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

(11) **EP 3 168 820 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
17.05.2017 Bulletin 2017/20

(51) Int Cl.:
G08B 21/02 *(2006.01)* ***G08B 25/01*** *(2006.01)*

(21) Numéro de dépôt: **16198252.5**

(22) Date de dépôt: **10.11.2016**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA ME
Etats de validation désignés:
MA MD

(30) Priorité: **13.11.2015 FR 1502382**

(71) Demandeur: **Thales**
92400 Courbevoie (FR)

(72) Inventeurs:
- **MONCET, Eric**
  78141 Velizy Cedex (FR)
- **ROCHE, Elodie**
  78141 Velizy Cedex (FR)
- **ABEILLE, Eric**
  78141 Velizy Cedex (FR)
- **BOISNON, Jean-Michel**
  78141 Velizy Cedex (FR)
- **LARMOIRE, Thierry**
  78141 Velizy Cedex (FR)

(74) Mandataire: **Lavoix**
2, place d'Estienne d'Orves
75441 Paris Cedex 09 (FR)

(54) **EQUIPEMENT DE SÉCURISATION D'UNE PERSONNE ET SYSTÈME ASSOCIÉ**

(57) L'invention concerne un équipement de sécurisation (16) d'une personne comprenant un bracelet (20) et un boîtier (22) tenu par le bracelet (20) et qui comporte :
- un récepteur (28) propre à recevoir des données,
- un processeur (32) propre à associer à chaque donnée un degré de dangerosité, et propre à envoyer des données à communiquer et propre à transmettre des données à émettre,
- une interface (34) propre à communiquer des données envoyées, et
- un émetteur (30) propre à émettre des données transmises.

L'équipement (16) est propre à fonctionner selon au moins deux modes de fonctionnement, chaque mode étant associé de manière biunivoque à un degré de dangerosité seuil, les données que le processeur (32) est propre à envoyer dans un mode étant les données associées à un degré de dangerosité supérieur ou égal au degré de dangerosité seuil du mode considéré.

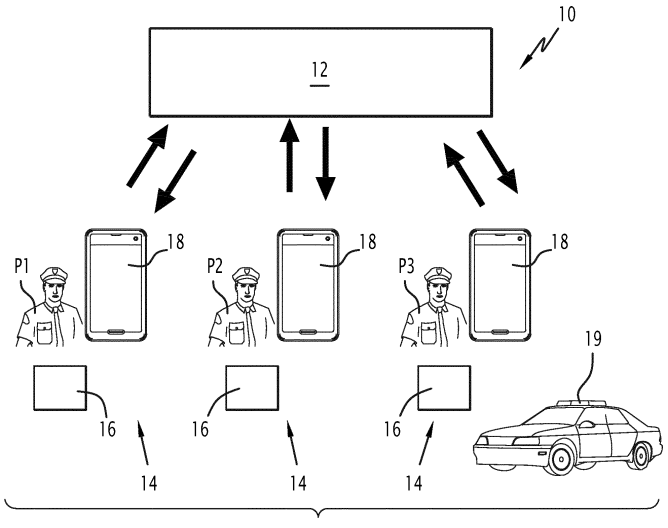

FIG.1

EP 3 168 820 A1

Description

[0001] La présente invention concerne un équipement de sécurisation d'une personne. La présente invention se rapporte également à un système de sécurisation associé.

[0002] Dans le domaine de la sécurité, de nombreux personnels sont impliqués et ont à prendre des décisions rapidement avec peu d'éléments.

[0003] De fait, de nombreux incidents et accidents de ces personnels ont pour cause une décision inadaptée prise par le personnel. Par exemple, lors d'un contrôle routier, un comportement de routine ne convient pas si la voiture contrôlée est une voiture volée. Dans une telle situation, le voleur, se sentant découvert, peut avoir une réaction violente mettant en danger la vie du personnel effectuant le contrôle.

[0004] Il est donc souhaitable d'améliorer la sécurité du personnel impliqué dans ces contrôles.

[0005] Pour cela, il est connu d'utiliser des gilets pare-balles. Un gilet pare-balles est un équipement principalement destiné à protéger le thorax, l'abdomen et le dos contre le tir d'armes à feu en absorbant l'impact. Les gilets sont fabriqués avec des fibres tissées serrées, principalement le Kevlar. Ce type de gilet peut alors protéger celui qui le porte contre les projectiles d'armes de poing et de fusils, ainsi que les shrapnels de certains dispositifs explosifs comme les grenades.

[0006] Toutefois, bien qu'un tel équipement permette de protéger efficacement le personnel en cas d'attaque directe, un tel équipement est difficile à camoufler. De ce fait, pour une mission de filature, l'emploi d'un tel équipement est mal adapté et conduit, dans certaines circonstances à mettre en danger le personnel.

[0007] Il existe donc un besoin pour un équipement de sécurisation d'une personne permettant d'améliorer la sécurité du personnel dans toutes les situations.

[0008] Pour cela, il est décrit un équipement de sécurisation d'une personne. L'équipement de sécurisation comprend un bracelet propre à être enroulé sur un poignet d'une personne, un boîtier tenu par le bracelet, l'ensemble du boîtier et du bracelet étant portable par la personne. Le boîtier comporte un récepteur propre à recevoir des données, un processeur propre à associer à chaque donnée un degré de dangerosité pour la personne, le processeur étant propre à envoyer des données à communiquer à la personne et étant propre à transmettre des données à émettre. Le boîtier comporte également une interface propre à communiquer à la personne des données envoyées par le processeur, et un émetteur propre à émettre des données transmises par le processeur. L'équipement de sécurisation est propre à fonctionner selon au moins deux modes de fonctionnement, notamment trois modes de fonctionnement, chaque mode de fonctionnement étant associé de manière biunivoque à un degré de dangerosité seuil, les données que le processeur est propre à envoyer dans un mode de fonctionnement étant les données associées à un degré de dangerosité supérieur ou égal au degré de dangerosité seuil du mode de fonctionnement considéré.

[0009] Suivant des modes de réalisation particuliers, l'équipement de sécurisation d'une personne comprend une ou plusieurs des caractéristiques suivantes, prise(s) isolément ou suivant toutes les combinaisons techniquement possibles :

- l'interface est propre à vibrer lorsque le récepteur reçoit des données dont le degré de dangerosité est supérieur ou égal au degré de dangerosité seuil le plus haut de l'ensemble des degrés de dangerosité seuil.
- l'équipement de sécurisation comporte, en outre, un bouton de basculement, l'actionnement du bouton de basculement modifiant le mode de fonctionnement de l'équipement de sécurisation.
- l'équipement de sécurisation comporte, en outre, un bouton d'alerte, l'actionnement du bouton d'alerte étant une donnée à émettre.
- le récepteur est propre à recevoir des données provenant d'un réseau global de communication et d'un réseau local de communication, le réseau local de communication regroupant l'équipement de sécurisation et au moins un autre équipement de sécurisation tel que précédemment décrit, l'émetteur est propre à émettre des données sur le réseau global de communication et le réseau local de communication, et le boîtier comporte, en outre, un détecteur d'accessibilité au réseau, le détecteur étant propre à détecter l'accessibilité au réseau global de communication, le récepteur recevant des données provenant du réseau local de communication et l'émetteur émettant des données sur le réseau local de communication lorsque le détecteur détecte que le réseau global de communication n'est pas accessible pour l'équipement de sécurisation.
- les données sont choisies dans le groupe comprenant :

  + des données issues d'autres équipements appartenant à la personne,
  + des données utilisant la position géographique de la personne,
  + des données liées à la position géographique de la personne par rapport à la position géographique des autres équipements, et
  + des données liées à la position géographique de la personne par rapport à un découpage géographique d'une zone.

