(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 105 867***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **19 15691**

(51) Int Cl[8] : ***G 08 B 21/00*** *(2019.12), H 04 L 29/08*

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

(54) dispositif, système et procédé de traitement de données d'alerte, programmes d'ordinateur correspondants.

(22) **Date de dépôt :** 27.12.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 02.07.21 Bulletin 21/26.

(45) **Date de la mise à disposition du public du brevet d'invention :** 18.11.22 Bulletin 22/46.

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

Se reporter à la fin du présent fascicule

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *WaryMe Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** BERGER Boris.

(73) **Titulaire(s) :** WaryMe Société par actions simplifiée.

(74) **Mandataire(s) :** CABINET VIDON BREVETS & STRATEGIE.

FR 3 105 867 - B1

Description

Titre de l'invention : dispositif, système et procédé de traitement de données d'alerte, programmes d'ordinateur correspondants

[0001] 1. Domaine

[0002] L'invention se rapporte au domaine de la gestion d'alerte et de crise. Plus particulièrement, l'invention se rapporte au domaine des dispositifs et systèmes de traitement de données d'alerte en provenance de dispositifs d'alerte et de gestion de crise au sein d'une organisation.

[0003] 2. Art Antérieur

[0004] Les organisations sont de plus en plus confrontées à des problématiques de gestion de crise. Dans la vie d'une organisation, une crise peut survenir à tout moment, et il n'est pas nécessairement possible d'éviter de telles crises. L'organisation doit donc s'organiser pour faire face à ces crises. De telles crises peuvent se rapporter à des évènements climatiques, à des évènements industriels (incendie, crise sanitaire par exemple) ou encore à des évènements liés à des personnes (attaque terroriste, par exemple). Pour gérer le plus efficacement possible de telles crises, les organisations procèdent généralement à l'établissement de plans de gestion de crise.

[0005] D'une manière générale, tout plan de gestion de crise débute par une analyse des risques. Au regard de l'activité de l'organisation et de la nature de la crise (météorologique, sanitaire, sociale, dysfonctionnement, panne, décès…), les risques diffèrent, ainsi que les solutions à mettre en place. L'étape de l'analyse des risques permet de savoir comment réagir. Le plan de gestion de crise découle de l'analyse pour prendre en compte des scenarii possibles et y apporter des réponses opérationnelles. Il peut s'agir de détailler la marche à suivre pour assurer la continuité d'une activité, de désigner une personne responsable des échanges avec les pouvoirs publics, d'identifier des administrations, partenaires ou prestataires à contacter en priorité, d'imaginer un plan d'évacuation du public ou des équipes, etc. Chaque solution à mettre en œuvre dépend tant de l'organisation que de la crise à affronter. En revanche, l'attribution des différents rôles à chaque acteur de la crise et la mise en place d'une salle de crise en fonction des besoins, apparaissent comme des prérequis à toute bonne gestion de crise. C'est au sein de cette salle que les informations essentielles aux choix des réponses à apporter sont délivrées, en temps réel.

[0006] Le plan de gestion de crise constitue ainsi un outil important de la gestion des crises survenant dans les organisations. Ces plans de gestion de crise reposent généralement sur une communication d'information sous une forme ascendante : les informations de terrain sont remontées, par une ou plusieurs personnes, en salle de crise. Le comité de

gestion de crise centralise les informations remontées, les compile et prend les décisions adéquates en fonction des données compilées et du plan de gestion de crise préalablement établi.

[0007] Cependant, les outils techniques et pratiques de collecte de l'information sont très banals : il apparait ainsi que la communication téléphonique reste le moyen de communication le plus employé pour remonter une information (par une personne déclenchant une alerte) ou pour gérer une crise (par un gestionnaire en charge), alors même qu'une telle communication repose sur des dispositifs et des composants qui ne sont pas nécessairement bien adaptés à ce type de situation. En effet, la communication téléphonique (voire vidéophonique) est essentiellement mise en œuvre pour transmettre, en temps plus ou moins réel des informations sur une alerte ou une crise en cours à une autorité compétente (en salle de crise). Pour ce faire, on utilise par exemple le réseau téléphonique traditionnel (réseau voix), voire un protocole de voix sur IP (H323, SIP) et plus rarement une solution de streaming vidéo en temps réel. Ces moyens sont particulièrement mal adaptés, surtout lors d'un déclenchement d'alerte, c'est-à-dire peu de temps après la survenance d'un évènement déclenchant (potentiellement) une crise et donc une nécessité de gestion d'une telle crise.

[0008] Ainsi, quelle que soit la technologie employée, la survenance d'un évènement entraine généralement la mise en œuvre des étapes suivantes :

[0009] a. déclenchement de l'alerte (volontaire ou automatique) ;

[0010] b. le dispositif d'utilisateur engage un appel téléphonique vers un numéro d'alerte préalablement déterminé (par exemple vers un téléopérateur spécialisé en gestion de ce type d'évènement) ;

[0011] c. le récepteur (un téléopérateur dans un centre d'appel) est en communication bidirectionnelle avec l'émetteur de l'alerte.

[0012] Les informations sont remontées par l'émetteur de l'alerte à destination de l'opérateur, qui lui-même remonte ces informations au centre de gestion de crise. Dans ce cas de figure, l'opérateur ne reçoit des informations qu'en provenance d'une seule et unique personne. Si plusieurs personnes transmettent des informations au centre de gestion de crise (par exemple parce qu'une alerte est déclenchée par plusieurs personnes), cela implique que plusieurs opérateurs sont disponibles et en charge de la collecte, de l'ordonnancement et de la transmission de ces informations à destination du centre de gestion de crise. On fait donc face à un problème de gestion de ressources humaine et de cout important. Il faut être capable de mobiliser un grand nombre d'opérateurs pour prendre en charge les appels téléphoniques. Le dimensionnement de l'infrastructure téléphonique du centre d'appel a aussi un impact (nombre d'appels téléphoniques qui peuvent être pris simultanément). À titre d'exemple, on peut se rapporter aux attentats du 13 novembre 2015 à Paris. Un grand nombre d'appels télé-

phoniques vers le numéro d'urgence (17) n'ont pas pu être reçus et/ou gérés. Ainsi la police a mis beaucoup de temps à comprendre que plusieurs attaques étaient menées simultanément en plusieurs endroits différents. Cette lenteur de prise en charge peut avoir eu un impact sur le nombre des victimes.

[0013] Par ailleurs, techniquement, la solution de l'art antérieur n'est pas fiable : d'une part, les informations sont essentiellement transmises vocalement par le déclencheur de l'alerte à l'opérateur : le déclencheur de l'alerte est dans l'obligation de s'exprimer pour rende compte de la situation ce qui n'est pas nécessairement possible ou souhaitable (notamment en cas de menaces terroristes ou de menaces sur les personnes). Éventuellement, une communication à base de messages (de type SMS) est envisageable : un tel message peut être émis automatiquement par le dispositif du déclencheur de l'alerte, entrainant un appel « automatique » du centre d'appel vers ce dispositif. Il n'en reste pas moins que l'émetteur de l'alerte n'est pas nécessairement en situation de pouvoir répondre, que ce soit vocalement ou par SMS. Quoi qu'il en soit, un appel téléphonique ne peut être routé que vers un seul destinataire, dont le numéro de téléphone est configuré dans le dispositif appelant (par exemple le terminal d'utilisateur). La téléphonie classique ne permet pas de router un appel vers plusieurs personnes simultanément pour permettre la réception et le traitement par un groupe d'encadrants. C'est pourquoi, quand le dispositif d'utilisateur est configuré (c'est-à-dire quand ces situations d'urgence ou de crise ont été prévues à l'avance) c'est généralement pour un traitement par un centre de téléassistance, dont l'organisation garantit la réception 24/7 des appels de détresse, qui monte (ou fait monter) ainsi lui-même, si nécessaire (après une levée de doute), une salle de crise. Outre le prix élevé d'une telle manière de faire (le centre de téléassistance, disponible 24/7, certifié APSAD P3, est le principal poste de coût d'une solution de type « Protection du Travailleur Isolé (PTI)), le centre de télésurveillance ne fait que recevoir l'alerte, réalise le premier niveau de levée de doute (fausse alerte) et exécute une procédure définie préalablement par l'organisation client. Cette procédure prévoit généralement l'appel aux forces de secours publics (si besoin) et le rappel des responsables de l'organisation cliente. La plus-value du centre de téléassistance est donc essentiellement sa capacité à assurer la réception de l'appel téléphonique (téléopérateurs disponibles 24/7), l'enregistrement de l'appel (infrastructure télécom), et le rappel de l'entreprise selon une procédure prédéfinie. Par ailleurs, intrinsèquement, l'appel téléphonique comporte de nombreux inconvénients : d'une part, il nécessite une phase d'établissement (de plusieurs secondes voire dizaines de secondes, pendant lesquelles il n'y a pas d'enregistrement audio de l'émetteur de l'alerte), et l'appel peut ne pas aboutir (d'établissement d'appel). Par ailleurs, une fois connecté, la liaison téléphonique ne permet que de prendre connaissance de ce qu'il se passe au

moment de l'appel (et pas ce qu'il s'est passé au début, au moment du déclenchement), ce qui est peu efficace.

