

19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

11) N° de publication : **2 930 828**
(à n'utiliser que pour les
commandes de reproduction)

21) N° d'enregistrement national : **08 04504**

51) Int Cl⁸ : G 06 F 9/45 (2006.01), G 06 F 9/40

12)

DEMANDE DE BREVET D'INVENTION

A1

22) Date de dépôt : 07.08.08.

30) Priorité :

43) Date de mise à la disposition du public de la demande : 06.11.09 Bulletin 09/45.

56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

60) Références à d'autres documents nationaux apparentés :

71) Demandeur(s) : CONTINENTAL AUTOMOTIVE FRANCE Société par actions simplifiée — FR et CONTINENTAL AUTOMOTIVE GMBH — DE.

72) Inventeur(s) : MESTRIE CHRISTOPHE, POITEVIN PIERRE, RAYNAL BENOIT et BAUER RUDOLF.

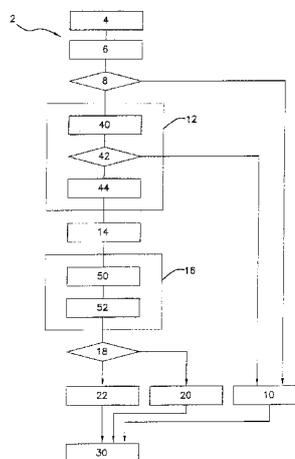
73) Titulaire(s) :

74) Mandataire(s) :

54) PROCÉDE DE VALIDATION DE LA MODIFICATION D'UN PROGRAMME INSTALLE POUR UNE UNITE DE COMMANDE ELECTRONIQUE D'UN VEHICULE AUTOMOBILE.

57) Le procédé de validation de la modification d'un programme installé pour une unité de commande électronique d'un véhicule automobile par la reprogrammation d'un certain nombre de modules logiciels comprend une étape de réception (4) d'un fichier (17) de type ODX concernant les nouveaux modules logiciels de reprogrammation.

Le procédé comprend en outre les étapes de réception (40) des informations de vérification concernant l'ensemble des modules installés sous la forme d'un tableau de vérification (15), de mise à jour (14) du tableau de vérification (15) à l'aide du fichier ODX (17), et de vérification de la cohérence interne (16) du nouveau programme sur la base du tableau de vérification (15) mis à jour.



FR 2 930 828 - A1



L'invention se rapporte à un procédé de modification d'un programme installé pour une unité de commande électronique d'un véhicule automobile.

Classiquement, une unité de commande électronique dénommée en anglais ECU (acronyme pour "Engine Control Unit") d'un véhicule automobile comprend un microprocesseur et une mémoire de stockage d'un programme apte à être exécuté par le microprocesseur.

Le programme comprend plusieurs modules logiciels parmi lesquelles des modules de lancement, des données de calibration, et des modules d'applications.

Classiquement, lorsqu'un programme installé dans l'unité de commande est modifié, l'outil de reprogrammation (le terme "outil" désignant ici un logiciel et son support physique permettant ladite reprogrammation) reçoit le code à reprogrammer ainsi que les emplacements de la mémoire dans lesquels il doit placer ledit code à reprogrammer.

Un inconvénient des procédés de modification classiques est le fait qu'ils ne garantissent pas la cohérence du nouveau programme formé par les nouveaux modules de remplacement et les modules précédents restants, même si toutes les vérifications, dénommées en anglais « checksum », de chaque module logiciel du nouveau programme d'ensemble de l'ECU sont détectées satisfaisantes.

Un défaut de cohérence pouvant entraîner un dysfonctionnement intolérable de l'ECU, il est alors nécessaire de refaire une batterie de tests longs en temps et coûteux avant la livraison du matériel reprogrammé.

Le but de l'invention est de s'affranchir de la nécessité de refaire cette batterie de tests longs et coûteux.