- il est défini une distance maximale entre deux équipements de sécurisation, une donnée étant que l'autre équipement de sécurisation le plus proche se trouve à une distance plus grande que la distance maximale.
- l'interface comporte un écran propre à afficher des données envoyées par le processeur et une unité

de vibration propre à générer des vibrations pour communiquer à la personne, des données envoyées par le processeur.

[0010] Il est aussi décrit un système de sécurisation d'un ensemble de personnes. Le système comporte, pour chaque personne, au moins un équipement de sécurisation tel que précédemment décrit.

[0011] Suivant un mode de réalisation particulier, le système de sécurisation comporte, en outre, un serveur central, chaque équipement de sécurisation étant propre à échanger des données avec le serveur central via un réseau global de communication et chaque équipement de sécurisation étant propre à échanger des données avec un autre équipement de sécurisation via un réseau local de communication regroupant les équipements de sécurisation du système.

[0012] D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit de modes de réalisation de l'invention, donnée à titre d'exemple uniquement et en référence aux dessins qui sont :

- figure 1, une vue schématique d'un exemple de système de sécurisation d'un ensemble de personnes, chaque personne étant équipée d'un équipement de sécurisation d'une personne,
- figure 2, une vue schématique d'un équipement de sécurisation d'une personne de la figure 1, et
- figure 3, une vue schématique d'un scénario d'utilisation du système de sécurisation selon la figure 1.

[0013] Un système 10 de sécurisation d'un ensemble de personnes est présenté schématiquement à la figure 1.

[0014] Dans le cas de la figure 1, l'ensemble de personnes comporte trois policiers. Pour la suite, le premier policier est noté P1, le deuxième policier est noté P2 et le troisième policier P3.

[0015] Dans ce cas particulier, ainsi que l'indique l'accolade sur la figure 1, les trois policiers P1, P2 et P3 forment une patrouille.

[0016] Le système 10 est propre à améliorer la sécurité des policiers P1, P2 et P3 sur leur terrain d'intervention.

[0017] Le système 10 comporte un serveur central 12 et, pour chacun des policiers P1, P2 et P3, un ensemble d'équipements 14.

[0018] Le serveur central 12 est adapté pour communiquer avec l'ensemble d'équipements 14.

[0019] Le serveur central 12 est un serveur propre à collecter diverses données de sécurité.

[0020] La collection de données est effectuée par réception d'informations provenant de bases de données ou d'équipements dédiés comme des caméras ou l'ensemble d'équipements 14.

[0021] Les données sont, par exemple, des données issues de vidéoprotection, d'alertes enlèvements ou de recensements de vol.

[0022] Plus généralement, les données sont l'ensemble des données relatives au terrain d'intervention et aux personnes présentes sur le terrain d'intervention.

[0023] Les données sont soit collectées automatiquement soit par saisie manuelle d'un opérateur.

[0024] Le serveur central 12 est un serveur distant par rapport à la patrouille et au terrain d'intervention. Cela permet de garantir que le serveur central 12 soit dans un lieu sécurisé.

[0025] Le serveur central 12 est propre à envoyer les données collectées. L'ensemble d'équipements 14 varie selon les policiers P1, P2 et P3 considérés.

[0026] Le premier policier P1 est équipé d'un équipement de sécurisation 16 et d'un ordiphone 18. Un ordiphone est plus souvent désigné par le terme anglais « smartphone ».

[0027] Le deuxième policier P2 est également équipé d'un équipement de sécurisation 16 et d'un ordiphone 18.

[0028] Le troisième policier P3 est équipé d'un équipement de sécurisation 16, d'un ordiphone 18 et d'un véhicule 19.

[0029] Dans l'exemple illustré, il est supposé, pour simplifier que l'équipement de sécurisation 16 est le même pour chacun des policiers P1, P2 et P3, de sorte que, par exemple, la seule différence entre l'équipement de sécurisation 16 du premier policier P1 et l'équipement de sécurisation 16 du deuxième policier P2 est le nom du policier équipé par l'équipement de sécurisation 16.

[0030] De même, il est supposé pour simplifier, que l'ordiphone 18 est le même pour chacun des policiers P1, P2 et P3.

[0031] Un équipement de sécurisation 16 est illustré plus spécifiquement à la figure 2.

[0032] A titre d'exemple, l'équipement de sécurisation 16 est l'équipement de sécurisation du premier policier P1.

[0033] L'équipement de sécurisation 16 est un équipement de sécurisation d'une personne. Un tel équipement permet d'améliorer la sécurité de la personne équipée par l'équipement de sécurisation 16.

[0034] L'équipement de sécurisation 16 fonctionne usuellement en collaboration avec l'ordiphone 18.

[0035] Toutefois, en variante, l'équipement de sécurisation 16 est propre à fonctionner en l'absence de l'ordiphone 18. C'est en particulier le cas lorsque l'équipement de sécurisation 16 comporte les organes pour communiquer en wi-fi ou en 3G/4G.

[0036] L'équipement de sécurisation 16 comprend un bracelet 20 et un boîtier 22.

[0037] Le bracelet 20 est propre à être enroulé sur un poignet d'une personne.

[0038] Par exemple, le bracelet 20 est réalisé en un matériau suffisamment souple pour épouser la forme du poignet.

[0039] Selon l'exemple particulier de la figure 2, le bracelet 20 comporte deux parties 24 et 26 qui sont attachables l'une à l'autre par une attache non représentée sur la figure.

[0040] Selon l'exemple de la figure 2, les deux parties 24 et 26 sont des bandes présentant une largeur identique.

[0041] Le boîtier 22 est tenu par le bracelet 20.

[0042] En l'occurrence, chaque partie 24 et 26 est reliée à une partie du boîtier 22 de manière à ce que chaque partie 24 et 26 soit en regard l'une de l'autre.

[0043] Le boîtier 22 présente une forme cylindrique avec une base quelconque.

[0044] Par l'expression « une forme cylindrique », il est entendu que le boîtier 22 présente la forme d'un solide délimité par deux plans parallèles et par la base.

[0045] Selon l'exemple de la figure 2, la base du boîtier 22 est rectangulaire. Dans ce cas, le boîtier 22 a une forme parallélépipédique.

[0046] En variante, la base du boîtier 22 est un disque.

[0047] Le boîtier 22 est propre à vibrer.

[0048] Le boîtier 22 comporte un récepteur 28, un émetteur 30, un processeur 32, une interface 34, un bouton de basculement 36, un bouton d'alerte 38 et un détecteur 40.

[0049] En variante, le boîtier 22 comporte d'autres organes.

[0050] Parmi ces organes, il peut être cité un bouton de démarrage et d'arrêt, une caméra, un microphone, un haut-parleur ou un capteur de fréquences cardiaques.

[0051] Le boîtier 22 comporte également un ou plusieurs des organes précités.

[0052] Le récepteur 28 est propre à recevoir des données.

[0053] Dans le cadre d'une réception de données, de telles données peuvent être qualifiées de « notifications ».

[0054] Selon l'exemple de la figure 2, le récepteur 28 est une antenne.

[0055] Le récepteur 28 est propre à recevoir des données provenant d'un réseau global de communication. Le réseau global est noté R1 dans la suite.

[0056] Le réseau global R1 est un réseau permettant de relier par communication le serveur central 12 et l'ensemble d'équipements 14 de chaque policier P1, P2 et P3.

[0057] Autrement formulé, chaque équipement de sécurisation 16 est propre à échanger des données avec le serveur central 12 sur le réseau global R1.

[0058] Le réseau global R1 est un réseau sans fil.

[0059] Par exemple, le réseau global R1 est un réseau « wifi ». Il est entendu par l'expression « réseau wi-fi » que le réseau utilisé est conforme à un ensemble de normes concernant les réseaux sans fil qui ont été mises au point par le groupe de travail 11 du Comité de normalisation LAN/MAN de l'IEEE (IEEE 802).

