



(43) Date de la publication internationale
12 janvier 2017 (12.01.2017)

WIPO | PCT

(10) Numéro de publication internationale
WO 2017/006041 A1

- (51) Classification internationale des brevets :
G06F 9/54 (2006.01) *G06F 13/16* (2006.01)
- (21) Numéro de la demande internationale :
PCT/FR2016/051692
- (22) Date de dépôt international :
4 juillet 2016 (04.07.2016)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
1556384 6 juillet 2015 (06.07.2015) FR
- (71) Déposant : VALEO EQUIPEMENTS ELECTRIQUES
MOTEUR [FR/FR]; 2 rue André Boulle, 94046 Creteil
Cedex (FR).
- (72) Inventeur : YMLAHI-OUAZZANI, Abdelillah; 13 Rue
Jacques Daguerre, 92500 Rueil Malmaison (FR).
- (74) Mandataire : DE LA BIGNE, Guillaume; LLR, 11 Bou-
lebard de Sébastopol, 75001 Paris (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 CONTROLLING AN ELECTRONIC COMPUTING UNIT OF A MOTOR VEHICLE, CORRESPONDING ELECTRONIC COMPUTING UNIT AND MOTOR VEHICLE

(54) Titre : PROCÉDÉ DE COMMANDE D'UNE UNITÉ DE CALCUL ÉLECTRONIQUE D'UN VÉHICULE AUTOMOBILE, UNITÉ DE CALCUL ÉLECTRONIQUE ET VÉHICULE AUTOMOBILE CORRESPONDANTS

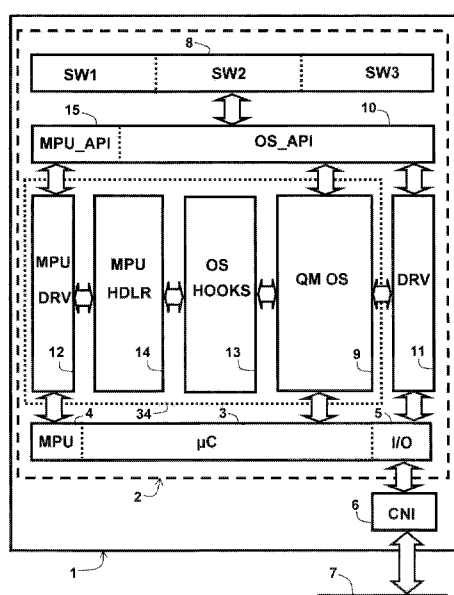


FIG. 1

(57) Abstract : The invention relates to a method for controlling an electronic computing unit (1) of a motor vehicle according to the invention, of the type which is based on a first operating system (9) that complies with a first security requirement level of the ISO 26262 standard, a first interface of application programs (10), a first event manager of a real-time environment and first drivers (11) of peripherals executed by a central processing unit (3) of a microprocessor (2) also comprising a memory protection unit (4). In accordance with the invention, the method also implements a second interface of application programs (15), a second event manager (14) and a second peripheral driver (12) which are specific to the memory protection unit and separate from the first operating system.

(57) Abrégé : Le procédé de commande d'une unité de calcul électronique (1) de véhicule automobile selon l'invention est du type de ceux basés sur un premier système d'exploitation (9) conforme à un premier niveau d'exigence en termes de sécurité de la norme ISO 26262, une première interface de programmes d'application (10), un premier gestionnaire d'événements d'un environnement temps réel et des premiers pilotes (11) de périphériques exécutés par une unité centrale de calcul (3) d'un microprocesseur (2) comprenant en outre une unité de protection mémoire (4). Conformément à l'invention, le procédé met également en œuvre une seconde interface de programmes d'application (15), un second gestionnaire d'événements (14) et un second pilote (12) de périphérique spécifiques à l'unité de protection mémoire et distincts du premier système d'exploitation.

PROCEDE DE COMMANDE D'UNE UNITE DE CALCUL ELECTRONIQUE D'UN VEHICULE AUTOMOBILE, UNITE DE CALCUL ELECTRONIQUE ET VEHICULE AUTOMOBILE CORRESPONDANTS

5 DOMAINE TECHNIQUE DE L'INVENTION.

La présente invention concerne un procédé de commande d'une unité de calcul électronique d'un véhicule automobile.

L'invention concerne également une unité de calcul électronique apte à la mise en œuvre de ce procédé, ainsi que le véhicule automobile comprenant cette
10 unité de calcul électronique.

ARRIERE PLAN TECHNOLOGIQUE DE L'INVENTION.

De nos jours, des systèmes d'exploitations (ou OS, acronyme en terminologie anglaise de "Operating System") embarqués sont couramment utilisés dans les
15 unités de calcul électroniques (ECU ou "Electronique Computing Unit" en terminologie anglaise) de véhicules automobiles. En général, il revient à un système d'exploitation l'enchaînement des tâches, le traitement des interruptions, et la gestion des ressources.

Les enjeux classiques des systèmes d'exploitations embarqués sont la
20 capacité de réponse temporelle (c'est-à-dire un déterminisme temps réel) et l'extensibilité (c'est-à-dire la portabilité de microprocesseurs de bas de gamme à des microprocesseurs de haut de gamme).

En ce qui concerne le logiciel dans l'automobile, le standard ISO 26262 établit un cadre formel pour la sécurité fonctionnelle des modules. La norme ISO
25 26262 stipule que la sûreté et la sécurité du logiciel doivent être prises en compte de manière systématique pendant tout le cycle de développement du logiciel.

Un niveau d'exigence en termes de sécurité, ou ASIL défini par la norme (acronyme de "Automotive Safety Integrity Level" en terminologie anglaise), est attribué sur la base du risque de l'occurrence d'un évènement dangereux en
30 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.

Avec l'arrivée de la norme ISO 26262, les systèmes d'exploitation embarqués sont soumis à un nouvel ensemble d'exigences pour satisfaire aux contraintes de sécurité. Par conséquent, les implémentations classiques pour l'automobile ont été

remaniées et de nouvelles solutions de systèmes d'exploitation de sécurité ont été mises sur le marché avec des coûts importants.

