécurité d'au moins un des premier, deuxième et troisième modules étant inférieur de deux degrés au premier niveau d'exigence en termes de sécurité.

Dans un troisième mode de réalisation de l'invention, des première et seconde unités électroniques de calcul exécutent chacune un premier module identique ayant une cotation ASIL D et, respectivement, des deuxième et troisième modules différents ayant une autre cotation ASIL QM.

L'invention concerne également un système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards correspondant à des niveaux d'exigence en termes de sécurité croissants QM, A, B, C, D tels que ceux définis par la norme ISO 26262, apte à la mise œuvre du procédé exposé ci-dessus.

Ce système est du type de ceux implémentant cette fonction avec un premier niveau d'exigence en termes de sécurité et comprenant au moins une première unité de calcul électronique, des moyens d'acquisition d'une donnée d'entrée de la fonction et des moyens de génération d'au moins une première donnée de sortie de la fonction présentant un second niveau d'exigence en termes de sécurité inférieur au premier niveau d'exigence en termes de sécurité.

Dans le système selon l'invention, le premier niveau d'exigence en termes de sécurité est coté D ou C et le second niveau d'exigence en termes de sécurité est coté B, A ou QM pour une diversité de conception de ces moyens de génération inférieure à quatre.

Selon l'invention, ce système comprend en outre une seconde unité de calcul électronique générant au moins une seconde donnée de sortie de la fonction, et des moyens de commutation pour produire au moins une donnée de sortie nominale en commutant la première donnée de sortie ou la seconde donnée de sortie selon un état des première et seconde unités électroniques de calcul, ces première et seconde unités électroniques de calcul étant passives après défaillance.

Dans le premier mode de réalisation de l'invention, le système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards comprend en outre un ensemble identique de trois modules

différents réalisant cette fonction exécutés par chacune des première et seconde unités électroniques de calcul, et des premier et second voteurs majoritaires générant les première et seconde données de sortie, le second niveau d'exigence en termes de sécurité d'au moins un de ces trois modules étant inférieur de deux degrés au premier niveau d'exigence en termes de sécurité.

Dans le deuxième mode de réalisation de l'invention, le système comprend en outre d'une part, un premier et un deuxième modules parmi un ensemble de trois modules différents réalisant la fonction exécutés par la première unité de calcul électronique, et, d'autre part, le deuxième et un troisième modules parmi cet ensemble de trois modules différents exécutés par la seconde unité de calcul électronique, et des premier et second voteurs majoritaires prenant en compte des première, deuxième et troisième sorties intermédiaires générées respectivement par les premier, deuxième et troisième modules, le second niveau d'exigence en termes de sécurité d'au moins un des premier, deuxième et troisième modules étant inférieur de deux degrés au premier niveau d'exigence en termes de sécurité.

Dans le troisième mode de réalisation de l'invention, le système comprend en outre un premier module identique ayant une cotation ASIL D exécuté par chacune des première et seconde unités électroniques de calcul et des deuxième et troisième modules différents ayant une autre cotation ASIL QM exécutés respectivement par ces première et seconde unités électroniques de calcul.

Dans ces trois mode de réalisation du système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon l'invention, cette fonction est de préférence une détection d'un objet, la donnée d'entrée est issue d'un LIDAR, ou d'un radar, ou d'une caméra, et d'au moins une donnée de sortie nominale génère avantageusement une commande d'un groupe comprenant une commande de direction, une commande moteur et une commande de freinage.

Selon l'invention, au moins une donnée de sortie génère préférentiellement la commande au moyen d'un module de planification de trajectoire coté ASIL D.

L'invention concerne aussi un véhicule automobile du type de ceux comportant un système d'assistance à la conduite avancé autorisant une conduite automatique sur autoroute comprenant un système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards tel que décrit précédemment.

Ces quelques spécifications essentielles auront rendu évidents pour l'homme de métier les avantages apportés par le procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon l'invention, ainsi que par le système correspondant, et par le véhicule automobile comprenant un tel système, par rapport à l'état de la technique antérieur.

Les spécifications détaillées de l'invention sont données dans la description qui suit en liaison avec les dessins ci-annexés. Il est à noter que ces dessins n'ont d'autre but que d'illustrer le texte de la description et ne constituent en aucune sorte une limitation de la portée de l'invention.

BREVE DESCRIPTION DES DESSINS.

La **Figure 1** est un schéma synoptique d'une architecture matérielle Duplex-Double opérationnelle après défaillance connue de l'état de la technique.

La **Figure 2** est un schéma synoptique d'un système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards, basé sur l'architecture montrée sur la **Figure 1**, connu de l'état de la technique.

La **Figure 3** est un schéma synoptique d'un système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards, basé sur l'architecture montrée sur la **Figure 1**, selon le premier mode de réalisation de l'invention.

La **Figure 4** est un schéma synoptique d'un système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards, basé sur l'architecture montrée sur la **Figure 1**, selon le deuxième mode de réalisation de l'invention.

La **Figure 5** est un schéma synoptique d'un système d'assistance à la conduite avancé autorisant une conduite automatique sur autoroute connu de l'état de la technique.

La **Figure 6** est un schéma synoptique d'un système d'assistance à la conduite avancé autorisant une conduite automatique sur autoroute basé sur le système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards montré sur la **Figure 3**.

DESCRIPTION DES MODES DE REALISATION PREFERES DE L'INVENTION.

Ainsi que cela a déjà été rappelé en préambule, une architecture 1 possible pour l'implémentation des fonctions critiques d'un véhicule autonome est celle déjà largement utilisée en avionique représentée sur la **Figure 1**.

Une donnée d'entrée 2 de la fonction à réaliser est traitée simultanément par deux unités électroniques de calcul 3, 4 qui génèrent des données de sortie 5, 6. On notera ici que les termes « donnée(s) de sortie » utilisés dans la présente demande ne doivent pas être interprétés de manière stricte et couvrent également une ou des commandes de sortie.

Une donnée de sortie nominale 7 est formée soit par une première donnée de sortie 5 générée par une première 3 des unités électroniques de calcul 3, 4 quand celle-ci fonctionne normalement, soit par une seconde donnée de sortie 6 générée par une seconde 4 des unités électroniques de calcul 3, 4 quand la première 3 est en défaillance.

Le passage de l'une à l'autre des données de sortie 5, 6 est assuré par un commutateur 8 en fonction de l'état 9 de la première unité électronique de calcul 3.