[0060] Selon un autre exemple, le réseau global R1 est un réseau de type 3G. A titre d'illustration le réseau global R1 est conforme aux normes UMTS ou CMDA 2000.

[0061] La norme UMTS (acronyme pour « Universal Mobile Télécommunications System » qui signifie littéralement « système de télécommunications mobile universel ») est une norme délimitant une technologie de téléphonie cellulaire dont la partie radio repose sur une technique dite à étalement de spectre (la technique d'accès multiple W-CDMA, acronyme anglais de « Wideband Code Division Multiple Access » qui signifie « multiplexage par code à large bande »).

[0062] La norme CDMA (acronyme pour « Code division multiple access » qui signifie « accès multiple par répartition en code ») délimite une technologie de communication utilisant un système de codage des transmissions, utilisant la technique d'étalement de spectre. Une telle technologie permet à plusieurs liaisons numériques d'utiliser simultanément la même fréquence porteuse.

[0063] Selon un autre exemple, le réseau global R1 est un réseau de type 4G.

[0064] Le récepteur 28 est également propre à recevoir des données provenant d'un réseau local de communication.

[0065] Le réseau local de communication est noté réseau local R2 dans la suite de la description.

[0066] Le réseau local R2 regroupe l'équipement de sécurisation 16 et au moins un autre équipement de sécurisation 16.

[0067] Le réseau local R2 regroupe dans le cas de la figure 1 les trois équipements de sécurisation 16.

[0068] Autrement formulé, chaque équipement de sécurisation 16 est propre à échanger des données avec un autre équipement de sécurisation 16 sur le réseau local R2.

[0069] Le réseau local R2 est, par exemple, un réseau ad-hoc.

[0070] Selon un cas particulier, le réseau local R2 est un réseau wi-fi sécurisé ou non.

[0071] L'émetteur 30 est propre à émettre des données.

[0072] Selon l'exemple de la figure 2, l'émetteur 30 est une antenne distincte du récepteur 28.

[0073] En variante, le récepteur 28 et l'émetteur 30 sont confondus.

[0074] L'émetteur 30 est propre à émettre des données sur le réseau global R1.

[0075] L'émetteur 30 est également propre à émettre des données sur le réseau local R2.

[0076] Le processeur 32 joue le rôle d'un contrôleur des éléments du boîtier 22.

[0077] Le processeur 32 est, par exemple, un circuit logique programmable.

[0078] Un circuit logique programmable, ou réseau logique programmable, est un circuit intégré logique qui peut être reprogrammé après sa fabrication. Un tel circuit logique programmable est composé de nombreuses cellules logiques élémentaires et bascules logiques librement connectables. Ce type de composant électronique est communément désigné par différents acronymes anglais dont notamment FPGA (acronyme pour « field-programmable gate array » qui signifie « réseau de portes programmables in situ »), PLD (acronyme pour

« programmable logic device » qui signifie « circuit logique programmable »), EPLD (acronyme pour « erasable programmable logic device » qui signifie « circuit logique programmable et effaçable »), CPLD (acronyme pour « complex programmable logic device » qui signifie « circuit logique programmable complexe »), PAL (acronyme pour « programmable array logic » qui signifie « réseau logique programmable ») ou PLA (acronyme pour « programmable logic array » qui signifie « réseau logique programmable »).

[0079] En variante, le processeur 32 est un calculateur.

[0080] Selon une autre variante, le processeur 32 est un processeur informatique propre à mettre en oeuvre des produits programme d'ordinateurs.

[0081] Plus précisément, le processeur 32 est propre à associer à chaque donnée un degré de dangerosité pour la personne qui est équipée de l'équipement de sécurisation 16.

[0082] Par exemple, le processeur 32 comporte une mémoire mémorisant une base de données donnant pour chaque type d'information un degré de dangerosité.

[0083] A titre d'illustration, si la donnée est la présence d'une menace dans l'environnement du premier policier P1, le degré de dangerosité est important. La présence d'une personne connue des services de police est un exemple de menace.

[0084] L'expression du degré de dangerosité dépend du contexte.

[0085] A titre d'exemple, bien que non réaliste, le degré de dangerosité est binaire, de sorte que les données sont traitées selon qu'elles sont considérées comme dangereuses ou non.

[0086] Dans un traitement plus complexe, le degré de dangerosité comporte plusieurs stades, par exemple, un chiffre de 1 à 7. Dans un tel cas, à titre d'explication, un degré de dangerosité de 1 correspond à une donnée relative à une information neutre (carte des lieux par exemple) alors qu'un degré de dangerosité de 7 correspond à une donnée relative à une information vitale pour le premier policier P1.

[0087] D'autres exemples sont détaillés dans la suite de la description en référence à des exemples d'utilisation du système 10.

[0088] Le processeur 32 est propre à envoyer des données à communiquer.

[0089] Le processeur 32 envoie les données à communiquer à l'interface 34.

[0090] Le processeur 32 est propre à transmettre des données à émettre.

[0091] Le processeur 32 envoie les données à émettre à l'émetteur 30.

[0092] Le processeur 32 est propre à contrôler le récepteur 28 et l'émetteur 30.

[0093] En particulier, lorsque le processeur 32 reçoit un signal provenant du détecteur 40 indiquant que le réseau global R1 n'est pas accessible pour l'équipement 16, le processeur 32 est propre à contrôler le récepteur 28 pour que le récepteur 28 reçoive uniquement des données provenant du réseau local R2.

[0094] Similairement et éventuellement conjointement, lorsque le processeur 32 reçoit un signal provenant du détecteur 40 indiquant que le réseau global R1 n'est pas accessible pour l'équipement 16, le processeur 32 est propre à contrôler l'émetteur 30 pour que l'émetteur 30 transmette uniquement des données sur le réseau local R2.

[0095] Le processeur 32 est également propre à contrôler le fonctionnement de l'équipement de sécurisation 16.

[0096] L'équipement de sécurisation 16 est propre à fonctionner selon au moins deux modes de fonctionnement, chaque mode de fonctionnement étant associé de manière biunivoque à un degré de dangerosité seuil, les données que le processeur 32 est propre à envoyer dans un mode étant les données associées à un degré de dangerosité supérieur ou égal au degré de dangerosité seuil du mode de fonctionnement considéré.

[0097] Le degré de dangerosité seuil est paramétrable par l'utilisateur de l'équipement de sécurisation 16.

[0098] Une manière commode de paramétrer le degré de dangerosité seuil de chaque mode de fonctionnement M1, M2 et M3 est que l'utilisateur indique quelle donnée il souhaite connaître et ce, selon le mode de fonctionnement M1, M2 et M3.

[0099] En ce sens, le degré de dangerosité est à entendre comme un degré de dangerosité perçu par l'utilisateur de l'équipement de sécurisation 16 et non comme un degré de dangerosité objectif pour l'utilisateur de l'équipement de sécurisation 16.

[0100] Cela revient à dire que le degré de dangerosité est un moyen de classer le traitement (en l'occurrence l'affichage) des données arrivant au processeur 32.

[0101] A titre d'illustration, dans le cas particulier de la figure 2, l'équipement de sécurisation 16 est propre à fonctionner selon trois modes de fonctionnement M1, M2 et M3.

[0102] Pour la suite, le premier degré de dangerosité seuil associé au premier mode de fonctionnement M1 est noté DDS1, le deuxième degré de dangerosité seuil associé au deuxième mode de fonctionnement M2 est noté DDS2 et le troisième degré de dangerosité seuil associé au troisième mode de fonctionnement M3 est noté DDS3.

