(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 152 107 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
07.11.2001 Bulletin 2001/45

(51) Int Cl.[7]: **E05B 49/00**

(21) Numéro de dépôt: **01400875.9**

(22) Date de dépôt: **05.04.2001**

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: **03.05.2000 FR 0005630**

(71) Demandeur: **Delphi Technologies, Inc.**
Troy, MI 48007 (US)

(72) Inventeur: **Lelandais, Guy**
91190 Gif-sur-Yvette (FR)

(74) Mandataire: **Laget, Jean-Loup**
Cabinet Peuscet,
78, avenue Raymond Poincaré
75116 Paris (FR)

(54) Systéme a anti-piratage pour l'accès mains libres d'un véhicule automobile

(57) Système d'accès dit mains libres pour véhicule automobile (V), comportant un dispositif d'identification (I) et une unité centrale sur le véhicule, apte à engendrer, à une cadence d'horloge haute prédéterminée, un train de bits d'anti-piratage, chaque bit étant émis sous la forme d'un signal d'interrogation radio-fréquence, de façon qu'après réception par le dispositif d'identification, ce dernier émet un signal de réponse vers l'unité centrale de commande, cette dernière comportant au moins un mélangeur (70) apte à mélanger le signal de réponse et le train de bits d'anti-piratage, pour délivrer un signal (V12) représentatif des décalages temporels successifs de chaque bit dudit train d'anti-piratage, ce dernier signal étant reçu à l'entrée d'un intégrateur (75) pour faire la somme des temps de réponse liés à chaque créneau de décalage temporel de bit d'anti-piratage, la sortie dudit intégrateur étant reliée à au moins un premier comparateur pour comparer ladite somme de temps de réponse avec une première valeur de seuil prédéterminée (76a), au-delà de laquelle est détectée une tentative de piratage provoquant l'arrêt de ladite communication.

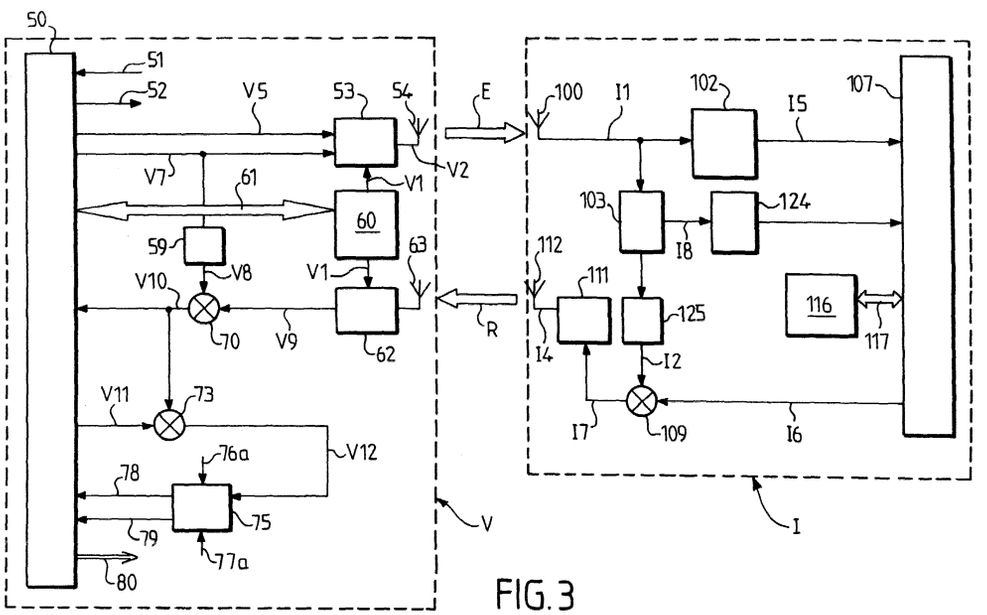

FIG.3

EP 1 152 107 A1

Description

[0001] La présente invention concerne un système d'accès dit mains libres pour véhicule automobile, c'est à dire un système de communication non filaire permettant d'entrer dans le véhicule sans clé. Ce système peut également s'appliquer au démarrage mains libres du véhicule, c'est à dire au démarrage sans clé.

[0002] Un tel système comporte généralement un dispositif d'identification destiné à être porté par un utilisateur et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/ décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique. L'initialisation du protocole de communication peut être activée en actionnant la poignée extérieure de porte, pour l'accès mains libres, ou en appuyant sur un bouton de démarrage, dans le mode démarrage mains libres. Le système est apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite prédéterminée du véhicule, généralement de l'ordre de quelques mètres, pour éviter, d'une part, les interférences avec d'autres sources de signaux de l'environnement, et, d'autre part, pour éviter le fonctionnement du système à une distance telle que l'utilisateur est trop éloigné du véhicule pour être conscient des opérations effectuées par ledit système.

[0003] Certains systèmes actuellement proposés utilisent des systèmes à induction magnétique à très courte portée, pour à la fois alimenter en énergie et transporter les informations depuis l'unité centrale du véhicule vers le dispositif d'identification qui se trouve dans le champ électromagnétique engendré par les antennes du véhicule. Toutefois, un tel système ne permet une communication qu'à très courte distance du véhicule de l'ordre de quelques cm. Un autre système couramment proposé consiste à utiliser des ondes porteuses à basse fréquence, de l'ordre de 125 kHz pour la communication depuis le véhicule vers le dispositif d'identification, et des ondes porteuses à ultra haute fréquence, par exemple de l'ordre de 434 ou 868 MHz, pour la zone Europe, et de 315 ou 902 MHz pour la zone USA. Toutefois, dans ce cas, le dispositif d'identification doit comporter une pile pour alimenter ses circuits électroniques propres. Pour minimiser la consommation électrique, on peut prévoir, à titre d'exemple, que le dispositif d'identification soit en sommeil pendant 9 ms et en éveil 1 ms, pendant des périodes de 10 ms.

[0004] Bien entendu, la communication bidirectionnelle entre le véhicule et le dispositif d'identification est cryptée, afin d'éviter tout fonctionnement intempestif du système et pour le sécuriser vis à vis des malfaiteurs. Sur la figure 1 des dessins annexés, on a représenté un exemple de système d'encryptage déjà connu. Sur cette figure 1, on a représenté un véhicule V qui comporte dans son unité centrale une mémoire 1 contenant une clé secrète K et un générateur de nombres aléatoires 2, les nombres aléatoires R engendrés ayant, par exemple, une longueur de 56 bits. Ce nombre aléatoire R est émis vers le dispositif d'identification I, comme indiqué par la flèche 3. Simultanément, ce même nombre aléatoire R est mélangé avec la clé secrète K suivant une fonction associative complexe f, dans un mélangeur 4 qui est relié à son entrée à la mémoire 1 et au générateur de nombres aléatoires 2. Le mélangeur 4 délivre, en sortie, un signal représentatif du mélange de la clé secrète K et du nombre aléatoire R, à savoir le signal f(R, K). Ce signal est mémorisé dans une mémoire 5 reliée à la sortie du mélangeur 4. Ce signal est envoyé au dispositif d'identification I, sous la forme d'un signal d'une longueur par exemple de 28 bits, comme indiqué par la flèche 6. Dans le véhicule V, le signal f(R, K) est mélangé à nouveau à la clé secrète K dans un mélangeur 7, qui est relié à son entrée aux mémoires 1 et 5 précitées. Ce mélangeur 7 mélange les deux signaux suivant une fonction associative complexe g. Le véhicule V mémorise alors dans une mémoire 8 reliée à la sortie du mélangeur 7 le signal représentatif du mélange, à savoir le signal g(R, f, K).

[0005] Du côté du dispositif d'identification, la même clé secrète K est mémorisée dans une mémoire 11 et un mélangeur 14 ayant la même fonction associative f reçoit en entrée la clé secrète fournie par la mémoire 11 du dispositif d'identification I et le nombre aléatoire R reçu par le dispositif d'identification en provenance du véhicule. Le dispositif d'identification I mémorise le signal en sortie du mélangeur 14 dans une mémoire 15 et compare ce signal dans un comparateur 16 avec le signal reçu suivant la flèche 6 en provenance du véhicule V. Si les deux signaux ne sont pas identiques, sous réserve du temps de retard propre au matériel et à la transmission du signal dans la zone de transmission autorisée, le dispositif d'identification interrompt la communication comme étant non-autorisée. En revanche, si les deux signaux correspondent, le signal est mélangé dans un mélangeur 17 avec la clé secrète fournie par la mémoire 11 du dispositif d'identification I, suivant la même fonction associative g précitée. Le signal de sortie du mélangeur 17 est mémorisé dans une mémoire 18 du dispositif d'identification pour être ensuite envoyé vers le véhicule suivant la flèche 9 sous la forme d'un signal ayant une longueur par exemple de 20 bits. Enfin, le signal reçu par la flèche 9 est comparé avec le signal reçu de la mémoire 8 du véhicule dans un comparateur 10. Si ces deux signaux correspondent, sous réserve des retards dus au temps de réponse du matériel et de la transmission du signal dans la zone autorisée, le reste de la communication est autorisé et l'unité centrale du véhicule pourra, le cas échéant, commander la condamnation ou la décondamnation des serrures des ouvrants du véhicule. Bien entendu, un autre protocole de cryptage pourra être utilisé pour sécuriser la transmission des données.