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
5 indiqué par QM ("Qualité Management" c'est-à-dire "Gestion de la Qualité") est assigné aux fonctions non- critiques.

Un système d'exploitation qui satisfait aux exigences de la norme ISO 26262 est appelé "Safety OS". Comparé à un "QM OS" (c'est-à-dire un OS avec une
10 gestion de qualité classique), un "Safety OS" fournit des fonctions de protection pour des protections spatiales et temporelles.

D'une part, les protections temporelles ont pour but de contrôler le taux de lancement, le temps d'exécution et le verrouillage/ déverrouillage des ressources partagées par un programme.

15 D'autre part, les protections spatiales ont pour but de contrôler les droits d'accès à la mémoire RAM (acronyme de "Random Acces Memory" en terminologie anglaise, c'est-à-dire "mémoire à accès aléatoire"), la mémoire de type "Flash", et les périphériques.

Une protection mémoire est une caractéristique d'un OS qui supporte
20 l'implémentation de protections spatiales, le plus souvent sur une unité de protection mémoire, ou MPU (acronyme en terminologie anglaise de "Memory Protection Unit"), du microprocesseur.

Quand elle est activée, la MPU supervise les bus d'instructions et de données de l'unité centrale de traitement, ou CPU (acronyme en terminologie
25 anglaise de "Central Processing Unit"), du microprocesseur, et les accès à la mémoire RAM, Flash et aux périphériques sont contrôlés. L'accès est accordé quand les droits d'accès (en lecture, en écriture, ou d'exécution) sont valides. Cependant, quand les droits d'accès sont restreints, toute violation d'accès déclenche une erreur de la MPU, arrête la CPU et l'exécution du programme.

30 Il revient à l'implémentation du Safety OS d'offrir les services appropriés pour initialiser et remettre à zéro les registres de la MPU.

Dans l'état de la technique, il est connu qu'une protection mémoire mettant en œuvre une MPU permet une détection et une prise en compte d'une erreur plus
rapides; l'impact sur la charge de la CPU est réduit puisque la plus grande partie du
35 traitement est faite par le matériel.

En réponse aux défis de tout ordre posés par le développement de systèmes d'exploitation embarqués, les constructeurs et les équipementiers de l'automobile ont pour la plupart adopté une architecture logicielle standard: AUTOSAR.

Les développements d'AUTOSAR (acronyme en terminologie anglaise de "AUTomotive Open System ARchitecture", c'est-à-dire "Architecture de Système Ouvert d'Automobile") visent à remplir toutes les exigences de la norme ISO 26262 à partir des modules de base de l'OS ("AUTOSAR basic software" ou "AUTOSAR BSW") accessible librement, mais développés seulement au niveau d'exigence QM.

Il s'en suit que la mise en œuvre d'une MPU a été le plus souvent associée à la nécessité d'acheter un système d'exploitation de type "Safety OS", tel que "AUTOSAR Safety", avec un impact des coûts important sur le budget des projets.

De plus, la vérification de la conformité à la norme ISO 26262 des différentes couches de l'OS est souvent rendue difficile par la disparité des contributeurs et l'absence des codes sources.

Pour pallier cet inconvénient, il a été proposé des techniques de tests des OS du commerce, et de leur conformité à la norme ISO 26262, même si les exécutable seulement sont disponibles.

Une telle technique est décrite notamment dans l'article "Binary-Level Fault Injection for AUTOSAR Systems", Mafijul Md. Islam et al., 2014 Tenth European Dependable Computing Conference, p.138- 141, 2014, IEEE.

La technique est évaluée sur une unité électronique de calcul comprenant un microprocesseur de la société Freescale de la série MPC5567 fonctionnant sous AUTOSAR.

Le microprocesseur MPC5567 comporte une unité de gestion de la mémoire ("Memory Management Unit", ou MMU, en terminologie anglaise, qui est une MPU avec une fonction supplémentaire de translation des adresses.

La technique décrite n'a pas besoin de connaître ni les connecteurs de l'OS, ni les appels du gestionnaire d'évènements de son environnement temps réel, et considère l'OS comme une boîte noire.

Cependant, cette technique, en regardant l'OS globalement comme une boîte noire, ne fait pas la distinction entre les contraintes normatives portant sur l'OS de base et celles afférentes à la mise en œuvre d'une MPU.

De la sorte, l'utilisation d'un OS de base ayant un niveau d'exigence en terme de sécurité QM associé à un mécanisme de protection mémoire spécifique en dehors de l'OS de niveau de criticité supérieur n'est pas envisagée dans cet article

pour répondre au besoin d'un "Safety OS".

Or ce découplage de l'OS et du mécanisme de protection mémoire permettrait aux constructeurs et équipementiers d'automobiles d'intégrer une protection mémoire tout en conservant leurs OS QM habituels dans leurs projets, et
5 correspondrait à un besoin de réduction des coûts.

DESCRIPTION GENERALE DE L'INVENTION.

La présente invention vise par conséquent à satisfaire ce besoin.

Elle a précisément pour objet un procédé de commande d'une unité de calcul
10 électronique de véhicule automobile du type de ceux basés sur un premier système d'exploitation conforme à un premier niveau d'exigence en termes de sécurité de la norme ISO 26262, une première interface de programmes d'application, un premier gestionnaire d'évènements d'un environnement temps réel et des premiers pilotes de périphériques exécutés par une unité centrale de calcul d'un microprocesseur
15 comprenant en outre une unité de protection mémoire.

Le procédé selon l'invention met en œuvre en outre une seconde interface de programmes d'application, un second gestionnaire d'évènements et un second pilote de périphérique, spécifiques à cette unité de protection mémoire, et distincts du premier système d'exploitation.

20 Selon l'invention, le premier système d'exploitation, le second gestionnaire d'évènements et le second pilote sont équivalents à un second système d'exploitation conforme à un second niveau d'exigence en termes de sécurité de la norme ISO 26262 supérieur au premier niveau d'exigence en termes de sécurité.

Dans le procédé de l'invention, le premier niveau d'exigence en termes de
25 sécurité est de préférence coté QM.

