

DESCRIPTION**TITRE : Procédé de sécurisation des communications au standard V2X ; Dispositif et protocole associés.**

La présente invention concerne le domaine des véhicules autonomes et, plus particulièrement, la sécurisation des communications entre les dispositifs d'un système de conduite automatique.

La conduite automatique repose sur la communication d'informations pour étendre les domaines d'usage des véhicules impliqués. Le domaine d'usage d'un véhicule, ou ODD (« Operational Design Domain of the vehicles »), est le domaine d'utilisation du véhicule tel que le fonctionnement de l'ensemble du système de conduite automatique soit garanti.

Le standard V2X vise à normaliser les communications entre les dispositifs d'un système de conduite automatique.

Le standard V2X (« Vehicle-to-Everything » ou « Vehicle avec tout ») permet à un véhicule d'échanger des informations avec d'autres éléments de son environnement, que ce soit avec un autre véhicule V2V (« Vehicle-to-Vehicle » ou « Véhicule-à-Véhicule »), avec un équipement d'infrastructure V2I (« Vehicle-to-Infrastructure » ou « Véhicule-à-Infrastructure »), avec un piéton V2P (« Vehicle-to-Pedestrian » ou « Véhicule-à-Piéton »), etc.

Le standard V2X est fondé sur des communications selon la norme IEEE 802.11 (c'est-à-dire du type Wi-Fi), en particulier la norme IEEE 802.11p-2010, mais une évolution du V2X, le V2X cellulaire ou C-V2X (« Cellular V2X »), envisage des communications selon la norme 4G LTE or 5G (c'est-à-dire du type GSM), en particulier la norme LTE-V2X (3GPP standard, version of 2016).

Pour pouvoir opérer un véhicule en délégation de conduite, il faut pouvoir démontrer sa sûreté.

Le document CN111726784 propose par exemple une stratégie pour augmenter la sécurité globale d'un système de conduite automatique en établissant une coopération entre les usagers d'une route et les équipements d'infrastructure de cette route en mettant à profit le standard V2X.

Cependant, cette stratégie ne permet pas de garantir le niveau de sécurité de chaque contribution au fonctionnement global du système, en particulier des communications. Le niveau de sécurité effectivement atteint par le système proposé n'est donc pas défini.

Ainsi, il n'est à l'heure actuelle pas possible de déterminer le niveau de sûreté offert par un système de conduite automatique en se basant sur les informations de connectivité standard.

Il est par conséquent nécessaire de prévoir une personne à bord du véhicule pour
5 prendre le contrôle de ce dernier en cas de danger. Cette personne préposée à la sécurité peut être un conducteur qui surveille l'évolution du véhicule sans toucher le volant, mais est prêt à le faire lorsqu'il y a un danger.

L'invention a donc pour but de résoudre ce problème, en proposant notamment des
10 dispositifs de communication permettant de garantir le niveau de sécurité des communications au standard V2X entre les dispositifs d'un système de conduite autonome.

Pour cela l'invention a pour objet un procédé de sécurisation des communications
au standard V2X entre un dispositif émetteur et un dispositif récepteur d'un système de
conduite automatique, caractérisé en ce que ledit procédé comporte : une étape de
synchronisation temporelle des calculateurs vitaux des dispositifs émetteur et récepteur à
15 partir d'au moins une source temporelle externe commune ; une étape de génération d'un
message au standard V2X par le dispositif émetteur consistant à dater le message en
requérant une date courante auprès du calculateur vital du dispositif émetteur et en
incorporant la date courante en tant que date de message dans un champ du message au
standard V2X ; une étape d'émission du message au standard V2X par le dispositif
20 émetteur ; une étape de réception du message au standard V2X par le dispositif récepteur ;
et, une étape de vérification d'une validité temporelle du message au standard V2X reçu
par le dispositif récepteur en comparant une date courante donnée par le calculateur vital
du dispositif récepteur avec la date d'émission incorporée dans le message au standard
V2X reçu.

25 Suivant des modes particuliers de réalisation, ce procédé comporte une ou plusieurs
des caractéristiques suivantes, prises isolément ou suivant toutes les combinaisons
techniquement possibles :

- l'étape de synchronisation temporelle des calculateurs vitaux des dispositifs
émetteur et récepteur utilise au moins une seconde source de temps externe, dite source
30 de temps externe annexe, qui peut être différente pour les dispositifs émetteur et récepteur,
la synchronisation temporelle du calculateur vital du dispositif émetteur, respectivement du
dispositif récepteur, étant faite en tenant compte des références temporelles délivrées par
les première et seconde sources externes.