Une indication de l'état, ou le statut 10, de la seconde unité électronique de calcul 4 permet de mettre en évidence 11 les erreurs cachées.

Dans le but d'implémenter une fonction qualifiée à un premier niveau ASIL C ou D, il est connu de l'état de la technique de mettre en œuvre, répartis deux à deux dans les unités de calcul électroniques 3, 4, quatre modules différents 12, 13, 14, 15 qualifiés à un second niveau ASIL A ou B, respectivement, comme cela est représenté sur la **Figure 2**.

Ce procédé consistant à mettre en œuvre, pour réaliser une fonction d'un véhicule automobile qualifiée à un premier niveau d'exigence en termes de sécurité, des modules qualifiés à un second niveau inférieur au premier, est bien connu de l'état de la technique.

Toutefois, un tel procédé connu exige le plus souvent d'être en mesure de développer plusieurs modules 12, 13, 14, 15 différents, ce qui n'est pas toujours possible pour certaines fonctions.

Au contraire, dans le procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards correspondant aux niveaux d'exigence en termes de sécurité croissants QM, A, B, C, D de la norme ISO 26262, selon l'invention, la diversité des modules 12, 13, 14, 15 est limitée.

Dans un premier mode de réalisation, le procédé selon l'invention est mis en œuvre dans un système 16 représenté sur la **Figure 3**.

La diversité de conception est réduite à trois en implémentant trois algorithmes 12, 13, 14 dans les deux unités de calcul électroniques 17, 18 qui comprennent des voteurs 19, 20 effectuant un vote majoritaire entre des sorties intermédiaires 21, 22, 23 générées par les algorithmes 12, 13, 14.

Dans le cas de la production d'une faute dans l'un des trois algorithmes 12, 13, 14, les deux unités de calcul électroniques 17, 18 seront impactées mais resteront opérationnelles étant donné que les deux autres algorithmes 12, 13, 14 continueront de fournir des sorties cohérentes.

Pour réaliser une fonction ASIL D, les trois modules 12, 13, 14 doivent être développé en ASIL B. Pour réaliser une fonction ASIL C, l'un des modules redondants 12, 13, 14 peut être développé en ASIL A, les deux autres modules étant développés en ASIL B.

Dans ce premier mode de réalisation, la **Figure 3** est un exemple d'implémentation d'une fonction en ASIL D par trois modules 12, 13, 14 en ASIL B.

Un avantage de ce premier mode de réalisation de l'invention est que les deux unités de calcul électroniques 17, 18 sont identiques et qu'elles peuvent par conséquent avoir une même référence de stock. Toutefois, un désavantage est que trois modules 12, 13, 14 redondants sont exécutés sur chaque ECUs 17, 18. Cela accroît la puissance de calcul à mettre en œuvre ainsi que la taille de la mémoire nécessaire.

Une variante possible de ce premier mode de réalisation est d'exécuter en permanence des premier et deuxième modules 12, 13, mais de ne lancer l'exécution d'un troisième module 14 qu'en cas de désaccord entre les première et deuxième sorties intermédiaires 21, 22 des premier et deuxième modules 12, 13. Cela diminue la charge de calcul des ECUs. Cependant, cela n'est applicable que si l'intervalle de temps de tolérance de défaillance est relativement long.

Dans un deuxième mode de réalisation, le procédé selon l'invention est mis en œuvre dans un système 24 représenté sur la **Figure 4**.

La diversité de conception est également réduite à trois, seulement deux 12, 13 des trois algorithmes 12, 13, 14 diversifiés sont exécutés sur la première unité de calcul électronique 25 et deux autres 13, 14 parmi ces trois sont exécutés sur la seconde unité de calcul électronique 26.

La sortie intermédiaire 21, 23 du module 12, 14 qui n'est pas exécuté sur l'une des unités de calcul électroniques 25, 26 lui est envoyée par l'autre module 12, 14, de façon que les voteurs majoritaires 19, 20 génèrent les données de sortie 5, 6 de la fonction.

Dans ce deuxième mode de réalisation, la **Figure 4** est un exemple d'implémentation d'une fonction en ASIL D par trois modules 12, 13, 14 en ASIL B.

L'avantage de ce deuxième mode de réalisation de l'invention comparé au premier mode de réalisation est que moins de puissance de calcul et moins de mémoire sont nécessaires. Le désavantage est la nécessité d'une communication croisée entres les deux ECUs et de deux ECUs diversifiés.

Dans un troisième mode de réalisation de l'invention, le premier module implémentant la fonction qui est exécuté sur chaque unité de calcul électronique est qualifié ASIL D, et les deuxième et troisième modules différents qualifiés ASIL QM sont exécutés chacun sur chacune des unités de calcul électroniques 3, 4.

Une diversité de conception pour le premier module n'est pas nécessaire, puisqu'il est qualifié au même niveau d'exigence en termes de sécurité ASIL D que la fonction à implémenter. De la sorte la diversité de conception reste inférieure à quatre.

Un exemple typique d'application de l'invention est un système d'assistance à la conduite avancé (ou ADAS, c'est-à-dire "Advanced Driving Assistance System" en terminologie anglaise) de niveau quatre, tel qu'un système autorisant une conduite automatique sur autoroute (ou MDS, c'est-à-dire "Motorway Driver System" en terminologie anglaise). Le conducteur humain peut se reposer sur le MDS pour contrôler le véhicule en circulant sur une autoroute, ce qui lui permet de répondre à ses courriels, de regarder la télévision, etc....

Le MDS a une image complète de l'environnement de conduite du véhicule grâce à ses capteurs redondants. Il peut suivre les autres véhicules, il peut aussi prendre des décisions, telles que freiner ou braquer pour éviter des collisions avec les autres véhicules, ou même effectuer un dépassement pour conserver une vitesse donnée.

La **Figure 5** montre une vue d'ensemble d'un MDS 27 simplifié connu de l'état de la technique, prenant seulement en compte les capteurs avant 28, 29, 30. Un système complet nécessite également des capteurs arrière et des capteurs latéraux, pour entre autres choses permettre un changement de voie.

Trois capteurs avant 28, 29, 30 de technologies diverses (LIDAR 28, radar 29, caméra 30) sont utilisés pour maintenir des performances de détection suffisantes (détection des objets et leur suivi 31, 32, par le LIDAR 28 et le radar 29, ou simple détection des objets 33 par la caméra 30) dans n'importe quelles conditions environnementales après une première défaillance.

