

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
8 juillet 2010 (08.07.2010)

PCT

(10) Numéro de publication internationale
WO 2010/076127 A1

(51) Classification internationale des brevets :
G06Q 10/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2009/066568

(22) Date de dépôt international :
8 décembre 2009 (08.12.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0807493 30 décembre 2008 (30.12.2008) FR

(71) Déposant (pour tous les États désignés sauf US) :
THALES [FR/FR]; 45 rue de Villiers, F-92200 Neuilly
Sur Seine (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : **PAULY,
Bernard** [FR/FR]; 10 Parc de Diane, F-78350 Jouy En
Josas (FR).

(74) Mandataires : **LUCAS, Laurent** et al.; Immeuble
Visium, 22, Avenue Aristide Briand, F-94117 Arcueil
Cedex (FR).

(81) États désignés (sauf indication contraire, pour tout titre
de protection nationale disponible) : AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

(54) Title : COMPUTER-IMPLEMENTED METHOD FOR EVALUATING THE SECURITY OF CRITICAL SYSTEMS

(54) Titre : PROCÉDE MIS EN OEUVRE PAR ORDINATEUR D'EVALUATION DE LA SECURITE DE SYSTEMES
CRITIQUES

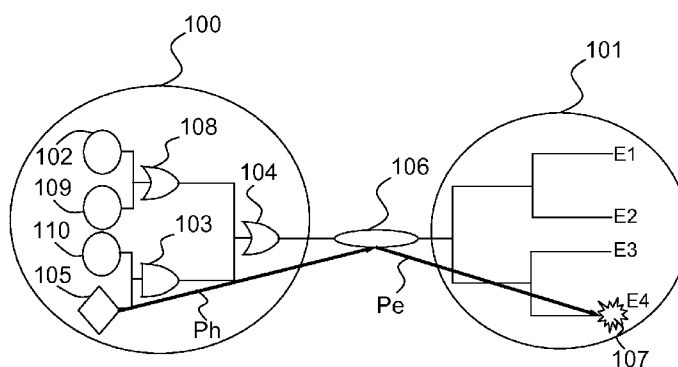


FIG.1

(57) Abstract : The invention relates to a method for evaluating the security of at least one critical system, said system being represented by a functional architecture including functions and subfunctions enabling the generation of a physical architecture, at least one malfunction tree (100) associated with said architecture being generated in order to predict the impact on the system security of the malfunctions of one or more functions or subfunctions, said malfunctions being referred to as primary events, said tree consisting of logic gates (103, 104, 108) enabling the evaluation of the occurrence probability (Ph) of an initial event after one or more system malfunctions. The functional independence level between at least two functions or subfunctions forming the function architecture is evaluated using coupling indicators, the depth of the malfunction tree being selected so that the functional independence between primary events (102, 105, 109, 110) of the malfunction tree is guaranteed.

(57) Abrégé :

[Suite sur la page suivante]

WO 2010/076127 A1



L'invention a pour objet un procédé d'évaluation de la sécurité d'au moins un système critique, ledit système étant représenté par une architecture fonctionnelle composée de fonctions et de sous-fonctions permettant de générer une architecture physique, au moins un arbre de défaillance (100) associé à ladite architecture étant construit afin de prévoir l'impact sur la sécurité du système des défaillances d'une ou plusieurs fonctions ou sous-fonctions, ces défaillances étant appelées événements primaires, ledit arbre étant composé de portes logiques (103, 104, 108) permettant l'évaluation de la probabilité d'occurrence (Ph) d'un événement initial suite à une ou plusieurs défaillances du système. Le niveau d'indépendance fonctionnelle entre au moins deux fonctions ou sous-fonctions composant l'architecture fonctionnelle est évalué à l'aide d'indicateurs de couplage, la profondeur de l'arbre de défaillance étant choisie de manière à ce que l'indépendance fonctionnelle entre les événements primaires (102, 105, 109, 110) de l'arbre de défaillance soit garantie.

Procédé mis en œuvre par ordinateur d'évaluation de la sécurité de systèmes critiques

5 L'invention concerne un procédé mis en œuvre par ordinateur d'évaluation de la sécurité de systèmes critiques et s'applique notamment aux domaines des systèmes critiques pour le contrôle de trafic aérien, pour le ferroviaire ou le nucléaire.

10 Dans un système critique, une panne peut avoir des conséquences dramatiques. Il est donc primordial de tenir compte des contraintes en termes de sécurité lors de sa conception. A titre d'exemple, la méthodologie SAM, acronyme venant de l'expression anglo-saxonne « Safety Assessment Methodology » et développée depuis quelques années pour les systèmes de
15 contrôle de trafic aérien et comprend trois étapes.

La première étape vise notamment à répertorier les objectifs à atteindre en termes de sécurité du système.

Dans un deuxième temps, l'architecture du système est analysée de manière à répondre au mieux aux objectifs de sécurité identifiés pendant
20 l'étape précédente. Cette analyse d'architecture se décompose, par exemple, en une analyse de l'architecture logique ou fonctionnelle et en une analyse de l'architecture physique. L'architecture physique est également appelée architecture technique ou architecture de déploiement. Ces architectures peuvent être analysées à l'aide de modèles permettant de faire
25 le lien entre les défaillances du système, les dangers et les effets en résultant. Ainsi, un système ou un sous système peut être associé à un niveau de sécurité. Ce niveau de sécurité tient compte notamment de la distance entre une défaillance du système et sa conséquence finale opérationnelle en incluant l'influence de barrières de sécurité. Les barrières
30 de sécurités peuvent être de plusieurs natures, par exemple logiciel, matériel ou être des procédures opérationnelles. Ladite distance est évaluée en calculant le produit de deux probabilités. La première probabilité P_e est la probabilité entre l'occurrence du danger et sa conséquence potentielle finale. La seconde probabilité P_h est la probabilité d'occurrence du danger suite à
35 une ou plusieurs défaillances du système.