A cet effet, l'invention a pour objet un procédé de validation de la modification d'un programme installé pour une unité de commande électronique d'un véhicule automobile en un nouveau programme, le programme installé comprenant une pluralité de modules logiciels installés, le nouveau programme comprenant de nouveaux modules de remplacement d'un certain nombre desdits modules installés et des modules installés demeurant inchangés, le procédé comprenant une étape consistant à recevoir des informations fournies dans un fichier de type ODX (acronyme anglais pour "Open Diagnostic data eXchange" qui est une norme de description formelle des informations de diagnostic des calculateurs véhicule) concernant les nouveaux modules logiciels, le procédé étant remarquable en ce qu'il comprend les étapes consistant à :

- recevoir des informations de vérification concernant l'ensemble des modules installés sous la forme d'un tableau de vérification,
- mettre à jour le tableau de vérification en remplaçant les informations de vérification des modules installés destinés à être remplacés par les informations du fichier ODX concernant les nouveaux modules de remplacement, et
- vérifier la cohérence interne du nouveau programme sur la base du tableau de vérification mis à jour.

Le fichier de type ODX contient des informations pertinentes concernant les nouveaux modules logiciels actuels de remplacement, notamment les tables de correspondance d'adresse, les références, les cohérences entre variables... Ce fichier de type ODX est généré en même temps que les modules logiciels sont compilés et est pris comme paramètre d'entrée par l'outil de validation mettant en œuvre le procédé de validation afin de faire l'analyse de cohérence.

Suivant des modes particuliers de réalisation, le procédé de modification d'un programme comporte l'une ou plusieurs des caractéristiques suivantes :

- pour un programme installé ou un nouveau programme, les informations de vérification comprennent les références d'identification de chaque module présent dans le programme, une référence d'identification comprenant un code d'identité et une référence de version, pour chaque module un paramètre booléen d'état de validité, des paramètres de cohérence et des tables de correspondance d'adresses.
- pendant la mise à jour du tableau de vérification, les paramètres d'état de validité des nouveaux modules sont mis dans un état valide.
- l'étape de vérification de cohérence interne du nouveau programme comprend une étape de vérification du paramètre d'état de validité de chaque module répertorié par le code d'identité du module.
- l'étape de vérification de cohérence interne du nouveau programme comprend une étape de vérification de cohérence élémentaire de chaque module du nouveau programme avec un certain nombre d'autres modules fondés sur les paramètres de cohérence et les tables de correspondance d'adresses.
- le tableau de vérification des modules installés est fourni par l'unité de commande électronique ECU pendant l'exécution d'un module logiciel de recherche intégré dans un module logiciel de lancement constructeur du

programme installé, le module de lancement étant modifiable seulement par le constructeur et faisant partie du programme installé, et étant activable par un outil informatique distinct de l'ECU.

L'invention sera mieux comprise à la lecture de la description de deux formes de réalisation qui vont suivre, données uniquement à titre d'exemple et faite en se référant aux dessins sur lesquels :

- la Figure 1 est un ordinogramme du procédé selon l'invention,
- la Figure 2 est une vue d'un exemple des fichiers manipulés au cours de la mise en œuvre du procédé décrit à la figure 1.

En référence à la figure 1, le procédé 2 décrit concerne la validation d'un programme informatique complexe qui vient d'être modifié, ce programme complexe étant destiné ici à la mise en œuvre d'une unité de commande électronique ECU d'un véhicule automobile et incluant la gestion de tâches critiques, voire de sécurité pour la bonne marche du véhicule.

Le programme à installer qui va être modifié est ici appelé nouveau programme.

Le programme installé avant modification comprend une pluralité de modules logiciels installés parmi lesquels :

- un module de lancement émis par le constructeur fournisseur de l'ECU et modifiable seulement par ce dernier,
- un module de lancement émis par le client correspondant à une personnalisation de certaines tâches non sécuritaires de l'ECU souhaitées par le client,
- divers modules d'application permettant de faire fonctionner le moteur à combustion interne de manière adéquate, parmi lesquels par exemple un module appelé « Volcano » destiné à une interface de communication particulière, et
- divers fichiers de données de calibration associés selon le cas à un module de lancement ou un module d'application.