Une fusion des informations 34 complémentaires issues des capteurs avant 28, 29, 30 permet d'identifier la route, les autres véhicules, les obstacles…

Une planification de la trajectoire 35 détermine la trajectoire du véhicule. Le contrôle latéral et longitudinal 36 calcule les commandes de direction 37, moteur 38 et de freinage 39 de manière que le véhicule suive la trajectoire planifiée.

En ce qui concerne le niveau d'exigence en termes de sécurité, pour le MDS, prendre une mauvaise décision ou ne pas détecter un obstacle est coté ASIL D. Chaque capteur avant 28, 29, 30 est qualifié seulement ASIL B grâce à la redondance de ces capteurs avant 28, 29, 30.

Dans cet état de la technique, la fusion des informations 34 des capteurs avant 28, 29, 30, la planification de trajectoire 35, et le contrôle latéral et longitudinal 36 doivent être qualifiés à ASIL D.

De plus, le système MDS 27 doit rester opérationnel après une première défaillance, car il peut prendre plus de dix seconde au conducteur pour reprendre la main. La perte brusque complète de la disponibilité du système 27 doit donc être qualifiée ASIL D.

Le procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon l'invention permet de réduire les niveaux d'exigence en termes de sécurité ASIL D des fonctions de fusion des informations 34 et de planification de trajectoire 35, et également du contrôle latéral et longitudinal 36.

La **Figure 6** est un exemple de système MDS 40 basé sur l'invention, où seule la réduction du niveau d'exigence en termes de sécurité est appliquée à la fonction de fusion des informations 24, tandis que la fonction de planification de trajectoire et le le contrôle latéral et longitudinal 41 restent qualifiés ASIL D, dans le but de simplifier le schéma.

Trois modules différents 12, 13, 14 implémentant la fonction "fusion des informations" 34 sont exécutés par les deux unités de calcul électroniques 17, 18 en application du premier mode de réalisation de l'invention montré sur la **Figure 3**.

Cette implémentation évite le recours à quatre modules différents si seulement deux modules étaient exécutés dans chaque ECU 17, 18, comme il est connu de l'état de la technique (**Figure 2**).

Les données de sortie 5 de la première unité de calcul électronique 17 forment les commandes de direction 37, moteur 38 et de freinage 39 à moins que cette première unité de calcul électronique 17 ne soit plus opérationnelle. Dans ce cas le commutateur 8 fournit les commandes 37, 38, 39 issues de la deuxième unité électronique 18.

Une variante possible de cet exemple est l'implémentation de la fonction "fusion des informations" 34 en application du deuxième mode de réalisation de l'invention montré sur la **Figure 4**. La seule différence est que le premier module 12 implémentant la fonction "fusion des informations" n'est pas implémenté dans la seconde unité de calcul électronique 26 et que le troisième module 14 implémentant cette fonction n'est pas implémenté dans la première unité de calcul électronique 25. De plus, la sortie intermédiaire 21 du premier module 12 est envoyée à la seconde unité de calcul électronique 26, et la sortie intermédiaire 23 du troisième module 14 est envoyée à la première unité de calcul électronique 25.

Comme il va de soi, l'invention ne se limite pas aux seuls modes de réalisation préférentiels décrits ci-dessus.

Une description similaire pourrait porter sur des systèmes opérationnels après défaillance dans le domaine de l'automobile différents d'un MDS, notamment des systèmes de direction assistée électriques (ou EPS, acronyme de "Electric Power Steering" en terminologie anglaise) ou de freinage.

Ces autres modes de réalisation ne sortiraient pas du cadre de la présente invention dans la mesure où ils résultent des revendications ci-après.

REVENDICATIONS

1) Procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards correspondant à des niveaux d'exigence en termes de sécurité croissants, notés QM, A, B, C, D, le procédé étant du type de ceux implémentant ladite fonction avec un premier niveau d'exigence en termes de sécurité par au moins des moyens (12, 13, 14, 15) présentant un second niveau d'exigence en termes de sécurité inférieur audit premier niveau d'exigence en termes de sécurité, caractérisé en ce que ladite fonction est réalisée en parallèle à partir d'au moins une donnée d'entrée (2) par des première et seconde unités électroniques de calcul (3, 4, 17, 18, 25, 26) passives après défaillance générant respectivement au moins des première et seconde données de sortie (5, 6) constituant alternativement au moins une donnée de sortie nominale (7) de ladite fonction selon un état desdites première et seconde unités électroniques de calcul (3, 4, 17, 18, 25, 26), ledit premier niveau d'exigence en termes de sécurité étant coté D ou C et ledit second niveau d'exigence en termes de sécurité étant coté B, A ou QM, pour une diversité desdits moyens (12, 13, 14) inférieure à quatre.

2) Procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon la revendication 1 précédente, caractérisé en ce que lesdites première et seconde unités électroniques de calcul (17, 18) exécutent chacune un ensemble identique de trois modules (12, 13, 14) différents réalisant ladite fonction et générant lesdites première et seconde données de sortie (5, 6) par l'intermédiaire de premier et second voteurs majoritaires (19, 20), ledit second niveau d'exigence en termes de sécurité d'au moins un desdits trois modules étant inférieur de deux degrés audit premier niveau d'exigence en termes de sécurité.

3) Procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon la revendication 1 précédente, caractérisé en ce que lesdites première et seconde unités électroniques de calcul (25, 26) exécutent respectivement, d'une part, un premier et un deuxième modules (12, 13), et, d'autre part, ledit deuxième et un troisième modules (13, 14) parmi un ensemble de trois modules (12, 13, 14) différents réalisant ladite fonction et générant lesdites première et seconde données de sortie (5, 6) par l'intermédiaire de premier et second voteurs majoritaires (19, 20) prenant en compte des première, deuxième et troisième sorties

intermédiaires (21, 22, 23) générées respectivement par lesdits premier, deuxième et troisième modules (12, 13, 14), ledit second niveau d'exigence en termes de sécurité d'au moins un desdits premier, deuxième et troisième modules (12, 13, 14) étant inférieur de deux degrés audit premier niveau d'exigence en termes de sécurité.

4) Procédé d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon la revendication 1 précédente, caractérisé en ce que lesdites première et seconde unités électroniques de calcul (3, 4) exécutent chacune un premier module identique ayant une cotation ASIL D et, respectivement, des deuxième et troisième modules différents ayant une autre cotation ASIL QM.