2

Durant la troisième étape de conception, le passage d'une architecture logique ou fonctionnelle à une architecture physique est réalisé. Dans la pratique, les considérations de sécurité ne sont pas suffisamment prises en compte lors de la deuxième phase. Un certain nombre de
5 corrections doivent alors être apportées lorsque cette transition est opérée. Cette prise en compte tardive d'une partie des contraintes de sécurité mène à des architectures physiques sous-optimales.

Lors de la deuxième étape, c'est-à-dire pendant l'étape d'analyse de
10 l'architecture logique ou fonctionnelle, le lien statistique entre l'occurrence de la défaillance d'une fonction ou d'une sous-fonction du système et l'occurrence d'un danger peut être analysé à l'aide d'un arbre de défaillance FTA, acronyme venant de l'expression anglo-saxonne « Fault Tree Analysis ». Pour cela, les fonctions ou sous-fonctions concernées par
15 chaque objectif de sécurité sont identifiées. Une analyse de type arbre de défaillance permet d'identifier les différentes causes possibles d'un danger. Dans la suite de la description, un danger est appelé également événement initial. La décomposition est poursuivie à partir d'un événement initial jusqu'aux défaillances ou événements primaires, lesdits événements
20 primaires étant également désignés par l'expression anglo-saxonne « Basic Events », et de vérifier que l'objectif de sécurité est atteint. Un objectif de sécurité est appelé objectif SR dans la suite de la description, acronyme venant de l'expression anglo-saxonne « Security Requirements ». L'arbre de défaillances FTA est habituellement composé de portes logiques de types ET
25 et OU. De manière à tenir compte des imperfections du modèle, une hypothèse conservatrice est prise. Lorsqu'une porte ET est identifiée, la probabilité admissible Pfh d'occurrence des causes immédiates associées est augmentée d'un facteur 10. Par exemple, Pfh est majorée à 10^{-5} si la valeur ciblée est de 10^{-6} . Lorsqu'une porte OU est identifiée, alors la
30 probabilité des événements de cause immédiate garde la même probabilité que celle de l'événement initial « père ». Cette solution permet de modéliser et d'étudier la sécurité d'une architecture fonctionnelle, mais les hypothèses faites pour simplifier sa mise en œuvre réduisent sa précision. Une partie du problème concernant la maîtrise de la sécurité du système critique est alors
35 reportée sur l'étape de conception.

Il apparaît que deux limitations sont inhérentes à cette approche. D'une part, l'indépendance des événements primaires n'est pas garantie et d'autre part l'évaluation des portes logiques ET et OU n'est pas réalisée suffisamment précisément. Ces limitations ont pour conséquence un manque
5 de fiabilité de l'évaluation de l'architecture logique ou fonctionnelle du système critique.

Un but de l'invention est notamment de pallier les inconvénients précités. A cet effet l'invention a pour objet un procédé d'évaluation de la sécurité d'au
10 moins un système critique, ledit système étant représenté par une architecture fonctionnelle composée de fonctions et de sous-fonctions permettant de générer une architecture physique, au moins un arbre de défaillance associé à ladite architecture étant construit afin de prévoir l'impact sur la sécurité du système des défaillances d'une ou plusieurs
15 fonctions ou sous-fonctions, ces défaillances étant appelées événements primaires, ledit arbre étant composé de portes logiques permettant l'évaluation de la probabilité d'occurrence d'un événement initial suite à une ou plusieurs défaillances du système. Le niveau d'indépendance fonctionnelle entre au moins deux fonctions ou sous-fonctions composant
20 l'architecture fonctionnelle est évalué à l'aide d'indicateurs de couplage, la profondeur de l'arbre de défaillance étant choisie de manière à ce que l'indépendance fonctionnelle entre les événements primaires de l'arbre de défaillance soit garantie.

Un indicateur de couplage comprend, par exemple, N niveaux de
25 couplage, chaque niveau de couplage correspondant à un ensemble flou.

Le niveau d'indépendance fonctionnelle entre au moins deux fonctions ou sous-fonctions F_i , F_j du système correspond, par exemple, au degré d'appartenance à un des N ensembles flous correspondant aux N niveaux de couplage d'un indicateur de couplage donné.

30 Un indicateur de couplage peut être associé, par exemple, à quatre niveaux de couplage « dépendant », « moyennement dépendant », « peu dépendant » ou « indépendant ».

Selon un mode de réalisation, plusieurs indicateurs de couplage distincts sont associés au même ensemble d'au moins deux fonctions ou sous-

fonctions F_i , F_j du système et sont combinés à l'aide de fonctions logiques ET et OU.

Selon un aspect de l'invention, une étape calcule le degré d'appartenance aux ensembles flous suite à la combinaison de plusieurs indicateurs de couplage, ledit degré d'appartenance correspondant au maximum des degrés d'appartenance à chaque ensemble flou desdits indicateurs de couplage.

Selon un autre aspect de l'invention, une étape calcule un facteur de couplage FC d'au moins deux fonctions ou sous fonctions F_i et F_j en utilisant la règle de Mamdani, ladite règle étant appliquée aux degrés d'appartenance aux ensembles flous résultant d'une combinaison de plusieurs indicateurs de couplage.

Les portes logiques de l'arbre de défaillance sont définies, par exemple, selon leur degré d'appartenance à une porte ET ou à une porte OU.

Le degré d'appartenance d'une porte logique de l'arbre de défaillance est déterminé, par exemple, à l'aide d'au moins un indicateur de couplage.