[0014] Il est donc nécessaire de proposer une solution qui permette de résoudre ces inconvénients de l'art antérieur.

[0015] 3. Résumé

[0016] L'invention ne présente pas ces inconvénients de l'art antérieur. L'invention se rapporte à un procédé de traitement de données relatives à un incident, procédé mis en œuvre au sein d'un système comprenant un dispositif d'alerte et un serveur d'incident connectés par l'intermédiaire d'un réseau de communication. Un tel procédé comprend les étapes suivantes, mises en œuvre au sein du dispositif d'alerte, postérieurement à la survenance d'un incident déclencheur d'une alerte :

[0017] - Instanciation d'une donnée représentative d'un déclenchement d'une alerte ;

[0018] - Activation d'un module de captation sonore dudit dispositif d'alerte et enregistrement, au sein d'un espace de stockage dudit dispositif d'alerte, d'un flux sonore issu du module de captation ;

[0019] - Obtention d'une position initiale dudit dispositif d'alerte au sein d'un environnement ;

[0020] et postérieurement à l'activation du module de captation et à l'obtention de la position du dispositif d'alerte :

[0021] - Établissement d'une liaison de communication avec le serveur d'incident, comprenant la transmission, par le dispositif d'alerte, de la donnée représentative du déclenchement d'alerte ;

[0022] et lorsque la liaison de communication est établie :

[0023] - La transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte.

[0024] Selon une caractéristique particulière, le procédé comprend une étape d'obtention d'une donnée représentative de la disponibilité de liaison de communication de sorte à conserver lesdites données audios de l'enregistrement effectué au sien du dispositif d'alerte jusqu'à ce qu'elles soient reçues par ledit serveur d'incident.

[0025] Selon un mode de réalisation particulier, l'étape d'enregistrement, au sein d'un espace de stockage dudit dispositif d'alerte, d'un flux sonore issu du module de captation et l'étape d'obtention de la position initiale dudit dispositif d'alerte au sein d'un environnement sont mises en œuvre parallèlement.

[0026] Selon une caractéristique particulière, l'étape d'établissement de la liaison de communication avec le serveur d'incident comprend :

[0027] - une étape de construction une requête d'incident (rqi) comprenant la donnée représentative du déclenchement d'alerte et au moins une donnée représentative d'une localisation approximative du dispositif d'alerte ;

[0028] - une étape de transmission, au serveur d'incident, de ladite requête d'incident (rqi) ;

[0029] - une étape de réception, en provenance du serveur d'incident, d'une réponse confirmant l'établissement de la liaison de communication0

[0030] Selon un mode de réalisation particulier, la transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte comprend :

[0031] - la préparation de trames de données audios à partir dudit enregistrement audio ;

[0032] - la transmission de trames de données audios au serveur d'incident ;

[0033] - la réception, en provenance du serveur d'incident, d'accusés de réception de trames de données audios.

[0034] Selon une caractéristique particulière, le procédé comprend une étape de suppression d'une trame de donnée courante uniquement postérieurement à la réception d'un accusé de réception pour cette trame de donnée courante.

[0035] Selon un mode de réalisation particulier, le procédé comprend en outre la transmission de messages comprenant des données de déplacement du dispositif d'alerte.

[0036] Selon un autre aspect, l'invention se rapporte également à un dispositif d'alerte pour le traitement de données relatives à un incident, dispositif comprenant des moyens de connexion à un serveur d'incident connectés par l'intermédiaire d'un réseau de communication. Un tel dispositif comprend des moyens de traitement de données d'incident, moyens mis en œuvre postérieurement à la survenance d'un incident déclencheur d'une alerte et comprenant :

[0037] - Instanciation d'une donnée représentative d'un déclenchement d'une alerte ;

[0038] - Activation d'un module de captation sonore dudit dispositif d'alerte et enregistrement, au sein d'un espace de stockage dudit dispositif d'alerte, d'un flux sonore issu du module de captation ;

[0039] - Obtention d'une position initiale dudit dispositif d'alerte au sein d'un environnement ;

[0040] et postérieurement à l'activation du module de captation et à l'obtention de la position du dispositif d'alerte :

[0041] - Établissement d'une liaison de communication avec le serveur d'incident, comprenant la transmission, par le dispositif d'alerte, de la donnée représentative du déclenchement d'alerte ;

[0042] et lorsque la liaison de communication est établie :

[0043] - Une pluralité d'étapes de transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte.

[0044] Dans un mode de réalisation, le dispositif d'alerte prend la forme d'un terminal de

communication muni d'une application dédiée.

[0045] Selon un autre aspect, l'invention se rapporte également à un système de traitement de données relatives à un incident qui comprend un serveur d'incident et au moins un dispositif d'alerte tel que précédemment décrit.

[0046] L'invention vise aussi un support d'informations lisible par un processeur de données, et comportant des instructions d'un programme tel que mentionné ci-dessus.

[0047] Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

[0048] D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

[0049] Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

[0050] Selon un mode de réalisation, l'invention est mise en œuvre au moyen de composants logiciels et/ou matériels. Dans cette optique, le terme "module" peut correspondre dans ce document aussi bien à un composant logiciel, qu'à un composant matériel ou à un ensemble de composants matériels et logiciels.

[0051] Un composant logiciel correspond à un ou plusieurs programmes d'ordinateur, un ou plusieurs sous-programmes d'un programme, ou de manière plus générale à tout élément d'un programme ou d'un logiciel apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Un tel composant logiciel est exécuté par un processeur de données d'une entité physique (terminal, serveur, etc) et est susceptible d'accéder aux ressources matérielles de cette entité physique (mémoires, supports d'enregistrement, bus de communication, cartes électroniques d'entrées/sorties, interfaces utilisateur, etc).

[0052] De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Il peut s'agir d'un composant matériel programmable ou avec processeur intégré pour l'exécution de logiciel, par exemple un circuit intégré, une carte à puce, une carte à mémoire, une carte électronique pour l'exécution d'un micrologiciel (firmware), etc.

[0053] 4. Dessins

[0054] D'autres caractéristiques et avantages apparaîtront plus clairement à la lecture de la

description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

[0055] - [Fig.1] décrit un système dans lequel l'invention est mise en œuvre ;

[0056] - [Fig.2] décrit les étapes de la transmission de données par le dispositif d'alerte ;

[0057] - [Fig.3] décrit succinctement un dispositif d'alerte.

[0058] 5. Description

[0059] 5.1. Rappels du principe

[0060] Comme indiqué précédemment, l'invention permet de résoudre au moins certains des inconvénients de l'art antérieur en proposant une combinaison de deux techniques pour répondre aux problèmes rencontrés, notamment en termes d'accessibilité à une information pertinente en provenance des « lanceurs d'alerte ». Ainsi, on combine d'une part une technique de multiplexage de données et d'autre part une technique de conservation locale de données (au sein du dispositif d'alerte). De manière additionnelle, une technique de diffusion « large » est également mise en œuvre. Plus particulièrement, les problèmes précédemment mentionnés sont résolus d'une part en effectuant un enregistrement multimédia immédiat, au sein du dispositif d'utilisateur, dès la survenue de l'évènement déclencheur d'une alerte et d'autre part en établissant, avec au moins un serveur, une connexion de données. Cette connexion de données est utilisée pour transmettre, dès qu'elles sont disponibles, d'une part les données multimédia enregistrées et d'autre part d'autres données techniques relatives au dispositif d'utilisateur et à son environnement, comme cela est explicité par la suite. Grace à cette combinaison, l'invention permet de résoudre de nombreux problèmes de l'art antérieur relatifs à la gestion des alertes de détresse, en situation d'urgence, tout en limitant les couts de gestion.