5) Système d'implémentation (1, 16, 24, 27, 40) d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards correspondant à des niveaux d'exigence en termes de sécurité croissants, notés QM, A, B, C, D, apte à la mise œuvre du procédé selon l'une quelconque des revendications 1 à 4 précédentes du type de ceux implémentant ladite fonction avec un premier niveau d'exigence en termes de sécurité et comprenant au moins une première unité de calcul électronique (3, 17, 25), des moyens d'acquisition d'une donnée d'entrée (2) de ladite fonction et des moyens de génération (12, 13, 14) d'au moins une première donnée de sortie (5) de ladite fonction présentant un second niveau d'exigence en termes de sécurité inférieur audit premier niveau d'exigence en termes de sécurité, caractérisé en ce qu'il comprend en outre une seconde unité de calcul électronique (18, 26) générant au moins une seconde donnée de sortie (6) de ladite fonction, et un commutateur (8) produisant au moins une donnée de sortie nominale (7) en commutant ladite première donnée de sortie (5) ou ladite seconde donnée de sortie (6) selon un état desdites première et seconde unités électroniques de calcul (16, 17, 25, 26), lesdites première et seconde unités électroniques de calcul étant passives après défaillance, et ledit premier niveau d'exigence en termes de sécurité étant coté D ou C et ledit second niveau d'exigence en termes de sécurité étant coté B, A ou QM, pour une diversité desdits moyens (12, 13, 14) inférieure à quatre.

6) Système d'implémentation (16, 40) d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon la revendication 5 précédente,

caractérisé en ce qu'il comprend en outre un ensemble identique de trois modules (12, 13, 14) différents réalisant ladite fonction exécutés par chacune desdites première et seconde unités électroniques de calcul (17, 18), et des premier et second voteurs majoritaires (19, 20) générant lesdites première et seconde données de sortie (5, 6), ledit second niveau d'exigence en termes de sécurité d'au moins un desdits trois modules étant inférieur de deux degrés audit premier niveau d'exigence en termes de sécurité.

7) Système d'implémentation (24) d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon la revendication 5 précédente, caractérisé en ce qu'il comprend en outre d'une part, un premier et un deuxième modules (12, 13) parmi un ensemble de trois modules (12, 13, 14) différents réalisant ladite fonction exécutés par ladite première unité de calcul électronique (25), et, d'autre part, ledit deuxième et un troisième modules (13, 14) parmi ledit ensemble de trois modules (12, 13, 14) différents exécutés par ladite seconde unité de calcul électronique (26), et des premier et second voteurs majoritaires (19, 20) prenant en compte des première, deuxième et troisième sorties intermédiaires (21, 22, 23) générées respectivement par lesdits premier, deuxième et troisième modules (12, 13, 14), ledit second niveau d'exigence en termes de sécurité d'au moins un desdits premier, deuxième et troisième modules (12, 13, 14) étant inférieur de deux degrés audit premier niveau d'exigence en termes de sécurité.

8) Système d'implémentation d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon la revendication 5 précédente, caractérisé en ce qu'il comprend en outre un premier module identique ayant une cotation ASIL D exécuté par chacune desdites première et seconde unités électroniques de calcul (3, 4) et des deuxième et troisième modules différents ayant une autre cotation ASIL QM exécutés respectivement par lesdites première et seconde unités électroniques de calcul (3, 4).

9) Système d'implémentation (40) d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon l'une quelconque des revendications 5 à 8 précédentes, caractérisé en que ladite fonction est une détection d'un objet, ladite donnée d'entrée (2) est issue d'un LIDAR (28), ou d'un radar (29), ou d'une caméra (30), et ladite au moins une donnée de sortie nominale (7) génère une commande

d'un groupe comprenant une commande de direction (37), une commande moteur (38) et une commande de freinage (39).

10) Système d'implémentation (40) d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon la revendication 9 précédente, caractérisé en que ladite au moins une donnée de sortie (5, 6) génère ladite commande (37, 38, 39) au moyen d'un module de planification de trajectoire (41) coté ASIL D.

11) Véhicule automobile du type de ceux comportant un système d'assistance à la conduite avancé autorisant une conduite automatique sur autoroute, caractérisé en qu'il comprend un système d'implémentation (16, 24, 40) d'une fonction d'un véhicule automobile conforme à des niveaux ASIL standards selon l'une quelconque des revendications 5 à 10 précédentes.

