(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 811 177**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 08408**

(51) Int Cl[7] : **H 04 L 12/26**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 29.06.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.01.02 Bulletin 02/01.

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

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

(71) **Demandeur(s) :** *SATE SARL Société à responsabilité limitée* — FR.

(72) **Inventeur(s) :** BRATIGNY JEAN PIERRE, ALBINET GUY, CARAMELLE GERARD, FLOC'H PHILIPPE et MORLAT DIDIER.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET CLAUDE GUIU.

(54) PROCEDE DE SURVEILLANCE A DISTANCE DE SITES OU DE PERSONNES ET DISPOSITIF LE METTANT EN OEUVRE.

(57) L'invention concerne un procédé de réception et de traitement d'informations à caractère sécuritaire émises par des équipements de sécurité fixes ou des équipements portatifs pour la protection de sites ou pour la gestion de personnes évoluant dans un environnement à risques remarquable en ce que les informations étant émises sur un réseau téléphonique on réceptionne les informations par au moins un modem ou analogue d'au moins un serveur secondaire, puis on enregistre les informations reçues dans un fichier dit d'enregistrement du serveur secondaire, puis on compare les informations reçues avec les informations d'au moins une base de données d'au moins un serveur secondaire et/ ou un serveur primaire, ce dernier étant connecté à au moins un serveur secondaire via Internet, afin de déterminer si lesdites informations sont des informations normales, des informations d'alarme, ou des informations d'anomalie, puis on traite les informations par un opérateur qui se connecte sur le serveur secondaire via Internet ou via un réseau intranet, et finalement on enregistre les informations traitées dans un fichier dit historique d'un serveur secondaire et/ ou d'un serveur primaire, lesdites informations étant alors accessibles en se connectant sur Internet.

Un autre objet de l'invention concerne un dispositif mettant en oeuvre ledit procédé.

FR 2 811 177 - A1

La présente invention concerne un procédé de surveillance à distance de sites comprenant des équipements de sécurité tels que des alarmes ou des caméras de vidéosurveillance ou de surveillance à distance de personnes évoluant dans un milieu à risque munies d'un équipement portatif.

Dans le domaine de la surveillance de sites, on connaît bien les équipements de sécurité fixes tels qu'un dispositif d'alarme incendie, une alarme anti-vol ou un système de télésurveillance par exemple, qui transmettent, si ces derniers sont activés, une alarme à une station centrale de télésurveillance dite SCT par le réseau téléphonique afin qu'un agent intervienne sur le site où l'alarme s'est produite.

De la même manière, on connaît bien les gardiens de surveillance qui effectuent des rondes sur les sites à surveiller en étant munis d'équipements portatifs dits équipements PTI, c'est-à-dire des équipements pour la protection de travailleurs isolés ; ceux-ci sont conçus de manière à transmettre un signal d'alarme à une SCT située à distance soit lorsque le porteur de l'appareil est conscient et donne lui-même volontairement l'alerte, soit lorsque le porteur n'est plus capable physiquement de donner l'alerte, qu'il soit toujours conscient ou non. Ces équipements PTI comportent généralement un détecteur de mouvement et/ou un détecteur de verticalité, ainsi que des moyens pour émettre un signal d'alarme si le porteur de l'appareil reste immobile ou dans une position autre que la position verticale pendant une période de temps prédéterminée ; lesdits moyens d'émission étant classiquement des appareils de radiocommunication à liaison bidirectionnelle, le signal d'alarme est transmis par ondes radio à un transmetteur téléphonique qui envoie par le réseau téléphonique ledit signal d'alarme à la SCT pour qu'un opérateur le prenne en charge. On entend par "prise en charge" de l'alarme par l'opérateur, la prise de connaissance de l'alarme par ledit opérateur puis son traitement qui consiste alors à exécuter les consignes d'un

client en cas d'alarme, c'est-à-dire prévenir une personne extérieure pour qu'elle se rende sur les lieux par exemple ; chaque centrale de télésurveillance reçoit naturellement les consignes des clients qui lui sont rattachés.

Tous ces procédés et ces dispositifs présentent l'inconvénient de dépendre d'une station centrale de télésurveillance qui ne couvre qu'une région déterminée. Or, pour couvrir un vaste territoire tel que l'ensemble des pays européens par exemple, il faut multiplier les stations centrales de télésurveillance grevant ainsi de manière significative les coûts de fonctionnement. Par ailleurs, ces stations centrales de télésurveillance, outre leurs coûts élevés de fonctionnement et d'infrastructure, ne présentent pas un niveau de sécurité optimum ; en effet, en cas de panne du réseau téléphonique ou en cas de coupure volontaire dudit réseau téléphonique, ces stations centrales de télésurveillance ne peuvent plus recevoir les signaux d'alarme émis par les équipements de sécurité fixes ou portatifs et ne sont plus en mesure d'assurer la sécurité des sites qu'elles ont en charge. De plus, le nombre de signaux d'alarme traités par ces stations centrales de télésurveillance est limité par le nombre d'opérateurs présents dans chacune des stations.

L'un des buts de l'invention est donc de pallier à ces inconvénients en proposant un procédé de réception et de traitement d'informations à caractère sécuritaire émises par des équipements de sécurité fixes ou portatifs pour la protection de sites ou pour la gestion de personnes évoluant dans un environnement à risques qui décentralise le traitement desdites informations sécuritaires supprimant ainsi la vulnérabilité des stations centrales de télésurveillance.

A cet égard et conformément à l'invention, le procédé de réception et de traitement d'informations à caractère sécuritaire émises par des équipements de sécurité fixes tels qu'un dispositif d'alarme incendie ou un système de télésurveillance, ou des équipements portatifs pour la

protection de sites ou pour la gestion de personnes évoluant dans un environnement à risques est remarquable en ce que, les informations à caractère sécuritaire étant émises sur un réseau téléphonique, on réceptionne les informations par au moins un modem ou analogue d'au moins un serveur secondaire qui décroche, vérifie la trame de l'information, ladite trame étant du type (n,x,b) où (n) correspond au numéro de l'appareil, (x) au type d'alarme et (b) à un code de position, puis, envoie un accusé de réception à l'équipement de sécurité émettant les informations et finalement raccroche. Les informations reçues sont alors enregistrées dans un premier fichier dit fichier d'enregistrement d'au moins un serveur secondaire, puis on compare lesdites informations reçues avec les informations d'au moins une base de données d'au moins un serveur secondaire et/ou un serveur primaire, ce dernier étant connecté à au moins un serveur secondaire via Internet, afin de déterminer si lesdites informations sont des informations normales, c'est-à-dire des informations résultant d'une exploitation normale, des informations d'alarme, c'est-à-dire des informations résultant de la transmission d'une alarme depuis un site ou un équipement portatif, ou des informations d'anomalie, c'est-à-dire des informations résultant de l'incohérence entre les évènements prévus et le déroulement réel des évènements.