- l'étape de synchronisation temporelle d'un calculateur vital consiste en : lancement
35 par le calculateur vital de l'exécution d'un serveur de temps ; émission d'une requête vers
la source temporelle externe commune et réception d'une réponse comportant une

première date ; émission d'une requête vers la source temporelle externe annexe et réception d'une réponse comportant une seconde date ; vérification de la cohérence entre les première et seconde dates, et, en cas d'incohérence, les étapes précédentes sont itérées, et, en cas de cohérence, une référence temporelle interne est établie en
5 considérant qu'il s'agit d'une base de temps commune à tous les composants du système ; et maintenir la référence temporelle interne.

- l'étape de génération d'un message au standard V2X consiste en outre à calculer, par le dispositif émetteur, un code d'authentification portant sur les champs du message au standard V2X et une étape d'incorporation du code d'authentification calculé dans un
10 champ du message, et, en ce que le procédé comporte une étape de vérification d'intégrité du message au standard V2X reçu par le dispositif récepteur en calculant un code d'authentification attendu à partir des champs du message au standard V2X reçu et en comparant le code d'authentification attendu et le code d'authentification présent dans le message au standard V2X reçu.

15 - un code d'authentification est calculé à partir des différents champs du message au standard V2X en utilisant un algorithme de hachage, de préférence l'algorithme SHA-256 avec une clé de hachage secrète dynamique connues des différents dispositifs du système de conduite automatique.

- le code d'authentification est incorporé dans le champ optionnel ou un champ
20 d'extension propre au standard V2X.

L'invention a également pour objet un dispositif de communication compatible du standard V2X, caractérisé en ce qu'il comporte un calculateur vital et un module de radiocommunication, le dispositif étant configuré pour mettre en œuvre les étapes côté
dispositif d'émission et/ou les étapes côté dispositif de réception du procédé précédent.

25 De préférence, le calculateur vital est une plateforme vitale du type « 2oo2 ».

De préférence encore, la plateforme vitale est de nature à garantir un niveau de sûreté élevé respectant le niveau SIL 4 ou ASIL D.

L'invention a également pour objet un protocole de communication compatible du standard V2X selon lequel chaque message au standard V2X comporte un champ
30 incorporant une date de message du message au standard V2X et éventuellement un champ incorporant un code d'authentification du message au standard V2X.

L'invention et ses avantages seront mieux compris à la lecture de la description détaillée qui va suivre d'un mode de réalisation particulier, donné uniquement à titre d'exemple illustratif et non limitatif, cette description étant faite en se référant aux dessins
35 annexés sur lesquels :

[Fig 1] La figure 1 est une représentation schématique d'un mode de réalisation d'un système de conduite automatique selon l'invention ;

[Fig 2] La figure 2 est un chronogramme du processus de synchronisation d'une source de temps interne telle que celle de la figure 2 ; et,

5 [Fig 3] La figure 3 est une représentation sous forme de blocs du procédé de sécurisation des communications selon l'invention mis en œuvre dans le système de la figure 1 ; et,

[Fig 4] La figure 4 est une représentation de la structure d'un message V2X telle que modifiée selon la présente invention.

10 Tout en restant compatible du standard V2X, l'invention met en œuvre des mécanismes sûrs permettant de réaliser : une synchronisation des dispositifs de communication du système de conduite automatique ; un horodatage d'un message par le dispositif de communication émetteur de ce message ; et le contrôle de la validité temporelle de ce message par le dispositif de communication récepteur de ce message.

15 De préférence, l'invention met également en œuvre des mécanismes sûrs permettant de réaliser : une sécurisation des données contenues dans un message émis (et par conséquent la date avec laquelle le message a été horodaté) et le contrôle de l'intégrité du message reçu.

La figure 1 représente schématiquement un système de conduite automatique 1.

20 Ce système comporte des premier et second dispositifs de communication 2 et 3 permettant des échanges selon le standard V2X.

Dans le mode de réalisation de la figure 1, le premier dispositif 2 est associé à un équipement d'infrastructure 4, et le second dispositif 3 est embarqué à bord d'un véhicule 5.