[0103] De plus, il est supposé que le premier degré de dangerosité seuil DDS1 est strictement supérieur au deuxième degré de dangerosité seuil DDS2 et que le deuxième degré de dangerosité seuil DDS2 est strictement supérieur au troisième degré de dangerosité seuil DDS3.

[0104] Aussi, dans le premier mode de fonctionnement M1, l'équipement de sécurisation 16 affiche moins de données que dans le deuxième mode de fonctionnement M2.

[0105] Similairement, dans le deuxième mode de fonctionnement M2, l'équipement de sécurisation 16 affiche moins de données que dans le troisième mode de fonc-

tionnement M3.

[0106] Selon un mode de réalisation particulier, dans le premier mode de fonctionnement M1, les données envoyées par le processeur 32 sont un SOS envoyé par un autre policier P1, P2 et P3, des données relatives à la restriction d'une zone (par exemple, zone surveillée par la police et dans laquelle on ne souhaite pas voir de policiers en uniforme) et des données relatives à une personne recherchée.

[0107] Dans le deuxième mode de fonctionnement M2, les données envoyées comprennent les données envoyées dans le premier mode de fonctionnement M1 et d'autres données. Les autres données comprennent des données relatives à une agression physique sur une personne à proximité. La notion de proximité est définie par l'utilisateur en fonction de la mission à accomplir. Les autres données comprennent également des données relatives à un véhicule signalé. Un véhicule signalé est, par exemple, un véhicule volé ou surveillé par un système de lecture automatique de plaques minéralogiques. Les autres données comportent également des données relatives à la proximité d'armes à feu ou d'explosifs. Les autres données comprennent aussi une donnée d'historique sur la zone. Par exemple, les données sont des données relatives à la survenu d'épisodes violents dans une période de temps donnée, par exemple quatre semaines.

[0108] Dans le troisième mode de fonctionnement M3, les données envoyées comprennent les données envoyées dans le deuxième mode de fonctionnement M2 et d'autres informations. Les autres informations sont relatives à la zone du terrain d'intervention : la zone est-elle polluée ? La zone est-elle une zone de manifestation ? Où se situe la foule ? Y a-t-il des bouchons routiers ?

[0109] En variante, la répartition des données est différente et d'autres données sont envoyables par le processeur 32.

[0110] De plus, chaque mode de fonctionnement M1, M2, M3 est caractérisé par une couleur spécifique.

[0111] Similairement, en variante et/ou en complément, chaque mode de fonctionnement M1, M2, M3 est caractérisé par un logo spécifique.

[0112] L'interface 34 est propre à communiquer au policier P1, P2, P3 des données envoyées par le processeur 32.

[0113] L'interface 34 comporte une unité de vibration et un écran. Seul l'écran est visible sur les figures.

[0114] L'écran est propre à afficher des données envoyées par le processeur 32.

[0115] Les données affichées sont des messages, des photos ou des images.

[0116] Dans le cas particulier représenté, l'écran présente des dimensions réduites.

[0117] Par exemple, l'aire de la surface de l'écran sur laquelle des données sont affichables est inférieure ou égale à 15 cm^2, notamment inférieure ou égale à 11 cm^2.

[0118] Du fait de cette taille de l'écran, lorsque les données à afficher sont trop grandes par rapport à la taille de l'écran, une seule partie des données est affichée sur l'écran. Pour accéder à la totalité des données, le policier P1, P2 et P3 utilise son ordiphone 18 qui est en communication avec l'équipement de sécurisation 16.

[0119] Selon un mode de réalisation particulier, l'interface 34 est également une interface de saisie d'informations par le policier P1, P2 et P3.

[0120] Cela permet également au policier P1, P2 et P3 d'interagir avec l'interface 34, par exemple, pour dire qu'il va rejoindre un autre policier P1, P2 et P3.

[0121] L'unité de vibration est propre à faire vibrer le boîtier 22.

[0122] En particulier, lorsque le récepteur 28 reçoit des données dont le degré de dangerosité est supérieur ou égal au degré de dangerosité seuil DDS1 le plus haut de l'ensemble des degrés de dangerosité seuil DDS1, DDS2 et DDS3, le processeur 32 fait vibrer l'unité de vibration.

[0123] L'unité de vibration est propre à générer des vibrations différentes.

[0124] A titre d'illustration, lorsque le policier reçoit une alarme SOS, l'unité de vibration vibre de façon à transmettre les lettres S - O - S en 'morse vibré', soit 3 courtes vibrations puis 3 longues vibrations et 3 courtes vibrations.

[0125] Dans certains modes de fonctionnement, les données envoyées sont exclusivement affichées ou vibrées.

[0126] Dans d'autres modes de fonctionnement, certaines données envoyées sont à la fois affichées par l'écran et « vibrées » à l'aide de l'unité de vibration.

[0127] Le bouton de basculement 36 est, selon l'exemple de la figure 2, un bouton poussoir.

[0128] En variante, le bouton de basculement 36 est une zone tactile de l'écran..

[0129] L'actionnement du bouton de basculement 36 modifie le mode de fonctionnement de l'équipement de sécurisation 16.

[0130] Par exemple, un appui simple permet de basculer dans le premier mode M1, un double appui permet de basculer dans le deuxième mode M2 et un appui prolongé permet de basculer dans le troisième mode M3.

[0131] En variante, l'appui simple sur le bouton de basculement 36 permet de passer au mode suivant. De fait, lorsque l'équipement est dans le premier mode M1, un appui simple permet de basculer dans le deuxième mode M2 ; lorsque l'équipement est dans le deuxième mode M2, un appui simple permet de basculer dans le troisième mode M3 et lorsque l'équipement est dans le troisième mode M3, un appui simple permet de basculer dans le premier mode M1.

[0132] Le bouton d'alerte 38 est, selon l'exemple de la figure 2, un bouton poussoir.

[0133] En variante, le bouton d'alerte 38 est une zone tactile de l'écran.

[0134] Dans ces deux cas, ce sont les doubles clics qui sont détectés pour éviter les fausses alertes en cas de simple clic accidentel.

[0135] L'actionnement du bouton d'alerte 38 étant une donnée à émettre.

[0136] Dans un mode de réalisation particulier, le bouton d'alerte 38 fait changer le statut du policier P1, P2, P3. Un policier P1, P2 ou P3 ayant actionné le bouton d'alerte 38 apparaîtra sur une carte par un point rouge.

[0137] Le détecteur 40 est un détecteur d'accessibilité au réseau.

[0138] Plus spécifiquement le détecteur 40 est propre à détecter l'accessibilité au réseau global R1.

[0139] Selon un mode de réalisation particulier, le détecteur 40 fait partie du processeur 32. Le détecteur 40 est propre à analyser le bruit sur le récepteur 28 et à choisir le type de communication via le réseau global R1 ou via le réseau local R2.

[0140] Il est à noter que le détecteur 40 est propre à favoriser l'utilisation du réseau global R1 pour assurer une bonne mise à jour du processeur 32.

[0141] Le détecteur 40 émet un signal vers le processeur 32. Le signal émis est un signal indiquant que le réseau global R1 n'est pas accessible pour l'équipement 16.

[0142] Dans un mode de réalisation particulier, le signal est un signal binaire, un « 0 » indiquant que le réseau global R1 n'est pas accessible alors qu'un « 1 » indique que le réseau global R1 est accessible.

[0143] L'ensemble du boîtier 22 et du bracelet 20 sont portables par la personne. Il est entendu par cette expression, le bracelet 20 et l'ensemble des éléments du boîtier 22.

[0144] Par exemple, le poids de l'ensemble du boîtier 22 et du bracelet 20 est inférieur à 100 grammes, par exemple inférieur à 70 grammes.

[0145] Similairement, l'encombrement total de l'ensemble du boîtier 22 et du bracelet 20 est inférieur à 40 cm^3.