Si les informations reçues sont des informations normales, les informations sont enregistrées dans un second fichier dit fichier historique d'un serveur secondaire et/ou d'un serveur primaire. Si les informations reçues sont des informations d'alarme ou d'anomalie, ces dernières sont traitées par un opérateur qui se connecte sur un serveur secondaire via Internet ou via un réseau intranet ; le traitement des informations consiste alors dans la mise à disposition des informations sur au moins un serveur secondaire à au moins un opérateur, puis dans l'envoi au serveur secondaire par l'opérateur prenant en charge les informations d'alarme ou d'anomalie un accusé de prise en charge desdites informations et, finalement, dans

l'exécution des opérations correspondant aux dispositions spécifiées dans la ou les bases de données du serveur secondaire et/ou du serveur primaire comme, par exemple, l'appel à un acteur externe qui intervient sur le site émettant les informations d'alarme ou d'anomalie.

Par ailleurs, la mise à disposition des informations à un opérateur consiste soit à mettre les informations simultanément à la disposition d'au moins deux opérateurs, les informations étant traitées par le plus diligent d'entre-eux, soit à mettre les mêmes informations successivement à la disposition d'au moins deux opérateurs jusqu'à ce qu'un opérateur soit disponible pour les saisir puis les traiter.

Après le traitement des informations, on enregistre finalement les informations traitées dans le fichier historique d'un serveur secondaire et/ou d'un serveur primaire, celles-ci étant alors accessibles par les clients en se connectant sur Internet.

Par ailleurs, et selon une première caractéristique particulièrement avantageuse du procédé conforme à l'invention, la ou les bases de données d'au moins un serveur secondaire et/ou au moins un serveur primaire sont constituées par des clients qui se connectent auxdits serveurs primaires et/ou secondaires via Internet et remplissent les différents champs des bases de données tels que, par exemple, leur situation géographique, le matériel utilisé, les consignes en cas d'alarme, etc...

Selon une autre caractéristique particulièrement avantageuse du procédé conforme à l'invention, les connexions aux serveurs primaires et/ou aux serveurs secondaires par les opérateurs via Internet ou via un réseau intranet ou par les clients via Internet sont sécurisées, chaque serveur primaire et secondaire, chaque client et chaque opérateur possédant une clé de certification unique que le ou les serveurs primaires vérifient à chaque connexion sur un serveur primaire ou secondaire, les clés de certification étant attribuées par le ou les serveurs primaires.

Un autre objet de l'invention concerne un dispositif mettant en œuvre le procédé de réception et de traitement d'informations à caractère sécuritaire remarquable en ce qu'il comprend au moins un serveur primaire connecté au réseau Internet, c'est-à-dire qu'il possède une adresse DNS (Domain Name Server), et d'au moins un serveur secondaire également connecté au réseau Internet et muni d'au moins un modem ou analogue pour recevoir les informations émises par des équipements portatifs ou des équipements de sécurité fixes.

On comprend bien que, contrairement à l'art antérieur, les informations à caractère sécuritaire sont envoyées par une ligne téléphonique à l'un des serveurs secondaires de sorte que, si un premier serveur secondaire est en panne ou inaccessible en raison d'une panne du réseau téléphonique reliant les équipements de sécurité au premier serveur secondaire, lesdites informations soient envoyées à un second serveur secondaire pour qu'elles soient traitées quoiqu'il arrive.

D'autres avantages et caractéristiques ressortiront mieux de la description qui va suivre, de plusieurs variantes d'exécution, données à titre d'exemples non limitatifs, du procédé et du dispositif conformes à l'invention, en référence aux dessins annexés sur lesquels :

- la figure 1 est une représentation schématique du dispositif conforme à l'invention,

- la figure 2 est un schéma synoptique d'un équipement portatif transmettant les informations au dispositif conforme à l'invention,

- les figures 3 et 4 représentent, de manière schématique, des organigrammes de fonctionnement du dispositif de réception et de traitement d'informations sécuritaires conforme à l'invention,

- la figure 5 représente, de manière schématique, un organigramme de fonctionnement du traitement des informations reçues conformément à l'invention.

Le dispositif de réception et de traitement

d'informations à caractère sécuritaire suivant l'invention, représenté sur la figure 1, est constitué d'une part d'un serveur primaire 1 comprenant sur des moyens de support, tels qu'un disque dur par exemple, une ou plusieurs bases de données et d'autre part, d'un serveur secondaire 2 qui comprend également sur des moyens de support une ou plusieurs bases de données et muni d'un ou plusieurs modems 3 ou analogues, de préférence entre 2 et 10 modems suivant le nombre d'équipement de sécurité à gérer, pour recevoir les informations émises sur un premier réseau téléphonique 4 par des équipements de sécurité portatifs 5 ou fixes 6. Les serveurs primaire 1 et secondaire 2 sont avantageusement des "serveurs web" comprenant respectivement une adresse DNS (Domain Name Server), lesdits serveurs 1 et 2 étant connectés sur Internet 7, schématiquement représenté sur la figure 1 par un cercle, par une liaison permanente 8 du type RNIS, Câble ou analogue, de manière à pouvoir notamment échanger les données de leurs bases de données respectives. Les serveurs primaire 1 et secondaire 2 consistent, dans un exemple de réalisation non limitatif, en un ordinateur du type PC dont le "hardware" et le software, c'est-à-dire les éléments matériels et logiciels de l'ordinateur, ont été adaptés à la fonction serveur.

Afin d'assurer un haut niveau de sécurité, le dispositif de réception et de traitement d'informations à caractère sécuritaire suivant l'invention comprend avantageusement plusieurs serveurs primaires 1 et plusieurs serveurs secondaires 2 connectés sur Internet 7, lesdits serveurs primaires et secondaires étant aptes à échanger les données de leurs bases de données respectives de sorte que, si un premier serveur secondaire 2 est en panne ou inaccessible en raison d'une panne du réseau téléphonique 4 auquel il est connecté, les informations émises par un équipement portatif 5 ou fixe 6 soient envoyées à un second serveur secondaire 2 pour qu'elles soient traitées.

Le dispositif comprend, par ailleurs, un ou plusieurs ordinateurs opérateur 9, c'est-à-dire des ordinateurs du

type PC ou analogues constituant le poste de travail des opérateurs qui traitent les alarmes, connectés au serveur secondaire 2 par une liaison intranet 10.

Selon une variante d'exécution du dispositif selon l'invention, le ou les ordinateurs opérateurs 9 sont respectivement munis d'un modem 11 afin de se connecter sur l'un quelconque des serveurs secondaires 2 via une connexion 12 à Internet 7, lesdits serveurs secondaires 2 étant eux-mêmes connectés à Internet 7 par une liaison permanente 8 comme on la vu précédemment.

Il va de soi que le dispositif peut comprendre un ordinateur distant 9' muni d'un modem 11 connecté à l'un quelconque des serveurs secondaires 2 uniquement via une connexion 12 à Internet 7 sans être connecté à un réseau intranet 10. De plus, il est bien évident que les modems 11 des ordinateurs opérateurs 9 connecté à un réseau intranet 10 peuvent avantageusement être substitués par un "routeur", non représenté sur la figure 1, sans pour autant sortir du cadre de l'invention.