Dans le procédé de l'invention encore, le second pilote utilise des premiers connecteurs de tâches et des seconds connecteurs d'interruptions du premier système d'exploitation.

Le procédé de commande d'une unité de calcul électronique de véhicule
30 automobile selon l'invention comprend une première étape appelant une première fonction de la seconde interface de programmes d'application initialisant au moins un registre de l'unité de protection mémoire.

Le procédé selon l'invention comprend en outre une deuxième étape appelant une deuxième fonction de la seconde interface de programmes
35 d'application initialisant une protection des tâches.

Le procédé selon l'invention encore comprend en outre une troisième étape appelant une troisième fonction de la seconde interface de programmes d'application initialisant une protection des interruptions.

Selon l'invention, le second gestionnaire d'évènements transmet à la
5 seconde interface de programmes d'application des violations de la protection des tâches et de la protection des interruptions.

L'invention concerne également une unité de calcul électronique de véhicule automobile apte à ma mise en œuvre du procédé de commande décrit ci-dessus.

Cette unité de calcul électronique est du type de celles comprenant un
10 microprocesseur comportant au moins une unité centrale de calcul et une unité de protection mémoire associées à au moins une mémoire de programme, au moins une mémoire de données, et à au moins une interface d'entrées/ sorties.

Au moins une mémoire de programme stocke des premiers codes informatiques représentatifs d'un système d'exploitation conforme à un niveau
15 d'exigence en termes de sécurité coté QM de la norme ISO 26262, d'une première interface de programmes d'application, d'un premier gestionnaire d'évènements d'un environnement temps réel et de premiers pilotes de périphériques aptes à être connectés à l'au moins une interface d'entrées/ sorties, exécutés par l'au moins une unité centrale de calcul.

Selon l'invention, l'au moins une mémoire de programme stocke en outre des
20 seconds codes informatiques représentatifs d'une seconde interface de programmes d'application, d'un second gestionnaire d'évènements et d'un second pilote spécifiques à l'unité de protection mémoire distincts des premiers codes informatiques.

Un véhicule automobile comprenant au moins une unité de calcul
25 électronique tirera bénéfice de l'invention décrite ci-dessus.

Ces quelques spécifications essentielles auront rendu évidents pour l'homme de métier les avantages apportés par le procédé de commande d'une unité de calcul électronique de véhicule automobile selon l'invention, ainsi que par l'unité de
30 calcul électronique correspondante, et par le véhicule automobile comprenant une telle unité de calcul électronique, 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
35 une limitation de la portée de l'invention.

BREVE DESCRIPTION DES DESSINS.

La **Figure 1** est un schéma synoptique d'une architecture logicielle d'une unité de calcul électronique selon l'invention.

La **Figure 2** illustre en détail le procédé de commande de l'unité de calcul électronique montrée sur la **Figure 1**.

Les **Figure 3, 4 et 5** illustrent respectivement des première, deuxième et troisième étapes du procédé de commande selon l'invention.

DESCRIPTION DU MODE DE REALISATION PREFERE DE L'INVENTION.

Dans le mode de réalisation préféré de l'invention, montré sur la **Figure 1**, l'unité de calcul électronique 1 de véhicule automobile dont il s'agit comporte un microprocesseur 2 comprenant une unité centrale de calcul 3, une unité de protection mémoire 4 et une interface d'entrées/ sorties 5.

L'unité de calcul électronique 1 acquiert des données en provenance de capteurs du véhicule et transmet des commandes à des équipements, ou en général échange des informations avec des périphériques, au moyen d'une interface de communication réseau 6 entre l'interface d'entrées/ sorties 5 et un réseau embarqué 7.

Pour ce faire, de manière connue en soi, l'unité de calcul électronique est commandée par des modules logiciels 8 exécutés sur le microprocesseur 2 sur lequel est implémenté un système d'exploitation 9 standardisé de type AUTOSAR, spécifiquement conçu pour les applications de l'automobile.

Les modules logiciels 8 développés en fonction des besoins des utilisateurs communiquent avec le système d'exploitation 9 via une première interface de programmes d'application 10 également standardisée, et communiquent avec les périphériques au moyens de premiers pilotes 11 appropriés fournis par les fabricants.

Le choix d'une version de base du système d'exploitation 9, telle que AUTOSAR BSW, permettrait de limiter les coûts mais ne permettrait pas à l'unité de calcul électronique 1 de satisfaire aux exigences de la norme ISO 26262 pour des degrés d'exigence supérieurs à QM, car cette version de base ne gère pas de mécanisme de protection mémoire.

Tout en étant basé sur un système d'exploitation 9 coté QM, le procédé de commande de l'unité de calcul électronique 1 selon l'invention, gère l'unité de

protection mémoire 4 du microprocesseur 2 comme le montre bien l'architecture logicielle de la **Figure 1**.

Un second pilote 12 spécifique à l'unité de protection mémoire 4 permet de contrôler le système d'exploitation 9 au moyen de ses connecteurs 13 si un second
5 gestionnaire d'évènements 14, spécifique également à l'unité de protection mémoire 4, rapporte un évènement de violation mémoire.

Une seconde interface de programmes d'application 15 permet à l'utilisateur de programmer l'unité de protection mémoire 4 et de rapporter la cause de la violation mémoire aux modules logiciels 8.

10 La **Figure 2** montre l'intégration de la seconde interface de programmes d'application 15, du second pilote 12 et du second gestionnaire d'évènements 14 dans le procédé de commande selon l'invention de l'unité de calcul électronique 1.

Au moment du démarrage 16 de l'unité de calcul électronique 1, un code de lancement 17 effectue le lancement du système d'exploitation 9 et une configuration
15 de l'unité de protection mémoire 4.

Pour ce faire une première fonction MPU_Init() de la seconde interface de programmes d'application 15 est appelée 18 afin d'effectuer une initialisation des registres de l'unité de protection mémoire 4.

La **Figure 3** montre une première séquence d'appel correspondante gérée
20 par le second gestionnaire d'évènements 14.