[0006] Toutefois, malgré ce protocole de cryptage, il existe une façon de pirater le système, sans connaître ni la clé secrète, ni les différentes fonctions associatives du protocole d'encryptage. Ce procédé de piratage est représenté sur la figure 2. Selon ce procédé, on suppose que l'utilisateur U qui porte le dispositif d'identification I est situé à une distance du véhicule V supérieure à la distance autorisée de communication, par exemple de 10 à 100 m de distance du véhicule. Dans ce cas, un pirate équipé d'un premier boîtier relais 20 peut s'approcher du véhicule V à une distance suffisante pour communiquer avec celui-ci, par exemple à une distance de l'ordre de 1 à 5 m. Ce pirate actionne le début de la communication, par exemple en tirant sur la poignée extérieure de portière. Ceci déclenche l'émission des signaux basse fréquence par le véhicule vers le boîtier relais 20, comme indiqué par la flèche en zig-zag 21. Ce signal 21 envoyé par le véhicule est reçu par une bobine 22 du boîtier relais 20, qui est reliée à un récepteur 23 à 125 kHz. Ce récepteur 23 est relié à un émetteur à large bande à haute fréquence, de l'ordre de plusieurs MHz. L'émetteur 24 émet via son antenne 25, comme représenté par la flèche 26, vers un deuxième boîtier relais 30, qui est porté par un autre pirate qui suit de près l'utilisateur U. L'échange d'informations entre les deux boîtiers relais 20 et 30 s'effectuant à très haute fréquence, il est possible d'effectuer cette communication à grande distance. Le deuxième boîtier relais 30 comporte une antenne 31 pour recevoir le signal 26 émis par le boîtier relais 20. L'antenne 31 est reliée à un récepteur large bande à la même fréquence que l'émetteur 24 du premier boîtier relais 20. Le signal ainsi reçu est retransmis à basse fréquence à 125 kHz par un émetteur 33 qui est relié à une bobine d'émission 34 afin d'envoyer un signal 35 vers le dispositif d'identification I qui soit conforme au signal 21 émis par le véhicule. Le signal 35 étant la répétition du signal authentique du véhicule, le dispositif d'identification I va le reconnaître et émettre à son tour son signal de réponse 36, ledit signal de réponse 36 étant envoyé à haute fréquence et reçu par une antenne 37 du deuxième boîtier relais 30, par exemple à 434 MHz. L'antenne 37 est reliée à un récepteur 38, qui va convertir le signal à 434 MHz en un signal à une fréquence différente, par exemple à 315 MHz. Le signal est alors émis par un émetteur à large bande 39 via une antenne 40 vers le premier boîtier relais 20, cette différence de fréquence étant nécessaire pour que les différents signaux n'interfèrent pas entre eux. Bien entendu, la fréquence du signal 41 émis en retour par le deuxième boîtier relais 30 est différente à la fois de la fréquence du signal 26 et du signal 36. Ce signal 41 est capté par une antenne 27 du premier boîtier relais 20, ladite antenne 27 étant reliée à un récepteur large bande 28 de la même fréquence que l'émetteur 39. Le récepteur 28 est relié à un émetteur 29 qui transforme le signal à 315 MHz en un signal à 434 MHz qui est envoyé via l'antenne 42 du premier boîtier relais 20 vers le véhicule V, comme représenté par la flèche en zig-zag 43.

[0007] Il suffit que les pirates utilisent des boîtiers relais ayant des liaisons à large bande, par exemple supérieure à 50 MHz, ce qui est possible car les systèmes pirates n'ont pas à respecter les réglementations ; le temps de transit supplémentaire dû à la distance peut être alors de l'ordre de quelques nanosecondes, ce qui est négligeable en comparaison avec les constantes de temps nécessaires pour la transmission normale autorisée. A titre d'exemple, la communication totale peut être de l'ordre de 20 à 40 ms, et la durée totale du fonctionnement du système pour déclencher la décondamnation ou la condamnation des serrures électriques peut être de l'ordre de 100 ms.

[0008] Pour détecter un tel piratage et interrompre la communication, une solution pourrait consister à mesurer le temps de propagation des ondes radio UHF, en comparant ce temps mesuré avec un temps prédéterminé correspondant à une communication dans une zone limitée autorisée autour du véhicule. Toutefois, pour détecter le temps de retard dû à la distance, par rapport à un temps de communication global, il est nécessaire de disposer de large bande passante, ce qui correspond à une cadence de communication rapide, par exemple de l'ordre de 20 à 40 Mb/s. Avec une telle cadence de communication, il est nécessaire d'opérer à très haute fréquence, par exemple à 2,4 GHz. Mais pour mesurer des temps très courts, il est nécessaire d'avoir une bande passante très importante, ce qui vient se heurter aux réglementations applicables qui limitent fortement les bandes passantes autorisées, pour éviter une saturation de l'environnement par des ondes électromagnétiques.

[0009] L'invention a pour but d'éliminer les inconvénients précités et de proposer un système d'accès dit mains libres pour véhicule automobile, permettant de détecter un piratage du système, notamment par l'intermédiaire de boîtiers relais, en prenant compte du temps de propagation du signal entre le véhicule et le dispositif d'identification.

[0010] A cet effet, l'invention a pour objet un système d'accès dit mains libres pour véhicule automobile, comportant un dispositif d'identification destiné à être porté par un utilisateur et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/ décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique, ledit système étant apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite prédéterminée du véhicule, caractérisé par le fait que ladite unité centrale est apte à engendrer, à une cadence d'horloge haute prédéterminée, lors de la communication, un train de bits d'anti-piratage, chaque bit dudit train étant émis vers le dispositif d'identification sous la forme d'un signal d'interrogation radio-fréquence repré-

sentatif dudit bit, de façon qu'après réception dudit signal d'interrogation par le dispositif d'identification, ce dernier émet, avec un retard au moins égal à un temps bit utile, un signal de réponse vers l'unité centrale de commande, cette dernière comportant au moins un mélangeur apte à mélanger, d'une part, le signal de réponse reçu en provenance du dispositif d'identification et, d'autre part, le train de bits d'anti-piratage engendré par l'unité centrale et retardé d'un temps bit utile, pour délivrer en sortie dudit mélangeur un signal représentatif des décalages temporels successifs de chaque bit dudit train d'anti-piratage, ce dernier signal étant reçu à l'entrée d'un intégrateur pour faire la somme des temps de réponse liés à chaque créneau de décalage temporel de bit d'anti-piratage, la sortie dudit intégrateur étant reliée à au moins un premier comparateur pour comparer ladite somme de temps de réponse avec une première valeur de seuil prédéterminée, au-delà de laquelle est détectée une tentative de piratage provoquant l'arrêt de ladite communication.

[0011] On entend par "temps d'émission utile" le temps d'émission de l'information binaire dudit bit par rapport au temps total de la cellule à laquelle est associé ledit bit qui comprend généralement ledit temps utile et un temps de silence pour permettre la réception du signal réémis par le dispositif d'identification pendant ledit temps de silence.

[0012] Avantageusement, la somme des temps de réponse effectuée par l'intégrateur, est arrêtée lorsque l'unité centrale de commande détecte la réception du dernier bit du train d'anti-piratage.

[0013] Selon une autre caractéristique, la sortie de l'intégrateur est reliée à au moins un second comparateur pour comparer ladite somme de temps de réponse avec une autre valeur de seuil prédéterminée inférieure à ladite première valeur de seuil prédéterminée, au-delà de laquelle est détectée une communication au-delà de ladite distance limite prédéterminée.

[0014] Selon encore une autre caractéristique, le dispositif d'identification comporte un retardateur de signal numérique apte à retarder d'un temps bit utile le signal d'interrogation reçu en provenance du véhicule, un oscillateur générateur d'ondes porteuses en radio fréquence, relié en sortie à un modulateur de phase ou d'amplitude, qui est commandé par le signal en sortie dudit retardateur, pour délivrer en sortie dudit modulateur ledit signal de réponse destiné à être émis vers le véhicule. Dans ce cas, le dispositif d'identification peut comporter un détecteur de front descendant pour détecter le front descendant du signal d'interrogation reçu en provenance du véhicule, ledit détecteur étant apte à faire basculer ledit oscillateur du dispositif d'identification entre un état d'arrêt correspondant au mode réception du dispositif d'identification et un état de fonctionnement correspondant à son mode d'émission.

[0015] Selon encore une autre caractéristique, le train de bits d'anti-piratage est engendré par l'unité centrale après l'émission des données d'authentification cryptées vers le dispositif d'identification. Dans ce cas, le dispositif d'identification peut comporter un mélangeur pour mélanger le signal en sortie dudit retardateur avec un signal numérique d'authentification crypté de réponse du dispositif d'identification, à une cadence plus lente que celle du train de bits d'anti-piratage, le signal de sortie de ce mélangeur étant apte à commander le modulateur précité du dispositif d'identification.