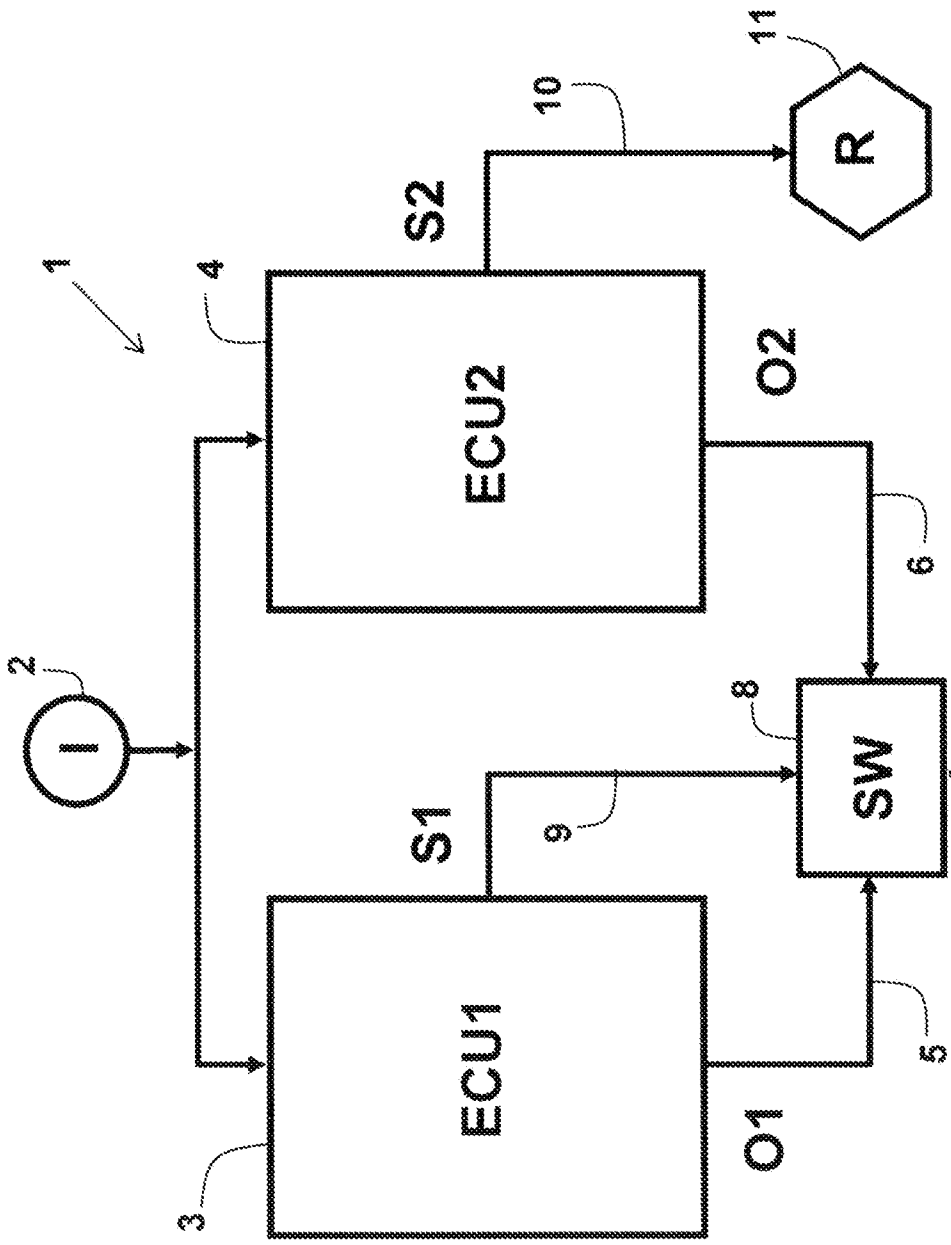

FIG. 1 (Etat de la technique)

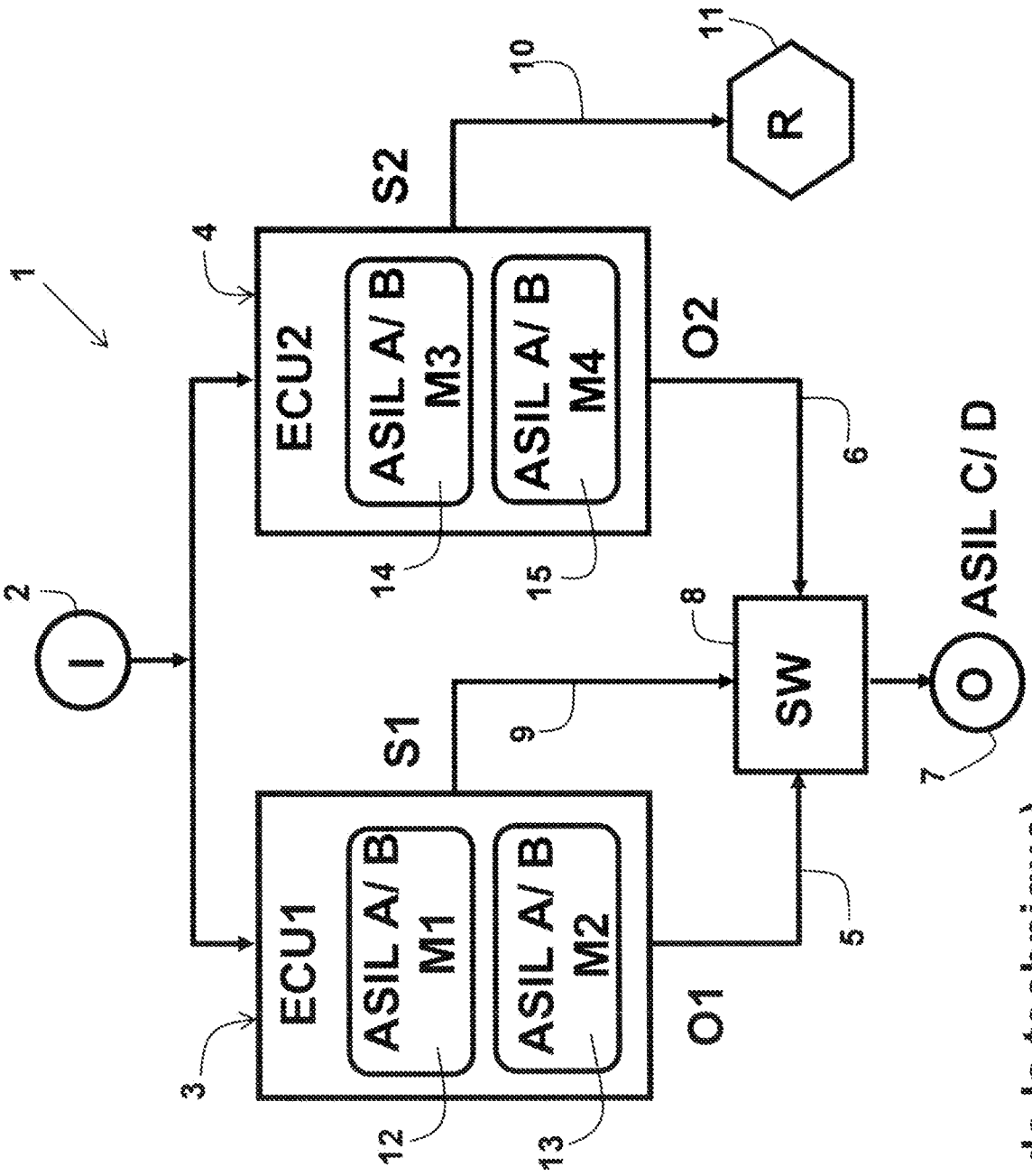

FIG. 2 (Etat de la technique)