25 Dans le mode de réalisation présenté ici en détail, l'équipement d'infrastructure 4 est un feu de circulation tricolore, placé à l'intersection de deux routes. L'état de cet équipement peut prendre trois valeurs possibles, qui sont identifiées par la couleur du feu (« vert », « orange » ou « rouge »).

30 Le but de la communication V2X, entre le premier dispositif 2 en tant que dispositif émetteur et le second dispositif 3 en tant que dispositif récepteur, est alors d'informer le véhicule 5 de la présence d'une intersection et de l'état du feu tricolore qui la protège, afin que le calculateur de pilotage 7 du véhicule détermine une trajectoire adaptée pour le véhicule 5.

Le premier dispositif de communication 2 comporte :

- 35
- un module de géolocalisation 21 ;
 - un module de radiocommunication V2X 22 ;

- un module de communication annexe 23 ;
- un calculateur vital 24 ; et
- un module de routage 25.

Le module de géolocalisation 21 est notamment propre à recevoir des signaux de géolocalisation émis par une constellation de satellites 11. Ces signaux comportent en particulier un signal d'horloge. La constellation de satellites 11 constitue par conséquent un exemple d'une source externe commune de référence temporelle. Le module de géolocalisation 21 exécute par exemple un serveur de temps 41 permettant, en réponse à une requête d'interrogation, d'indiquer une date selon la référence temporelle de la source externe commune.

Le module de radiocommunication V2X 22 permet la génération de messages selon le standard V2X, la transmission de messages selon le standard V2X avec les autres dispositifs de communication du système de conduite automatique 1, en particulier le second dispositif de communication 3, et le traitement des messages selon le standard V2X.

Le module de communication annexe 23 permet d'établir une liaison avec un réseau externe 12, par exemple un réseau IP, comme l'Internet. Le module 23 est connecté au réseau externe 12 par une liaison filaire (Ethernet par exemple) ou sans fil (4G/LTE par exemple). Cette liaison permet une communication du premier dispositif 2 avec un central de contrôle 13 distant, qui permet la gestion des équipements d'infrastructure par un opérateur.

Cette liaison permet surtout au premier dispositif 2 de communiquer avec une plateforme externe 14 constituant une première source externe annexe de référence temporelle. Cette plateforme externe exécute par exemple un serveur de temps 42, permettant, en réponse à une requête d'interrogation, d'indiquer une date selon la référence temporelle de la source externe commune.

Le calculateur vital 24 constitue en particulier une source interne de référence temporelle. Le calculateur vital 24 exécute par exemple un serveur de temps 43, permettant, en réponse à une requête d'interrogation, d'indiquer une date selon la référence temporelle de la source interne. Le calculateur vital 24 du premier dispositif est synchronisé à partir de la source externe commune et de la première source externe annexe. Selon l'invention, une date délivrée par le calculateur vital 24 permet notamment d'horodater des messages V2X émis par le dispositif 2.

Le calculateur vital 24 est avantageusement en charge de vérifier la validité de l'information issue du contrôleur 6, par exemple en la corrélant avec les mesures effectuées par le moyen de mesure 15.

Le calculateur vital 24 est également en charge de signer ou de vérifier en sûreté l'intégrité du « champ HMAC » d'un message V2X.

Le module de routage 25 permet d'interfacer les différents modules 21, 22, 23 et 24 entre eux et avec un contrôleur 6 de l'équipement d'infrastructure 4 et des moyens 15 de mesure de l'état de l'équipement d'infrastructure 4.

Le module de routage 25 est relié, par une connexion externe, au contrôleur 6. Ce contrôleur 6 est propre à déterminer l'état courant de l'équipement d'infrastructure 4. En variante, il est également propre à déterminer l'état à venir de l'équipement d'infrastructure 4. L'état à venir est soit l'état de l'équipement d'infrastructure au prochain pas de temps, soit le prochain état vers lequel va basculer l'équipement d'infrastructure. Dans ce dernier cas, l'état à venir comporte une information temporelle correspondant à l'instant prévu pour ce basculement.

Les moyens de mesure 15 permettent de mesurer le courant de lampe de chacune des trois lampes du feu tricolore 4 et d'appliquer un signal de mesure adapté au routeur 25.

Le second dispositif de communication 3 est de préférence identique au premier dispositif 2 venant d'être décrit.

Le second dispositif 3 comporte ainsi :

- un module de géolocalisation 31 ;
- un module de radiocommunication V2X 32 ;
- un module de communication annexe 33 ;
- un calculateur vital 34 ; et
- un module de routage 35.