Par ailleurs, le dispositif comprend avantageusement un ordinateur opérateur 9 connecté par un réseau intranet 10 au serveur primaire 1 afin, notamment, d'effectuer sa maintenance, c'est-à-dire de mettre à jour sa ou ses bases de données, etc... ; toutefois, les autres ordinateurs opérateurs 9 peuvent également se connecter au serveur primaire 1 via la connexion 12 à Internet 7 pour effectuer ces travaux de maintenance.

Les bases de données du serveur secondaire 2 sont avantageusement mises à jour par un client C qui se connecte sur ledit serveur secondaire 2 par une liaison Internet 7 au moyen d'un modem 11 classique. Le client C accède aux paramétrages de la base de données concernant ses équipements portatifs 5 ou fixes 6, dont l'accès est contrôlé par un "login" et un mot de passe, à travers un "browser" de navigation tel que "Netscape Communicator" ou "Internet Explorer" respectivement des sociétés NETSCAPE et MICROSOFT. En effet, à chaque serveur secondaire 2 correspond une adresse URL, c'est-à-dire un site Internet,

telle que par exemple http://www.< nom de domaine >.< com, net, fr, be, de, etc... > sur lequel se connecte le client C qui remplit alors les formulaires mis en ligne sur le site Internet, le client C donnant des informations relatives à ces équipements (code de référence, type d'équipement, etc...), des informations relatives à la localisation de ces équipements, des informations relatives au traitement des informations reçues (conditions et codes d'alerte, conditions de fonctionnement normal, etc...), des informations relatives à la gestion des alarmes ou anomalies (consignes à appliquer par l'opérateur), etc..., toutes ces informations venant constituer les bases de données du serveur secondaire 2. Le client C peut avantageusement consulter en temps réel sur le site Internet associé au serveur secondaire 2 qui gère ses équipements de sécurité 5 et/ou 6, en se connectant audit serveur secondaire de la même manière que précédemment, l'historique des évènements rattachés aux équipements de sécurités 5 et/ou 6 et plus généralement aux sites surveillés.

Par ailleurs, l'équipement de sécurité portatif 5 est avantageusement réalisé à partir d'un téléphone portable du type GSM ou analogue dont le boîtier 13 est représenté schématiquement par un rectangle en traits mixtes sur la figure 2. Ce boîtier 13 porte une antenne externe 14 et il contient les composants habituels d'un téléphone portable à savoir une source d'énergie électrique autonome 15 telle qu'une batterie rechargeable ou non ou bien encore des piles, par exemple, un circuit d'émission-réception 16 auxquels sont connectés des moyens 17 de commande de ce circuit, un haut-parleur 18 et un microphone 19.

Un module d'extension comportant un boîtier additionnel 20, indiqué d'une manière schématique sur la figure 1 par un rectangle en traits mixtes, est fixé d'une manière amovible au boîtier 13 du téléphone portable. Ce boîtier additionnel 20 contient un microprocesseur 21 à plusieurs entrées qui sont connectées respectivement à un détecteur de mouvement 22, à un détecteur de

verticalité 23, à un bouton de commande multifonction 24 et éventuellement à un récepteur infrarouge 25. Le microprocesseur 21 est par ailleurs connecté, à ses sorties, à un émetteur de signal sonore 26, une interface 27 à un circuit de codage 28 qui est connecté au circuit d'émission-réception 16 du téléphone portable afin d'émettre, à partir de l'antenne 14 du téléphone portable vers un réseau téléphonique, des informations sécuritaires codées dont la trame est du type (n,x) ou (n,x,b) de natures différentes suivant les situations détectées, où (n) correspond au numéro de l'appareil, (x) au type d'alarme et (b) à un code de position. Le circuit de codage 28 et l'interface 27 sont connectés respectivement au circuit d'émission-réception 16 du téléphone portable. Le boîtier additionnel 20 contient également un circuit d'alimentation 29 qui est connecté à la source d'énergie électrique autonome 15 contenue dans le boîtier 13 et qui est relié aux divers composants du module d'extension en vue de leur alimentation en courant électrique.

Le récepteur infrarouge 25 est prévu dans le boîtier 20 du module d'extension lorsque l'équipement est destiné à être utilisé dans un système de localisation comprenant des balises B réparties à distances les unes des autres et émettant respectivement des signaux codés b d'un rayonnement infrarouge qui sont destinés à être captés par ledit récepteur infrarouge 25 lorsque le porteur de l'équipement passe à proximité de chaque balise B. Ces balises B émettent des informations les identifiant et, le cas échéant, des indications concernant les différents états de la balise, c'est-à-dire le niveau de charge de la batterie (batterie faible), une tentative de falsification, de vol ou de déplacement, par exemple, lesdites balises étant fixes ou mobiles, autonomes ou couplées à un organe central.

Il va de soi que l'équipement de sécurité portatif 5 est réalisé à partir d'un téléphone portable du type GSM, du type DETC, satellite ou analogues. De plus, l'équipement de sécurité portatif 5 peut également consister dans un

appareil de radiocommunication du type à liaison bidirectionnelle, les informations émises étant transmises par ondes radio à un transmetteur téléphonique qui les envoie par le réseau téléphonique à un serveur secondaire 2.

On décrira maintenant, en référence aux figures 1 à 5, le fonctionnement du dispositif de réception et de traitement des informations à caractère sécuritaire suivant l'invention comprenant un unique serveur primaire 1 et un unique serveur secondaire 2, les informations sécuritaires étant émises par un équipement portatif 5 tel que décrit précédemment.

Selon les figures 1 à 3, lorsqu'un gardien équipé d'un équipement de sécurité portatif 5 actionne le bouton de commande multifonction 24 à la suite d'une agression ou lorsqu'il passe, par exemple, à proximité d'une balise B qui émet une information codée b captée par le récepteur infrarouge 25 de l'équipement portatif 5, ce dernier envoie à un serveur secondaire 2 une information sécuritaire, opération 101 sur la figure 3, dont la trame est du type (n,x,b) dans un premier temps via les relais téléphoniques du type GSM, puis dans un second temps via un réseau téléphonique 4 standard. Au cours d'une opération 102, le modem 3 du serveur secondaire 2 décroche, puis ledit serveur vérifie sur ses bases de données si la trame (n,x,b) des informations émises par l'équipement portatif 5 sont correctes (opération 103), c'est-à-dire si (n) correspond bien à un numéro de l'appareil enregistré dans les bases de données du serveur secondaire 2.

Lorsque le résultat de la vérification de la trame (n,x,b) des informations reçues par le modem 3 est positif, le serveur secondaire 2 envoie, au cours d'une opération 104, un accusé de réception à l'équipement portatif 5 qui a émis les informations sécuritaires, puis le modem 3 raccroche (opération 105) prêt à recevoir un nouvel appel d'un équipement de sécurité. Les informations ainsi reçues sont alors enregistrées (opération 106) dans un premier fichier dit fichier d'enregistrement du serveur

secondaire 2.