Selon un mode de réalisation, les probabilités d'occurrence Ph sont évaluées en intégrant les degrés d'appartenance aux portes ET et OU à chaque niveau logique de l'arbre de défaillance.

Le système critique est, par exemple, un système de contrôle du trafic aérien.

Le système critique est, par exemple, un système de contrôle du trafic ferroviaire.

Le système critique est, par exemple, un système de contrôle d'au moins un réacteur nucléaire.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit donnée à titre illustratif et non limitatif, faite en regard des dessins annexés parmi lesquels :

30

- la figure 1 donne un exemple d'arbres utilisé pour l'évaluation de l'architecture de systèmes critiques ;
- la figure 2 illustre le principe des règles appliquées aux portes ET et OU de l'arbre de défaillance ;

- la figure 3 donne des exemples de fonctions d'appartenance associées à des ensembles flous pouvant être utilisés dans le cadre de l'invention pour un indicateur de couplage ;
- la figure 4 présente une manière de calculer le niveau de couplage entre deux fonctions F_i et F_j ;
- La figure 5 représente un schéma bloc donnant les entrées et sorties d'un exemple de mise en œuvre du procédé selon l'invention.

La figure 1 donne un exemple d'arbres utilisés pour l'évaluation de l'architecture de systèmes critiques. Un premier arbre 100 est l'arbre de défaillances FTA. L'exemple de la figure présente deux niveaux logiques, c'est-à-dire qu'il y a, en partant de la base de l'arbre, deux niveaux de ramification. Le nombre de niveaux logiques de l'arbre est aussi appelé profondeur dans la suite de la description. Les événements initiaux se trouvent en amont de l'arbre FTA et représentent chacun un type de défaillance du système. Pour un événement initial donné 105, la probabilité Ph d'occurrence d'un danger 106 suite à cet événement peut être estimée en parcourant l'arbre FTA. Inversement, pour un danger donné, il est possible en remontant l'arbre FTA de déterminer la ou les fonctions potentiellement responsables dudit danger. L'arbre FTA est composé de porte ET 103 et de portes OU 104, 108 permettant d'évaluer les valeurs de Ph .

Un système critique contient des barrières de sécurité. Ces barrières de sécurité peuvent être considérées selon leur capacité à contrôler une défaillance en fonction du temps, c'est-à-dire avant, pendant et après la défaillance. Il est alors intéressant de considérer leurs propriétés en termes de prévention de défaillance, de détection de défaillance, de contrôle de propagation de défaillance et de recouvrement de défaillance.

Pour qu'un arbre de défaillances FTA soit correctement évalué de manière qualitative ou quantitative, l'indépendance des événements initiaux 102, 105, 109, 110 est requise. Ainsi, dans le cadre de l'invention, avant de procéder à l'évaluation de l'architecture du système critique, l'arbre FTA est développé avec une profondeur suffisante pour s'assurer que les

événements primaires sont indépendants entre eux et que chaque situation ou événement peut-être atteint.

Dans le cadre de l'invention, il est notamment proposé d'étudier la validité de la logique des portes ET et OU lors de la construction de l'arbre.

5 Un mode de défaillance correspond à la manière dont un élément de l'architecture fonctionnelle à évaluer peut créer une défaillance. Lors de la décomposition fonctionnelle de l'architecture à évaluer, les interactions entre les fonctions et sous-fonctions peuvent induire des incertitudes entre les logiques ET et OU vis-à-vis des causes immédiates des modes de
10 défaillance. Il peut être choisi, par exemple, qu'une porte ET soit placée entre deux fonctions ou sous fonctions (causes de l'événement père) dans la mesure où l'occurrence d'une des défaillances cause décrite d'un côté de la branche du ET peut-être compensée et récupérée par une fonction ou sous-fonction assurée dans l'autre branche du ET. De plus il est important de
15 garantir que la possibilité de propagation de la défaillance de l'autre côté de la branche du ET soit contrôlée et réduite, ou si possible éliminée. Il est donc utile d'introduire la notion de niveau de couverture fonctionnelle commune entre deux ou plusieurs branches d'une porte ET. Ainsi, dans le cadre de l'invention, des instances ET/OU sont utilisés dans l'arbre des défaillances
20 FTA, lesdites instances étant évaluées selon leur degré d'appartenance à une porte ET ou à une porte OU. Ces degrés peuvent prendre une valeur comprise entre 0 et 1, par exemple. Le degré d'appartenance d'une porte à la logique OU peut être considéré comme le complément du degré d'appartenance d'une porte à la logique ET.

25

Selon l'invention, des indicateurs de couplage sont introduits dans le but notamment de quantifier le degré de dépendance entre plusieurs fonctions ou sous-fonctions de l'architecture fonctionnelle à évaluer. Ainsi, lors de la construction de l'arbre de défaillance FTA, si deux fonctions ou
30 sous-fonctions ne sont pas considérées comme suffisamment indépendantes, il est décidé d'ajouter un ou plusieurs niveaux logiques à l'arbre.

Le tableau ci-dessous donne un exemple d'indicateur de couplage. Quatre niveaux de couplage allant de « dépendant » à « indépendant » sont
35 définis pour quantifier la dépendance entre deux fonctions F_i ou F_j .

L'indicateur de couplage de l'exemple analyse le niveau d'interaction humaine nécessaire à l'activation desdites fonctions. Suivant les cas un ou plusieurs indicateurs peuvent être utiles pour estimer le niveau de dépendance entre deux fonctions.