[0016] On peut prévoir alors que l'unité centrale du véhicule comporte un démodulateur de phase ou d'amplitude pour démoduler le signal reçu par le véhicule en provenance du dispositif d'identification, une porte logique OU exclusif dont les entrées sont reliées respectivement audit démodulateur de phase et à un retardateur de signal numérique, ledit retardateur étant apte à retarder d'un temps bit utile chaque bit du train d'anti-piratage engendré par l'unité centrale, ladite porte logique étant apte à délivrer en sortie un signal numérique représentatif du signal crypté de réponse du dispositif d'identification.

[0017] Dans une première forme de réalisation, le signal délivré en sortie de la porte logique OU exclusif précitée est comparé par l'unité centrale à un signal numérique crypté d'authentification engendré par l'unité centrale, afin d'authentifier le dispositif d'identification.

[0018] Dans une autre forme de réalisation, la sortie de ladite porte logique OU exclusif est reliée à une entrée d'une deuxième porte logique OU exclusif dont l'autre entrée reçoit un signal numérique crypté d'authentification engendré par l'unité centrale, afin de délivrer en sortie ledit signal représentatif des décalages temporels successifs de chaque bit du train d'anti-piratage.

[0019] On peut également prévoir que l'unité centrale est apte à commander alternativement l'arrêt et le démarrage de l'oscillateur de l'unité centrale suivant ladite haute cadence d'horloge prédéterminée pour faire basculer l'unité centrale respectivement en mode réception et émission. Etant donné que l'on utilise un oscillateur à très haute fréquence, par exemple de l'ordre de 2,4 GHz, il est possible d'arrêter et de redémarrer l'oscillateur pour chaque bit du train d'anti-piratage, car le temps de relaxation de ce type d'oscillateur est faible.

[0020] Selon une autre caractéristique, l'unité centrale de commande comporte un oscillateur générateur d'ondes porteuses en radio fréquence, relié à un modulateur de phase ou d'amplitude, qui est commandé par le train de bits d'anti-piratage engendré par l'unité centrale du véhicule.

[0021] Dans une variante, le dispositif d'identification peut comporter une unité de mesure de longueur moyenne des bits reçus, pour mesurer, après démodulation du signal d'interrogation reçu en provenance du véhicule, la longueur moyenne des bits d'anti-piratage reçus, ladite unité de mesure étant apte à provoquer l'interruption de la communication lorsque ladite longueur moyenne est inférieure à une valeur prédéterminée, par exemple 90 % de la longueur utile du bit émis par le

véhicule. Cette unité a pour but d'éviter qu'un pirate contourne le dispositif d'anti-piratage constitué par l'intégrateur, en écourtant la réception du signal émis en provenance du véhicule, afin de provoquer un signal de réponse anticipé de la part du dispositif d'identification, cette réponse anticipée ayant pour but de compenser la durée de propagation du signal due à l'éloignement.

[0022] Selon encore une autre caractéristique, l'unité centrale est apte à commander l'arrêt ou le fonctionnement d'un récepteur à ladite haute cadence d'horloge, de façon que ledit récepteur délivre au mélangeur de l'unité centrale un signal numérique représentatif de l'interprétation du début du signal de réponse reçu en provenance du véhicule. En effet, la fin du signal de réponse n'est pas traitée par l'unité centrale, car ladite fin vient se chevaucher avec l'émission du bit d'anti-piratage suivant, en raison du retard dû à la propagation du signal.

[0023] A titre d'exemple, le temps bit utile peut être compris entre 50 ns et 1µs, par exemple de l'ordre de 200 ns.

[0024] L'invention sera mieux comprise, et d'autres buts, détails, caractéristiques et avantages de celle-ci apparaîtront plus clairement au cours de la description explicative détaillée qui va suivre d'un mode de réalisation particulier de l'invention, donné uniquement à titre illustratif et non limitatif, en référence au dessin schématique annexé, dans lequel :

- la figure 1 est un schéma synoptique fonctionnel représentant le protocole d'encryptage pour sécuriser la transmission bidirectionnelle de données entre un véhicule et un dispositif d'identification ;
- la figure 2 est un schéma synoptique fonctionnel illustrant un moyen de piratage du système d'encryptage par l'intermédiaire de deux boîtiers relais ;
- la figure 3 est un schéma synoptique fonctionnel simplifié d'un système d'accès mains libres conforme à l'invention ;
- la figure 4 est un schéma synoptique fonctionnel plus détaillé correspondant au schéma de la figure 3 ;
- la figure 5 représente plusieurs chronogrammes illustrant les trames complètes d'interrogation émises par le véhicule et reçues en réponse par le véhicule ;
- la figure 6 est une vue partielle et agrandie d'une portion des chronogrammes de la figure 5, indiquée par la flèche VI, correspondant au début de la séquence d'anti-piratage ;
- la figure 7 reprend les deux premiers chronogrammes de la figure 5 ; et
- la figure 8 est une vue partielle et agrandie d'une portion des chronogrammes de la figure 7, indiquée par la flèche VIII, au cours de la séquence d'anti-piratage.

[0025] On va maintenant se référer aux figures 3 et 4, qui représentent le système d'accès mains libres selon l'invention respectivement sous forme simplifiée et plus détaillée.

[0026] Le véhicule automobile V comporte dans son unité centrale un micro-contrôleur 50, qui est généralement dans un état de semi-sommeil ou d'attente d'un réveil. Lorsque l'utilisateur actionne la poignée extérieure de porte, un signal d'activation est envoyé au micro-contrôleur 50, comme indiqué par la flèche 51. En réponse, le micro-contrôleur envoie un signal d'alimentation général, comme représenté par la flèche 52, pour alimenter les différents composants électroniques de l'unité centrale. Puis, le micro-contrôleur 50 engendre une série de signaux à faible cadence sk, par exemple de l'ordre de 2 à 100 Kb/s sur la ligne V5. Les données véhiculées sur la ligne V5 sont successivement un signal d'éveil e, un signal représentatif d'un nombre aléatoire R d'une longueur par exemple de 56 bits, un signal représentatif de la fonction f (R,K) d'une longueur par exemple de 28 bits, et d'un signal représentatif de données de service s, par exemple d'une longueur de 100 à 5 000 bits, par exemple des données sur la maintenance, le réglage du véhicule, etc (voir figure 5). La ligne V5 est reliée à un émetteur 53 pour émettre via une antenne 54 les signaux vers le dispositif d'identification I comme représenté par la flèche E. L'émetteur 53 comporte, comme mieux visible sur la figure 4, un oscillateur 55 pour engendrer une onde porteuse à ultra haute fréquence, par exemple à 2,4 GHz, ledit oscillateur étant alimenté par la ligne 52. L'oscillateur 55 est relié à un modulateur de phase 56 ou un modulateur d'amplitude du type à modulation à 50 % et à 100 % selon que la valeur du bit transmis est à 0 ou 1, dont la sortie est reliée à l'antenne 54 précitée.

[0027] Le signal émis E, par exemple avec une amplitude de l'ordre de 2V efficace, est reçu par une antenne 100 du dispositif d'identification I avec une atténuation de l'ordre de -40 dBm, ce qui représente un coefficient d'atténuation de 100 fois, c'est à dire que le signal reçu par le dispositif d'identification présente une amplitude de l'ordre de 20 mV. L'antenne 100 est reliée à un filtre radio-fréquence 101 (uniquement représenté sur la figure 4) pour éliminer les fréquences parasites. La sortie du filtre 101 est reliée à un embranchement, d'une part, vers un récepteur à faible cadence et à faible consommation 102 et, d'autre, part à un amplificateur logarithmique 103 qui permet de délivrer en sortie un signal de l'ordre de 2V efficace, et sert de récepteur haute fréquence. Les signaux à faible cadence sk ne sont pas transmis par l'amplificateur 103, mais passent essentiellement via le récepteur 102. Comme mieux visible sur la figure 4, le récepteur 102 comprend successivement un détecteur d'enveloppe radio-fréquence 104 pour reconstituer les signaux à faible cadence sur la ligne I5, qui correspondent à ceux de la ligne V5. La sortie du détecteur d'enveloppe 104 est reliée à un amplificateur basse fréquence 105, dont la sortie est reliée en parallèle, d'une part, à un décodeur de séquence d'éveil 106 et, d'autre part, à un micro-contrôleur 107 du dis-

positif d'identification I via une ligne 108. Au démarrage de la communication avec le véhicule, seul le décodeur 106 est alimenté en permanence par la pile du dispositif d'identification. Autrement dit, les données d'éveil e sont décodées par le décodeur 106, afin d'envoyer un ordre d'éveil au micro-contrôleur 107, à la sortie du décodeur 106. Le micro-contrôleur 107 éveille alors tous les autres composants électroniques du dispositif d'identification. Ainsi, les données suivantes, à savoir les signaux R, f et s, sont transmis directement au micro-contrôleur 107 via la ligne en parallèle 108.