En cours d'exécution 19 de l'un des modules logiciels 8 de l'unité de calcul électronique 1 par le système d'exploitation 9, une seconde fonction MPU_SetTaskProtection() de la seconde interface de programmes d'application 15 est invoquée 20 au moment du lancement d'une tâche 21 en fournissant un premier
25 connecteur de début de tâche OS_PreTaskHook() 22 du système d'exploitation 9.

Comme le montre bien une seconde séquence d'appel représentée sur la **Figure 4**, celle-ci est également gérée par le second gestionnaire d'évènements 14.

Après déclenchement 23 de l'exécution de la tâche 21 et sa complétion 24, une première réinitialisation MPU_ResetTaskProtection() 25 de l'unité de protection
30 mémoire 4 est appelée en fournissant un premier connecteur de fin de tâche OS_PostTaskHook() 26 du système d'exploitation 9.

Les modules logiciels 9 dans les applications de l'automobile travaillant essentiellement dans un environnement temps réel, les vecteurs d'interruption sont également protégés dans le procédé de commande d'une unité de calcul
35 électronique 1 selon l'invention.

Dans ce but, une troisième fonction MPU_SetIsrProtection() de la seconde interface de programmes d'application 15 est invoquée 27 au moment du lancement d'un sous-programme d'interruption 28 en fournissant un second connecteur de début d'interruption OS_PrelsrHook() 29 du système d'exploitation 9.

5 Comme le montre bien une troisième séquence d'appel représentée sur la **Figure 5**, celle-ci est également gérée par le second gestionnaire d'évènements 14.

Après déclenchement 30 de l'exécution du sous-programme d'interruption 28 et sa complétion 31, une seconde réinitialisation MPU_ResetIsrProtection() 32 de l'unité de protection mémoire 4 est appelée en fournissant un second connecteur de fin d'interruption OS_PostIsrHook() 33 du système d'exploitation 9.

L'unité de protection mémoire 4 est configurée dynamiquement à chaque changement de contexte au cours du fonctionnement 19 de l'unité de calcul électronique 1. L'unité de protection mémoire 4 est initialisée en premier par la première fonction MPU_Init() 18 de la seconde interface de programmes d'application 15, ensuite les deuxième et troisième fonctions MPU_SetTaskProtection() 20, MPU_SetIsrProtection() 27 sont appelées pour initialiser les registres de l'unité de protection mémoire 4 avec des nouveaux droits d'accès pour chaque tâche 21 et sous-programme d'interruption 28, respectivement.

En ajoutant un tel mécanisme de protection mémoire 4, 12, 14, 15 en dehors du système d'exploitation 9 coté QM, le procédé selon l'invention permet d'obtenir un autre système d'exploitation équivalent 34 ayant un niveau d'exigence en termes de sécurité supérieur, tout en limitant les coûts.

Comme il va de soi, l'invention ne se limite pas au seul mode de réalisation préférentiel décrit ci-dessus.

25 Notamment, le système d'exploitation AUTOSAR BSW cité n'est qu'un exemple parmi d'autres de systèmes d'exploitations cotés QM pouvant être mis en œuvre dans un système embarqué. La seule restriction est que le système d'exploitation choisi soit suffisamment ouvert pour que les connecteurs de tâches et d'interruptions puissent être utilisés.

30 La description ci-dessus porte implicitement sur une unité de calcul électronique 1 comprenant un seul microprocesseur 2 avec une seule unité centrale de calcul 3. Une description similaire pourrait porter sur une unité de calcul électronique 1 comprenant des co-processeurs et/ ou, un ou des microprocesseurs multi-coeurs, notamment dans des architectures matérielles ou logicielles

redondantes où les questions de protection des données/ instructions dans des mémoires partagées sont particulièrement importantes.

Il est considéré que le microprocesseur 2 comprend une unité de protection mémoire ou MPU 4. L'homme de métier connaît des microprocesseurs, tels que le
5 microprocesseur de référence MPC5567, déjà cité, qui comporte une unité de gestion de la mémoire ou MMU. Comme déjà indiqué, une MMU est une MPU 4 avec une fonction supplémentaire de translation des adresses, mais reste, pour les fonctions de protection mémoire, une MPU 4. La présente description pourrait donc s'appliquer sans modification à une unité de calcul électronique 1 comprenant un
10 microprocesseur 2 muni d'une MMU.

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 de commande d'une unité de calcul électronique (1) de véhicule automobile du type de ceux basés sur un premier système d'exploitation (9) conforme à un premier niveau d'exigence en termes de sécurité de la norme ISO 26262, une première interface de programmes d'application (10), un premier gestionnaire d'évènements d'un environnement temps réel et des premiers pilotes (11) de périphériques exécutés par une unité centrale de calcul (3) d'un microprocesseur (2) comprenant en outre une unité de protection mémoire (4), caractérisé en ce qu'il met en œuvre en outre une seconde interface de programmes d'application (15), un second gestionnaire d'évènements (14) et un second pilote (12) de périphérique spécifiques à ladite unité de protection mémoire (4) et distincts dudit premier système d'exploitation (9).

2) Procédé de commande d'une unité de calcul électronique de véhicule automobile selon la revendication 1, caractérisé en ce que ledit premier système d'exploitation (9), ledit second gestionnaire d'évènements (14) et ledit second pilote (11) sont équivalents à un second système d'exploitation (34) conforme à un second niveau d'exigence en termes de sécurité de la norme ISO 26262 supérieur audit premier niveau d'exigence en termes de sécurité.

3) Procédé de commande d'une unité de calcul électronique (1) de véhicule automobile selon la revendication 2, caractérisé en ce que ledit premier niveau d'exigence en termes de sécurité est coté QM.

4) Procédé de commande d'une unité de calcul électronique (1) de véhicule automobile selon l'une quelconque des revendications 1 à 3 précédentes, caractérisé en ce que ledit second pilote (12) utilise des premiers connecteurs de tâches (13; 22, 26) et des seconds connecteurs d'interruptions (13; 29, 33) dudit premier système d'exploitation (9).

5) Procédé de commande d'une unité de calcul électronique (1) de véhicule automobile selon la revendication 4, caractérisé en ce qu'il comprend une première étape appelant une première fonction (18) de ladite seconde interface de

programmes d'application (15) initialisant au moins un registre de ladite unité de protection mémoire (4).