5

	Dépendant	Moyennement dépendant	Peu dépendant	Indépendant
<u>Indicateur :</u> Interaction humaine pour l'activation	Activation automatique des deux fonctions	L'activation des fonctions Fi et Fj est parfois réalisée manuellement	L'activation des fonctions Fi et Fj est souvent réalisée manuellement	L'activation des fonctions Fi et Fj n'est réalisée que manuellement

Il est possible de combiner plusieurs indicateurs. Une manière de réaliser cette combinaison est détaillée plus loin dans la description.

Comme explicité précédemment, une des conditions de fiabilité de l'analyse par arbre FTA est la garantie d'indépendance des événements primaires 102, 105, 109, 110. L'utilisation d'indicateurs de couplage permet de déterminer la profondeur de l'arbre FTA.

En plus de l'analyse descendante de type FTA, il est possible de procéder, dans le cadre de l'analyse globale de sécurité, à une analyse complémentaire pour déterminer les causes communes de défaillances.

L'analyse de l'indépendance des événements primaires permet de contribuer à la préparation de cette analyse de causes communes de défaillances CCA, acronyme venant de l'expression anglo-saxonne « Common Cause Analysis ». Le calcul des indicateurs de couplage va aider à l'analyse de ces aspects d'indépendance.

L'analyse des degrés d'indépendance doit-être considérée en 2 temps. Dans un premier temps, l'indépendance des événements primaires à l'intérieur du même ensemble de fonctions est considérée. Dans un second temps, l'indépendance des fonctions entre-elles est étudiée afin d'en déduire l'indépendance des événements primaires de chaque groupe fonctions avec ceux des autres groupes fonctions.

La figure 1 montre également un second arbre 101 permettant de lier statistiquement l'occurrence d'un danger 106 avec un effet E1, E2, E3, E4,

résultant de ce danger. Par exemple, l'occurrence d'un danger 106 aura pour conséquence un effet E4 107 avec une probabilité P_e , P_e étant donc la probabilité entre l'occurrence du danger et sa conséquence potentielle finale.

5 La figure 2 illustre le principe des règles appliquées aux portes ET/OU 301. Un évènement père 200 est appliqué en entrée de ladite instance 201. Le degré d'appartenance à une porte ET ou OU peut être déterminé, par exemple, en tenant compte de la possibilité de récupérer une défaillance. Si la possibilité de récupérer la défaillance « Evènement A » 202 par la
10 fonction ou sous-fonction associée à « Evènement B » 203 est importante (ou réciproquement), et si la possibilité de propagation de la défaillance « Evènement A » vers B (ou réciproquement) est faible, alors il est vraisemblable que la porte ET soit plus justifiée que la porte OU.

Si la possibilité de récupérer la défaillance « Evènement A » 202 par la
15 fonction ou sous-fonction associée à « Evènement B » 203 (ou réciproquement) est moins forte ou faible ou si la possibilité de propagation de la défaillance de « Evènement A » 202 vers B 203 (ou réciproquement) est forte, alors il est vraisemblable que la porte OU soit plus justifiée que la porte ET.

20 Une porte ET implique que si l'évènement père 200 a une probabilité égale à 10^{-n} , alors les évènements A 202 et B 203 ont une probabilité égale à $10^{(1-n)}$. Dans le cas d'une porte OU, par mesure conservatrice, les probabilités restent inchangées.

Pour tenir compte du degré d'appartenance μ à la logique ET ou $(1-\mu)$
25 à la logique OU, les probabilités peuvent être exprimées par l'expression suivante :

$$P = \frac{10^{-n}}{10^{-1} \times 10^{(1-\mu)}} \quad (1)$$

30 Ainsi il est bien vérifié que dans le cas d'une porte ET, si $\mu = 1$, alors $P = 10^{(1-n)}$. Et, dans le cas d'une porte OU, si $\mu = 0$ alors $P = 10^{(-n)}$. Donc dans les cas aux limites, l'évaluation actuelle reste inchangée.

De manière à évaluer le degré d'appartenance d'une porte à la logique ET ou à la logique OU, un exemple d'indicateurs de couplage est présenté dans le tableau suivant.

Indicateurs de couplage	Fort	Faible
Parties communes des spécifications utilisateur	Plutôt ET	Plutôt OU
Partage de sous-fonctions : niveau des sous fonctions utilisées en commun par Fi et Fj	Plutôt ET	Plutôt OU
Réutilisation des traitements : Fi réutilise les traitements de Fj pour satisfaire à ses spécifications	Plutôt OU	Plutôt ET
Données et ressources communes : Fi et Fj utilisent un niveau de ressources et de données en commun	Plutôt OU	Plutôt ET
Echange de données : volume de données échangé par Fi et Fj pendant une période de référence	Plutôt OU	Plutôt ET

5

La figure 3 donne des exemples de fonctions d'appartenance associées à des ensembles flous pouvant être utilisés pour un indicateur de couplage donné dans le cadre de l'invention. Afin d'évaluer les aspects de couplage pour une architecture logique ou fonctionnelle, l'invention utilise notamment les principes de la logique floue. Un des avantages de la logique floue est de permettre à la fois une représentation de l'imprécision sous forme d'ensembles flous et la quantification de l'incertitude par des nombres flous. Ainsi les ensembles flous peuvent être modifiés par des variables linguistiques telles que « très », « un peu », « pas », « extrêmement » ou « plus ou moins ». Cela permet notamment de représenter de nouveaux ensembles flous dérivés de l'ensemble flou initial.

Dans le cadre de l'invention, des ensembles flous candidats sont préalablement définis pour l'évaluation de l'architecture fonctionnelle ciblée. Ces derniers sont la base des règles qui vont permettre d'évaluer le niveau de couplage, par exemple entre deux fonctions ou sous-fonctions Fi, Fj de l'architecture à évaluer.

