(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 087 983***
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **18 60038**

(51) Int Cl[8] : ***H 04 L 9/12*** *(2019.01), H 04 W 12/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 30.10.18.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.05.20 Bulletin 20/18.

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

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

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

(71) **Demandeur(s) :** *AIRBUS DEFENCE AND SPACE SAS Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** CHATAIN FRANCIS.

(73) **Titulaire(s) :** AIRBUS DEFENCE AND SPACE SAS Société par actions simplifiée.

(74) **Mandataire(s) :** PLASSERAUD IP.

(54) SYSTEME DE SUPERVISION AMELIORE DE CAPTEURS CONNECTES.

(57) L'invention propose un système de supervision comprenant des terminaux et une passerelle en communication avec un réseau extérieur, la passerelle comprenant au moins un récepteur radiofréquence de liaison avec les terminaux, un calculateur et une mémoire, dans lequel

chaque terminal comprend au moins une alimentation électrique, un module capteur connecté à un module de gestion,

des identifiants de modules de gestion étant associés à au moins un paramètre de déchiffrement dans une table mémorisée dans la passerelle,

le module capteur comprenant au moins un capteur et une mémoire stockant des informations relatives à au moins un protocole de communication,

le module de gestion comprenant au moins un calculateur, une mémoire mémorisant au moins son identifiant et stockant des données représentatives des mesures effectuées, un module de chiffrement, un émetteur radiofréquence et un module d'interface,

le module d'interface pilotant les échanges avec le module capteur en fonction des informations lues en mémoire dudit module,

le module de chiffrement chiffrant des données de mesures dudit capteur et des données de service et/ou de contrôle comprenant au moins une donnée représentative du module capteur,

le module de gestion réalisant l'envoi, à la passerelle, via le module émetteur radiofréquence, d'au moins les données chiffrées et de l'identifiant non-chiffré du module de gestion,

la passerelle comprenant un module de déchiffrement réalisant un déchiffrement en fonction dudit paramètre de déchiffrement associé, dans la table, à l'identifiant reçu du module de gestion.

FR 3 087 983 - A1

DOMAINE DE L'INVENTION

La présente invention concerne le domaine des objets connectés dans un contexte d'usage industriel également appelé I.IOT (Industrial Internet of Things). L'industrie 4.0 est en effet marquée par une ultra-connectivité permettant des fonctions avancée de supervision.

ETAT DE LA TECHNIQUE

La vulnérabilité aux cyberattaques est une préoccupation majeure à laquelle doivent répondre les architectes systèmes. On connait les réseaux privés filaires non reliés à Internet pour lesquels la protection physique de leur site d'implantation offre une bonne sécurité. L'ouverture au réseau Internet peut toutefois s'avérer un avantage compétitif majeur incontournable. De plus les connexions filaires entraînent un coût d'installation particulièrement important.

Les systèmes de communication par ondes radiofréquences, tels que le WiFi, permettent aisément la supervision de capteurs reliés sur des réseaux domestiques sécurisés par clé de chiffrement symétrique. Une caméra peut ainsi être installée et paramétrée pour communiquer avec un centre de sécurité distant, via Internet. On comprend cependant que ce type d'installation est difficilement transposable, voire incompatible avec le monde de l'industrie du fait des contraintes d'installation ou de maintenance découlant du nombre beaucoup plus important de capteurs à superviser.

Il existe ainsi un besoin de simplification dans la supervision des objets connectés, tout en conservant une sécurité accrue de façon à permettre un déploiement massif sécurisé et agile d'objets connectés.

PRESENTATION DE L'INVENTION

L'invention a pour but de remédier au moins en partie aux inconvénients de l'art antérieur en proposant un système de supervision comprenant une pluralité de terminaux et une passerelle en liaison de communication avec un réseau extérieur, la passerelle comprenant au moins un module récepteur radiofréquence de liaison avec la pluralité de terminaux, un calculateur et une mémoire, caractérisé en ce que chaque terminal comprend au moins une alimentation électrique, un module capteur connecté via un connecteur à un module de gestion, une pluralité d'identifiants de modules de gestion étant chacun associé à au moins un paramètre de déchiffrement dans une table mémorisée dans la passerelle, le module capteur, comprenant au moins un capteur et au moins une mémoire stockant des

informations relatives à au moins un protocole de communication et aux broches utiles du connecteur, le module de gestion, comprenant au moins un calculateur, une mémoire mémorisant au moins son identifiant et stockant par ailleurs des données représentatives des mesures effectuées, un module de chiffrement, un module émetteur radiofréquence et un module d'interface, le module d'interface pilotant les échanges avec le module capteur en fonction des informations, lues en mémoire du module capteur, relatives audit protocole de communication et aux broches utiles, le module de chiffrement réalisant le chiffrement des données représentatives des mesures effectuées par ledit capteur et de données de service et/ou de contrôle comprenant au moins une donnée représentative du module capteur, le module de gestion réalisant l'envoie, à la passerelle, via le module émetteur radiofréquence, d'au moins les données chiffrées et de l'identifiant non-chiffré du module de gestion, la passerelle comprenant un module de déchiffrement réalisant un déchiffrement en fonction dudit paramètre de déchiffrement associé, dans la table, à l'identifiant reçu du module de gestion.

Selon une caractéristique de l'invention, la passerelle comprend un module émetteur radiofréquence de liaison avec la pluralité de terminaux, chaque terminal comprenant un module récepteur radiofréquence, les données chiffrées transmises par chaque terminal comprenant un code de contrôle, la passerelle comprenant un module d'envoi de message de réponse,

et en ce que chaque message de réponse, faisant suite à la réception de données provenant du module de gestion, comprend au moins le code de contrôle retransmis à ce module de gestion comme accusé de réception.

Selon une autre caractéristique de l'invention, chaque module de gestion comprend un module de vérification d'accusé de réception déclenchant une mise en veille des modules émetteur et récepteur en cas de confirmation de réception ou déclenchant en cas d'échec de réception, au-delà d'une temporisation déterminée, une réémission du même message, la puissance d'émission étant augmentée.

Selon une autre caractéristique de l'invention, le nombre de réémissions et d'augmentations successives de la puissance d'émission sont limités, le module de gestion déclenchant l'envoi d'un message d'alerte après un nombre déterminé d'échecs de réémissions.

Selon une autre caractéristique de l'invention, le message de réponse comprend une commande de paramétrage dudit terminal ou une commande d'actionneur.

Selon une autre caractéristique de l'invention, la passerelle réalise une authentification du module de gestion par un succès lors du déchiffrement du message reçu.

Selon une autre caractéristique de l'invention, le module d'interface comprend un module de détection de connexion et d'initialisation du module d'interface déclenchant une lecture en mémoire de données de configuration du module capteur comprenant au moins les informations relatives audit protocole de communication et aux broches utiles.

Selon une autre caractéristique de l'invention, les données de configuration comprennent également des données représentatives du type dudit capteur, du format des données mesurées ainsi que d'un canal associé en cas de pluralité de capteurs.

Selon une autre caractéristique de l'invention, le module de détection de connexion et d'initialisation déclenche par ailleurs un envoi d'une trame chiffrée, à la passerelle, représentative de la configuration du module capteur comprenant les données de configuration.

Selon une autre caractéristique de l'invention, la passerelle est en liaison de communication chiffrée avec un serveur dédié du réseau extérieur comprenant au moins un applicatif dédié pour l'exploitation des données de mesure, le module de gestion réalisant un chiffrement des données de contrôle déchiffrables par la passerelle et par l'applicatif dédié et un chiffrement des données de mesures déchiffrables uniquement par l'applicatif dédié.

Selon une autre caractéristique de l'invention, l'applicatif dédié comprend un module d'envoi de commandes chiffrées aux modules de gestions, chaque commande étant déchiffrable uniquement par chaque module de gestion à qui cette commande est adressée.

Selon une autre caractéristique de l'invention, la passerelle comprend un module de coupure d'alimentation de sa liaison de communication avec le serveur dédié et de remise sous tension en cas de sollicitation par un des modules de gestion.

De façon avantageuse, le système de supervision selon l'invention est hautement versatile et permet un déploiement rapide et sécurisé. En effet, ce système peut être intégralement géré par un client, en localisant les terminaux et la passerelle dans ses locaux.

Avantageusement encore, la structure des terminaux permet une supervision présentant une agilité accrue. Un ou plusieurs nouveaux capteurs peuvent aisément venir en remplacement d'un précédent capteur pour des besoins d'évolution ou de maintenance. La mise en place sécurisée d'objets connectés supplémentaires est également facilitée.

De façon avantageuse, pour les opérations de maintenance ou de maintenance prédictive ou préventive des systèmes de supervision dans les entreprises l'invention apportera des gains notamment dans :

- une efficacité opérationnelle accrue des équipements,
- un abaissement des coûts d'exploitation des équipements,
- la qualité accrue de fabrication ou d'une manière générale de la production des produits dans l'entreprise,
- des économies d'énergie de ressources ou de matériel.

Un autre avantage réside dans la récupération simple, rapide et sécurisée des données de surveillance.

Un avantage est également une grande agilité pour le déploiement de solutions de supervision pouvant répondre à des contraintes techniques variées. Un même système de supervision pourra ainsi répondre simultanément à plusieurs cas d'usage tels que la supervision énergétique d'un bâtiment, la supervision d'une ligne de production et le support des outils de logistiques.

Avantageusement encore un mécanisme de rupture protocolaire intégré à la passerelle permet une résistance accrue aux attaques.

Un avantage est également que la structure s'appuyant sur un micro réseau radiofréquence indépendant permet une économie d'énergie tout en renforçant la sécurité par un rayonnement limité.

DESCRIPTION DES FIGURES

D'autres caractéristiques, buts et avantages de l'invention ressortiront de la description qui suit, qui est purement illustrative et non limitative, et qui doit être lue en regard des dessins annexés sur lesquels :

- La figure 1 représente schématiquement un exemple de système de supervision selon l'invention,
- La figure 2 représente schématiquement un exemple plus détaillé de terminal.
- La figure 3 représente schématiquement un exemple plus détaillé de passerelle.
- Les figures 4a à 4c représentent schématiquement trois types de configuration d'un système de supervision selon l'invention,
- La figure 5 représente schématiquement un procédé de transmission de données générées par un capteur au sein d'un système de supervision,
- Les figures 6a et 6b représentent un exemple de structure respectivement d'un message émis par un terminal et d'un message émis en réponse par une passerelle,
- La figure 7 représente schématiquement un protocole de création de clés de chiffrement utilisé pour les transmissions au sein du système de supervision.

