



(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
06.07.2011 Bulletin 2011/27

(51) Int Cl.:
G01V 11/00 (2006.01) G08B 13/00 (2006.01)

(21) Numéro de dépôt: **10196843.6**

(22) Date de dépôt: **23.12.2010**

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

• **Lamarque, Thierry**
78114, Magny-les-Hameaux (FR)
• **D'Hose, Johan**
91120, Palaiseau (FR)

(30) Priorité: **30.12.2009 FR 0906395**

(71) Demandeur: **Thales**
92200 Neuilly Sur Seine (FR)

(74) Mandataire: **Lucas, Laurent Jacques et al**
Marks & Clerk France
Conseils en Propriété Industrielle
Immeuble " Visium "
22, avenue Aristide Briand
94117 Arcueil Cedex (FR)

(72) Inventeurs:
• **Zouaoui, Rhalem**
92340, Bourg la Reine (FR)

(54) **Dispositif pour estimer le niveau de menace que représente un individu**

(57) La présente invention concerne un dispositif comportant au moins un détecteur de menace.
Le détecteur de menace estime le niveau de menace

que représente un individu à partir de mesures effectuées lorsque l'individu passe dans une zone de mesure.
Application : sécurisation des infrastructures

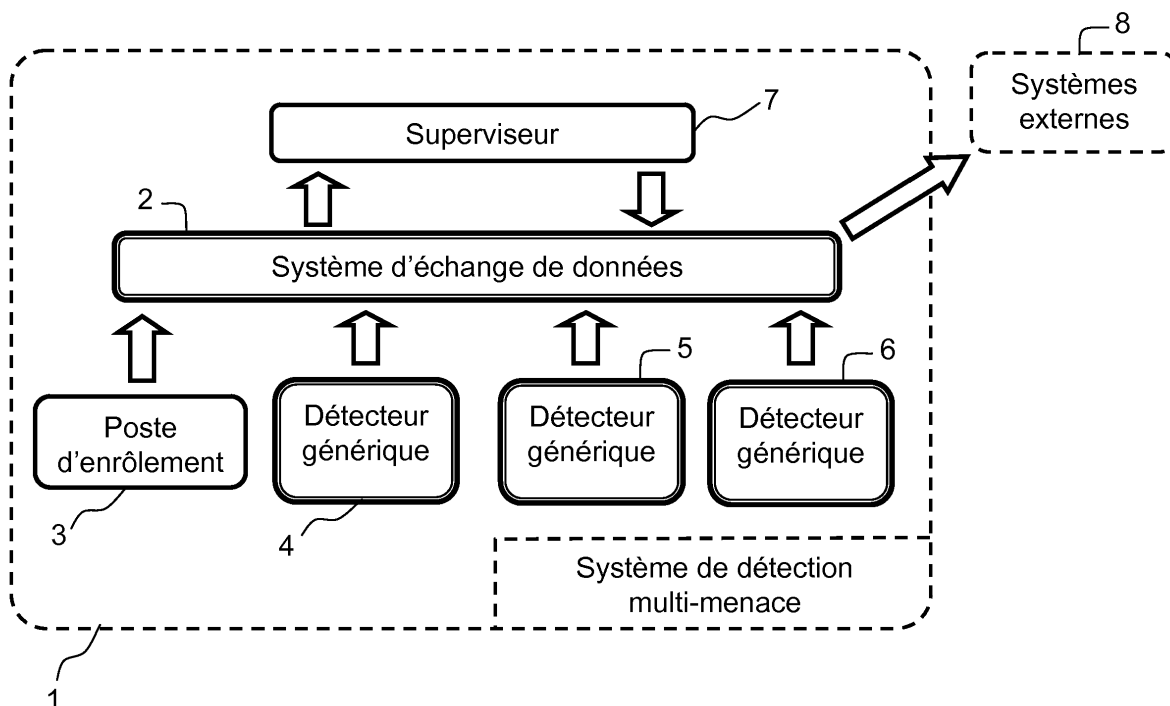


FIG.1

Description

[0001] La présente invention concerne un dispositif pour estimer le niveau de menace que représente un individu, sans que l'individu collabore. Elle s'applique notamment dans le domaine de la sécurisation des infrastructures, par exemple les portiques de sécurité utilisés dans les aéroports.

[0002] Les portiques de sécurité visent à détecter et estimer d'éventuelles menaces que peuvent représenter des individus.

[0003] Par exemple, les détecteurs de métaux comportent des capteurs capables de détecter tout objet métallique transporté par un individu. Et en fonction de la quantité de métal détecté, le niveau de menace estimé est plus ou moins élevé. Les portiques à ondes millimétriques comportent des capteurs capables de mesurer le rayonnement naturel du corps et ainsi de détecter des objets cachés sous les vêtements qui feraient obstacle au rayonnement naturel du corps. Et en fonction de la taille et de la forme de l'objet détecté, le niveau de menace estimé est plus ou moins élevé. Les détecteurs de trace, également appelés « nez électroniques », sont quant à eux capables de détecter la présence de composés chimiques, notamment les précurseurs d'explosifs. Et en fonction de la variété et de la quantité de précurseurs détectés, le niveau de menace estimé est plus ou moins élevé.

[0004] Un inconvénient majeur de ces différents types de portique est qu'ils n'adressent qu'un seul type de menace à la fois. Or, pour tenter de faire face aux nouvelles menaces terroristes qui sont par nature difficilement identifiables, les systèmes de sécurité doivent aujourd'hui fournir des fonctionnalités de détection multi-menace, capables d'adresser plusieurs types de menaces à la fois et de générer le "profil de menace" d'un individu. Mais rassembler de telles fonctionnalités au sein d'un même système nécessite d'intégrer une grande variété de capteurs, ce qui n'est pas sans poser de nombreuses difficultés.

[0005] Tout d'abord, parce-que les systèmes actuels de détection mono-menace utilisent des formats spécifiques propriétaires pour échanger de l'information, qu'il s'agisse de recevoir un ordre de type marche / arrêt ou encore d'envoyer à un opérateur un rapport de détection contenant le résultat d'une estimation d'un niveau de menace relatif à un individu sur lequel des mesures ont été prises. Généralement, l'opérateur reçoit le rapport via un système de supervision pouvant notamment comporter un écran d'affichage. Le fait qu'il existe autant de formats de message que de types de capteurs rend particulièrement difficile l'intégration de capteurs hétérogènes dans un même système de détection multi-menaces.

[0006] Ensuite, parce-que dans les lieux publics où la foule est libre d'aller et venir à sa guise, les systèmes de détection multi-menaces doivent être efficaces même dans un mode d'utilisation non-coopératif, c'est-à-dire que les individus sont contrôlés à leur insu. Par exemple,

un système de détection multi-menaces dans un aéroport peut avoir à faire des mesures sur des individus traversant un couloir étroit à des allures variables de marche lente, de marche rapide, voire au pas de course. Dans cette configuration spatiale, qui sera qualifiée de configuration « à la chaîne » dans la suite de la présente demande, les capteurs doivent effectuer leurs mesures l'un après l'autre sur un même individu qui suit le couloir. A son insu, l'individu peut passer d'abord dans la zone de mesure d'un détecteur de métaux, puis immédiatement après dans la zone de mesure d'un détecteur de traces et enfin dans la zone de mesure d'un détecteur à ondes millimétriques. Le détecteur de métaux et le détecteur à ondes millimétriques ne mettent que quelques dixièmes de secondes pour envoyer leurs rapports. L'individu se trouve donc encore très probablement dans le couloir lorsque le détecteur de métaux et le détecteur à ondes millimétriques envoient leurs rapports. Alors que le détecteur de traces met quant à lui plusieurs secondes pour récolter des échantillons sur un individu grâce à des dispositifs de soufflerie et d'aspiration, analyser les échantillons et envoyer son rapport. L'individu a alors très probablement déjà quitté le couloir lorsque le détecteur de traces envoie son rapport. Ainsi, en cas de débit important d'individus dans le couloir, le système de supervision reçoit des rapports en rafales désordonnées, c'est-à-dire que les rapports correspondant à un même individu ne sont pas reçus dans l'ordre de passage de l'individu dans les zones de mesure des détecteurs. Le système de supervision reçoit des rapports complètement mélangés correspondant à divers individus. Il lui est alors bien difficile d'associer entre eux les rapports correspondant à un même individu.