Concernant l'exemple de la figure 3, quatre ensembles flous sont considérés : « dépendant », « moyennement dépendant », « peu

dépendant » et « indépendant ». Ceux-ci sont associés à un indicateur de couplage nommé « activation par interaction humaine ». Les courbes présentées à l'aide de la figure 3 sont les fonctions d'appartenance associées à ces quatre ensembles flous. Ces dernières correspondent aux
5 termes linguistiques basés sur les univers de valeurs termes linguistiques indiqués en abscisse du diagramme. En ordonnées du diagramme sont représentés les degrés d'appartenance aux ensembles flous considérés.

Comme explicité précédemment, plusieurs indicateurs de couplage peuvent être combinés afin d'évaluer l'indépendance entre deux fonctions F_i et F_j ou le degré d'appartenance des portes de l'arbre FTA à la logique ET
10 ou à la logique OU. Une manière de combiner ces indicateurs de couplage est explicitée dans la suite de la description.

La figure 4 présente une manière de calculer le niveau de couplage, appelé également facteur de couplage, entre deux fonctions F_i et F_j . Cette
15 méthode peut également être appliquée afin d'évaluer l'appartenance des portes de l'arbre FTA. Ce calcul peut être réalisé à partir de la combinaison de plusieurs indicateurs de couplage appliqués à ces deux fonctions. En effet, plusieurs indicateurs de couplage, utilisés notamment pour évaluer
20 l'indépendance entre deux fonctions ou sous-fonctions F_i et F_j , peuvent être reliés logiquement par des portes OU, par exemple. Le degré d'appartenance résultant pour les ensembles flous « dépendant », « moyennement dépendant », « peu dépendant » ou « indépendant » associés à chaque indicateur sera le maximum des degrés d'appartenance
25 pour chaque indicateur de couplage. L'exemple de la figure 4 considère l'utilisation de portes OU pour relier logiquement les indicateurs de couplage, mais il est également possible que lesdits indicateurs soient évalués conjointement avec des portes ET.

Il est possible de calculer le facteur de couplage des deux fonctions ou sous-fonctions F_i et F_j en utilisant la règle de Mamdani. Celle-ci consiste
30 en un calcul de la projection 400 sur l'axe des abscisses du centre de gravité 401 de l'aire 402 délimitant les degrés d'appartenance aux ensembles flous « dépendant », « moyennement dépendant », « peu dépendant » ou « indépendant ». Le facteur de couplage FC peut alors s'exprimer en utilisant
35 l'expression suivante :

$$FC = \frac{\sum_i X_i \times Y_i}{\sum_i X_i} \quad (2)$$

Dans laquelle :

- 5 X_i représente les valeurs en abscisse, c'est-à-dire de résultat de l'application des règles de logique floue ;
 Y_i représente les valeurs en ordonnées, c'est-à-dire le niveau de couplage entre F_i et F_j .

Pour l'exemple de la figure 4, $X_i = [0,25 ; 0,5 ; 0,75 ; 1]$ et $Y_i = [0,25 ; 0,5 ; 1 ; 0,5]$, ce qui implique que $FC = 0.69$.

10

La figure 5 représente un de schéma bloc donnant les entrées et sorties d'un exemple de mise en œuvre du procédé selon l'invention.

- 15 Lors de la conception d'un système critique, des objectifs de sécurité SR sont choisis et servent de critère de conception. De manière à évaluer la sécurité de l'architecture fonctionnelle, des indicateurs de couplage IC sont définis tels qu'explicités précédemment dans la description.

- 20 Pour une architecture fonctionnelle AF donnée composée notamment de fonctions et de sous fonctions, au moins un arbre de défaillance FTA est construit. Les règles de couplage basées sur le calcul des indicateurs de couplage vont servir d'une part pour l'évaluation des instances ET et OU en tenant compte du sous-ensemble des indicateurs choisi dans ce but, et d'autre part pour déterminer la profondeur de l'arbre en vérifiant l'indépendance des événements primaires.

- 25 En remontant l'arbre de défaillances FTA depuis sa base jusqu'aux événements primaires, les probabilités Ph sont évaluées en intégrant les degrés d'appartenance aux portes ET et OU à chaque niveau logique de l'arbre de défaillance. La fiabilité de l'évaluation de la distance entre la défaillance d'un niveau considéré dans l'arbre et un danger est ainsi améliorée. Ces probabilités sont ensuite comparées aux objectifs de sécurité SR et un résultat R est ensuite fourni, ledit résultat indiquant, par exemple, si
 30 lesdits objectifs de sécurité sont atteints.

REVENDICATIONS

- 1- Procédé d'évaluation de la sécurité d'au moins un système critique, ledit système étant représenté par une architecture fonctionnelle composée de fonctions et de sous-fonctions permettant de générer une architecture physique, au moins un arbre de défaillance (100) associé à ladite architecture étant construit afin de prévoir l'impact sur la sécurité du système des défaillances d'une ou plusieurs fonctions ou sous-fonctions, ces défaillances étant appelées événements primaires, ledit arbre étant composé de portes logiques (103, 104, 108) permettant l'évaluation de la probabilité d'occurrence (Ph) d'un événement initial suite à une ou plusieurs défaillances du système, ledit procédé étant caractérisé en ce que le niveau d'indépendance fonctionnelle entre au moins deux fonctions ou sous-fonctions composant l'architecture fonctionnelle est évalué à l'aide d'indicateurs de couplage, la profondeur de l'arbre de défaillance étant choisie de manière à ce que l'indépendance fonctionnelle entre les événements primaires (102, 105, 109, 110) de l'arbre de défaillance soit garantie.
- 2- Procédé selon la revendication 1 caractérisé en ce qu'un indicateur de couplage comprend N niveaux de couplage, chaque niveau de couplage correspondant à un ensemble flou.
- 3- Procédé selon la revendication 2 caractérisé en ce que le niveau d'indépendance fonctionnelle entre au moins deux fonctions ou sous-fonctions F_i , F_j du système correspond au degré d'appartenance à un des N ensembles flous correspondant aux N niveaux de couplage d'un indicateur de couplage donné.
- 4- Procédé selon l'une quelconque des revendications 2 ou 3 caractérisé en ce qu'un indicateur de couplage est associé à quatre niveaux de couplage « dépendant », « moyennement dépendant », « peu dépendant » ou « indépendant ».