DESCRIPTION DETAILLEE D'AU MOINS UN MODE DE REALISATION DE L'INVENTION

Le système de supervision 1 tel que représenté à la figure 1 permet par exemple la récupération de données représentatives de mesures effectuées par des capteurs au sein d'une installation. Avantageusement, le système de supervision 1 selon l'invention ne comprend pas de cœur de réseau, également désigné par server network, comme dans une architecture d'IoT classique. Ainsi selon la présente invention tous les composants peuvent aisément être installés dans les locaux de l'organisme qui souhaite accéder et exploiter les données générées par ses capteurs. Les composants installés dans les locaux de l'organisme peuvent comprendre les terminaux et la ou les passerelles. Les composants installés dans les locaux de l'organisme peuvent aussi comprendre le serveur d'applicatif par exemple intégré à la passerelle. Les clients sont généralement distants pour des besoins opérationnels mais on pourrait également envisager un ou plusieurs clients utilisateurs de l'applicatif dédié, disposés dans les locaux de l'organisme.

Le système de supervision 1 comprend une pluralité de terminaux 10 et une ou plusieurs passerelles 20 en liaison de communication avec un réseau extérieur 32 comme par exemple Internet, des réseaux intranet WiFi ou filaires ou des réseaux de téléphonie mobile. Les données générées par les terminaux sont

centralisées automatiquement et de façon sécurisés par l'applicatif dédié via la ou les passerelles. Les passerelles 20 collectent les données et les retransmettent à l'applicatif dans le serveur 30. L'applicatif dédié permet par exemple aux clients 40 de réaliser une exploitation et une supervision à distance.

Le terminal se décompose en trois blocs fonctionnels dont une alimentation 13, un module de gestion 12 et un module capteur 11. Le module capteur 11 peut comprendre un ou plusieurs types de capteurs et de façon avantageuse est interchangeable. On prévoit, comme expliqué par la suite, une initialisation automatique du module de gestion 12 en fonction du module capteur connecté.

De même, comme expliqué par la suite, on prévoit une connexion automatique entre une pluralité de capteurs et une passerelle. Une passerelle est par exemple préconfigurée pour se connecter automatiquement à un nombre déterminé de modules de gestion référencés en mémoire. On peut ainsi aisément installer de nouveaux capteurs de supervision ou simplement remplacer un module de gestion ou un module capteur lors d'opération de maintenance, ceci tout en assurant la sécurité des données et un contrôle de l'authenticité des terminaux.

Parmi les applications envisageables pour des objets connectés, il en existe de nombreuses dans le domaine de l'industrie, où l'utilisation d'objets connectés dans un système de supervision selon l'invention fait espérer des gains substantiels de coûts et d'efficacité, comme par exemple:

- La surveillance d'équipements, et mise en place de maintenance prédictive ou préventive,
- La gestion de la consommation des ressources et des infrastructures,
- L'efficacité des procédés logistiques,

Le système de supervision présente avantageusement une architecture matérielle et une organisation logicielle qui répond aux exigences de sécurité tout en gardant une grande facilité de déploiement. Les composants matériels sont extrêmement modulaires permettant de très facilement de s'adapter à des besoins aussi différents que variés avec des briques techniques communes. De plus la structure du système de supervision s'appuie avantageusement sur des procédures d'appairage, de gestion matérielle avancée et de configurations évoluées et sécurisées.

En référence à la figure 2, chaque terminal 10 comprend au moins une alimentation électrique 13, par exemple une pile ou une batterie rechargeable.

L'alimentation électrique peut également comprendre un transformateur connecté au réseau électrique. L'alimentation électrique 13 peut être logée dans le module de gestion ou dans un module séparé adapté pour être monté de manière amovible sur le module de gestion 12.

Chaque terminal 10 comprend également un module capteur 11 et un module de gestion 12 connectés entre eux via un connecteur en deux parties 14a et 14b. Le connecteur est par exemple formé par des ports GPIO (pour l'acronyme anglais General Purpose Input/Output) portés par le module capteur 11 et le module de gestion 12. Le connecteur peut supporter, par exemple, un bus I2C, un bus SPI, un bus UART tel que RS232 ou RS485 ou des lignes digitales ou analogiques d'entrée ou de sortie.

Le module capteur 11 est par exemple un module pouvant être assemblé de manière amovible au module de gestion 12. Le module capteur 11 comprend alors un boîtier dans lequel sont agencés des composants du module capteur, ce boîtier étant conformé pour pouvoir être monté de manière amovible à un boitier du module de gestion dans lequel sont agencés les composants du module de gestion. La connexion entre le module capteur 11 et le module de gestion 12 peut s'effectuer par une connexion mécanique amovible, par exemple avec encliquetage.

Le module capteur 11 comprend au moins un capteur 110, et peut comprendre plusieurs capteurs 110a et 110b. Les capteurs peuvent être de types très variés, par exemple :

- capteurs de surveillance de l'environnement, adaptés pour relever au moins grandeur telle que la température, la pression, l'humidité, la luminosité, la qualité de l'air,
- capteurs de surveillance de consommation d'électricité, d'eau, de gaz,
- capteurs de surveillance d'une installation électrique par mesure de courant ou de tension,
- capteurs de grandeurs mécaniques par mesure de vibrations, accélérations, détections de choc, de mouvements, mesure de déformations, ouverture de porte, etc.
- capteurs de position.

Le module capteur 11 comprend également une mémoire 111 stockant des informations 111a relatives à au moins un protocole de communication et aux

broches utiles du connecteur assurant la connexion entre le module capteur et le module de gestion.

En particulier la mémoire 111 stocke des informations 111a relatives au nombre de capteurs 110 présents dans le module capteur et des informations propres à chaque capteur, référencé 110, 110a ou 110b, contenu dans le module capteur 11. Ces dernières informations peuvent comprendre, pour chaque capteur :

- le type du capteur,
- un identifiant du capteur,
- un protocole de communication avec le capteur, identifiant par exemple le type ou format des données générées par le capteur (par exemple nombre entier, flottant, chaîne de caractères…), le mode d'accès aux données ou la fréquence d'accès aux données,
- un mode de fonctionnement du capteur tel qu'un déclenchement suite à un seuil de surveillance franchi, un écart de variation détecté ou un changement de valeur détecté.

Chaque module capteur 11 d'un terminal peut en outre comprendre un ou plusieurs actionneurs et peut également comprendre un calculateur 112. Ce calculateur 112 peut par exemple être configuré pour commander le ou les actionneurs du terminal. Le calculateur peut par exemple se présenter sous la forme d'un processeur, un microprocesseur ou un microcontrôleur.

Le module capteur 11 peut comprendre des modules fonctionnels de collecte 113 des données et de transfert 114 des données vers le module de gestion, ces modules 113 et 114 pouvant se présenter sous la forme de programmes ou sous-programmes enregistrés dans la mémoire 111.

Le module de gestion 12 peut également réaliser des accès directement en mémoire du module capteur 11.

Le module de gestion 12 comprend au moins un calculateur 121, comme par exemple un microcontrôleur, un microprocesseur ou un microordinateur et une mémoire 122. La mémoire 122 stocke notamment l'identifiant ID1 du module de gestion.

La mémoire peut aussi stocker des données 127 représentatives des mesures effectuées par le ou les capteurs du module capteur 11. Par exemple, ces données 127 peuvent être fournies par le ou les capteurs et stockées de manière temporaire par la mémoire 122 en attendant leur envoi à la passerelle 20.

Le module de gestion 12 peut comprendre un module d'interface 129 avec le module capteur 11, réalisant le pilotage des échanges avec le module capteur, et en particulier pilotant la récupération des données générées par les capteurs, en fonction des informations 111a lues dans la mémoire 11 du module capteur, relatives au protocole de communication et aux broches utiles du connecteur. Ainsi ce module d'interface 129 peut accéder en lecture à la mémoire du module capteur, pour en déduire les modalités de récupération, puis récupérer des données représentatives des mesures réalisées par le ou les capteurs.

On peut aussi envisager des informations 111a se présentant sous la forme d'un code déterminé et représentatif de la configuration du capteur 11, afin d'économiser la bande passante lors de la retransmission de cette information 111a vers le serveur.

Le module d'interface 129 peut comprendre en outre un module 126 de détection de connexion et d'initialisation. Ce module 126 de détection et d'initialisation déclenche notamment une lecture, dans la mémoire du module capteur, des données 111a de configuration du module capteur, comprenant au moins les informations relatives au protocole de communication et aux broches utiles du connecteur. Les données de configuration 111a peuvent comprendre également des données représentatives du type de capteur, du format des données mesurées ou d'un canal associé à chaque capteur, en cas d'une pluralité de capteurs dans le module capteur.

Cette initialisation avec réception des données de configuration peut être mise en œuvre à la mise sous tension du terminal. Ceci permet notamment, dans le cas où le terminal comprend un module capteur amovible et interchangeable, que le module capteur 11 soit porteur de toutes les informations nécessaires à la récupération et au traitement des données générées par ses capteurs, toutes ces informations étant récupérées par le module de gestion 12 par exemple lors d'une première connexion. Ceci permet avantageusement d'utiliser une grande diversité de capteurs différents avec un déploiement immédiat.

Le module de gestion 12 comprend également un module de chiffrement 123 par exemple de données représentatives des mesures générées par les capteurs du module capteur et de données de service et/ou de contrôle. Les données de services et/ou de contrôle comprennent notamment au moins une donnée

représentative du module capteur. Les données représentatives du module capteur comprennent par exemple les données de configuration 111a.

Le module de gestion peut également comprendre un module 152 de déchiffrement notamment pour le déchiffrement d'une commande reçue.

Le module de chiffrement 123 peut par exemple être mis en œuvre par le calculateur 121 et/ou par un composant cryptographique sécurisé. Le composant cryptographique sécurisé stocke par exemple des clés de chiffrement/déchiffrement. Le composant cryptographique sécurisé peut également réaliser des opérations de dérivations d'une clé sélectionnée en fonction d'un compteur interne au composant cryptographique, la clé dérivée étant alors utilisée comme clé de session.