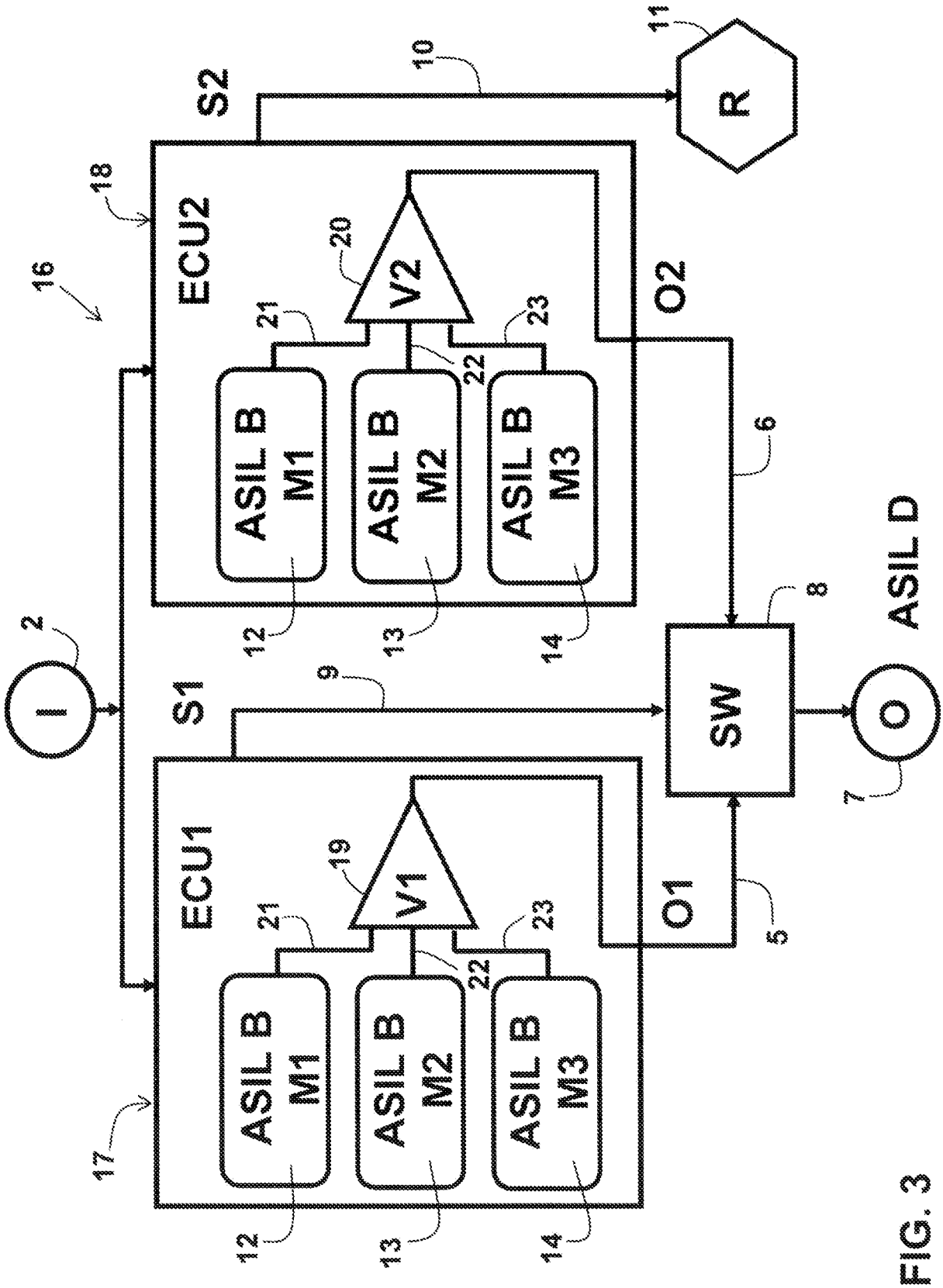
I
2
S1
S2
ECU1
ECU2
16
17
18
V1
V2
19
20
21
22
23
ASIL B M1
ASIL B M2
ASIL B M3
12
13
14
O1
O2
5
6
9
10
SW
8
O
7
ASIL D
R
11

FIG. 3

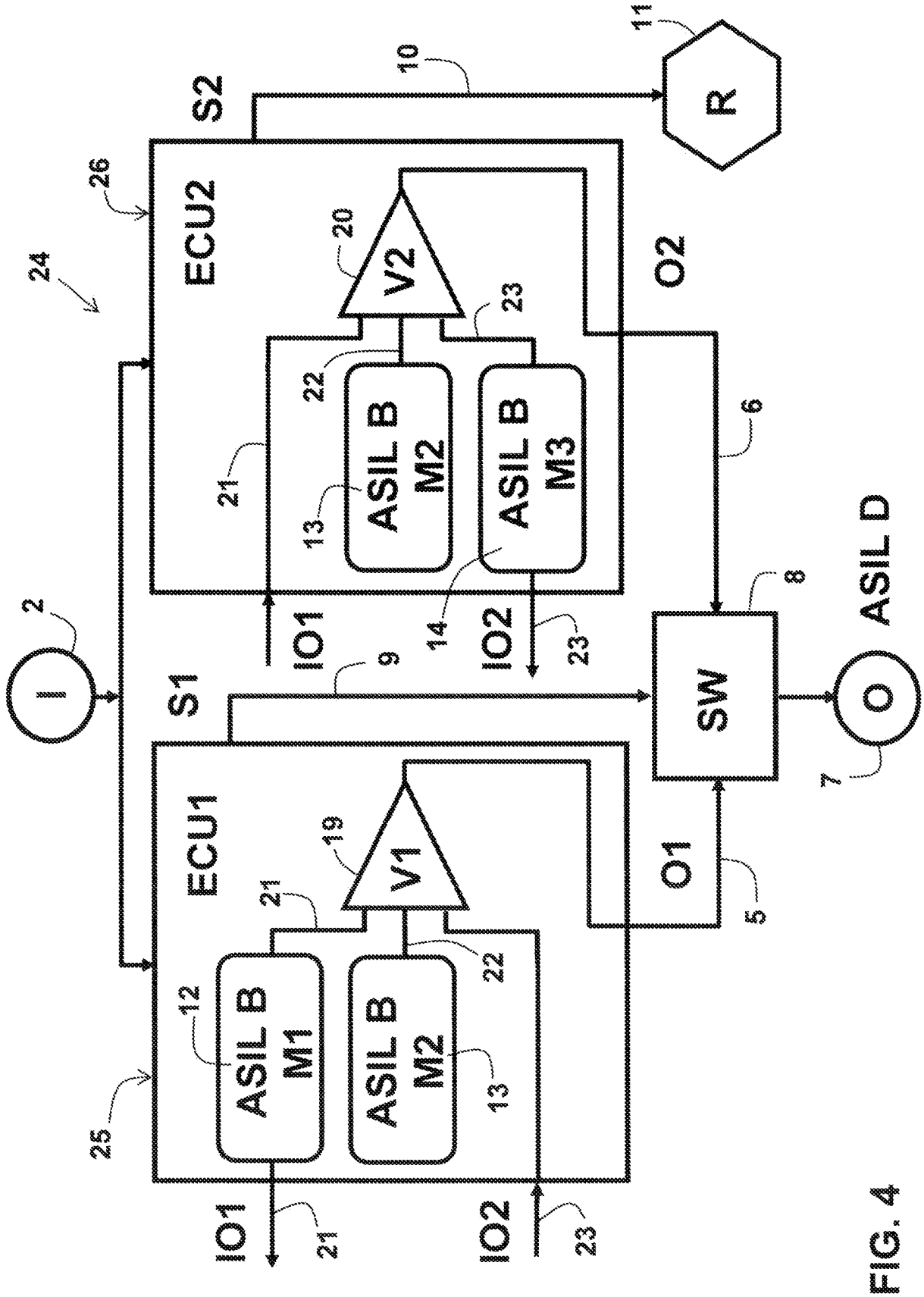
24
26
ECU2
S2
10
11
R
20
V2
O2
23
22
21
ASIL B
M2
13
ASIL B
M3
6
2
I
IO1
9
14
IO2
23
S1
SW
8
ASIL D
O
7
ECU1
19
V1
21
O1
5
22
12
ASIL B
M1
ASIL B
M2
13
25
IO1
21
IO2
23