Le nouveau programme comprend un certain nombre de nouveaux modules remplaçant des modules installés de version plus ancienne et des modules installés qui demeurent inchangés.

Le procédé de validation 2 est mis en œuvre par un outil de validation comportant un ordinateur, distinct de l'ECU, ayant une structure classique de microprocesseur avec

une mémoire, apte à communiquer et échanger des données avec l'ECU y compris commander l'activation de certains modules logiciels du programme installé sur l'ECU.

Le procédé de validation 2 comprend un ensemble d'étapes 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 30.

5 Dans une première étape 4, l'outil de validation reçoit des informations de cohérence associées à l'ensemble des nouveaux modules logiciels de remplacement et présentés sous la forme d'un fichier de type ODX, ODX désignant un format connu d'échanges de données d'identification et de cohérence de produits logiciels normalisé par le consortium industriel ASAM (acronyme anglais pour "Association for
10 Standardisation of Automation and Measuring systems"). Pendant cette étape, les nouveaux modules logiciels de remplacement n'ont pas été installés dans l'ECU.

Par exemple, ces informations sont constituées par une clé d'authentification d'un projet entre un client et le constructeur automobile, la référence d'identification d'un module incluant un code commun d'identité et un code de numéro de version, un code
15 référence de compatibilité entre deux modules logiciels, par exemple entre celui d'un module de lancement client et un module de lancement constructeur.

Dans une étape suivante 6, l'outil de validation active le module installé de lancement émis par le constructeur et modifiable seulement par ce dernier.

Dans une étape 8, l'activité du module installé de lancement est testée.

20 Si le module installé de lancement n'est pas détecté comme fonctionnant alors un message est émis dans une étape 10 indiquant que la vérification de cohérence interne du nouveau programme n'est pas possible du fait de l'inactivité du module logiciel de lancement installé.

Dans le cas d'un test réussi de détection de fonctionnement du module de
25 lancement installé, alors dans une étape 12, des informations de vérification sont fournies par l'ECU et reçues par l'outil de validation concernant l'ensemble des modules installés sous la forme d'un tableau de vérification. Ce tableau de vérification est stocké dans la mémoire de l'outil de validation.

Les informations de vérification comprennent notamment les références
30 d'identification de chaque module présent dans le programme, une référence d'identification comprenant un code d'identité et une référence de version, pour chaque module un paramètre booléen d'état de validité, des paramètres de cohérence et des tables de correspondance d'adresses.

Par exemple, le tableau de vérification concernant les modules logiciels installés contient les informations suivantes :

- une clé d'authentification d'un projet entre un client et le constructeur automobile,
- 5 - la référence d'identification du module de lancement du constructeur,
- le code référence de compatibilité entre le module de lancement client et le module de lancement constructeur,
- un masque de mise en relation des données de vérification entre le module de lancement du constructeur et le module de lancement du client,
- 10 - la référence d'identification du module de lancement du client,
- un masque de mise en relation des données de vérification entre le module de lancement du constructeur et un premier module d'application dénommé « ECU_SW »,
- le paramètre booléen d'état de validité du module de lancement client représentatif de l'état de présence du module au sein du programme d'ensemble,
- 15 - la référence d'identification du premier module d'application dénommé « ECU_SW »,
- un masque de mise en relation des données de vérification entre le premier module d'application dénommé « ECU_SW » et un module contenant des données de calibration,
- 20 - le paramètre booléen d'état de validité du module d'application dénommé « ECU_SW » représentatif de l'état de présence du module au sein du programme d'ensemble,
- 25 - un masque de mise en relation des données de vérification entre le premier module d'application dénommé « ECU_SW » et un deuxième module d'application « Volcano » dénommé « VCF_SW »,
- la référence d'identification du module contenant des données de calibration,
- le paramètre booléen d'état de validité du module contenant des données de calibration,
- 30 - la référence d'identification du deuxième module d'application « Volcano » dénommé « VCF_SW »,

- le paramètre booléen d'état de validité du deuxième module d'application « Volcano » dénommé « VCF_SW ».

