(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 038 093**

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

(21) **N° d'enregistrement national :** **16 55827**

(51) Int Cl[8] : ***G 06 F 17/30*** *(2016.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 22.06.16.

(30) **Priorité :** 24.06.15 EP 15305973.8; 07.09.15 EP 15184146.7.

(43) **Date de mise à la disposition du public de la demande :** 30.12.16 Bulletin 16/52.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ELECTRICITE DE FRANCE Société anonyme* — FR.

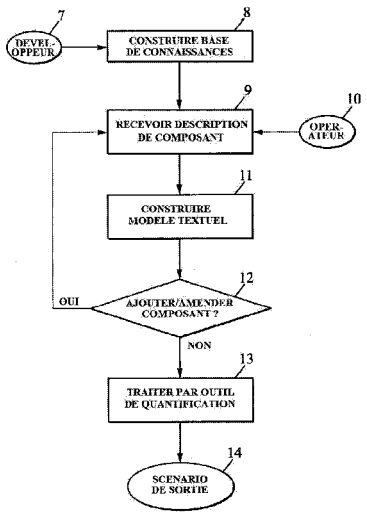
(72) **Inventeur(s) :** KRIAA SIWAR, LAAROUCHI YOUSSEF et BOUISSOU MARC.

(73) **Titulaire(s) :** ELECTRICITE DE FRANCE Société anonyme.

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) METHODE D'EVALUATION DE LA SURETE ET DES RISQUES DE SECURITE D'UN PROCEDE INDUSTRIEL.

(57) Il est divulgué une méthode mise en oeuvre par ordinateur et un dispositif informatique (2) pour évaluer des risques de sécurité d'une architecture industrielle. Ils sont conçus pour délivrer des données d'une liste classée de scores d'évaluation de risques associés à des scénarios d'attaque à l'intérieur de procédés industriels d'exploitation de l'architecture industrielle, en utilisant une base de connaissances.



FR 3 038 093 - A1

METHODE D'EVALUATION DE LA SURETE ET DES RISQUES DE SECURITE D'UN PROCEDE INDUSTRIEL

La présente invention concerne le domaine de la sûreté et de la sécurité de procédés industriels. En particulier, elle divulgue une méthode pour évaluer à la fois les risques de sûreté et les risques de sécurité d'un procédé industriel par l'utilisation d'une base de connaissances de procédés industriels.

Le terme « procédé industriel » fait référence à tout procédé effectué dans tout type d'industrie. La production d'énergie électrique à partir d'une centrale nucléaire, la fabrication de pneus à partir d'une machine-outil unique, la récolte de fraises et le décollage d'un avion depuis un porte-avions constituent des exemples de procédés industriels.

Dans la présente description, une distinction est établie entre « risques de sûreté » et « risques de sécurité » de procédés industriels. Un risque de sûreté concerne un risque accidentel, comme une défaillance d'un dispositif, tandis qu'un risque de sécurité concerne une attaque malveillante, comme une cyberattaque.

Des infrastructures industrielles reposent sur des systèmes de commande industrielle (ICS). Les ICS proposent les moyens nécessaires pour commander et superviser de grandes infrastructures essentielles. Leur défaillance ou leur dysfonctionnement peut engendrer des conséquences défavorables sur le système et sur son environnement, c'est pourquoi leur sûreté est prise en compte avec attention depuis longtemps. Historiquement, les ICS étaient isolés et basés sur des composants simples et des normes propriétaires qui étaient complètement maîtrisées.

Pour faciliter la supervision et la commande du procédé industriel et pour réduire le coût d'exploitation du système, les ICS modernes intègrent de plus en plus des technologies d'informations et de communication (ICT). Par exemple, des ICS peuvent s'appuyer sur des systèmes d'informations (IS). Les IS sont des systèmes composés de personnes et d'ordinateurs traitant ou interprétant des informations.

Ainsi, les ICS sont en migration vers des protocoles standardisés et en format ouvert et ils utilisent de plus en plus des produits disponibles dans le commerce (COTS). Cette tendance engendre néanmoins une plus grande complexité des ICS et les expose à des cyberattaques exploitant des vulnérabilités déjà existantes dans les composants ICT. De telles attaques peuvent atteindre des composants essentiels à

l'intérieur du système et modifier son fonctionnement en provoquant des dangers potentiels de sûreté.

Pour des procédés industriels supervisés et commandés par des ICS modernes, comme SCADA (commande de supervision et acquisition de données), les risques de sûreté et de sécurité convergent et peuvent avoir des interactions réciproques. Une analyse de risques conjointe couvrant à la fois les aspects de sûreté et de sécurité est devenue cruciale et elle conditionne une gestion de risques optimale ainsi qu'une optimisation des ressources.

Plusieurs approches ont été proposées pour traiter séparément les risques de sûreté ou les risques de sécurité, mais il n'y a que quelques approches qui traitent conjointement les risques de sûreté et de sécurité.

Parmi ces quelques approches, on trouve des approches génériques. Ces approches génériques s'appuient sur des exigences, généralement spécifiées dans des normes comme ISO/CEI 15026 ou ISO/CEI 27005, qui sont prises en compte lors de la conception et de l'exploitation de procédés industriels. Des risques de sûreté et de sécurité sont ainsi évalués en vérifiant si ces exigences sont remplies. Ces vérifications sont traitées manuellement par des ingénieurs et des experts en sûreté/sécurité, ce qui prend beaucoup de temps et ce qui est très coûteux. En outre, ces approches génériques sont plus efficaces pour la phase de conception des procédés industriels, mais pas forcément pour la phase d'exploitation à long terme des procédés industriels.

Des approches basées sur des modèles ont également été proposées. Ces approches basées sur des modèles s'appuient sur une représentation formelle ou semi-formelle de procédés industriels. Chaque approche parmi les quelques approches basées sur des modèles proposés pour l'évaluation à la fois des risques de sûreté et de sécurité nécessite qu'un analyste dédié construise manuellement un modèle correspondant au procédé industriel.

En particulier, l'analyste doit interpréter le procédé industriel, sur la base de sa compréhension du système et de ses risques associés, pour construire manuellement un modèle pouvant être traité par des outils de quantification. Cela nécessite donc un travail fastidieux de la part de l'analyste, ce qui prend également beaucoup de temps et ce qui est très coûteux. En outre, l'analyste doit reconstruire manuellement le modèle chaque fois que le procédé industriel change.

Pour répondre à ces besoins, un premier aspect de l'invention concerne une méthode mise en œuvre par ordinateur pour l'évaluation de risques de sécurité d'une architecture industrielle, comprenant :

une étape préliminaire de :

- construction d'une base de connaissances décrivant des risques industriels associés à des procédés industriels respectifs d'exploitation de ladite architecture industrielle,

et des étapes courantes de :

- réception, en entrée, d'une description d'un procédé industriel,
- utilisation de ladite base de données pour évaluer un risque associé au dit procédé industriel, et
- fourniture, en sortie, de données d'évaluation dudit risque,

dans laquelle ladite base de connaissances comprend des données de fonction pour calculer des scores de risques industriels associés à la fois à :

- des scénarios d'attaque de ladite architecture industrielle, et
- des procédés industriels d'exploitation de ladite architecture industrielle,

de manière à fournir, en sortie, des données d'une liste classée de scores d'évaluation de risques associés à des scénarios d'attaque à l'intérieur de procédés industriels d'exploitation de ladite architecture industrielle.

Le terme « procédé industriel d'exploitation » n'est pas limité à une exploitation spécifique d'une structure. Au lieu de cela, il fait référence à tout procédé dans tout domaine d'application. Comme cela a été susmentionné, la production d'énergie électrique à partir d'une centrale nucléaire, la fabrication de pneus à partir d'une machine-outil unique, la récolte de fraises et le décollage d'un avion depuis un porte-avions constituent des exemples de procédés industriels d'exploitation.

Le terme « architecture industrielle » fait référence à une méta-architecture virtuelle couvrant une pluralité de procédés industriels réels possibles. L'architecture industrielle est ainsi définie par la pluralité de procédés industriels compris dans la base de connaissances et couverts par ladite architecture industrielle.

Par exemple, la base de connaissances peut couvrir la méta-architecture industrielle virtuelle de production d'énergie. Dans ce cas, l'architecture industrielle est définie par tous les procédés industriels de production d'électricité couverts par la

base de connaissances (par exemple par une centrale nucléaire, un panneau solaire, une éolienne, etc.). Dans un mode de réalisation, l'architecture industrielle n'est pas limitée et elle couvre tous les procédés industriels existants.

Puisque la base de connaissances est apte à évaluer des risques industriels par la réception d'une description d'un procédé industriel en entrée, la méthode peut être facilement mise en œuvre, même par un opérateur qui ignore le fonctionnement d'outils de quantification complexes. Le préambule de la revendication un fait référence à une méthode d'évaluation de risques de sécurité. Néanmoins, dans ce préambule de la revendication un, il faut bien comprendre que les « risques de sécurité » signifient à la fois des risques de sûreté et/ou de sécurité comme cela a été précédemment défini dans l'introduction de la présente description.