En cas d'échec de la vérification de la trame (n,x,b) des informations reçues avec les bases de données du serveur secondaire 2, on vérifie ladite trame avec les bases de données du serveur primaire 1 au cours d'une opération 107. De la même manière que précédemment, lorsque le résultat de la vérification de la trame (n,x,b) des informations reçues par le modem 3 est positif, le serveur secondaire 2 envoie un accusé de réception à l'équipement portatif 5 (opération 104) qui a émis les informations sécuritaires, puis le modem 3 raccroche (opération 105) prêt à recevoir un nouvel appel d'un équipement de sécurité. Les informations ainsi reçues sont alors enregistrées (opération 106) dans le fichier d'enregistrement du serveur secondaire 2.

En référence à la figure 4, les informations reçues ainsi enregistrées dans le fichier d'enregistrement du serveur secondaire 2 sont, au cours d'une opération 108, comparée avec les informations contenues dans les bases de données du serveur secondaire 2 afin de déterminer s'il s'agit d'informations normales, c'est-à-dire des informations résultant d'une exploitation normale, d'informations d'alarme, c'est-à-dire des informations résultant de la transmission d'une alarme depuis un site ou un équipement portatif, ou d'informations d'anomalie, c'est-à-dire des informations résultant de l'incohérence entre les évènements prévus et le déroulement réel des évènements. En effet, cette opération de comparaison 107 consiste à déterminer le type d'alarme (x) des informations reçues, la base de données du serveur secondaire 2 comprenant les consignes associées à chaque type d'alarme (x). Si les informations reçues sont des informations normales 109, celles-ci sont alors enregistrées dans un second fichier dit fichier historique du serveur secondaire 2 au cours d'une opération 110, le fichier historique étant alors accessible en se connectant au serveur secondaire 2 via Internet comme on le verra plus loin. Si les informations reçues sont des informations

d'anomalies 111 ou des informations d'alarme 112, celles-ci sont alors traitées par un opérateur au cours d'une opération 113 que l'on décrira plus en détail un peu plus loin.

Par contre, dans l'hypothèse où les bases de données du serveur secondaire 2 ne permettent pas de déterminer le type d'alarme, par exemple, lorsque les bases de donnée du serveur secondaire 2 ne sont pas à jour, on opère une comparaison des informations reçues avec les bases de données du serveur primaire 1, schématiquement représenté en pointillés sur la figure 4, au cours d'une opération 108' afin de déterminer le type d'informations, c'est-à-dire de déterminer si les informations sont des informations normales, des informations d'alarme ou des informations d'anomalie. De la même manière que précédemment, Si les informations reçues sont des informations normales 109', celles-ci sont alors enregistrées dans le fichier historique du serveur secondaire 2 au cours d'une opération 110. Si les informations reçues sont des informations d'anomalies 111' ou des informations d'alarme 112', celles-ci sont alors traitées par un opérateur au cours de l'opération 113.

Les bases de données du serveur primaire 1 et du serveur secondaire 2 sont avantageusement mises à jour simultanément, c'est-à-dire que la modification d'un champ des bases de données du serveur secondaire 2 entraîne la modification simultanée du champ correspondant des bases de données du serveur primaire 1 et inversement.

L'opération de traitement des informations 113, en référence à la figure 5, consiste dans une première opération 114 à mettre à la disposition des opérateurs les informations sur le serveur secondaire 2. Cette opération consiste soit à mettre les informations simultanément à la disposition d'au moins deux opérateurs, les informations étant traitées par le plus diligent d'entre-eux, soit à mettre lesdites informations successivement à la disposition d'au moins deux opérateurs jusqu'à ce que l'un d'entre-eux soit disponible pour saisir les informations

puis les traiter. Au cours d'une opération 115, l'opérateur se connecte au serveur secondaire 2 via Internet 7 ou un réseau intranet 10 pour prendre en charge les informations à traiter puis il envoie un accusé de prise en charge des informations au serveur secondaire 2 (opération 116) ces informations n'étant alors plus à la disposition des autres opérateurs. L'opérateur concerné exécute alors les consignes correspondant à l'information d'alarme (opération 117) ces consignes consistant à prévenir une personne extérieure pour qu'elle se rende sur les lieux par exemple, puis il enregistre les informations traitées dans le fichier historique au cours de l'opération 110. Ce fichier historique comprend ainsi toutes les informations concernant les informations normales telles que les passages d'un gardien devant les bornes B, par exemple, les informations d'anomalies et les informations d'alarme en précisant les actions effectuées par les opérateurs lors de l'opération de traitement 113 ; toutes ces informations sont accessibles par un client C qui se connecte au serveur secondaire 2 via Internet 7 comme on l'a déjà dit.

REVENDICATIONS

1 - Procédé de réception et de traitement d'informations à caractère sécuritaire émises par des équipements de sécurité fixes (6) tels qu'un dispositif d'alarme incendie ou un système de télésurveillance, ou des équipements portatifs (5) pour la protection de sites ou pour la gestion de personnes évoluant dans un environnement à risques **caractérisé** en ce que, les informations à caractère sécuritaire étant émises sur un réseau téléphonique (4), on met en œuvre au moins les étapes suivantes :

- réception des informations par au moins un modem (3) ou analogue d'au moins un serveur secondaire (2), puis

- enregistrement des informations reçues dans un premier fichier dit fichier d'enregistrement du serveur secondaire (2), puis

- comparaison des informations reçues avec les informations d'au moins une base de données d'au moins un serveur secondaire (2) et/ou un serveur primaire (1), ce dernier étant connecté à au moins un serveur secondaire (2) via Internet (7), afin de déterminer si lesdites informations sont des informations normales, c'est-à-dire des informations résultant d'une exploitation normale, des informations d'alarme, c'est-à-dire des informations résultant de la transmission d'une alarme depuis un site ou un équipement portatif (5), ou des informations d'anomalie, c'est-à-dire des informations résultant de l'incohérence entre les évènements prévus et le déroulement réel des évènements, puis

- traitement des informations par un opérateur qui se connecte sur le serveur secondaire (2) via Internet (7) ou via un réseau intranet (10), et finalement

- enregistrement des informations traitées dans un second fichier dit fichier historique d'un serveur secondaire (2) et/ou d'un serveur primaire (1), lesdites informations étant alors accessibles en se connectant sur Internet (7).

2 - Procédé selon la revendication précédente

caractérisé en ce que la réception des informations consiste dans le décrochage du modem (3), la vérification de la trame de l'information, l'envoi d'un accusé de réception à l'équipement de sécurité (5,6) émettant les informations et finalement, au raccrochage.

3 - Procédé selon la revendication 1 **caractérisé** en ce que, si les informations reçues sont des informations normales, lesdites informations sont enregistrées dans le fichier historique d'un serveur secondaire (2) et/ou d'un serveur primaire (1).