Dans une étape 14, le tableau de vérification fournie à l'étape 12 est mis à jour au sein de l'outil de validation en remplaçant les informations de vérification des modules installés destinés à être reprogrammés par les informations du fichier de format ODX concernant les nouveaux modules de remplacement fournies à l'étape 4.

En outre, un champ supplémentaire est créé dans le tableau de vérification mis à jour, destiné à recevoir du fichier ODX fourni à l'étape 4 la clé d'authentification du projet entre le client et le constructeur de l'ECU.

10 La figure 2 illustre un exemple de mise à jour d'un tableau de vérification 15 fourni à l'étape 12, contenant les informations décrites à titre d'exemple ci-dessus avec la mise en correspondance des champs modifiés par le fichier ODX 17 représentée par des flèches.

Le tableau de vérification 15 mis à jour est représenté à gauche de la figure 2 tandis que le fichier de type ODX 17 est représenté à droite de la figure 2.

15 Le champ du fichier ODX 17 contenant la clé d'authentification du projet entre le client et le constructeur est dénommé « sig_si_key_nr ». Son contenu est transféré dans le champ supplémentaire dénommé « sig_si_key_nr[ODX] ».

Le champ du fichier ODX 17 contenant le code référence de compatibilité entre le module de lancement client et le module de lancement constructeur est dénommé
20 « c_sie_boot_ref ». Son contenu est transféré dans le champ dénommé également « c_sie_boot_ref » du tableau de vérification 15 et remplace le code référence de compatibilité entre le module installé de lancement client et le module installé de lancement constructeur.

Le champ du fichier ODX 17 contenant la référence d'identification du nouveau module de lancement du client est dénommé « c_boot_ref ». Son contenu est transféré
25 dans le champ dénommé également « c_boot_ref » et remplace la référence d'identification du module installé de lancement du client.

Le transfert de la référence d'identification du nouveau module de lancement du client s'accompagne d'une mise à l'état présent du champ du tableau de vérification
30 contenant le paramètre booléen d'état de validité du module de lancement client, ce champ étant dénommé « c_boot_validity ».

En revenant à la figure 1, le procédé de validation se poursuit par une étape 16 dans laquelle la cohérence interne du nouveau programme à installer est vérifiée en se

fondant sur le tableau de vérification mis à jour au sein de l'outil de validation, comme par exemple celui décrit à la figure 2.

5 Ensuite, dans une étape 18 le résultat de cohérence est testé. Dans le cas où il n'existe pas de cohérence interne du nouveau programme, l'outil de validation affiche cet état de non cohérence dans une étape 20. Dans le cas où il existe une cohérence interne du nouveau programme, l'outil de validation affiche cet état de cohérence dans une étape 22.

10 Dans une étape 30, l'outil de validation autorise la reprogrammation de l'ECU lorsqu'une cohérence interne est détectée dans l'étape 22 et interdit la reprogrammation en un nouveau programme dans les autres cas c'est à dire lorsque les étapes 10 ou 20 sont activées.

L'étape 12 comprend une suite d'étapes 40, 42 et 44.

Dans une étape 40, un module logiciel de recherche, intégré dans le module logiciel installé de lancement du constructeur, est activé par l'outil de validation.

15 Dans une étape 42, l'activation du module de recherche est testée.

Si le module de recherche n'est pas détecté comme fonctionnant alors un message est émis dans l'étape 10 indiquant que la vérification de cohérence interne du nouveau programme n'est pas possible du fait de l'inactivité du module logiciel de recherche.

20 Dans une étape 44, le module de recherche extrait les informations de vérification concernant l'ensemble des modules installés et les rassemble dans un tableau de vérification concernant l'ensemble des modules d'origine.