En outre, la méthode permet une modélisation formelle du procédé industriel, ainsi que des attaques et des modes de défaillance qui lui sont associés, grâce à la base de connaissances. Le modèle généré est ensuite traité, ce qui engendre une analyse qualitative et quantitative de risques. Il facilite les analyses de risques pour les ingénieurs et les non-experts puisqu'il génère automatiquement des scénarios d'attaques et de défauts/défaillances à l'origine d'un événement indésirable donné. L'automatisation de la génération de scénarios de risques facilite la modélisation de différentes hypothèses sur la même architecture de système. Il suffit d'ajouter ces changements en intégrant de nouvelles entrées (sans avoir à recommencer depuis le début). Enfin, la méthode propose une approche robuste puisque l'architecture de système peut être directement et facilement modifiée et de nouveaux scénarios de risques peuvent être à nouveau générés.

Dans un mode de réalisation, la méthode comprend l'utilisation de ladite base de connaissances pour :

- calculer d'éventuelles défaillances aléatoires en raison de procédés d'exploitation normaux de manière à évaluer des risques de sûreté, et calculer des défaillances en raison d'attaques de ladite architecture industrielle de manière à évaluer des risques de sécurité,

- fournir un modèle de gestion de risques de sûreté et de sécurité, et évaluer des conflits entre la gestion de sûreté et la gestion de sécurité,

- délivrer des données d'aide à la prise de décision sur la base de ladite évaluation de conflits pour aider un utilisateur en matière de prise de risque dans l'exploitation de ladite architecture industrielle.

Un outil efficace pour améliorer des mesures de sûreté et de sécurité est ainsi fourni. En particulier, l'interaction réciproque et la convergence des risques de sûreté et de sécurité sont prises en compte.

Dans un autre mode de réalisation, l'attaque prise en compte par la base de connaissances est une cyberattaque. Ainsi, l'usage croissant des ICT dans des procédés industriels est pris en compte pour évaluer ce type de nouveaux problèmes de sécurité.

Dans un mode de réalisation, des données en entrée sont utilisées pour modéliser une architecture d'informations dans un réseau d'entreprise. En variante ou en combinaison, lesdites données en entrée sont utilisées pour modéliser une architecture de commande d'un réseau de supervision et de commande, et/ou d'un réseau de procédé et de terrain.

Le terme « réseau d'entreprise » fait référence à tout réseau utilisé par au moins un opérateur d'une entreprise. En particulier, il fait référence à un réseau utilisé par des opérateurs d'une entité responsable du procédé industriel. Tous les types de réseaux impliqués dans le procédé industriel peuvent être modélisés et le modèle généré peut représenter complètement des entités impliquées dans le procédé industriel.

Dans un mode de réalisation, la description du procédé industriel reçue en entrée comprend une description d'au moins un composant compris dans le procédé industriel. Ainsi, les compétences des opérateurs chargés de l'évaluation des risques du procédé industriel peuvent être limitées à une connaissance complète du procédé industriel. En effet, la base de connaissances permet de construire un modèle à partir de la seule description de composants du procédé industriel, ce qui limite les compétences analytiques et de modélisation de l'opérateur au minimum.

Le terme « composant » fait référence à toute entité physique ou non physique comprise dans le procédé industriel ou reliée à celui-ci. Un poste de travail, un serveur, un processeur, un capteur, un actionneur, un réseau sans fil, un canal de signalisation, un port Ethernet, la qualification d'un intervenant, une localisation d'un dispositif impliqué dans le procédé industriel ou un risque spécifique relatif à un

dispositif impliqué dans le procédé industriel constituent des exemples de composants compris dans le procédé industriel. La description du composant comprend généralement un identifiant du composant ainsi que des paramètres et/ou des caractéristiques attachés à ce composant.

Dans un autre mode de réalisation, l'étape de la réception en entrée de la description du procédé industriel comprend :

- affichage d'une interface graphique comprenant un élément graphique correspondant au composant compris dans le procédé industriel ; et
- sur détection d'une sélection de l'élément graphique, la réception en entrée de la description du composant.

L'utilisation d'éléments graphiques pour recevoir une entrée de l'opérateur facilite davantage l'utilisation de la base de connaissances pour évaluer des risques.

Dans un mode de réalisation, le procédé industriel comprend un système d'information, et l'étape de la réception en entrée de la description du procédé industriel comprend :

- analyse du système d'information pour détecter le composant compris dans le procédé industriel ; et
- sur détection du composant compris dans le système d'information, l'extraction d'une description du composant à partir du système d'information pour recevoir en entrée ladite description extraite du composant.

Le terme « système d'information » fait référence à tout système composé de personnes et d'ordinateurs qui traite ou interprète des informations relatives au procédé industriel. Un système de gestion de relation client (CRM), un système de commande industrielle (ICS), une base de données de paramètres, une planification de ressources d'entreprise (ERP), un moteur de recherche, un réseau Ethernet, ou un système d'information géographique dans un circuit intégré constituent des exemples de systèmes d'information.

Ainsi, les ressources humaines nécessaires pour évaluer des risques relatifs à un procédé industriel sont très limitées. En effet, la méthode permet l'extraction des données nécessaires à la base de connaissances pour évaluer les risques. De cette manière, la tâche des opérateurs humains est réduite au contrôle des composants entrés automatiquement et, si nécessaire, à l'ajout de composants manquants.

Dans un mode de réalisation, une description d'une pluralité de composants compris dans le procédé industriel est reçue en entrée, ladite pluralité de composants constituant le procédé industriel. Ainsi, la tâche de l'opérateur est limitée à l'entrée des composants.

Dans un autre mode de réalisation, la base de connaissances comprend un bloc logiciel exécutant un programme orienté objet comprenant une pluralité de classes, au moins une classe de ladite pluralité de classes correspondant à un composant de l'architecture industrielle. Dans ce mode de réalisation, l'étape de l'utilisation de ladite base de données pour évaluer un risque relatif au dit procédé industriel comprend en outre :

- instanciation d'au moins un objet à partir de ladite classe en fonction de la description du composant reçu en entrée ;
- construction d'un modèle textuel à partir dudit au moins un objet.

Comme cela a été expliqué ci-dessus, l'architecture industrielle est une méta-architecture virtuelle couvrant plusieurs procédés industriels possibles. L'architecture industrielle comprend généralement un grand nombre de composants disponibles qui peuvent être utilisés dans un procédé industriel couvert par l'architecture industrielle. Dans ce mode de réalisation, des composants de l'architecture industrielle correspondent à des classes, au sens de la programmation orientée objet.

Dans la programmation orientée objet, une classe est un modèle programme-code extensible destiné à créer des objets en fournissant des valeurs initiales d'état (variables de membres) et des mises en œuvre de comportement (fonctions ou méthodes de membres). Une classe peut être comparée à un moule qui, lorsqu'il est rempli, donne un objet ayant la forme du moule avec toutes ses caractéristiques. Par conséquent, lorsque l'opérateur indique une description d'un composant compris dans le procédé industriel, la base de connaissance appelle la classe correspondant au composant et instancie un objet sur la base de la description du composant.

Des propriétés de la programmation orientée objet sont particulièrement pertinentes pour cette méthode. En particulier, l'héritage permet de modifier dynamiquement le modèle textuel en ajoutant des objets d'une manière simplifiée. En effet, lors de l'ajout d'un composant, comme un nouveau port dans un serveur, un nouvel objet peut être facilement instancié en appelant directement la sous-classe appropriée qui hérite de la classe parent utilisée pour instancier l'objet correspondant

au serveur. En outre, le mécanisme d'héritage permet de structurer facilement les connaissances et d'éviter les redondances.

Ainsi, ce mode de réalisation propose une approche robuste puisque le modèle correspondant au procédé industriel peut être directement et facilement modifié et de nouveaux scénarios de risques peuvent être générés à nouveau d'une manière dynamique.

Dans un autre mode de réalisation, la liste classée de scores d'évaluation de risques est fournie par l'application d'un outil de quantification au modèle textuel, ledit outil de quantification comprenant au moins un élément parmi un outil de simulation de Monte-Carlo et un outil de méthode de Markov. Ainsi, des outils efficaces sont utilisés pour obtenir la liste classée de scores.

Un deuxième aspect de l'invention concerne un produit de programme informatique enregistré sur un support de mémorisation et exécutable par un ordinateur sous la forme d'un logiciel comprenant au moins un module logiciel configuré pour mettre en œuvre la méthode selon le premier aspect de l'invention.

Un troisième aspect de l'invention concerne un dispositif informatique comprenant un circuit de traitement comprenant une unité de mémoire mémorisant un programme informatique pour effectuer la méthode selon le premier aspect de l'invention.