[0061] Plus particulièrement, en relation avec la [Fig.1], l'invention se rapporte à un système, comprenant un serveur d'incident (SI), connecté à un réseau de communication (NTWK1, NTWK2). Un tel serveur comprend des moyens d'établissement de communication avec au moins un dispositif d'utilisateur (de type terminal de communication), appelé dispositif d'alerte (DAs). Les dispositifs d'alerte (DAs) et le serveur (SI) entrent en communication par l'intermédiaire d'un ou de plusieurs réseaux de communication (NTWK1, NTWK2), dont celui auquel le serveur d'incident est connecté. Les moyens d'établissement de communication comprennent notamment l'établissement d'une liaison de transmission de données entre le serveur d'incident et le dispositif d'alerte. Cette liaison de transmission est de préférence de type UDP/IP ou TCP/IP et comprend une configuration de transmission de trames d'incidents, selon un protocole de transmission spécifique.

[0062] Le serveur d'incident (SI) comprend une base de données (DB1), de type base de données relationnelle, au sein de laquelle chaque dispositif d'alerte (DAs) est identifié

par l'intermédiaire d'un identifiant unique, permettant notamment de lier ce dispositif d'alerte à au moins une organisation d'appartenance, qui est également identifiée au sein de la base de données. En fonction des modes de réalisation, le serveur peut être un serveur physiquement présent au sein de l'organisation elle-même ou bien être un ensemble de serveurs d'un opérateur d'un gestionnaire externe. Le serveur comprend également des moyens d'enregistrement de données multimédia (DB2), ces moyens permettant de sauvegarder et de traiter des données multimédia qui sont reçues en provenance de dispositifs d'alerte, selon une typologie de trames particulière. Le serveur d'incident comprend également des moyens de communication avec au moins un dispositif de gestion d'incident (DGIs). Un dispositif de gestion d'incident est un dispositif d'utilisateur prenant par exemple la forme d'un terminal de communication et/ou d'un ordinateur portable. Il s'agit d'un dispositif en possession d'un responsable désigné de l'organisation, en charge par exemple d'effectuer (au moins partiellement) la réception et le traitement des alertes (de faire la levée de doute (fausse alerte, déclenchement par erreur) et de qualifier l'événement (quelle est la situation)) et éventuellement de gérer une crise associée à une ou plusieurs alertes. Le dispositif de gestion d'incident comprend par exemple des moyens de mise en œuvre et de suivi d'un plan de gestion de crise préalablement codifié.

[0063] Le dispositif d'alerte quant à lui comprend au moins des moyens de communication avec un ou plusieurs réseaux de communications, selon une ou plusieurs technologies de communication. Il comprend également au moins un module de captation sonore (microphone) et au moins un module de localisation. Les différentes fonctions du dispositif d'alerte sont pilotées par un microprocesseur et le dispositif d'alerte comprend une mémoire tampon, en charge notamment de l'enregistrement de l'environnement sonore capté par le module de captation sonore. Le dispositif d'alerte comprend optionnellement un ou plusieurs modules de captation visuels (modules photos/videos) permettant l'enregistrement de l'environnement visuel. Le dispositif d'alerte peut également comprendre un module d'analyse, comprenant notamment des moyens de traitement des données multimédia (et plus particulièrement sonores) captées et enregistrées en mémoire tampon. Optionnellement, il peut intégrer un accéléromètre et un gyroscope, pour mesurer les mouvements, lesquels sont également une source d'information importante pendant une alerte (chute, immobilité, courir, marcher …) Il peut également intégrer les données venant d'accessoires, par exemple d'un capteur cardiaque ou d'une montre connectée.

[0064] Lors de la survenance d'un incident, le procédé suivant est mis en œuvre au sein du système préalablement présenté. Ce procédé comprend :

[0065] 1. Une émission d'une alerte par le dispositif d'alerte, comprenant les étapes ordonnées suivantes :

[0066] i Un déclenchement de l'alerte (volontaire ou automatique) : l'alerte est déclenchée par le dispositif d'alerte lors de la survenance de l'incident.

[0067] ii Le déclenchement de l'alerte implique une activation de l'enregistrement audio (écoute d'ambiance) à l'aide du module de captation sonore et l'obtention d'une position du dispositif d'alerte (la position peut être une position absolue, obtenue par GPS ou une position relative (par exemple obtenue par triangulation Wi-Fi ou Bluetooth au sein d'un bâtiment). Les trames (audio et position) sont enregistrées en continu au sein de la mémoire tampon du dispositif d'alerte. Les trames sont conservées en mémoire tampon au moins tant qu'un acquittement de réception de ces trames n'est pas parvenu au dispositif d'alerte (voir par la suite) ;

[0068] iii Un établissement d'une liaison de communication (sécurisée) avec le serveur d'incident, comprenant la transmission, par le dispositif d'alerte, de son identifiant ;

[0069] iv Une émission d'un message d'alerte vers le serveur d'incident, au travers de la liaison de communication ; cette émission comprend, si cela est possible (les paramètres de la liaison de communication le permettent), l'émission les trames enregistrées en mémoire tampon. La disponibilité de la liaison de communication pour transmission des trames est monitorée en permanence : s'il advient que le statut de disponibilité de la liaison est modifié, le dispositif d'alerte adapte sa politique de transmission des trames en fonction de la disponibilité de la liaison.

[0070] v De manière complémentaire, en fonction des modes de réalisation, le dispositif d'incident transmet, sous la forme de trames spécifiques, des données complémentaires du dispositif d'alerte, telle que des données de déplacement et/ou d'orientation (vitesse, accélération, orientation, etc.), des données de connectivités (force du signal, SSID, BSSID, etc.), des données physiologiques de l'utilisateur, ...

[0071] 2. Traitement de l'alerte par le serveur d'incident et mise en œuvre du routage en fonction de paramètres de routage :

[0072] i Le serveur reçoit le message d'alerte. En fonction des paramètres de routage (notamment de règles de sécurité définie par l'administrateur de l'organisation), le serveur d'incident identifie au moins un dispositif de gestion d'incident et transmet un message d'alerte au dispositif de gestion d'incident. Ce message d'alerte comprend au moins un identifiant du dispositif d'alerte ayant déclenché l'alerte ;

[0073] ii Le serveur reçoit et enregistre les trames (audio et GPS) de l'alerte en provenance du dispositif d'alerte et accuse réception (acquitte) des données reçues au dispositif d'alerte ;

[0074] iii Optionnellement, le serveur d'incident effectue un ou plusieurs traitements sur les données reçues, notamment des traitements de reconnaissance et de discrimination ;

[0075] iv Le serveur notifie au dispositif de gestion d'incident (au moins un) de l'alerte en cours et transmet les données à sa disposition (au fur et à mesure de leur réception,

après requête reçue du dispositif de gestion d'incident et leur traitement éventuel) ;

[0076] 3. Réception de l'alerte par le dispositif de gestion d'incident :

[0077] i Le dispositif de gestion d'incident reçoit l'alerte, notifie celle-ci à l'utilisateur (par l'intermédiaire d'un signal sonore et/ou visuel et/ou vibratoire) et requiert l'obtention des données multimédia auprès du serveur d'incident ;

[0078] ii Le dispositif de gestion d'incident reçoit les données multimédia en provenance du serveur d'incident ;

[0079] iii L'utilisateur est prévenu, il se rend sur l'application pour traiter et écouter l'alerte. Les premiers instants de l'alerte (audio et GPS) sont disponibles dès réception de l'alerte.

[0080] 4. Gestion de l'alerte / Transmission temps réel :

[0081] i Côté dispositif d'alerte, les données sont enregistrées et transmises en temps réel, à destination du serveur d'incident, tant que l'incident n'est pas clos ou tant qu'une commande d'interruption de transmission n'est pas reçue par le dispositif d'alerte.

[0082] ii Les données sont reçues par le serveur d'incident et distribuées vers les dispositifs de gestion d'incidents en flux constant.