[0028] Après émission des données de service s, le micro-contrôleur 50 du véhicule V engendre des bits d'anti-piratage h à la cadence lente sk du micro-processeur, lesdits bits d'anti-piratage étant reçus par une mémoire tampon à générateur de séquences binaires aléatoires 58, pour délivrer en sortie les bits d'anti-piratage à haute cadence fk, sur une ligne V7. La sortie de la mémoire tampon 58 est reliée à un embranchement, d'une part, avec le modulateur de phase ou d'amplitude 56 pour moduler en phase l'onde porteuse engendrée par l'oscillateur 55, et d'autre part, avec un retardateur numérique d'un temps bit utile 59, dont la fonction sera expliquée plus loin. Chaque bit d'anti-piratage est transmis sous la forme d'un signal radio-fréquence via l'antenne 54 en direction du dispositif d'identification I. La trame globale d'émission V2 des signaux par l'antenne 54 est illustrée sur les figures 5 et 7. En se référant plus particulièrement à la figure 6, on a représenté le début de la trame d'interrogation des bits d'anti-piratage h sur la ligne V2. Sur la ligne V2 de la figure 6, on constate que chaque bit d'anti-piratage est porté par une onde oscillante à très haute fréquence ayant un temps bit Ta par exemple de l'ordre de 200 ns. L'émission des bits d'anti-piratage h1, h2...hn est autorisée ou interdite, en fonction d'un signal de commande V1 qui est émis par une unité de gestion de base de temps 60 du véhicule V, laquelle unité 60 est apte à délivrer les signaux d'horloge à faible cadence sk, à moyenne cadence mk et à haute cadence fk. Bien entendu, l'unité 60 est reliée au micro-contrôleur 50, comme indiqué par la double flèche 61. Le signal V1 est engendré à la haute cadence fk prédéterminée et commande alternativement, d'une part, l'arrêt et le démarrage de l'oscillateur 55 et, d'autre part, un récepteur 62 de l'unité centrale.

[0029] Le dispositif d'identification I reçoit via son antenne 100 sur la ligne I1 (voir figure 6) un signal qui correspond au bit d'anti-piratage h1 émis par le véhicule V, avec un temps retard δ qui correspond au temps de propagation du signal entre le véhicule et le dispositif d'identification. Le signal passe alors par l'amplificateur 103, dont la sortie est reliée à un embranchement entre, d'une part, une unité de mesure de longueur moyenne de bit 124 et, d'autre part, un retardateur numérique 125 pour retarder le signal d'un temps bit utile Tb, à la fréquence fk. On a représenté sur la figure 8 le signal I2 qui correspond au signal numérique en sortie du retardateur 125, ledit signal étant retardé d'un temps bit utile Tb, Tb pouvant être égal ou différent de Ta. La sortie du retardateur 125 est reliée à une entrée d'une porte logique OU exclusif 109, dont l'autre entrée reçoit un signal de commande crypté d'authentification g, dont la trame est représentée sur la ligne I6. Comme visible sur la ligne I6 représentée sur la figure 8, la cadence des bits du signal g est à moyenne cadence mk, plus faible que la haute cadence fk des bits d'anti-piratage h. A cet effet, on prévoit que le micro-contrôleur 107 du dispositif d'identification transmet à faible cadence sk le signal g à une mémoire tampon 110 qui délivre en sortie le signal g à la cadence moyenne mk vers le mélangeur 109.

[0030] Le mélangeur 109 délivre en sortie un signal numérique de commande représenté en 17. La sortie du mélangeur 109 est reliée à un émetteur 111 pour émettre un signal de réponse R via une antenne 112, à une amplitude de l'ordre de 2V efficace, vers le véhicule V, comme représenté par la flèche R.

[0031] Lors de la réception de chaque signal représentatif d'un bit d'anti-piratage, le dispositif d'identification est apte à détecter le front descendant F du signal à la sortie de l'amplificateur 103, dans un détecteur de front descendant 113, comme visible sur la figure 4. Ce dernier est apte à commander une bascule 114 avec un faible retard de sécurité ε pour éviter tout chevauchement entre la réception et l'émission du signal au niveau du dispositif d'identification. Cette bascule 114 commande le démarrage d'un oscillateur haute fréquence 115 de l'émetteur 111, après le léger retard ε, lequel oscillateur 115 est relié en sortie à un modulateur de phase ou d'amplitude 118 dudit émetteur 111, ledit modulateur 118 étant commandé par le signal 17 en sortie du mélangeur 109. Simultanément à la détection du front descendant, le détecteur 113 envoie un signal de synchronisation de bit via la ligne 119 à une unité de gestion de base de temps 116 qui délivre les signaux d'horloge sk, mk et fk précités, ladite unité 116 étant reliée au micro-contrôleur 107 via la ligne 117. Ladite unité 116 est apte à commander la bascule 114, pour la faire basculer dans son état d'arrêt de l'oscillateur 115, au bout du temps bit Tb, comme visible sur la figure 4. Bien entendu, on pourrait prévoir le léger retard ε proche de 0 s.

[0032] En partant de l'hypothèse que les signaux électromagnétiques transmis se propagent à la vitesse de la lumière, à savoir 3.10^8 m/s, on peut considérer que la durée de transmission des signaux est de l'ordre de 3 ns par mètre de distance entre le véhicule et le dispositif d'identification I. Autrement dit, pour un trajet aller-retour entre le véhicule V et le dispositif d'identification I, espacé d'une distance d'environ 5 mètres, la durée de propagation δ serait de l'ordre de 30 ns. A cette durée de propagation δ, on pourrait ajouter le temps de réponse des circuits électroniques, qui pourrait être de l'ordre de quelques ns, ou dizaines de ns, selon la bande passante attribuée à la porteuse.

[0033] Le signal réémis R par le dispositif d'identification est reçu par un récepteur 62 via une antenne 63, avec une atténuation de l'ordre de - 40 dBm, ce qui re-

présente un coefficient d'atténuation de 100 fois, c'est à dire que le signal reçu par le véhicule présente une amplitude de l'ordre de 20 mV. Comme mieux représenté sur la figure 4, le récepteur 62 comporte un filtre radiofréquence 64 relié à l'antenne 63, dont le signal de sortie est représenté par la ligne V3, ce signal étant délivré à l'entrée d'un amplificateur logarithmique 65 qui présente un gain de 80 dB, ce qui permet d'atteindre un coefficient de multiplication allant jusqu'à 10 000 fois, et notamment de délivrer en sortie dudit amplificateur 65 un signal de l'ordre de 2V efficace. L'amplificateur 65 est commandé par le signal V1 et est relié en sortie à un démodulateur de phase ou d'amplitude 67.

[0034] Etant donné que l'amplificateur 65 est commandé par le signal V1, ledit amplificateur bascule dans son état inactif lorsque débute l'émission du deuxième bit d'anti-piratage h2, comme indiqué sur la ligne V1 de la figure 6. Toutefois, comme l'unité centrale reçoit le signal de réponse en provenance du dispositif d'identification I avec un retard égal à $2\delta + \varepsilon$, seul le début du signal de réponse est traité par le récepteur 65 et donc démodulé par le démodulateur 67, comme indiqué sur la ligne V9, dont le signal démodulé présente une durée Tc qui est inférieure à la durée Ta du bit d'émission et à la durée Tb du bit de réponse. Par exemple, pour un temps bit Ta et Tb de l'ordre de 200 ns, et une durée de décalage normal de l'ordre de 50 ns, la durée Tc du bit analysé en réponse par l'unité centrale est de l'ordre de 150 ns, ce qui correspond à 75 % du signal initial.

[0035] Le démodulateur de phase 67 délivre un signal représentatif de la fonction hog sur la ligne V9 qui est reliée à une entrée d'une porte logique OU exclusif 70. Cette porte logique 70 reçoit sur son autre entrée un signal V8 représentatif de la fonction h, délivré en sortie du retardateur numérique 59. La porte logique 70 pourrait être remplacée par un autre type de mélangeur, comme représenté sur la figure 3. Le signal V8 correspond au signal V7 avec un retard correspondant au décalage Tb du retardateur numérique 125 du dispositif d'identification I. La porte logique 70 délivre en sortie un signal V10, qui est représentatif du décalage entre les signaux V8 et V9, c'est à dire un signal représentatif du signal encrypté d'authentification g émis par le dispositif d'identification I, avec un petit décalage correspondant au temps de propagation du signal qui est égal à 2δ, comme visible sur la figure 8.

[0036] La sortie de la porte logique 70 est reliée à un embranchement entre, d'une part, un filtre passe-bas 71 à la cadence moyenne mk qui est la cadence correspondant au signal g et, d'autre part, une autre porte logique OU exclusif 73. Le filtre passe-bas 71 est relié à une mémoire tampon 72, qui transforme ledit signal de la cadence mk à la cadence sk avant de l'envoyer au micro-contrôleur 50 qui va comparer le signal g reçu en provenance du dispositif d'authentification avec le signal g engendré au niveau du véhicule, en vue de l'authentification de la communication, ce qui correspond à la dernière étape 10 illustrée sur le schéma de la figure 1. Il est à noter que cette comparaison entre les deux fonctions g s'effectue par auto-corrélation entre les signaux, le seuil d'auto-corrélation acceptable étant par exemple fixé à 90 %, sachant qu'un niveau d'auto-corrélation de 50 % correspond à la comparaison de deux signaux aléatoires.