[0146] Le fonctionnement du système 10 est maintenant décrit en référence à plusieurs scenarii d'utilisations.

[0147] Selon un exemple illustré par la figure 3, les trois policiers P1, P2 et P3 ont à appréhender un suspect S dans une zone spatiale 100. Pour la suite, il est également supposé que le suspect S a un complice C.

[0148] Dans ce cas particulier, les trois policiers P1, P2 et P3 sont en civil pour ne pas attirer l'attention.

[0149] La zone spatiale 100 comporte quatre rues 102, 104, 106 et 108 se croisant à une intersection.

[0150] Dans l'exemple proposé, la zone spatiale 100 est découpée selon un découpage en sept zones : une première zone Z1, une deuxième zone Z2, une troisième zone Z3, une quatrième Z4, une cinquième zone Z5, une sixième zone Z6 et une septième zone Z7.

[0151] La première zone Z1 est délimitée d'une part par la première rue 102 et d'autre part par une première barrière 112. Chaque barrière est représentée par une ligne pointillée sur la figure 3 et se présente sous la forme d'une demi-droite ayant pour origine l'intersection.

[0152] La deuxième zone Z2 est délimitée d'une part par la première barrière 112 et d'autre part par la deuxième rue 104. La troisième zone Z3 est délimitée d'une part par la deuxième rue 104 et d'autre part par une deuxième barrière 114. La quatrième zone Z4 est délimitée d'une part par la deuxième barrière 114 et par une troisième barrière 116. La cinquième zone Z5 est délimitée d'une part par la troisième barrière 116 et d'autre part par la troisième rue 106. La sixième zone Z6 est délimitée par la troisième rue 106 et d'autre part par la quatrième rue 108. La septième zone Z7 est délimitée d'une part par la quatrième rue 108 et d'autre part par la première rue 102.

[0153] Dans le cas illustré, le premier policier P1 et le complice C sont dans la première zone Z1, le deuxième policier P2 est dans la troisième zone Z3 et le troisième policier P3 ainsi que le suspect S sont dans la quatrième zone Z4.

[0154] Par exemple, selon un scénario, supposons que le premier policier P1 identifie le complice C.

[0155] Le premier policier P1 appuie sur le bouton d'alerte 38 de l'équipement de sécurisation 16 deux fois.

[0156] Dans ce cas, il est supposé qu'il a été convenu qu'un double appui sur le bouton d'alerte 38 est le signe que le complice C a été vu.

[0157] Dans un tel scénario, l'émetteur 30 de l'équipement de sécurisation 16 émet une donnée relative au fait que le complice C a été vu via le réseau global R1.

[0158] Le serveur central 12 est aussi capable de géolocaliser le premier policier P1, par exemple, par une triangulation du signal de l'ordiphone 18 du premier policier P1.

[0159] Le serveur central 12 émet alors des informations sur la présence du complice C dans la première zone Z1. Une telle information est supposée être une donnée dont le degré de dangerosité est compris entre le premier degré de dangerosité seuil DDS1 et le deuxième degré de dangerosité seuil DDS2.

[0160] Supposons que l'équipement de sécurisation 16 du deuxième policier P2 soit dans le deuxième mode M2.

[0161] Le deuxième policier P2 est alors averti de la présence du complice C dans la première zone Z1 et peut venir en renfort du premier policier P1 ou choisir de modifier sa position selon son intuition.

[0162] Supposons que l'équipement de sécurisation 16 du troisième policier P3 soit dans le premier mode M1. Le troisième policier P3 étant proche du suspect S et cherchant à vérifier qu'il s'agit bien de lui ne veut que les données les plus importantes pour sa sécurité. Dans le premier mode M1, le troisième policier P3 n'est pas averti de la présence du complice C dans la première zone Z1.

[0163] Dans un tel scénario, le système de sécurisation 10 a permis d'améliorer le niveau d'information du deuxième policier P2 sans mettre en danger le troisième policier P3.

[0164] Selon un autre scénario, supposons que le troisième policier P3 identifie le suspect S mais capte uniquement le réseau local R2.

[0165] Le troisième policier P3 appuie sur le bouton d'alerte 38 de l'équipement de sécurisation 16 une fois.

[0166] Dans ce cas, il est supposé qu'il a été convenu qu'un appui simple sur le bouton d'alerte 38 est le signe que le suspect S a été vu.

[0167] Dans un tel scénario, l'émetteur 30 de l'équipement de sécurisation 16 émet une donnée relative au fait que le suspect S a été vu via le réseau local R2 (pas de connexion au réseau global R1).

[0168] Les deux policiers P1 et P2 reçoivent l'information qui est ensuite transmise au réseau global R1 puisque le premier et le deuxième policiers P1 et P2 ont accès au réseau global R1.

[0169] Le serveur central 12 est capable de géolocaliser le troisième policier P3, par exemple, par une triangulation du signal de l'ordiphone 18 du troisième policier P3.

[0170] Le serveur central 12 émet alors des informations sur la présence du suspect S dans la quatrième zone Z4. Une telle information est supposée être une donnée dont le degré de dangerosité est supérieur au premier degré de dangerosité seuil DDS1.

[0171] Dans une telle situation, les deux policiers P1 et P2 sont informés de l'endroit où se trouve le suspect S rapidement. Du point de vue du troisième policier P3, cette information est transmise discrètement par appui sur le bouton d'alerte 38. Sa sécurité est améliorée puisque sa couverture n'est pas mise en péril et que des renforts (le premier et le deuxième policiers P1 et P2) arrivent rapidement.

[0172] Dans les scénarii illustrés, ont été utilisées des données utilisant la position géographique de la personne considérée ou des données liés à l'actionnement d'un bouton d'alerte.

[0173] D'autres scénarii sont envisageables.

[0174] Par exemple, le deuxième policier P2 peut chuter gravement. L'actionnement du bouton d'alerte 38, notamment par un double clic, couplé à une géolocalisation permet de le sauver rapidement.

[0175] Selon un autre exemple, le troisième policier P3 est dans son véhicule 19 et le véhicule 19 est équipé d'un dispositif de reconnaissance de plaques d'immatriculation. Dans l'hypothèse où il reconnaît une plaque de voiture volée, il est possible d'avertir les autres policiers P1 et P2.

[0176] En variante, supposons que, pour des raisons de sécurité, il est défini une distance maximale entre deux policiers P1, P2 et P3. Le système 10 permet de détecter qu'un policier, par exemple le troisième policier P3, s'éloigne trop des autres policiers P1 et P2 et de l'avertir. Dans ce cas, une donnée échangée est l'autre équipement de sécurisation 16 le plus proche se trouve à une distance plus grande que la distance maximale.

[0177] Selon un autre scénario, si la cinquième zone Z5 est interdite au passage, le système 10 permet d'avertir discrètement le troisième policier P3 de sa proximité avec une telle zone interdite.

[0178] Selon un autre scénario, le policier P1, P2, P3 peut prendre une photo de son environnement de manière discrète afin de partager la situation sur le terrain avec le serveur central 12, et avec les autres policiers P1, P2, P3. Dans ce cas, le boîtier 22 comporte un appareil photo ou une caméra.

[0179] Selon un autre scénario, le policier P1, P2, P3 peut effectuer une prise de son ambiant de manière discrète afin de partager la situation sur le terrain avec le serveur central 12, et avec les autres policiers P1, P2, P3. Dans ce cas, le boîtier 22 comporte un microphone. Dans ces différents scénario, il apparaît que le système de sécurisation 10 permet, grâce à l'emploi de l'équipement de sécurisation 16 d'améliorer la circulation de données entre une patrouille de trois policiers P1, P2 et P3 avec une bonne discrétion.

[0180] Il en résulte une sécurité accrue pour chacun des trois policiers P1, P2 et P3.