Un quatrième aspect de l'invention concerne un dispositif pour évaluer des risques d'une architecture industrielle, comprenant :

- un processeur apte à effectuer :

• une étape préliminaire de construction d'une base de connaissances décrivant des risques industriels associés à des procédés industriels respectifs d'exploitation de ladite architecture industrielle ;

• des étapes courantes de :

- réception, en entrée, d'une description d'un procédé industriel,

- utilisation de ladite base de données pour évaluer un risque associé au dit procédé industriel, et

- fourniture, en sortie, de données d'évaluation dudit risque,

- une mémoire pour mémoriser la base de connaissances, ladite base de connaissances comprenant des données de fonction pour calculer des scores de risques industriels associés à la fois à des scénarios d'attaque de ladite architecture

industrielle, et des procédés industriels d'exploitation de ladite architecture industrielle,

de manière à fournir, en sortie, des données d'une liste classée de scores d'évaluation de risques associés à des scénarios d'attaque à l'intérieur de procédés industriels d'exploitation de ladite architecture industrielle.

La présente invention est illustrée à titre d'exemple, et non pas à titre de limitation, sur les figures des dessins annexés, sur lesquels des numéros de référence similaires renvoient à des éléments similaires et sur lesquels :

- la figure 1 représente un contexte d'utilisation de la présente invention selon un mode de réalisation de la présente invention ;
- la figure 2 représente un organigramme des étapes d'une méthode selon un mode de réalisation de l'invention ;
- la figure 3 représente une vue d'ensemble d'un bloc logiciel compris dans la base de connaissances selon un mode de réalisation de l'invention ;
- la figure 4 représente une illustration de composants d'un procédé industriel pour lequel des risques sont évalués, selon un mode de réalisation de l'invention ;
- la figure 5 représente un dispositif de mise en œuvre de l'invention selon un mode de réalisation de l'invention.

L'invention est décrite ci-après dans son application de l'évaluation de risques dans le domaine de la production d'énergie. Néanmoins, l'invention n'est pas limitée à cette application et elle peut facilement être appliquée à d'autres domaines/secteurs d'activités, comme la fabrication de biens, la logistique, l'agriculture, l'armée, etc.

La figure 1 illustre, selon un mode de réalisation de l'invention, une centrale nucléaire 1 comprenant un serveur 3, un ordinateur 4 et un actionneur 5 reliés par un réseau interne, comme un système de commande industrielle (ICS). Dans ce mode de réalisation, la centrale 1 est utilisée pour exploiter un procédé industriel et le serveur 3, l'ordinateur 4 et l'actionneur 5 sont des composants de ce procédé industriel. Les composants 3, 4 et 5 sont également reliés à un réseau externe 6, comme l'Internet.

Un dispositif 2, décrit ci-après en référence à la figure 5, est utilisé par un opérateur pour évaluer des risques du procédé industriel exploité par la centrale 1, comme cela est détaillé ci-après en référence aux étapes 9 à 14 de la figure 2 en particulier.

La figure 2 est un organigramme décrivant des étapes de la méthode pour évaluer des risques du procédé industriel selon un mode de réalisation de l'invention.

Une étape préliminaire 8 de construction d'une base de connaissances décrivant des risques industriels associés à des procédés industriels respectifs d'exploitation d'une architecture industrielle est traitée par un développeur 7. Comme cela a été susmentionné, l'architecture industrielle est une méta-architecture virtuelle couvrant une pluralité de procédés industriels réels possibles.

Dans le présent exemple de l'industrie de production d'énergie, l'architecture industrielle comprend tous les procédés industriels possibles relatifs à la production d'énergie. Par conséquent, la base de connaissances est apte à couvrir la production d'électricité par une centrale nucléaire, la maintenance d'un barrage, l'installation d'une nouvelle ligne d'électricité, etc.

Dans cet exemple, la base de connaissances est ainsi capable de traiter tous les types de composants pouvant être utilisés ou concernant la production d'énergie. Comme cela va être détaillé ci-après, un objectif de la base de connaissances est de construire un modèle compréhensible par des outils de quantification à partir d'une description du procédé industriel. Pour cela, la base de connaissances doit être apte à identifier des composants et à les ajouter au modèle.

Dans un mode de réalisation, la base de connaissances comprend un bloc logiciel exécutant un programme orienté objet comprenant une pluralité de classes, au moins une classe de ladite pluralité de classes correspondant à un composant de l'architecture industrielle. Le bloc logiciel est généralement compris dans un programme logiciel apte à exécuter la méthode selon l'invention. Le bloc logiciel peut également être le programme logiciel complet.

Typiquement, un langage orienté objet pouvant être utilisé pour le bloc logiciel est le langage FIGARO. FIGARO permet la représentation de modèles stochastiques avec des états discrets et une échelle de temps continue grâce à deux types de règles : les règles d'occurrence et d'interaction (décrites ci-après). Dans la base de connaissances, FIGARO est utilisé pour modéliser les différents composants du système.

La figure 3 représente une vue d'ensemble de classes possibles comprises dans la base de connaissances, dans un mode de réalisation de l'invention. Cette

figure décrit des composants de l'architecture industrielle, leurs attributs associés ainsi que les attaques et les défaillances possibles sur chaque composant.

Une brève description des classes impliquées dans la figure 3 est donnée ci-après. La figure 3 représente un exemple de classes comprises dans une architecture industrielle qui est plus élargie que l'architecture industrielle dans le domaine de la production d'énergie. Pour cette base de connaissances, il est ci-après supposé que différentes machines (physical_cpt) sont reliées à un réseau (network_zone) et hébergent différents services (software_cpt). Des composants logiciels échangent différents flux de données (data_flow) et peuvent héberger certaines vulnérabilités (vulnerabilite) qui peuvent être exploitées par un assaillant (assaillant). Des précisions concernant d'autres hypothèses faites pour cette base de connaissances sont également données après la liste suivante de classes.

- Classe « composant » : la super classe composant modélise un composant qui peut tomber en panne accidentellement ou qui peut être compromis par un assaillant. La classe composant comporte deux types d'événements de risques : le premier est une défaillance accidentelle qui modélise une défaillance accidentelle d'un composant pouvant survenir aléatoirement ; le deuxième est une étape d'attaque appelée accès. L'élément booléen « physical_access » est initialement réglé à VRAI ou FAUX selon qu'il est possible ou non d'accéder physiquement au composant. Si l'élément physical_access est réglé à VRAI, l'étape d'attaque d'accès peut survenir avec un taux de danger constant lambda et le composant est compromis. Les éléments booléens « echec » et « compromised_host » modélisent respectivement le fait que le composant est défaillant et le fait que le composant est compromis par un assaillant.

Les deux classes héritant des caractéristiques de cette classe sont « network_zone » et « physical_cpt ».

- Classe « network_zone » : la classe network_zone modélise un ensemble de machines reliées l'une à l'autre en utilisant des technologies filaires ou sans fil. La classe network_zone prend le contrôle de l'étape d'attaque d'accès pour la conditionner à la détermination si le réseau est filaire et peut être accédé physiquement par l'assaillant ou s'il est sans fil et sans mécanisme d'authentification. Pour les réseaux sans fil, l'attaque de brouillage peut survenir aléatoirement. Des règles d'interaction, expliquées ci-après, propagent l'effet d'indisponibilité pour des

données envoyées par des éléments reliés au réseau, en cas de défaillance de réseau ou d'attaques de brouillage.

- Classe « physical_cpt » : une distinction est établie dans cette base de connaissances entre les composants physiques (physical_cpt) qui représentent les machines dans le réseau et les composants logiciels (software_cpt) s'exécutant sur ces machines. Cette relation est modélisée par la classe « link_machine_soft ». Un composant physique appartient à une zone de réseau et peut héberger un composant logiciel ou de nombreux composants logiciels.

Les règles d'interaction modélisent le fait que, lorsqu'un composant physique physical_cpt est compromis, alors tous les composants logiciels s'exécutant sur celui-ci sont également compromis, et lorsqu'un composant logiciel software_cpt est défaillant, alors toutes les données envoyées depuis ses composants logiciels hébergés ne sont pas disponibles.

- Classe « software_cpt » : cette classe modélise un composant logiciel s'exécutant sur un hôte donné, par exemple des applications client-serveur. Un composant logiciel software_cpt peut envoyer et recevoir des données à partir d'autres composants logiciels. L'interface de données modélise une donnée de sortie output_data du composant logiciel software_cpt.

Il est supposé, pour cette base de connaissances, qu'un logiciel ne peut pas être défaillant. Il peut néanmoins être altéré par un assaillant (compromised_software).

- Classe « data_flow » : cette classe modélise un flux de données entre deux composants logiciels. Dans cette base de connaissances, des données peuvent être soit fausses soit indisponibles.