[0083] Les avantages de cette manière de procéder sont nombreux :

[0084] - Routage multi utilisateurs : L'incident peut être routée vers plusieurs interlocuteurs simultanément, ce qui ne peut être fait de façon simple avec un appel téléphonique. Ainsi il reste possible de continuer à traiter l'incident par un centre de téléassistance, mais il peut également être traité par des personnels de terrain, plus à proximité du dispositif d'alerte de l'incident, pour une organisation locale, plus efficace et plus rapide, de la réponse à apporter à l'incident ;

[0085] - Routage multi critères : Le routage n'est pas figé comme l'est un appel téléphonique (pas de souplesse de destination). Des règles spécifiques peuvent être utilisées pour router les incidents vers des personnels appropriés, en accord avec les règles de sécurité définies par l'organisation ;

[0086] - Réactivité sur le poste récepteur : l'incident est reçu sur le dispositif de gestion d'incident. Les trames de données sont automatiquement reçues et enregistrées en local, sans aucune action de la part d'un utilisateur. Ainsi, lorsque l'utilisateur réagit et ouvre l'application pour visualiser l'incident, les premiers instants ont déjà été téléchargés et sont disponibles pour écoute sans latence.

[0087] 5.2. Description d'un mode de réalisation

[0088] On présente, en relation avec la [Fig.2], un mode de réalisation du système précédemment présenté, dans lequel seul un flux audio est transmis par les dispositifs d'alerte suite à la déclaration d'un incident.

[0089] 5.2.1. Dispositif d'alerte

[0090] Le dispositif d'alerte est en charge de transmettre, en temps réel, des données à des-

tination du serveur d'incident.

[0091] Un incident (Inc) est détecté (201) au niveau du dispositif d'alerte (DA) : il peut s'agir d'une détection automatique (chute, bruit inhabituellement élevé, au-delà d'un seuil sonore paramétré) ou d'une saisie manuelle d'un incident (appui sur une touche physique d'alerte sur le dispositif d'alerte ou appui sur une touche d'une IHM en cas d'affichage sur le dispositif d'alerte). L'incident peut être qualifié (p.ex. incendie, fuite, intrusion, attaque, etc.) ou bien non qualifié. En cas d'absence de qualification, celle-ci reviendra au serveur d'incident ou au dispositif de gestion d'incident.

[0092] Le dispositif d'alerte (DA) met en œuvre, parallèlement, deux actions :

[0093] - Il obtient (202) sa position (loc) ; pour ce faire, soit il obtient sa position à partir d'un module de localisation GPS, lorsque cela est possible, soit il obtient sa position l'utilisation d'un réseau de communication (Wi-Fi, Bluetooth) ; la position (loc) peut avoir été déterminée avant la survenue de l'incident, de manière périodique, afin de pouvoir être obtenue immédiatement lors de la détection de l'incident ; la position obtenue est datée et enregistrée en base (203)

[0094] - Il active (204) le module d'enregistrement sonore (snd) et enregistre (205) les sons perçus au sein d'une mémoire tampon d'enregistrement sonore, tout en datant ces enregistrements (heure et date de début) ;

[0095] Le dispositif d'alerte met en œuvre l'enregistrement des sons perçus et des positions de manière continue (206), sans interruption, tant que l'incident n'est pas clôturé ou qu'une commande d'interruption n'est pas reçue en provenance du serveur d'incident (SI). La périodicité d'obtention des positions est fonction des mouvements constatés par le dispositif d'alerte : en cas d'absence de mouvement, la position n'est pas nécessairement modifiée et/ou transmise, et ce afin de limiter les traitements mis en œuvre par le dispositif d'alerte et de ne pas impacter outre mesure la charge de la batterie (l'obtention de la position étant une opération gourmande de ce point de vue).

[0096] Le dispositif d'alerte (DA) transmet (207) au serveur d'incident (SI) une requête d'incident (rqi). Cette requête d'incident comprend à minima un identifiant du dispositif d'alerte et/ou un Identifiant unique de contexte d'alerte dont la valeur dépend de l'identifiant du dispositif d'alerte ; cette requête peut comprendre également, lorsqu'elle est disponible, une position (même approximative) du dispositif d'alerte et/ou une qualification de l'incident (voir plus haut).

[0097] Le dispositif d'alerte réceptionne (208), en provenance du serveur d'incident, une réponse (acki) à la requête d'incident, permettant au dispositif d'alerte de préparer les trames qui vont être transmises au serveur d'incident. La réponse peut comprendre également des paramètres d'établissement d'une session de transmission de données à destination du serveur d'incident, si nécessaire (i.e. paramètres de transmission de données par l'intermédiaire d'un protocole de transmission dédié).

[0098] A la suite de la préparation de la session de transmission de données à destination du serveur d'incident, le dispositif d'alerte prépare (209) les trames (frms) à destination du serveur d'incident et transmet (210) ces trames à destination du serveur d'incident. En fonction des modes de réalisation, serveur d'incident accuse réception de ces trames (211), soit de manière unitaire soit par lot. Préférentiellement, le protocole UDP est utilisé pour le transport des trames du dispositif d'alerte vers le serveur d'incident. Le serveur d'incident réceptionne les trames UDP et transmet lui-même, au dispositif d'alerte, à intervalle régulier, des trames UDP dont le contenu comprend des accusés de réception pour un lot de trames précédemment reçues. Cette manière de procéder permet de tirer avantage du protocole UDP tout en permettant au dispositif d'alerte de supprimer les trames qui ont été correctement reçues par le serveur d'incident, et ainsi de libérer une partie de sa mémoire tampon.

[0099] A réception (220) d'une commande de fin d'incident (cmdi) ou d'interruption de transmission, le dispositif d'alerte cesse la transmission des données au serveur d'incident et acquitte (221) la prise en compte de cette commande (acke).

[0100] 5.2.2. Serveur d'incident

[0101] Le serveur d'incident est en charge de la réception des données en provenance d'un dispositif d'alerte, puis de traiter ces données en fonction de l'incident remonté et de transmettre des données traitées au dispositif de gestion d'incidents. Plus particulièrement, le serveur d'incident (SI) :

[0102] - Réceptionne (207), en provenance d'un dispositif d'alerte (DA), un une requête d'incident (rqi) ;

[0103] - Accuse réception (208), de cette requête (acki) auprès du dispositif d'alerte (DA) ;

[0104] - Recherche (212), au sein d'une base de données, d'au moins un dispositif de gestion d'incident (DGI) auquel l'alerte reçue doit être transmise ;

[0105] - Transmet (213), aux dispositifs de gestion identifiés (DGI), une requête d'alerte (rqid) ;

[0106] - Reçoit (214), en provenance du dispositif de gestion identifié (DGI), un accusé de réception (ackid) de la requête d'alerte : cette réception déclenche la prise en compte de l'alerte par un gestionnaire : tant qu'une requête d'acquittement n'est pas reçu, le dispositif de gestion d'incident auquel la requête est transmise n'est pas considéré comme ayant été valablement informé de l'incident.

[0107] En parallèle, le serveur d'incident reçoit (210) les trames en provenance du dispositif d'alerte et acquitte (211) réception de ces trames (individuellement ou par lots en fonction du mode de réalisation). Optionnellement, il réalise (215) un ou plusieurs traitements de ces trames, notamment pour détecter, dans les trames sonores, des évènements particuliers (bruits anormaux ou au contraire absence de bruit). Pour ce faire, il met en œuvre un module de détection paramétré de manière adéquate afin de

fournir des trames complémentaires (horodatées) qui marquent, dans le flux sonore de base, les évènements particuliers de ce flux éventuellement détectés. Ces trames complémentaires peuvent être transmises, au dispositif de gestion d'incident, avec les trames reçues en provenance du dispositif d'alerte ou bien être transmises à part, au fur et à mesure de l'analyse qui est faite des trames reçues. Ainsi cette analyse complémentaire permet de fournir des informations additionnelles au dispositif de gestion d'incident, afin que l'utilisateur de celui-ci soit le plus à même de réagir de manière appropriée.

[0108] En parallèle, le serveur d'incident transmet (216) les trames du dispositif d'alerte au dispositif de gestion d'incident (DGI) et reçoit optionnellement des acquittements (217) de ces trames. Les trames transmises (216) peuvent être identiques à celle reçues (210) ou peuvent comprendre des données complémentaires.