25 L'étape 16 de vérification de la cohérence du nouveau programme comprend une étape 50 de vérification de la présence de tous les modules logiciels nécessaires au nouveau programme et une étape suivante 52 de vérification de cohérence élémentaire de chaque module du nouveau programme avec un certain nombre d'autres modules du programme en fonction de paramètres de cohérence et de tables de correspondance d'adresses.

30 Dans l'étape 50, le paramètre d'état sous la forme d'un booléen de présence de chaque module répertorié par son code identifiant dans le tableau de vérification mis à jour est testé.

Si le paramètre d'état de présence du module attendu est à l'état présent, alors le test est réussi pour ce module. Dans le cas contraire il est signalé l'absence du module et l'impossibilité de reprogrammer le programme installé en un nouveau programme.

Par exemple supposons que le module installé contenant les données de calibration soit en réalité absent du programme installé alors qu'il y est nécessaire et qu'un nouveau module de données de calibration n'apparaît pas dans le fichier ODX 17 de reprogrammation, alors la reprogrammation en un nouveau programme est empêchée et l'anomalie d'absence est signalée dans l'étape 20.

Il est à remarquer que lorsqu'un nouveau module vient à pallier l'absence d'un module installé dans le programme installé, la mise à l'état présent du paramètre d'état correspondant est effectuée à l'étape 14 de mise à jour du tableau de vérification.

Dans l'étape 52, il est vérifié tout d'abord si la clé d'authentification du projet entre le client et le constructeur transférée dans le champ supplémentaire dénommé « sig_si-key_nr[ODX] » du tableau mis à jour et la clé d'origine d'authentification du projet entre le client et le constructeur contenue dans le champ dénommé « sig_si-key_nr » du même tableau sont identiques.

Si les clés d'authentification sont identiques alors l'étape 52 est poursuivie par la comparaison deux par deux des informations des divers modules entre eux lorsqu'un masque autorise de procéder à une telle comparaison entre deux modules sélectionnés.

Dans l'exemple de la figure 2, les vérifications suivantes seront effectuées au moyen de masques de comparaison pour les couples de modules suivant :

- le module de lancement constructeur et le module de lancement client,
- le module de lancement client et le module de la première application,
- le module de la première application et le module comprenant les données de calibration,
- le module comprenant les données de calibration et module de la deuxième application.

Avantageusement, le procédé de validation 2 de la reprogrammation et l'outil de validation qui le met en œuvre permet de vérifier la validité du nouveau programme d'ensemble simplement et rapidement sans avoir à recommencer la batterie de tests initiaux déjà effectués pour la validation du programme installé.

En variante, le programme installé est enregistré dans une mémoire distincte de l'unité de commande électronique ECU.