FIG. 4

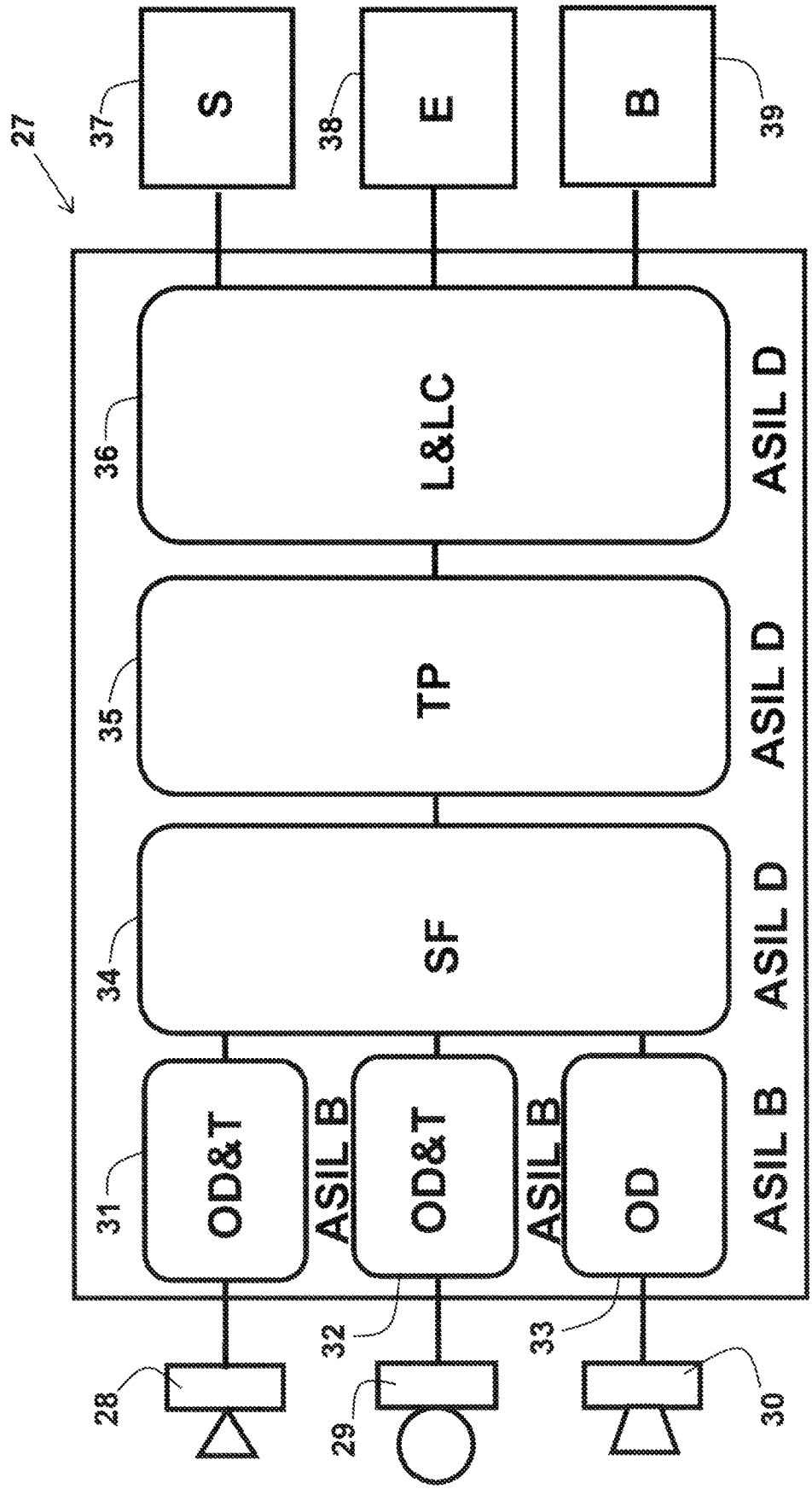

FIG. 5 (Etat de la technique)