4 - Procédé selon la revendication 3 **caractérisé** en ce que, si les informations reçues sont des informations d'alarme ou d'anomalie, le traitement des informations par un opérateur consiste au moins dans les étapes suivantes :

- mise à disposition des informations sur au moins un serveur secondaire (2) à au moins un opérateur, puis
- envoi au serveur secondaire (2) par l'opérateur prenant en charge les informations d'alarme ou d'anomalie, d'un accusé de prise en charge des informations, puis
- exécution des opérations correspondantes aux dispositions spécifiées dans la ou les base du serveur secondaire (2) et/ou du serveur primaire (1) comme, par exemple, l'appel à un acteur externe qui intervient sur le site émettant les informations d'alarme ou d'anomalie.

5 - Procédé selon la revendication 4 **caractérisé** en ce que la mise à disposition des informations sur au moins un serveur secondaire (2) consiste à mettre lesdites informations simultanément à la disposition d'au moins deux opérateurs, les informations étant traitées par le plus diligent d'entre-eux.

6 - Procédé selon la revendication 4 **caractérisé** en ce que la mise à disposition des informations sur au moins un serveur secondaire (2) consiste à mettre lesdites informations successivement à la disposition d'au moins deux opérateurs jusqu'à ce qu'un opérateur soit disponible pour les saisir puis les traiter.

7 - Procédé selon l'une quelconque des revendications précédentes **caractérisé** en ce que la ou les bases de

données d'au moins un serveur secondaire (2) et/ou au moins un serveur primaire (1) sont constituées par des clients C qui se connectent auxdits serveurs primaires (1) et/ou secondaires (2) via Internet (7) et remplissent les différents champs des bases de données tels que, par exemple, leur situation géographique, le matériel utilisé, les consignes en cas d'alarme, etc...

8 - Procédé selon l'une quelconque des revendications précédentes **caractérisé** en ce que les connexions aux serveurs primaires (1) et/ou aux serveurs secondaires (2) par les opérateurs via Internet (7) ou via un réseau intranet (10) ou par les clients via Internet (7) sont sécurisées, chaque serveur primaire (1) et secondaire (2), chaque client C et chaque opérateur possédant une clé de certification unique que le ou les serveurs primaires vérifient à chaque connexion sur un serveur primaire ou secondaire, les clés de certification étant attribuées par le ou les serveurs primaires (1).

9 - Dispositif mettant en œuvre le procédé de réception et de traitement d'informations à caractère sécuritaire selon l'une quelconque des revendications précédentes **caractérisé** en ce qu'il comprend au moins un serveur primaire (1) connecté au réseau Internet (7), c'est-à-dire qu'il possède une adresse DNS (Domain Name Server), et d'au moins un serveur secondaire (7) également connecté au réseau Internet (7) et muni d'au moins un modem (3) ou analogue pour recevoir les informations émises par des équipements portatifs (5) ou des équipements de sécurité fixes (6).

10 - Dispositif selon la revendication précédente **caractérisé** en ce qu'il comprend au moins un ordinateur opérateur (9) pour le traitement des informations d'alarme ou d'anomalie connecté à au moins un serveur secondaire (2) par un réseau intranet (10).

11 - Dispositif selon la revendication 9 **caractérisé** en ce qu'il comprend au moins un ordinateur opérateur (9,9') distant pour le traitement des informations d'alarme ou d'anomalie connecté à au moins un

serveur secondaire (2) par le réseau Internet (7).

12 - Dispositif selon l'une quelconque des revendications 9 à 11 **caractérisé** en ce que les équipements portatifs (5) sont des téléphones portables comprenant un boîtier (13) contenant une source d'énergie électrique autonome (15) pour alimenter un circuit électronique d'émission-réception (16) relié à une antenne (14) portée par le boîtier (13), un microphone (19), un haut-parleur (18), un module d'extension (20) contenant un microprocesseur (21) connecté, à ses entrées, à des moyens de détection de mouvement (22) et/ou de verticalité (23), à un bouton de commande multifonctions (24), et à des moyens de localisation (25), et, à ses sorties, à une interface (27) et à des moyens de codage (28) des informations sécuritaires eux-mêmes connectés au circuit d'émission-réception (16), et à un circuit d'alimentation électrique (29) des divers composants se trouvant dans le boîtier (20) du module d'extension, ce circuit d'alimentation (29) étant connecté à la source d'énergie autonome (15) du téléphone portable de manière à pouvoir émettre, à partir de l'antenne (14) du téléphone vers un réseau téléphonique (4), des informations sécuritaires codées dont la trame est du type (n,x) ou (n,x,b) et de natures différentes suivant les situations détectées, où (n) correspond au numéro de l'appareil, (x) au type d'alarme et (b) à un code de position.

13 - Dispositif selon la revendication 12 **caractérisé** en ce que chaque équipement portatif (5) comprend des moyens (25) pour le rendre utilisable conjointement avec un système externe de localisation comprenant des balises (B) espacées émettant des informations sous la forme de rayonnement codé.

14 - Dispositif selon la revendication 13 **caractérisé** en ce que les balises (B) sont fixes ou mobiles, autonomes ou couplées à un organe central.

15 - Dispositif selon l'une quelconque des revendications 13 ou 14 **caractérisé** en ce que les balises (B) émettent des informations les identifiant et,

le cas échéant, des indications concernant les différents états de la balise (batterie faible, tentative de falsification, de vol ou de déplacement, par exemple).

16 - Dispositif selon l'une quelconque des revendications 13 à 15 **caractérisé** en ce que les informations émises par les balises (B) et reçues par le récepteur (13) sont émises sous la forme de rayonnement infrarouges codés.