REVENDEICATIONS

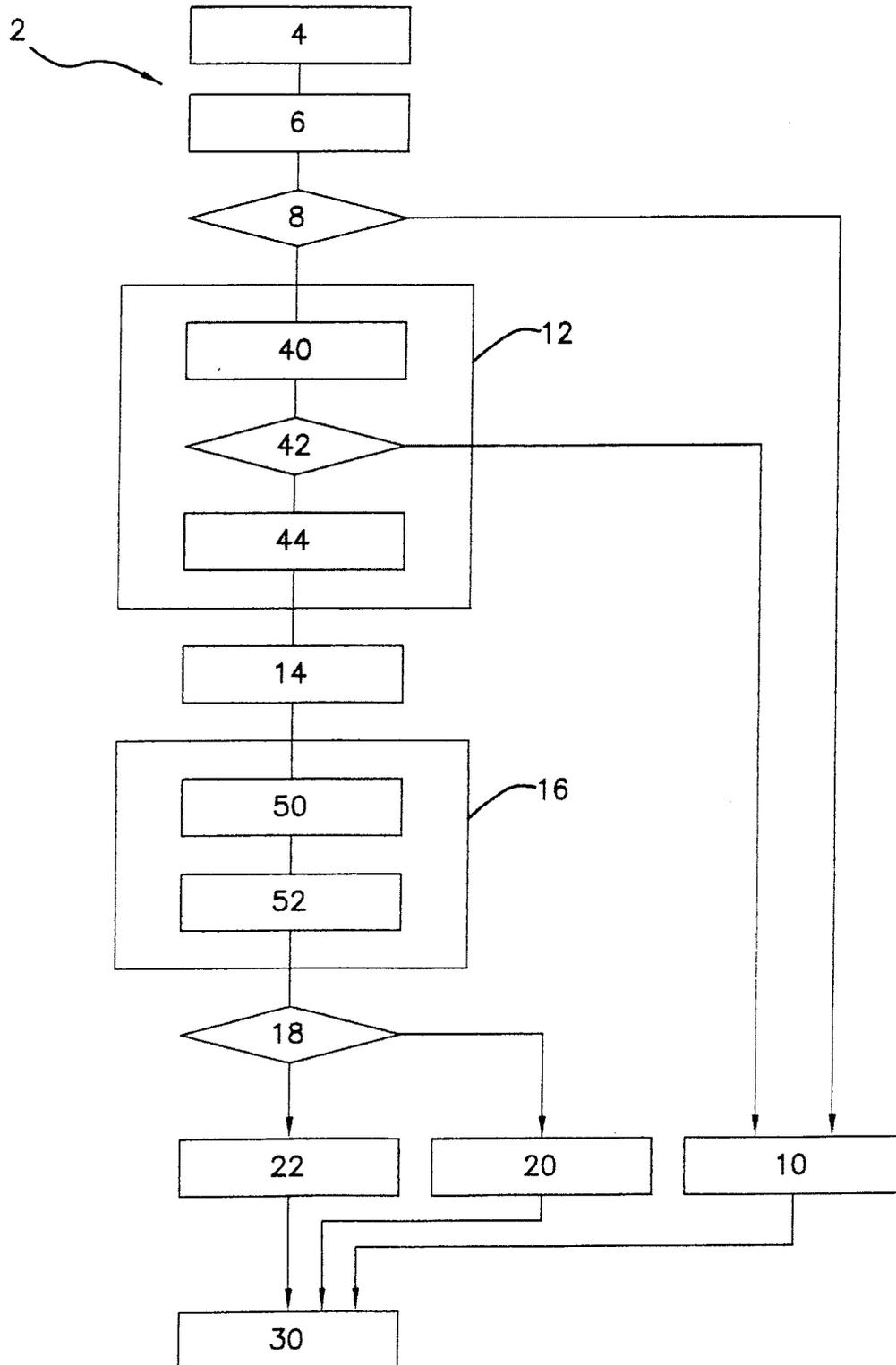
1. Procédé de validation de la modification d'un programme installé dans une unité de commande électronique ECU d'un véhicule automobile en un nouveau programme, le programme installé comprenant une pluralité de modules logiciels installés, le nouveau programme comprenant de nouveaux modules de remplacement d'un certain nombre desdits modules installés et des modules installés demeurant inchangés, le procédé mis en œuvre par un ordinateur comprenant une étape consistant à recevoir (14) des informations fournies dans un fichier de type ODX (17) concernant les nouveaux modules logiciels, caractérisé en ce qu'il comprend les étapes consistant à ce que :
- 10 - l'ordinateur reçoit (12) de l'unité de commande ECU des informations de vérification concernant l'ensemble des modules installés sous la forme d'un tableau de vérification (15),
 - l'ordinateur met à jour (14) le tableau de vérification (15) en remplaçant les informations de vérification des modules installés destinés à être remplacés par les informations du fichier ODX (17) concernant les nouveaux modules de remplacement, et
 - 15 - l'ordinateur vérifie (16) la cohérence interne du nouveau programme sur la base du tableau de vérification (15) mis à jour,
 - dans le cas où le nouveau programme est vérifié comme étant cohérent, l'ordinateur autorise (30) la reprogrammation de l'ECU.
- 20 2. Procédé de modification d'un programme selon la revendication 1, caractérisé en ce que pour un programme installé ou un nouveau programme, les informations de vérification comprennent les références d'identification de chaque module présent dans le programme, une référence d'identification comprenant un code d'identité et une référence de version, pour chaque module un paramètre booléen d'état de validité, des paramètres de cohérence et des tables de correspondance d'adresses.
- 25 3. Procédé de modification d'un programme selon l'une des revendications 1 et 2, caractérisé en ce que, pendant la mise à jour du tableau de vérification, les paramètres d'état de validité des nouveaux modules sont mis dans un état valide.
4. Procédé de modification d'un programme selon l'une des revendications 1 à 3, caractérisé en ce que l'étape de vérification de cohérence interne (16) du nouveau programme comprend une étape (50) de vérification du paramètre d'état de validité de chaque module répertorié par le code d'identité du module.
- 30 5. Procédé de modification d'un programme selon l'une des revendications 1 à 4, caractérisé en ce que l'étape de vérification de cohérence interne (16) du nouveau