Le module de géolocalisation 31 est propre à recevoir des signaux de géolocalisation émis par la constellation de satellites 11, qui constitue bien une source de référence temporelle commune aux dispositifs 2 et 3. Le module de géolocalisation 31 exécute par exemple un serveur de temps 51 permettant, en réponse à une requête d'interrogation, d'indiquer une date selon la référence temporelle de la source externe commune.

Le second dispositif 3 est connecté de sorte que le module de communication 33 soit maintenant relié à une seconde source externe annexe de référence temporelle associée au véhicule 5, par exemple à un serveur de temps 52 exécuté par le calculateur de pilotage 7 du véhicule.

Le calculateur vital 34 constitue notamment une source interne de référence temporelle. Il exécute par exemple un serveur de temps 53 permettant, en réponse à une requête d'interrogation, d'indiquer une date selon la référence temporelle de la source interne. Le calculateur vital 34 du second dispositif est synchronisé à partir de la source

externe commune et de la seconde source externe annexe. Selon l'invention, une date délivrée par le calculateur vital 34 permet notamment d'horodater des messages V2X émis par le dispositif 3.

Le calculateur vital 34 est également en charge de signer ou de vérifier en sûreté l'intégrité du « champ HMAC » d'un message V2X.

Le module de radiocommunication V2X 32 est propre à recevoir un message V2X, à vérifier son intégrité, puis sa validité temporelle, avant de transmettre l'information contenue dans le message V2X reçu vers le calculateur de pilotage 7 via le module de routage 35. Cette information est par exemple l'état de l'équipement d'infrastructure 4 associé au premier dispositif 1 dont un message vient d'être reçu.

Un calculateur vital, comme le calculateur 24 ou le calculateur 34, est une plateforme de traitement vital du type « 2oo2 » (« two out of two » ou « deux parmi deux ») de nature à garantir un niveau de sûreté élevé dans les calculs réalisés, comme la détermination de la référence temporelle interne à partir des références temporelles externes délivrées par les deux sources commune et annexe auquel le module d'horloge est couplé. Le calculateur vital respecte par exemple le niveau 4 de la norme SIL (« Safety Integrity Level ») ou D de la norme ASIL (« Automotive Safety Integrity Level »).

Le flux de données du processus de synchronisation 100 de la source temporelle interne d'un dispositif de communication est représenté sur la figure 2 :

- dans l'étape 110, le module d'horloge lance l'exécution du serveur de temps 43.

Celui-ci est calibré en interrogeant la source externe commune et la source externe annexe. Pour ce faire :

- dans l'étape 130a, le module 24 émet une requête vers la source externe commune, plus précisément le serveur de temps 41 du module 21 (la requête est par exemple une requête selon le standard « Network Time Protocol » - NTP) ;

- dans l'étape 140a, le serveur de temps 41 du module 21 répond à la requête en délivrant une première date fondée sur la référence temporelle de la source externe commune (la requête est par exemple une réponse NTP) ;

- dans l'étape 130b, le module 24 émet une requête vers la source externe annexe, c'est-à-dire le serveur de temps 42 ;

- dans l'étape 140b, le serveur de temps 42 répond à la requête en délivrant une seconde date fondée sur la référence temporelle de la première source externe annexe ;

- Puis, dans l'étape 155, si le module 24 conclut à une cohérence entre les première et seconde dates entre elles, la référence temporelle interne est établie en considérant qu'il s'agit d'une base de temps commune à tous les composants du système 1. A défaut, le processus 100 boucle sur l'étape 110 et est itéré à nouveau ;

- Dans l'étape 160, le module 24 maintient la référence temporelle interne.

Le processus 100 est exécuté périodiquement pour éliminer tout risque de dérive temporelle de la source temporelle interne.

Une fois le module 24 synchronisé, c'est la date délivrée par le serveur de temps 43
5 qui est utilisée pour dater les messages V2X émis par le dispositif 2.

Une description similaire pourrait être faite pour le dispositif 3 afin de synchroniser la source temporelle interne que constitue le module 34.

En se référant à la figure 3, le procédé de communication 200 comporte :

Une étape préalable de synchronisation des différents dispositifs du système en
10 mettant en œuvre, sur chaque dispositif, le processus 100 décrit précédemment.