Le chiffrement réalisé par le module de gestion est un chiffrement symétrique par une ou plusieurs clés de session pour chaque message. La ou les clés de session peuvent être modifiées régulièrement voire à chaque nouveau message. La ou les clés de session sont avantageusement propres à chaque module de gestion. Les clés de session utilisées par chaque module de gestion sont obtenues notamment en utilisant une donnée propre au module de gestion telle que l'identifiant ID1 du module de gestion. L'identifiant ID1 du module de gestion est par ailleurs transmis en clair dans le message, la passerelle étant en mesure de retrouver en mémoire cet identifiant. Le module de gestion 12 peut comprendre par exemple un module de transfert 128 pour la mise en œuvre des envois de données vers la passerelle, via le module émetteur. Chaque message comprend par exemple un entête non-chiffrée, des données générées chiffrées, des informations de service chiffrées et/ou des informations de contrôle chiffrées. Les données générées, les informations de services et les informations de contrôle sont de préférence chiffrées indépendamment les unes des autres.

Le module de chiffrement 123 génère par ailleurs une ou plusieurs clés de session pour chaque nouveau message en utilisant un compteur mémorisé du nombre de messages envoyés, la passerelle étant par ailleurs en mesure d'incrémenter un compteur en mémoire associé à l'identifiant du terminal, à chaque message reçu.

Le chiffrement/déchiffrement par clé symétrique utilise par exemple un chiffrement AES 128 CCM* ou un chiffrement AES256.

Le sous-programme de génération de clé peut par exemple se présenter sous la forme d'un protocole de dérivation d'un secret tel que NIST-800-108-KDF, X9.63-KDF, NIST-800-56-KDF-A/B, NIST-800-56-KDF-C ou HKDF.

Le sous-programme de génération peut par exemple dériver une clé en fonction d'un ou plusieurs paramètres tels qu'un compteur de messages, un identifiant, un aléa ou un compteur mémorisé dans un composant de sécurité.

K' = F (K, Cmpt)

La clé dérivée K' par la fonction de dérivation F est par exemple obtenue à partir de la clé K et du compteur Cmpt. Plusieurs paramètres peuvent également être agrégés ou combinés pour former une des variables de la fonction F.

Le module de gestion 12 comprend également un module 124 émetteur radiofréquence. Le module de gestion 12 peut aussi comprendre un module 125 récepteur radiofréquence. Ces deux modules peuvent être formés par un même module émetteur/récepteur radiofréquence.

Les émissions radiofréquences entre les terminaux et la ou les passerelles sont par exemple réalisées dans les bandes ISM (industriel, scientifique et médical). Ces bandes de fréquences peuvent être utilisées notamment dans un espace réduit pour des applications industrielles.

Les modules fonctionnels du module de gestion 12 peuvent être constitués par des logiciels ou des composants matériels, ou une combinaison de programmes ou de sous-programmes implémentés un ou plusieurs composants matériels. Par exemple il peut s'agir de briques logicielles stockées dans une mémoire et exécutées par le calculateur 121. En variante, ces modules fonctionnels peuvent être mis en œuvre par des calculateurs respectifs.

Comme représenté à la figure 3, la passerelle 20 comprend au moins un module récepteur 21 radiofréquence de liaison avec la pluralité de terminaux 10, un calculateur 23, et une mémoire 24. La passerelle 20 peut comprendre également un microordinateur comprenant le calculateur et la mémoire.

La passerelle 20 peut comprendre aussi au moins un module émetteur 22 radiofréquence de liaison avec la pluralité de terminal, chaque terminal comprenant alors aussi un module récepteur radiofréquence 125. Un code de contrôle est par exemple ajouté dans chaque message émis par chaque terminal, ce code de contrôle étant déchiffré avant d'être renvoyé, par un module 51 d'envoi de messages de réponse, au terminal concerné.

Chaque module de gestion comprend un module 151 de vérification d'accusé de réception. Ce module reste en attente d'un accusé de réception pendant une temporisation déterminée puis peut réaliser un ou plusieurs nouveaux envois du message précédemment émis. La puissance est par exemple augmentée à chaque nouvel envoi du même message.

Le module 151 de vérification d'accusé de réception recevant l'accusé de réception peut également réaliser une lecture d'une donnée de paramétrage contenu dans le message de réponse, comme par exemple, une augmentation ou une diminution de la puissance d'émission. La puissance d'émission peut avantageusement être réglée au minimum nécessaire.

Le module 151 de vérification d'accusé de réception, en cas d'absence d'accusé réception peut également émettre un message d'alerte, par exemple sur une fréquence générique et selon un protocole de communication générique compatibles avec toute passerelle. Il s'agît par exemple d'une émission de type broadcast. Le message d'alerte vise notamment à signifier l'absence de connexion du module de gestion avec une passerelle.

La passerelle peut également comprendre plusieurs émetteur/récepteur radiofréquence. Les terminaux peuvent par exemple communiquer avec la passerelle chacun via deux canaux dont un est utilisé en réception et l'autre en émission.

La mémoire 24 de la passerelle stocke dans une table T une pluralité d'identifiants de terminaux correspondant par exemple aux identifiants de leur module de gestion, avec lesquels la passerelle est appariée. Dans cette table T, chaque identifiant de terminal est associé à au moins un paramètre de déchiffrement de message envoyé par le terminal.

Les procédés de chiffrement et de déchiffrement utilisant des clés symétriques seront décrits plus en détails ci-après.

La mémoire 24 peut comporter en outre un module 25 de déchiffrement. Ce module de déchiffrement 25 comprend par exemple un composant cryptographique sécurisé, dans lequel sont stockés des clés de déchiffrement. Le module de déchiffrement stocke également les programmes de déchiffrement. En particulier, le module de déchiffrement est configuré pour réaliser un déchiffrement d'au moins une partie des données chiffrées reçues en provenance d'un terminal.

La passerelle peut également comprendre un module de chiffrement, notamment lorsque le serveur d'applicatif est inclus dans la passerelle dans une configuration de type « edge computing ».

Ainsi la passerelle tente de réaliser un déchiffrement d'un message dont la clé symétrique n'est pas stockée par la passerelle mais générée par cette dernière en fonction de l'identifiant du module de gestion. Le paramètre associé à l'identifiant ID1 du terminal dans la table T est de plus variable dans le temps et correspond par exemple au nombre de message reçus en provenance de ce terminal. Ainsi un succès de déchiffrement du message provenant du module de gestion correspond à une authentification de ce module de gestion.

La passerelle 20 est par ailleurs en liaison de communication avec le réseau extérieur 32 tel que par exemple Internet, un réseau intranet ou un réseau de téléphonie mobile, via une interface dédiée. A cet égard, elle peut comprendre un module 26 de rupture protocolaire pour isoler et protéger les données échangées. Le module de rupture protocolaire 26 comprend notamment une interface optique en liaison de part et d'autre avec deux équipements alimentés par des sources d'alimentation distinctes. De plus le protocole de communication est également modifié de part et d'autre du module de rupture protocolaire en passant par exemple d'un protocole série à un protocole Ethernet. Pour la gestion de la communication avec le réseau extérieur, le module de rupture protocolaire utilise par exemple un microcontrôleur pouvant être éteint en cas d'absence de données à transmettre, limitant ainsi la surface d'attaque cyber de la passerelle. L'alimentation du microcontrôleur est coupée. Le microcontrôleur est par la suite remis sous tension pour une nouvelle transmission sur le réseau extérieur.

La passerelle 20 comporte aussi un module 28 d'envoi de réponses aux terminaux suite à la réception d'un message en provenance d'un terminal.

En référence aux figures 4a à 4c, le système de supervision comprend en outre un serveur 30 comprenant un applicatif dédié pour l'exploitation des données de supervision, c'est-à-dire permettant l'exploitation et la visualisation des données de supervision en liaison avec des entités clientes 40.

Dans un cas représenté schématiquement en figure 4a, ce serveur 30 est intégré à la passerelle 20. Des clients 40 (applications clientes hébergées par exemple sur PC, tablette, smartphone) peuvent accéder à ce serveur 30 via le réseau extérieur tel qu'un intranet 32a. L'applicatif peut comprendre par ailleurs un

module d'envoi de commandes chiffrées aux modules de gestions 12. Chaque commande est par exemple déchiffrable uniquement par chaque module de gestion 12 à qui cette commande est adressée.

Dans un autre cas représenté schématiquement en figure 4b, le serveur 30 hébergeant l'applicatif est distant de la passerelle 20 et relié à cette dernière via une liaison intranet. Des clients 40 peuvent accéder à ce serveur 30 d'applicatif via le réseau extérieur tel qu'un réseau intranet 32a. La passerelle peut en outre comprendre un module 27 de mise en veille de sa liaison de communication avec le serveur 30 dédié, et de réveil en cas de sollicitation par un des modules de gestion des terminaux. La liaison entre la passerelle 20 et le serveur 30 d'applicatif est par exemple chiffrée de façon à réaliser un sur-chiffrement. Le protocole HTTPS est par exemple mis en œuvre entre le serveur 30 d'applicatif et la passerelle 20. L'applicatif peut comprendre par ailleurs un module 251 d'envoi de commandes chiffrées aux modules de gestions 12. Chaque commande est par exemple déchiffrable uniquement par chaque module de gestion 12 à qui cette commande est adressée.

Dans un autre cas représenté schématiquement en figure 4c, le serveur 30 est distant de la passerelle 20 et reliée à celle-ci via le réseau extérieur tel qu'Internet ou WiFi. Des clients 40 peuvent par exemple accéder à ce serveur 30 via le réseau extérieur Internet 32b. La passerelle 20 peut en outre comprendre un module 27 de mise en veille de sa liaison de communication avec le serveur dédié, et de réveil en cas de sollicitation par un des modules de gestion des terminaux. L'applicatif peut comprendre par ailleurs un module 251 d'envoi de commandes chiffrées aux modules de gestions 12. Chaque commande est par exemple déchiffrable uniquement par chaque module de gestion 12 à qui cette commande est adressée.

La liaison entre la passerelle 20 et le serveur 30 d'applicatif est par exemple chiffrée de façon à réaliser un sur-chiffrement. Le protocole HTTPS est par exemple mis en œuvre entre le serveur 30 d'applicatif et la passerelle 20. L'envoi de données à l'applicatif comprend par exemple :

- une mise sous tension de l'électronique en sortie de la passerelle,
- l'envoi d'un certificat du Server Application et d'une requête
- l'établissement de la connexion sécurisée HTTPS

- l'envoi de messages avec le surchiffrement de la couche TLS (Transport layer Secure) comprenant les données de supervision.

En référence à la figure 7, on va décrire des exemples de clés de chiffrement symétriques utilisées pour le chiffrement et le déchiffrement des messages échangés au sein du système de supervision.

