(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 047 140**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **16 50643**

(51) Int Cl[8] : ***H 04 W 12/08*** *(2017.01), H 04 W 88/08, B 60 W 50/08*

(12) **BREVET D'INVENTION** **B1**

(54) SYSTEME DE COMMUNICATION SECURISE ENTRE UN VEHICULE ET UN SERVEUR DISTANT.

(22) **Date de dépôt :** 27.01.16.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 28.07.17 Bulletin 17/30.

(45) **Date de la mise à disposition du public du brevet d'invention :** 02.02.18 Bulletin 18/05.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *PEUGEOT CITROEN AUTOMOBILES SA Société anonyme* — FR.

(72) **Inventeur(s) :** LE PAVEC ANNE.

(73) **Titulaire(s) :** PEUGEOT CITROEN AUTOMOBILES SA Société anonyme.

(74) **Mandataire(s) :** PEUGEOT CITROEN AUTOMOBILES SA Société anonyme.

FR 3 047 140 - B1

SYSTEME DE COMMUNICATION SECURISE ENTRE UN VEHICULE ET UN SERVEUR DISTANT

[0001] L'invention porte sur un système de communication entre un véhicule et un serveur distant, notamment un serveur privé.

[0002] Elle porte plus particulièrement sur les conditions d'utilisation des ressources télématiques du véhicule dans le but de prolonger l'activité professionnelle des passagers durant les trajets.

[0003] Les entreprises peuvent proposer des solutions/services à leurs employés leur permettant de poursuivre leur activité professionnelle. Des entreprises de mobilité (exemple taxi) peuvent proposer ce même type de solutions /Services à leur clients

[0004] Avec l'avènement des voitures connectées, la voiture peut se transformer en poste de travail étendu pour les passagers du véhicule pendant les trajets y compris le conducteur quand ce dernier ne conduit pas.

[0005] Un poste de travail étendu doit être compris comme une extension du poste habituel de travail au sein duquel une partie de l'activité professionnelle du conducteur peut continuer à s'exercer sensiblement dans les mêmes conditions de confidentialité et de sécurité que dans son poste de travail habituel.

[0006] Au sein de ce poste de travail étendu, le passager peut poursuivre une tâche non achevée ou en commencer une nouvelle, pendant une partie du trajet ou la totalité du trajet. Il est bien entendu compris que l'activité professionnelle concernée par la présente invention se limite à celle ne nécessitant que des moyens « bureautiques » tels qu'un ordinateur portable et/ des périphériques associés à ce dernier ainsi qu'un terminal de communication de type Smartphone ou tablette qui seraient connectés au réseau de l'entreprise via la plateforme télématique de la voiture.

[0007] De tels postes de travail étendus sont déjà connus dans les transports publics dans lesquels sont mis à la disposition des voyageurs des espaces dédiés, équipés d'une prise secteur et d'une connexion à Internet sans fil (Wi-fi, Bluetooth ,...) ou filaire (Port USB, ...). Le voyageur peut ainsi connecter son ordinateur personnel, sa tablette ou son Smartphone à un serveur de son entreprise et échanger des informations via une liaison sécurisée de type VPN.

[0008] Toutefois, ces solutions ne partagent pas les ressources télématiques déjà présentes dans le véhicule pour offrir aux passagers du véhicule des services tels que ceux accessibles via un abonnement à des services connectés de type « infotainment » terme anglo-saxon généralement utilisé pour définir des services alliant information et divertissements.

[0009] Le passage obligatoire par la plateforme télématique du véhicule permet de vérifier que les conditions réglementaire sont bien vérifiées (voir également infra.)

[0010] La plupart des véhicules automobiles disposent déjà de ressources télématiques embarquées telle qu'une plateforme ou boitier télématique autonome (PT) permettant des échanges d'informations entre le véhicule et l'environnement extérieur : Internet, serveurs d'applications, Smartphones, Services d'urgence, infrastructures, autres véhicules, concessions, garages, gestionnaires de flotte, loueur, domicile, ...

[0011] Il est connu, notamment du document US8983681, un système et un procédé de communication entre une plateforme télématique d'un véhicule et un serveur distant au moyen d'une liaison sans fil supportant un réseau de communication sécurisé de type de type VPN (Virtual Private Network). Une telle liaison permet d'échanger des informations de manière unique sécurisée une fois le réseau virtuel constitué.

[0012] Il est également connu d'interdire ou inhiber l'accès à certaines fonctionnalités offertes par la plateforme télématique tant que le véhicule roule (vitesse longitudinale non nulle) ceci afin de ne pas distraire le conducteur pendant

la conduite. Ainsi, le visionnage de vidéos ou photos sur l'écran du véhicule ou le paramétrage de fonctionnement du véhicule, sont inhibés tant que le véhicule roule.