[0109] Comme indiqué précédemment, la transmission peut être effectuée vers plusieurs dispositifs de gestion d'incident, lorsque plusieurs « gestionnaires de crise » sont identifiés, pour répondre à l'incident remontés par le dispositif d'alerte. Les dispositifs de gestions d'incident d'une organisation peuvent être destinataires, indistinctement, de toutes les remontées d'incidents ou alors ils peuvent être sélectionnés, par le serveur d'incident, en fonction de la qualification de l'incident telle que remontée par dispositif d'alerte, par le serveur d'incident ou par un gestionnaire de crise de l'organisation. Auquel cas, une première phase consiste à diffuser l'alerte de manière générale, jusqu'à l'obtention d'une qualification adéquate, puis ensuite à restreindre la transmission de données aux seuls dispositifs de gestion d'incidents concernés.

[0110] De manière similaire, le serveur d'incident peut recevoir des données de la part de plusieurs dispositifs d'alerte, de manière concomitante, et ce pour un même incident ou pour des incidents différents au sein d'une même organisation. Auquel cas, le serveur d'incident est en mesure de tenter de grouper des incidents déclarés isolément (i.e. par plusieurs dispositifs d'alerte séparés), afin de constituer un seul incident, rapporté par plusieurs dispositifs d'alerte. Dans une telle situation, le serveur d'incident compare les positions transmises par les dispositifs d'alerte d'une même organisation. Lorsque les positions des différents dispositifs d'alerte « déclarants » sont corrélées (par exemple parce qu'elles se trouvent dans un périmètre donné, comme les locaux d'une organisation), alors un premier critère de regroupement est positionné. En second lieu, lorsque la qualification des incidents est identique, un second critère de regroupement est positionné. En troisième lieu, lorsqu'une analyse (215) des trames, reçues en provenance des différents dispositifs d'alerte, entraine l'extraction d'évènements sonores identiques (bruits de fond ayant une ressemblance au-delà d'un seuil de ressemblance prédéterminé et horodatage des trames identique ou proche), un troisième critère de regroupement est positionné.

[0111] En fonction de modes de réalisation, un ou plusieurs critères de regroupement peuvent être sont suffisant pour regrouper les incidents en un seul et même incident. Le dispositif de gestion d'incident est alors notifié, par la transmission d'un message de regroupement adapté.

[0112] 5.2.3. Dispositif de gestion d'incidents

[0113] Le dispositif de gestion d'incidents est en charge de gérer les incidents remontés par le serveur d'incident. Dans le cadre de la survenue d'un incident, il met en œuvre la méthode suivante :

[0114] - Réceptionne (213) une requête d'alerte (rqid) en provenance du serveur d'incident ;

[0115] - Transmet (214), au serveur d'incident, un accusé de réception (ackid) de la requête d'alerte : cette réception déclenche la prise en compte de l'alerte par le gestionnaire.

[0116] - Réceptionne (216) les trames (frms) de flux en provenance du serveur d'incident ;

[0117] - Transmet (217) optionnellement, au serveur d'incident, un accusé de réception (ackf) de ces trames au serveur d'incident ;

[0118] - Traite (218) les données d'incident reçues ;

[0119] - Transmet (219), au serveur d'incident, des commandes (cmdx) que le serveur répercute, si besoin, aux dispositifs d'alerte.

[0120] En fonction des modes de réalisation, les traitements (218) mis en œuvre par le dispositif de gestion d'incident comprennent :

[0121] - Obtention d'un plan de gestion de crise, sous la forme d'une structure de données comprenant un arbre de décision ;

[0122] - Affichage, sur l'écran du dispositif de gestion d'incident, d'une donnée représentative de l'arbre de décision en fonction de la qualification affecté audit incident ;

[0123] - Lorsqu'une action est mise en œuvre, au sein de l'arbre de décision, par l'utilisateur du dispositif de gestion d'incidents, transmission (219), au serveur d'incident, d'une donnée représentative de l'action menée et/ou d'une commande (cmdx).

[0124] Une telle transmission entraine, au niveau du serveur, une mise à jour d'un statut associé à l'incident et, optionnellement, si l'action en question le requiert, la transmission d'une commande à destination d'une part du ou des dispositifs d'alerte impactés et d'autre part d'un ou plusieurs autres dispositifs de gestion d'alerte.

[0125] Les traitements mis en œuvre au sein du dispositif de gestion d'incident comprennent également la mise en œuvre d'une interface « d'écoute » du/des flux audio en provenance du ou des terminaux d'alerte. Une interface spécifique est dédiée à l'écoute et permet, à l'utilisateur en charge de la gestion de l'incident, de balayer le flux audio :

[0126] - L'interface autorise l'écoute du flux audio depuis l'origine (i.e. depuis la survenance de l'incident), et non pas, comme dans l'art antérieur, depuis la « prise de l'appel ». Le gestionnaire d'incident est donc en mesure de retracer le déroulé de l'incident depuis le commencement. Il n'y a donc pas de perte d'information, comme

dans les solutions de l'art antérieur.

[0127] - Le flux audio est disponible même en l'absence de prise de parole de la part de l'utilisateur du dispositif d'alerte.

[0128] - Les trames d'évènements sonores (traitées par le serveur d'incident, en 215), transmises par le serveur d'incident, permettent d'identifier, dans l'affichage réalisé, les points d'intérêt du flux audio, et permettent, le cas échéant au gestionnaire de crise de qualifier l'incident et/ou de sélectionner, au sein de l'arbre de décision, une ou plusieurs actions à mener.

[0129] 5.3. Autres caractéristiques et avantages

[0130] 5.3.1. Règles de routage de l'incident

[0131] Le serveur d'incident route les incidents vers des groupes d'utilisateurs distincts en fonction des critères suivants (non limité à ces critères) :

[0132] - Groupe d'appartenance du dispositif d'alerte.

[0133] - Zone géographique : Le groupe de destination est fonction de la zone géographique dans laquelle se trouve le dispositif d'alerte de l'incident.

[0134] - Calendrier horaire : deux groupes de récepteurs distincts reçoivent les incidents de jour (HO, Heures Ouvrées) et de nuit (Heures Non Ouvrées)

[0135] - Non réponse : En cas de non réception ou non réponse de l'incident par le groupe de destination, l'incident est routé au bout d'un temps prédéterminé (par exemple une minute), vers un groupe de secours (backup).

[0136] Ainsi, le serveur d'incident offre la possibilité de déterminer de manière simple les dispositifs de gestion d'incidents les plus à même de répondre à un incident donné.

[0137] 5.3.2. Enregistrement et cache

[0138] Pour assurer qu'aucune perte d'information ne survienne, principalement au niveau de la réception des trames du flux audio, un mécanisme de sauvegarde est mis en œuvre. Ainsi, pour pallier le risque de perte de connexion réseau (ou chute de la bande passante disponible), toutes les trames sont numérotées, et enregistrées (cache) à trois niveaux différents :

[0139] - sur le dispositif d'alerte : les trames sont créées en avance de phase, par un processus s'exécutant en parallèle des autres tâches, dès la survenue de l'incident. Dès qu'une connexion est disponible, les trames préparées à l'avance sont transmises selon l'ordonnancement préétabli ;

[0140] - sur le serveur, les trames sont enregistrées et sauvegardées telles quelles, dès leur arrivée et ordonnées selon l'ordre attribué par le dispositif d'alerte ;

[0141] - le dispositif de gestion d'incident, les trames sont également enregistrées et sauvegardées telle qu'elle, dès leur arrivée et ordonnées selon l'ordre attribué par le dispositif d'alerte.

[0142] Ainsi, même en cas de coupure réseau, cette manière de faire permet d'une part au

serveur de transmettre les trames qu'il a reçu, même si le dispositif d'alerte est coupé. Il en est de même pour le dispositif d'incident, qui peut continuer à se déplacer au travers des trames qu'il a reçu, même s'il est temporairement déconnecté du serveur d'incident.

[0143] 5.3.3. Fiabilité de la transmission

[0144] - En cas de défaillance partielle du réseau de transmission (réseau mobile 3G/4G ou WiFi), tant du côté du dispositif d'alerte que du (des) récepteur(s) (les dispositifs de gestion d'incident), les trames de données sont numérotées et enregistrées. Le protocole de transmission est en mesure d'effectuer une reprise et de transmettre à nouveau les trames perdues/non reçues une fois la connexion rétablie.

[0145] - Dans les cas les plus défavorables, lorsqu'il n'y a aucun accès au réseau pendant toute la durée de l'incident : les données de l'incident sont enregistrées sur le dispositif d'alerte. Le protocole les transmet au serveur d'incident lorsque le dispositif d'alerte obtient un accès au réseau. Bien qu'il n'aura pas été forcément possible de porter assistance au moment de l'incident, la récupération de ces données à posteriori est tout de même possible (à des fin d'enquête notamment).