Puis, côté équipement d'infrastructure 4, pour la diffusion de l'état de cet équipement, le procédé comporte une étape 210 de détermination de l'état de l'équipement d'infrastructure. La détermination de l'état de l'équipement d'infrastructure est une fonction vitale. Par exemple, le calculateur vital 24 compare l'état du feu de signalisation indiqué par
15 le contrôleur 6 et l'état correspondant au courant de lampe mesuré par les moyens de mesure 15 afin de déterminer l'état vital.

A l'étape 220, le module 22 met en forme un message selon le standard V2X, par exemple un message SPAT.

Le standard V2X définit un message SPAT (« Signal Phase and Timing » ou
20 « Phase et synchronisation des signaux ») permettant à un équipement d'infrastructure d'informer l'environnement sur son état.

Selon l'invention, certains de ces champs de la partie de charge utile d'un message au format V2X sont utilisés pour passer les informations utiles à la fonction de validité temporelle et, de préférence également, les informations utiles à la fonction de vérification
25 d'intégrité selon l'invention. Cela permet de rester compatible avec le standard V2X tout en permettant de mettre en œuvre une détection de la corruption des messages de nature à garantir un niveau de sécurité élevé.

Pour la fonction de validité temporelle, le message est daté avec une date de message. La date de message incorporée dans le message est celle retournée par le
30 serveur de temps interne 43 sur requête du module 22 lorsqu'il prépare le message V2X à émettre.

Pour la fonction de vérification d'intégrité, le message comporte un code HMAC (« hash-based message authentication code » ou « code d'authentification de message fond sur une fonction de hachage »).

35 Par exemple un code HMAC tronqué de 64 bits est généré par le calculateur vital 24, sur demande du module 22, à partir des différents champs du message SPAT (sauf la

portion destinée à incorporer le code HMAC qui ne comporte alors que des zéros) en utilisant de préférence l'algorithme SHA-256 et une clé de hachage secrète dynamique de 64 octets connues des différents dispositifs du système 1.

Une fois la charge utile du message SPAT préparée, le message est codé en base 64, puis communiqué à l'unité de radiocommunication du module 22 pour sa transmission (étape 230).

Côté véhicule 5, le message V2X est reçu puis décodé par le dispositif 3 (étape 240).

Dans l'étape 250 de vérification de l'intégrité du message V2X reçu, le module 32 décode le message reçu. Sur demande du module 32, le calculateur vital 34 du second dispositif 3 calcule un code HMAC sur les champs du message SPAT (sauf la portion incorporant le code HMAC calculé par l'émetteur, qui ne comporte alors que des zéros) et compare le code HMAC ainsi calculé avec le code HMAC contenu dans le champ du message V2X reçu. En cas de comparaison négative, le message V2X reçu est rejeté. En cas de comparaison positive, le procédé se poursuit à l'étape 260. Cela permet de vérifier l'intégrité des données et l'authenticité du message V2X reçu.

Puis, dans l'étape 260, le calculateur vital 34 du dispositif 3 extrait la date de message incorporée dans le message V2X reçu et la compare à la date courante du dispositif 3. Cette dernière est obtenue par interrogation de la source temporelle interne du dispositif 2. Si la date de message diffère de manière trop importante de la date courante du dispositif 3, le message V2X est rejeté. Dans le cas contraire, le message V2X reçu est validé temporellement. Cela permet de vérifier la validité temporelle du message V2X reçu.

En cas de vérification positive, les informations contenues dans le message V2X (en l'occurrence l'état de l'équipement d'infrastructure 4) sont transmises au calculateur 7 pour prise en compte (étape 270).

La figure 4 représente la structure d'un message SPAT comme exemple de message V2X pouvant être modifié pour incorporer une date de message et éventuellement un code de vérification d'intégrité. On notera qu'un champ non-optionnel du standard est dit d'extension.

La partie d'en-tête du message comporte :

Un champ « Protocole Version » ou de « Version de Protocole » ;

Un champ « Message ID » ou d' « Identifiant de Message » ;

Un champ « Station ID » ou d' « Identifiant de Station ».

La partie de charge utile comporte :

Un champ optionnel « MoY » pour « Moment of the Year » ou d'« instant de l'année », c'est-à-dire de datation du message ;

Un champ « Desc. Name » ou de « Nom de Description » codé sur 63 bytes ;

Un champ « Intersection List » ou de « Liste d'Intersection » codé sur entre 1 et 32 bytes ;

Un champ optionnel « Regional » ou de « paramètres locaux » codé sur entre 1 et 4 bytes.