- La classe « IT_sys_cpt » modélise une machine généralement utilisée à des niveaux élevés de l'architecture d'information de système et fournissant des fonctionnalités évoluées. Cette machine exécute un système d'exploitation donné qui peut être Windows ou Linux dans cette base de connaissances. L'attribut « privilege » modélise le privilège par défaut dont l'utilisateur légitime dispose sur sa machine. « Vuln_configuration » modélise une vulnérabilité provoquée par une mauvaise configuration de la machine. Un assaillant peut exploiter une telle vulnérabilité, si elle existe, pour obtenir des privilèges racine (ou root, en anglais) sur la machine (privilege_escalation_attack).

- La classe « vulnerabilite » modélise une vulnérabilité associée au logiciel IT (pour technologies de l'information, ou « Information Technology » en anglais), qui peut avoir les conséquences suivantes : élévation des privilèges, perte de confidentialité, perte d'intégrité ou refus de service.

- La classe « IT_soft_cpt » modélise un composant logiciel s'exécutant sur une machine IT_sys_cpt. Un composant logiciel informatique peut avoir de nombreuses vulnérabilités ou aucune vulnérabilité. Quatre étapes d'attaques génériques sont associées à cette classe pour modéliser des vulnérabilités d'exploitation avec les quatre conséquences possibles d'une vulnérabilité. Des règles d'interaction propagent l'effet d'altération de données en cas d'élévation des privilèges ou de perte d'intégrité et l'effet d'indisponibilité de données en cas de refus de service.

- La classe « assaillant » modélise un assaillant qui se trouve initialement sur une machine physique. Cette machine constitue donc un hôte compromis.

Pour la construction de cette base de données, les hypothèses suivantes ont été adoptées.

• Il est établi une distinction entre des machines physiques et des composants logiciels s'exécutant sur celles-ci. Cette hypothèse permet d'avoir un niveau suffisant de détails dans lequel des défaillances et des attaques, comme d'accès physique, sont associées aux machines physiques et des cyberattaques exploitant des vulnérabilités sont associées au composant logiciel qui héberge une vulnérabilité spécifique.

• Il est dit qu'une machine physique est compromise si un assaillant parvient à obtenir des privilèges racine sur celle-ci. Si tel est le cas, il peut compromettre tous les composants logiciels s'exécutant sur cette machine. Cette hypothèse est assez crédible puisque le fait qu'un logiciel soit compromis sur cette machine ne signifie pas que l'assaillant peut compromettre tous les autres services à moins d'être parvenu à obtenir des privilèges racine.

• Une vulnérabilité peut être associée à un composant logiciel ou à une machine physique. Si elle est associée à une machine physique, la vulnérabilité modélise une mauvaise configuration de machine (par exemple des fichiers système qui ne sont pas protégés en écriture) qui est censée permettre une élévation des privilèges lorsqu'elle est exploitée par un assaillant.

• Pour les réseaux de niveau IT, comme un réseau d'entreprise, l'accent est mis sur la propagation d'attaque (plusieurs étages, plusieurs sauts) entre différentes machines de niveau IT jusqu'à ce qu'un composant ayant une action de commande sur le procédé soit atteint. Lorsque le réseau de commande est atteint, l'accent est mis sur l'intégrité/disponibilité de données (fausses/indisponibles) puisque la modification ou l'indisponibilité constitue généralement la raison principale engendrant des événements indésirables.

Ainsi, la base de connaissances peut être considérée comme un langage spécifique au domaine permettant de décrire les composants types d'infrastructures industrielles numériques et les attributs de sécurité associés (authentification, contrôle d'accès, redondance). Chaque composant est associé aux attaques et aux modes de défaillance pouvant survenir sur celui-ci.

La base de connaissances comprend deux types de règles, à savoir les règles d'occurrence et les règles d'interaction (également appelées « règles de l'interaction »). Les règles d'occurrence spécifient les attaques et les dysfonctionnements pouvant survenir sur chaque type de composant de l'architecture. Un exemple de règle pour une instance associée à une machine comprise dans le procédé industriel est présenté ci-après :

```
GROUP groupe_simu
    IF ((access OR IT_EXISTS x A hosted_software SUCH_THAT
compromised_software(x) OR IT_EXISTS y A network SUCH_THAT
compromised_host(y)) AND privilege='user' AND
vuln_configuration )
MAY_OCCUR
FAULT privilege_escalation
DIST EXP(0.001)
INDUCING privilege <-- 'racine';
```

Les règles d'interaction décrivent les effets de propagation d'attaque/défaillance entre des composants interconnectés. Un exemple de règles d'interaction associées à l'architecture de réseau est présenté ci-après :

```
network_unavailable
    GROUP groupe_simu
    IF echec    OR jamming_attack OR denial_of_service_attack
    THEN FOR_ALL x A connectedElements
    DO (
    FOR_ALL y A hosted_software(x) DO (
    FOR_ALL z A out_data(y) DO not_available(z))) ;
```

Ainsi, les règles d'occurrence décrivent l'occurrence d'attaques/défaillances et les conditions préalables à leur réalisation. Les règles d'interaction décrivent comment les conséquences de ces attaques/défaillances se propagent dans l'architecture.

En référence à la figure 2, l'étape préliminaire de la construction de la base de connaissances est généralement effectuée une fois (avec d'éventuelles mises à jour régulières) et la base de connaissances obtenue est ensuite intégrée dans un logiciel final. Le logiciel final est ensuite distribué à des opérateurs pour l'évaluation des risques de divers procédés industriels, à condition que lesdits procédés industriels soient couverts par la base de connaissances.

A l'étape 9, un opérateur 10 lance ledit logiciel final sur un dispositif 2 pour évaluer des risques du procédé industriel de production d'électricité avec la centrale nucléaire 1. A cette étape, l'opérateur saisit une description du procédé industriel. Un ingénieur de sécurité, un intervenant, un technicien, un expert, un consultant ou un employé de la centrale 1 constituent des exemples d'un opérateur pouvant utiliser le dispositif 2.

En particulier, l'opérateur 10 entre une liste de description de composants compris dans le procédé industriel. Dans ce cas, cette liste peut comprendre une description des composants 3, 4 et 5, une description du réseau interne reliant ces composants, une liste de personnes en mesure d'accéder à l'ordinateur 4, etc.

Dans un mode de réalisation, une interface graphique comprenant un élément graphique correspondant au composant compris dans le procédé industriel est affichée et une description d'un composant est reçue à la détection d'une sélection de l'élément graphique par l'opérateur.

Dans un autre mode de réalisation, le dispositif 2 est un ordinateur relié au réseau interne qui est apte à extraire automatiquement une description du procédé industriel. Pour cela, les étapes suivantes peuvent être appliquées :

- l'analyse d'un système d'information du procédé industriel, par exemple pris en charge par le réseau interne, pour détecter le composant compris dans le procédé industriel ; et

- à la détection du composant compris dans le système d'information, l'extraction d'une description du composant à partir du système d'information pour recevoir, en entrée, ladite description extraite du composant.

Dans un mode de réalisation, le système complet 2 est un dispositif distant, comme un serveur relié au réseau 6. Il est ainsi possible d'évaluer des risques du procédé industriel à distance, ce qui permet de gagner du temps et de faire des économies de coûts.

A l'étape 11, un modèle textuel est construit à partir de la base de connaissances. Pour cela, les sous-étapes suivantes sont appliquées : (1) l'instanciation d'au moins un objet d'une classe, comprise dans la base de connaissances, en fonction de la description du composant reçu en entrée et (2) la construction d'un modèle textuel à partir dudit au moins un objet. Concrètement, le modèle textuel est un texte et/ou un fichier graphique qui peut être compris par des outils de quantification.

Le modèle textuel peut être en évolution dynamique puisque, comme cela a été susmentionné, des propriétés d'une programmation orientée objet sont particulièrement pertinentes pour cette méthode. En particulier, l'héritage permet de modifier dynamiquement le modèle textuel en ajoutant des objets d'une manière simplifiée. En effet, lors de l'ajout d'un composant, comme un nouveau port dans un serveur, un nouvel objet peut être facilement instancié en appelant directement la sous-classe appropriée, héritant de la classe parent qui a été utilisée pour instancier l'objet correspondant au serveur. En outre, le mécanisme d'héritage permet de structurer facilement les connaissances et d'éviter les redondances.

Une étape 12 est ainsi prévue pour demander à l'opérateur, ou pour envoyer automatiquement une demande au système d'information lorsque des descriptions de composants sont automatiquement extraites, de déterminer si une modification du

procédé industriel est survenue. Si tel est le cas, la méthode revient à l'étape 9 pour que l'opérateur modifie/ajoute une description d'un composant.