[0037] Le micro-contrôleur 50 délivre le signal g propre au véhicule à une mémoire tampon 74 à la cadence sk, afin qu'il la renvoie à la cadence mk à l'autre entrée de la porte logique 73 précitée. On a représenté sur la ligne V11 le signal g qui correspond exactement au signal g engendré par le dispositif d'identification et émis sur la ligne I6, comme représenté sur la figure 8. La porte logique 73 mélange les signaux V10 et V11 afin de ne délivrer en sortie que les décalages dus au temps de propagation du signal entre le véhicule V et le dispositif d'identification I, comme représenté sur la ligne V12. La sortie de la porte logique 73 est reliée à l'entrée d'un intégrateur 75, qui va délivrer en sortie un signal V13 qui va monter par escalier en fonction du temps, pour chaque créneau C représentatif du temps de propagation du signal. La ligne V13 est reliée à un embranchement entre, d'une part, un premier comparateur 76 recevant sur une autre entrée une valeur limite de seuil 76a qui correspond à la durée de propagation maximale acceptable, par exemple 50 ns x n, n étant le nombre de bits d'anti-piratage, et, d'autre part, un second comparateur 77 recevant sur une autre entrée une autre valeur limite de seuil 77a inférieure à la valeur 76a et qui correspond au temps de propagation sur la distance autorisée. Selon que l'amplitude du signal de sortie sur la ligne V13 est supérieure ou non à cette valeur limite 76a, un signal de tentative de piratage sera envoyé ou non via la ligne 78 par le premier comparateur 76 au micro-contrôleur 50. De manière analogue, si l'amplitude du signal de sortie sur la ligne V13 est supérieure à la valeur 77a, mais inférieure à la valeur 76a, le second comparateur 77 enverra au micro-contrôleur 50 via la ligne 79, un signal indiquant que la communication se fait hors de la distance autorisée, sans toutefois constituer une tentative de piratage. L'intégrateur 75 va effectuer la somme des décalages temporels élémentaires jusqu'à la fin de la trame d'anti-piratage, comme indiqué par la flèche 75a, à moins que la communication soit interrompue préalablement par les premier et deuxième comparateurs 76 et 77 précités.

[0038] Enfin, le micro-contrôleur 50 peut délivrer différents signaux de sortie aux autres composants du véhicule par la voie 80 représentée sur les figures 3 et 4.

[0039] Toutefois, un pirate pourrait essayer de pieger le système de l'invention en écourtant la réception du signal émis par le véhicule. A titre d'exemple, dès que le pirate détecte avec un boîtier-relais l'émission par le véhicule d'un bit d'anti-piratage, il peut réémettre vers l'autre boîtier-relais uniquement le début dudit signal, afin de provoquer l'émission anticipée du signal de réponse par le dispositif d'identification. Avantageusement, le signal est écourté d'une durée qui correspon-

drait à la durée de propagation du signal sur la distance supplémentaire entre le dispositif d'identification et le véhicule, par rapport à la distance maximale autorisée. Ainsi, comme le détecteur 113 du dispositif d'identification I est apte à détecter le front descendant du signal reçu en provenance du véhicule, le fait d'écourter le signal émis par le véhicule permet d'anticiper sur l'émission par le dispositif d'identification du signal de réponse, ce qui supprime ainsi tout décalage non autorisé entre l'émission et la réception du signal d'anti-piratage par le véhicule, ce qui peut ainsi piéger le système.

[0040] Pour éviter qu'un pirate puisse ainsi piéger le système, l'unité de mesure de longueur moyenne de bits 124 du dispositif d'identification I permet de mesurer la longueur moyenne des bits reçus par le dispositif d'identification en provenance du véhicule. A titre d'exemple si la longueur moyenne ainsi mesurée est inférieure à 90 % de la longueur attendue du bit émis par le véhicule, l'unité 124 va alors envoyer un signal de tentative de piratage via la ligne 131 vers le micro-contrôleur 107 et un signal d'arrêt via la ligne 130 à l'unité de gestion de base de temps 116. Autrement dit, l'unité 124 permet de vérifier l'intégrité du bit reçu par le dispositif d'identification et permet ainsi de détecter une tentative de piratage, même dans le cas où le pirate écourte la réémission du signal vers le dispositif d'identification. En effet, si ce signal écourté peut piéger l'intégrateur 75 de l'unité centrale de commande du véhicule, en revanche l'unité 124 interprétera ce signal écourté comme un signal erroné et provoquera ainsi l'interruption de la communication.

[0041] A titre d'exemple, la cadence d'horloge intermédiaire mk est entre 20 et 60 fois inférieure à la cadence fk.

[0042] En variante, on pourrait remplacer les antennes 54 et 63 du véhicule V par une antenne unique 82 représentée en traits interrompus sur la figure 4, laquelle antenne 82 serait reliée à un diplexeur 81 représenté en traits interrompus sur la figure 4, afin de commuter entre le mode de réception et le mode d'émission selon le cas. De manière analogue, on pourrait remplacer les antennes 100 et 112 du dispositif d'identification par une antenne unique 121 reliée à un diplexeur 120, représentés en traits interrompus sur la figure 4. Les diplexeurs 81 et 120 pourraient ainsi communiquer entre eux, comme indiqué par la double flèche T.

[0043] Comme visible sur la figure 5, sur la ligne V3, après la réception du signal hog, le véhicule V reçoit en provenance du dispositif d'identification un signal hos où s représente des données de service qui viennent moduler le signal h par inversion de phase, comme cela était le cas pour le signal g dont la longueur est inférieure à celle du signal h.

[0044] Bien que l'invention ait été décrite en liaison avec un exemple particulier de réalisation, il est bien évident qu'elle n'y est nullement limitée et qu'elle comprend tous les équivalents techniques des moyens décrits ainsi que leurs combinaisons si celles-ci entrent dans le cadre de l'invention.

Revendications

1. Système d'accès dit mains libres pour véhicule automobile (V), comportant un dispositif d'identification (I) destiné à être porté par un utilisateur (U) et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique, ledit système étant apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite prédéterminée du véhicule, **caractérisé par le fait que** ladite unité centrale est apte à engendrer, à une cadence d'horloge haute prédéterminée (fk), lors de la communication, un train de bits d'anti-piratage (h), chaque bit (h1, h2, h3) dudit train étant émis vers le dispositif d'identification (I) sous la forme d'un signal d'interrogation radio-fréquence (E) représentatif dudit bit, de façon qu'après réception dudit signal d'interrogation par le dispositif d'identification, ce dernier émet, avec un retard au moins égal à un temps bit utile (Tb), un signal de réponse vers l'unité centrale de commande, cette dernière comportant au moins un mélangeur (70) apte à mélanger, d'une part, le signal de réponse (R) reçu en provenance du dispositif d'identification et, d'autre part, le train de bits d'anti-piratage (h) engendré par l'unité centrale et retardé d'un temps bit utile (Tb), pour délivrer en sortie dudit mélangeur un signal (V12) représentatif des décalages temporels successifs de chaque bit dudit train d'anti-piratage, ce dernier signal étant reçu à l'entrée d'un intégrateur (75) pour faire la somme des temps de réponse liés à chaque créneau (C) de décalage temporel de bit d'anti-piratage, la sortie dudit intégrateur étant reliée à au moins un premier comparateur (76) pour comparer ladite somme de temps de réponse avec une première valeur de seuil prédéterminée (76a), au-delà de laquelle est détectée une tentative de piratage provoquant l'arrêt de ladite communication.

2. Système selon la revendication 1, **caractérisé par le fait que** la somme des temps de réponse effectuée par l'intégrateur (75), est arrêtée lorsque l'unité centrale de commande détecte la réception du dernier bit du train d'anti-piratage (75a).

3. Système selon la revendication 1 ou 2, **caractérisé par le fait que** la sortie de l'intégrateur (75) est reliée à au moins un second comparateur (77) pour comparer ladite somme de temps de réponse avec une autre valeur de seuil prédéterminée (77a) inférieure à ladite première valeur de seuil prédéterminée (76a), au-delà de laquelle est détectée une

communication au-delà de ladite distance limite prédéterminée.

4. Système selon l'une des revendications 1 à 3, **caractérisé par le fait que** le dispositif d'identification (I) comporte un retardateur de signal numérique (125) apte à retarder d'un temps bit utile (Tb) le signal d'interrogation reçu en provenance du véhicule (V), un oscillateur (115) générateur d'ondes porteuses en radio fréquence, relié en sortie à un modulateur de phase ou d'amplitude (118), qui est commandé par le signal en sortie dudit retardateur, pour délivrer en sortie dudit modulateur ledit signal de réponse (I4) destiné à être émis vers le véhicule.

5. Système selon la revendication 4, **caractérisé par le fait que** le dispositif d'identification (I) comporte un détecteur de front descendant (113) pour détecter le front descendant (F) du signal d'interrogation reçu en provenance du véhicule (V), ledit détecteur étant apte à faire basculer ledit oscillateur (115) du dispositif d'identification entre un état d'arrêt correspondant au mode réception du dispositif d'identification et un état de fonctionnement correspondant à son mode d'émission.

6. Système selon la revendication 4 ou 5, **caractérisé par le fait que** le train de bits d'anti-piratage (h) est engendré par l'unité centrale après l'émission des données d'authentification cryptées (R, f) vers le dispositif d'identification (I).

7. Système selon la revendication 6, **caractérisé par le fait que** le dispositif d'identification comporte un mélangeur (109) pour mélanger le signal en sortie dudit retardateur (125) avec un signal numérique d'authentification crypté de réponse (g) du dispositif d'identification, à une cadence (mk) plus lente que celle du train de bits d'anti-piratage (h), le signal de sortie (I7) de ce mélangeur étant apte à commander le modulateur (118) précité du dispositif d'identification.