5 **6)** Procédé de commande d'une unité de calcul électronique (1) de véhicule automobile selon la revendication 5, caractérisé en ce qu'il comprend en outre une deuxième étape appelant une deuxième fonction (20) de ladite seconde interface de programmes d'application (15) initialisant une protection des tâches (21).

10 **7)** Procédé de commande d'une unité de calcul électronique (1) de véhicule automobile selon la revendication 6, caractérisé en ce qu'il comprend en outre une troisième étape appelant une troisième fonction (27) de ladite seconde interface de programmes d'application (15) initialisant une protection des interruptions (28).

15 **8)** Procédé de commande d'une unité de calcul électronique (1) de véhicule automobile selon la revendication 7, caractérisé en ce que ledit second gestionnaire d'évènements (14) transmet à ladite seconde interface de programmes d'application (15) des violations de ladite protection des tâches (21) et de ladite protection des interruptions (28).

20 **9)** Unité de calcul électronique (1) de véhicule automobile apte à sa mise en œuvre du procédé de commande selon l'une quelconque des revendications 1 à 8 précédentes, ladite unité de calcul électronique (1) étant du type de celles comprenant un microprocesseur (2) comportant au moins une unité centrale de calcul (3) et une unité de protection mémoire (4) associées à au moins une mémoire
25 de programme, au moins une mémoire de données, et à au moins une interface d'entrées/ sorties (5), ladite au moins une mémoire de programme stockant des premiers codes informatiques représentatifs d'un système d'exploitation (9) conforme à un niveau d'exigence en termes de sécurité coté QM de la norme ISO 26262, d'une première interface de programmes d'application (10), d'un premier
30 gestionnaire d'évènements d'un environnement temps réel et de premiers pilotes (11) de périphériques aptes à être connectés à ladite au moins une interface d'entrées/ sorties (5), exécutés par ladite au moins une unité centrale de calcul (3), caractérisée en ce que ladite au moins une mémoire de programme stocke en outre des seconds codes informatiques représentatifs d'une seconde interface de
35 programmes d'application (15), d'un second gestionnaire d'évènements (14) et d'un

second pilote (12) spécifiques à ladite unité de protection mémoire (4) distincts desdits premiers codes informatiques (9, 10, 11).

- 10)** Véhicule automobile, caractérisé en qu'il comprend au moins une unité de calcul
- 5 électronique (1) selon la revendication 9 précédente.