[0007] L'invention a notamment pour but de surmonter les inconvénients précités des systèmes de détection multi-menace à capteurs hétérogènes, notamment de réguler l'envoi des rapports de détection par les capteurs, de telle sorte que les systèmes de détection de menace puissent enfin être utilisés dans un mode non-coopératif. Pour cela, l'invention propose notamment d'envoyer des rapports de détection normalisés contenant les mesures brutes, une estimation de la menace ainsi que des signatures physiques de l'individu. L'invention propose également de fractionner les rapports en plusieurs parties: une première partie envoyée dès la sortie de la zone de mesure et une deuxième partie envoyée une fois les détections achevées. A cet effet, l'invention a pour objet un dispositif comportant au moins un détecteur de menace. Le détecteur de menace estime le niveau de menace que représente un individu à partir de mesures effectuées lorsque l'individu passe dans une zone de mesure.

[0008] Par exemple, le dispositif peut comporter un détecteur de présence afin de détecter la présence de l'individu dans la zone de mesure.

[0009] Avantageusement, le détecteur de présence peut comporter un faisceau infrarouge que l'individu interrompt lorsqu'il pénètre dans la zone de mesure et un

faisceau infrarouge que l'individu interrompt lorsqu'il quitte la zone de mesure.

[0010] Dans un mode de réalisation préférentiel, le détecteur de menace peut détecter des métaux pouvant être transportés par l'individu ou des traces de précurseurs dans la fabrication d'explosif pouvant être transportés par l'individu ou encore des objets pouvant être cachés sous les vêtements de l'individu.

[0011] Avantageusement, le dispositif peut comporter au moins un détecteur de signature physique pouvant effectuer des mesures dans la zone de mesure, afin de reconnaître l'individu si celui-ci est connu dans une base de données des individus susceptibles de passer dans la zone de mesure. La base peut contenir, pour chacun desdits individus, un identifiant associé à sa signature physique reconnaissable par le détecteur de signature physique.

[0012] Par exemple, le détecteur de signature physique peut être une caméra capable de détecter le visage de l'individu.

[0013] Dans un mode de réalisation préférentiel, le dispositif peut envoyer un rapport conforme à un format prédéterminé indépendant du type des mesures effectuées ainsi que de la nature de la menace estimée.

[0014] Avantageusement, le rapport peut contenir les mesures brutes effectuées lorsque l'individu passe dans la zone de mesure ainsi que le niveau de menace estimé à partir de ces mesures.

[0015] Dans un mode de réalisation préférentiel, le rapport peut être envoyé en plusieurs parties distinctes afin que l'envoi des données puisse débiter avant que les détections de menace et de signature physique soient achevées.

[0016] Outre le fait de permettre de construire un système de détection multi-menaces utilisable en mode non-coopératif, l'invention a encore pour principal avantage qu'elle permet de construire un système de détection multi-menace totalement modulaire, autorisant aussi bien des configurations spatiales « à la chaîne » dans des couloirs étroits que des configurations spatiales dispersées sur de grandes surfaces. Un tel système de détection multi-menace peut donc s'adapter à n'importe quel agencement des lieux à sécuriser.

[0017] D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit faite en regard de dessins annexés qui représentent :

- la figure 1, par un diagramme, un exemple d'architecture d'un système de détection multi-menace non-collaboratif;
- la figure 2, par un diagramme, un exemple d'architecture d'un détecteur générique selon l'invention;
- la figure 3, par un schéma et un chronogramme, un exemple de zone de mesure d'un détecteur générique selon l'invention;
- la figure 4, par un schéma et par un chronogramme, un exemple de configuration séquentielle de modules de mesure incluant des détecteurs génériques

selon l'invention;

- la figure 5, par un schéma et par un chronogramme, un exemple de configuration non-séquentielle de modules de mesure incluant des détecteurs génériques selon l'invention;
- la figure 6, par un schéma, un exemple de structure de rapport générique selon l'invention;
- la figure 7, par un chronogramme, des exemples de processus de détection réalisés par des détecteurs génériques selon l'invention disposés en configuration séquentielle;
- la figure 8, par un chronogramme, des exemples de processus d'envoi d'un rapport générique par un détecteur générique selon l'invention;
- la figure 9, par un chronogramme, un exemple d'envoi en deux parties par un détecteur générique d'un rapport générique selon l'invention.

[0018] La figure 1 illustre par un diagramme un exemple d'architecture d'un système 1 de détection multi-menace non-collaboratif. Le système 1 se compose de plusieurs éléments qui communiquent par l'intermédiaire d'un système d'échange de données 2. Le système 1 comporte un poste d'enrôlement 3 qui entretient une base de données des individus susceptibles d'être présents dans l'infrastructure à sécuriser, cette base n'étant pas représentée sur la figure 1. La base de données contient notamment un identifiant associé à une signature physique pour chaque individu enregistré. Le système 1 comporte également des détecteurs génériques 4, 5 et 6 selon l'invention. Un détecteur générique selon l'invention regroupe plusieurs capteurs physiques ainsi que des modules de traitement automatisé pour estimer le niveau de menace à partir des mesures prises par les capteurs physiques. Avantageusement, chacun des détecteurs génériques 4, 5 et 6 peut envoyer à un superviseur 7 des rapports génériques selon l'invention, qui peuvent notamment contenir les mesures prises par les capteurs physiques ainsi que les résultats d'estimation du niveau de menace. Le superviseur 7 peut informer un opérateur du niveau de menace par voie d'affichage ou d'alerte. Il peut éventuellement communiquer les mesures et le niveau de menace à des systèmes externes 8 appropriés.

[0019] Avantageusement, un rapport générique peut être un rapport à la structure et au format normalisés selon l'invention, de telle sorte que, quel que soit le détecteur générique 4, 5 ou 6 qui l'ait émis, le superviseur 7 est capable de l'interpréter par les mêmes moyens. La figure 6 illustre la structure normalisée d'un rapport générique selon l'invention. Dans la suite de la présente demande, le terme "rapport" sera simplement utilisé pour désigner des rapports génériques envoyés par des détecteurs génériques selon l'invention.

[0020] La figure 2 illustre par un diagramme un exemple d'architecture d'un détecteur générique selon l'invention, comme les détecteurs génériques 4, 5 et 6.

[0021] Tout d'abord, un détecteur générique collecte diverses informations sur un individu qui se trouve dans

sa zone de mesure, comme par exemple sa vitesse de déplacement, sa trajectoire et certaines caractéristiques de son comportement. Pour cela, un détecteur générique détecte dans un premier temps la présence éventuelle d'un individu dans sa zone de mesure, par exemple grâce à un détecteur de présence 22. Il s'agit d'un capteur physique, comme par exemple une barrière infrarouge. La présence d'un individu est alors détectée lorsque celui-ci coupe un faisceau infrarouge. Un détecteur générique est également capable de détecter au moins une signature physique d'un individu dans sa zone de mesure, grâce à au moins un détecteur de signature 21 par exemple. Par exemple, le détecteur de signature 21 peut être une caméra permettant de détecter le visage d'un individu dans sa zone de mesure sans la collaboration de ce dernier. Un détecteur générique est enfin capable de détecter au moins une menace que représente un individu dans sa zone de mesure, grâce à un détecteur de menace 20. Il s'agit d'un capteur physique, comme par exemple un détecteur de métaux, de traces de précurseurs dans la fabrication d'explosif ou encore d'objets cachés sous les vêtements.