8. Système selon la revendication 7, **caractérisé par le fait que** l'unité centrale du véhicule (V) comporte un démodulateur de phase ou d'amplitude (67) pour démoduler le signal reçu par le véhicule en provenance du dispositif d'identification (I), une porte logique OU exclusif (70) dont les entrées sont reliées respectivement audit démodulateur de phase et à un retardateur de signal numérique (59), ledit retardateur étant apte à retarder d'un temps bit utile (Tb) chaque bit du train d'anti-piratage (h) engendré par l'unité centrale, ladite porte logique (70) étant apte à délivrer en sortie un signal numérique (V10) représentatif du signal crypté de réponse du dispositif d'identification.

9. Système selon la revendication 8, **caractérisé par le fait que** le signal (V10) délivré en sortie de la porte logique OU exclusif (70) précitée est comparé par l'unité centrale à un signal numérique crypté d'authentification engendré par l'unité centrale, afin d'authentifier le dispositif d'identification.

10. Système selon la revendication 8 ou 9, **caractérisé par le fait que** la sortie de ladite porte logique OU exclusif (70) est reliée à une entrée d'une deuxième porte logique OU exclusif (73) dont l'autre entrée reçoit un signal numérique crypté d'authentification (g) engendré par l'unité centrale, afin de délivrer en sortie ledit signal (V12) représentatif des décalages temporels successifs de chaque bit du train d'anti-piratage.

11. Système selon l'une des revendications 1 à 10, **caractérisé par le fait que** l'unité centrale de commande comporte un oscillateur (55) générateur d'ondes porteuses en radio fréquence, relié à un modulateur de phase ou d'amplitude (56), qui est commandé par le train de bits d'anti-piratage (h) engendré par l'unité centrale du véhicule (V).

12. Système selon la revendication 11, **caractérisé par le fait que** l'unité centrale est apte à commander alternativement l'arrêt et le démarrage de l'oscillateur (55) de l'unité centrale suivant ladite haute cadence d'horloge prédéterminée (fk) pour faire basculer l'unité centrale respectivement en mode réception et émission.

13. Système selon la revendication 12, **caractérisé par le fait que** l'unité centrale est apte à commander l'arrêt ou le fonctionnement d'un récepteur (62) à ladite haute cadence d'horloge (hk), de façon que ledit récepteur (62) délivre au mélangeur (70) de l'unité centrale un signal numérique (V9) représentatif de l'interprétation du début du signal de réponse reçu en provenance du véhicule.

14. Système selon l'une des revendications 1 à 13, **caractérisé par le fait que** le dispositif d'identification (I) comporte une unité (124) de mesure de longueur moyenne des bits reçus, pour mesurer, après démodulation du signal d'interrogation (E) reçu en provenance du véhicule (V), la longueur moyenne des bits d'anti-piratage reçus, ladite unité de mesure étant apte à provoquer l'interruption de la communication lorsque ladite longueur moyenne est inférieure à une valeur prédéterminée, par exemple 90 % de la longueur utile Ta du bit émis par le véhicule.

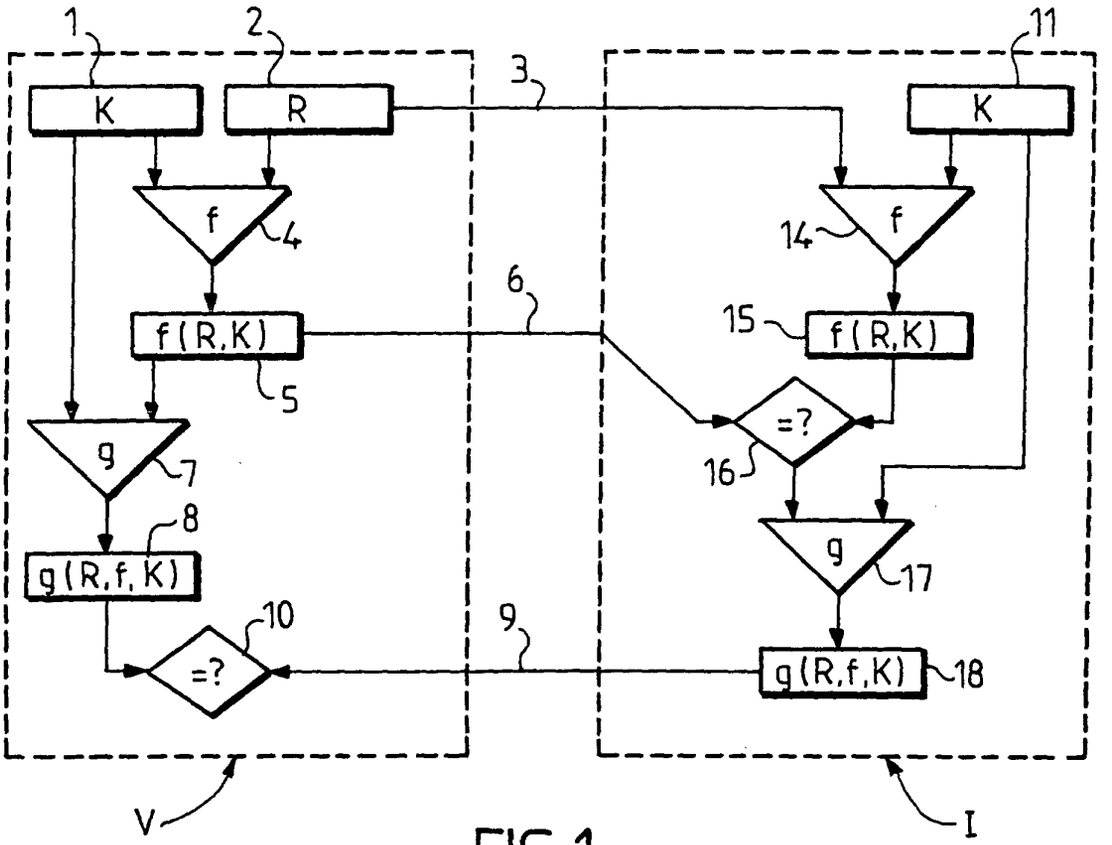
1
2
3
11
K
R
K
f
4
14
f
6
15
f(R,K)
f(R,K)
5
=?
16
g
7
8
g
g(R,f,K)
17
10
9
=?
g(R,f,K)
18
V
I

FIG.1

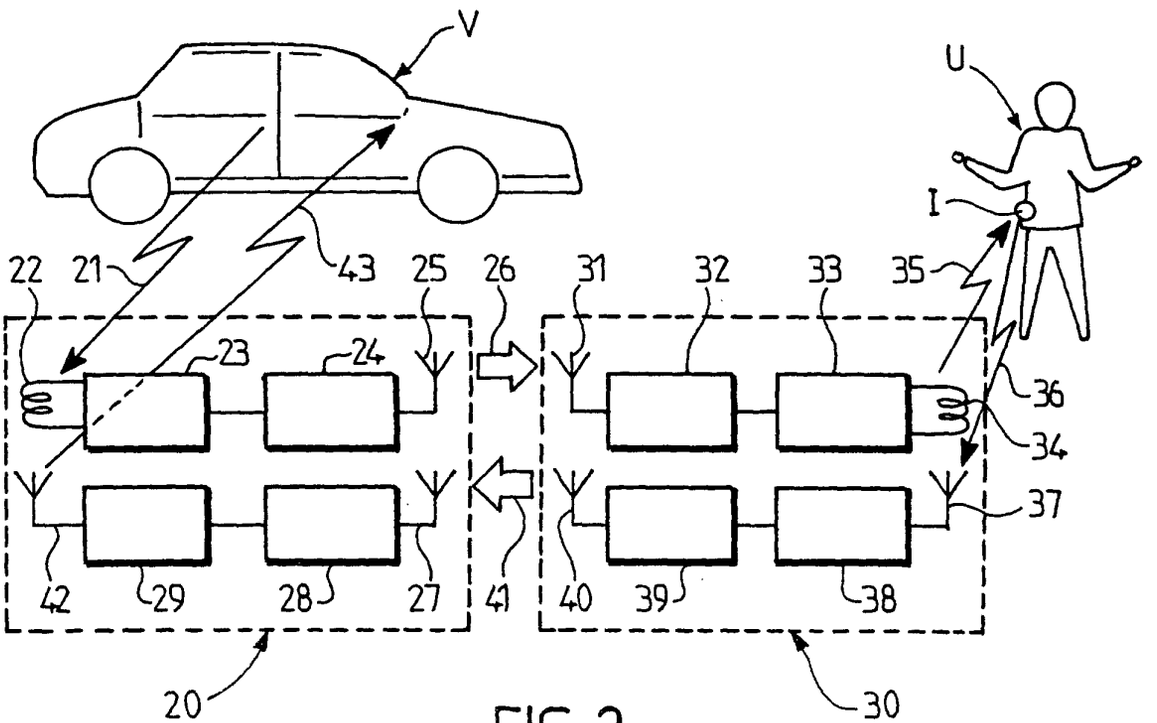
V
U
I
22
21
43
25
26
31
32
33
35
23
24
36
34
37
42
29
28
27
41
40
39
38
20
30