13

- 5- Procédé selon l'une quelconque des revendications 2 à 4 caractérisé en ce que plusieurs indicateurs de couplage distincts sont associés au même ensemble d'au moins deux fonctions ou sous-fonctions F_i , F_j du système et sont combinés à l'aide de fonctions logiques ET et OU.
- 5
- 6- Procédé selon l'une quelconque des revendications 3 à 5 caractérisé en ce qu'une étape calcule le degré d'appartenance aux ensembles flous suite à la combinaison de plusieurs indicateurs de couplage, ledit degré d'appartenance correspondant au maximum des degrés d'appartenance à chaque ensemble flou desdits indicateurs de couplage.
- 10
- 7- Procédé selon la revendication 6 caractérisé en ce qu'une étape calcule un facteur de couplage FC d'au moins deux fonctions ou sous-fonctions F_i et F_j en utilisant la règle de Mamdani (400, 401, 402), ladite règle étant appliquée aux degrés d'appartenance aux ensembles flous résultant d'une combinaison de plusieurs indicateurs de couplage.
- 15
- 8- Procédé selon l'une quelconque des revendications 2 à 7 caractérisé en ce que les portes logiques de l'arbre de défaillance sont définies selon leur degré d'appartenance à une porte ET ou à une porte OU.
- 20
- 9- Procédé selon la revendication 8 caractérisé en ce que le degré d'appartenance d'une porte logique de l'arbre de défaillance est déterminé à l'aide d'au moins un indicateur de couplage.
- 25
- 10- Procédé selon l'une quelconque des revendications 8 ou 9 caractérisé en ce que les probabilités d'occurrence P_h sont évaluées en intégrant les degrés d'appartenance aux portes ET et OU à chaque niveau logique de l'arbre de défaillance.
- 30
- 11- Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que le système critique est un système de contrôle du trafic aérien.
- 35

- 12- Procédé selon l'une quelconque des revendications 1 à 10 caractérisé en ce que le système critique est un système de contrôle du trafic ferroviaire.
- 5
- 13- Procédé selon l'une quelconque des revendications 1 à 10 caractérisé en ce que le système critique est un système de contrôle d'au moins un réacteur nucléaire.