programme comprend une étape de vérification de cohérence élémentaire (52) de chaque module du nouveau programme avec un certain nombre d'autres modules fondé sur les paramètres de cohérence et les tables de correspondance d'adresses.

6. Procédé de modification d'un programme selon l'une des revendications 1 à 5, caractérisé en ce que le tableau de vérification (15) des modules installés est fourni par l'unité de commande électronique ECU pendant l'exécution (40) d'un module logiciel de recherche intégré dans un module logiciel de lancement constructeur du programme installé, le module de lancement étant modifiable seulement par le constructeur et faisant partie du programme installé, et étant activable par un outil informatique distinct de l'ECU.
7. Système de validation de la modification d'un programme installé dans une unité de commande électronique ECU d'un véhicule automobile en un nouveau programme, le programme installé comprenant une pluralité de modules logiciels installés, le nouveau programme comprenant de nouveaux modules de remplacement d'un certain nombre desdits modules installés demeurant inchangés, ledit système comprenant
- des moyens de réception d'informations provenant de l'unité de commande électronique ECU et concernant l'ensemble des modules installés sous la forme d'une table de vérification (15),
 - des moyens de mise à jour du tableau de vérification (15) apte à remplacer des informations de vérification des modules installés destinés à être remplacés par des informations d'un fichier ODX (17) concernant les nouveaux modules de remplacement,
 - des moyens de vérification de la cohérence interne du nouveau programme sur la base du tableau de vérification (15) mis à jour, et
 - des moyens d'autorisation de la reprogrammation de l'ECU dans le cas où le nouveau programme est vérifié comme étant cohérent.