FIG.2

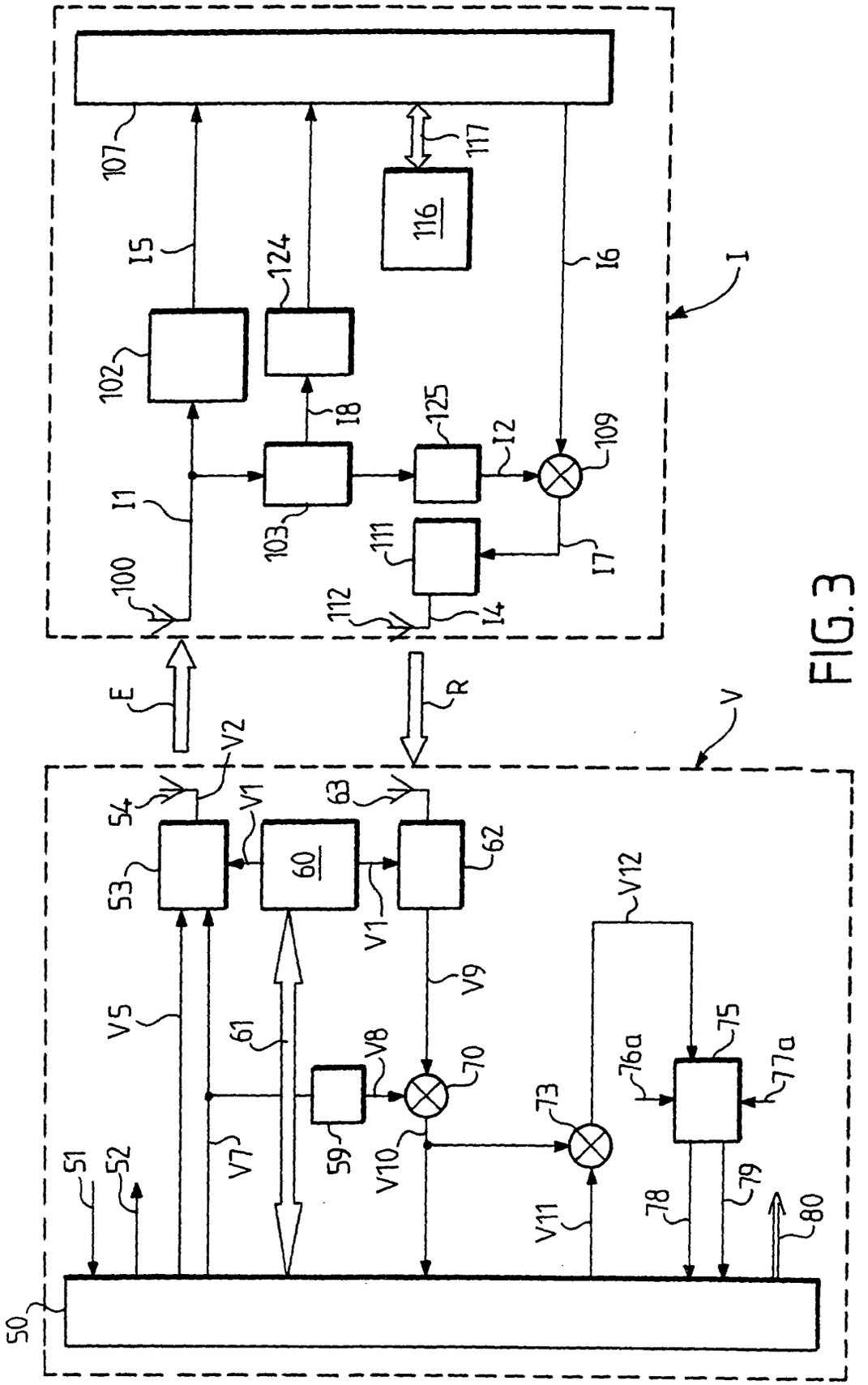
I
107
117
116
I5
124
I6
102
18
125
I2
109
I1
103
111
I7
100
112
I4
E
R
V
V2
54
V1
63
53
60
62
V12
V1
V9
V5
61
V8
70
73
76a
75
77a
V7
59
V10
V11
78
79
80
51
52
50

FIG.3

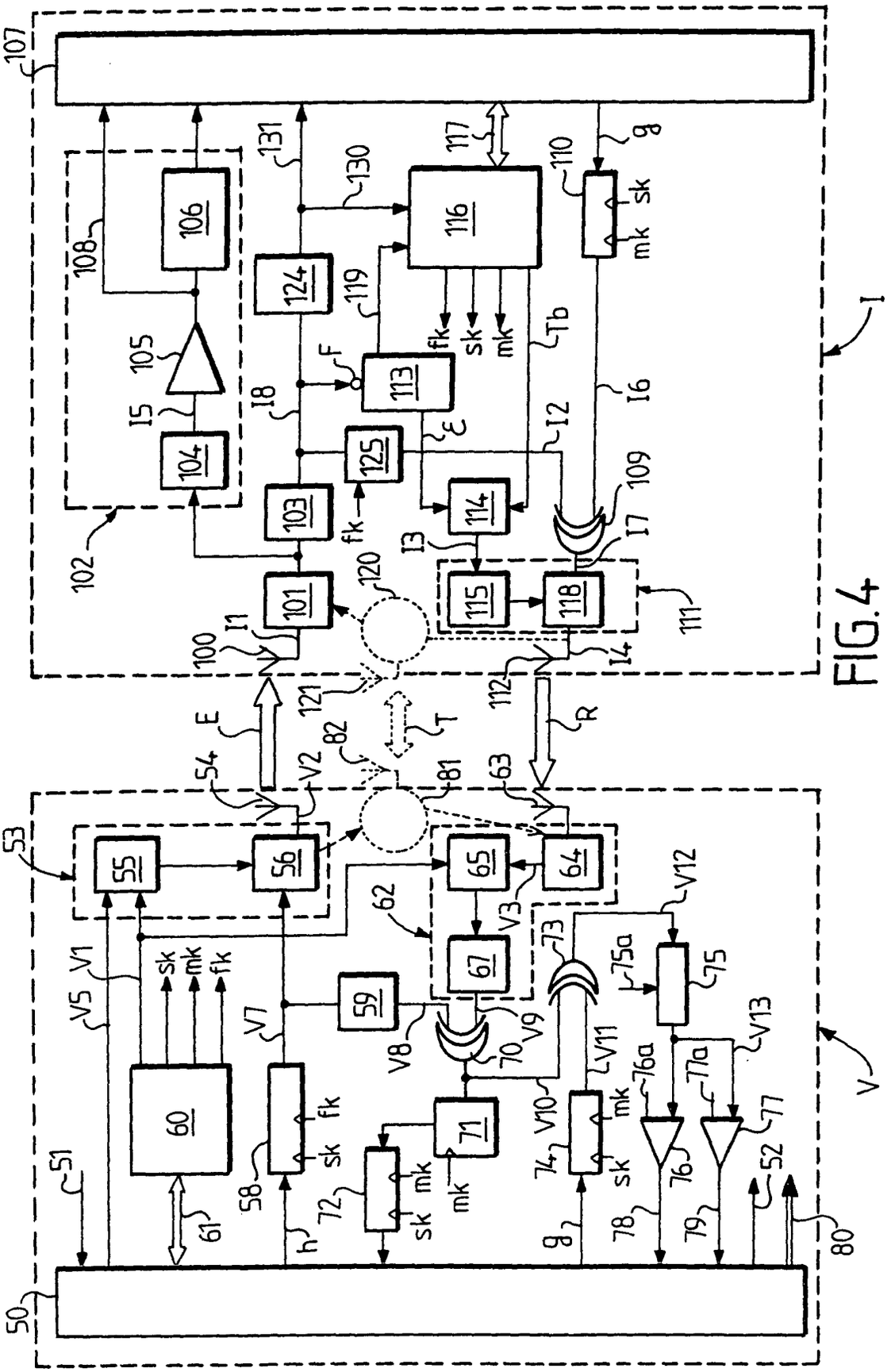
107
106
108
105
15
104
102
131
130
124
119
116
117
110
g
sk
mk
18
F
113
fk
sk
mk
Tb
16
12
125
103
114
109
17
13
fk
101
120
115
118
111
100
11
14
I
121
112
E
T
R
82
54
V2
81
63
53
55
56
65
64
V12
62
V3
73
67
V1
sk
mk
fk
75a
75
V5
59
V7
V9
V8
70
V11
V13
60
58
71
V10
74
76a
77a
61
h
72
sk
mk
mk
sk
76
77
51
52
g
78
79
80
50
V