[0146] - Multiplier les canaux de transmission : afin de sécuriser la remontée de l'incident, en cas de défaillance du réseau de transmission de données, un mode dégradé est mis en place, s'appuyant sur la transmission d'informations par SMS (lorsque le réseau GSM reste disponible) ou autre technique de transmission de messages adaptée (bluetooth, LORA, Zigbee). L'incident reçu par SMS, par le serveur d'incident, est traité et routé de la même façon que dans le cas nominal (en respectant les règles de sécurité configurées). De même, pour les utilisateurs des dispositifs de gestion d'incident, il n'y a pas de différence d'expérience utilisateur (sauf pour la réception du flux audio). Pour les utilisateurs des dispositifs de gestion d'incident, le traitement de l'incident reste identique et n'entraine pas de différence en termes d'expérience utilisateur.

[0147] - Transmission double flux : à la réception d'un incident, pour qualifier au mieux la situation et faire la levée de doute, il est capital de pouvoir naviguer entre l'écoute du début de l'incident (les premières secondes apportant beaucoup d'information sur la situation du dispositif d'alerte) et l'écoute du direct (le « Live ») qui permet de comprendre comment la situation évolue. Pour garantir cela, Les données transmises vers un utilisateurs des dispositifs de gestion d'incident contiennent à la fois les trames de début de l'incident et les trames de fin (le direct), ce qui en fait un protocole de transmission double flux (deux flux de données simultanés). Le double flux est adapté en fonction de la bande passante disponible au niveau du dispositif d'alerte. Avec une priorité pour le flux « Live » quand la bande passante disponible est limitée.

[0148] 5.3.4. Écoute d'ambiance et géolocalisation

[0149] L'incident, une fois déclenché, permet au personnel de l'équipe de sécurité/gestion de crise (chargé de recevoir et traiter les incidents), de localiser la personne disposant du dispositif d'alerte et d'écouter son environnement sonore, afin d'effectuer une levée de doute, qualifier l'urgence de la situation, et définir la meilleure réponse à apporter, en fonction de plan de gestion de crise.

[0150] Une fois l'incident déclenché, le dispositif d'alerte transmet en temps réel les données qui permettent à l'équipe de gestion de crise de comprendre la situation dans laquelle se trouve le dispositif d'alerte (et son porteur) : géolocalisation et enregistrement audio peuvent être joués depuis le début de l'incident, ou à n'importe quel moment, jusqu'au « direct » qui permet d'écouter l'environnement sonore de l'utilisateur en direct. Ainsi, il est possible de qualifier à distance, la gravité de la situation. Par exemple, en cas de prise d'otage, l'enregistrement audio permet aux forces de l'ordre de suivre en temps réel et de l'intérieur, l'évolution de la situation. Les enregistrements audio peuvent être rejoués à posteriori, et exportés, en cas de suite judiciaire ou pour formation à la gestion de crise et conflits. Ainsi, le protocole de transmission de données proposé offre plus d'efficacité et de souplesse que les solutions s'appuyant sur un appel téléphonique. Ce protocole comprend notamment une définition de trames de transmission de données à destination du serveur d'incident, lesquelles sont acquittées, afin de permettre au dispositif d'alerte de maintenir en continu un registre des données effectivement réceptionnées par le serveur d'incident avant de les effacer.

[0151] Le premier message transmis par le dispositif d'alerte est un message de type « MSG_SOS_START_REQ » qui comprend un identifiant unique de contexte d'alerte, généré par le dispositif d'alerte lui-même et qui est utilisé comme pivot des communications suivantes entre le serveur d'incidents et le dispositif d'alerte. Le message comprend également des données initiales telles que l'heure et la date de déclenchement, identifiant de la localisation, un identifiant de règle d'alerte, une donnée représentative d'un mode de déclenchement et une localisation initiale. Ce premier message permet au serveur d'incident d'initialiser un contexte d'incident et re répondre au dispositif d'alerte en accusant réception de ce message.

[0152] A la suite de la réception de ce message, le dispositif d'alerte transmet au serveur les trames contenant les données représentatives de l'alerte sous la forme de messages de type « MSG_SOS_FRAME_REQ » qui comprennent les données de l'alerte, envoyée par l'émetteur de l'alerte vers le serveur. Plusieurs types de données peuvent être contenus : Localisation GPS, audio, vidéo, Début, Fin, Interruption, qualification, présence (récepteurs), rapport périodique, action. Chacune des trames comprend un identifiant unique permettant au serveur d'organiser la réception de celles-ci et de les ordonnancer. A titre d'acquittement, le serveur d'incident émet un message de type «

MSG_SOS_FRAME_RESP » comprenant d'une part un identifiant de la Dernière trame reçue côté serveur et d'autre part un identifiant (calculé par le serveur) de la première trame manquante côté serveur (demande de reprise).

[0153] D'autres type de messages sont également échangés entre le dispositif d'alerte et le serveur d'incident comme par exemple des messages de terminaison, qui sont soit transmis à l'initiative du dispositif d'alerte soit à l'initiative du serveur d'incident et qui permettent de terminer une alerte (par exemple an cas de faux positifs, ou bien d'une fin de l'incident).

[0154] 5.3.5. Contenu des trames de transport de données captées lors de l'incident

[0155] Les trames de données transportées par le protocole d'incident sont typées, afin de pouvoir traiter différents types d'informations :

[0156] - audio (enregistrement de l'environnement sonore),

[0157] - localisation (du dispositif d'alerte),

[0158] Les trames peuvent aussi porter des données connexes, comprenant :

[0159] - mouvements et la position de l'utilisateur (immobilité, chute, marche, course, ...) ;

[0160] - événements sonores singuliers (cri, bris de glace, coup de feu) ;

[0161] - données issues de capteurs physiologiques (rythme cardiaque).

[0162] 5.3.6. Contenu des trames de transport de données liées à l'incident

[0163] Le protocole comprend également des trames typées qui permettent de réaliser le transport de données relatives à la prise en charge de l'incident :

[0164] - Qualification : Les utilisateurs impliqués dans l'incident (le dispositif d'alerte et les dispositifs de gestion d'incidents) peuvent qualifier la nature de l'événement. Cette information est transmise en temps réel vers l'ensemble des autres utilisateurs, par l'intermédiaire d'une trame de type « qualification » ;

[0165] - Prise en charge : La liste des utilisateurs en écoute sur l'incident est partagée. Ainsi, un dispositif de gestion d'incident, même sans prendre l'incident en charge, peux savoir combien de récepteurs sont (ou ont été) en écoute de l'incident. De son côté, le dispositif d'alerte a la possibilité de savoir si son incident a été prise en charge. Ces informations sont transmises par l'intermédiaire d'une trame de type « prise en charge » ;

[0166] - Messages texte : il est possible de transmettre des messages texte vers le dispositif d'alerte de l'incident ou même entre récepteurs, grâce à une ou plusieurs trames de type « message texte » ;

[0167] - Messages vocaux : il est possible de transmettre des messages vocaux vers le dispositif d'alerte de l'incident ou entre dispositifs de gestion d'incidents, grâce à une ou plusieurs trames « message vocal ».

[0168] 5.3.7. Enregistrement audio

[0169] L'enregistrement audio est une composante importante du système. En effet, en effectuant un enregistrement audio dès le déclenchement de l'alerte, on permet à

l'opérateur de disposer d'informations cruciales sur la situation rencontrée par le déclencheur de l'alerte. Or, l'obtention de ces informations peut ne pas résulter en un simple enregistrement audio à partir du dispositif d'utilisateur. En effet, lorsque le dispositif d'utilisateur est un smartphone, les composants de captation sonore mis en œuvre ont pour effet de réduire voire totalement annuler l'ambiance sonore pour ne laisser passer que la voix. Un appel téléphonique est en effet principalement dédié aux échanges vocaux. Le codec et le niveau de compression correspondant sont donc sélectionnés pour favoriser la voix humaine à proximité du micro. Ce qui n'offre pas une bonne qualité pour l'enregistrement de l'environnement sonore contenant des bruits qui ne sont pas dans le spectre de la voix humaine et à une certaine distance du micro. Au contraire, dans le cadre de l'invention, on cherche justement à capter l'ambiance sonore et non pas (uniquement) la voix. Ainsi, selon l'invention, on effectue un enregistrement audio de meilleure qualité, et n'applique pas de filtre favorisant la voix. L'écoute d'ambiance est meilleure, ce qui permet de mieux comprendre l'environnement dans lequel se trouve le déclencheur de l'alerte.