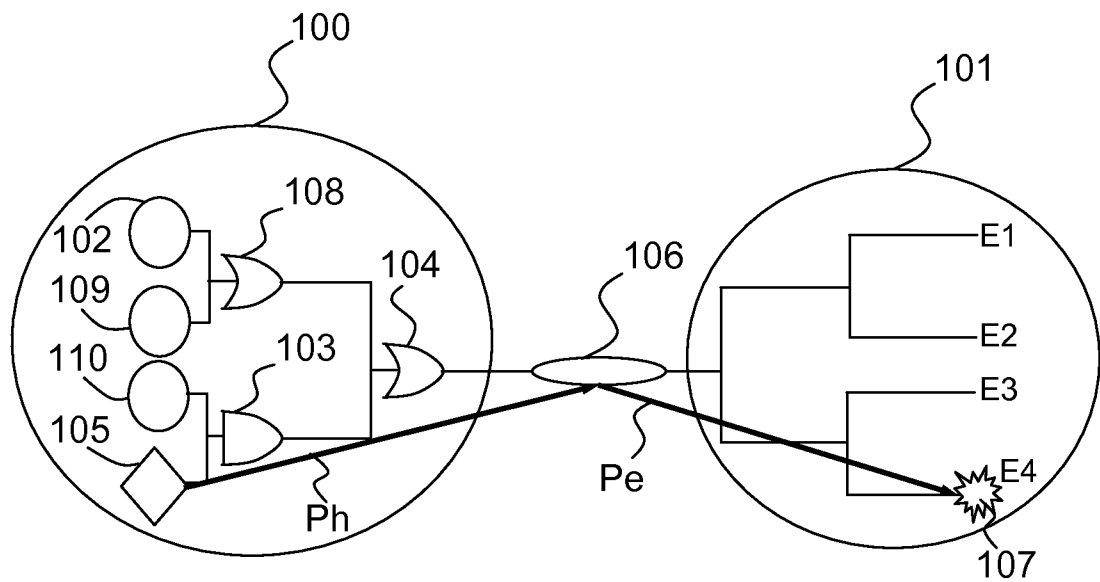


FIG.1

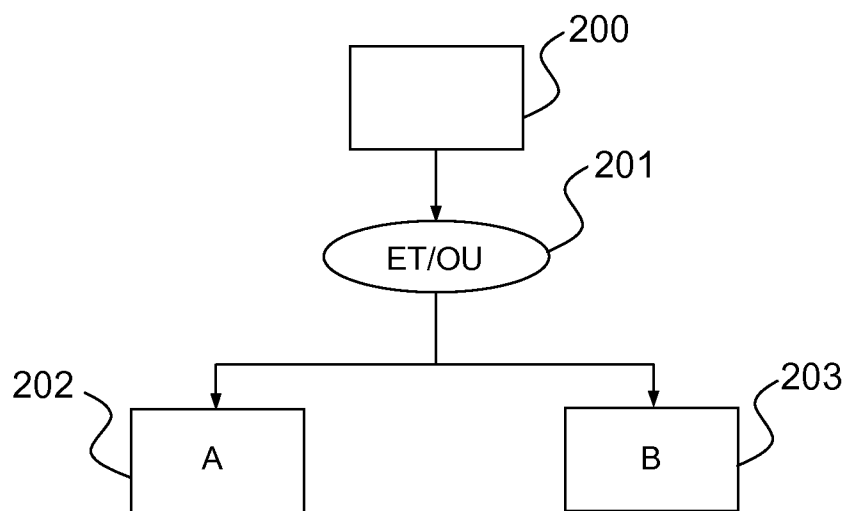


FIG.2

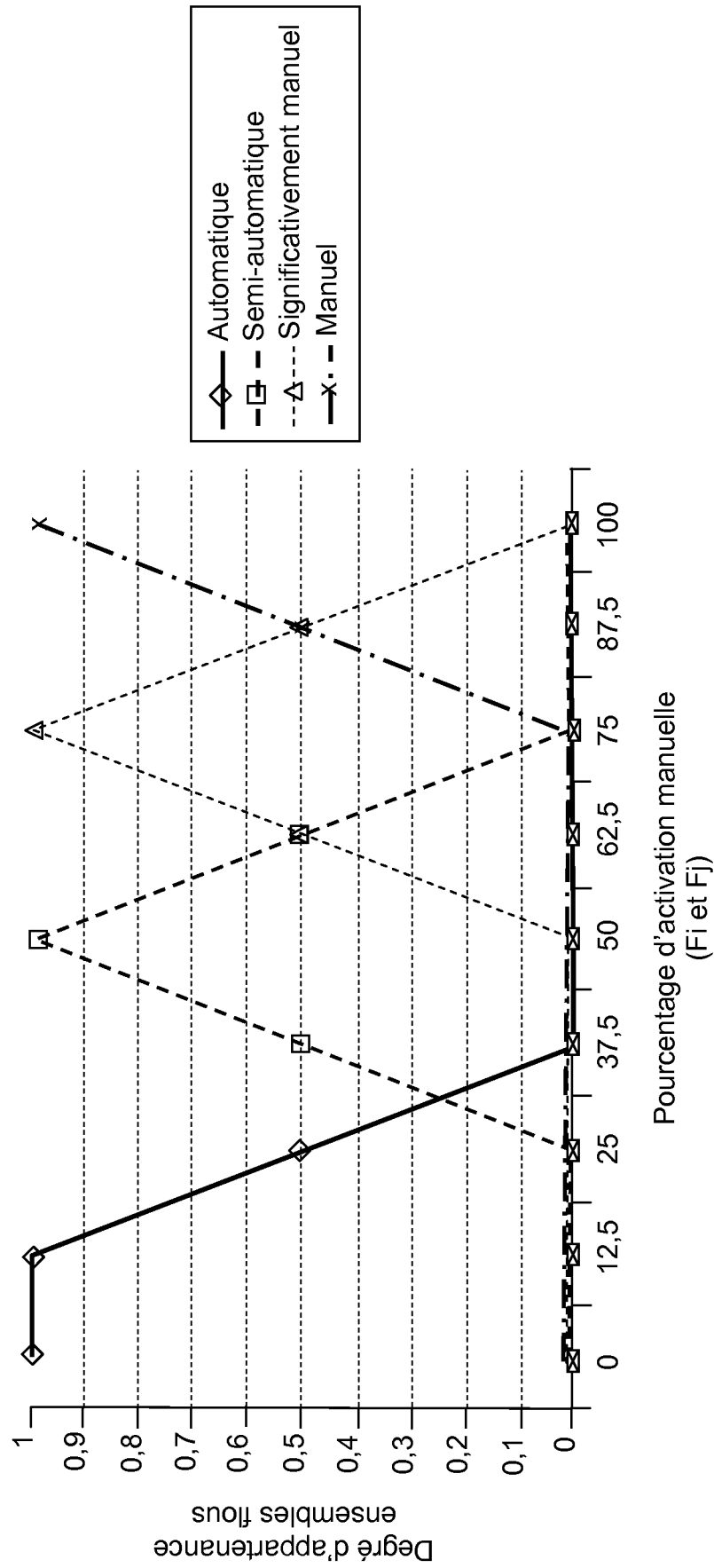


FIG.3

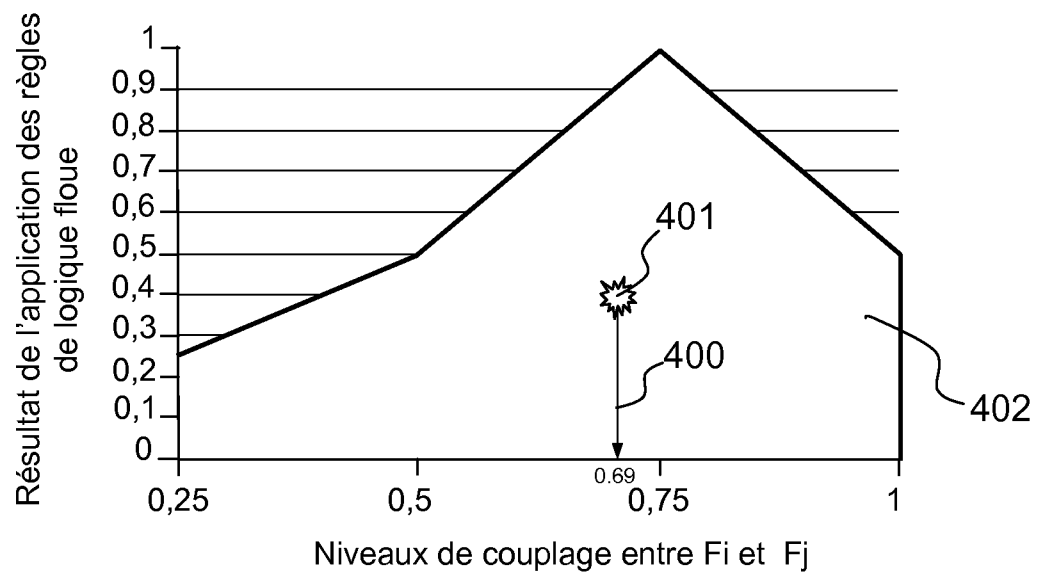


FIG.4

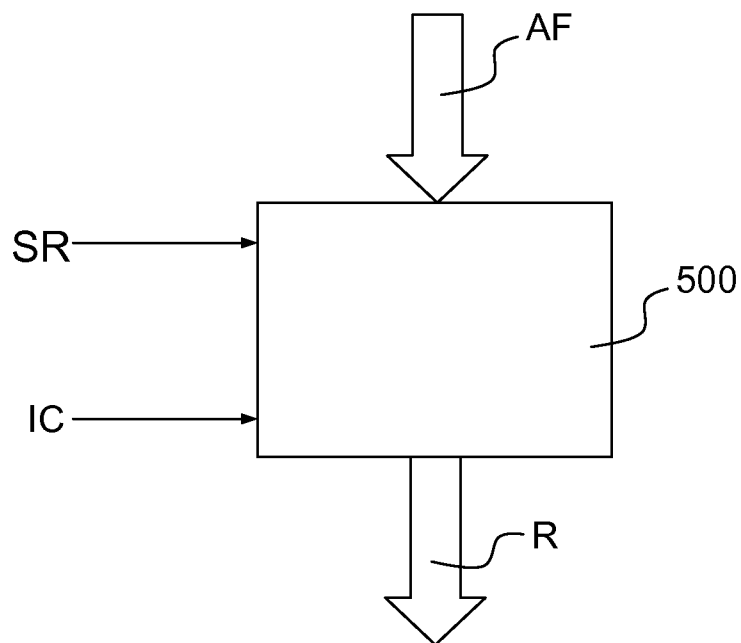


FIG.5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/066568

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q10/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
L	EPO: "Mitteilung des Europäischen Patentamts vom 1. Oktober 2007 über Geschäftsmethoden = Notice from the European Patent Office dated 1 October 2007 concerning business methods = Communiqué de l'Office européen des brevets, en date du 1er octobre 2007, concernant les méthodes dans le domaine des activités" JOURNAL OFFICIEL DE L'OFFICE EUROPEEN DES BREVETS.OFFICIAL JOURNAL OF THE EUROPEAN PATENT OFFICE.AMTSBLATTT DES EUROPAEISCHEN PATENTAMTS, OEB, MUNCHEN, DE, vol. 30, no. 11, 1 November 2007 (2007-11-01), pages 592-593, XP007905525 ISSN: 0170-9291 La description et les dessins ayant été dûment considérés, l'objet revendiqué concerne des processus correspondant à des	1-13

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

9 February 2010

Date of mailing of the international search report

24/02/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Rachkov, Vassil

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/066568

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	objets et des activités de nature non technique. Aucune recherche n'est à effectuer pour ces aspects de l'invention telle que revendiquée (Règle 39 PCT). Les seuls aspects techniques identifiables de l'invention telle que revendiquée concernent l'utilisation de techniques informatiques conventionnelles afin de traiter des données de nature non-technique. Les techniques informatiques employées sont considérées être universellement connues car largement répandues et accessibles à tous à la date de dépôt / priorité de la demande ci-présente. La notoriété d'un tel art antérieur ne peut être raisonnablement contestée. Aucune preuve écrite n'est donc considérée nécessaire. -----	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2009/066568