[0181] Autrement dit, le système de sécurisation 10 assure la protection des policiers P1, P2 et P3 par l'apport d'une information juste et fournie à un instant adapté.

[0182] De fait, l'équipement de sécurisation 16 est connecté à un serveur central 12 qui centralise les données et redescend les données pertinentes aux personnes équipées avec un équipement de sécurisation 16. Une synchronisation est générée entre chaque équipement de sécurisation 16 et le serveur central 12.

[0183] Cela permet de développer le sixième sens des policiers P1, P2 et P3.

[0184] Le système de sécurisation 10 permet également de diminuer les temps de latence de transmission entre les messages.

[0185] Le système de sécurisation 10 offre la possibilité de fonctionner en mode local avec les autres membres de la patrouille auquel l'utilisateur de l'équipement de sécurisation 16 appartient.

[0186] L'équipement de sécurisation 16 est bien adapté pour un emploi en mouvement et en situation d'interpellation d'un suspect S. Plus généralement, l'emploi est compatible avec des missions de terrain du fait de la discrétion et de la liberté octroyée aux mains des policiers P1, P2 et P3. Dans certains modes de fonctionnement, l'équipement de sécurisation 16 informe le policier P1, P2 ou P3 par une simple vibration du boîtier 22.

[0187] De plus, le système de sécurisation 10 permet que les informations données au policier P1, P2 ou P3 soit toujours mises à jour puisque sont mis en relation un serveur central 12 avec une communication déportée sur chaque interface 34 pourvu que le réseau global R1 soit accessible.

[0188] De manière générale, dans chaque scénario, le policier P1, P2 ou P3 a accès à des données relatives à une vue globale de la situation, à la géolocalisation des personnes équipées, aux personnes faisant partie d'une patrouille, à la présence de zones de foule, de zones dangereuses, de manifestations, à des informations sur l'évolution de la mission en cours ou à des biodonnées.

[0189] Les biodonnées sont des données relatives à la santé du policier P1, P2 ou P3. Par exemple, les bat-

tements du coeur du policier P1, P2 ou P3 sont enregistrés.

[0190] L'accès facilité à ces informations permet de répondre aux besoins des policiers P1, P2 et P3 rencontrés lors de situations concrètes. Parmi ces différentes situations, il peut être mentionné le besoin d'aide et de support à un équipier, l'isolement d'un policier la prise discrète de photos ou l'écoute discrète.

[0191] Pour améliorer encore la sécurisation des policiers P1, P2 et P3, l'équipement de sécurisation 16 a l'apparence d'un objet banalisé.

[0192] Par exemple, l'équipement de sécurisation 16 forme une montre, le boîtier 22 étant dans ce cas un cadran.

[0193] De plus, un des avantages du système de sécurisation 10 est sa reconfigurabilité.

[0194] De fait, il est possible d'intégrer aisément de nouveaux équipements par une modification du processeur 32 et du serveur central 12.

[0195] Ainsi, le système de sécurisation 10 est capable d'enrichir aisément ses capacités d'alerte en fonction de l'évolution technologique.

[0196] L'équipement de sécurisation 16 s'applique pour toute personne ayant un besoin de protection et/ou de discrétion.

[0197] A titre d'illustration, la personne fait partie d'une force de sécurité privée ou publiques.

[0198] Selon un autre exemple, la personne fait partie de service de secours, comme les pompiers.

[0199] Selon encore un autre exemple, la personne est une célébrité.

[0200] D'autres modes de réalisation sont envisageables.

[0201] En particulier, pour améliorer la prise d'informations par le policier P1, P2 ou P3, plusieurs types d'affichage sont utilisés.

[0202] Par exemple, un premier affichage est un affichage de type carte.

[0203] Dans un tel mode de réalisation, une carte est affichée et des données sont représentées sur la carte.

[0204] Par exemple, des données sont affichées sous forme de disque présentant une couleur spécifique et/ou de pictogramme.

[0205] A titre d'illustration, l'orientation d'un policier P1, P2 ou P3 est illustrée par des flèches.

[0206] Des données complémentaires sont également affichables comme une donnée de distance permettant au policier P1, P2 ou P3 de mieux appréhender la situation.

[0207] Selon un mode de réalisation, la carte est affichée de sorte que le centre de l'écran corresponde à la position actuelle du policier P1 équipé par l'équipement de sécurisation 16.

[0208] En variante, le policier P1 peut interagir avec la carte, notamment pour agrandir une zone ou la réduire selon son besoin.

[0209] Un deuxième affichage est un affichage permettant de déterminer les membres de la patrouille pour la mission à effectuer et leur statut.

[0210] Par exemple, il est affiché une interface avec neuf visages, les neuf visages des membres de la patrouille.

[0211] Selon un mode de réalisation, un visage surligné selon une première couleur indique que la personne ne participe pas à la mission. Un visage surligné selon une deuxième couleur indique que la personne est en danger.

[0212] En complément, un visage encadré selon une première couleur indique que la personne est disponible. Un visage encadré selon une deuxième couleur indique que la personne est en train d'aller secourir une autre personne en danger.

[0213] Un troisième affichage est un affichage banalisé.

[0214] Le passage d'un affichage à l'autre s'effectue par une action de glissement sur l'écran.

[0215] Sur ces affichages, sont superposables des affichages de messages permettant d'interagir avec le policier P1, P2 ou P3.

[0216] Un exemple d'interaction consiste à obtenir une information du policier P1, P2 ou P3.

[0217] Un exemple de message est un besoin d'aide avec deux réponses possibles « non » ou «j'y vais ». Un tel message fait suite à une demande d'aide émanant d'un autre membre de la patrouille.

[0218] Un autre exemple d'interaction consiste à informer le policier P1 P2 ou P3.

[0219] A titre d'illustration, si le policier entre dans une zone polluée, le serveur central communique un message du type « entrée dans la zone interdite ».

[0220] De plus, selon une variante, dans certaines modes de fonctionnement M1, M2 ou M3, l'affichage à l'écran de données dure un temps limité pour éviter de mettre en péril la position du policier P1, P2 ou P3.

[0221] Dans un mode de réalisation, le mode de fonctionnement M1, M2 ou M3 est considéré comme une donnée à communiquer à la personne.

[0222] Par exemple, un pictogramme dédié est affiché lorsqu'un mode de fonctionnement M1, M2 ou M3 est choisi.

[0223] D'autres modes de réalisations de l'invention sont obtenus en combinant les précédents modes de réalisations lorsque ces modes de réalisations sont techniquement compatibles.

Revendications

1. Equipement de sécurisation (16) d'une personne (P1, P2, P3), l'équipement de sécurisation (16) comprenant :

   - un bracelet (20) propre à être enroulé sur un poignet d'une personne (P1, P2, P3),
   - un boîtier (22) tenu par le bracelet (20), l'ensemble du boîtier (22) et du bracelet (20) étant

portable par la personne (P1, P2, P3),

le boîtier (22) comportant :

- un récepteur (28) propre à recevoir des données,
- un processeur (32) propre à associer à chaque donnée un degré de dangerosité pour la personne (P1, P2, P3), le processeur (32) étant propre à envoyer des données à communiquer à la personne (P1, P2, P3) et étant propre à transmettre des données à émettre,
- une interface (34) propre à communiquer à la personne (P1, P2, P3) des données envoyées par le processeur (32), et
- un émetteur (30) propre à émettre des données transmises par le processeur (32),

l'équipement de sécurisation (16) étant propre à fonctionner selon au moins deux modes de fonctionnement, notamment trois modes de fonctionnement (M1, M2, M3), chaque mode de fonctionnement (M1, M2, M3) étant associé de manière biunivoque à un degré de dangerosité seuil (DDS1, DDS2, DDS3), les données que le processeur (32) est propre à envoyer dans un mode de fonctionnement (M1, M2, M3) étant les données associées à un degré de dangerosité supérieur ou égal au degré de dangerosité seuil (DDS1, DDS2, DDS3) du mode de fonctionnement (M1, M2, M3) considéré.