[0022] Ensuite, un détecteur générique est capable d'envoyer au superviseur 7 des rapports contenant notamment les résultats d'estimation d'un niveau de menace, l'estimation étant effectuée par un module de calcul 23 à partir des mesures prises par le détecteur 20.

[0023] Sur réception des rapports envoyés par les détecteurs génériques 4, 5 et 6, le superviseur 7 accomplit différentes tâches. Il est notamment chargé d'associer les rapports à l'individu concerné. Dans un mode de réalisation particulier, le superviseur 7 peut réaliser cette association à l'aide de la signature physique de l'individu mesurée par la caméra 21 et incorporée dans le rapport, ainsi qu'à l'aide de la base de données des individus mise à jour par le poste d'enrôlement 3, cette base associant la signature physique de l'individu à son identifiant. Le superviseur 7 permet aussi de configurer spatialement le système 1. En effet, un avantage important du système 1 de détection multi-menace selon l'invention est sa modularité, le système 1 pouvant être notamment utilisé dans les deux configurations spatiales des détecteurs génériques 4, 5 et 6 illustrées par les figures 4 et 5. Le choix de la configuration spatiale des détecteurs génériques 4, 5 et 6 dépend de l'agencement des lieux à sécuriser.

[0024] La figure 3 illustre par un schéma et un chronogramme un exemple de zone de mesure de l'un quelconque des détecteurs génériques 4, 5 ou 6 selon l'invention. La zone peut être délimitée par des barrières matérielles et/ou immatérielles. Par exemple, la zone de mesure peut être délimitée par deux panneaux en bois 31 et 32 et par deux faisceaux infrarouges 33 et 34. Le détecteur générique traite uniquement les mesures effectuées au passage d'un individu dans le sens de la flèche dans la zone de mesure entre l'instant T_{in} d'entrée dans la zone et l'instant T_{out} de sortie de la zone. La durée du processus de traitement des mesures entre les

instants T_{in} et T_{out} est illustrée par le rectangle hachuré. La même symbolique sera utilisée pour représenter des durées de processus dans les figures 4, 5, 7, 8 et 9. Dans la suite de la présente demande, l'ensemble formé par un détecteur générique et les barrières matérielles et/ou immatérielles délimitant sa zone de mesure sera appelé "module de mesure".

[0025] La figure 4 illustre par un schéma et par un chronogramme un exemple de configuration séquentielle de modules de mesure 44, 45 et 46 incluant les détecteurs génériques 4, 5 et 6 respectivement selon l'invention. Dans cette configuration, les modules de mesure sont disposés de telle sorte qu'un individu passe successivement et directement d'une zone de mesure à une autre. Les détecteurs génériques 4, 5 et 6 traitent uniquement les mesures effectuées au passage de l'individu dans le sens de la flèche dans leurs zones de mesure respectives, l'individu quittant lesdites zones aux instants T_{4out} , T_{5out} et T_{6out} respectivement. A l'instant T_{4out} , le module de mesure 44 commence à envoyer son rapport. Un rectangle hachuré 40 commençant à l'instant T_{4out} illustre la durée de cet envoi. A l'instant T_{5out} , le module de mesure 45 commence à envoyer son rapport. Un rectangle hachuré 41 commençant à l'instant T_{5out} illustre la durée de cet envoi. A l'instant T_{6out} , le module de mesure 46 commence à envoyer son rapport. Un rectangle hachuré 42 commençant à l'instant T_{6out} illustre la durée de cet envoi. Dans le présent exemple de configuration séquentielle, le module de mesure 46 est le module maître alors que les modules de mesure 44 et 45 sont des modules esclaves. Ceci signifie que le superviseur 7 ne tente d'associer les rapports reçus des modules de mesure 44, 45 et 46 qu'une seule fois pour toutes, lorsqu'il a fini de recevoir dans son intégralité le rapport envoyé par le module maître 46. Un rectangle hachuré 43 illustre la durée de cette association.

[0026] La figure 5 illustre par un schéma et par un chronogramme un exemple de configuration non-séquentielle des modules de mesure 44, 45 et 46 selon l'invention. Les modules de mesure 44, 45 et 46 sont autonomes et séparés par des zones non surveillées. Par exemple, l'individu traverse d'abord le module de mesure 45, puis le module de mesure 46 et enfin le module de mesure 44, cet ordre dépendant uniquement de sa volonté. A l'instant T_{5out} , le module de mesure 45 commence à envoyer son rapport. Un rectangle hachuré 50 commençant à l'instant T_{5out} illustre la durée de cet envoi. A l'instant T_{6out} , le module de mesure 46 commence à envoyer son rapport. Un rectangle hachuré 51 commençant à l'instant T_{6out} illustre la durée de cet envoi. A l'instant T_{4out} , le module de mesure 44 commence à envoyer son rapport. Un rectangle hachuré 52 commençant à l'instant T_{4out} illustre la durée de cet envoi. En configuration non-séquentielle, le superviseur 7 tente d'associer les rapports reçus des modules de mesure 45, 46 et 44 chaque fois qu'il a fini de recevoir un rapport dans son intégralité, qu'il s'agisse du rapport du module de mesure 45, 46 ou 44. Des rectangles hachurés 53, 54 et 55 illustrent res-

pectivement la durée de ces associations.

[0027] La figure 6 illustre par un schéma un exemple de structure d'un rapport générique 60 selon l'invention. Le rapport générique 60 encapsule sous un format normalisé les résultats issus d'une ou de plusieurs détections de menace effectuées par le détecteur générique 4, 5 ou 6 dans sa zone de mesure. L'encapsulation des résultats est réalisée après le passage d'un individu dans la zone de mesure du détecteur générique. Le rapport générique 60 regroupe différents éléments de données.

[0028] Le rapport générique 60 peut notamment comporter un élément 67 incluant la date de création du rapport. Cette information peut faciliter l'archivage et le traitement des rapports. Elle peut par exemple permettre au superviseur 7 de classer les rapports par date de création.

[0029] Le rapport générique 60 peut également comporter un élément 68 incluant le ou les identifiants du ou des détecteurs de menace. Le superviseur 7 peut utiliser ces informations pour interpréter les données issues de la détection des menaces.

[0030] Le rapport générique 60 peut également comporter un élément 69 regroupant les résultats de la détection de présence, comme illustré par des éléments 70 et 71 pour les instants d'entrée et de sortie dans la zone de mesure et la vitesse de déplacement respectivement.

[0031] Le rapport générique 60 peut également comporter un élément 64 regroupant les résultats d'une ou de plusieurs détections de signature. Il peut s'agir des résultats de détections biométriques, comme illustré par des éléments 65 et 66 pour la détection du visage et de la position des yeux respectivement. Mais il peut également s'agir de solution RFID ou de toute autre solution non-collaborative.

[0032] Le rapport générique 60 peut enfin comporter un élément 61 regroupant les résultats de la ou des détections de menace. L'élément 61 peut notamment comporter un élément 62 qui peut lui-même regrouper une ou des estimations « métier » du ou des niveaux de menace. Le résultat d'une estimation d'un niveau de menace peut se représenter sous la forme d'une valeur comprise entre 0 et 100, cette échelle étant arbitraire. Le calcul de cette valeur peut être réalisé par un traitement automatisé chargé d'interpréter des données brutes regroupées dans un élément 63 et correspondant aux mesures prises lors du passage de l'individu dans la zone de mesure. Ces données brutes 63 peuvent également être exploitées par le superviseur 7 comme compléments d'information, par exemple afin de déterminer plus précisément la nature de la menace ou encore comme éléments de comparaison avec les résultats d'un autre détecteur générique en vue de fusionner des données. Pour cela, les données brutes 63 peuvent être encodées à l'aide d'un codec spécifique au type de données, puis envoyées au superviseur 7 sous forme de vecteurs. Le superviseur 7 se charge alors de décoder les vecteurs à l'aide du même codec.