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. G06Q10/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

G06Q

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
L	EPO: "Mitteilung des Europäischen Patentamts vom 1. Oktober 2007 über Geschäftsmethoden = Notice from the European Patent Office dated 1 October 2007 concerning business methods = Communiqué de l'Office européen des brevets, en date du 1er octobre 2007, concernant les méthodes dans le domaine des activités" JOURNAL OFFICIEL DE L'OFFICE EUROPEEN DES BREVETS.OFFICIAL JOURNAL OF THE EUROPEAN PATENT OFFICE.AMTSBLATT DES EUROPAEISCHEN PATENTAMTS, OEB, MUNCHEN, DE, vol. 30, no. 11, 1 novembre 2007 (2007-11-01), pages 592-593, XP007905525 ISSN: 0170-9291 La description et les dessins ayant été dûment considérés, l'objet revendiqué concerne des processus correspondant à des	1-13

☒ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

9 février 2010

Date d'expédition du présent rapport de recherche internationale

24/02/2010

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Rachkov, Vassil

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2009/066568

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
	objets et des activités de nature non technique. Aucune recherche n'est à effectuer pour ces aspects de l'invention telle que revendiquée (Règle 39 PCT). Les seuls aspects techniques identifiables de l'invention telle que revendiquée concernent l'utilisation de techniques informatiques conventionnelles afin de traiter des données de nature non-technique. Les techniques informatiques employées sont considérées être universellement connues car largement répandues et accessibles à tous à la date de dépôt / priorité de la demande ci-présente. La notoriété d'un tel art antérieur ne peut être raisonnablement contestée. Aucune preuve écrite n'est donc considérée nécessaire. -----	