[0170] 5.3.8. Dispositif d'alerte

[0171] La [Fig.3] illustre schématiquement un dispositif d'alerte selon la présente technique.

[0172] On présente, en relation avec la [Fig.3], une architecture simplifiée d'un dispositif de d'alerte à mettre en œuvre la méthode de traitement de données d'incidents telle que présentée précédemment. Un tel dispositif d'alerte comprend une mémoire 31, une unité de traitement 32 équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 33, mettant en œuvre le procédé selon l'invention. Dans au moins un mode de réalisation, l'invention est mise en œuvre sous la forme d'une application installée sur un dispositif de communication en possession de l'utilisateur et/ou par l'intermédiaire d'un dispositif dédié uniquement à la gestion d'alerte, telle qu'une montre ou un pendentif. Un tel dispositif d'alerte comprend :

[0173] - Des moyens d'instanciation d'une donnée représentative d'un déclenchement d'une alerte ;

[0174] - Des moyens d'activation d'un module de captation sonore dudit dispositif d'alerte et des moyens d'enregistrement, au sein d'un espace de stockage dudit dispositif d'alerte, d'un flux sonore issu du module de captation ;

[0175] - Des moyens d'obtention d'une position initiale dudit dispositif d'alerte au sein d'un environnement ;

[0176] - Des moyens d'établissement d'une liaison de communication avec le serveur d'incident, comprenant la transmission, par le dispositif d'alerte, de la donnée représentative du déclenchement d'alerte ;

[0177] - Des moyens de transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte.

[0178] Ces moyens se présentent sous la forme d'une application logicielle spécifique, ou encore sous la forme de composants matériels dédiés construits en vue de la réalisation de ces fonctions, tel qu'un élément de sécurisation (SE) ou un environnement d'exécution sécurisé. L'élément de sécurisation peut se présenter sous la forme d'une carte Sim, USim, UICC, ou encore un composant de sécurité spécifique, greffé sur la carte mère du dispositif de contrôle. Plus particulièrement, dans au moins un mode de réalisation, ces moyens se présentent sous la forme de plusieurs composants matériels auxquels sont adjoint plusieurs composants logiciels coopérant ensemble pour mettre en œuvre le procédé de traitement de données précédemment présenté.

Revendications

[Revendication 1] Procédé de traitement de données relatives à un incident, procédé mis en œuvre au sein d'un système comprenant un dispositif d'alerte et un serveur d'incident connectés par l'intermédiaire d'un réseau de communication, procédé caractérisé en ce qu'il comprend les étapes suivantes, mises en œuvre au sein du dispositif d'alerte, postérieurement à la survenance d'un incident déclencheur d'une alerte :

- Instanciation d'une donnée représentative d'un déclenchement d'une alerte ;
- Activation d'un module de captation sonore dudit dispositif d'alerte et enregistrement, au sein d'un espace de stockage dudit dispositif d'alerte, d'un flux sonore issu du module de captation ;
- Obtention d'une position initiale dudit dispositif d'alerte au sein d'un environnement ;

et postérieurement à l'activation du module de captation et à l'obtention de la position du dispositif d'alerte :

- Établissement d'une liaison de communication avec le serveur d'incident, comprenant la transmission, par le dispositif d'alerte, de la donnée représentative du déclenchement d'alerte ;

et lorsque la liaison de communication est établie :

- La transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte ;

la transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte comprenant :

- la préparation de trames de données audios à partir dudit enregistrement audio ;
- la transmission de trames de données audios au serveur d'incident ;
- la réception, en provenance du serveur d'incident, d'accusés de réception de trames de données audios.

[Revendication 2] Procédé de traitement de données selon la revendication 1, caractérisé en ce qu'il comprend une étape d'obtention d'une donnée représentative de la disponibilité de liaison de communication de sorte à conserver lesdites données audios de l'enregistrement effectué au sien du dispositif d'alerte jusqu'à ce qu'elles soient reçues par ledit serveur d'incident.

[Revendication 3] Procédé de traitement de données selon la revendication 1, caractérisé en ce que l'étape d'enregistrement, au sein d'un espace de stockage dudit dispositif d'alerte, d'un flux sonore issu du module de captation et l'étape d'obtention de la position initiale dudit dispositif d'alerte au sein d'un environnement sont mises en œuvre parallèlement.

[Revendication 4] Procédé de traitement de données selon la revendication 1, caractérisé en ce que l'étape d'établissement de la liaison de communication avec le serveur d'incident comprend :
- une étape de construction une requête d'incident (rqi) comprenant la donnée représentative du déclenchement d'alerte et au moins une donnée représentative d'une localisation approximative du dispositif d'alerte ;
- une étape de transmission, au serveur d'incident, de ladite requête d'incident (rqi) ;
- une étape de réception, en provenance du serveur d'incident, d'une réponse confirmant l'établissement de la liaison de communication0

[Revendication 5] Procédé de traitement de données selon la revendication 1, caractérisé en ce qu'il comprend une étape de suppression d'une trame de donnée courante uniquement postérieurement à la réception d'un accusé de réception pour cette trame de donnée courante.

[Revendication 6] Procédé de traitement de données selon la revendication 1, caractérisé en ce qu'il comprend en outre la transmission de messages comprenant des données de déplacement du dispositif d'alerte.

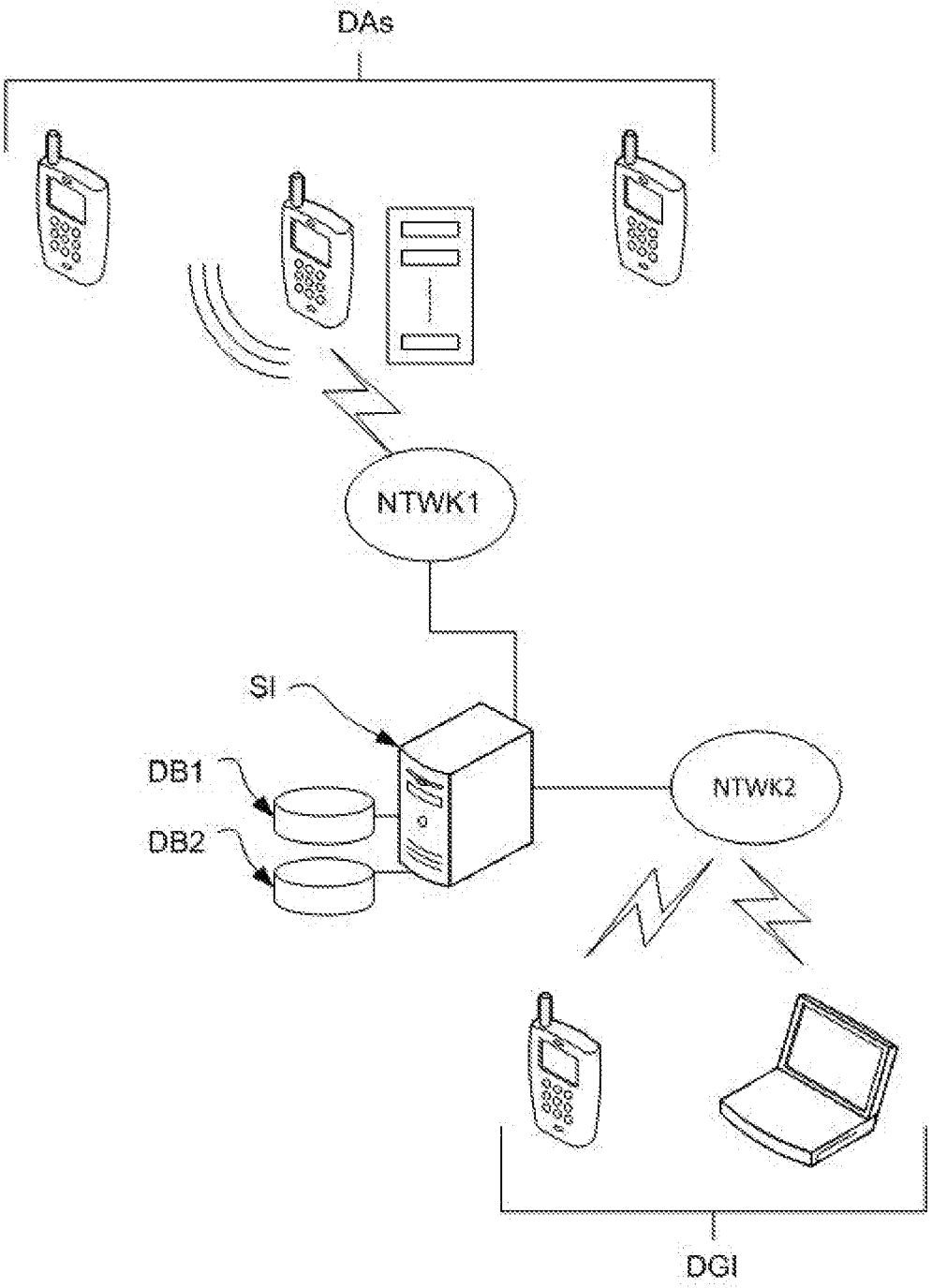
[Revendication 7] Dispositif d'alerte pour le traitement de données relatives à un incident, dispositif comprenant des moyens de connexion à un serveur d'incident connectés par l'intermédiaire d'un réseau de communication, dispositif caractérisé en ce qu'il comprend des moyens de traitement de données d'incident, moyens mis en œuvre postérieurement à la survenance d'un incident déclencheur d'une alerte et comprenant :
- Instanciation d'une donnée représentative d'un déclenchement d'une alerte ;
- Activation d'un module de captation sonore dudit dispositif d'alerte et enregistrement, au sein d'un espace de stockage dudit dispositif d'alerte, d'un flux sonore issu du module de captation ;
- Obtention d'une position initiale dudit dispositif d'alerte au sein d'un environnement ;
et postérieurement à l'activation du module de captation et à l'obtention de la position du dispositif d'alerte :