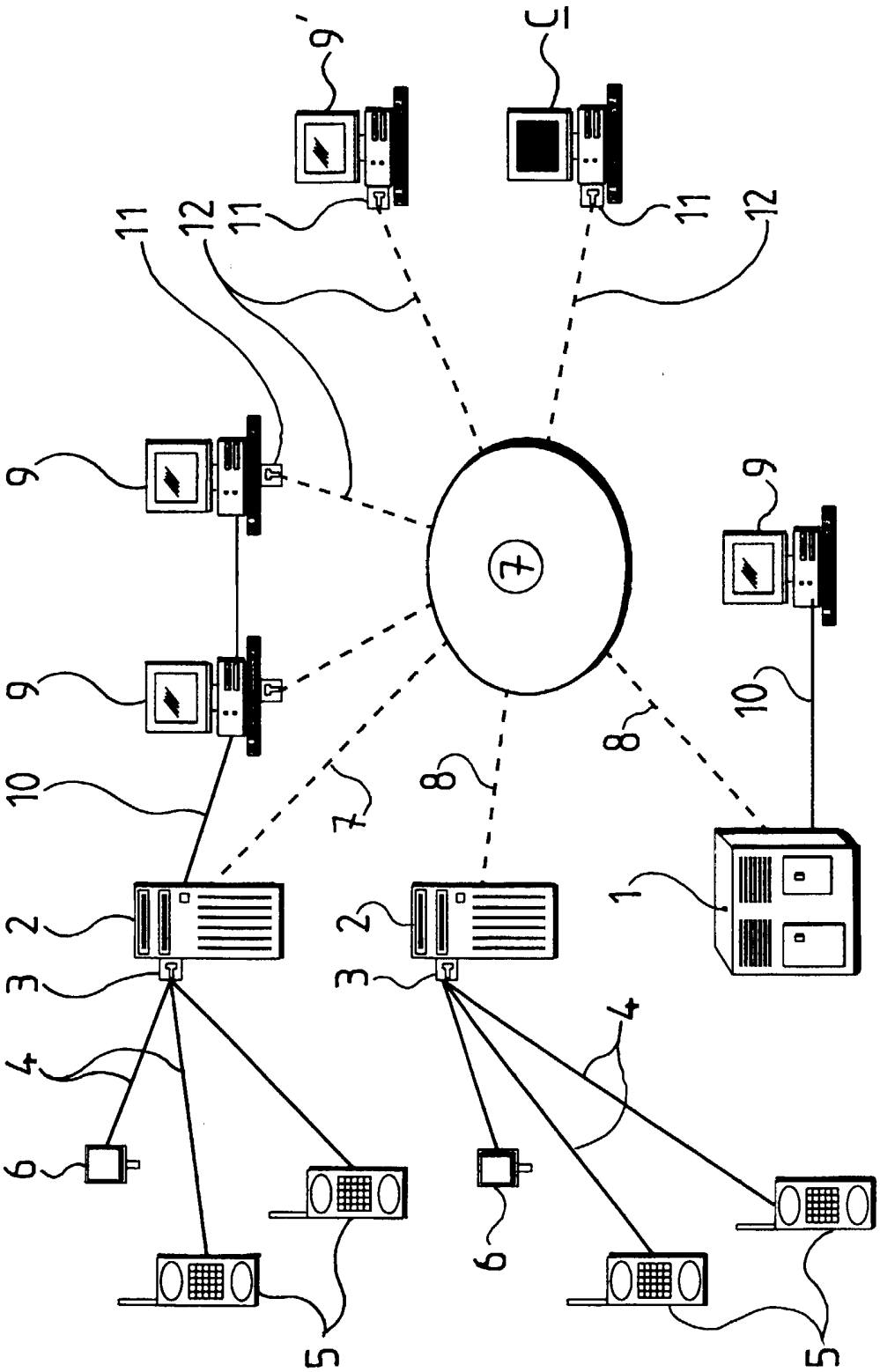
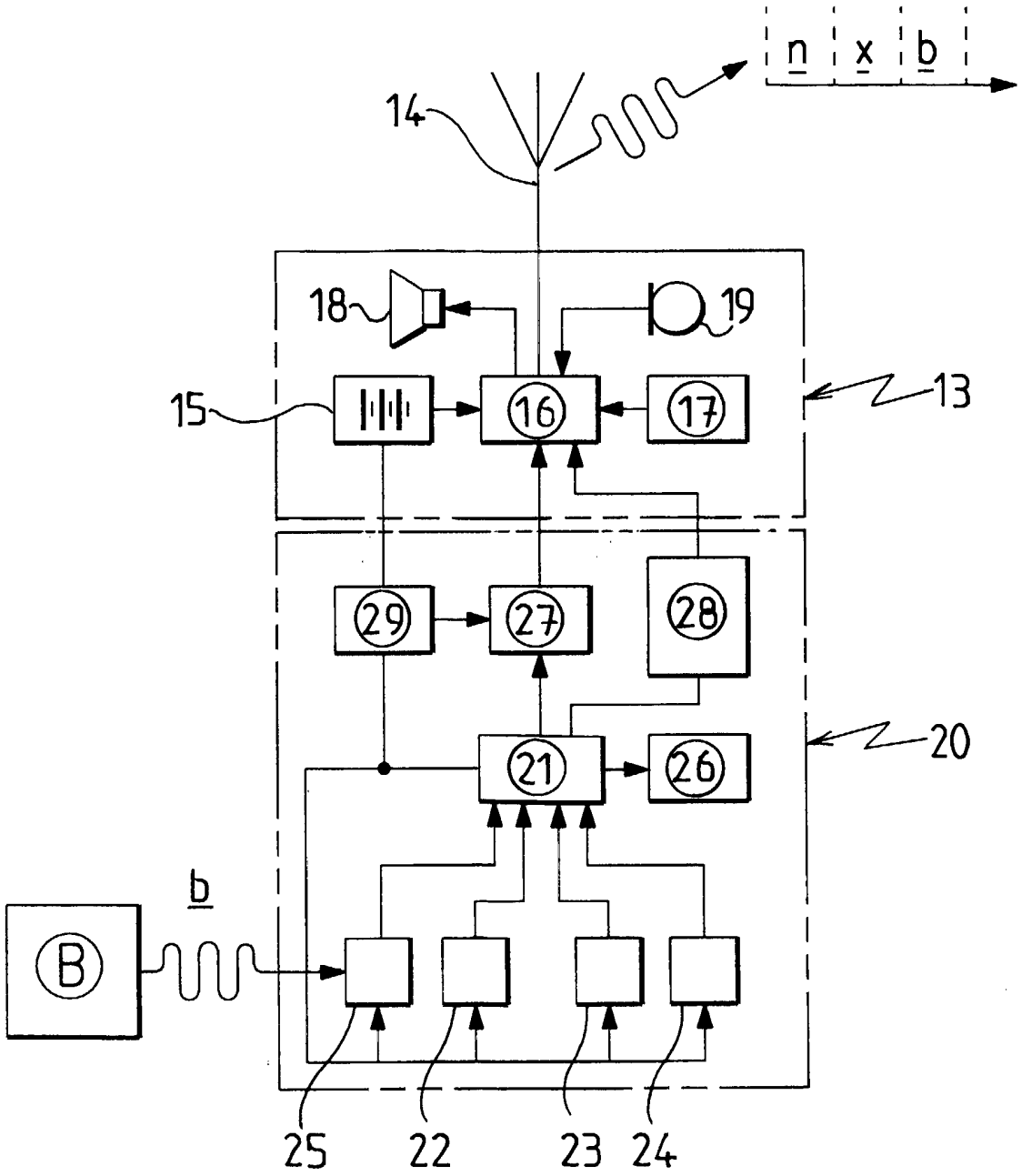