[0013] En effet, la réglementation interdit tout comportement accidentogène par manque d'attention quand le véhicule roule.

[0014] Toutefois, les différentes solutions de l'état de l'art, ne permettent pas l'identification de l'équipement mobile appartenant au passager et donc, notamment par ce bais, de l'identification du passager lui-même.

[0015] Identification d'autant plus importante et nécessaire qu'elle permettra de valider l'équipement qui sera dédié à l'échange d'informations confidentielles à l'intérieur du véhicule.

[0016] Pour réaliser cela, il faut des interactions étroites entre les ressources télématiques du véhicule, les moyens bureautiques embarqués, la prise en compte du profil de l'utilisateur, de ses droits d'accès et de son équipement : tablette et/ou Smartphone privé ou professionnel, etc.

[0017] A cet effet, la présente invention a pour premier objet un système de communication sécurisé entre un véhicule automobile doté d'une plateforme télématique et au moins un serveur distant privé, caractérisé en ce qu'il comporte un dispositif d'identification d'au moins un équipement mobile de communication et de vérification des droits d'accès d'un passager à bord du véhicule audit équipement mobile, la plateforme télématique étant apte à communiquer avec le serveur distant privé pour recevoir et émettre des données confidentielles par voie d'ondes, à partir d'un réseau privé sécurisé de type VPN, établi entre le véhicule et le serveur distant privé, la restitution des données sur l'équipement mobile n'étant autorisée que si l'équipement mobile a été identifié et que les droits d'accès ont été vérifié par le dispositif d'identification et de vérification en fonction d'un paramétrage déterminé.

[0018] Selon une caractéristique, l'équipement mobile est couplé à la plateforme télématique et n'est apte à échanger des données via la liaison sécurisée que si

ledit équipement a été paramétré par le passager avant la connexion au serveur distant privé.

[0019] Selon une autre caractéristique, à défaut de paramétrage par le passager du véhicule, la diffusion des informations à l'intérieur du véhicule est limitée à la diffusion sur l'équipement mobile appartenant au conducteur.

[0020] Selon une autre caractéristique, le dispositif d'identification et de vérification des droits d'accès comporte un ensemble de moyens aptes à lire au moins un code confidentiel.

[0021] La présente invention a pour deuxième objet, un véhicule automobile comportant une plateforme télématique, un dispositif d'identification d'au moins un équipement mobile de communication et de vérification des droits d'accès d'un passager à bord du véhicule audit équipement mobile, couplé à la plateforme télématique ; ladite plateforme étant apte à communiquer directement avec un serveur distant privé pour recevoir et émettre des données via une liaison sans fil à partir d'un réseau privé sécurisé de type VPN établi entre le véhicule et le serveur distant privé, et à ne restituer les données sur l'équipement mobile que si l'équipement mobile a été identifié et que les droits d'accès ont été vérifié par le dispositif d'identification et de vérification (DIV) en fonction d'un paramétrage déterminé.

[0022] La présente invention a pour troisième objet, une application du système tel que décrit ci-dessus, à l'utilisation du véhicule automobile comme poste de travail étendu pour au moins un passager dudit véhicule disposant d'un moins un équipement de communication mobile couplé à la plateforme télématique du véhicule.

[0023] La présente invention permet ainsi d'offrir aux passagers d'un véhicule disposant de ressources télématiques, la possibilité de poursuivre une tache qui aurait été interrompue par un trajet automobile et ce en toute sécurité et confidentialité des échanges, quasiment comme si le passager était dans son environnement professionnel habituel.

[0024] D'autres caractéristiques et avantages apparaîtront encore à travers la description qui suit d'un exemple de réalisation donné à titre indicatif et non limitatif, en regard du dessin annexé à la figure 1, d'un mode de réalisation d'un système de communication selon l'invention.

[0025] La figure 1 illustre un véhicule VHL doté d'une plateforme télématique PT, et d'un dispositif DIV d'identification et de vérification des droits d'accès du passager désireux de connecter un équipement mobile en passant par ou au travers de ladite plateforme télématique en utilisant une IHM (Interface Homme machine) couplée la plateforme télématique du véhicule.

[0026] La plateforme télématique PT est apte à communiquer avec un serveur distant privé SE qui est par exemple l'un des serveurs de l'entreprise dans laquelle le passager du véhicule exerce son activité professionnelle habituelle.