[0033] La figure 7 illustre par un chronogramme des

exemples de processus de détection réalisés par n détecteurs de menace, où n est un entier non-nul, disposés au sein d'un même détecteur générique. Dans le présent exemple de réalisation, chaque détecteur générique comporte des barrières infrarouges connectées à une carte d'acquisition pour détecter la présence d'un individu dans sa zone de mesure, un détecteur spécifique à la menace à détecter, comme un détecteur de métal ou de traces de précurseurs d'explosifs ou d'objets cachés sous les vêtements, un dispositif biométrique pour détecter le visage et les yeux de manière non collaborative et une caméra CCD (Charge-Coupled device) à faible résolution. Un individu passe d'abord dans la zone de mesure du détecteur générique 1, puis immédiatement dans la zone de mesure du détecteur générique 2, et ainsi de suite jusqu'à passer en dernier dans la zone de mesure du détecteur générique n. Comme explicité précédemment, chaque détecteur générique i, où $i \in \{1, \dots, n\}$, est capable de réaliser plusieurs processus de détection de présence C_x^{DP} , où $x \in \{1, \dots, r\}$, plusieurs processus de détection de menace C_y^{DM} , où $y \in \{1, \dots, s\}$, et plusieurs processus de détection de signature C_z^{DS} , où $z \in \{1, \dots, t\}$. Comme explicité précédemment, ces processus de détection sont effectués uniquement à partir de mesures prises au passage de l'individu dans la zone de mesure du détecteur i. Par exemple, l'individu passe dans la zone de mesure du détecteur 1 dans l'intervalle de temps $[T_{in}, T_{out}]$. Comme illustré par la figure 7, ces processus de détection nécessitent des temps de réponse plus ou moins longs, qu'il faut prendre en considération pour éviter de perdre des informations. En particulier, comme illustré par la figure 7, les processus de détection de menace C_1^{DM} et de signature C_1^{DS} par le détecteur générique 1 peuvent se poursuivre après l'instant T_{out} où l'individu quitte la zone de mesure du détecteur générique 1. Il n'est donc pas possible pour le détecteur générique 1 d'envoyer la totalité du rapport, alors même que l'individu a quitté sa zone de mesure.

[0034] La figure 8 illustre par un chronogramme des exemples de processus d'envoi d'un rapport par le détecteur générique 1 selon l'invention. L'individu passe dans la zone de mesure du détecteur 1 dans l'intervalle de temps $[T_{in}, T_{out}]$. Comme explicité précédemment, il peut ne pas être possible au détecteur générique 1 d'envoyer un rapport dès que l'individu a quitté sa zone de mesure, ledit détecteur 1 n'ayant pas encore terminé ses processus de détection de menace C_1^{DM} et de signature C_1^{DS} à l'instant T_{Ev1} , où $T_{Ev1} = T_{out} + \Delta T_{DP2}$ et où ΔT_{DP2} est le temps de réponse du processus de détection de présence C_2^{DP} . Pour remédier à cela, le détecteur 1 peut avantageusement envoyer en k parties, où k est un entier non-nul, un rapport générique tel que le rapport générique 60 décrit à la figure 6. Le nombre k de parties dépend des événements déclencheurs disponibles Ev_k . Il peut s'agir d'événements de détection comme la sortie de l'individu de la zone de mesure, une quantité suffisante de données ou encore une alarme. Il peut s'agir également d'événements systèmes comme des anomalies. Il peut

enfin s'agir d'événements temporels comme l'expiration d'un délai. Ainsi, comme illustré par la figure 8, lorsque l'événement E_{vk} survient à l'instant T_{Evk} , un processus d'envoi E_k d'une $k^{\text{ème}}$ partie de rapport commence.

[0035] La figure 9 illustre par un chronogramme un exemple d'envoi par le détecteur générique 1 d'un rapport en deux parties. L'individu passe dans la zone de mesure du détecteur 1 dans l'intervalle de temps $[T_{in}, T_{out}]$. La détection de sortie de l'individu de la zone de mesure à l'instant T_{Ev1} , est le premier événement déclencheur d'un premier processus envoi E_1 . La première partie inclut l'ensemble des résultats biométriques et de localisation, ainsi qu'une partie des résultats de la détection de menace. La fin du délai d'exécution du processus de détection le plus long effectué par le détecteur 1, qui est le processus de détection de menace C_1^{DM} dans le présent exemple de réalisation, est le deuxième événement déclencheur d'un deuxième processus d'envoi E_2 . Le processus de détection de menace C_1^{DM} se termine au plus tard à l'expiration d'un délai ΔT_{max} à compter de l'instant T_{out} , le délai ΔT_{max} correspondant au plus gros volume de données que C_1^{DM} peut être amené à traiter. C'est pourquoi le détecteur générique 1 exécute, à partir de l'instant T_{out} , un processus d'attente Δt_{1}^{Dm} permettant de retarder le début du processus E_2 d'une durée ΔT_{max} jusqu'à l'instant T_{Ev2} . La deuxième partie inclut les résultats obtenus pendant le délai d'exécution de la détection de menace.

[0036] L'invention décrite précédemment a encore pour principaux avantages de permettre l'envoi des résultats de détection de menace sous un format générique au superviseur, favorisant ainsi l'évolutivité du système. De plus, l'invention permet d'associer les résultats de détection de menace aux résultats de détection de signature de l'individu. Enfin, un système de détection multi-menaces construit à partir de détecteurs génériques selon l'invention peut être utilisé dans une configuration spatiale « à la chaîne » jusqu'à des débits très élevés où chaque zone de mesure est traversée en permanence par un individu.

des mesures effectuées ainsi que de la nature de la menace estimée, le dispositif étant **caractérisé en ce que** le rapport est envoyé en plusieurs parties distinctes afin que l'envoi des données puisse débiter avant que les détections de menace et de signature physique soient achevées.

2. Dispositif selon la revendication 1, **caractérisé en ce qu'il** comporte un détecteur de présence (22) afin de détecter la présence de l'individu dans la zone de mesure.
3. Dispositif selon la revendication 2, **caractérisé en ce que** le détecteur de présence comporte un faisceau infrarouge que l'individu interrompt lorsqu'il pénètre dans la zone de mesure et un faisceau infrarouge que l'individu interrompt lorsqu'il quitte la zone de mesure.
4. Dispositif selon la revendication 1, **caractérisé en ce que** le détecteur de menace détecte :
 - des métaux pouvant être transportés par l'individu, ou ;
 - des traces de précurseurs dans la fabrication d'explosif pouvant être transportés par l'individu, ou ;
 - des objets pouvant être cachés sous les vêtements de l'individu.
5. Dispositif selon la revendication 1, **caractérisé en ce que** le détecteur de signature physique est une caméra capable de détecter le visage de l'individu.
6. Dispositif selon la revendication 1, **caractérisé en ce que** le rapport contient les mesures brutes effectuées lorsque l'individu passe dans la zone de mesure ainsi que le niveau de menace estimé à partir de ces mesures.