L'ensemble des clés utilisées au sein du système de supervision est par exemple dérivé à partir d'une clé unique Kapp qui appartient par exemple à l'organisme au sein duquel est installé le système de supervision.

A partir d'au moins cette clé unique Kapp et d'un identifiant de la passerelle, est dérivée une clé maître de la passerelle KCGTW, qui est stockée dans la passerelle comme par exemple dans un composant sécurisé de la passerelle. A partir de cette clé maître de la passerelle KCGTW est dérivée, pour chaque terminal, et grâce à au moins un identifiant du terminal, une clé maître de service, KCT, qui est propre à chaque terminal.

Un composant sécurisé est par exemple du type Java Card.

La clé maître de service KCT est dérivée pour générer des premières clés locales KCTERM#, également propres à chaque terminal, et qui sont stockées dans leur terminal respectif. Ces premières clés locales KCTERM# sont par exemple stockées, sous la forme d'une liste, dans le composant sécurisé du terminal. La clé maître de service KCT n'est de préférence pas stockée dans le terminal.

Les premières clés locales KCTERM# sont par exemple dérivées à partir d'au moins la clé maître propre au terminal KCT et d'un numéro de rang dans la liste de premières clés. Le numéro de rang est par exemple un entier allant de 1 à 6. Le numéro de rang peut également se présenter sous la forme d'un entier allant de 7 à 12.

La clé de session KSC# est déterminée à partir de la liste des premières clés locales KCTERM# en fonction d'un compteur local. Il peut s'agir par exemple d'une sélection de la clé se trouvant au rang correspondant au compteur de message émis. Le rang de la clé sélectionnée correspond par exemple au compteur modulo le nombre de premières clés.

Il peut également s'agir par exemple d'une sélection de la clé se trouvant au rang calculé selon un compteur de message émis où chaque première clé est utilisée successivement un nombre de fois déterminée avant de passer au rang suivant ou de revenir au rang initial.

On peut encore, suite à la sélection de la clé en fonction du compteur de message émis, réaliser une opération de dérivation en fonction de la clé sélectionnée et d'un compteur interne à un composant cryptographique sécurisé, ce composant mémorisant également la liste des premières clés et réalisant l'opération de dérivation.

Une clé maître d'applicatif KDT, propre à chaque terminal, est par ailleurs dérivée de la clé unique Kapp à partir d'un identifiant du serveur dédié à l'applicatif 30, de l'identifiant de la passerelle et de l'identifiant du terminal.

Cette clé maître d'applicatif KDT est utilisée pour dériver des secondes clés locales KDTERM#, et des troisième clés locales KATERM# qui sont stockées d'usine dans chaque terminal, par exemple dans un composant cryptographique sécurisé de chaque terminal, sous la forme de listes respectives.

Les secondes clés locales KDTERM# et les troisièmes clés locales KATERM# sont par exemple dérivées à partir d'au moins la clé maître d'applicatif KDT et des numéros de rangs des clés dans leur liste respective.

Un compteur est de même utilisé pour réaliser au moins une sélection dans la liste des deuxièmes ou troisièmes clés.

Les clés de session KSD# ou KSA# peut être obtenues en opérant une sélection dans leur liste respective.

Les clés de session KSD# ou KSA# peuvent également être obtenues en opérant une sélection dans leur liste respective puis une opération de dérivation en fonction du compteur ou d'un compteur interne à un composant de sécurité. Le compteur interne est par exemple mis à jour en fonction du compteur externe au composant de sécurité.

Le serveur peut détenir uniquement la clé unique Kapp sans mémoriser la clé maître de données KDT, ce qui permet de renforcer la sécurité.

Chaque terminal comporte par exemple l'ensemble des premières clés locales KCTERM#, des deuxièmes clés locales KDTERM# ainsi que des compteurs de messages reçus et de messages envoyés par le terminal.

Le terminal peut également comporter l'ensemble des troisièmes clés locales et un compteur du nombre de commandes reçues, en fonction duquel une clé de déchiffrement est déterminée.

Dans le cas de la détermination de la clé de session par dérivation d'une clé locale, pour un chiffrement ou un déchiffrement, la liste de clé locale peut être

mémorisée dans le composant cryptographique sécurisé qui réalise par ailleurs l'opération de dérivation.

La passerelle stocke par ailleurs une table comprenant chaque identifiant de terminal avec lequel elle est appariée associé à au moins un compteur propre à chaque terminal. Ce compteur peut être utilisé pour recenser le nombre de messages reçus par la passerelle en provenance du terminal correspondant. Cette table peut être mémorisée dans un composant sécurisé de la passerelle. La passerelle peut également stocker aussi, pour chaque terminal, un compteur supplémentaire du nombre d'utilisation de chaque clé locale par le terminal.

Le serveur 30 dédié à l'applicatif comprend un calculateur et une mémoire, dans laquelle sont stockés les identifiants de la passerelle 20 et des terminaux 10, ainsi que la clé unique Kapp.

Le serveur 30 stocke également une table comprenant chaque identifiant de terminal associé à au moins un compteur propre à chaque terminal. Ce compteur peut être utilisé pour recenser le nombre de messages reçus par le serveur d'applicatif en provenance du terminal correspondant. Cette table peut être mémorisée dans un composant sécurisé du serveur. Le serveur peut également stocker aussi, pour chaque terminal, un compteur supplémentaire du nombre d'utilisation de chaque clé locale par le terminal. Le serveur d'applicatif peut également stocker, dans la table, un compteur de commandes chiffrées envoyées à chaque terminal. Le compteur du nombre de commandes envoyées peut être associé à un deuxième compteur du nombre d'utilisations successives de la clé de chiffrement utilisée.

La mémorisation de la clé unique Kapp ainsi que les opérations de dérivation pour l'obtention de la clé maître d'applicatif KDT, des secondes clés locales KDTERM# et des troisième clés locales KATERM# peuvent également être réalisées par un composant hautement sécurisé par exemple de type HSM (High Secure Module). Ce composant hautement sécurisé peut être mis en œuvre dans un deuxième serveur en liaison de communication avec le serveur d'applicatif. Le serveur d'applicatif transmet par exemple son identifiant ainsi que les identifiants de la passerelle et du terminal au composant hautement sécurisé qui transmet en retour, au serveur d'applicatif, les secondes clés locales KDTERM# et les troisième clés locales KATERM#.

En référence aux figures 5, 6a et 6b, on va maintenant décrire un procédé de transmission de données mis en œuvre par un système de supervision selon l'invention.

Ce procédé peut comprendre une étape préliminaire 90, réalisée lors de la mise sous tension d'un terminal, de récupération des données de configuration du module capteur par le module de détection et d'initialisation.

Cette étape est par exemple suivie de l'envoi 91 d'une trame chiffrée, au serveur, via la passerelle, représentative de la configuration du module capteur. La trame transmise 91 à la passerelle est retransmise 92 à l'applicatif . Cette trame peut notamment comprendre une liste des capteurs, les numéros de canaux correspondants, le ou les types de capteurs, ceci pour permettre à l'applicatif d'ensuite identifier les données des capteurs dans les trames ultérieurement envoyées par le module de gestion, en fonction par exemple de leur taille et position. Pour le chiffrement de cette trame, on utilise par exemple une des clés de chiffrement symétriques stockées par le terminal ou une clé dérivée d'une de ces clés, la sélection et la dérivation étant par exemple réalisée en fonction du compteur de messages émis par le terminal.

Le procédé comprend ensuite une étape 100 de récupération de données représentatives des mesures effectuées par le ou les capteurs, grâce au module d'interface 129, puis le chiffrement 110, au moyen du module de chiffrement d'une part des données récupérées et d'autre part de données de service et/ou de contrôle comprenant au moins une donnée représentative du module capteur. Les données de service et/ou de contrôle peuvent également comprendre des informations de configuration du terminal. Avantageusement ces données de service et/ou de contrôle peuvent comprendre un code de contrôle ACK utilisé ensuite comme accusé de réception. Le code de contrôle ACK diffère par exemple pour chaque message et est par exemple généré à l'aide d'un aléa et d'une variable correspondant par exemple à une horloge interne.

Avantageusement la clé de chiffrement symétrique utilisée pour le chiffrement des données de service et/ou de contrôle peut être différente de la clé utilisée pour le chiffrement des données représentatives des mesures effectuées par les capteurs. Ces deux clés de session proviennent par exemple de deux listes distinctes KCTERM# et KDTERM#.

Pour les données de service et/ou de contrôle, la clé de chiffrement utilisée est une clé de session KSC# déterminée à partir de l'une des premières clés locales KCTERM# et du compteur d'envoi de messages du terminal.

Avantageusement, les premières clés locales peuvent être utilisées successivement un nombre prédéterminé de fois avant d'utiliser la clé suivante dans la liste. La sélection de la première clé locale utilisée pour la clé de session KSC# est réalisée au moyen d'une variable déterminée en fonction d'un compteur mémorisé dans le terminal.

Par exemple, la valeur du compteur d'envoi de messages du terminal permet, en connaissant le nombre maximum d'utilisations successives d'une première clé locale, de déterminer le rang dans la liste de la première clé locale à utiliser. La clé de session peut résulter de cette sélection ou être engendrée par une opération supplémentaire, comme par exemple une opération de dérivation au moyen d'un composant cryptographique sécurisé.

Pour les données représentatives des mesures effectuées par les capteurs, la clé de chiffrement utilisée est une clé de session KSD# déterminée à partir de l'une des deuxièmes clés locales KDTERM# et du compteur d'envoi de messages du terminal.

Les deuxièmes clés locales KDTERM# peuvent aussi être utilisées un nombre prédéterminé de fois, et la sélection de la deuxième clé locale utilisée pour déterminer la clé de session KSD# est réalisée à partir d'une variable déterminée en fonction d'un compteur du terminal.

Par exemple, la valeur du compteur du nombre de messages envoyés par le terminal permet, en connaissant le nombre maximum d'utilisations successives d'une même deuxième clé locale, de déterminer le rang dans la liste de la deuxième clé locale utilisée. La clé de session peut résulter de cette sélection ou être engendrée par une opération supplémentaire, comme par exemple une opération de dérivation au moyen d'un composant cryptographique sécurisé.

Le module de gestion 12 réalise ensuite l'envoi 200, à la passerelle 20, via le module émetteur radiofréquence, d'un message M comprenant des données chiffrées et l'identifiant non-chiffré, en clair, du terminal.