1/5

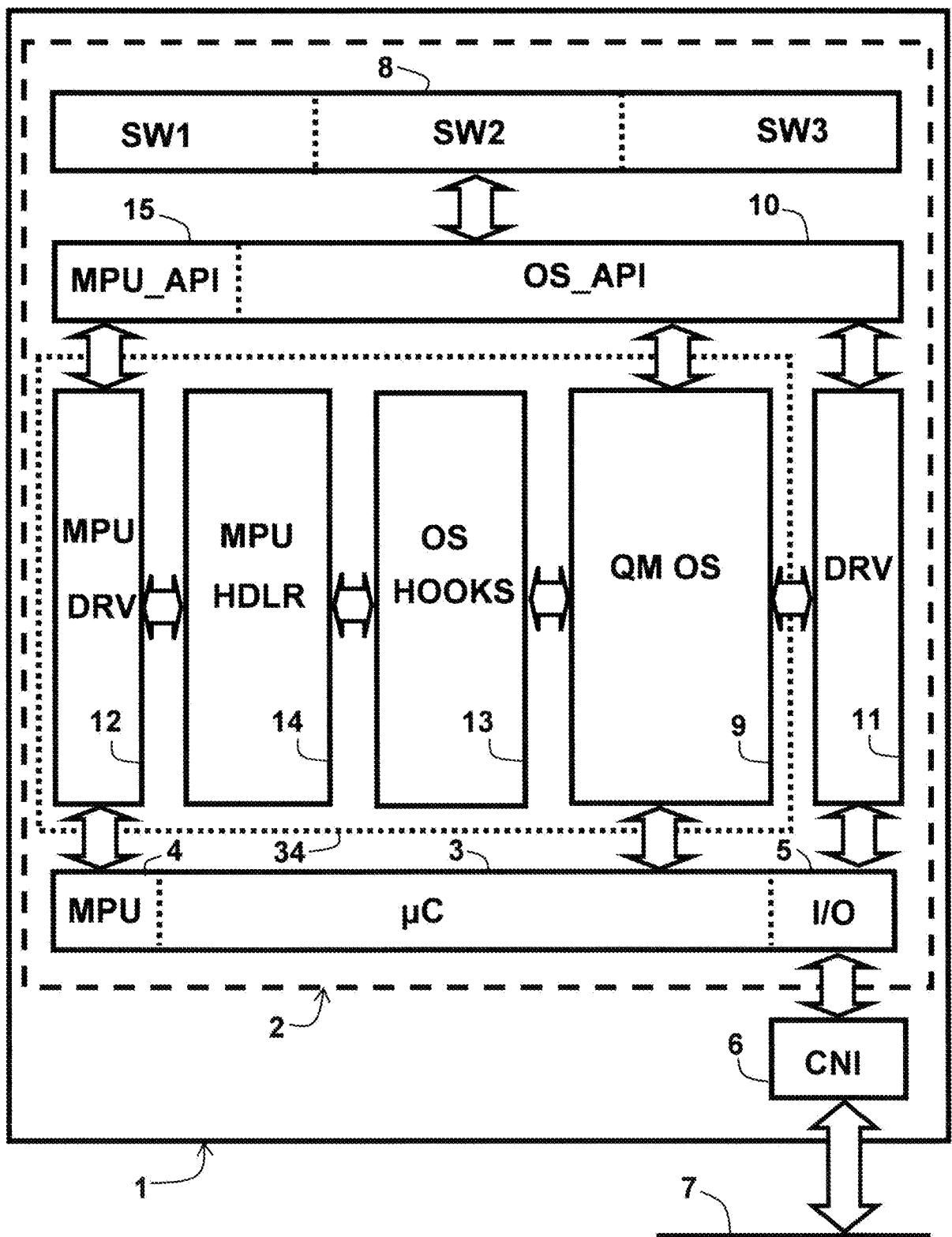


FIG. 1

2/5

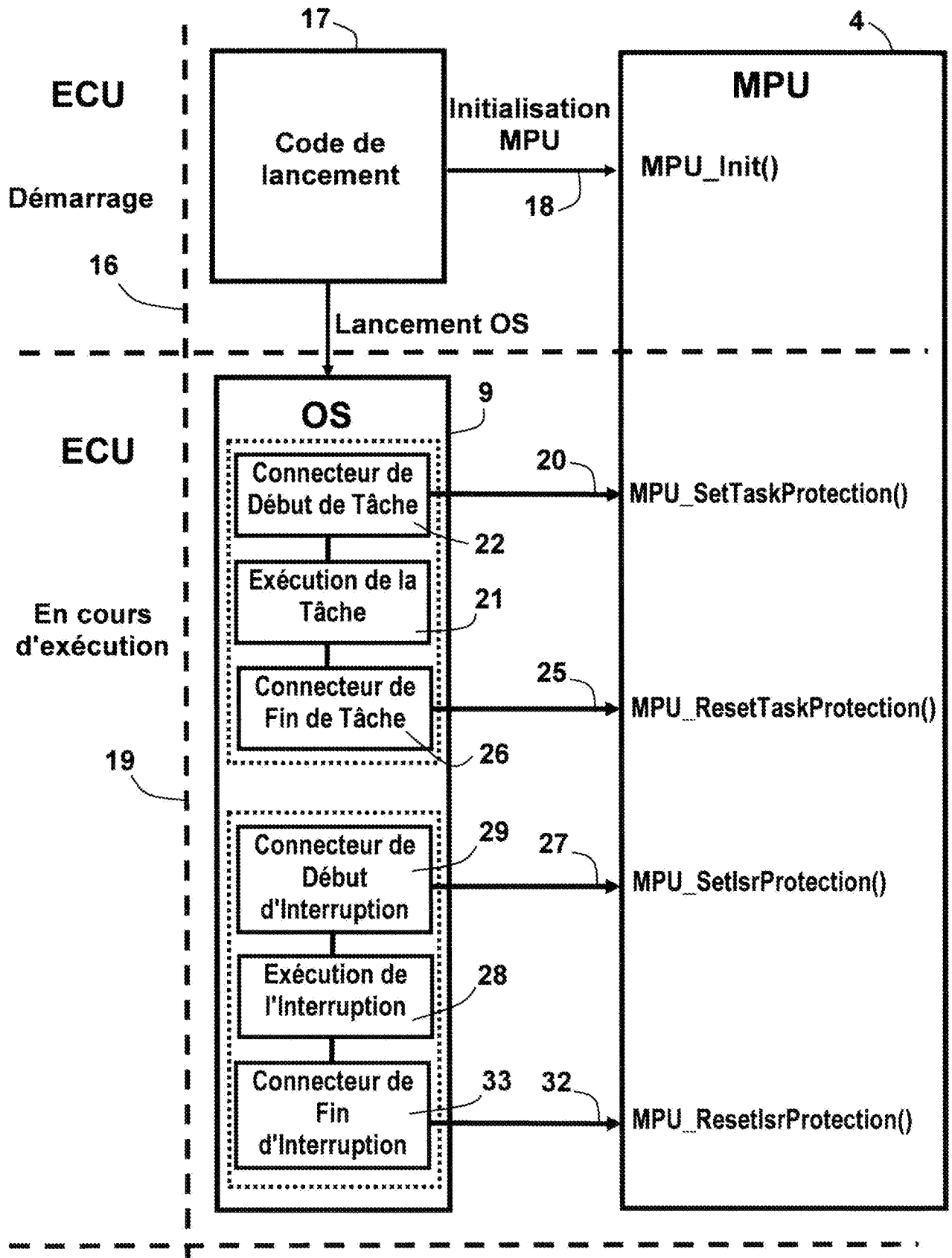


FIG. 2