Revendications

1. Dispositif comportant au moins un détecteur de menace (20) estimant le niveau de menace que représente un individu à partir de mesures effectuées lorsque l'individu passe dans une zone de mesure, le dispositif comportant au moins un détecteur de signature physique (21) effectuant des mesures dans la zone de mesure, afin de reconnaître l'individu si celui-ci est connu dans une base de données des individus susceptibles de passer dans la zone de mesure, la base contenant pour chacun desdits individus un identifiant associé à sa signature physique reconnaissable par le détecteur de signature physique (21), le dispositif envoyant un rapport conforme à un format prédéterminé indépendant du type

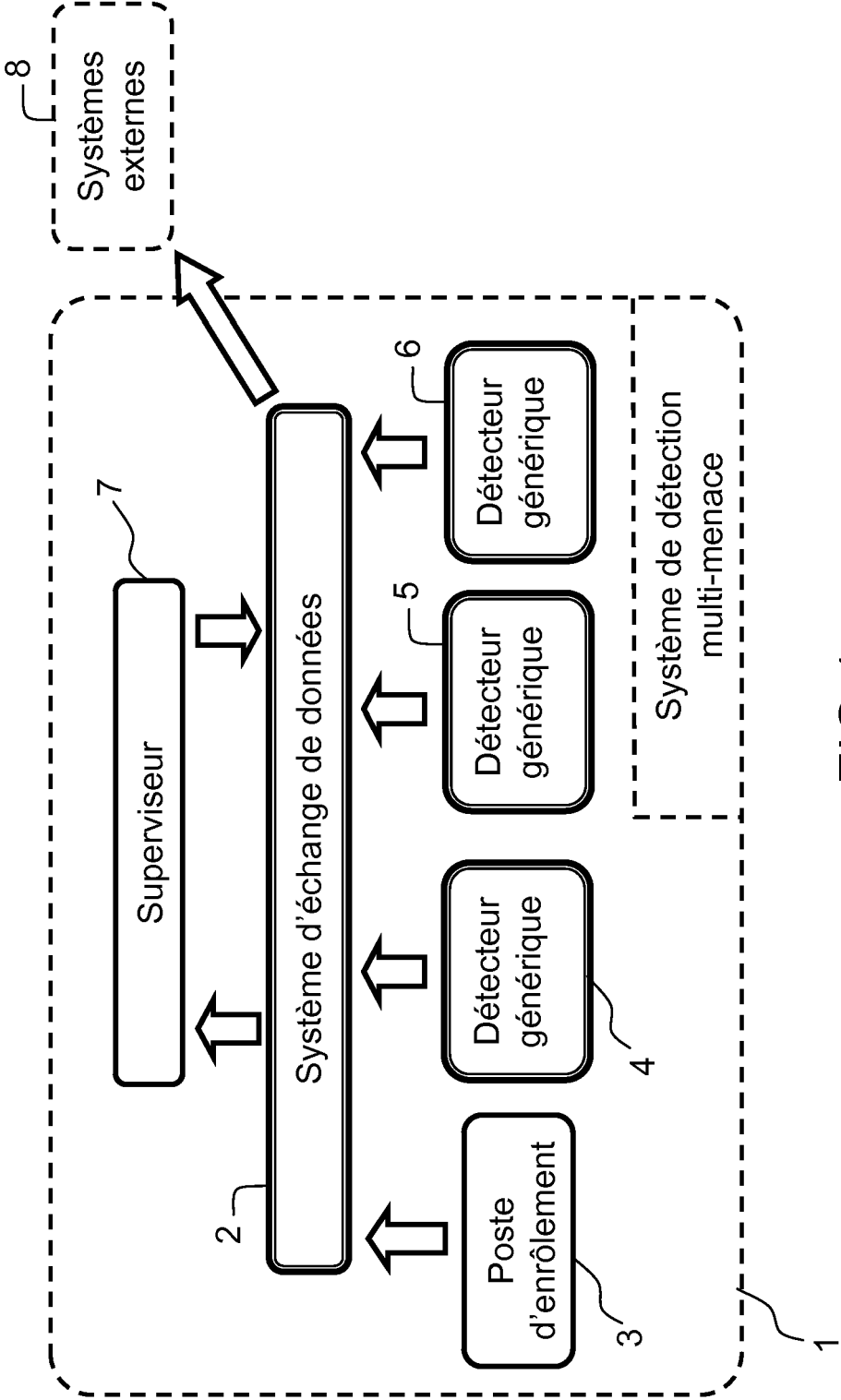


FIG.1

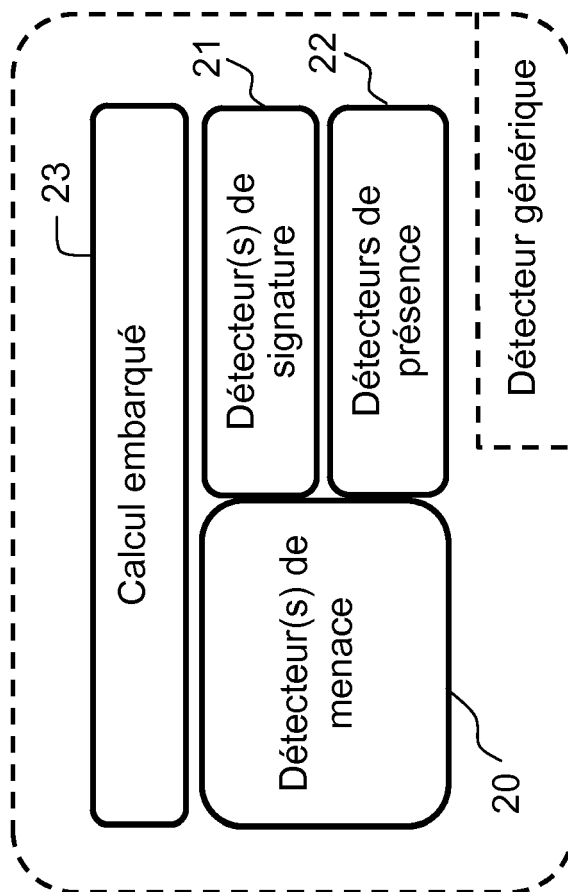


FIG.2