[0027] La plateforme télématique PT reçoit et émet des données par la voie des ondes et, à partir d'un réseau privé sécurisé de type VPN, établit une connexion sécurisée entre le véhicule VHL et le serveur distant privé SE.

[0028] La connexion audit réseau privé sécurisé SE, est conditionnée par le paramétrage des droits d'accès déterminé par le passager au moment de son entrée dans le véhicule ou déjà préprogrammé par défaut ou pas, dans le véhicule.

[0029] Le dispositif d'identification permet d'identifier l'équipement mobile qui est connecté à la plateforme télématique, et que le passager a bien les droits pour utiliser ledit équipement en fonction du paramétrage programmé ou programmé par le passager au moment de son entrée dans le véhicule.

[0030] Si ces conditions sont réunies alors un échange bidirectionnel, montant et descendant des données entre le serveur distant privé et l'équipement est possible.

[0031] Une application particulièrement intéressante est celle dans laquelle, le véhicule est un véhicule avec chauffeur, et dans lequel un ou plusieurs passagers sont assis à l'arrière du véhicule.

[0032] Lors d'un arrêt ponctuel du véhicule, permettant au passager de sortir du véhicule momentanément, la connexion sera alors suspendue pour pouvoir être reprise sans avoir à ressaisir à nouveau les identifiants et mots de passe de la connexion. Toutefois, une nouvelle connexion ne sera possible que si le système détecte que le passager est bien le même qu'avant l'interruption de la communication

[0033] Les méthodes d'identification du passager et/ou de mouvement du passager sont déjà connues et rappelées ci-après à titre indicatif : reconnaissance faciale, reconnaissance d'iris, …, détection d'empreintes sur le volant ou poignée du véhicule, …, reconnaissance vocale, capteurs de siège, capteurs d'ouverture/fermeture de portes, etc.

[0034] La détection d'ouverture d'une porte associée à la non reconnaissance faciale du passager pourra signifier qu'un nouveau passager est entré dans le véhicule et que la confidentialité des échanges n'est plus garantie.

[0035] Dans ce cas, le nouveau passager devra disposer des mêmes droits d'accès que le précédent passager ou que le précédent passager lui ait délégué ses droits d'accès pour pouvoir prendre et/ou partager la communication.

[0036] Une réunion virtuelle entre les passagers du véhicule et des utilisateurs distants connectés au réseau privé pourra alors se tenir en toute sécurité et confidentialité.

[0037] Le système pourra le cas échéant commander le verrouillage des portes même si le véhicule est à l'arrêt pour garantir la sécurité ainsi que le noircissement des vitres.

[0038] Toute tentative d'effraction pourra être détectée interrompant instantanément la connexion et détruisant toutes les données enregistrées dans l'équipement ou les équipements mobiles connectés.

[0039] Le passager peut paramétrer avant ou pendant trajet, le mode de diffusion des informations qui seront échangées entre le véhicule et le serveur distant. Ainsi

quand il ne souhaite pas que le conducteur ait accès aux informations confidentielles, il peut choisir de ne pas afficher les informations confidentielles sur l'écran du véhicule ou de brouiller ces informations. Les informations ne seront alors affichées en clair que sur l'un des équipements mobiles appartenant au passager.

[0040] A défaut de paramétrage par le passager du véhicule, la diffusion des informations à l'intérieur du véhicule est limitée à la diffusion sur l'équipement mobile appartenant au conducteur.

[0041] Les codes d'accès : identifiants, mots de passe peuvent être mémorisés dans le véhicule mais le paramétrage est à refaire avant chaque nouveau trajet. Par défaut, le mode confidentiel est sélectionné : affichage uniquement sur le Smartphone du passager connecté au véhicule.

[0042] Dès qu'un changement de situation par rapport au paramétrage ou à la confidentialité des échanges survient, le passager est averti.

[0043] Dans le cas où les conditions ne seraient pas réunies et donc le cas où une connexion sécurisée avec le serveur d'entreprise serait interdite, le passager est informé de cet état par un affichage approprié sur de son Smartphone SMP.

[0044] Les terminaux mobiles présents dans le véhicule peuvent être connectés à la plateforme télématique par une liaison filaire de type USB, ou sans fil, par exemple via les standards de communication Bluetooth, Wifi, etc.

[0045] Le passager peut alors visualiser directement sur l'écran de son Smartphone SMP et/ou sur l'écran d'affichage couplé à la plateforme télématique PT si le seul passager est le conducteur, le suivi et l'établissement de la connexion en saisissant ses identifiants et mots de passe

[0046] Dans un exemple de scénario, où le conducteur est le seul passager et qu'il ne conduit pas, l'information est affichée sur un écran appartenant au véhicule et le conducteur demande l'autorisation de se connecter au réseau de son entreprise via un code sécurisé émis au travers de la plateforme télématique du

véhicule en utilisant l'IHM (interface homme-machine) associée à l'écran : bouton ou « push » physique sur la planche de bord et/ou menu et touches associées sur un écran tactile.