2. Équipement de sécurisation selon la revendication 1, dans lequel l'interface (34) est propre à vibrer lorsque le récepteur (28) reçoit des données dont le degré de dangerosité est supérieur ou égal au degré de dangerosité seuil le plus haut (DDS1) de l'ensemble des degrés de dangerosité seuil (DDS1, DDS2, DDS3).

3. Équipement de sécurisation selon la revendication 1 ou 2, dans lequel l'équipement de sécurisation (16) comporte, en outre, un bouton de basculement (36), l'actionnement du bouton de basculement (36) modifiant le mode de fonctionnement (M1, M2, M3) de l'équipement de sécurisation (16).

4. Équipement de sécurisation selon l'une quelconque des revendications 1 à 3, dans lequel l'équipement de sécurisation (16) comporte, en outre, un bouton d'alerte (38), l'actionnement du bouton d'alerte (38) étant une donnée à émettre.

5. Équipement de sécurisation selon l'une quelconque des revendications 1 à 4, dans lequel :

- le récepteur (28) est propre à recevoir des données provenant d'un réseau global de communication (R1) et d'un réseau local de communication (R2), le réseau local de communication (R2) regroupant l'équipement de sécurisation (16) et au moins un autre équipement de sécurisation (16) selon l'une quelconque des revendications 1 à 4,
- l'émetteur (30) est propre à émettre des données sur le réseau global de communication (R1) et le réseau local de communication (R2), et
- le boîtier (22) comporte, en outre, un détecteur (40) d'accessibilité au réseau, le détecteur (40) étant propre à détecter l'accessibilité au réseau global de communication (R1), le récepteur (28) recevant des données provenant du réseau local de communication (R2) et l'émetteur (30) émettant des données sur le réseau local de communication (R2) lorsque le détecteur (40) détecte que le réseau global de communication (R1) n'est pas accessible pour l'équipement de sécurisation (16).

6. Équipement de sécurisation selon l'une quelconque des revendications 1 à 5, dans lequel les données sont choisies dans le groupe comprenant :

- des données issues d'autres équipements (14) appartenant à la personne (P1, P2, P3),
- des données utilisant la position géographique de la personne (P1, P2, P3),
- des données liées à la position géographique de la personne (P1, P2, P3) par rapport à la position géographique des autres équipements (14), et
- des données liées à la position géographique de la personne (P1, P2, P3) par rapport à un découpage géographique d'une zone.

7. Équipement de sécurisation selon l'une quelconque des revendications 1 à 6, dans lequel il est défini une distance maximale entre deux équipements de sécurisation (16), une donnée étant que l'autre équipement de sécurisation (16) le plus proche se trouve à une distance plus grande que la distance maximale.

8. Équipement de sécurisation selon l'une quelconque des revendications 1 à 7, dans lequel l'interface 34 comporte un écran propre à afficher des données envoyées par le processeur (32) et une unité de vibration propre à générer des vibrations pour communiquer à la personne (P1, P2, P3), des données envoyées par le processeur (32).

9. Système de sécurisation (10) d'un ensemble de personnes (P1, P2, P3), le système comportant, pour chaque personne (P1, P2, P3), au moins un équipement de sécurisation (16) selon l'une quelconque des revendications 1 à 8.

10. Système de sécurisation (10) selon la revendication 9, le système de sécurisation (10) comportant, en outre, un serveur central (12), chaque équipement de sécurisation (16) étant propre à échanger des données avec le serveur central (12) via un réseau global de communication (R1) et chaque équipement de sécurisation (16) étant propre à échanger des données avec un autre équipement de sécurisation (16) via un réseau local de communication (R2) regroupant les équipements de sécurisation (16) du système (10).

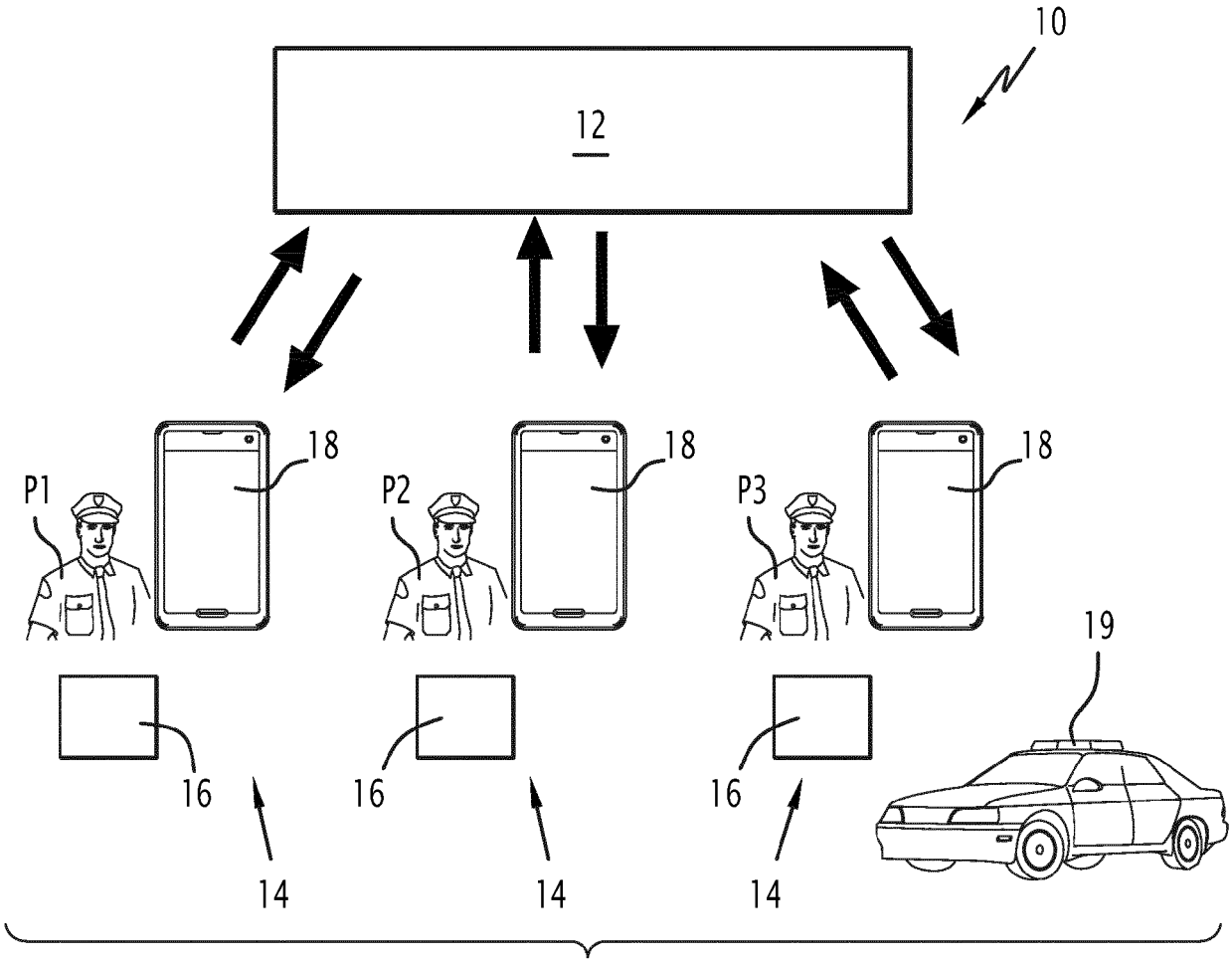
10
12
18
18
18
P1
P2
P3
19
16
16
16
14
14
14