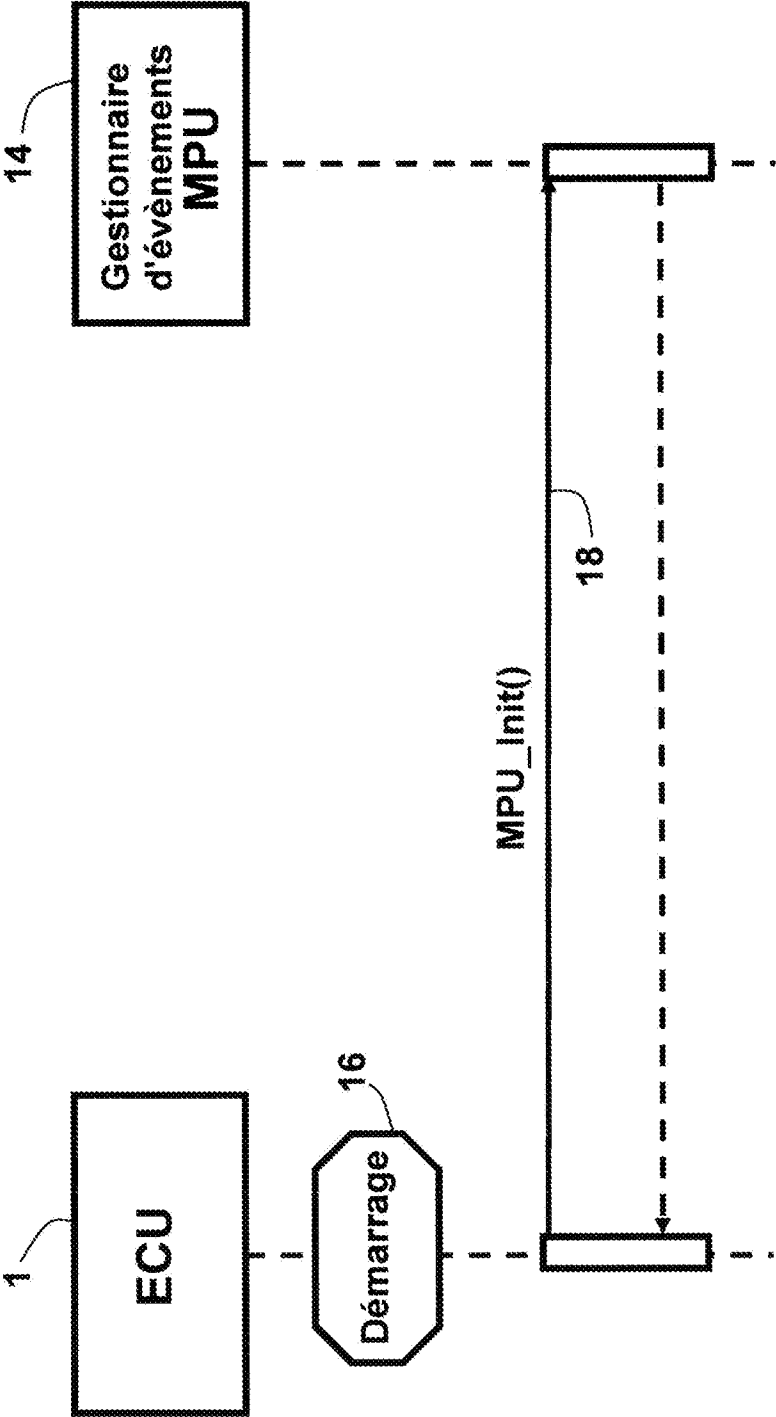


FIG. 3

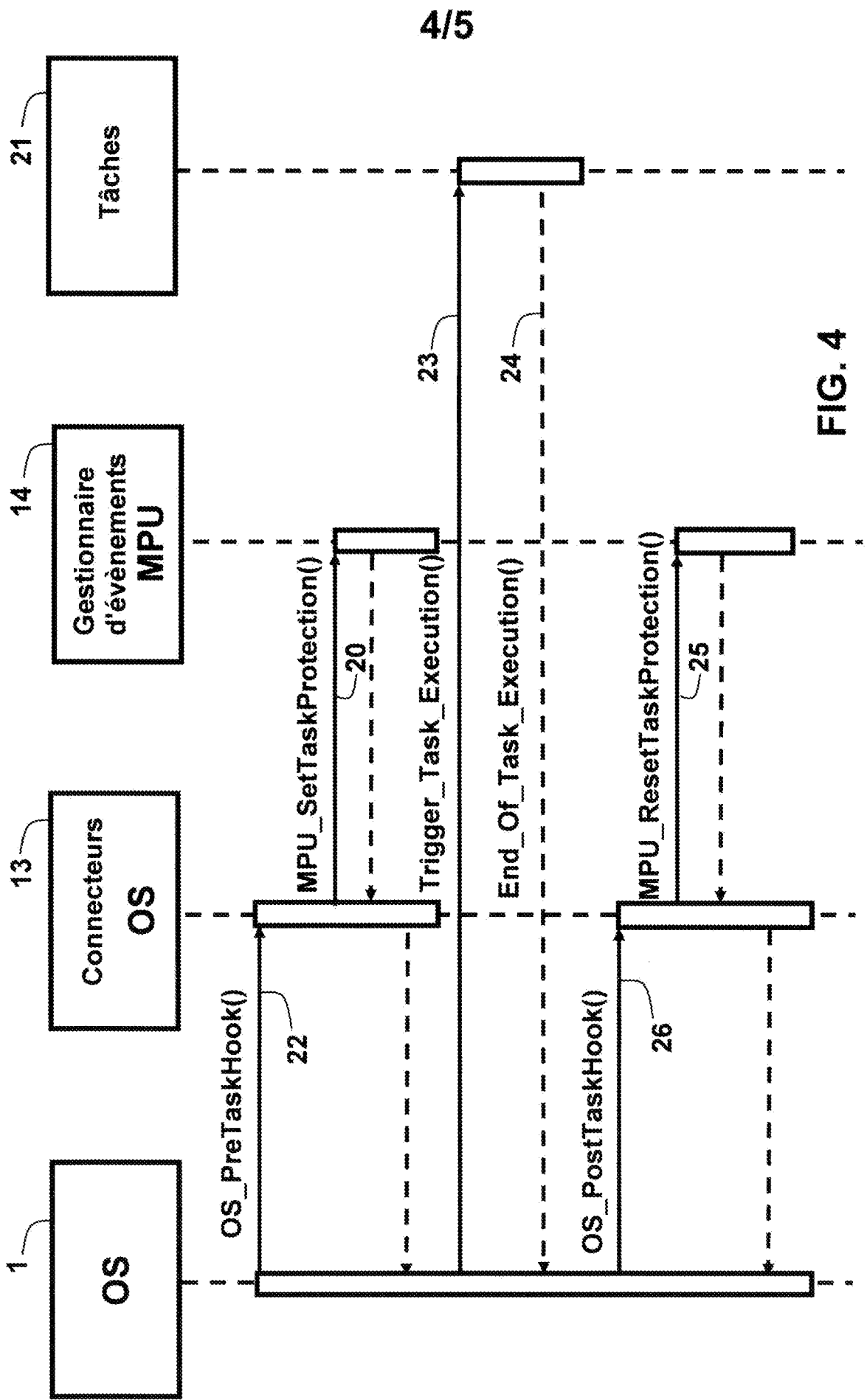
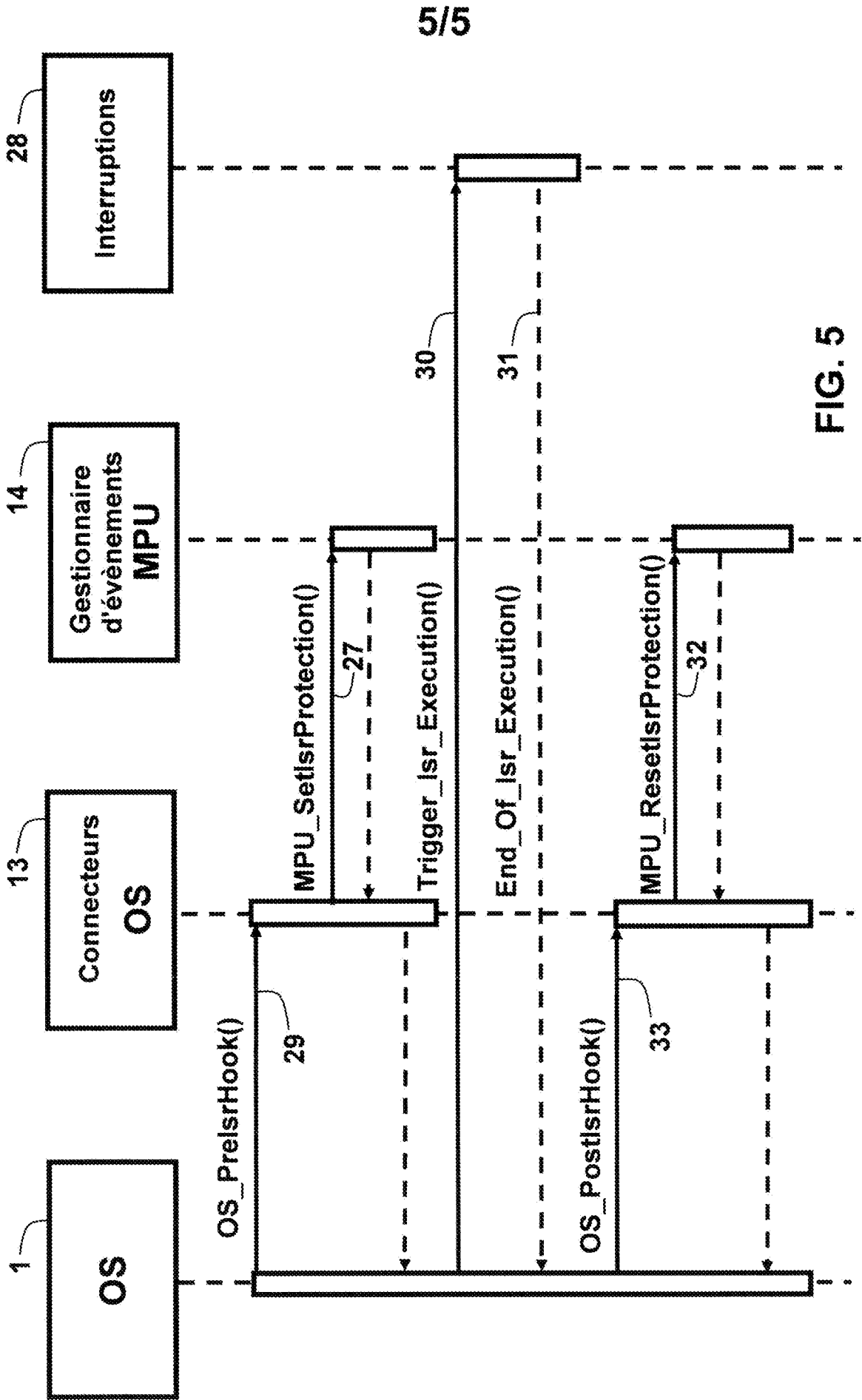