Dans un exemple de réalisation représenté schématiquement sur la figure 6a, le message M envoyé comprend:

- un bloc en clair BI comprenant au moins l'identifiant du terminal et le cas échéant un identifiant de la passerelle, un identifiant du type de réseau (par exemple point à point ou étoile) ainsi qu'un mode d'utilisation du réseau (vers une passerelle dédiée ou sur une fréquence générique),

- un bloc BS de données de service/configuration, chiffré avec une clé de session KSC# déterminée à partir de premières clés locales KCTERM#, et

- un bloc BD de données de supervision générées par des capteurs, chiffré avec une clé de session KSD# déterminée à partir de deuxièmes clés locales KDTERM#.

Le compteur de messages envoyés mémorisé par le terminal est incrémenté 210 après l'étape d'envoi. Une temporisation est également démarrée pour surveiller la réception d'un message d'accusé de réception en provenance de la passerelle.

Le procédé peut ensuite comprendre une étape 300 de réception, par la passerelle, du message émis par le terminal.

Le procédé comprend alors une étape suivante de génération 310 de la clé de session ayant permis le chiffrement des données de service et/ou de contrôle du message. La passerelle permet ici le déchiffrement de la partie service ou contrôle du message, l'ensemble du message étant déchiffré ultérieurement pas l'applicatif.

La passerelle met ainsi en œuvre une recherche, dans la table mémorisée, de l'identifiant du terminal qui était contenu en clair dans le message, pour récupérer notamment la valeur mémorisée du compteur d'envoi de messages associé à l'identifiant du terminal, dans cette table.

La clé maître de service KCT, propre au terminal, est générée par la passerelle en dérivant la clé maître KCGTW mémorisée par la passerelle avec au moins l'identifiant du terminal comme paramètre de dérivation.

La passerelle est ensuite capable de retrouver au moins une des premières clés locales KCTERM# obtenue par dérivation de la clé maître de service KCT et d'un paramètre calculé en fonction du compteur de message. Le rang est par exemple calculé en fonction du nombre de message et en fonction du nombre d'utilisations successives de chacune des premières clés KCTERM#.

La détermination de la clé de session KSC# peut correspondre à la première clé de rang correspondant au nombre de message reçus ou une opération supplémentaire peut être réalisée sur cette première clé, comme par exemple une

nouvelle opération de dérivation de cette première clé et d'un paramètre tel qu'un compteur des utilisations successives de la même clé.

Une fois la clé de session obtenue, la passerelle incrémente le compteur de messages reçus associé à l'identifiant du terminal, dans la table mémorisée, lors d'une étape 320.

Le procédé comprend ensuite le déchiffrement 330 des données de contrôle et/ou de service contenues dans le message et chiffrées avec la clé de session.

En cas d'échec de déchiffrement 340, le message n'est pas traité. Les étapes 310 et 320 de génération de clé de session KSC# et d'incrémentation du compteur sont alors répétées par la passerelle, pour effectuer au moins une nouvelle tentative de déchiffrement du message avec une valeur incrémentée du compteur. Ceci permet, dans le cas où un précédent message émis par le terminal n'aurait pas été reçu par la passerelle, que celle-ci incrémente son compteur afin qu'il rattrape la valeur du compteur du terminal. La passerelle répète par exemple ces étapes de tentative de déchiffrement un nombre maximum déterminé de fois, par exemple 3 fois.

En cas de succès du déchiffrement du message, la passerelle aura d'une part accès aux données de contrôle ou de service et de plus la passerelle aura réalisé une vérification de l'identité du terminal par déchiffrement du codage propre à ce terminal.

Une authentification du terminal peut aussi être réalisée via un code MIC (Message Interchange Control).

Suite au déchiffrement, la passerelle met en œuvre deux actions. Une première action 350 est d'envoyer, au terminal, un message de réponse M' comprenant un accusé de réception ACK formé par exemple par le code de contrôle contenu dans le bloc des données de contrôle/service BS.

Le message de réponse peut également comprendre une commande de paramétrage du terminal, comme par exemple une commande de réglage d'abaissement ou d'augmentation du niveau de puissance d'émission du terminal, ou une commande d'un actionneur du terminal, ou toute autre commande à exécuter par le terminal. Les commandes sont de préférence chiffrées par l'applicatif, dans le cas d'une réponse fournie par l'applicatif, via la passerelle.

Le message de réponse M' peut être au moins en partie chiffré. Par exemple, en référence à la figure 6b, il peut comprendre un bloc en clair BI' comprenant

l'identifiant du terminal et/ou celui de la passerelle, ainsi que l'accusé de réception, et un bloc chiffré BC comprenant, le cas échéant, une commande à exécuter par le terminal. Comme on va le voir plus en détails ci-après, les commandes proviennent de préférence du serveur 30 d'applicatif et le chiffrement est réalisé par l'applicatif.

Chaque module de gestion d'un terminal peut comprendre un module de vérification d'accusé de réception, adapté pour déclencher une mise en veille des modules émetteur et récepteur du terminal en cas de bonne réception de l'accusé de réception. Ce module de vérification d'accusé de réception peut également incrémenter un compteur de réponse ou de commandes reçues par le terminal.

En revanche, en cas d'échec de réception, le module de gestion 12 réémet le même message au cours d'une nouvelle étape 200, en augmentant la puissance d'émission, et sans incrémenter son compteur de messages envoyés.

Suite à une réémission du message, si le terminal reçoit ensuite un signal d'accusé de réception provenant de la passerelle, le module de gestion 12 mémorise par exemple le niveau de puissance d'émission permettant la bonne réception par la passerelle.

En revanche, si toujours aucun message d'accusé réception ne lui parvient, le terminal réitère l'étape de réémission du message en augmentant la puissance, un nombre de fois déterminé, par exemple trois fois. Après le nombre déterminé d'échecs, le terminal génère un message d'alerte au cours d'une étape 220. Le message d'alerte peut être un message sur une fréquence dite usine, c'est-à-dire une fréquence commune à tous les systèmes de supervision et en particulier à toutes les passerelles, le message étant envoyé à pleine puissance.

Une deuxième action effectuée par la passerelle 20 une fois le module authentifié est de transférer 400 le message reçu du terminal 10, c'est-à-dire avec un bloc BS de données de contrôle/service chiffrées, et un bloc de données BD des capteurs également chiffrées, au serveur 30 dédié à l'applicatif. L'identifiant de la passerelle en clair est agrégé en entête du message retransmis.

Dans le cas où le serveur 30 dédié à l'applicatif est intégré à la passerelle 20, c'est la passerelle qui réalise la suite des étapes décrites ci-après.

Dans le cas où le serveur 30 dédié à l'applicatif est un serveur distant, la connexion entre la passerelle et le serveur applicatif est avantageusement une connexion sécurisée, de manière à fournir un sur-chiffrement des messages transmis.

Le serveur 30 dédié à l'applicatif, stockant la clé unique KAPP, est en mesure de déchiffrer d'une part le bloc de données de contrôle/service BS et d'autre part le bloc de données BD, par dérivations successives à partir de cette clé KAPP.

Pour le bloc BS, le serveur 30 dérive, à partir de la clé unique KAPP et de l'identifiant du terminal contenu en clair dans le message, la clé maître de la passerelle KCGTW, puis dérive successivement à partir de cette clé la clé maître de service KCT, une première clé locale KCTERM# et détermine une clé de session KSC# en utilisant un compteur mémorisé de messages reçus associé à chaque identifiant de terminal. A cet égard le serveur peut comprendre également le ou les compteurs permettant de déterminer le rang de première clé locale permettant de déterminer la clé KSC#.

Le serveur 30 peut également déchiffrer le bloc de données BD par détermination de la clé de session KSD# utilisée par le terminal pour le chiffrement du bloc BD, comme suit :

- dérivation de la clé unique Kapp à partir des identifiants de la passerelle, du terminal et du serveur d'applicatif,
- dérivation de la clé maître d'application KDT à partir de l'identifiant du terminal et de la passerelle contenus en clair dans le bloc d'identification BI du message,
- puis détermination des deuxièmes clés locales KDTERM# par dérivation de la clé KAT et d'une variable déterminée en fonction d'un compteur mémorisé par le serveur,
- puis détermination de la clé de session KSD# à partir des deuxièmes clés locales et du compteur de message reçus par le serveur.

Pour la détermination de la deuxième clé locale, le rang de la deuxième clé est déterminé à partir de la valeur du compteur de messages reçus par le serveur. Un deuxième compteur propre à chaque deuxième clé locale KDTERM#, mémorisé par le serveur, peut également être utilisé. Le rang est par exemple pris en compte. Après la sélection de la clé locale, une nouvelle dérivation peut être opérée prenant, par exemple, comme paramètre un compteur interne.

Le mode de chiffrement utilisé permet par exemple que le bloc de contrôle/service soit déchiffrable par la passerelle et par le serveur dédié à l'applicatif, tandis que le bloc de données générées par les capteurs n'est déchiffrable que par le serveur dédié à l'applicatif.

A réception d'un message transmis par la passerelle, le serveur dédié à l'applicatif dérive donc les clés de chiffrement du message et déchiffre le message au cours d'une étape 410.

Ce serveur 40 peut ensuite traiter les données, permettre leur téléchargement à distance et leur visualisation sur des applications clientes, etc., au cours d'une étape 420.

Le serveur applicatif 40 peut également comprendre un module d'envoi de commandes chiffrées aux modules de gestion des terminaux, pour par exemple renvoyer aux terminaux des commandes de configuration ou de contrôle, ou par exemple des commandes d'actionneurs des terminaux, au cours d'une étape 430.

Dans ce cas, la commande est avantageusement chiffrée par l'applicatif de telle sorte qu'elle soit uniquement déchiffrable par le module de gestion du terminal à qui cette commande est adressée.

A cet égard, la clé de chiffrement utilisée est avantageusement une clé de session KSA# déterminée à partir d'une troisième clé locale KATERM# en fonction d'un compteur de commandes envoyées par le serveur vers chaque terminal. Les troisièmes clés locales KATERM# sont elles-mêmes dérivées par le serveur à partir de la clé maître d'application KDT et d'un rang déterminé en fonction d'un compteur du serveur. Par exemple, le rang de la troisième clé locale KATERM# à utiliser peut être déterminé à partir de la valeur du compteur de commandes envoyées par le serveur.

La commande chiffrée envoyée par le serveur d'applicatif est par exemple envoyée à la passerelle, qui la mémorise et l'ajoute à un prochain message M' d'accusé de réception envoyé au terminal. La commande peut également être directement retransmise au terminal par la passerelle. La passerelle n'est pas ici en mesure de déchiffrer la commande chiffrée.