1/2

Fig 1



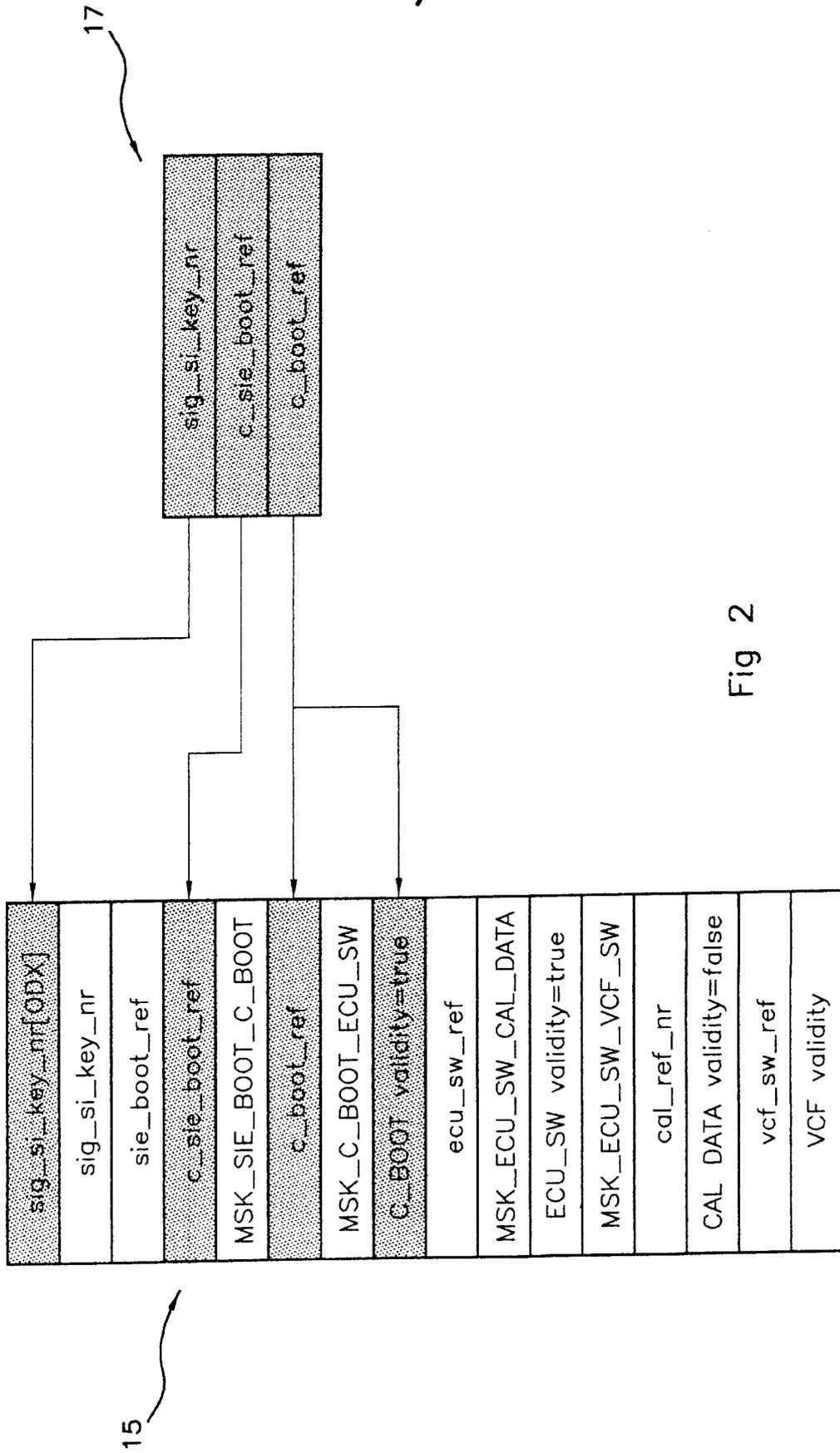


Fig 2



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement
national

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

FA 712794
FR 0804504

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 01/02954 A (KONINKL PHILIPS ELECTRONICS NV [NL]) 11 janvier 2001 (2001-01-11) * page 3, ligne 3 - ligne 15 *	1-7	G06F9/45 G06F9/40
A	US 2007/168453 A1 (ITO ATSUSHI [JP] ET AL) 19 juillet 2007 (2007-07-19) * alinéa [0011] *	1-7	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F
		Date d'achèvement de la recherche	Examineur
		26 février 2009	Ebert, Werner
CATÉGORIE DES DOCUMENTS CITÉS		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire			

1
EPO FORM 1503 12.99 (P04C14)

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0804504 FA 712794**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 26-02-2009

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0102954 A	11-01-2001	EP 1105796 A1	13-06-2001
		JP 2003504721 T	04-02-2003
		US 6467088 B1	15-10-2002

US 2007168453 A1	19-07-2007	WO 2006001260 A1	05-01-2006
		JP 4213749 B2	21-01-2009