[0047] Une fois l'autorisation acquise, il peut se connecter sur l'écran de son véhicule et/ou connecter ses équipements ou terminaux mobiles (Smartphone, PC...) pour accéder légalement et en toute sécurité au réseau de son entreprise.

[0048] Dans un autre d'exemple de scénario, où le passager ne conduit pas et qu'il n'est pas dans un véhicule avec chauffeur, un taxi ou un tout autre véhicule de transport de ce type, il peut également connecter ses équipements ou terminaux mobiles (Smartphone, PC...) à la plateforme télématique du véhicule pour accéder légalement et en toute sécurité au réseau de son entreprise,

[0049] Dans les deux scénarii, une fois le passager connecté au serveur de son entreprise, il peut naviguer sur le site intranet de son entreprise, avoir accès à sa messagerie professionnelle, au réseau interne de l'entreprise pour partager des informations avec d'autres terminaux connectés au réseau interne et des notes via une messagerie instantanée professionnelle, etc.

Revendications

1. Système de communication sécurisé entre un véhicule automobile (VHL) doté d'une plateforme télématique (PT) et au moins un serveur distant privé (SE) , caractérisé en ce qu'il comporte un dispositif (DIV) d'identification d'au moins un équipement mobile de communication (SMP) et de vérification des droits d'accès d'un passager à bord du véhicule (VHL) audit équipement mobile (SMP), la plateforme télématique (PT) étant apte à communiquer avec le serveur distant privé (SE) pour recevoir et émettre des données confidentielles par voie d'ondes, à partir d'un réseau privé sécurisé de type VPN, établi entre le véhicule et le serveur distant privé (SE), la restitution des données sur l'équipement mobile (SMP) n'étant autorisée que si l'équipement mobile (SMP) a été identifié et que les droits d'accès ont été vérifié par le dispositif d'identification et de vérification (DIV) en fonction d'un paramétrage déterminé.

2. Système de communication selon la revendication précédente, caractérisé en ce que l'équipement mobile (SMP) est couplé à la plateforme télématique (PT) et n'est apte à échanger des données via la liaison sécurisée que si ledit équipement (SMP) a été paramétré par le passager avant la connexion au serveur distant privé (SE).

3. Système selon la revendication précédente, caractérisé en ce qu'à défaut de paramétrage par le passager du véhicule (VHL), la diffusion des informations à l'intérieur du véhicule est limitée à la diffusion sur l'équipement mobile (SMP) appartenant au conducteur.

4. Système de communication selon l'une des revendications précédentes, caractérisé en ce que le dispositif d'identification et de vérification des droits d'accès (DIV) comporte un ensemble de moyens aptes à lire au moins un code confidentiel

5. Véhicule automobile (VHL) comportant une plateforme télématique (PT), un dispositif (DIV) d'identification d'au moins un équipement mobile de communication (SMP) et de vérification des droits d'accès d'un passager à bord du véhicule (VHL) audit équipement mobile (SMP), couplé à la plateforme télématique (PT) ; ladite plateforme (PT) étant apte à communiquer directement avec un serveur distant privé (SE) pour recevoir et émettre des données via une liaison sans fil à partir d'un réseau privé sécurisé de type VPN établi entre le véhicule (VHL) et le serveur distant privé (SE), et à ne restituer les données sur l'équipement mobile (SMP) que si l'équipement mobile (SMP) a été identifié et que les droits d'accès ont été vérifié par le dispositif d'identification et de vérification (DIV) en fonction d'un paramétrage déterminé.

6. Application du système selon l'une des revendications 1 à 4, à l'utilisation du véhicule automobile (VHL) comme poste de travail étendu pour au moins un passager dudit véhicule (VHL) disposant d'un moins un équipement de communication mobile couplé à la plateforme télématique (PT) du véhicule (VHL).

.