En revanche le terminal, qui dispose des troisièmes clés locales KATERM# et d'un compteur de commandes reçues, peut déterminer la clé de session KSA# permettant de déchiffrer le bloc de commande.

Le protocole de communication utilisé par le système de supervision, et la structure des clés de chiffrement utilisées permet de sécuriser les données de bout en bout, c'est-à-dire de leur acquisition par les capteurs à leur réception par le serveur d'applicatif.

REVENDICATIONS

1. Système de supervision comprenant une pluralité de terminaux (10a, 10b, 10c) et une passerelle (20) en liaison de communication avec un réseau extérieur (32), la passerelle (20) comprenant au moins un module récepteur radiofréquence (21) de liaison avec la pluralité de terminaux, un calculateur (23) et une mémoire (24), caractérisé en ce que

chaque terminal (10) comprend au moins une alimentation électrique (13), un module capteur (11) connecté via un connecteur (14a, 14b) à un module de gestion (12),

une pluralité d'identifiants de modules de gestion étant chacun associé à au moins un paramètre de déchiffrement dans une table (T) mémorisée dans la passerelle (20),

le module capteur (11), comprenant au moins un capteur (110) et au moins une mémoire (111) stockant des informations (111a) relatives à au moins un protocole de communication et aux broches utiles du connecteur,

le module de gestion (12), comprenant au moins un calculateur (121), une mémoire (122) mémorisant au moins son identifiant (ID1) et stockant par ailleurs des données représentatives des mesures effectuées (127), un module de chiffrement (123), un module émetteur radiofréquence (124) et un module d'interface (129),

le module d'interface (129) pilotant les échanges avec le module capteur (11) en fonction des informations (11a), lues en mémoire du module capteur, relatives audit protocole de communication et aux broches utiles,

le module de chiffrement (123) réalisant le chiffrement des données représentatives des mesures effectuées par ledit capteur et de données de service et/ou de contrôle comprenant au moins une donnée représentative du module capteur,

le module de gestion (12) réalisant l'envoie, à la passerelle (20), via le module émetteur radiofréquence (124), d'au moins les données chiffrées et de l'identifiant non-chiffré du module de gestion (12),

la passerelle (20) comprenant un module de déchiffrement (25) réalisant un déchiffrement en fonction dudit paramètre de déchiffrement associé, dans la table (T), à l'identifiant (ID1) reçu du module de gestion (11).

2. Système de supervision selon la revendication 1, caractérisé en ce que la passerelle comprend un module émetteur radiofréquence (22) de liaison avec la pluralité de terminaux, chaque terminal comprenant un module récepteur radiofréquence (125), les données chiffrées transmises par chaque terminal comprenant un code de contrôle, la passerelle comprenant un module (51) d'envoi de message de réponse (M'),

et en ce que chaque message de réponse (M'), faisant suite à la réception de données provenant du module de gestion (1), comprend au moins le code de contrôle retransmis à ce module de gestion comme accusé de réception.

3. Système de supervision selon la revendication 2, caractérisé en ce que chaque module de gestion (12) comprend un module (151) de vérification d'accusé de réception déclenchant une mise en veille des modules émetteur (124) et récepteur (125) en cas de confirmation de réception ou déclenchant en cas d'échec de réception, au-delà d'une temporisation déterminée, une réémission du même message (M), la puissance d'émission étant augmentée.

4. Système de supervision selon la revendication 3, caractérisé en ce que le nombre de réémissions et d'augmentations successives de la puissance d'émission sont limités, le module de gestion (11) déclenchant l'envoi d'un message d'alerte après un nombre déterminé d'échecs de réémissions.

5. Système de supervision selon l'une des revendications 2 à 4, caractérisé en ce que le message de réponse (M') comprend une commande de paramétrage dudit terminal ou une commande d'actionneur.

6. Système de supervision selon l'une des revendications précédentes, caractérisé en ce que la passerelle (20) réalise une authentification du module de gestion (11) par un succès lors du déchiffrement du message (M) reçu.

7. Système de supervision selon l'une des revendications précédentes, caractérisé en ce que le module d'interface (129) comprend un module (126) de détection de connexion et d'initialisation du module d'interface déclenchant une lecture en mémoire (111) de données de configuration (111a) du module capteur (11) comprenant au moins les informations relatives audit protocole de communication et aux broches utiles.

8. Système de supervision selon la revendication précédente, caractérisé en ce que les données de configuration (111a) comprennent également des données

représentatives du type dudit capteur (110, 110a, 110b), du format des données mesurées ainsi que d'un canal associé en cas de pluralité de capteurs.

9. Système de supervision selon la revendication 7 ou 8, caractérisé en ce que le module (126) de détection de connexion et d'initialisation déclenche par ailleurs un envoi (91) d'une trame chiffrée, à la passerelle (20), représentative de la configuration du module capteur (11) comprenant les données (111a) de configuration.

10. Système de supervision selon l'une des revendications précédentes, caractérisé en ce que la passerelle (20) est en liaison de communication chiffrée avec un serveur (30) dédié du réseau extérieur comprenant au moins un applicatif dédié pour l'exploitation des données de mesure, le module de gestion (12) réalisant un chiffrement des données de contrôle déchiffrables par la passerelle et par l'applicatif dédié et un chiffrement des données de mesures déchiffrables uniquement par l'applicatif dédié.

11. Système de supervision selon la revendication 10, caractérisé en ce que l'applicatif dédié comprend un module (251) d'envoi de commandes chiffrées aux modules de gestions (12), chaque commande étant déchiffrable uniquement par chaque module de gestion (12) à qui cette commande est adressée.

12. Système de supervision selon la revendication 10 ou 11, caractérisé en ce que la passerelle (20) comprend un module (27) de coupure d'alimentation de sa liaison de communication avec le serveur (30) dédié et de remise sous tension en cas de sollicitation par un des modules de gestion (12).