fig.1

fig.2



3/5

fig.3

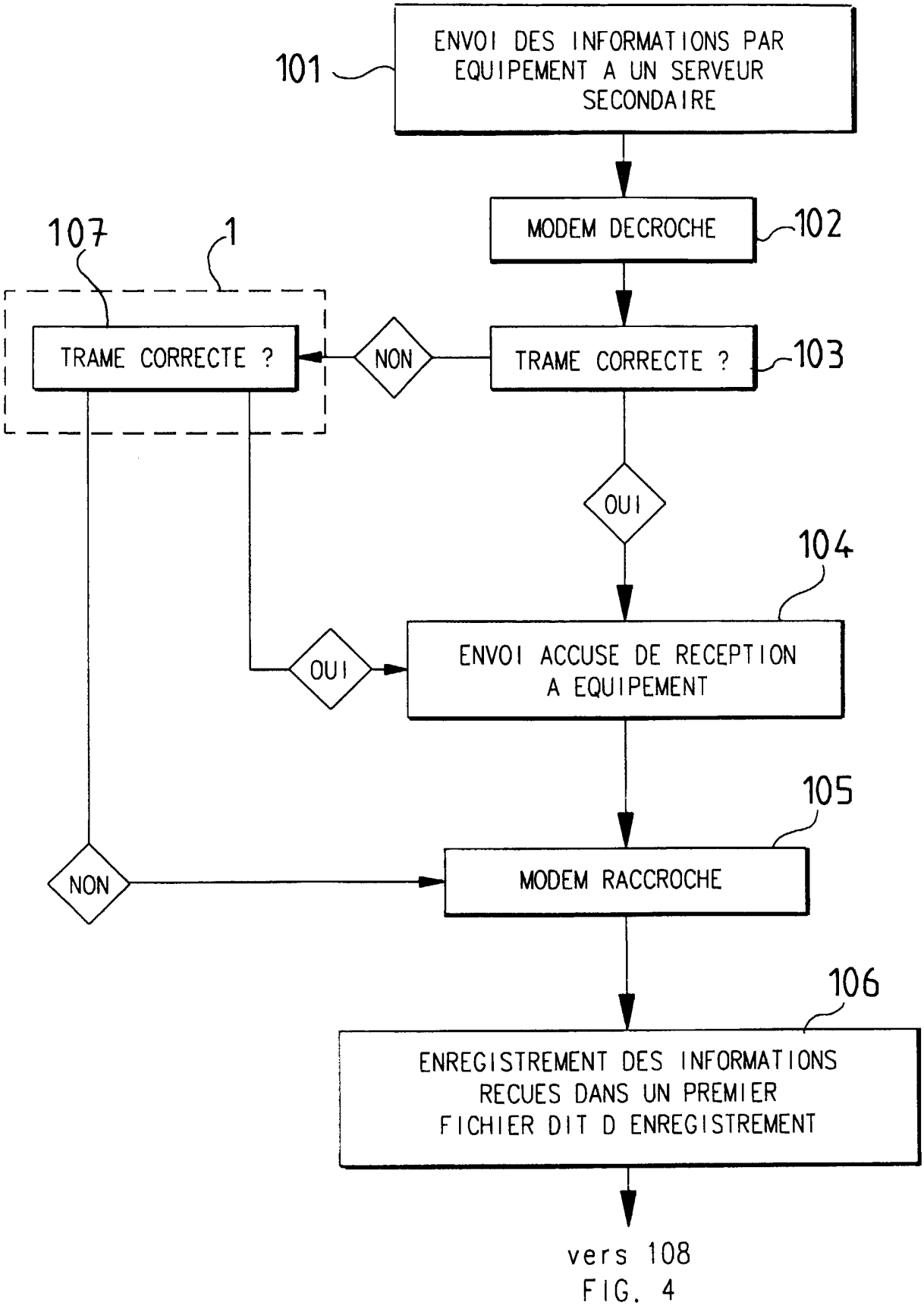

ENVOI DES INFORMATIONS PAR EQUIPEMENT A UN SERVEUR SECONDAIRE
101
MODEM DECROCHE
102
TRAME CORRECTE ?
103
NON
TRAME CORRECTE ?
107
1
OUI
104
OUI
ENVOI ACCUSE DE RECEPTION A EQUIPEMENT
105
NON
MODEM RACCROCHE
106
ENREGISTREMENT DES INFORMATIONS RECUES DANS UN PREMIER FICHIER DIT D ENREGISTREMENT
vers 108