FIG. 4



INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/051692

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F9/54 G06F13/16
ADD.

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)
G06F

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	David Haworth ET AL: "Freedom from Interference forAUTOSAR-based ECUs: a partitioned AUTOSAR stack", Automotive - Safety and Security 2012, 14 November 2012 (2012-11-14), pages 85-98, XP055270474, Retrieved from the Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.646.6783&rep=rep1&type=pdf [retrieved on 2016-05-03] the whole document ----- -/-	1-10



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

10 October 2016

Date of mailing of the international search report

20/10/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Michel, Thierry

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/051692

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ZUEPKE ALEXANDER ET AL: "AUTOBEST: a united AUTOSAR-OS and ARINC 653 kernel", 21ST IEEE REAL-TIME AND EMBEDDED TECHNOLOGY AND APPLICATIONS SYMPOSIUM, IEEE, 13 April 2015 (2015-04-13), pages 133-144, XP032777219, DOI: 10.1109/RTAS.2015.7108435 the whole document -----	1-10
A	Ludovic Pintard ET AL: "Using Fault Injection to Verify an AUTOSAR Application According to the ISO 26262", Journal Articles from SAE 2015 World Congress & Exhibition, 14 April 2015 (2015-04-14), pages 1-13, XP055270479, DOI: 10.4271/2015- Retrieved from the Internet: URL:https://hal.inria.fr/hal-01221422/document [retrieved on 2016-05-03] the whole document -----	1-10

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2016/051692

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G06F9/54 G06F13/16 ADD.		
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) G06F		
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	David Haworth ET AL: "Freedom from Interference forAUTOSAR-based ECUs: a partitioned AUTOSAR stack", Automotive - Safety and Security 2012, 14 novembre 2012 (2012-11-14), pages 85-98, XP055270474, Extrait de l'Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.646.6783&rep=rep1&type=pdf [extrait le 2016-05-03] le document en entier ----- -/--	1-10
☒ 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 10 octobre 2016		Date d'expédition du présent rapport de recherche internationale 20/10/2016
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Michel, Thierry

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	ZUEPKE ALEXANDER ET AL: "AUTOBEST: a united AUTOSAR-OS and ARINC 653 kernel", 21ST IEEE REAL-TIME AND EMBEDDED TECHNOLOGY AND APPLICATIONS SYMPOSIUM, IEEE, 13 avril 2015 (2015-04-13), pages 133-144, XP032777219, DOI: 10.1109/RTAS.2015.7108435 le document en entier -----	1-10
A	Ludovic Pintard ET AL: "Using Fault Injection to Verify an AUTOSAR Application According to the ISO 26262", Journal Articles from SAE 2015 World Congress & Exhibition, 14 avril 2015 (2015-04-14), pages 1-13, XP055270479, DOI: 10.4271/2015- Extrait de l'Internet: URL:https://hal.inria.fr/hal-01221422/document [extrait le 2016-05-03] le document en entier -----	1-10