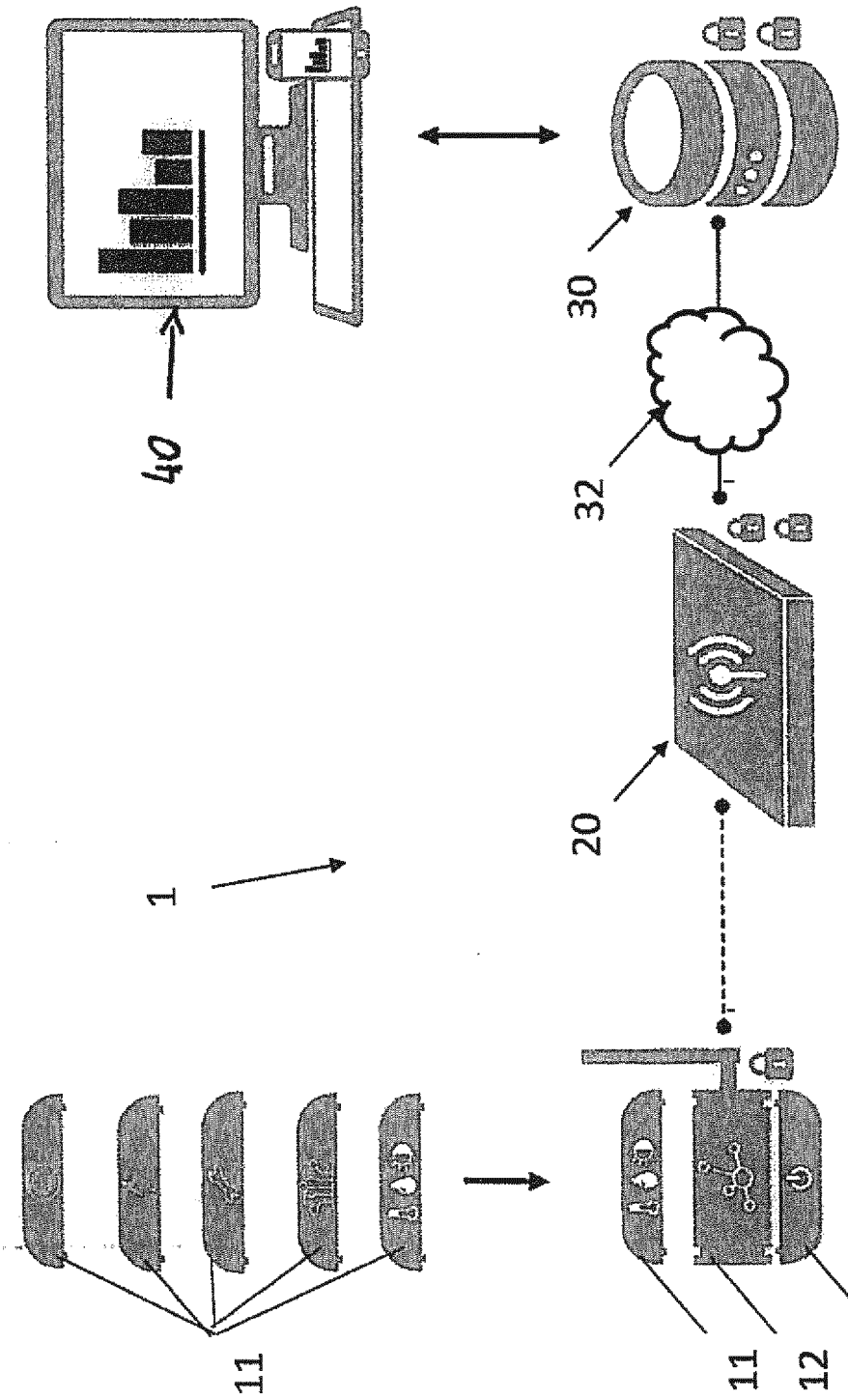


FIG. 1

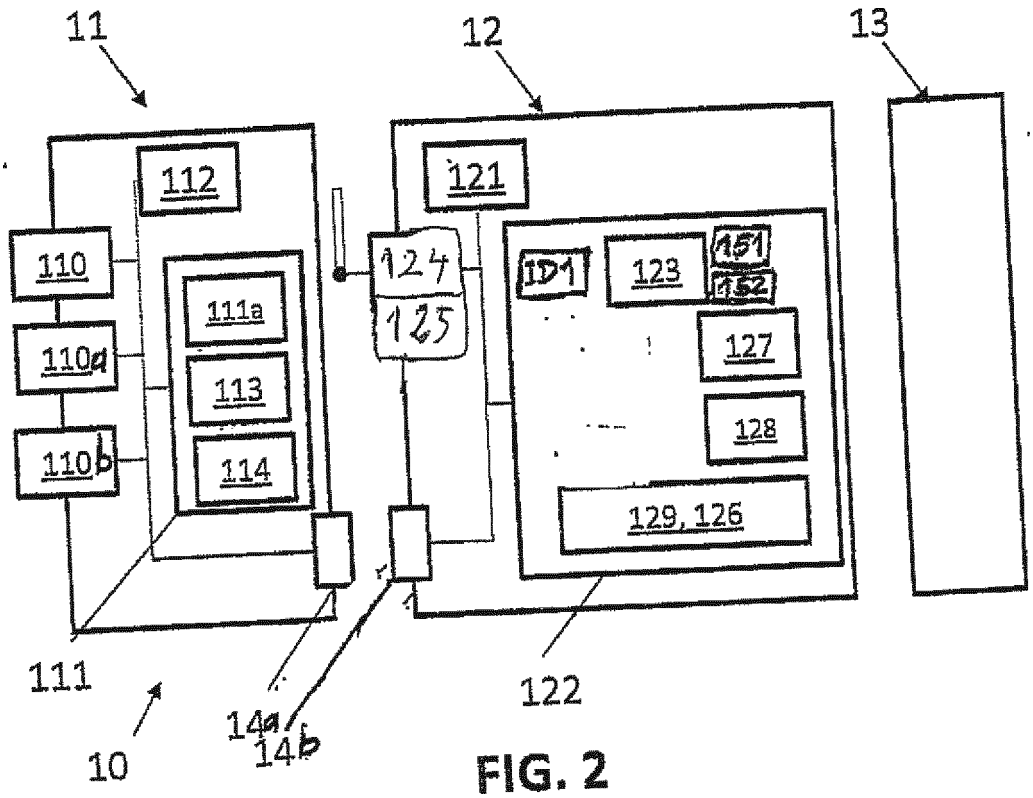

11
12
13
112
121
110
124
125
ID1
123
151
152
111a
113
110a
127
114
110b
128
129, 126
111
122
10
14a
14b