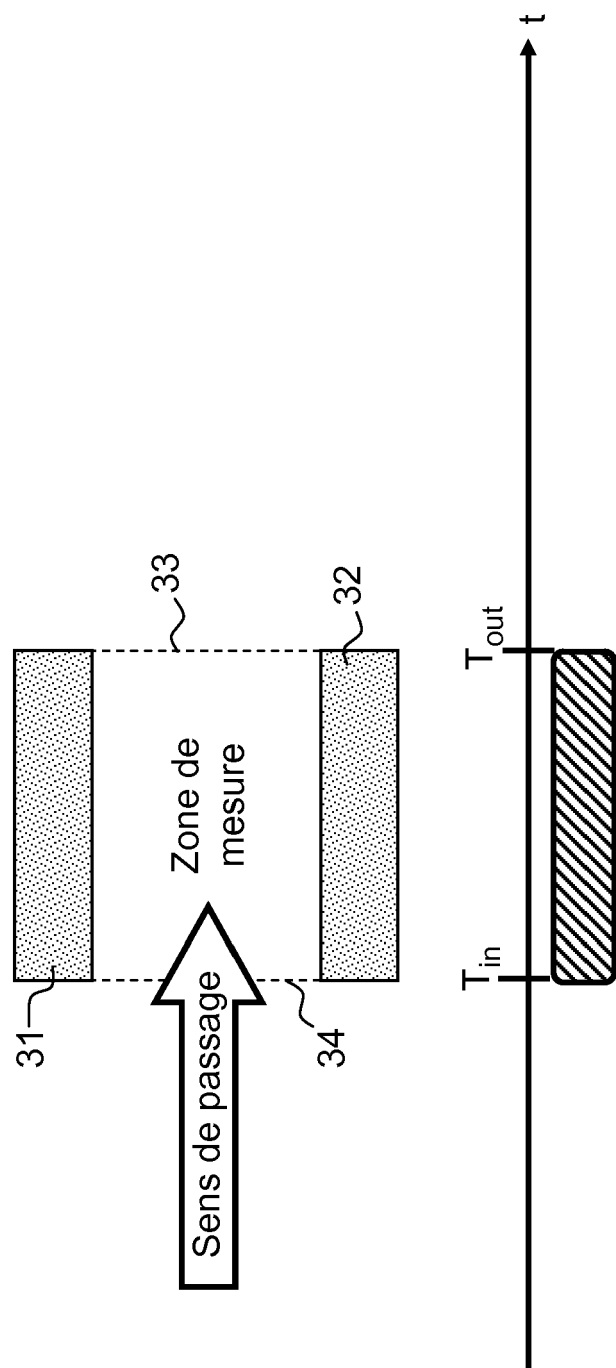


FIG.3

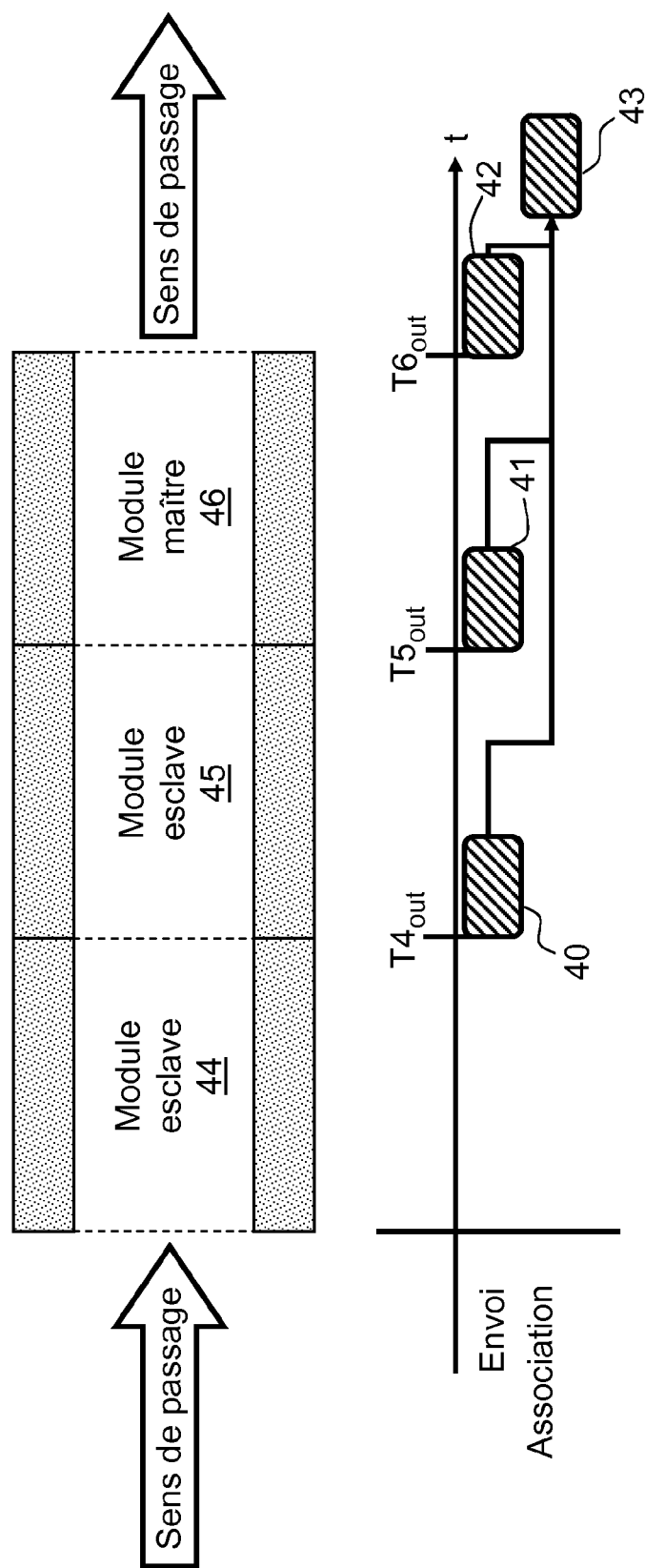


FIG.4

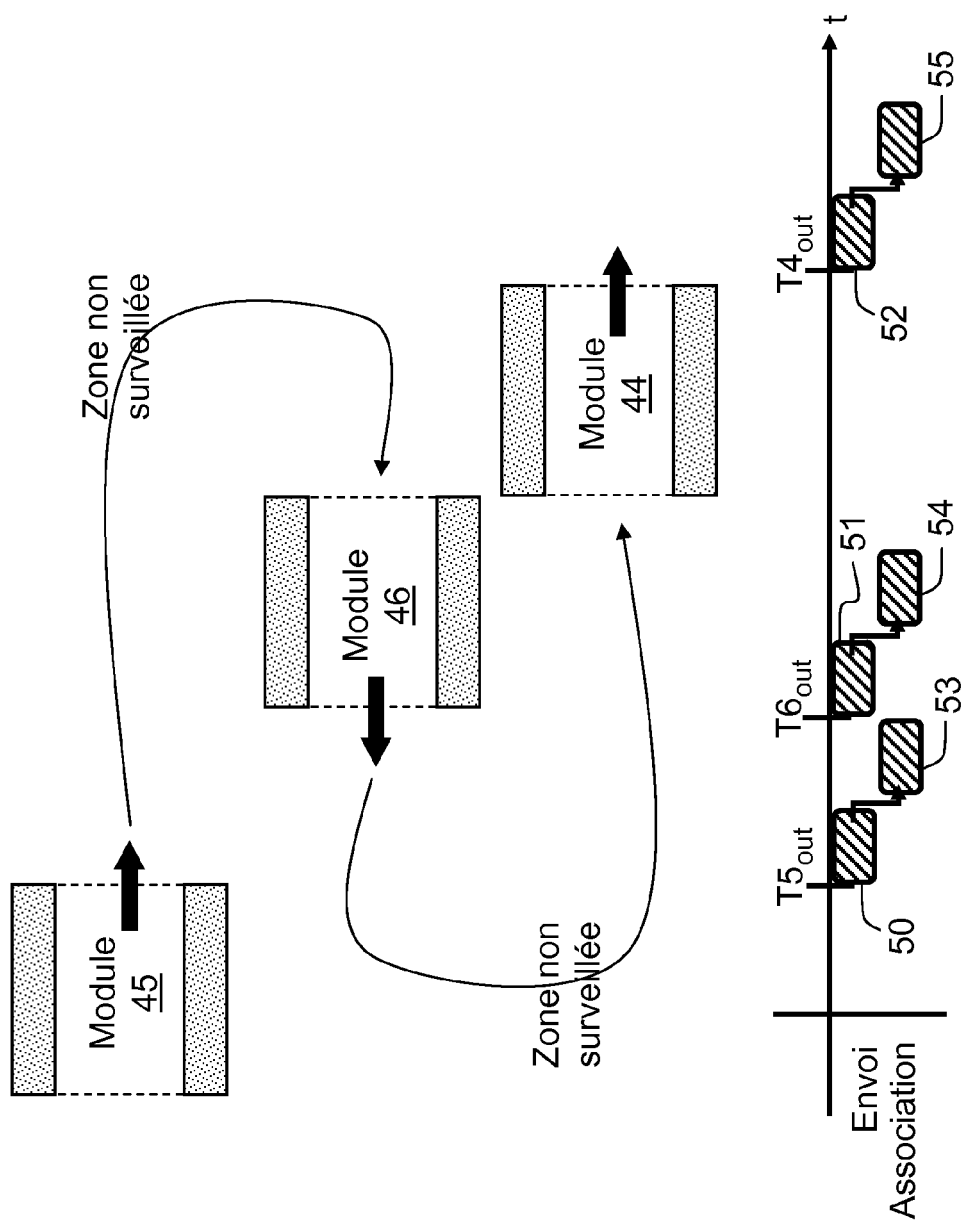


FIG.5

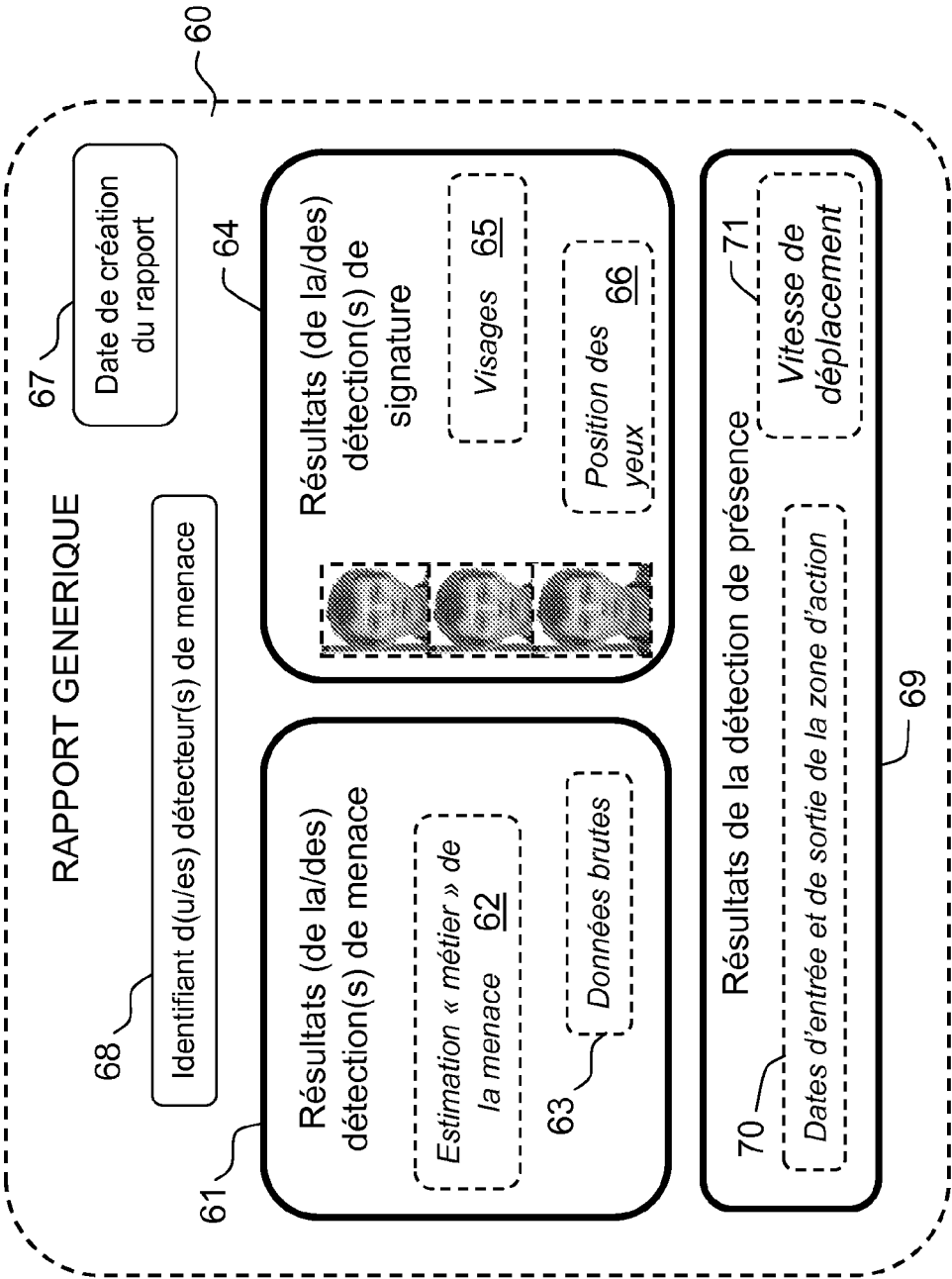


FIG.6

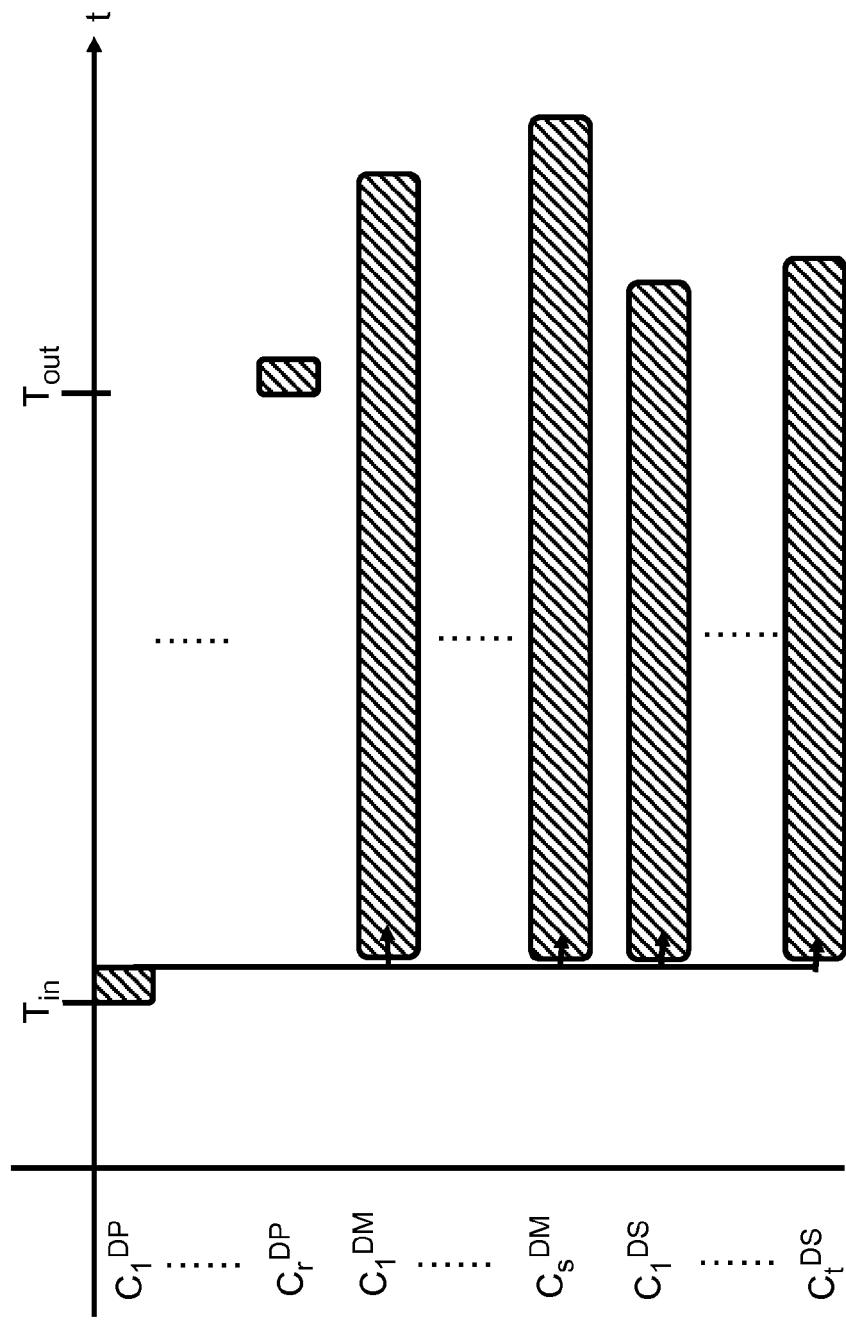


FIG.7

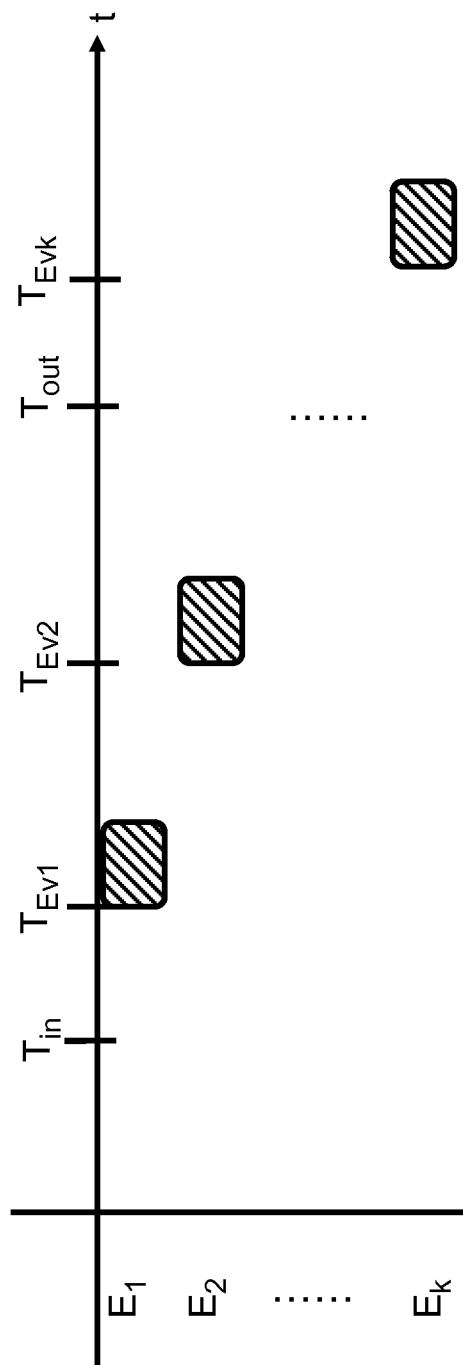


FIG.8

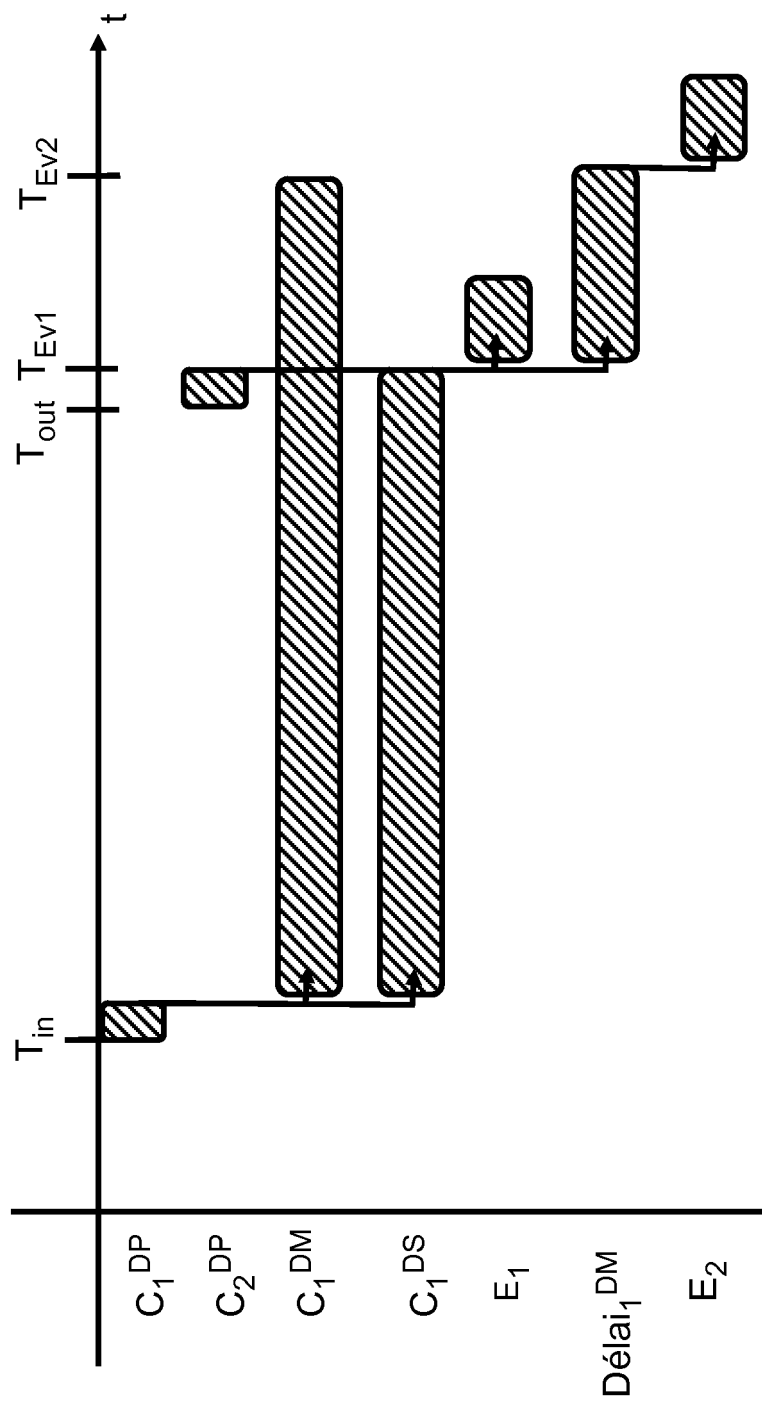


FIG.9



RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 10 19 6843

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
A	WO 2005/066912 A1 (ELBIT SYSTEMS LTD [IL]; NICE SYSTEMS LTD [IL]; DOBKIN URI [IL]; SHABTA) 21 juillet 2005 (2005-07-21) * abrégé * * page 6, ligne 5 - ligne 25 * * page 9, ligne 6 - ligne 10 * * page 9, ligne 22 - ligne 28 * * page 10, ligne 24 - page 14, ligne 24 * * page 15, ligne 22 - page 17, ligne 17 * * page 19, ligne 10 - ligne 19 * * page 20, ligne 5 - ligne 20 * * page 21, ligne 28 - page 22, ligne 14 * * figure 1B *	1-6	INV. G01V11/00 G08B13/00