FIG.1

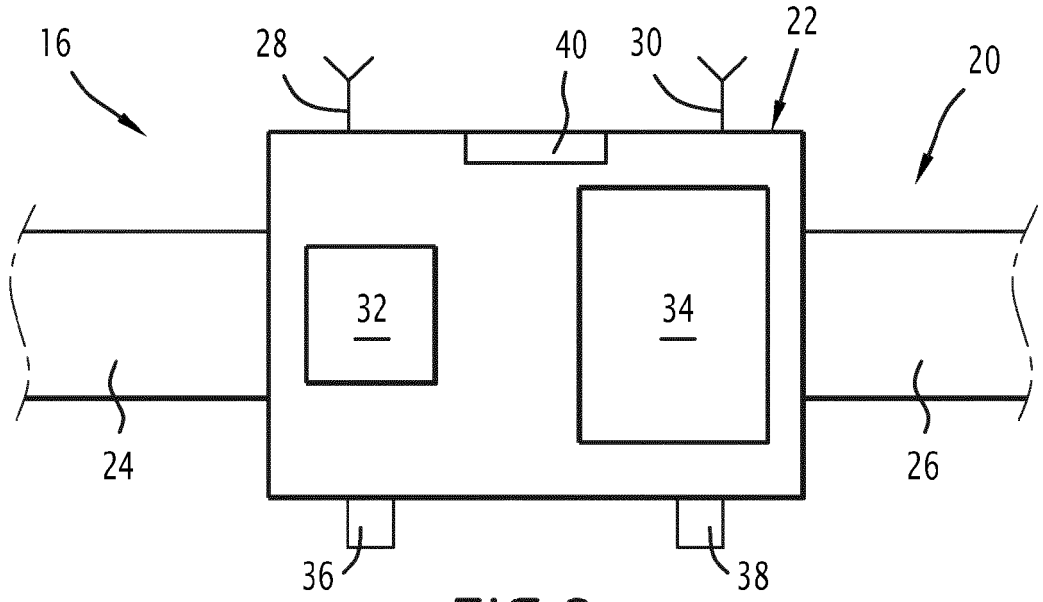
16
28
40
30
22
20
32
34
24
26
36
38

FIG.2

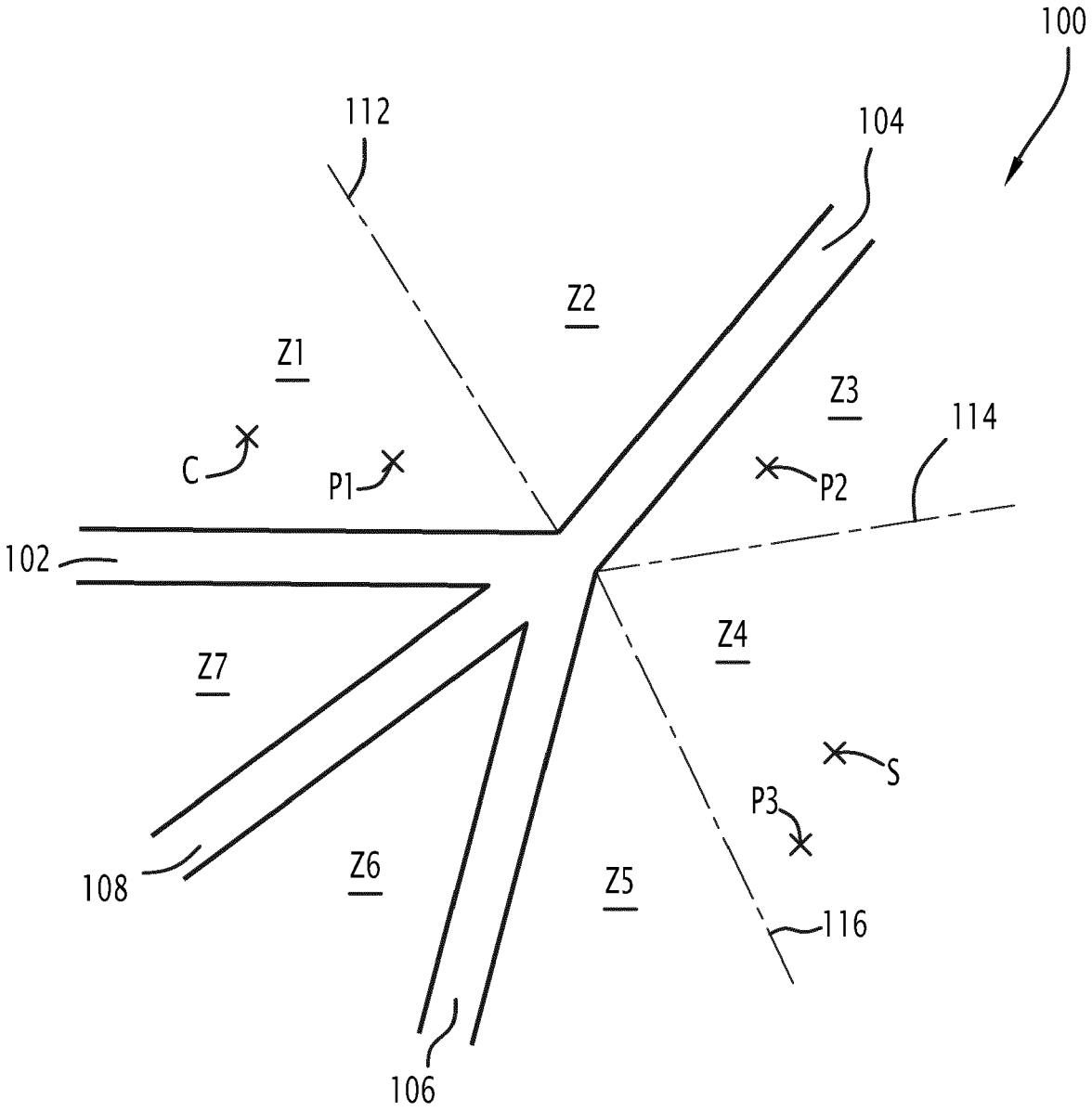

FIG.3

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 16 19 8252

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
Y A	US 2015/206419 A1 (JOHNSON JEFFREY DOUGLAS [US] ET AL) 23 juillet 2015 (2015-07-23) * alinéa [0005] * * alinéa [0087] - alinéa [0091] * * alinéa [0100] * * alinéa [0107] - alinéa [0108] * * alinéa [0111] - alinéa [0112] * * alinéa [0132] - alinéa [0139] * * alinéa [0141] * * figures 2,3,4 *	1-4,6-10 5	INV. G08B21/02 G08B25/01
Y	US 2011/046920 A1 (AMIS DAVID [US]) 24 février 2011 (2011-02-24) * Paragraphes [0003], [0005], [0030], [0092], [0093] *	1-4,6-10	
A	WO 2014/169232 A1 (INTREPID NETWORKS LLC [US]) 16 octobre 2014 (2014-10-16) * alinéa [0053] - alinéa [0058] * * alinéas [0105], [0106] * * alinéa [0111] *	1	

DOMAINES TECHNIQUES RECHERCHES (IPC)

G08B

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	16 mars 2017	Bourdier, Renaud

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

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

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 16 19 8252

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

16-03-2017

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2015206419 A1	23-07-2015	US 2015206419 A1	23-07-2015
		US 2015264550 A1	17-09-2015
US 2011046920 A1	24-02-2011	US 2011046920 A1	24-02-2011
		US 2015042467 A1	12-02-2015
WO 2014169232 A1	16-10-2014	US 2016119424 A1	28-04-2016
		WO 2014169232 A1	16-10-2014

EPO FORM P0460

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