FIG. 2

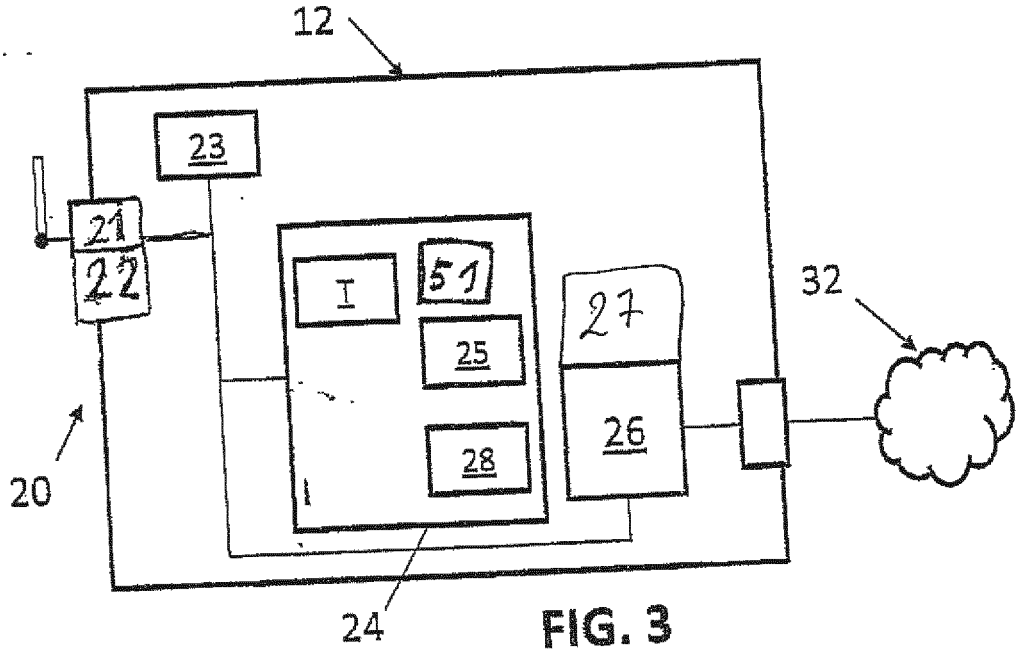

12
23
21
22
I
51
25
27
26
28
32
20
24

FIG. 3

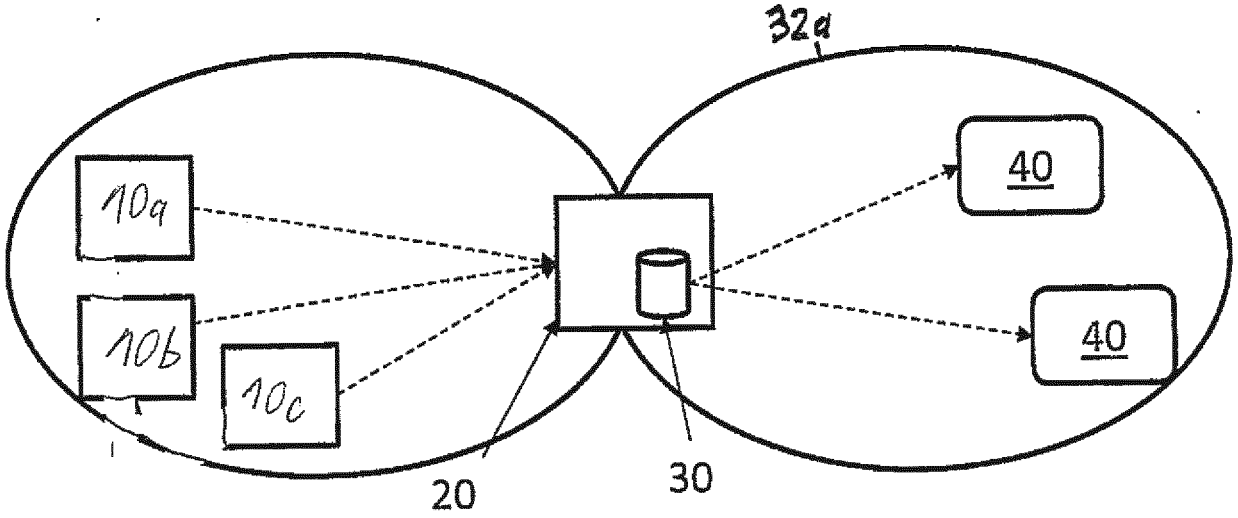


FIG. 4a

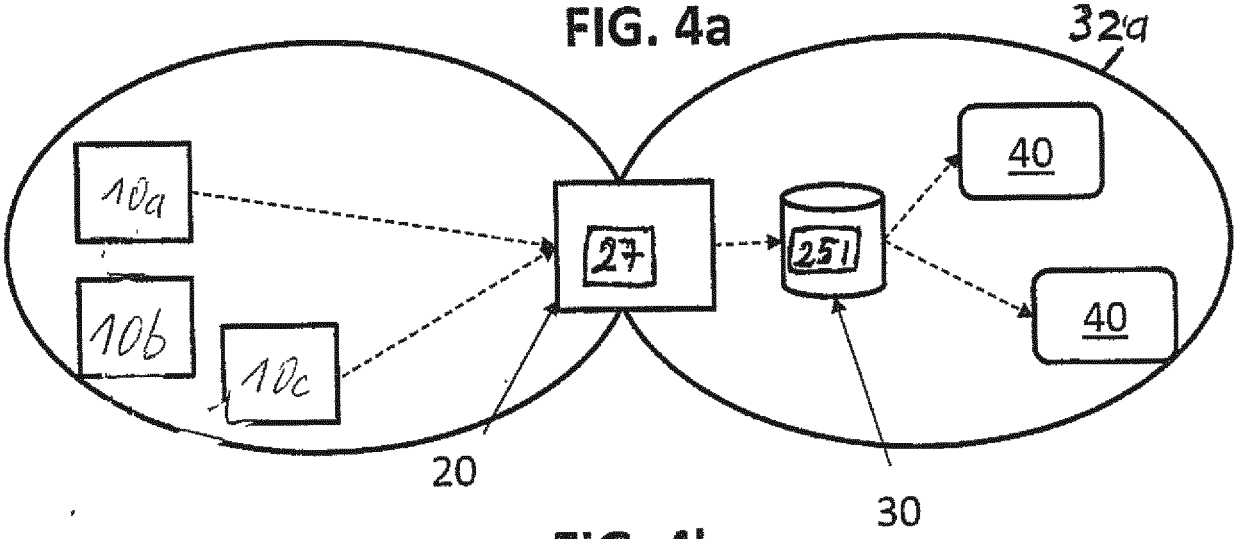


FIG. 4b

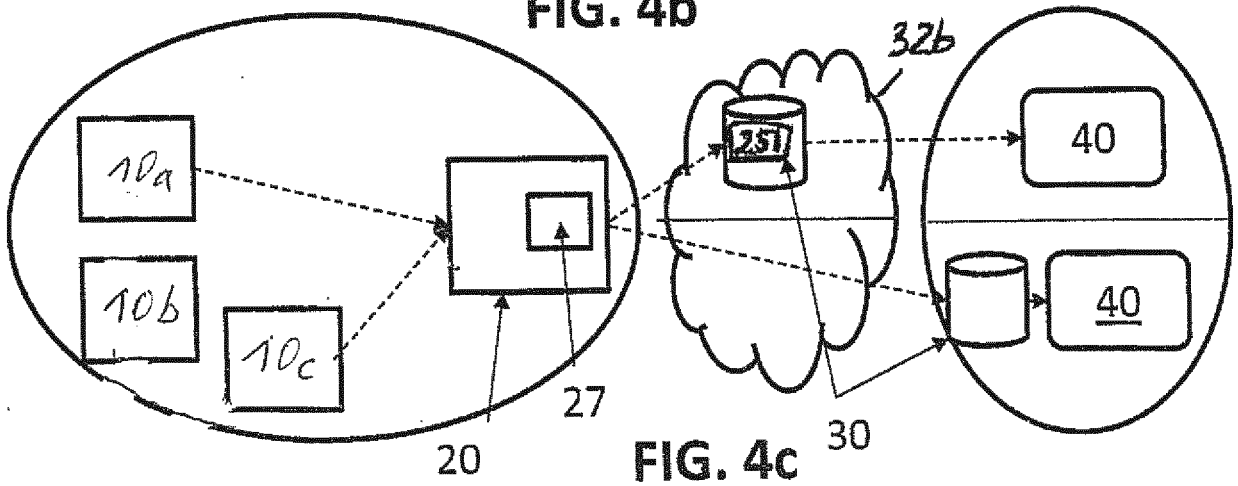


FIG. 4c

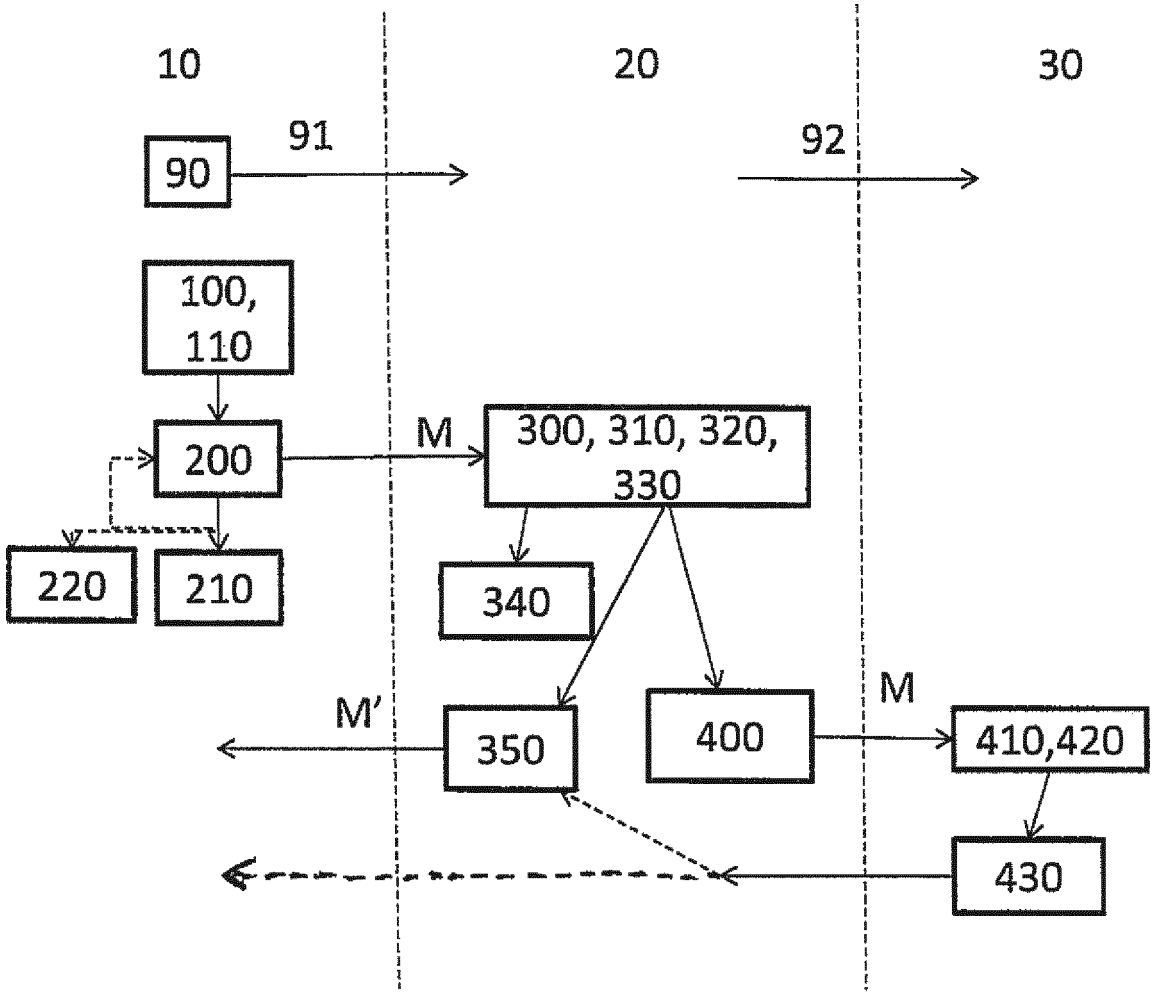


FIG. 5



FIG. 6a



FIG. 6b

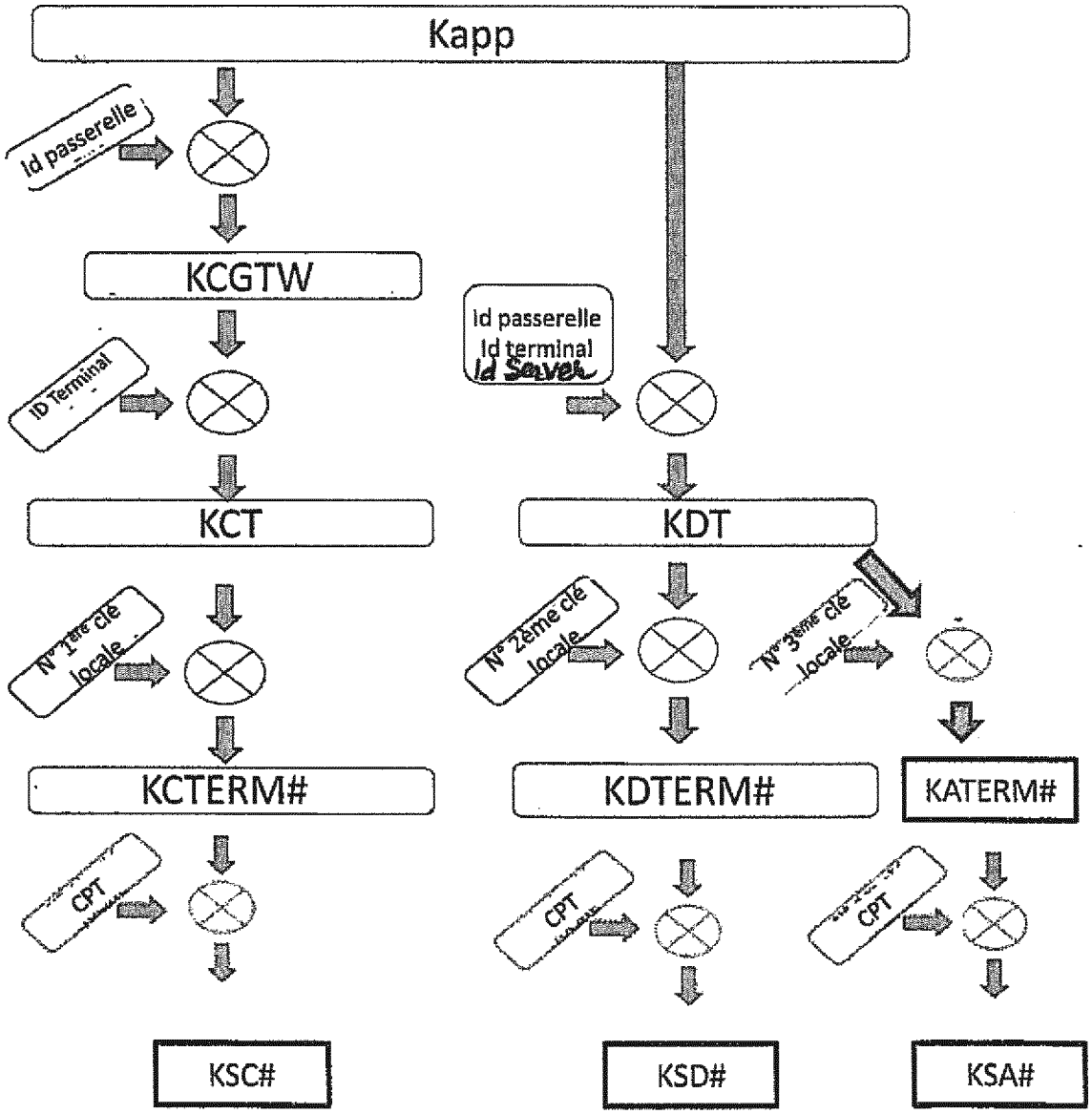

Kapp
Id passerelle
KCGTW
ID Terminal
KCT
N° 1ère clé locale
KCTERM#
CPT
KSC#
Id passerelle
Id terminal
Id Serveur
KDT
N° 2ème clé locale
N° 3ème clé locale
KDTERM#
KATERM#
CPT
CPT
KSD#
KSA#

FIG. 7

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 860753
FR 1860038

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	US 2018/288013 A1 (HENNEBERT CHRISTINE [FR] ET AL) 4 octobre 2018 (2018-10-04) * figure 1 * * alinéa [0008] - alinéa [0009] * * alinéa [0011] - alinéa [0012] * * alinéa [0016] * * alinéa [0018] - alinéa [0021] * * alinéa [0057] * -----	1-12	H04L9/12 H04W12/00
Y	GB 2 543 856 A (MOTHIVE LTD [GB]) 3 mai 2017 (2017-05-03) * figure 2 * * page 11, ligne 32 - page 12, ligne 15 * * page 20, ligne 5 - ligne 7 * -----	1-12	
Y	US 2018/160283 A1 (STAMATAKIS JULIEN G [US]) 7 juin 2018 (2018-06-07) * figure 1 * * figure 7 * * alinéa [0019] * * alinéa [0031] * -----	1-12	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W H04L

Date d'achèvement de la recherche	Examinateur
25 juin 2019	Caragata, Daniel

CATÉGORIE DES DOCUMENTS CITÉS

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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1860038 FA 860753

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 25-06-2019
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2018288013 A1	04-10-2018	EP 3386162 A1	10-10-2018
		FR 3064857 A1	05-10-2018
		US 2018288013 A1	04-10-2018
GB 2543856 A	03-05-2017	AUCUN	
US 2018160283 A1	07-06-2018	US 9534929 B1	03-01-2017
		US 9534930 B1	03-01-2017
		US 9538578 B1	03-01-2017
		US 9551594 B1	24-01-2017
		US 9554236 B1	24-01-2017
		US 9714843 B1	25-07-2017
		US 9714844 B1	25-07-2017
		US 9756511 B1	05-09-2017
		US 9762979 B1	12-09-2017
		US 9763118 B1	12-09-2017
		US 9813489 B1	07-11-2017
		US 9888336 B1	06-02-2018
		US 10171891 B1	01-01-2019
		US 2017105057 A1	13-04-2017
		US 2017105088 A1	13-04-2017
		US 2017328736 A1	16-11-2017
		US 2017366988 A1	21-12-2017
		US 2018077223 A1	15-03-2018
		US 2018160283 A1	07-06-2018

EPO FORM P0465