- Établissement d'une liaison de communication avec le serveur d'incident, comprenant la transmission, par le dispositif d'alerte, de la donnée représentative du déclenchement d'alerte ;
et lorsque la liaison de communication est établie :
- Une pluralité d'étapes de transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte ;
les multiples étapes de transmission, au serveur d'incident, de messages comprenant des données audios de l'enregistrement effectué au sien du dispositif d'alerte comprenant :
- la préparation de trames de données audios à partir dudit enregistrement audio ;
- la transmission de trames de données audios au serveur d'incident ;
- la réception, en provenance du serveur d'incident, d'accusés de réception de trames de données audios.

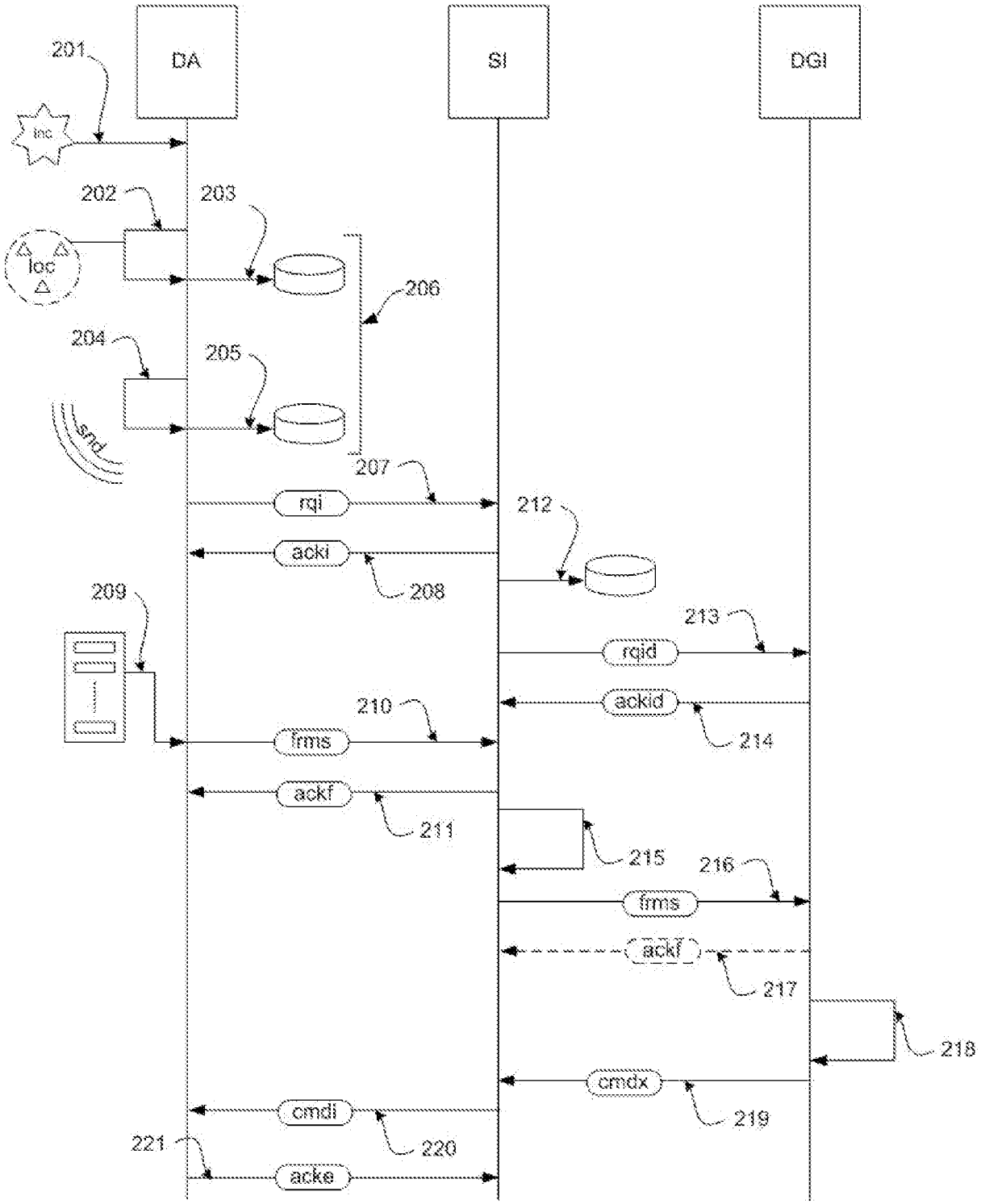
[Revendication 8] Système de traitement de données relatives à un incident comprenant un serveur d'incident et caractérisé en ce qu'il comprend un dispositif d'alerte selon la revendication 7.

[Revendication 9] Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'un procédé de traitement de relatives à un incident selon la revendication 1, lorsqu'il est exécuté sur un ordinateur.

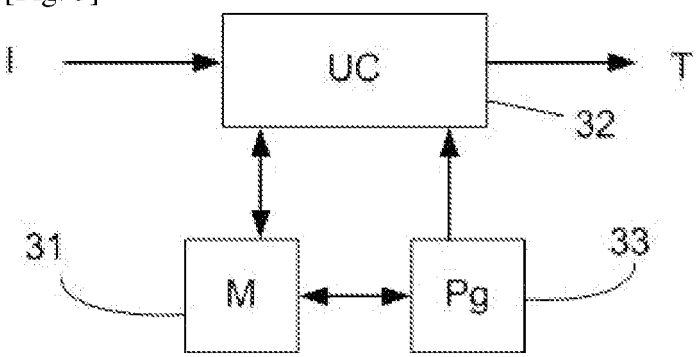
[Fig. 1]



[Fig. 2]


DA
SI
DGI
201
inc
202
203
loc
206
204
205
snd
207
rqi
212
acki
208
209
213
rqid
ackid
210
214
frms
ackf
211
215
216
frms
ackf
217
218
cmdx
219
cmdi
220
221
acke

[Fig. 3]


I
UC
T
32
31
M
Pg
33

RAPPORT DE RECHERCHE

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

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

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

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

☐ Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION
GB 2 510 245 A (PUBLIC WITNESS BUREAU LTD [GB]) 30 juillet 2014 (2014-07-30) US 10 462 642 B1 (RATHNAM SAI [US] ET AL) 29 octobre 2019 (2019-10-29) US 9 860 721 B2 (NAM KI-WON [KR]; TW MOBILE CO LTD [KR]) 2 janvier 2018 (2018-01-02)
2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL
NEANT
3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES
NEANT