Si tel n'est pas le cas, une liste classée de scores d'évaluation de risques est fournie à l'étape 13 par l'application d'un outil de quantification au modèle textuel. L'outil de quantification peut être un type de méthode de Markov ou de simulation de Monte-Carlo. FIGSEQ ou YAMS sont des exemples de tels outils de quantification. YAMS est un simulateur de Monte-Carlo ; FIGSEQ est un outil de calcul de fiabilité et de disponibilité de système basé sur l'exploration et la quantification de séquence allant de l'état initial du système jusqu'à un état de défaillance. Ces outils permettent de générer automatiquement des scénarios d'attaque et de défaut sur la base des règles d'occurrence décrites dans la base de connaissances. Les scénarios sont triés par ordre décroissant de probabilité d'occurrence.

La liste de fourniture, en sortie, de données d'évaluation dudit risque est ensuite fournie à l'étape 14.

Une application sur un cas d'étude va être décrite ci-après en référence à la figure 4. La description suivante du cas est concentrée sur les composants de réseau d'un procédé industriel.

Un modèle graphique du procédé industriel entré en utilisant la base de connaissances est représenté sur la figure 4. Il se compose de trois zones de réseau : un réseau d'entreprise, un réseau de commande de procédé et un réseau de terrain. Les liaisons du type « link_machine_soft » sont représentées par des flèches noires en pointillés et le flux de données entre les composants logiciels est représenté par des flèches bleues continues.

Un poste de travail 15 situé dans le réseau d'entreprise utilise une application client HTTP pour des raisons statistiques et d'optimisation. Cette application communique avec un serveur HTTP s'exécutant sur une machine 16 « http_ftp_server » placée dans une zone démilitarisée DMZ et hébergeant également un serveur ftp. Celui-ci communique avec le client ftp s'exécutant sur le serveur d'acquisition 17. Le logiciel de serveur SCADA (commande de supervision et acquisition de données) est également hébergé sur le serveur d'acquisition relié au réseau de commande de procédé. Il permet de superviser et de commander le procédé industriel global par la collecte de données auprès de contrôleurs de procédé et le

retour d'instructions. Les contrôleurs de procédé collectent des données auprès de capteurs et envoient des instructions à des actionneurs par l'intermédiaire d'électeurs, représentés par des portes k/n.

La porte k/n avant l'actionneur constitue un mécanisme de sûreté qui représente également une barrière pour les assaillants. Dans le cas où l'actionneur reçoit des instructions de différents contrôleurs de procédé, la porte k/n peut être utilisée comme un électeur : elle exécute les instructions uniquement si k instructions sur n sont cohérentes (sur la figure 4, k = n = 1). L'assaillant doit compromettre ou rendre k instructions indisponibles pour assurer le succès de son attaque.

Les hypothèses pour ce procédé industriel sont les suivants :

- l'accès physique à la station de l'opérateur est possible ;
- la machine http_ftp_server s'exécute avec des privilèges d'utilisateur ;
- il existe une vulnérabilité sur le serveur HTTP qui permet une élévation des privilèges ;
- le serveur d'acquisition fonctionne avec des privilèges d'utilisateur mais il a une vulnérabilité de configuration permettant d'acquérir des privilèges racine ;
- il existe une vulnérabilité sur le client ftp qui permet une perte d'intégrité ;
- le réseau de terrain utilise une liaison de communication sans fil pour échanger des données entre le contrôleur de procédé et d'autres dispositifs sur le terrain.

La base de connaissances est utilisée pour évaluer le risque associé à un événement indésirable : « actuator_does_not_act_properly ». Il est adopté une analyse pessimiste dans laquelle des conséquences de sûreté peuvent survenir si l'actionneur ne fonctionne pas correctement (c'est-à-dire s'il reçoit des instructions fausses ou s'il ne reçoit pas d'instructions). Par exemple, cette architecture est utilisée pour la commande et la supervision d'une usine chimique et le contrôleur de procédé envoie une instruction pour arrêter le chauffage mais le dispositif de chauffage ne répond pas, ce qui peut engendrer des températures dépassant des limites avec des conséquences de sûreté (explosion, blessures humaines).

La méthode selon l'invention produit alors les résultats suivants : après un an de fonctionnement sans maintenance, la probabilité que l'actionneur ne fonctionne pas correctement atteint 0,46. Bien entendu, cela semble très élevé, mais il est adopté une hypothèse pessimiste selon lequel l'événement indésirable survient lorsqu'un

actionneur dans le réseau de terrain reçoit une fausse instruction ou ne reçoit pas d'instruction du contrôleur de procédé. Le dysfonctionnement du dispositif de chauffage peut être insuffisant pour créer un risque de sûreté et il doit être combiné à des dysfonctionnements d'autres composants comme des mécanismes d'arrêt forcé.

Les scénarios d'attaque et de défaillance pouvant conduire à cet événement indésirable sont automatiquement générés grâce à l'outil de quantification. Ils sont basés sur les règles d'occurrence dans la base de connaissances décrivant des attaques (respectivement des défaillances) et les taux (l'inverse du temps moyen de compromis, respectivement du temps moyen de défaillance) de la distribution exponentielle associée à chaque règle. Ces scénarios sont triés dans un tableau dans l'ordre décroissant de leur probabilité d'occurrence et de leur contribution à l'événement indésirable.

Les trois premiers scénarios obtenus dans ce cas d'utilisation sont donnés dans le tableau 1 ci-après (où N° de séq. représente le numéro de séquence, Proba représente la probabilité, et Contrib. représente la contribution) :

N° de séq.	Transitions		Proba	Contrib.
	Nom	Taux		
1	access(workstation)	0.0001	1.77e-1	3.82e-1
	exploit_server_vuln_priv_escalation (IT_soft_cpt_http_server)	0.001		
	exploit_server_vuln_integrity_loss(IT_soft_cpt_client_ftp)	0.001		
	privilege_escalation(acquisition_server)	0.001		
	send_false_instructions_to_process_controller(scada_server_soft_cpt)	0.001		
2	access(workstation)	0.0001	1.77e-1	3.44 e-1
	exploit_server_vuln_priv_escalation (IT_soft_cpt_http_server)	0.001		
	exploit_server_vuln_integrity_loss(IT_soft_cpt_client_ftp)	0.001		
	privilege_escalation(acquisition_server)	0.001		
	send_no_instructions_to_process_controller(scada_server_soft_cpt)	0.001		
3	jamming_attack(field_network)	1e-5	5.39e-2	1.16e-1

Tableau 1

On peut constater par exemple que le scénario le plus probable (séquence N° 1 dans le tableau 1) comporte cinq étapes d'attaque. A la première étape, l'assaillant parvient à obtenir l'accès au poste de travail (« workstation » en anglais) 15 (ici parce que l'attribut d'accès physique de cette machine a été réglé à VRAI, mais l'assaillant peut avoir un accès distant). A la deuxième étape, l'assaillant exploite à distance la vulnérabilité existante du serveur http permettant une élévation des privilèges. Le serveur http est par conséquent compromis et l'assaillant dispose des privilèges racine sur la machine http_ftp_server, ce qui lui permet de compromettre le serveur ftp_server fonctionnant sur celle-ci. Puisque le serveur ftp communique avec un client ftp s'exécutant sur le serveur d'acquisition, l'assaillant essaye, à la troisième étape, d'exploiter à distance la vulnérabilité du client ftp. Le client ftp est alors compromis. Puisque la vulnérabilité n'engendre qu'une perte d'intégrité, l'assaillant doit également procéder à une attaque d'élévation des privilèges, à la quatrième étape, en exploitant la vulnérabilité de configuration associée au serveur d'acquisition afin de pouvoir compromettre le logiciel serveur SCADA. Si l'assaillant parvient à le compromettre, il peut alors envoyer des instructions fausses au contrôleur de procédé qui envoie alors des instructions fausses à l'actionneur.

Le deuxième scénario d'attaque (séquence N° 2 dans le tableau 1) est identique mais, au lieu de falsifier des données, l'assaillant crée un refus de service de sorte qu'aucune instruction ne soit envoyée au contrôleur de procédé qui n'envoie alors aucune instruction à l'actionneur lorsque cela est nécessaire.

Le troisième scénario d'attaque (séquence N° 3 dans le tableau 1) est une attaque de brouillage dans le réseau de terrain sans fil. Cette attaque est moins probable car l'assaillant doit se trouver à côté du contrôleur de procédé ou à côté de l'actionneur pour brouiller la communication, ce qui n'est pas facile.

Les trois scénarios de risque suivants, présentés dans le tableau 2 (séquence N° 4 à 6), sont purement accidentels. La défaillance du serveur d'acquisition, du réseau de terrain ou du contrôleur de procédé a pour conséquence que des instructions ne sont pas envoyées à l'actionneur lorsque cela est nécessaire.

N° de séq.	Transitions		Proba	Contrib.
	Nom	Taux		
4	accidental_failure(acquisition_server)	1^{e}-6	5.39^{e}-3	1.16^{e}-2
5	accidental_failure(field_network)	1^{e}-6	5.39^{e}-3	1.16^{e}-2
6	accidental_failure(process_controller_1)	1^{e}-6	5.39^{e}-3	1.16^{e}-2

Tableau 2

La figure 5 est un mode de réalisation possible pour un dispositif 2 permettant la présente invention.

Dans ce mode de réalisation, le dispositif 2 comprend un ordinateur, cet ordinateur comprenant une mémoire non volatile 21 pour mémoriser des instructions de programme pouvant être chargées dans une mémoire volatile 22 et aptes à amener un circuit 20 à effectuer les étapes de la présente invention lorsque les instructions de programme sont exécutées par le circuit 20. La base de connaissances peut être mémorisée dans des mémoires 21 et/ou 22 et/ou sur un serveur distant.

La mémoire 22 et la mémoire 21 peuvent également mémoriser des données et des informations utiles pour effectuer les étapes de la présente invention comme cela a été décrit ci-dessus.

Le circuit 20 peut être par exemple :

- un processeur ou une unité de traitement apte à interpréter des instructions dans un langage informatique, le processeur ou l'unité de traitement pouvant comprendre, être associé ou être attaché à une mémoire comprenant les instructions, ou
- l'association d'un processeur/unité de traitement et d'une mémoire, le processeur ou l'unité de traitement étant apte à interpréter des instructions dans un langage informatique, la mémoire comprenant ces instructions, ou
- une carte électronique dans laquelle les étapes de l'invention sont décrites dans une puce à silicium.

Cet ordinateur comprend une interface d'entrée 18 pour la réception de données utilisées pour la méthode susmentionnée selon l'invention, un processeur de

signal numérique 19 pour moduler/démoduler lesdites données et une interface de sortie 23 pour fournir un modèle empilé.

L'homme du métier peut se rendre compte que divers paramètres divulgués dans la description peuvent être modifiés et que divers modes de réalisation divulgués peuvent être combinés sans se départir du périmètre de l'invention.

En particulier, l'exemple d'un objet instancié en utilisant une classe est présenté dans certains modes de réalisation décrits ci-dessus. Néanmoins, la présente invention n'est pas limitée à des objets instanciés en utilisant des classes mais, au lieu de cela, elle couvre, dans un mode de réalisation dans lequel un langage orienté objet est utilisé, des objets instanciés en utilisant tous les types d'entités, comme des interfaces, des méthodes, des variables, des attributs, des constructeurs, etc. mis à disposition par des langages orientés objets. Plus généralement, la base de connaissances peut être comparée à un groupe de moules dans lequel des composants du procédé industriel sont remplis. Des objets résultant du moulage sont ensuite utilisés par des outils de quantification.

REVENDICATIONS

1. Méthode mise en œuvre par ordinateur pour l'évaluation de risques de sécurité d'une architecture industrielle, comprenant :

une étape préliminaire (8) de :

- construction d'une base de connaissances décrivant des risques industriels associés à des procédés industriels respectifs d'exploitation de ladite architecture industrielle, et des étapes courantes de :

- réception (9), en entrée, d'une description d'un procédé industriel,

- utilisation de ladite base de données pour évaluer (13) un risque associé au dit procédé industriel, et

- fourniture (14), en sortie, de données d'évaluation dudit risque,

dans laquelle ladite base de connaissances comprend des données de fonction pour calculer des scores de risques industriels associés :

- à des scénarios d'attaque de ladite architecture industrielle, et

- à des procédés industriels d'exploitation de ladite architecture industrielle,

de manière à fournir, en sortie, des données d'une liste classée de scores d'évaluation de risques associés à des scénarios d'attaque à l'intérieur de procédés industriels d'exploitation de ladite architecture industrielle.

2. Méthode selon la revendication 1, comprenant l'utilisation de ladite base de connaissances pour :

- calculer d'éventuelles défaillances aléatoires en raison de procédés d'exploitation normaux de manière à évaluer des risques de sûreté, et calculer des défaillances en raison d'attaques de ladite architecture industrielle de manière à évaluer des risques de sécurité,

- fournir un modèle de gestion de risques de sûreté et de sécurité, et évaluer des conflits entre la gestion de sûreté et la gestion de sécurité,

- délivrer des données d'aide à la prise de décision sur la base de ladite évaluation de conflits pour aider un utilisateur en matière de prise de risque dans l'exploitation de ladite architecture industrielle.

3. Méthode selon l'une quelconque des revendications 1 et 2, dans laquelle ladite attaque est une cyberattaque.

4. Méthode selon l'une quelconque des revendications précédentes, dans laquelle lesdites données en entrée sont utilisées pour modéliser une architecture d'informations dans un réseau d'entreprise.

5. Méthode selon l'une quelconque des revendications 1 à 3, dans laquelle lesdites données en entrée sont utilisées pour modéliser une architecture de commande d'un réseau de supervision et de commande et/ou un réseau de procédé et de terrain.

6. Méthode selon l'une quelconque des revendications précédentes, dans laquelle la description du procédé industriel reçue en entrée comprend une description d'au moins un composant (3, 4, 5, 15, 16, 17) compris dans le procédé industriel.

7. Méthode selon la revendication 6, dans laquelle l'étape de la réception en entrée de la description du procédé industriel comprend :

■ affichage (10) d'une interface graphique comprenant un élément graphique correspondant au composant compris dans le procédé industriel ; et

■ sur détection d'une sélection de l'élément graphique, réception en entrée de la description du composant.

8. Méthode selon la revendication 6, dans laquelle le procédé industriel comprend un système d'information, et

dans laquelle l'étape de la réception en entrée de la description du procédé industriel comprend :

■ analyse (10) du système d'information pour détecter le composant compris dans le procédé industriel ; et

■ sur détection du composant compris dans le système d'information, extraction d'une description du composant à partir du système d'information pour recevoir en entrée ladite description extraite du composant.

9. Méthode selon l'une quelconque des revendications 6 à 8, dans laquelle une description d'une pluralité de composants compris dans le procédé industriel est reçue en entrée, ladite pluralité de composants constituant le procédé industriel.

10. Méthode selon l'une quelconque des revendications précédentes, dans laquelle la base de connaissances comprend un bloc logiciel exécutant un programme orienté objet comprenant une pluralité de classes, au moins une classe de ladite pluralité de classes correspondant à un composant de l'architecture industrielle, et
dans laquelle l'utilisation de ladite base de données pour évaluer un risque relatif au dit procédé industriel comprend en outre :
- instanciation d'au moins un objet à partir de ladite classe en fonction de la description du composant reçu en entrée ;
- construction (11) d'un modèle textuel à partir dudit au moins un objet.

11. Méthode selon la revendication 10, dans laquelle la liste classée de scores d'évaluation de risques est fournie par l'application d'un outil de quantification au modèle textuel,
ledit outil de quantification comprenant au moins un élément parmi un outil de simulation de Monte-Carlo et un outil de méthode de Markov.

12. Produit programme informatique enregistré sur un support de mémorisation et exécutable par un ordinateur sous la forme d'un logiciel comprenant au moins un module logiciel configuré pour mettre en œuvre la méthode selon l'une quelconque des revendications 1 à 11.

13. Dispositif informatique (2) comprenant un circuit de traitement comprenant une unité de mémoire mémorisant un programme informatique pour effectuer la méthode selon l'une quelconque des revendications 1 à 11.

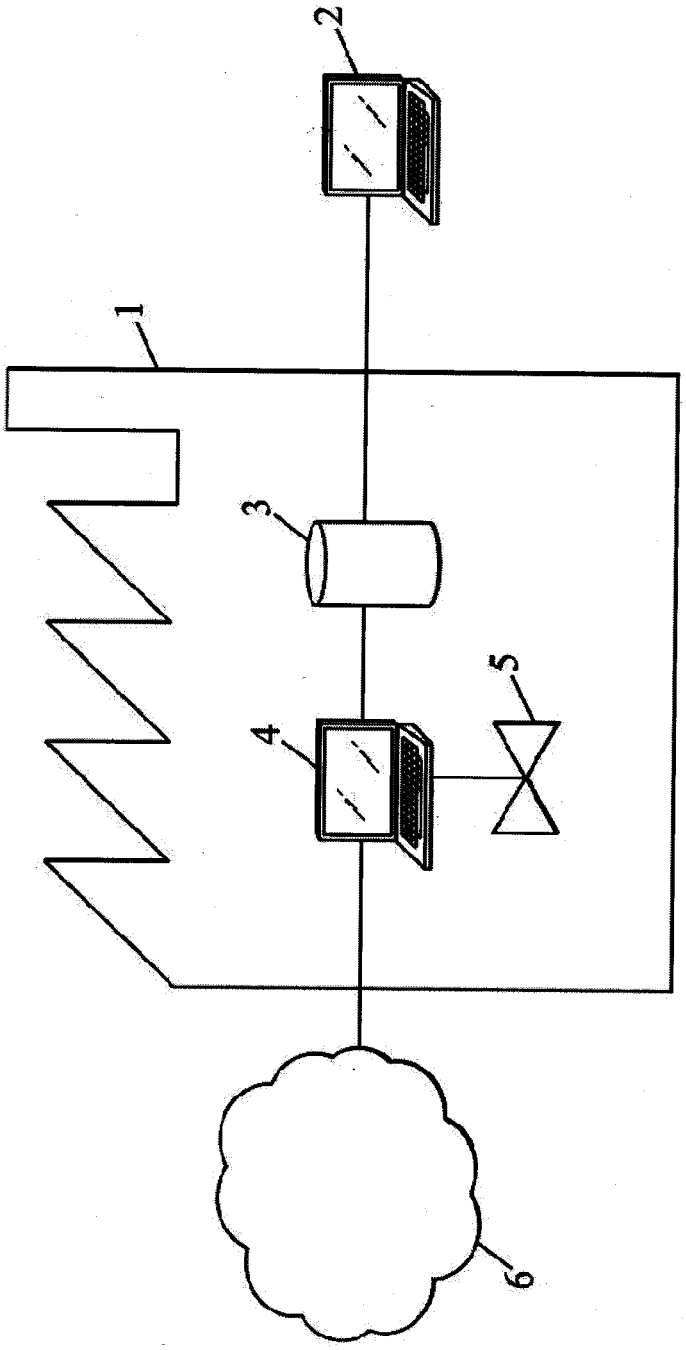


FIG. 1

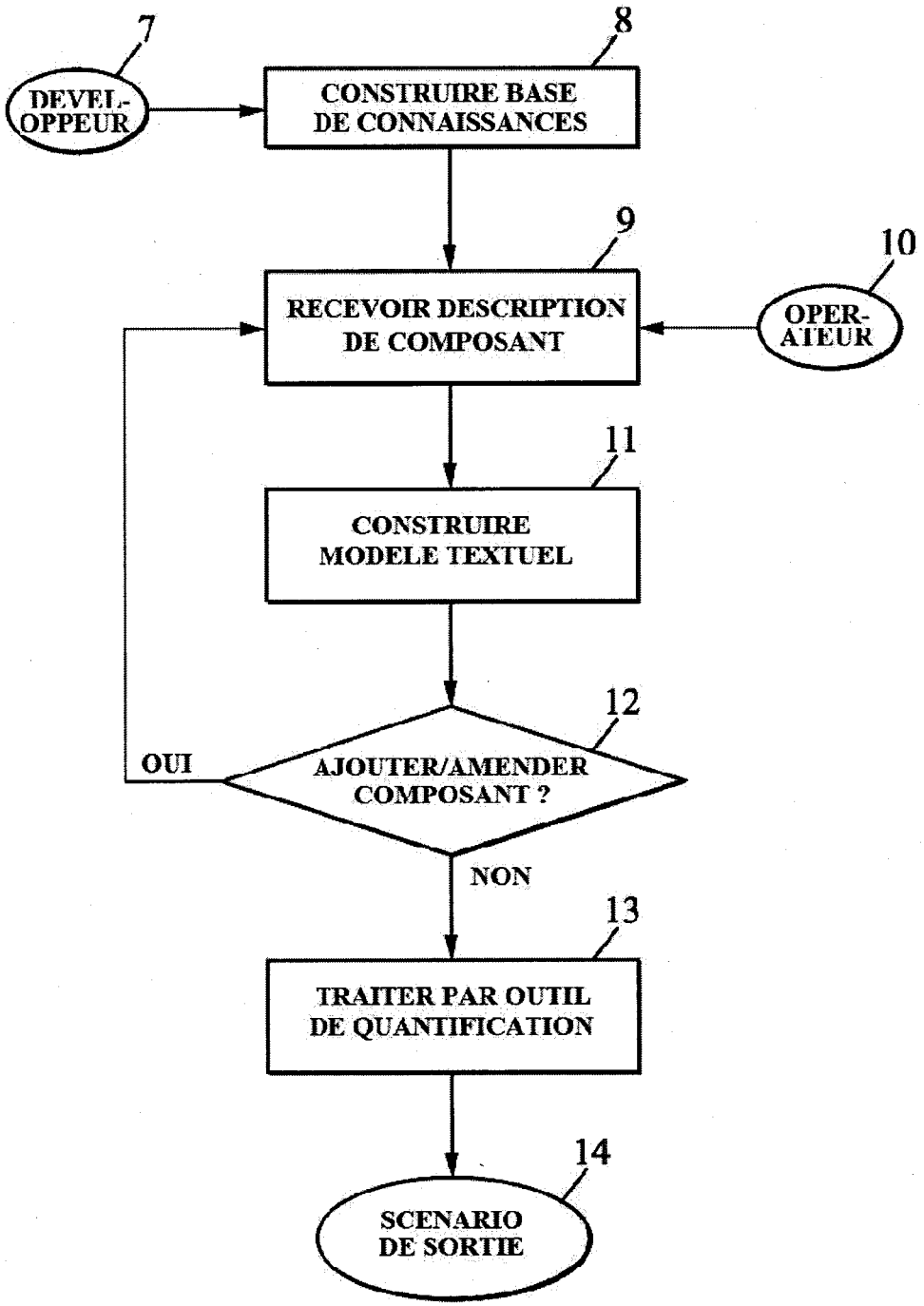

7
DEVEL-
OPPEUR
8
CONSTRUIRE BASE
DE CONNAISSANCES
9
RECEVOIR DESCRIPTION
DE COMPOSANT
10
OPER-
ATEUR
11
CONSTRUIRE
MODELE TEXTUEL
12
OUI
AJOUTER/AMENDER
COMPOSANT ?
NON
13
TRAITER PAR OUTIL
DE QUANTIFICATION
14
SCENARIO
DE SORTIE

FIG. 2

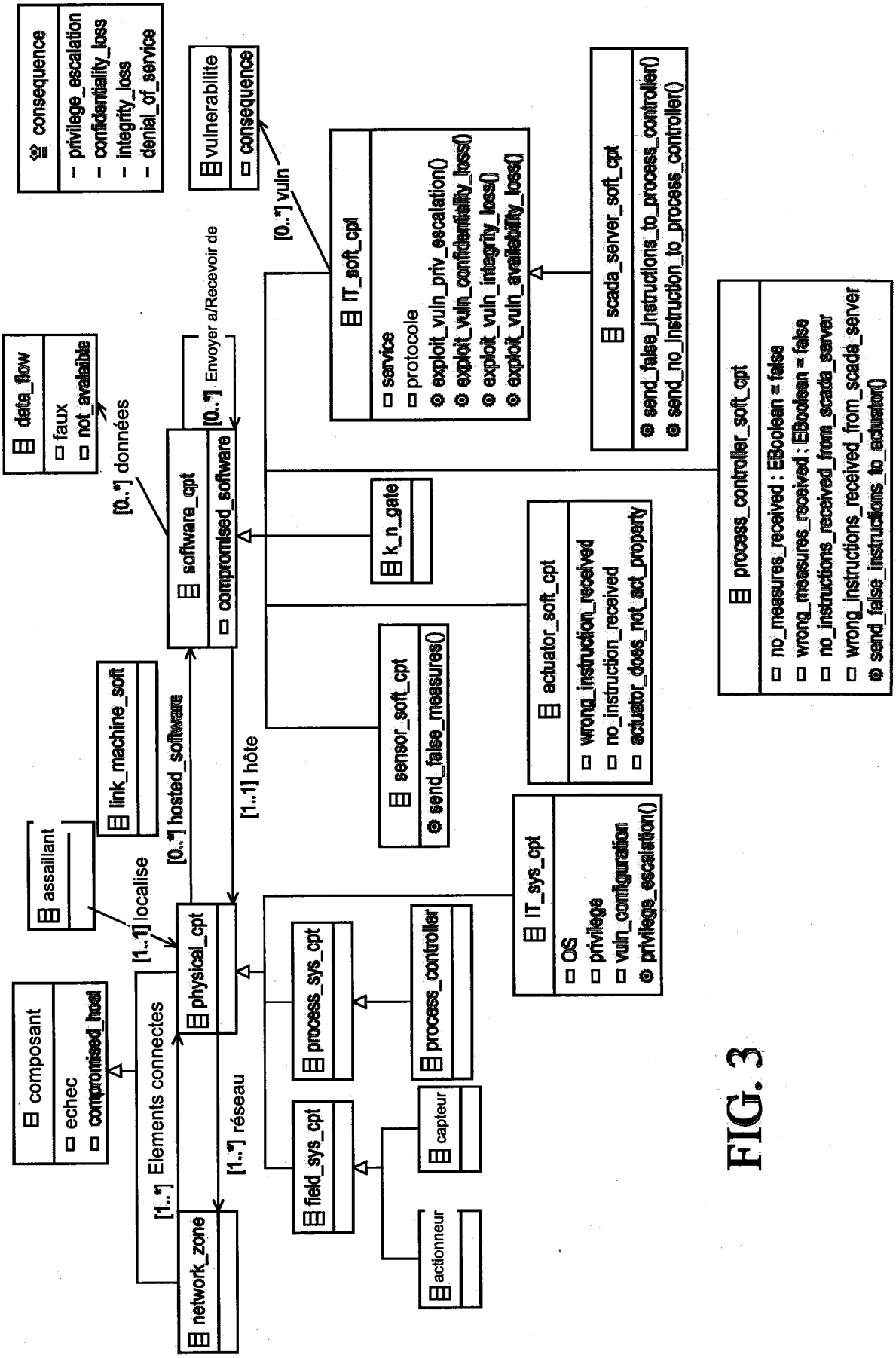

consequence
- privilege_escalation
- confidentiality_loss
- integrity_loss
- denial_of_service
vulnerabilite
consequence
[0..*] vuln
data_flow
faux
not_available
[0..*] données
[0..*] Envoyer a/Recevoir de
IT_soft_cpt
service
protocole
exploit_vuln_priv_escalation()
exploit_vuln_confidentiality_loss()
exploit_vuln_integrity_loss()
exploit_vuln_availability_loss()
scada_server_soft_cpt
send_false_instructions_to_process_controller()
send_no_instruction_to_process_controller()
process_controller_soft_cpt
no_measures_received : EBoolean = false
wrong_measures_received : EBoolean = false
no_instructions_received_from_scada_server
wrong_instructions_received_from_scada_server
send_false_instructions_to_actuator()
software_cpt
compromised_software
k_n_gate
actuator_soft_cpt
wrong_instruction_received
no_instruction_received
actuator_does_not_act_property
sensor_soft_cpt
send_false_measures()
IT_sys_cpt
OS
privilege
vuln_configuration
privilege_escalation()
link_machine_soft
[0..*] hosted_software
[1..1] hôte
assaillant
[1..1] localise
physical_cpt
process_sys_cpt
process_controller
composant
echec
compromised_host
[1..*] Elements connectes
[1..*] réseau
field_sys_cpt
capteur
actionneur
network_zone

FIG. 3

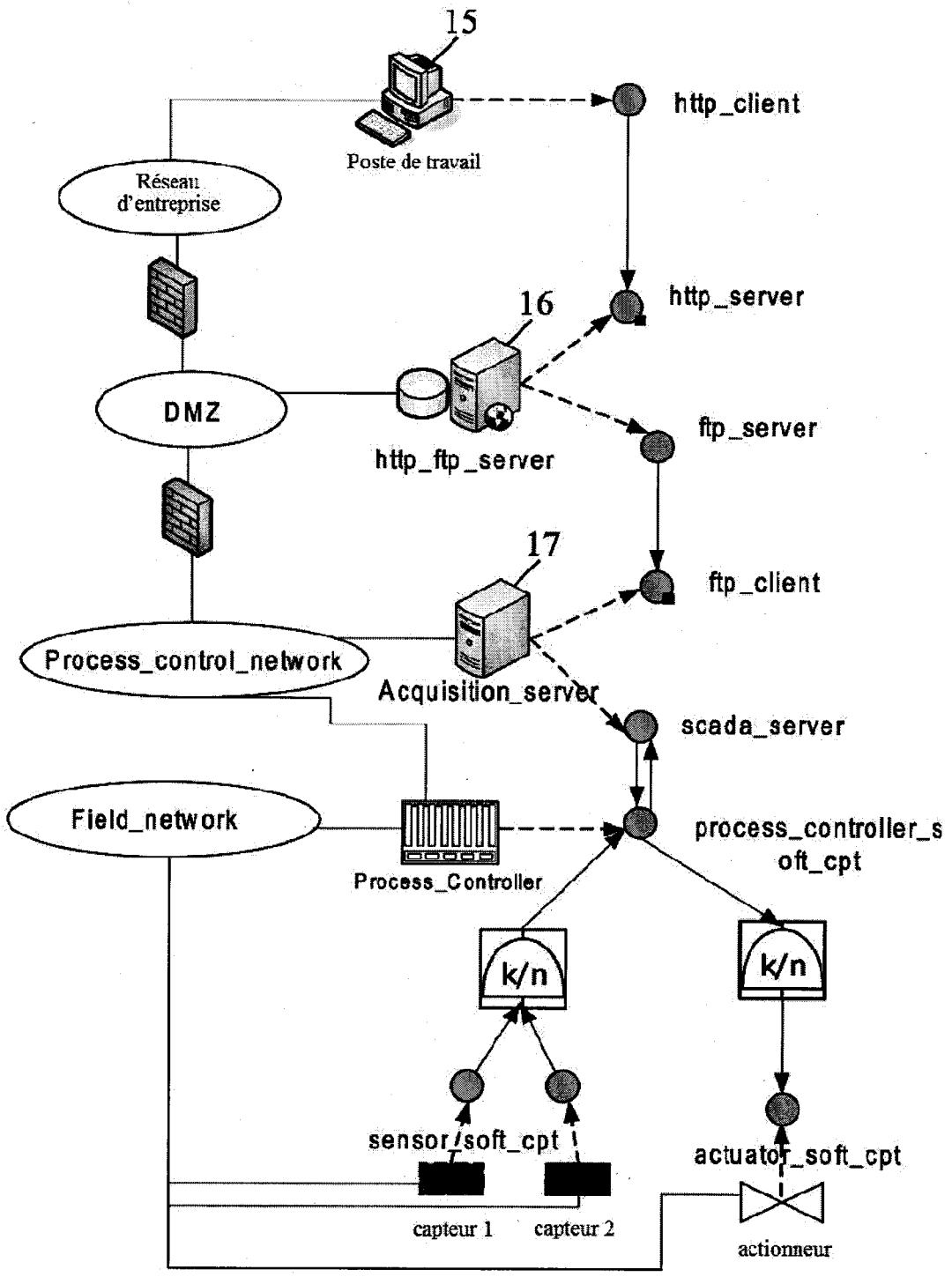

15
Poste de travail
http_client
Réseau d'entreprise
http_server
16
DMZ
http_ftp_server
ftp_server
17
ftp_client
Process_control_network
Acquisition_server
scada_server
Field_network
Process_Controller
process_controller_soft_cpt
k/n
k/n
sensor/soft_cpt
actuator_soft_cpt
capteur 1
capteur 2
actionneur

FIG. 4

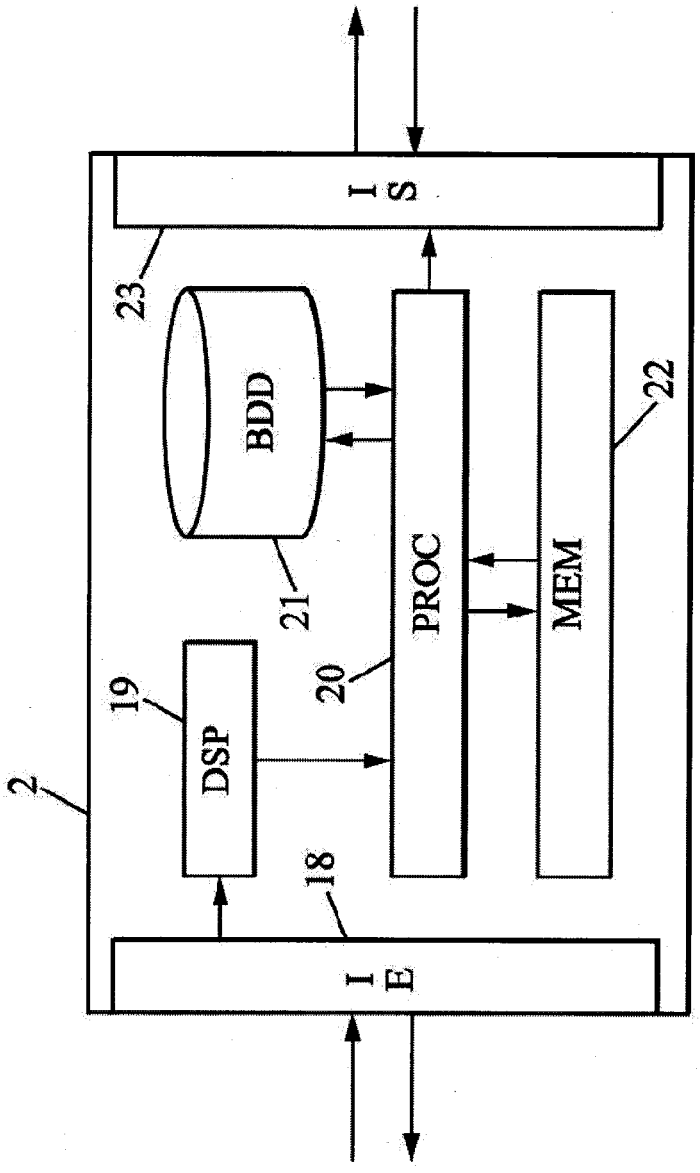


FIG. 5