A	WO 99/21148 A1 (IDS INTELLIGENT DETECTION SYST [CA]; HALEY LAWRENCE V [CA]) 29 avril 1999 (1999-04-29) * page 2, ligne 31 - page 3, ligne 30 * * page 4, ligne 9 - page 6, ligne 6 * * figure 1 *	1,2,4	
A,P	EP 2 204 783 A1 (THALES SA [FR]) 7 juillet 2010 (2010-07-07) * abrégé * * page 5, alinéa 28 - page 9, alinéa 24 * * figures 2,5,11 *	1-6	DOMAINES TECHNIQUES RECHERCHES (IPC) G08B G01V
A	JP 11 046889 A (BUNSHODO CO LTD) 23 février 1999 (1999-02-23) * abrégé * * figure 3 *	3	
A	US 2006/059557 A1 (MARKHAM THOMAS R [US] ET AL) 16 mars 2006 (2006-03-16) * page 6, alinéa 89 - page 7, alinéa 91 * * figures 6,7 *	1	
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche La Haye		Date d'achèvement de la recherche 31 janvier 2011	Examineur Van der Haegen, D
CATEGORIE DES DOCUMENTS CITES X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	

EPO FORM 1503 03.82 (P04C02)

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 10 19 6843

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.

Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

31-01-2011

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2005066912 A1	21-07-2005	EP 1704547 A1 US 2007122003 A1	27-09-2006 31-05-2007
WO 9921148 A1	29-04-1999	CA 2308747 A1 EP 1025554 A1 JP 2001521157 T	29-04-1999 09-08-2000 06-11-2001
EP 2204783 A1	07-07-2010	WO 2010076261 A1	08-07-2010
JP 11046889 A	23-02-1999	JP 3133019 B2	05-02-2001
US 2006059557 A1	16-03-2006	AUCUN	

EPO FORM P0460

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