Selon l'invention, le champ « Desc. Name » de description textuelle de l'équipement d'infrastructure est partiellement réaffecté à la protection du message. Son contenu est ainsi adapté pour comporter :

Un champ « Shortened DescName » ou de « Nom de Description abrégé » codé sur entre 1 et 43 bytes ;

Un champ « HMAC Tag » ou d'« d'étiquette HMAC » qui est une balise SHA codé sur 4 bytes, de contenu prédéfini comme par exemple la chaîne de caractère « %#%# » , afin d'indiquer la présence du champ HMAC suivant ; et,

Un champ « HMAC » codé sur 16 bytes et comportant le code HMAC calculé pour la fonction de vérification d'intégrité.

Les informations des champs « HMAC Tag » et « HMAC » sont formatées au format chaîne IA5 du standard V2X pour les champs de texte, afin d'assurer la compatibilité avec ce standard.

Le champ « Intersection List » comporte au moins une champ « Intersection State » ou d'« état d'Intersection » codé sur entre 1 et 32 bytes et qui est utilisé par l'invention de la façon suivante :

Un champ optionnel « Desc. Name » ou de « Nom de description » codé sur 63 bytes ;

Un champ « Msg Cnt- Rev » ou de « Contenu de Message » ;

Un champ « Intersection Status » ou de « Valeur de l'Etat de l'intersection » ;

Un champ « MoY » pour « Moment of the Year » ou « instant de l'année » qui est optionnel selon le standard mais obligatoire selon l'invention et qui est modifié pour comporter la date de message ;

Un champ « Desc » ou de « Description » codé sur 63 bytes ;

Un champ Optionnel « Enable Lanes Liste » ou de « Liste de Voies Ouvertes à la circulation » ;

Un champ « Movement List » ou de « Liste de Mouvement » codé sur entre 1 et 255 bytes.

Un champ optionnel « Maneu. Assist » ou d'« assistance à la Manœuvre » ; et,

Un champ optionnel « Regional » ou de « paramètres locaux » codé sur entre 1 et 4 bytes.

Si le mode de réalisation présenté ci-dessus concerne la communication depuis un dispositif émetteur équipant un équipement d'infrastructure vers un dispositif récepteur à bord d'un véhicule, l'invention est plus générale. Elle pourrait par exemple s'appliquer pour garantir des messages V2X de communication depuis un dispositif émetteur équipant un véhicule vers un dispositif récepteur associé à un équipement d'infrastructure. Ce cas est celui par exemple d'un véhicule prioritaire (ambulance, voiture de police...) ayant la possibilité de demander une modification de l'état de l'équipement d'infrastructure. Par exemple, que l'état des feux tricolores protégeant une intersection soient adaptés pour permettre à ce véhicule prioritaire un franchissement rapide de l'intersection concernée.

L'invention pourrait par exemple encore s'appliquer pour garantir des messages V2X de communication depuis un dispositif émetteur équipant un véhicule vers un dispositif récepteur équipant un autre véhicule.

Par ailleurs, si on a plus particulièrement présenté l'invention sur un message SPAT, d'autres types de message du standard V2X peuvent être altérés pour permettre la mise en œuvre des fonctions de vérification temporelle et de vérification d'intégrité.

L'invention permet d'inclure dans un échange V2X, une signature temporelle et une avantageusement également une signature de sécurité. Ces signatures sont codées/décodées par une implémentation standard des couches radio du standard V2X. Elles ne perturbent donc pas l'exploitation existante des champs des messages V2X. Dit autrement, un dispositif « ordinaire », c'est-à-dire qui ne mettrait pas en œuvre l'invention, reste capable de traiter les messages V2X altérés selon l'invention. Ce dispositif ordinaire ne pourrait donc pas vérifier ni la validité temporelle, ni l'intégrité des messages.

L'invention permet donc de fiabiliser la date d'un message et de vérifier la validité temporelle de ce message de manière sûre.

L'invention permet d'atteindre des niveaux de sûreté élevés, notamment le niveau SIL 4 (selon la norme EN 50126-1:2017) ou le niveau ASIL D (selon la norme ISO 26262-1:2018), tout en restant compatible du standard V2X. La solution proposée permet donc de garantir le niveau de sécurité des informations clés sur le trafic tout en restant compatible avec la norme de communication.