FIG. 4

fig.4

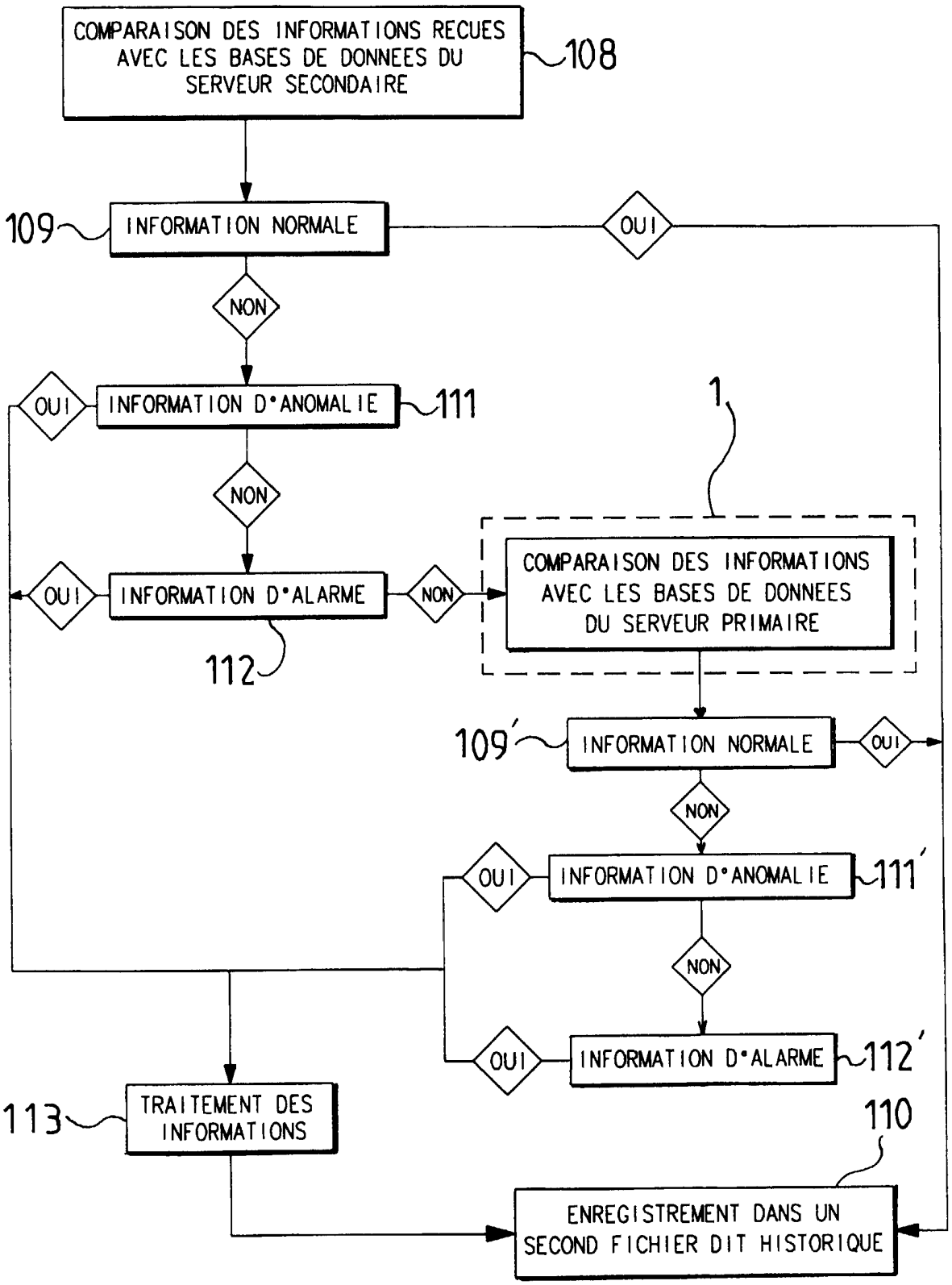
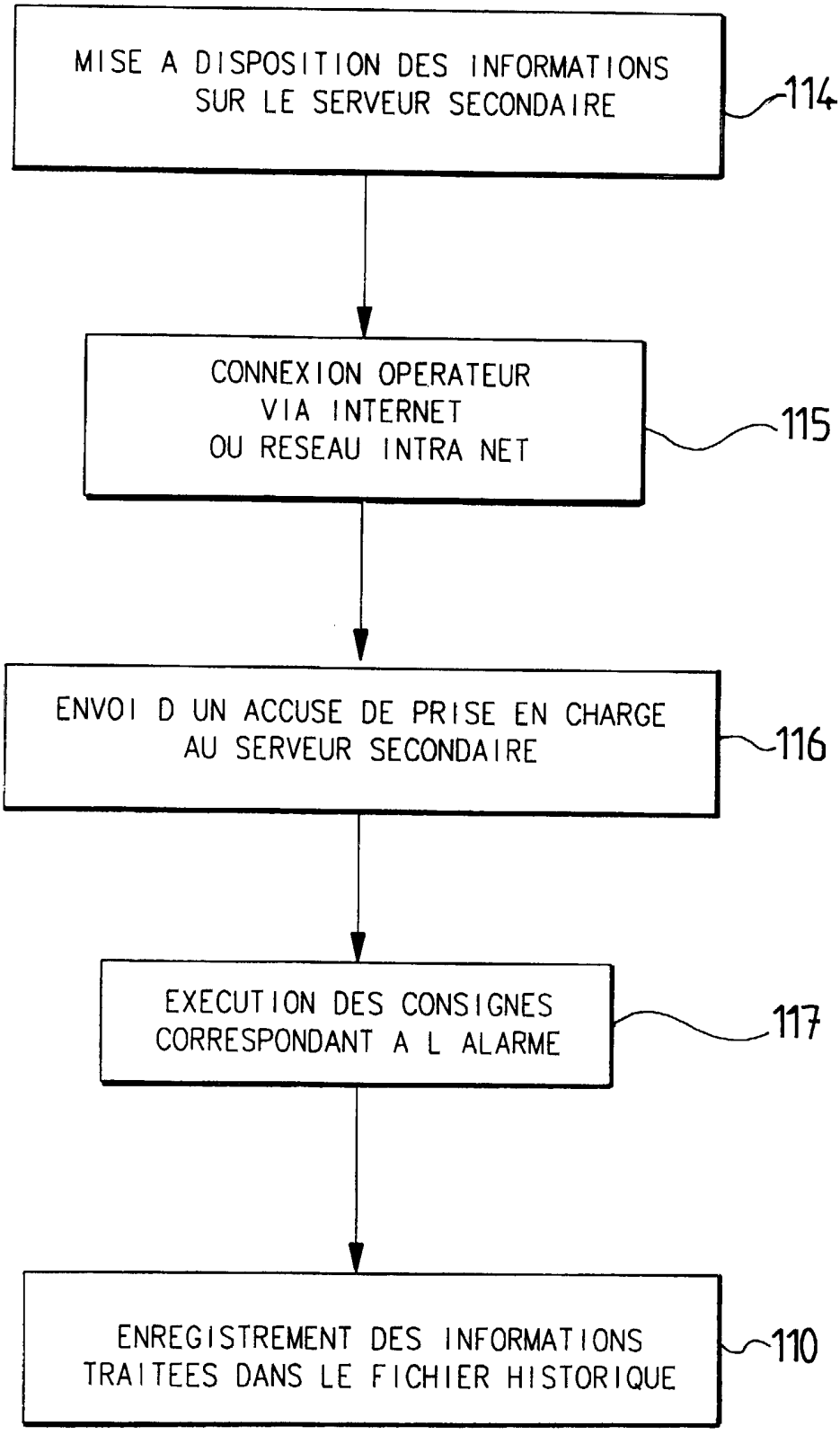

COMPARAISON DES INFORMATIONS RECUES AVEC LES BASES DE DONNEES DU SERVEUR SECONDAIRE
108
109
INFORMATION NORMALE
OUI
NON
OUI
INFORMATION D'ANOMALIE
111
1
NON
OUI
INFORMATION D'ALARME
NON
COMPARAISON DES INFORMATIONS AVEC LES BASES DE DONNEES DU SERVEUR PRIMAIRE
112
109'
INFORMATION NORMALE
OUI
NON
OUI
INFORMATION D'ANOMALIE
111'
NON
OUI
INFORMATION D'ALARME
112'
113
TRAITEMENT DES INFORMATIONS
110
ENREGISTREMENT DANS UN SECOND FICHIER DIT HISTORIQUE

fig.5


MISE A DISPOSITION DES INFORMATIONS SUR LE SERVEUR SECONDAIRE
114
CONNEXION OPERATEUR VIA INTERNET OU RESEAU INTRA NET
115
ENVOI D UN ACCUSE DE PRISE EN CHARGE AU SERVEUR SECONDAIRE
116
EXECUTION DES CONSIGNES CORRESPONDANT A L ALARME
117
ENREGISTREMENT DES INFORMATIONS TRAITEES DANS LE FICHIER HISTORIQUE
110

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

2811177

N° d'enregistrement national

FA 593510
FR 0008408

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 0 989 503 A (ULTRA PROIZV ELEKTRONSKIH NAPR) 29 mars 2000 (2000-03-29) * abrégé * * colonne 1, ligne 19 - ligne 56 * * colonne 2, ligne 16 - ligne 28 * * colonne 2, ligne 35 - ligne 50 * * colonne 5, ligne 15 - ligne 23 * * figure 1 *	1-16	H04L12/26
A	GB 2 325 548 A (NABAVI RICHARD PARVIZ) 25 novembre 1998 (1998-11-25) * abrégé * * revendication 1 * * figure 1 *	1-16	
A	US 5 717 379 A (PETERS WOLFGANG) 10 février 1998 (1998-02-10) * abrégé * * colonne 1, ligne 66 - colonne 2, ligne 8 * * colonne 3, ligne 30 - ligne 31 *	1-16	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04M G08B H04L

Date d'achèvement de la recherche	Examinateur
2 mars 2001	Lai, C

CATÉGORIE DES DOCUMENTS CITÉS

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

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)