FIG.4

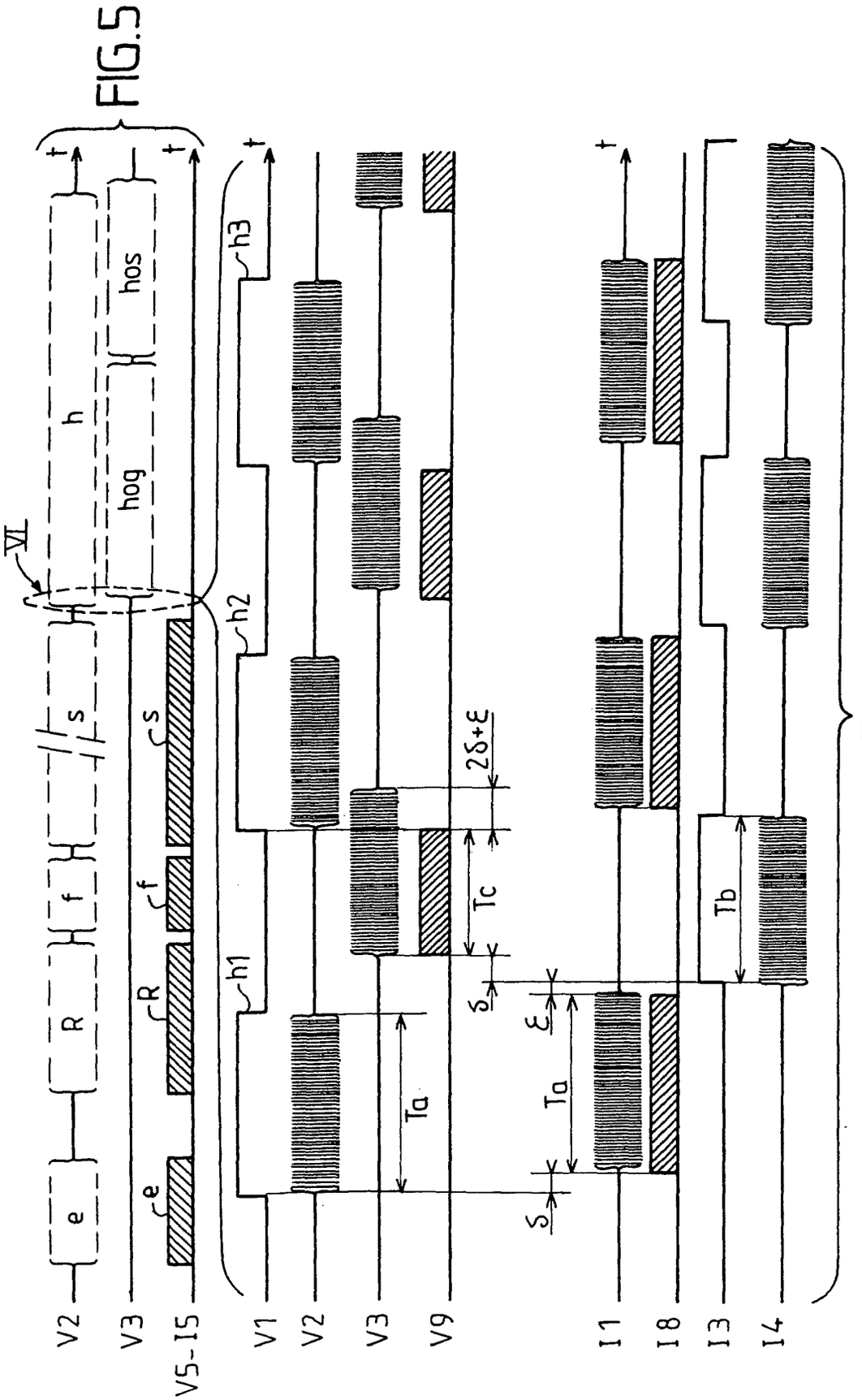
FIG.5
FIG.6
VI
h
hos
hog
s
f
R
e
t
V2
V3
V5-I5
V1
V2
V3
V9
I1
I8
I3
I4
h1
h2
h3
Ta
Tb
Tc
δ
ε
2δ+ε

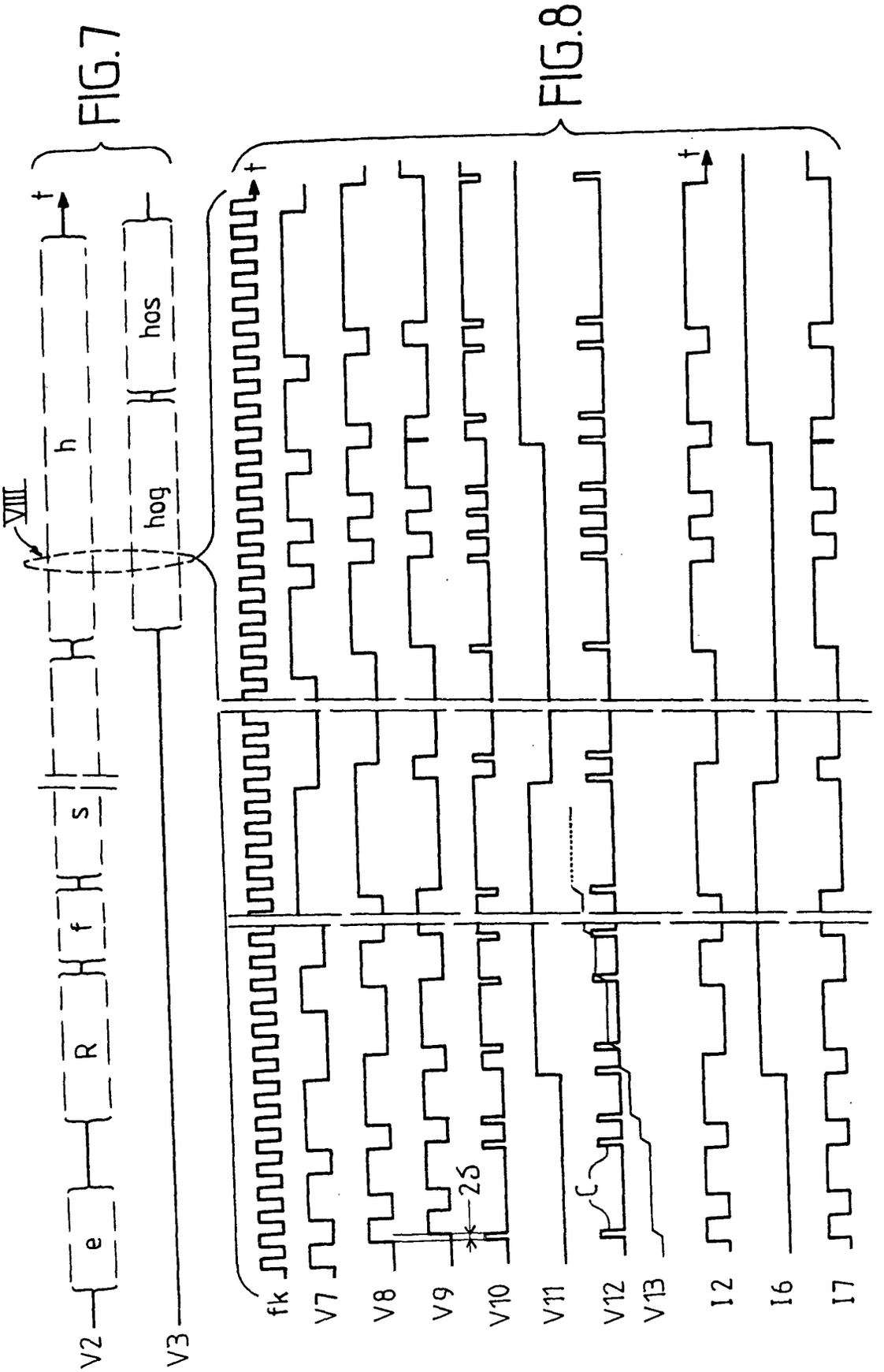
FIG.7
FIG.8
t
h
hos
hog
VIII
e
R
f
s
V2
V3
fk
V7
V8
V9
V10
V11
V12
V13
I2
I6
I7
25

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 01 40 0875

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
A	WO 00 12848 A (KOSTAL LEOPOLD GMBH & CO KG ;FROMM MICHAEL (DE); KRAMER DETLEV (DE) 9 mars 2000 (2000-03-09) * le document en entier *	1	E05B49/00
A	EP 0 983 916 A (MARQUARDT GMBH) 8 mars 2000 (2000-03-08) * abrégé * * alinéa '0007! - alinéa '0012! * * alinéa '0016! - alinéa '0033!; figures *	1	
A	DE 196 32 025 A (DAIMLER BENZ AG) 2 avril 1998 (1998-04-02) * colonne 2, ligne 25 - ligne 64 * * colonne 5, ligne 51 - colonne 6, ligne 33 *	1	
A	DE 40 20 445 A (BAYERISCHE MOTOREN WERKE AG) 2 janvier 1992 (1992-01-02) * le document en entier *	1	
			DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)
			E05B B60R

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	19 juillet 2001	Teutloff, H

CATEGORIE DES DOCUMENTS CITES

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

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 01 40 0875

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

19-07-2001

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0012848 A	09-03-2000	DE 19839696 A	02-03-2000
		DE 19839695 C	04-05-2000
		DE 19926234 A	14-12-2000
		AU 5737299 A	21-03-2000
		EP 1109981 A	27-06-2001
EP 0983916 A	08-03-2000	DE 19941428 A	15-06-2000
DE 19632025 A	02-04-1998	EP 0823520 A	11-02-1998
		US 5983347 A	09-11-1999
DE 4020445 A	02-01-1992	DE 4003280 A	08-08-1991
		DE 59009066 D	14-06-1995
		EP 0440974 A	14-08-1991
		ES 2071738 T	01-07-1995

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82