REVENDICATIONS

1. Procédé de sécurisation (200) des communications au standard V2X, dans sa version SAE J2735:2020-07, entre un dispositif émetteur (2) et un dispositif récepteur (3) d'un système de conduite automatique (1), caractérisé en ce que ledit procédé comporte :

- une étape (100) de synchronisation temporelle d'un calculateur vital (24) du dispositif émetteur (2) et d'un calculateur vital (34) du dispositif récepteur à partir d'au moins une source temporelle externe (11) commune ;

- une étape (220) de génération d'un message au standard V2X par le dispositif émetteur (2) consistant à dater le message en requérant une date courante auprès du calculateur vital (24) du dispositif émetteur et en incorporant la date courante en tant que date de message dans un champ du message au standard V2X ;

- une étape (230) d'émission du message au standard V2X par le dispositif émetteur (2) ;

- une étape (240) de réception du message au standard V2X par le dispositif récepteur (3) ; et,

- une étape (260) de vérification d'une validité temporelle du message au standard V2X reçu par le dispositif récepteur en comparant une date courante donnée par le calculateur vital du dispositif récepteur avec la date d'émission incorporée dans le message au standard V2X reçu.

2. Procédé selon la revendication 1, dans lequel l'étape (100) de synchronisation temporelle des calculateurs vitaux (24, 34) des dispositifs émetteur et récepteur utilise au moins une seconde source de temps externe, dite source de temps externe annexe, qui peut être différente pour les dispositifs émetteur et récepteur, la synchronisation temporelle du calculateur vital du dispositif émetteur, respectivement du dispositif récepteur, étant faite en tenant compte des références temporelles délivrées par les première et seconde sources externes.

3. Procédé selon la revendication 2, dans lequel l'étape de synchronisation temporelle de chaque calculateur vital (24, 34) consiste en :

- lancement (110) par le calculateur vital de l'exécution d'un serveur de temps (43, 53) ;

- émission (130a) d'une requête vers la source temporelle externe commune et réception (140a) d'une réponse comportant une première date ;

- émission (130b) d'une requête vers la source temporelle externe annexe et réception (140b) d'une réponse comportant une seconde date ;

- vérification (155) de la cohérence entre les première et seconde dates, et, en cas d'incohérence, les étapes précédentes sont itérées, et, en cas de cohérence, une référence

temporelle interne est établie en considérant qu'il s'agit d'une base de temps commune à tous les composants du système ; et,

- maintenir (160) la référence temporelle interne.

5 **4.** Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape (220) de génération d'un message au standard V2X consiste en outre à calculer, par le dispositif émetteur (2), un code d'authentification portant sur les champs du message au standard V2X et une étape d'incorporation du code d'authentification calculé dans un champ du message, et, en ce que le procédé comporte une étape (260) de vérification d'intégrité du message au standard V2X reçu par le dispositif récepteur en
10 calculant un code d'authentification attendu à partir des champs du message au standard V2X reçu et en comparant le code d'authentification attendu et le code d'authentification présent dans le message au standard V2X reçu.

5. Procédé selon la revendication 4, dans lequel le code d'authentification est calculé à partir des différents champs du message au standard V2X en utilisant un
15 algorithme de hachage, de préférence l'algorithme SHA-256 avec une clé de hachage secrète dynamique connues des différents dispositifs du système de conduite automatique.

6. Procédé selon la revendication 4 ou la revendication 5, dans lequel le code d'authentification est incorporé dans le champ optionnel ou un champ d'extension propre au standard V2X.

20 **7.** Dispositif de communication compatible du standard V2X, dans sa version SAE J2735:2020-07, caractérisé en ce qu'il comporte un calculateur vital (24, 34) et un module de radiocommunication, le dispositif étant configuré pour mettre en œuvre les étapes côté dispositif d'émission et/ou les étapes côté dispositif de réception du procédé selon l'une quelconque des revendications précédentes.

25 **8.** Dispositif selon la revendication 7, dans lequel le calculateur vital est une plateforme vitale du type « 2oo2 ».

9. Dispositif selon la revendication 8, dans lequel la plateforme vitale est de nature à garantir un niveau de sûreté élevé respectant le niveau SIL 4 ou ASIL D.

30 **10.** Protocole de communication compatible du standard V2X, dans sa version SAE J2735:2020-07, selon lequel chaque message au standard V2X comporte un champ incorporant une date de message du message au standard V2X et éventuellement un champ incorporant un code d'authentification du message au standard V2X.