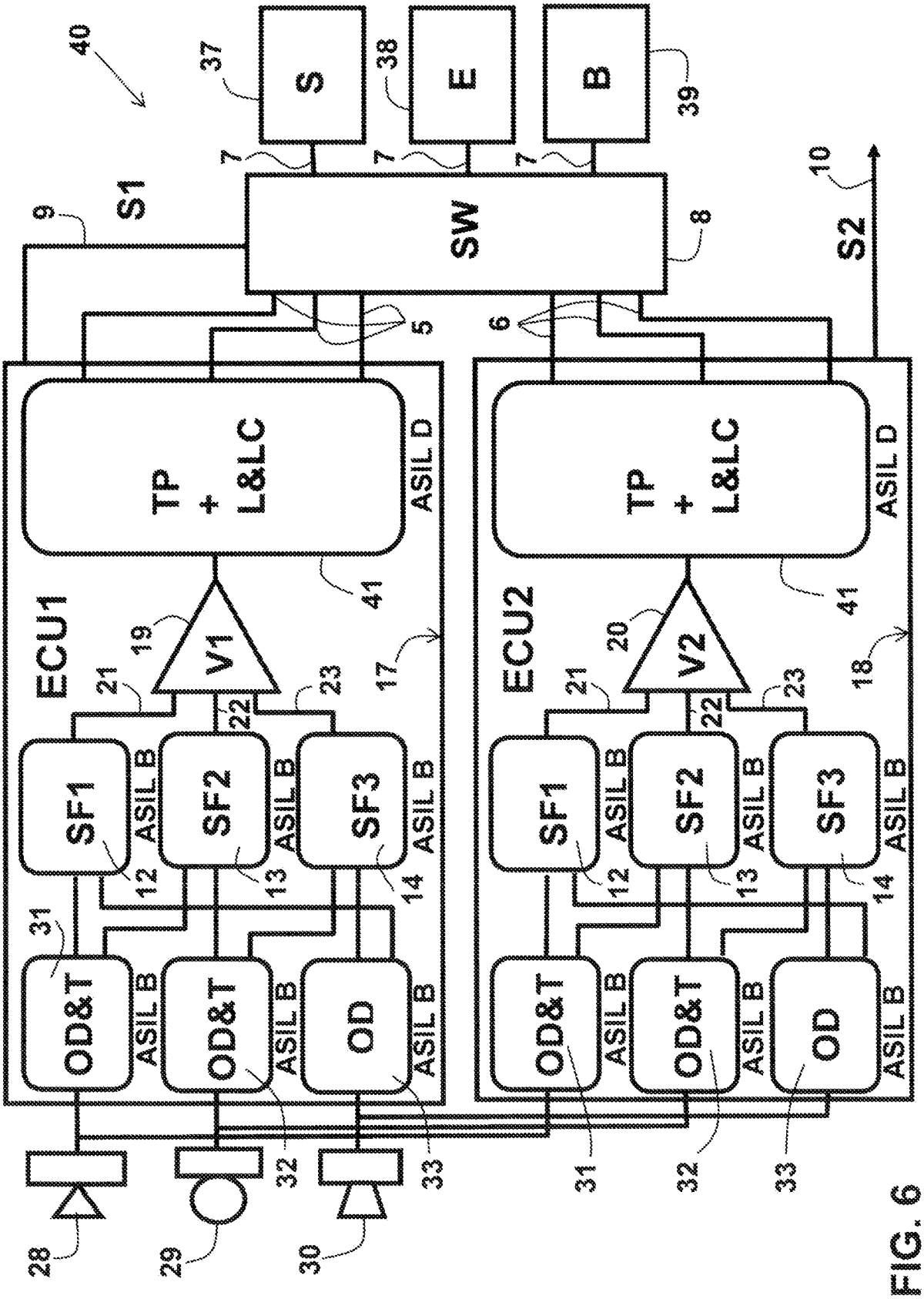
40
37
S
38
E
39
B
7
7
7
S1
9
SW
8
10
S2
5
6
ECU1
TP + L&LC
ASIL D
41
19
V1
21
22
23
17
SF1
SF2
SF3
ASIL B
12
13
14
31
OD&T
OD
32
33
28
29
30
ECU2
20
V2
18

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/050768

A. CLASSIFICATION OF SUBJECT MATTER
INV. B60W50/02
ADD. B60W50/029 B60W50/00

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)
B60W G05B

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 Y	US 2013/346783 A1 (WEBER JOCHEN [DE] ET AL) 26 December 2013 (2013-12-26) paragraphs [0007], [0023], [0053] - [0055] the whole document	1,5,11 9,10
Y	US 2014/067192 A1 (YOUSUF MOHAMMED ABDULLA [US]) 6 March 2014 (2014-03-06) paragraphs [0005], [0037], [0038], [0042], [0043], [0044]	9,10
Y	DE 10 2007 045398 A1 (CONTINENTAL TEVES AG & CO OHG [DE]) 2 April 2009 (2009-04-02) paragraphs [0013], [0015], [0031]	9,10
A	EP 2 765 045 A1 (PARAVAN GMBH [DE]) 13 August 2014 (2014-08-13) figure 1	1,5

☐ 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
10 June 2016	17/06/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Plenk, Rupert

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2016/050768

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013346783 A1	26-12-2013	CN 103250429 A	14-08-2013
		DE 102010041492 A1	29-03-2012
		EP 2622870 A1	07-08-2013
		JP 2013545424 A	19-12-2013
		US 2013346783 A1	26-12-2013
		WO 2012048929 A1	19-04-2012
US 2014067192 A1	06-03-2014	CN 103661378 A	26-03-2014
		DE 102013216444 A1	06-03-2014
		US 2014067192 A1	06-03-2014
DE 102007045398 A1	02-04-2009	AT 497611 T	15-02-2011
		DE 102007045398 A1	02-04-2009
		EP 2193408 A1	09-06-2010
		US 2010306601 A1	02-12-2010
		WO 2009040300 A1	02-04-2009
EP 2765045 A1	13-08-2014	DE 102013202253 A1	14-08-2014
		EP 2765045 A1	13-08-2014
		US 2014229064 A1	14-08-2014

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2016/050768

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. B60W50/02
ADD. B60W50/029 B60W50/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
B60W G05B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X Y	US 2013/346783 A1 (WEBER JOCHEN [DE] ET AL) 26 décembre 2013 (2013-12-26) alinéas [0007], [0023], [0053] - [0055] le document en entier	1,5,11 9,10
Y	US 2014/067192 A1 (YOUSUF MOHAMMED ABDULLA [US]) 6 mars 2014 (2014-03-06) alinéas [0005], [0037], [0038], [0042], [0043], [0044]	9,10
Y	DE 10 2007 045398 A1 (CONTINENTAL TEVES AG & CO OHG [DE]) 2 avril 2009 (2009-04-02) alinéas [0013], [0015], [0031]	9,10
A	EP 2 765 045 A1 (PARAVAN GMBH [DE]) 13 août 2014 (2014-08-13) figure 1	1,5

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 juin 2016	17/06/2016

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Plenk, Rupert

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2016/050768

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2013346783 A1	26-12-2013	CN 103250429 A	14-08-2013
		DE 102010041492 A1	29-03-2012
		EP 2622870 A1	07-08-2013
		JP 2013545424 A	19-12-2013
		US 2013346783 A1	26-12-2013
		WO 2012048929 A1	19-04-2012
US 2014067192 A1	06-03-2014	CN 103661378 A	26-03-2014
		DE 102013216444 A1	06-03-2014
		US 2014067192 A1	06-03-2014
DE 102007045398 A1	02-04-2009	AT 497611 T	15-02-2011
		DE 102007045398 A1	02-04-2009
		EP 2193408 A1	09-06-2010
		US 2010306601 A1	02-12-2010
		WO 2009040300 A1	02-04-2009
EP 2765045 A1	13-08-2014	DE 102013202253 A1	14-08-2014
		EP 2765045 A1	13-08-2014
		US 2014229064 A1	14-08-2014