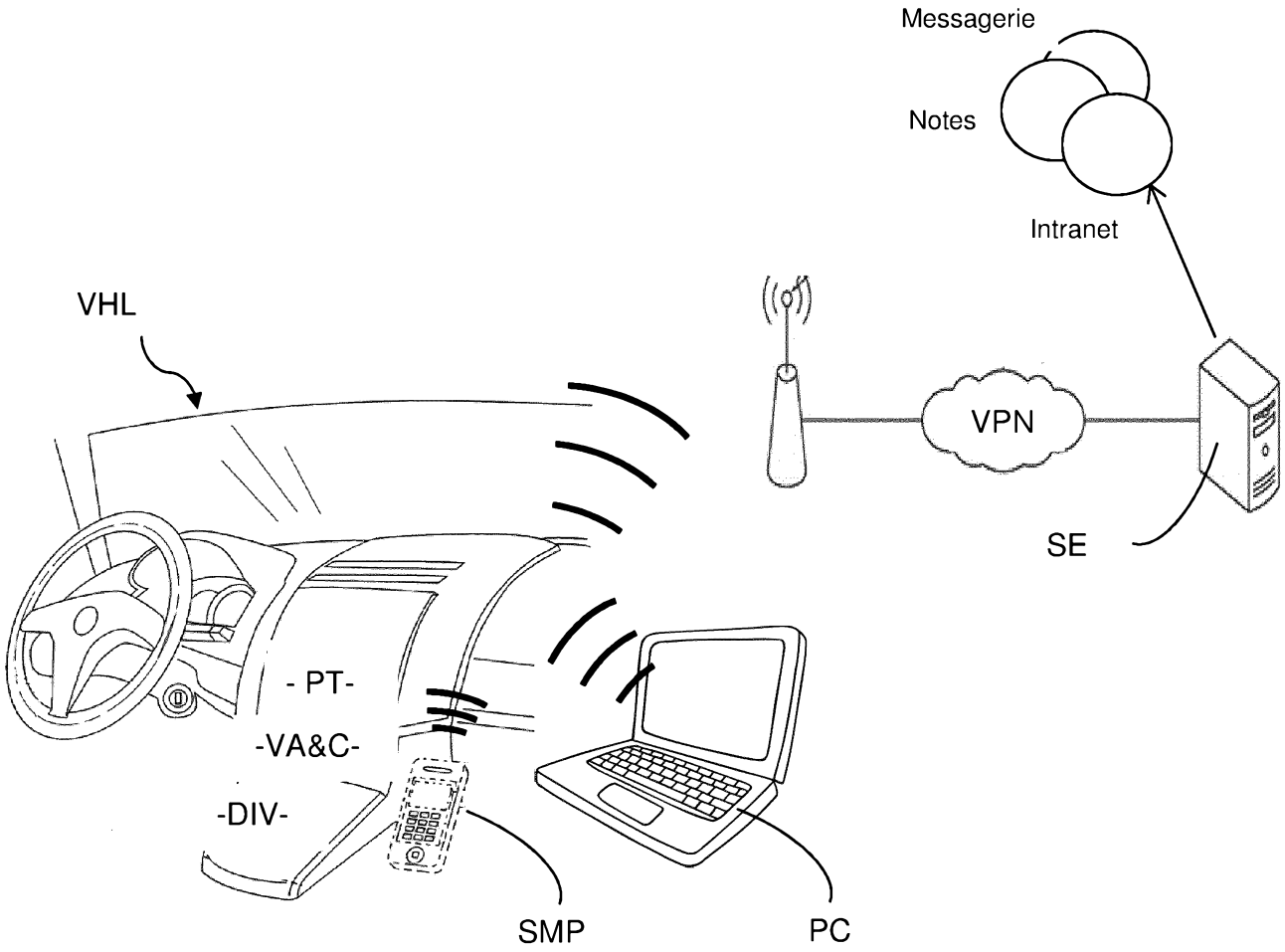

FIG. 1

N° d'enregistrement national : 1650643 N° de publication : 3047140

RAPPORT DE RECHERCHE

articles L.612-14, L.612-17 et R.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ÉTABLISSEMENT DU PRÉSENT RAPPORT DE RECHERCHE

- [x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.
- [x] Le demandeur a maintenu les revendications.
- [ ] Le demandeur a modifié les revendications.
- [ ] Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.
- [ ] Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.
- [ ] Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITÉS DANS LE PRÉSENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

- [x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.
- [ ] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.
- [ ] Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.
- [ ] Aucun document n'a été cité en cours de procédure.

N° d'enregistrement national : 1650643 N° de publication : 3047140

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

US 2015/005984 A1 (DE LOS SANTOS HANLY [US] ET AL)
1 janvier 2015 (2015-01-01)

US 2013/090782 A1 (YI KI HAK [CA] ET AL)
11 avril 2013 (2013-04-11)

US 2012/161927 A1 (PIERFELICE JEFFREY EDWARD [US] ET AL)
28 juin 2012 (2012-06-28)

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

NEANT

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT