UNIVERSITE DE LAUSANNE
FACULTE DES HAUTES ETUDES COMMERCIALES

ELABORATION DE TABLEAUX DE BORD SSI DYNAMIQUES : UNE APPROCHE A BASE D'ONTOLOGIES

THESE

Présentée à la Faculté des HEC
de l'Université de Lausanne

par

Lambert SONNA MOMO

Ingénieur Informaticien de l'Ecole Polytechnique Fédérale de Lausanne

Pour l'obtention du grade de
Docteur en Systèmes d'information

2009

UNIVERSITE DE LAUSANNE
FACULTE DES HAUTES ETUDES COMMERCIALES

ELABORATION DE TABLEAUX DE BORD SSI DYNAMIQUES : UNE APPROCHE A BASE D'ONTOLOGIES

THESE

Présentée à la Faculté des HEC
de l'Université de Lausanne

par

Lambert SONNA MOMO

Ingénieur Informaticien de l'Ecole Polytechnique Fédérale de Lausanne

Pour l'obtention du grade de
Docteur en Systèmes d'information

2009

UNIL | Université de Lausanne
HEC Lausanne
Le Doyen
Bâtiment Internef
CH-1015 Lausanne

IMPRIMATUR

Sans se prononcer sur les opinions de l'auteur, le Conseil de la Faculté des hautes études commerciales de l'Université de Lausanne autorise l'impression de la thèse de Monsieur Lambert SONNA MOMO, ingénieur informaticien de l'Ecole Polytechnique Fédérale de Lausanne en vue de l'obtention du grade de docteur en Systèmes d'information.

La thèse est intitulée :

ELABORATION DE TABLEAUX DE BORD SSI DYNAMIQUES : UNE APPROCHE A BASE D'ONTOLOGIES

Lausanne, le 16 mars 2009

Le doyen

Suzanne de Treville

Tél. ++41 21 692 33 66 | Fax ++41 21 692 34 35 | hecdoctorats@unil.ch

Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

Par la présente, je certifie avoir examiné la thèse de doctorat de

Lambert SONNA MOMO

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées durant le colloque de thèse ont été prises en considération et reçoivent ici mon approbation.

Signature : _____ Date : 9 Mars 2009

Prof. Solange GHERNAOUTI-HÉLIE
Directrice de thèse

Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

Par la présente, je certifie avoir examiné la thèse de doctorat de

Lambert SONNA MOMO

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées durant le colloque de thèse ont été prises en considération et reçoivent ici mon approbation

Signature : Yves Pigneur Date : 7 mars 2009

Prof. Yves PIGNEUR
Membre interne du jury

Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

Par la présente, je certifie avoir examiné la thèse de doctorat de

Lambert SONNA MOMO

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées durant le colloque de thèse ont été prises en considération et reçoivent ici mon approbation

Signature : _____ Date : 13.02.09

Prof. Jacky AKOKA
Co-directeur de thèse CNAM Paris

Université de Lausanne
Faculté des Hautes Etudes Commerciales

Doctorat en Systèmes d'Information

Par la présente, je certifie avoir examiné la thèse de doctorat de

Lambert SONNA MOMO

Sa thèse remplit les exigences liées à un travail de doctorat.
Toutes les révisions que les membres du jury et le soussigné ont demandées durant le colloque de thèse ont été prises en considération et reçoivent ici mon approbation

Signature : Jacqueline Reigner Date : 13 mars 2009

Dr Jacqueline REIGNER
Membre externe du jury

ELABORATION DE TABLEAUX DE BORD SSI DYNAMIQUES : UNE APPROCHE A BASE D'ONTOLOGIES

20 mars 2009

0.1 Remerciements

Je tiens à remercier en premier lieu mes directeurs le professeure Solange Ghernaouti et le professeur Jacky Akoka pour leur encadrement et soutien tout au long de ces années. Je suis reconnaissant pour leur disponibilité, leurs qualités pédagogiques et scientifiques. J'ai beaucoup appris à leurs côtés et je leur adresse toute ma gratitude. Le professeur Jacky Akoka m'a accueilli plusieurs fois au sein du CNAM à Paris. Ma considération est inestimable. Ses remarques et critiques pertinentes m'ont conduit vers la bonne voie. Au travers de nos discussions, il m'a apporté une compréhension plus approfondie des divers aspects du sujet. Son soutien m'a permis de ne jamais faiblir et de poursuivre toujours plus loin mes travaux.

Je remercie le professeure Suzanne de Tréville doyen de la faculté d'avoir accepter de présider cette thèse.

Je remercie le professeur Yves Pigneur et le Dr Jacqueline Reigner pour l'honneur qu'ils me font en acceptant de participer au jury et pour l'intérêt qu'ils accordent à mon travail.

Toute ma gratitude à toutes les personnes ayant relu, corrigé et commenté mon manuscrit et ayant ainsi participé à son amélioration.

Je remercie mes parents, mes frères et sœurs pour leurs encouragements et leur intérêt envers mon travail, ainsi qu'à toutes les autres personnes aimables et serviables qui m'ont soutenu et qui ont contribué à mon enrichissement personnel.

Enfin, je ne saurais terminer cette liste sans remercier mon épouse Eliane Pékéléko SONNA qui a cru en moi et qui m'a soutenu tout le long de ce travail, ainsi que mes enfants Victor William, Câline et Iris Janet.

0.2 Résumé

Dans un contexte économique de mondialisation croissante, les entreprises se développent dans un environnement en perpétuel évolution. La complexité des systèmes d'information rend le pilotage stratégique de plus en plus compliqué. La quantité de paramètres à prendre en compte ne cesse de croître et de changer. Les nouvelles technologies de l'information apportent des solutions efficaces et des outils performants avec l'accroissement du potentiel des machines, du système de gestion des bases de données et de l'évolution de l'internet. Les systèmes d'information permettent aux entreprises de centraliser de nombreuses informations, d'extraire des informations décisives et de piloter efficacement la stratégie. Le système d'information décisionnel a fait son apparition à côté du système d'information opérationnel. Cette complexité et ces évolutions constantes offrent des avantages significatifs, mais posent des défis scientifiques ardus qu'il faudra relever pour voir l'expansion technologique poursuivre son évolution.

Les entreprises, les organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes doivent porter une bien plus grande attention à la sécurité. Ils doivent en permanence adapter leur stratégie globale de sécurité aux évolutions de l'environnement, aux modifications des besoins, aux progrès des techniques d'attaque ou à la découverte des nouvelles vulnérabilités. Leur perception de la sécurité se modifie au fil du temps. Pour adapter la politique de sécurité, il faut analyser périodiquement l'écart entre l'état réel de la sécurité et les objectifs (stratégie de sécurité) que l'on s'est fixés. Le pilotage de la sécurité consiste à vérifier et à réduire en permanence cet écart ; l'ensemble des indicateurs, des alarmes, des statistiques qui permettent de le mettre en évidence est appelé Tableau de Bord de la Sécurité.

Les travaux sur les tableaux de bord, leur construction, leur utilisation ou leur évolution ont déjà quelques décennies. Leur extension est indispensable, dans l'environnement actuel des entreprises. La possibilité de concevoir des systèmes qui se reconfigurent, s'adaptent au contexte, et même se corrigent dans une certaine mesure, apparaît comme un facteur de passage à l'échelle supérieure, pour la croissance technologique. L'environnement des entreprises varie de manière exponentielle. Pour suivre la politique de sécurité nous devons adapter continuellement notre stratégie de sécurité à l'environnement. Ce n'est plus les tableaux de bord classiques mais les tableaux de bord dynamiques dont nous avons besoin. Nous entendons par tableau de bord dynamique, un système lié et évoluant avec la stratégie de sécurité. Un système dans lequel le risque est lié à un ensemble de contre-mesures et un ensemble d'indicateurs mesurant l'atteinte des objectifs des contre-mesures. Toute variation d'un attribut du risque doit se répercuter sur l'ensemble de contre-mesures associées.

Notre contribution se situe à trois niveaux. Dans un premier temps, nous avons construit trois ontologies dans les domaines suivants : risques, contre-mesures et indicateurs de sécurité. Nous avons fusionné ces trois ontologies pour avoir une ontologie globale de la sécurité que nous avons appelé ONTOSEC. L'ontologie globale nous a servi de médiateur pour intégrer les informations provenant des sources variées, permettant ainsi de résoudre le problème d'hétérogénéité structurelle et sémantique sur les informations. Nous avons proposé

une démarche formelle en cinq étapes pour le suivi et l'évolution d'ONTOSEC. Dans un deuxième temps, nous avons développé un tableau de bord sécurité qui s'appuie sur ce médiateur afin de répondre aux requêtes des utilisateurs, nous l'avons appelé Tableau de Bord de la sécurité Dynamique(TBSD). Dans un troisième temps, nous avons testé ce système dans le cas réel d'une appelée TELKOM SA. Il en découle, qu'outre les avantages liés au TBSD cités plus haut, il facilite l'implantation de la politique de sécurité, et surtout le pilotage de la sécurité dans un environnement changeant.

0.3 Abstract

In a context of an increasing economic globalization, companies grow in a perpetually evolving environment. The complexity of information systems makes the strategic piloting ever more complex. Concomitantly, the quantity of parameters to be taken into account tremendously grows and changes as well. With the enhancement of machines potentials, database management systems and the evolution of the Internet, new information technologies provide effective solutions and powerful tools for this purpose. The information systems allow companies to centralize a variety of information, to sideline decisive/significant information and to effectively control the strategy. Therefore, besides the operational information system appears the decision-making information system. In spite of the significant advantages that the complexity and constant evolutions give rise to/offer, critical scientific challenges need to be addressed in order to ensure the perpetuation/continuation of the technological expansion. Companies, organizations and individual users who develop, possess, supply, manage, maintain and use the systems have to pay greater attention to the security-related issue. They permanently have to adapt their global security strategy to the evolution of the environment, to the modifications of needs, to the progress of the techniques of attacks or to the discovery of the new vulnerabilities.

Their perception of safety itself changes with time. To adapt the security policy, it is necessary to periodically analyze the difference between the real state of security and the objectives that has been assigned. The piloting of safety consists in checking and reducing permanently this variation ; the whole of the indicators, alarms, and the statistics which make it possible to highlight it is called TBS. The works on dashboards, their construction, their use or their evolution are already some decades-old so that their extension has become unavoidable in a dynamic environment. The possibility of conceiving systems which re-configure, adapt themselves to the context, and even undertake mutual correction, to an extent, is therefore a critical upgrading factor for the technological growth. Companies environment currently varies in an exponential way. To comply with the security policy, continuous safety strategy too must be adapted to the environment. And the traditional dashboards need to be supplemented by the dynamic ones. By dynamic instrument panel, we mean a system intertwined and evolving with the safety/security strategy ; a system in which the risk is linked to a whole countermeasure and where a set of indicators measures the achievements of the countermeasure objectives. Any variation of the potentiality of the risk or its impact is echoed on the set of countermeasures associated.

Our contribution of this work is four fold. Firstly we have build a global ontology of the security known as ONTOSEC. This ontology consists of three local ontologies : the first deals with risks, the second addresses countermeasures and the third relates to safety/security indicators. Global ontology was used as a mediator to integrate information coming from a variety of sources ; it thus helped overcome the problem of structural and semantic heterogeneity on the information Thereafter, we used the java and eclipses environments for an instrument panel safety/security which built on this mediator to highlight the dynamic aspect of the system, we called this unit TBSD. In the third phase, we tested this system in the real case of a company ; it transpired/resulted that, in addition to the advantages related to the dynamic instrument panel referred to above,

it also facilitates the implementation of the security policy, and especially the piloting of safety in an evolving/changing context. We finally proposed a formal step with five stages for the follow-up and the evolution of this system.

Liste des algorithmes

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction

Le viel adage « Mieux vaut prévenir que guérir » reste d'actualité aujourd'hui. Les entreprises sont arrivées à un point où la sécurité du système d'information (SI) devient primordiale dans la vie de tous les jours. Elles doivent se préoccuper au jour le jour non seulement des incidents qui affectent leurs systèmes mais aussi des incidents susceptibles de les affecter. Le terme « Système d'Information » désigne ici tout système destiné à élaborer, traiter, stocker, acheminer de l'information.

De nos jours, les informations dans les entreprises sont de plus en plus réparties entre différents systèmes propriétaires et indépendants. Le problème d'intégration de ces sources d'informations devient crucial et primordial pour les entreprises, d'autant qu'elles contiennent des informations précieuses pour des applications métiers. De telles sources se prêtent à des intrusions de types divers, susceptibles de modifier ou détruire l'information, ou de la révéler à des tiers qui sont censés ne pas en avoir connaissance. Ces intrusions peuvent être simples, utilisant des technologies et des méthodes très répandues. Elles sont à la portée de services spécialisés dans la recherche du renseignement, comme à celle de particuliers à l'affût d'informations pouvant servir leurs intérêts, entre autres les organisations criminelles, terroristes ou susceptibles de compromettre l'ordre public.

La Sécurité des Systèmes d'Information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour conserver ou rétablir la disponibilité, l'intégrité et la confidentialité des informations provenant des sources variées. Pour mieux sécuriser les SI, les entreprises doivent en permanence mesurer l'écart entre l'état réel de leur sécurité et ce qui est prévu dans la PS. Pour le faire, les entreprises doivent utiliser des tableaux de bord de la sécurité (TBS). Les TBS sont confrontés à l'évolution croissante de la stratégie de sécurité qui elle même doit s'aligner sur le contexte évolutif de nos SI. Pour mieux répondre à cette problématique, les TBS actuels doivent se baser sur une architecture de médiation capable d'agréger des éléments de réponses provenant de différentes sources pour construire une réponse globale à la requête de l'utilisateur. De plus, ces architectures doivent prendre en charge une série de tâches destinées à la sélection, l'extraction et la transformation des informations mises à la disposition du TBS.

Dans ce travail de thèse nous nous intéressons à la sécurité des informations et à leur intégration par médiation afin de les rendre utilisables par les TBS. Ce travail s'insère dans le cadre de toute grande entreprise disposant de plusieurs sources hétérogènes de données et qui changent très souvent. L'objectif est de répondre à leur besoin en matière de sécurité et de prise de décision. La construction de cubes de données à la demande devient ainsi une solution pertinente [Settouti2005]. Chaque cube de données représente un contexte d'analyse ciblée. Du fait que les données changent très souvent, la solution des TBS basés sur un entrepôt de données centralisées comme le font la plupart de constructeurs semble peu indiquée. Notre approche consiste à définir un dispositif de médiation permettant, à partir d'une requête de l'utilisateur, de déployer le processus allant de la sélection des données dans les sources de données originales, à la construction des cubes de données.

Notre objectif est double, dans un premier temps il s'agira de créer un médiateur basé sur une ontologie de sécurité. Le spectre d'applications et de domaines s'intéressant aux ontologies ne cesse de s'élargir. Anciennement réservée aux systèmes experts simulant des raisonnements humains dans des domaines spécifiques, l'ontologie se retrouve maintenant dans une large famille de SI. Elle est utilisée pour décrire et traiter des ressources multimédia ; asseoir l'interopérabilité d'applications en réseaux ; piloter des traitements automatiques de la langue naturelle ; construire des solutions multilingues et interculturelles ; permettre l'intégration de sources hétérogènes d'information ; décrire des protocoles d'interactions complexes ; vérifier la cohérence de modèles, etc. Ces utilisations des ontologies se retrouvent dans de nombreux domaines d'application : intégration d'informations, gestion de ressources humaines, aide à l'analyse en biologie, commerce électronique, enseignement assisté par ordinateur, bibliothèques numériques, échanges commerciaux entre partenaires industriels, suivi médical informatisé etc. [Gruber93] a proposé la définition la plus citée de la littérature. Il considère l'ontologie comme étant "*une spécification formelle et explicite d'une conceptualisation partagée*". Le terme "*conceptualisation*" représente un modèle abstrait d'un domaine d'intérêt dont les concepts pertinents sont identifiés et recensés. Le mot *explicite* implique que les types de concepts ainsi que les contraintes exprimées sur les concepts soient explicitement définies. Le terme formel indique que l'ontologie doit être décrite dans un format (ou un langage) lisible par la machine. Le mot "*partagé*" fait référence au fait que l'ontologie doit capturer une partie consensuelle de la connaissance acceptée par toute ou une large partie de la communauté derrière l'ontologie.

Il existe plusieurs architectures pour mettre en place les ontologies dans un système d'intégration. Une architecture intéressante est de faire correspondre une ontologie locale à chaque source et de construire l'ontologie globale à partir de ces ontologies. Dans ce cas précis, nous avons construit une ontologie de tous les risques (OR) encourus par les SI. Cette ontologie locale est liée à toutes les sources de données contenant les menaces qui pèsent sur les SI. Nous avons construit une deuxième ontologie contenant toutes les mesures génériques nécessaires pour traiter les risques contenus dans OR. Une mesure peut être soit une mesure préventive, palliative, corrective ou dissuasive. Cette ontologie sera liée aux sources produisant des données nécessaires pour implanter les mesures de contrôles. Chaque mesure ayant un objectif précis. Nous avons construit une troisième ontologie des indicateurs de sécurité. Chaque indicateur permet de mesurer l'atteinte des objectifs

par la mesure. Nous avons intégré ces ontologies pour avoir une ontologie globale de la sécurité (ONTOSEC).

Quelques méthodologies ont été proposées pour "supporter" le développement des ontologies. Ces méthodes sont générales et ne prennent pas en compte le contexte d'intégration. Elles peuvent être classées en fonction de l'utilisation ou non des connaissances ainsi que des techniques d'apprentissage. Les toutes premières qui servaient à construire des ontologies d'entreprises, le faisaient sans connaissance à priori : elles étaient manuelles. La rétro-conception des ontologies [Gomez1999] est basée sur le *mapping* d'un modèle conceptuel d'une ontologie construite avec un autre modèle plus valide pour le reconstruire. Les méthodologies se distinguent selon les données en entrée : textes, dictionnaires, bases de connaissances, schémas relationnels, et semi-structurés, sources de données hétérogènes. Ben Mustapha et al. [BenMustapha2006] ont travaillé sur cette classification et ont proposé une synthèse. Les méthodes qui proposent de construire des ontologies dans le cadre d'un médiateur comme [Brisaboa2003] présentent une démarche de construction descendante. Il s'agit de construire l'ontologie globale puis les ontologies locales. Cette démarche en revanche ne simplifie pas la résolution des problèmes d'hétérogénéité sémantiques [Settouti2005]. L'approche que nous préconisons consiste à créer une ontologie globale de la sécurité, à partir des ontologies locales de risques, mesures et indicateurs de sécurité. Plusieurs modèles structuraux peuvent être appliqués à cette architecture. Ils se distinguent d'une part, par la façon dont est établie la correspondance entre le schéma global et les schémas des sources de données à intégrer, et d'autre part, par les langages utilisés pour modéliser le schéma global, les schémas des sources de données à intégrer et les requêtes des utilisateurs. Concernant le premier point on distingue l'approche Global As Views(GAV) de l'approche Local As Views(LAV). L'approche GAV, qui provient du monde des bases de données fédérées, consiste à définir le schéma global en fonction des schémas des sources de données à intégrer. Les systèmes qui suivent cette approche sont : HERMES [Subrahmanian1995], MONIS [Beneventano2000]. L'approche LAV est adoptée dans le système Observer [Observer1996]. Selon cette approche il est très facile d'ajouter une source d'information, sans aucun effet sur le schéma global. En revanche la construction des réponses à des requêtes est complexe, contrairement à la construction de réponses dans un système utilisant l'approche GAV qui consiste simplement à remplacer les prédicats du schéma global de la requête par leur définition. Le modèle nécessite une réécriture et un dépliement ; ce qui n'est pas chose facile. Le traitement de requêtes dans une architecture avec plusieurs ontologies modélisées selon GLAV est possible [Settouti2005] si la requête est exprimée dans un langage de requêtes qui prend en charge le niveau global et local.

Dans ce travail de thèse, nous avons développé dans un premier temps ONTOSEC. Cette ontologie pourra servir dans le cadre de développement d'une plate forme de médiation. Par la suite nous avons développé un TBS qui peut s'appuyer sur cette plate forme afin d'aider les acteurs du domaine à prendre des décisions. Le fait que le TBS s'appuie sur ONTOSEC pour répondre aux requêtes des utilisateurs, nous l'avons appelé tableau de bord e la sécurité dynamique (TBSD).

Ce premier chapitre situe brièvement le contexte de ce travail de thèse, énonce les objectifs visés, présente

les contributions apportées, et l'organisation du rapport.

1.1 Limites des tableaux de bord classiques

De nos jours, de nombreuses entreprises utilisent couramment pour le suivi de leurs indicateurs de sécurité des feuilles de calcul Excel ou des logiciels très peu adaptés au contexte et effectuent des requêtes manuelles aux bases de données. Elles sont souvent confrontées à des temps d'analyse de données longs dus à la masse importante d'informations et des divergences dans les chiffres. Les TB traditionnels s'avèrent donc rapidement insuffisants. En effet les données dont nous avons besoin pour analyser ou auditer nos systèmes sur le plan sécurité sont disséminées dans des sources très différentes : fichiers plats, bases hétérogènes, serveurs différents, documents XML. Il est donc nécessaire de regrouper ces données, de les classer, de les structurer en vue de leur analyse. De plus, les accès concurrentiels aux bases sont problématiques, par leur hétérogénéité, par leurs occurrences aléatoires, par leur interférence avec les transactions en cours (risques d'accès simultanés). Les responsables de sécurité gèrent donc une masse d'informations hétérogènes dispersées sur des systèmes différents et ces informations ne sont toujours pas interprétées de la même manière.

1.1.1 Les avantages d'un médiateur à base d'ontologies

Avec les nombreuses avancées dans les technologies de l'information, les solutions de sécurité sont devenues de plus en plus performantes et plus efficaces. Ayant pris conscience de l'extraordinaire potentielle des informations de l'entreprise, couplées à un SI puissant, un nombre grandissant d'éditeurs propose des solutions de sécurité pour ces informations. Très souvent, ces solutions de sécurité sont couplées avec des outils de *reporting* et des TB permettant d'analyser les informations, de voir l'état d'avancement de la PS. Très peu de ces méthodes proposent un système de médiation basé sur les ontologies. La quasi totalité propose un système d'entrepôt de données, pourtant un système de médiation à base d'ontologies a plusieurs avantages, parmi lesquelles :

- la réutilisation
    1. créer et conserver des bases de connaissances réutilisables ;
    2. assembler des bases de connaissances à partir des modules réutilisables ;
- le partage de l'information et la communication
    1. assurer l'interopérabilité entre les systèmes ;
    2. permettre l'échange des connaissances entre les systèmes.
- la réduction des coûts
  réduction des coûts d'exploitation : les coûts d'exploitation des données sont fortement réduits. En effet l'alimentation, la manipulation et l'extraction des données volumineuses est automatique. Chaque décideur peut avoir accès à l'information depuis son poste de travail.
- la qualité et pertinence de l'information

1. chaque terme dans le domaine a une sémantique formelle (descriptive) permettant son exploitation par l'ordinateur
2. l'accès facilité à l'information permet de pouvoir prendre des décisions fondées sur des données précises et non bâties sur de simples hypothèses.
3. la collecte et le rassemblement de l'information permet de créer un savoir collectif sur l'état de sécurité de l'entreprise. Le management des risques est facilité ; ce qui rend la réactivité et la souplesse de la PS grâce à l'implantation facilitée des mesures de sécurité.
4. l'information remontée offre une vue homogène consolidée et fiable des données. La prise de décision est alors facilitée et plus solide, les informations ne sont plus contradictoires.
5. les données étant regroupées et pré-analysées, les temps d'accès sont quasiment immédiats et permettent une meilleure réactivité.

1.2 Problématique et objectifs de la thèse

La SSI se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système, en mettant en place des mécanismes d'authentification et de contrôle. Ces mécanismes permettent d'assurer que les utilisateurs desdites ressources possèdent uniquement les droits qui leurs ont été octroyés. La sécurité doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le SI en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité. La PS est donc l'ensemble des orientations suivies par une entité en termes de sécurité. A ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du SI. Ainsi, il ne revient pas aux administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers ou aux responsables de la sécurité des SI (RSSI), si cette tâche existe au sein de l'organisation. Le rôle de l'administrateur informatique est donc de faire en sorte que les ressources informatiques et les droits d'accès à celles-ci soient en cohérence avec la PS retenue. De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de la conseiller sur les stratégies à mettre en œuvre, ainsi que d'être le point d'entrée concernant la communication aux utilisateurs des problèmes et recommandations en termes de sécurité. Pour synthétiser les informations remontées par les différents maillons de la chaîne ou contrôler la mise en œuvre de la sécurité avec les objectifs fixés, nous devons faire appel aux TB.

Si le terme TB est utilisé depuis déjà plusieurs décennies, il ne désigne pas pour autant le même concept. En un temps pas si lointain, le TB ne servait qu'à contrôler, dans le sens de vérifier, la conformité d'un résultat vis-à-vis des prévisions. Ce TB, utile pour évaluer les écarts entre l'existant et ce qui était prévu, est relativement simple à concevoir. Cependant, pour mettre en œuvre une stratégie dans un contexte changeant, ce n'est pas d'un TB de constat dont nous avons besoin, mais bien d'un TBDS. Il faut alors s'intéresser à une nouvelle

génération de TB proactifs, orientés pilotage et prise de décision quelle que soit l'évolution du contexte. Pour y arriver, plusieurs méthodes de développement de TB ont été proposées, mais il ne se dégage pas une tendance précise. Le Balanced Scorecard (BSC) développé par Kaplan et Northon [Kaplan1990] est un instrument de contrôle de gestion apparu au début des années 1990. Il vise la mesure et l'amélioration de la performance par la définition d'un ensemble d'indicateurs financiers et non financiers, directement liés à la stratégie de l'entreprise. La Généralisation de l'accès aux Informations décisionnelles en s'appuyant sur une Méthodologie d'inspiration Systémique facilitant l'expression des Individualités de l'entreprise (GIMSI) est une méthode de conception du système de Business intelligence (BI) et de TB orienté prise de décision. Structurée en 10 étapes, elle s'inscrit dans un mode de management moderne privilégiant la coopération, le partage de la connaissance et l'intégration performante des outils et techniques de la BI. L'approche par niveaux [CLUSIF1997a], méthode développée par le Club de la sécurité de l'information Français (CLUSIF), met l'accent très particulier sur l'établissement des indicateurs. Ainsi un TB bien précis et adapté à chaque niveau de l'entreprise est un atout certain pour optimiser la qualité des services de sécurité. L'approche [CNRS2004], proposée par le Centre National de Recherche Scientifique Français(CNRS), repose sur les évaluations de l'efficacité de la PS et des moyens mis en œuvre par domaine de sécurité (prévention, détection, réaction, reprise après incident). Elle a pour avantage de suivre de prêt les écarts entre les objectifs fixés et l'état courant de la sécurité. L'approche reposant sur le contexte du SI [DCSSI2003], proposée par la Direction Centrale de la Sécurité des Systèmes d'Information Française (DCSSI), est basée sur les objectifs stratégiques et les évolutions du contexte (du SI, des risques etc.). Elle se rapproche de la méthode par niveaux [CNRS2004] dans la mesure où elle permet de suivre toutes les actions liées à la SSI, permettant ainsi de contrôler que la stratégie définie dans la PS est mise en œuvre par les niveaux de pilotage et opérationnel, et à la remontée des informations pertinentes jusqu'aux décideurs. A ces méthodes s'ajoutent plusieurs méthodes propriétaires développées par des cabinets conseils ou des outils proposés par des éditeurs[1]. La plupart des éditeurs proposent deux types d'outils.

- Les suites logicielles dites blanches : il s'agit des outils du marché s'adressant à n'importe quel domaine d'activité pour lesquels une modélisation spécifique des données de l'entreprise est nécessaire. Ces solutions ont pour avantages d'évoluer fortement et répondent aux besoins métiers multi applications avec l'analyse multidimensionnelle [GMSIH2007]. Elles ont pour inconvénients la complexité d'intégration et un budget élevé. On peut citer la suite Cognos 8.2 de la société COGNOS[2] qui offre un environnement de travail complètement intégré comprenant plusieurs outils destinés à des profils utilisateurs différents. Cette suite propose un large panel de fonctionnalités avec des restitutions très variées : tableaux et graphiques de tout type (possibilité de disposer de graphiques avec plusieurs échelles pour afficher plusieurs indicateurs en même temps), gestion avancée des alertes avec un commentaire et un rapport associé à chacune d'entre elle. Les TB peuvent également être disponibles sur mobile grâce à la solution Cognos 8 Go ! Mobile.

[1] IBM, Microsoft, Oracle etc.

[2] http ://www.cognos.com/fr/

- Les solutions dites "pré-packagées", il s'agit des solutions "clé en mains" proposées par des éditeurs, dédiées au domaine de la sécurité et comprenant un choix de TB, un ensemble d'indicateurs pré-formatés, et des fonctionnalités diverses. Elles ont pour avantages la facilité de mise en oeuvre, et pour inconvénients la difficulté à créer des rapports différents de ceux prédéfinis. On peut citer PMSI de la société ABC Objectif[3]. Pour cette solution, le chargement de données externes se fait par fichier plat, le stockage par une base relationnelle et les datamarts métier. Les données sont présentées au sein d'un portail accessible aux utilisateurs disposant d'un compte et d'un mot de passe. L'administrateur peut facilement sélectionner les indicateurs visibles pour chaque type d'utilisateur dans une page d'administration.

Ces solutions sont modélisées selon une logique choisie par l'éditeur et il reste à les paramétrer dans le cadre de l'entreprise. Que ce soit les méthodes citées ci-dessus ou les outils existants, l'exploitation de la masse d'informations est problématique, poussant à une interprétation différente selon qu'on passe d'un secteur d'activité à un autre ou lorsqu'on change de culture. Dans un environnement informatique interactif et dynamique, où la reconfiguration et le déploiement des systèmes sont permanents, il manque aujourd'hui une référence, pour l'élaboration d'un TBS, qui s'adapte au contexte. Notre but dans ce travail de thèse est d'apporter une solution, en ajoutant dans la chaine de traitement de données une ontologie de la sécurité. Dans une première étape, nous construisons une ontologie de la sécurité que nous insérons dans le processus de traitement de l'information qui servira de construire les bases de connaissance qui seront exploitables par les TBS.

1.3 Contributions

Dans un premier temps nous avons analysé les travaux qui ont été réalisés dans ce domaine, ensuite nous avons analysé quelques méthodes de conception des ontologies, TB de pilotage et des TB de sécurité. Ces études nous ont permis de mieux comprendre les limites des méthodes classiques de développement de TB. Nous avons proposé une démarche pour construire une ontologie globale de sécurité. Cette démarche comprend cinq étapes : une étape d'extraction des termes de la base de la méthode harmonisée d'analyse de risques (MEHARI) pour choisir les bons termes, une étape de classification et d'analyse des termes extraits, une étape comportant les questions de compétences permettant ainsi de voir les termes qui répondent au mieux à la démarche, une étape de construction de la hiérarchie des classes. On arrive finalement à plus de 400 classes. Ensuite nous avons proposé une démarche d'évolution d'ONTOSEC. Cette démarche s'inspire des méthodes et des algorithmes d'évolution des ontologies. Nous avons proposé des algorithmes permettant d'ajouter, de supprimer ou de modifier des concepts dans ONTOSEC. Ces algorithmes s'appliquent lorsque le contexte change ; par exemple lorsqu'un risque n'est plus considéré pour l'entreprise comme tel, il devrait être pris comme tel et les répercussions sur les mesures associées ou les indicateurs associés devraient être pris en compte. Les parties les plus cruciales sont l'extraction de données, leur stockage, et la restitution de données sous forme exploitable par le TBDS. Le but est de donner l'impression d'interroger un système centralisé et homogène alors que les

[3]http ://www.pmsipilot.com

sources interrogées sont réparties, autonomes et hétérogènes.

Dans un deuxième temps nous avons développé cette ontologie à l'aide de l'éditeur PROTEGE 2000[4] de l'Université de Stanford. Nous avons ensuite développé un TBS s'appuyant sur cette architecture afin d'apporter une réponse aux problèmes cités plus haut. Nous nous sommes limités à charger les données manuellement dans l'ontologie, mais il peut aussi très bien se faire automatiquement par des adaptateurs, vendus sur le marché.

Pour terminer, nous appliquons le modèle dans le cadre propre de l'entreprise TELKOM SA. Nous concluons ce travail en donnant les perspectives futures.

1.4 Organisation de la thèse

Ce travail de thèse est organisé comme suit :

- le chapitre 1 (**Introduction**) introduit ce travail en présentant le contexte, et donne quelques définitions essentielles du domaine de la sécurité. Il présente les deux approches d'intégration des données : l'approche Global as View (GAV) et l'approche Local as View (LAV). Il énonce la problématique et les contributions apportées, et enfin présente l'organisation de ce document

- le chapitre 2 (**Théories et modèles**) présente la littérature théorique sur la sécurité des SI. Il présente des méthodes d'élaboration des TB telles que : Le BSC, GIMSI, la méthode par niveaux du CLUSIF, la méthode par domaines du CNRS, la méthode reposant sur la politique de sécurité la DCSSI, etc. Il élabore une comparaison de ces méthodes, présente les inconvénients, les avantages et les limites de chacune d'elles. Il fait une analyse des TB existants sur le marché. Il présente aussi la notion d'ontologie, les méthodes de construction et les différentes opérations de traitement : la suppression, l'ajout, la modification des concepts, le *matching* et le *mapping* des ontologies

- le chapitre 3 (**Construction d'une ontologie dans le domaine de la sécurité des systèmes d'information**) permet de concevoir une ontologie dans le domaine de la sécurité des SI : ONTOSEC. C'est une ontologie globale comprenant trois ontologies locales : risques, contre-mesures de sécurité et indicateurs de sécurité. Nous décrivons chaque terme et leurs attributs, les relations entre les termes. Nous avons développé un TBS qui exploite le méta modèle construit dans le chapitre précédent. Dans un premier temps chaque utilisateur peut en fonction de son niveau d'accès choisir dans la hiérarchie les indicateurs qu'il souhaite inclure dans le TB. L'application accède à l'ontologie et recueille les informations sur les mesures et les risques associés. Elle affiche les résultats de la requête. Tout changement (impact, potentialité) sur le risque, ou changement (efficacité) sur la mesure a un impact directement sur l'indicateur.

[4] http ://protege.stanford.edu/

Nous avons choisi une représentation en "bâtons" mais toute autre représentation est possible.

- le chapitre 4 (**Validation**) permet de valider notre approche dans le cas concret d'une entreprise appelée TELKOM SA.

- le chapitre 5 (**Conclusion**) conclut ce travail de thèse, résume les principales contributions et énonce les perspectives futures.

Chapitre 2

Théories et modèles de la sécurité des systèmes d'information

Ce chapitre nous permet, dans un premier temps, d'introduire les notions nécessaires sur la sécurité informatique. Il présente ensuite les concepts que nous allons être amenés à utiliser dans le travail de thèse.

2.1 Généralités

Information : l'information [ISO17799], constitue un bien pour l'organisme. Elle est à ce titre un élément important de l'activité de l'organisme et nécessite une protection adéquate. L'information se présente sur des supports variés, elle peut être disponible sur papier, stockée électroniquement, transmise par voie postale ou électronique, diffusée sur des supports audiovisuels ou verbalement. Quel que soit le support ou le moyen utilisé pour la partager ou la stocker, il convient de toujours protéger l'information de manière adéquate. Les définitions suivantes concernent les termes les plus employés dans le guide [PSI1994], et qui pourraient recevoir, selon les domaines d'application, des sens différents.

Organisme : par convention de lecture pour cette thèse, le terme "Organisme" désigne tout établissement public ou privé et comprend l'ensemble des biens, des personnes et des services attachés à la réalisation d'une mission ou d'un métier.

Système d'information : le SI comprend les matériels informatiques et les équipements périphériques, les logiciels et les microprogrammes, les algorithmes et les spécifications internes aux programmes. On inclue la documentation, les moyens de transmission, les procédures, les données et les paramètres de contrôle de sécurité, les données et les informations qui sont collectées, gardées, traitées, recherchées ou transmises par ces moyens ainsi que les ressources humaines qui les mettent en œuvre. En effet, le SI est caractérisé par l'organisation humaine qui donne une signalisation au recueil, au traitement, à la production des données contribuant au fonctionnement opérationnel.

Système informatisé : c'est un sous-ensemble d'un SI, il fait référence à la dimension électronique pour le recueil, le traitement, la transmission et le stockage des données. Il fait abstraction de l'organisation humaine ainsi que de tous les traitements et les transferts d'informations manuels.

Système informatique : il regroupe traditionnellement les centres informatiques de l'organisme, comprend les données, supports, logiciels, équipements, documentations. Il comprend l'aspect transmission, c'est-à-dire les équipements qui le supportent y compris les matériels d'extrémité (poste téléphonique, télécopie, etc.) et les équipements électroniques déconnectés ou isolés (micro ordinateurs, portables, photocopieuse, etc.) .

Système d'information décisionnel : c'est une exploitation coordonnée et cohérente des informations de l'entreprise et de son environnement dans le but de faciliter la prise de décision par les décideurs, c'est-à-dire la compréhension du fonctionnement actuel et l'anticipation des actions pour un pilotage éclairé de l'entreprise.

2.2 La sécurité des systèmes d'information

Après avoir défini les termes précédents, il convient de préciser ce qu'est la sécurité de l'information et quels en sont ses tenants et ses aboutissants. Dans le domaine de l'informatique, le mot "sécurité" peut couvrir plusieurs acceptions [Deswarte2003]. La première correspond à la sécurité "innocuité" (en anglais safety) et concerne la prévention de catastrophes. Dans ce sens, un système informatique aura une sécurité satisfaisante si aucune de ses défaillances éventuelles ne peut provoquer des dégâts importants, où si celles qui peuvent provoquer des dégâts importants sont suffisamment peu probables. Ce type de sécurité est bien évidemment une exigence majeure lorsque le bon fonctionnement du système informatique est nécessaire pour la sauvegarde de vies humaines ou de l'environnement, ou encore d'intérêts financiers importants. C'est en particulier le cas des systèmes tels que les systèmes de transport ou de contrôle des centrales nucléaires. Une seconde acception du terme de sécurité correspond au mot anglais "security" et concerne la capacité du système informatique à résister à des agressions externes physiques (incendie, inondation, bombes, etc.) ou logiques (erreurs de saisie, intrusions, piratages, logique malicieuse, etc.). C'est généralement le sens choisi par les spécialistes de l'audit de sécurité, lorsqu'ils doivent, pour une entreprise donnée, évaluer les risques liés à l'informatique. Mais plutôt que de définir la sécurité vis-à-vis des conséquences de la non sécurité (au sens safety) où vis-à-vis des agressions contre la sécurité (au sens "security"), il semble préférable, à l'instar des ITSEC [ITSEC1991], de considérer la sécurité comme la combinaison de quatre propriétés : la **confidentialité**, l'**intégrité**, la **disponibilité** et la **traçabilité** de l'information. Notons que ces quatres propriétés se rapportent à l'information, et le terme information doit être pris ici dans son sens le plus large, couvrant non seulement les données et les programmes, mais aussi les flux d'information, les traitements et la connaissance de l'existence de données, de programmes etc. Cette notion d'information doit aller jusqu'à couvrir le système informatique lui-même. La sécurité, telle qu'elle est ici appréhendée, implique d'empêcher la réalisation d'opérations illégitimes contribuant à mettre en défaut l'une des quatres propretés citées plus haut, mais aussi de garantir la possibilité de

réaliser les opérations légitimes dans le système. Assurer la sécurité du système, c'est assurer que les propriétés retenues soient vérifiées, autrement dit, garantir la non occurrence de défaillances vis-à-vis de ces propriétés.

2.2.1 Confidentialité

Selon les définitions données par les différents organismes de normalisation : *International Standard Organisation* (ISO) et le Centre Européen de Normalisation (CEN), la confidentialité est la propriété qui assure que seuls les sujets habilités, dans les conditions normalement prévues, ont accès au système. Son corollaire est la protection de la vie privée des sujets dont les données personnelles font l'objet d'un traitement automatisé et qui relève d'un principe constitutionnel. Dans un SI, les possibilités d'atteinte à la confidentialité sont nombreuses. Elles consistent à essayer d'obtenir des informations qui doivent être protégées selon la PS, en dépit des moyens de protection et des règles de sécurité. Par exemple, les écoutes passives consistent à accéder aux données transmises sur un canal de communication (câble de réseau, par exemple) ou stockées sur un support vulnérable (disques externes, par exemple). Une telle écoute peut, dans certaines circonstances, permettre d'accéder à des informations sensibles, comme le mot de passe d'un utilisateur tapé sur un terminal connecté à un ordinateur central, et qui transite en clair entre ce terminal et la machine. On voit également que cette attaque peut être particulièrement difficile à identifier à posteriori étant donné l'absence totale de traces laissées dans le système. Les atteintes à la confidentialité sont nombreuses :

- *hacker* ou *cracker* est une personne qui exploite les vulnérabilités du système pour y pénétrer. Plusieurs exploitent des mots de passe des utilisateurs autorisés pour accéder au système ;

- *social engineering* est une technique qui a pour but d'extirper des informations à des personnes. Contrairement aux autres attaques, elle ne nécessite pas de logiciel. La seule force de persuasion est la clé de voûte de cette attaque. Il y a quatre grandes méthodes de social engineering : par téléphone, par lettre, par internet et par contact direct.
  - Par téléphone : le hacker vous contactera par téléphone. C'est la technique la plus facile, son but est d'avoir le renseignement le plus rapidement possible. Un bon hacker aura préparé son personnage et son discours, il sera sûr de lui, il sera très persuasif dans le timbre de sa voix.

  - Par lettre : le hacker vous fera une lettre très professionnelle. Au besoin, il n'hésitera pas de faire appel à un imprimeur pour avoir du papier à lettre comportant un logo, un filagramme, téléphone, fax, email. Il utilisera très certainement une boîte postale pour l'adresse de sa société fictive.

  - Par internet : le hacker se fera facilement passer pour un opérateur système, un responsable informatique ou un ingénieur système.

  - Par contact direct : c'est le *social engineering* le plus difficilement réalisable par un hacker. Il sera équipé pour que vous n'y voyiez que du feu : costume, cravate, attaché-case, agenda rempli, docu-

ments divers, carte de visite, badge... Si le hacker prend de tels risques, c'est qu'il est déterminé à obtenir les renseignements souhaités, il sera donc très persuasif.

2.2.2 Intégrité

L'intégrité est la propriété qui assure qu'une information n'est modifiée que par les utilisateurs habituels dans les conditions normalement prévues. Cela signifie que le système informatique doit empêcher une modification[1] indue de l'information, c'est-à-dire une modification par des utilisateurs non autorisés ou une modification incorrecte par des utilisateurs autorisés. Il doit faire en sorte qu'aucun utilisateur ne puisse empêcher la modification légitime de l'information. De plus, il faut avoir l'assurance que toute modification de données est approuvée et que chaque programme se comporte de manière correcte (c'est-à-dire conformément aux fonctions qu'il est censé remplir, y compris dans ses interactions avec les autres processus). Il faut également s'assurer qu'aucune information ne puisse être modifiée par des intermédiaires, que cette altération soit intentionnelle (par exemple, un utilisateur intervient pour modifier une communication entre deux autres utilisateurs) ou accidentelle (une donnée modifiée lorsqu'elle est communiquée via un support de communication non fiable). Les principes de base utilisés pour établir les contrôles d'intégrité sont :

- le principe du moindre privillège. Les utilisateurs ne doivent avoir accès qu'aux fichiers et programmes dont ils ont besoin pour exercer leurs activités quotidiennes ;

- la séparation des tâches. Elle permet de s'assurer qu'il n'y ait pas un seul employé qui maîtrise le contrôle d'une transaction du début jusqu'à la fin ; plusieurs personnes doivent être responsable du traitement de la transaction. Par exemple toute personne chargée de valider les droits d'accès ne doit pas être simultanément la personne qui donne cet accès ;

- la rotation des tâches. Elle spécifie que l'assignation du travail doit se faire de manière périodique, de sorte que cela soit difficile aux utilisateurs de collaborer en ayant un contrôle total sur les transactions ou les utiliser de manière frauduleuse.

2.2.3 Disponibilité

La disponibilité est l'aptitude d'un SI à pouvoir être employé par les sujets habilités dans les conditions d'accès et d'usage normalement prévus. Le système informatique doit fournir l'accès à l'information pour que les utilisateurs autorisés puissent la lire ou la modifier. Il doit faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information. L'indisponibilité du SI résulte soit d'atteintes majeures à son intégrité au niveau des données, des logiciels ou des matériels telles qu'elles viennent d'être décrites, soit d'une défaillance de l'environnement technique et humain nécessaire à son fonctionnement.

[1] Le terme de modification doit être entendu au sens large, comprenant à la fois la création d'une nouvelle information, la mise à jour d'une information existante, et la destruction d'une information

La gestion de la sécurité implique l'identification des actifs informationnels d'une organisation et le développement, la documentation et l'implantation de politiques, de standards, de procédures et de directives. Des outils de management comme la classification de l'information, l'évaluation et l'analyse des risques sont utilisés pour identifier les menaces, classifier les actifs, hiérarchiser les vulnérabilités du système, en vue d'implanter des contrôles efficaces.

2.2.4 Traçabilité

L'information est aujourd'hui cruciale, la dématérialisation quasi-totale des échanges et des opérations impose aux organismes, de contrôler pleinement leur SI. La traçabilité est la clé d'une collecte utile de l'information à travers l'ensemble du SI, tant pour préserver les valeurs immatérielles de l'entreprise que pour réagir en cas d'actions anormales ou frauduleuses. Elle permet d'identifier préventivement, les anomalies, les erreurs et les tentatives de fraude ou de fuite d'informations, protégeant le patrimoine informationnel de l'entreprise. La traçabilité doit couvrir la totalité du SI, fédérant ainsi les données (logs) d'infrastructure (connexions Internet ou distante, service IP tels que DNS, DHCP, proxy, traces des opérations sur les serveu), mais aussi les traces au niveau applicatif (ERP, applications métier).

2.2.5 Autre facettes de la sécurité

La sécurité est parfois représentée par d'autres caractéristiques, telles que l'intimité, l'authenticité, l'auditabilité, la pérennité, la protection etc. Toutes ces propriétés peuvent être exprimées en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité, appliquées à des informations et des méta-informations [Deswarte 2003]. L'intimité concerne le respect des libertés individuelles et la protection de la vie privée. Elle se rapporte directement à la confidentialité d'informations (données à caractère personnel) et de méta-informations (identité de l'utilisateur qui a effectué une certaine opération).

L'authenticité est la propriété d'être vrai pour un message ; elle est équivalente à la fois à l'intégrité du contenu du message (intégrité des informations) et de son origine (méta-information).

L'auditabilité, avec les propriétés qui en découlent (imputabilité, irréfutabilité, etc.) [Trouessin 2000], l'auditabilité correspond à la disponibilité et à l'intégrité d'un ensemble de méta-informations relatives à l'existence d'une opération, à l'identité de la personne qui a réalisé l'opération, à l'instant de l'opération etc. La propriété de non répudiation garantit qu'un sujet ayant réalisé une action dans le système ne puisse nier l'avoir réalisée.

La non-répudiation correspond à la disponibilité et à l'intégrité de méta-informations telles que l'identité de l'émetteur (et éventuellement l'instant d'émission) d'un message pour la non-répudiation de l'origine, ou telles que la réception et l'identité du récepteur d'un message pour la non-répudiation de réception.

La pérennité permet de respecter les règles de conservation de l'information en fonction de sa nature pour éviter toute destruction.

Dans le paragraphe qui suit, nous traitons de la gestion de la sécurité de l'information, entendu comme un ensemble contenant : l'analyse du risque, la classification de l'information, la politique, les procédures, les standards, les *Baselines* et *guidelines* et les mesures de sécurité.

2.3 Gestion de risques

Le concept de gestion des risques a très certainement fait son apparition à la fin des années 50 aux États-Unis dans le domaine financier, en relation avec des questions d'assurance [Dubois1996]. Par la suite, cette notion a été étendue à d'autres domaines, citons par exemple l'environnement, la gestion de projets, le marketing, ainsi que la sécurité informatique qui nous intéresse ici. La gestion de risques est définie par [ISO17799], comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion de risques liés au SI : (1) améliorer la sécurité des SI, (2) justifier le budget lié à la sécurité des SI, (3) prouver la crédibilité du SI à l'aide des analyses effectuées. Lorsqu'on parle des risques, on ne peut pas ignorer la notion d'actif.

Les actifs sont définis comme étant l'ensemble des biens, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement. On distingue les "actifs business" et les "actifs systèmes". Du côté des "actifs business", on retrouve principalement des informations (par exemple des données importantes sur le personnel, les salaires etc.) et des processus (comme la gestion des transactions ou l'administration des comptes). Les "actifs systèmes" de l'organisme sont bien souvent entièrement (ou presque) gérés au travers du SI, ce qui entraîne une dépendance de ces actifs vis-à-vis de ce dernier. On retrouve dans les "actifs systèmes" les éléments techniques, tels les matériels, les logiciels et les réseaux, mais aussi l'environnement du système informatique. C'est cet ensemble qui forme le SI. Le but de la gestion des risques est donc d'assurer la sécurité des actifs, sécurité exprimée la plupart du temps en termes de confidentialité, intégrité et disponibilité, traçabilité constituant les objectifs de sécurité. Ces actifs à protéger sont soumis à des risques de sécurité. L'ISO définit le risque comme une combinaison de la menace, de la vulnérabilité et de l'impact.

RISQUE = MENACE * VULNERABILITE * IMPACT

Cette équation, très utilisée dans la gestion de risques, joue un rôle fondamental. Pour bien comprendre la notion de risques, nous allons nous pencher sur chacune de ses composantes.

La menace (source du risque), est l'attaque possible d'un élément, quelle que soit sa nature sur les actifs. C'est l'agent responsable du risque. "Une menace doit être décrite en citant l'élément menaçant identifié, l'at-

taque et le bien qui en est la cible. Les éléments menaçants devraient être caractérisés par des aspects tels que l'expertise, les ressources disponibles et la motivation. Les attaques devraient être caractérisées par des aspects tels que les méthodes d'attaque, toutes les vulnérabilités exploitées et l'opportunité" [ISO 15408].

"La sécurité a trait à la protection des biens contre les menaces, ces dernières étant classées selon leur potentiel de nuisance envers les biens à protéger. Toutes les catégories de menaces devraient être prises en compte, mais dans le domaine de la sécurité, une plus grande attention est accordée aux menaces liées à des activités humaines malveillantes ou non"[ISO 15408]. La vulnérabilité quant à elle, est une faille ou une faiblesse d'un actif vis à vis de la sécurité. Enfin, l'impact représente les conséquences du risque si la menace arrivait à se produire sur l'organisme et ses actifs.

Afin de protéger les actifs, une politique de traitement de risques doit être mise en place. Elle doit être constituée d'exigences de sécurité permettant de répondre aux risques. Ces exigences vont par la suite entrainer la mise en place de contrôles (ou contre- mesures) à implanter, afin de limiter la cause du risque. Les contres mesures sont de deux types : (1) sur la menace ou la vulnérabilité afin de limiter la cause du risque, (2) sur l'impact afin de limiter la conséquence du risque. L'objectif de la gestion des risques est de :

- pouvoir identifier les valeurs de l'entreprise, le niveau de vulnérabilité face aux menaces, le risque de perte totale ou partielle des valeurs ;
- mettre en place les outils et procédures adéquates pour réduire au maximum ces risques (prévention) ;
- permettre une reprise sur panne (correction) ;
- contrôler la pertinence, la cohérence de la PS et l'adéquation des outils par des contrôles internes, externes (audits).

Cette gestion des risques doit amener les responsables de l'entreprise à se poser les questions afin de les minimiser. Que dois-je protéger ? De qui ? De quoi ? Quels sont les risques ? Quel est le niveau actuel de la sécurité de l'entreprise ? Quel est le niveau à atteindre ? Quelles sont les contraintes ? Quels sont les moyens existants et comment les mettre en place ? La gestion des risques est le premier pallié à réaliser dans l'élaboration de la PS et offre de nombreux avantages. Elle permet d'obtenir une vision objective de son niveau de sécurité, de construire un argumentaire utile à l'arbitrage des dépenses, d'améliorer la SSI de manière à sensibiliser les acteurs du SI (décideurs, utilisateurs, partenaires....)

2.3.1 Classification des méthodes de gestion des risques

Il existe de nombreux outils contribuant à la gestion des risques. Il n'est pas nécessaire de tous les utiliser, mais préférable de suivre une démarche structurée reposant sur une expérience approuvée. Deux types d'approches se distinguent :

- par scénarios de risques
- par construction de risques.

Les premières proposent des scénarios type, elles ne sont pas exhaustives mais représentatives. Les secondes permettent de définir les risques de manière exhaustive et parfaitement adaptés au contexte étudié. Une des

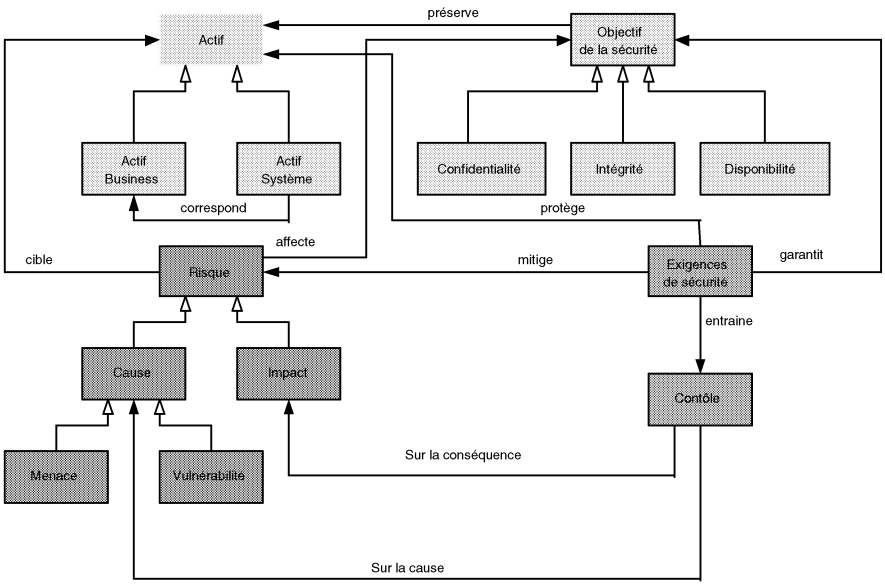

FIG. 2.1 – Les concepts de la gestion de risques

méthodes de gestion de risques par scénarios de risques est la méthode MEHARI alors que la méthode d'Expression des Besoins et d'Identification des Objectifs de Sécurité (EBIOS) permet de gérer par construction de risques. Une autre classification est celle proposée par la DCSSI et élaborée par le Cabinet Français de conseil en sécurité informatique(Intrinsec). La DCSSI distingue d'un côté les « catalogues SSI» et de l'autre les « méthodes SSI». Le terme «catalogue SSI» est employé pour tous les recueils de mesures, d'exigences, de vulnérabilités ou autres éléments sans démarche méthodologique. Parmi ceux-ci, on peut citer :

- les bonnes pratiques et mesures de sécurité : IT Baseline Protection Manual (BSI allemand), ISO 17799, ISO 13335, ACSI 33 (DSD australien), CM 5515 (Otan) ;
- la politique de sécurité : PSI (DCSSI), ISPME (CSE canadien), RFC 1244 (IETF)...
- les catalogues pour l'évaluation de produits : TCSEC (DoDaméricain), ITSEC (CEE), ISO 15408 ;
- les catalogues spécifiques : Sécurité des réseaux : MG-1 (CSE canadien), sécurité des sites : RFC 2196 (IEFT), sécurité des interconnexions : AC35-D/1027 (OTAN), modèle de maturité SSI : SSE-CM (ISSEA).

Le terme de « méthode SSI » désigne quant à lui les démarches de sécurité reposant sur une méthode. Parmi celles-ci, on peut citer :

- les méthodes contribuant à la gestion du risque SSI : Ebios (DCSSI), Marion, MEHARI (CLUSIF), MV3 (CF6), Cramm (CCTA anglais), Ninah (XP CONSEIL), Risk Management Guide, MG-2 (CSE canadien), SP800-30 (NIST), IAM (NSA), Buddy System (Countermeasures Corp.)...

- les méthodes d'audit ou contrôle interne SSI : Massia (DGA), ERSI (Forum des compétences), IPAK (CSI), SP800-26 (NIST)...
- les méthodes d'intégration de la SSI dans les projets : DSIS(DCSSI), Incas (CLUSIF), Orion (Cersiat)...
- les méthodes globales incluant des aspects SSI : COBIT
- les guides de rédaction : Feros, SSRS, SP800-18
- les autres méthodes : Domaines spécifiques : MESSEDI, MUSE.

Le cabinet de conseil Intrinsec distingue quant à lui d'un côté les normes et de l'autre les méthodes. Parmi les normes, on peut distinguer :

- les normes internationales organisationnelles : *Guidelines for the management of IT Security* (lGMITS),(ISO/IEC TR13335) lE Code of practice for information Security management(ISO/IEC 17799) en phase de révision, issu de la norme britannique BS 7799 Part1 - 1999 ;
- les normes internationales techniques : *Evaluation criteria for IT Security* (ISO/IEC 15408), ISO/IEC WD 15947 (norme portant sur le cadre des détections d'intrusions) ;
- les normes internationales de diagnostic et de qualité : ISO/IEC 19011 (Audit), ISO 9004 (Qualité) ;
- les normes nationales organisationnelles : BS 7799-1 (Code of practice for information Security management, élaborée par le British Standard Institute, à l'origine de la norme ISO/IEC 17799) ;
- les normes nationales d'évaluation : BS 7799-2 (Specification for information Security management Systems, élaborée par le British Standard Institute)

Parmi les méthodes, on peut citer :

- les méthodes Françaises : MARION, MEHARI, MELISA ;
- les méthodes non Françaises : COBIT, CRAMM 4.

Enfin, dans le cadre des critères communs ITSEC, la DCSSI a développé différentes méthodes :

- politique de sécurité interne (PSI) ;
- développement de SI sécurisés (DSIS) ;
- expression des besoins et identification des objectifs de sécurité (Ebios) ;
- fiche d'expression rationnelle des objectifs de SSI (Feros) ;
- réalisation des objectifs de sécurité par le choix des Fonctions (Roscof) ;
- guides d'aide à la rédaction des fournitures pour l'évaluation (Garde).

Mais comment faire son choix au milieu de la jungle des référentiels d'analyse de risques ? Une première aide précieuse est fournie via la présentation en amont des fondements caractérisant les concepts et la classification de ces méthodes en plusieurs classes. Ces concepts transcrivent le cadre de compréhension nécessaire pour appréhender sérieusement la matière. Pour réduire le choix au cœur des méthodes formelles, certaines sont actuellement très populaires, faisant référence dans leur domaine. Nous allons voir en détail la gestion de risques selon la méthode MEHARI.

2.3.1.1 Gestion de risques selon MEHARI

MEHARI [MEHARI2004] propose par ses bases de connaissances, plusieurs types d'assistance à la gestion de risques :

- une assistance à l'évaluation de l'exposition naturelle,
- des automatismes d'évaluation des facteurs de réduction de risques (dissuasion, prévention, protection, palliation et récupération) en fonction de la qualité des services de sécurité,
- un tableau générique d'impact intrinsèque pouvant être élaboré à la suite d'une classification ou directement à partir d'une échelle de disfonctionnement,
- des automatismes de calcul de la potentialité et de l'impact, en fonction de l'exposition naturelle, de l'impact intrinsèque et des facteurs d'atténuation du risque, c'est-à-dire en l'absence d'un type de phénomènes conjoncturels particuliers.

Evaluation de l'exposition naturelle : l'exposition naturelle peut varier pour une entreprise en fonction des phénomènes conjoncturels. Il reste pour beaucoup d'entres elles l'exposition normale ou standard à un type de risque.

Exposition naturelle standard : selon MEHARI, les risques se réfèrent à une liste limitée d'événements de base, qu'il s'agisse d'accidents, d'erreurs ou d'actes volontaires (malveillants ou non), pour lesquels une évaluation à priori de l'exposition est donnée. Ainsi, par exemple, il est estimé que l'exposition naturelle "standard " d'une entreprise à un incendie est de niveau 2 (plutôt improbable), à une panne d'équipement informatique de niveau 3 (plutôt probable) et à une erreur pendant un processus de saisie de niveau 4 (très probable). La liste de ces événements et de l'exposition naturelle standard est donnée en annexe A.

Exposition de l'entreprise à un type de risque : l'évaluation standard ci-dessus n'est qu'une évaluation par défaut, l'évaluation directe de l'entreprise à un type de risque particulier est de loin préférable. Pour cette évaluation, il convient de se référer aux définitions des niveaux d'exposition qui ont été données dans le document « Principes et Mécanismes de MEHARI » et qui sont rappelées en annexe B.

Evaluation de l'impact intrinsèque : c'est l'évaluation des conséquences de l'occurrence du risque indépendamment de toute mesure de sécurité. Pour chaque risque, il existe une ressource impliquée ou détériorée. Il peut s'agir d'un type de données ou d'informations dérobées, d'un type de ressource rendue indisponible, ou d'un type de ressource altérée, selon qu'il s'agisse d'un risque mettant en cause la confidentialité, la disponibilité ou l'intégrité d'une ressource. Evaluer l'impact intrinsèque revient à évaluer le niveau de criticité ou de gravité de la perte de la disponibilité, de la confidentialité ou d'intégrité selon le type de ressource mis en cause. La démarche d'évaluation des impacts intrinsèques consiste à remplir un tableau d'impact intrinsèque, basé sur celui fourni en annexe C. L'évaluation de l'impact intrinsèque de chaque risque sera faite très simplement, chaque risque faisant référence à un type de ressource du tableau d'impact intrinsèque et au critère (D, I, C).

Evaluation des facteurs de réduction de risque : l'évaluation de la potentialité et de l'impact d'un scénario de risque repose sur une analyse de l'existence de facteurs de réduction du risque et sur une évaluation de leur niveau. Ces facteurs sont la dissuasion et la prévention pour la potentialité, la protection, la palliation et la récupération pour l'impact. A chaque scénario est associé un ou plusieurs services de sécurité. Cette évaluation se fait en deux étapes : (1) le calcul d'indicateurs d'efficacité des services de sécurité, pour chaque type de mesure et (2) le calcul des facteurs de réduction de risque proprement dit. Pour chaque scénario et chaque type de mesure, on définit un indicateur d'efficacité.

- EFF-DISS : efficacité des mesures dissuasives.
- EFF-PREV : efficacité des mesures de prévention.
- EFF-PROT : efficacité des mesures de protection.
- EFF-PALL : efficacité des mesures palliatives.

Ces indicateurs sont calculés par le biais des formules comprenant les fonctions MIN (arg1 ; arg2 ;....) ou MAX (arg1 ; arg2 ;...), arg1, arg2,... étant les identifiants des services de sécurité. La fonction MIN signifie que les services appelés en argument sont complémentaires et que si l'un d'eux est faible, l'ensemble sera faible ; ça peut être le cas, par exemple de la gestion des autorisations d'accès et de l'authentification ; si l'un d'eux est faible, le contrôle d'accès dans son ensemble est faible. La fonction MAX signifie que les services appelés sont alternatifs : si l'un d'eux est de bonne qualité, l'ensemble le sera ; ça peut être le cas, par exemple et selon certains scénarios, du contrôle d'accès aux données et du chiffrement de ces données. MEHARI propose une assistance en fournissant des valeurs calculées pour les facteurs de réduction de risque ; ces valeurs doivent cependant être contrôlées avant utilisation. Les formules peuvent être de la forme :
EFF-PALL = arg1.
EFF-PREV=MAX (arg2 ; MIN (arg3, arg4, arg5)).
La première formule signifie que l'efficacité des mesures palliatives est directement fonction du service arg1 et a pour valeur le niveau de qualité de ce service. La deuxième formule indique que l'efficacité des mesures préventives est égale à la plus grande valeur du service arg2, et de la fonction représentant le minimum des services arg3, arg4, arg5.

Calcul des facteurs de réduction de risques : Les coefficients d'efficacité ci-dessus EFF-XXXX, étant calculés à partir des valeurs de service de sécurité ne sont pas des nombres. Pour faciliter la lecture et la compréhension, MEHARI définit les facteurs de réduction de la forme STATUS-XXXX (Par exemple STATUS-DISS, pour le facteur de dissuasion). Les STATUS sont obtenus par simple arrondi à la valeur entière la plus proche.
STATUS-XXXX = 1 si EFF-XXXX < 1,5 et STATUS-XXXX = 2 si 1,5 = EFF-XXXX < 2,5.
STATUS-XXXX = 3 si 2,5 = EFF-XXXX < 3,5 STATUS-XXXX = 4 si 3,5 = EFF-XXXX.
Où XXXX représente DISS, PREV, PROT, PALL ou RECUP et la valeur de l'exposition naturelle sera notée STATUS-EXPO. Avant de retenir les facteurs de réduction pour chaque risque, il convient de les contrôler en se référant aux définitions de base desdits facteurs en "annexe E".

Evaluation de la potentialité et de l'impact

Evaluation automatisée de la potentialité : STATUS-P La potentialité s'évalue en fonction d'un indicateur appelé STATUS-P qui est déduit directement des STATUS-EXPO, STATUS-DISS et STATUS-PREV par des grilles d'évaluation en annexe. Trois grilles standard sont prévues en fonction du type de cause. Événement naturel ou accidentel, erreur humaine, acte volontaire (malveillant ou non). La logique de ces grilles d'évaluation est de considérer que, pour un type de cause donné (accident, erreur ou acte volontaire), le même raisonnement devrait être suivi, indépendamment de la description précise du scénario : à exposition égale, dissuasion égale et prévention égale, il devrait être jugé que la potentialité de deux scénarios est la même.

Evaluation automatisée de l'impact : STATUS-I

L'évaluation de l'impact dépend de l'impact intrinsèque du scénario d'une part et du niveau des mesures de protection, palliatives, et de récupération mesurées par STATUS-PROT, STATUS-PALL, STATUS-RECUP. D'autres parts, cette évaluation se fait en deux étapes : (1) évaluation d'un indicateur de réduction d'impact : STATUS-RI et (2) évaluation de l'impact : STATUS-I.

Evaluation de la réduction d'impact : STATUS-RI

Une réduction d'impact STATUS-RI mesure l'atténuation des conséquences du risque, par rapport à l'impact intrinsèque. Il est prévu trois grilles standard d'évaluation en fonction du type de conséquence du scénario : Perte de disponibilité, d'intégrité et de disponibilité.

Evaluation de l'impact

L'impact résiduel est déduit de l'impact intrinsèque et de l'indicateur de réduction d'impact par la formule suivante : I = MIN (IMPACT INTRINSEQUE ; 5 - STATUS-RI).

Grille de calcul de STATUS-I				
STATUS-RI Impact intrinsèque	1	2	3	4
4	4	3	2	1
3	3	3	2	1
2	2	2	2	1
1	1	1	1	1

2.3.1.2 Expression des besoins de sécurité

Il consiste à évaluer les besoins consolidés et à les classer après avoir évalué la gravité d'un ensemble de situations de risques en s'appuyant sur un diagnostic de l'état des services de sécurité. Cette approche est

basée sur la définition de « besoins de service ». Un besoin de service de sécurité est établi pour chaque scénario. Un service de sécurité donné peut avoir un effet sur la gravité d'un scénario. Si tel est le cas, il est considéré qu'il existe, pour ce service, et du fait de ce scénario, un besoin de service. Pour plus de détails, voir "annexe G". Nous avons étudié dans cette section, tous les facteurs liés à la réduction de la potentialité du risque et de son impact. Il reste face à ces risques de noter quelques qualités permettant d'évaluer les mesures de sécurité qui sont mises en place afin de réduire le risque à un niveau acceptable.

2.4 Techniques pour sécuriser un SI

Afin d'éliminer les vulnérabilités, contrer les attaques, et garantir un niveau élevé de protection du SI, on peut utiliser des services, des mécanismes, des outils et des procédures que l'on nomme, de façon générale, des solutions ou des mesures de sécurité. Par exemple, un service d'identification et d'authentification aide à réduire le risque d'intrusion dans un système. Les politiques de sécurité seront présentées comme un dispositif nécessaire pour renforcer la sécurité des systèmes. Puis il conviendra d'aborder succinctement la manière avec laquelle on peut les construire et les implanter. Nous expliquons également d'autres contre-mesures pour renforcer la sécurité comme les mécanismes cryptographiques, l'audit, la détection d'intrusion et la tolérance aux intrusions.

Services de sécurité : un service de sécurité[2] est une réponse à un besoin de sécurité exprimé en termes génériques et fonctionnels décrivant la finalité du service, généralement en référence à certains types de menaces. Cette fonction est indépendante des mécanismes et solutions concrètes permettant la réalisation effective du service. Exemple : le service *Contrôle Accès*, dont la finalité ou la fonction, décrit implicitement par son titre, est de contrôler les accès, c'est à dire de ne laisser passer que les personnes autorisées. La fonction assurée par un service de sécurité peut, elle même, nécessiter plusieurs éléments complémentaires, qui peuvent être considérés comme des sous fonctions ; dans ce cas on parle de sous services de sécurité. Le contrôle d'accès nécessite la connaissance de ce qui est autorisé, de ce qui fait appel à une fonction d'authentification, et le filtrage des accès. Un ensemble de services de sécurité constitue une mesure de sécurité. Certains services peuvent être considérés comme des mesures générales, d'autres comme des mesures techniques. Les mesures générales sont des mesures de sécurité reconnues comme utiles, voire nécessaires, à la sécurité des SI, mais dont l'effet se situe davantage au plan organisation, du pilotage de la sécurité ou de la sensibilisation sans influence directe sur des situations de risques précises. Les mesures techniques ont un rôle précis, une finalité directe et ont un effet immédiat sur certaines situations de risques qu'il est possible de préciser. La mesure de la qualité de services de sécurité dépend de : l'efficacité du service, sa robustesse et les moyens de contrôle de son bon fonctionnement. Nous y reviendrons en détails lors de l'élaboration de notre démarche. Un service de qualité 1, est un service de qualité minimale. Il peut ne pas être efficace face à un scénario quelconque. Un service de qualité 2 reste efficace et résiste à un agresseur moyen, mais pourrait être insuffisant contre un bon professionnel du domaine considéré. Un service de qualité 3 reste efficace et résiste aux agresseurs mais pour-

[2] http ://www.CLUSIF.fr

rait être insuffisant face aux spécialistes (hackers chevronnés) ou d'événements exceptionnels (catastrophes naturelles). Un service de qualité 4 est le plus élevé et reste efficace et résiste aux agresseurs.

2.4.1 Politiques de sécurité

La gestion des autorisations a pour but de ne permettre que les actions autorisées, c'est-à-dire à empêcher qu'un utilisateur puisse exécuter les opérations qui ne devraient pas lui être permises [Deswarte2003]. Pour définir quelles sont les opérations permises et celles qui sont interdites, il faut définir une politique de sécurité (PS). Dominique Floquet et Serges Krief[3] le voient plutôt comme une vision stratégique de la direction en matière de sécurité. Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du SI de l'entreprise. Selon Solange Ghernaouti-Hélie[4] la PS permet de transcrire le travail de modélisation effectué pour comprendre les risques et leurs impacts, en des mesures concrètes de sécurité. Sa spécification est l'un des garants du bon dimensionnement des mesures de sécurité et d'une gestion efficace. Elle donne de la cohérence à la gestion et permet d'adopter vis à vis des risques et menaces, une attitude préventive et proactive et pas seulement réactive. Elle permet de lier la stratégie de sécurité de l'entreprise à sa réalisation opérationnelle. Elle doit être dynamique et remise en question de manière permanente afin de suivre l'évolution des systèmes, de l'environnement et des risques. Au vu de ceci, et selon Abou El Kalam[5] pour construire une politique de sécurité il faut d'une part, définir un ensemble de *propriétés* de sécurité qui doivent être satisfaites par le système ; par exemple une information catégorisée ne doit pas être transmise à un utilisateur non habilité à la connaître, et d'autre part établir un schéma d'autorisation, qui présente les règles permettant de modifier l'état de protection du système.
L'entreprise doit d'abord déterminer les normes générales de sécurité qui s'appliquent à l'ensemble de ses systèmes et de son personnel. Chaque employé de l'entreprise est concerné par la réalisation de la PS. Sa validité sera renforcée si l'organisation développe une éthique d'entreprise et si elle stipule également ses exigences de sécurité envers ses partenaires externes. La réalisation d'un inventaire complet, sous forme d'enquêtes et de questionnaires de tous les éléments matériels, logiciels, organisationnels, économiques et humains intervenant dans la chaîne sécuritaire, contribue à réaliser la PS.
Parallèlement, il est nécessaire d'effectuer une classification des ressources pour déterminer leur degré de sensibilité. Ce dernier indique leur importance en cas de perte, d'altération ou de divulgation des données. Plus les conséquences sont graves pour l'entreprise, plus la ressource est sensible, possède de la valeur et est à protéger. La PS peut s'appliquer à la totalité ou à une partie du SI de l'entreprise. Selon [PSSI2004], elle peut concerner l'ensemble du SI de l'entreprise, elle peut également être restreinte à un SI particulier, par exemple lié à un métier de l'entreprise ou à un système transversal (messagerie, intranet...). Dans ce cas, il peut exister plusieurs PS dans une entreprise. Elles doivent être cohérentes entre elles. Cette cohérence est assurée grâce à la formalisation d'une PS globale (PSG). Les autres politiques sont alors des déclinaisons de la PSG dans un environnement métier ou technique particulier, pour des instances spécialisées ou des cas particuliers. Pour

[3] Paroles de professeurs juin 2004
[4] auteur du livre : Sécurité Internet ; Stratégies et technologies, Dunod (octobre 2000)
[5] Thèse de doctorat sur les modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales

élaborer une PSG adaptée à l'entreprise, il est recommandé de réaliser une analyse des risques spécifiques au contexte afin d'en ajuster les règles de sécurité. La politique élaborée, il faut ensuite mettre en place les procédures, les standards, les directives et les configurations de référence.

2.4.1.1 Politique, Procédures, Standards, Directives et Configuration de référence

Les politiques, les procédures, les standards, les *Baselines* et *Guidelines* sont les éléments clés qui permettent de s'assurer que le personnel comprend les exigences nécessaires pour effectuer leurs tâches journalières. La PSG définit les exigences au niveau général, les standards spécifient les outils nécessaires, les directives désignent les paramètres à utiliser, et les procédures donnent étape par étape la manière d'exécuter les activités. La sécurité de l'information contient les directives du management permettant de créer un programme de sécurité établissant les buts, les objectifs et les responsabilités. Cette politique définit à un niveau très élevé, la philosophie du management. C'est un bref document. La politique fonctionnelle implémente à un niveau élevé la politique et définie les objectifs de la sécurité des informations. Les standards donnent plus de détails pour chaque domaine, les procédures décrivent comment implanter un standard.

Exemple de politique ;
La compagnie utilise le système de voice-mail et le système de mail électronique (email) pour effectuer les activités quotidiennes au sein de la compagnie. Ces systèmes sont composés des équipements et des données enregistrées dans le système et sont en tout moment la propriété de la compagnie .

- Tous les messages créés, reçus, envoyés ou enregistrés dans le système restent la propriété de la compagnie.
- Les messages doivent être limités dans le cadre du business et ne pas être envoyés pour des raisons personnelles.
- La compagnie se réserve le droit de vérifier tout message composé, envoyé ou reçu.
- Tout employé qui apprend toute violation de cette politique doit le notifier au directeur des ressources humaines.

Une politique est brève et est définie à un niveau très élevé de l'organisation. Une PS de l'information contient les directives du management pour créer un programme de sécurité, établir ses objectifs, comme le montre la figure 2.2. Une fois qu'une PSG d'entreprise globale a été approuvée par l'entité de direction de l'organisation, il convient de développer une infrastructure de prise en charge des objectifs de contrôle. Ce cadre peut inclure d'autres politiques fonctionnelles, telles que : politique de l'utilisation de l'e-mail et de l'internet, politique des accès à distance.

Du fait qu'une politique soit écrite à un niveau élevé de l'organisation, les organisations doivent en même temps développer des standards, directives, configuration de références et des procédures qui offrent aux employés, managers, une méthode consistante pour implanter les politiques. Les politiques donnent les exigences légales, et sont donc dérivées de ces éléments.

Standards sont définis comme des produits spécifiques ou mécanismes choisis pour une utilisation universelle dans l'organisation, dans le but de supporter la politique.

Exemple : lutte antivirus ;

- *politique : les propriétaires des informations sont responsables de leur apporter un environnement sécurisé dans lequel l'information peut être maintenue sans en violer l'intégrité ;*
- *standard : les Propriétaires des informations doivent utiliser le logiciel antivirus "XXXXX" pour s'assurer que le système est protégé contre tout élément destructif comme les virus.*

Configuration de références sont obligatoires et permettent d'implanter des *packages* sécurité pour s'assurer que le résultat de l'implantation soit à un niveau de sécurité consistant dans l'organisation. Elles sont crées pour informer des groupes d'utilisateurs comment implanter la sécurité pour chaque système, de sorte que le niveau de sécurité requis soit atteint de manière consistante. Elles sont plus générales et permettent d'atteindre les objectifs fixés par la politique en implantant les contrôles non couverts par les procédures. On peut citer comme exemple :

- *politique : les propriétaires des informations sont responsables de leur apporter un environnement sécurisé dans lequel l'information peut être maintenue sans violer l'intégrité ;*
- *standard : les propriétaires des informations doivent utiliser le logiciel de contrôle d'accès "XXXXX" pour s'assurer que le système est accessible seulement par les personnes autorisées ;*
- *Configuration de réferences : les valeurs des paramètres disponibles dans le logiciel de contrôle d'accès "XXXXX" doivent être configurée de la manière suivante pour s'assurer que tous les éléments de l'organisation maintiennent un niveau de sécurité consistent.*

Les Procédures sont des actions requises, décrivant pas à pas comment la politique, les standards et les directives seront implantés dans un environnement donné. On peut avoir comme exemple de procédures : enregistrement d'utilisateur, établissement de contrats pour des missions de sécurité, réponse aux incidents, destruction du matériel ;

- *politique : les propriétaires des informations sont responsables de leur apporter un environnement sécurisé dans lequel l'information peut être maintenue sans violer l'intégrité ;*
- *standard : les propriétaires des informations doivent utiliser le logiciel antivirus "XXXXX" pour s'assurer que le système est protégé contre tout élément destructif comme les virus ;*
- *procédures : tous les utilisateurs de l'anti virus "XXXXX" doivent avoir une signature anti virale mise à jour toutes les semaines. Les employés doivent éteindre leurs machines en fin de journée pour éviter*

tout accès non autorisé et toute contamination possible de virus.

- *les employés doivent protéger leurs disquettes en écriture dès que possible ;*
- *cette procédure doit être suivie pendant qu'on met à jour la signature antivirale toutes les semaines ;*
- *les employés doivent signaler tout accès non autorisé et infection de virus au groupe sécurité ou au help desk, et voici la procédure pour le faire (suivi de la procédure actuelle).*

Directives directives sont plus générales et permettent d'atteindre les objectifs de la politique en implémentant des contrôles non couverts par les procédures.

- *Politique : les propriétaires des informations sont responsables de leur apporter un environnement sécurisé dans lequel l'information peut être maintenue sans violer l'intégrité.*

- *Standard : les Propriétaires des informations doivent utiliser le logiciel antivirus "XXXXX" pour s'assurer que le système est protégé contre tout élément destructif comme les virus.*

- *Procédures : tous les utilisateurs de l'anti virus "XXXXX" doivent avoir une signature anti virale mise à jour toutes les semaines. Les employés doivent éteindre leurs machines en fin de journée pour éviter tout accès non autorisé et toute contamination possible de virus.*

- *Guidelines : les employés ayant accès à un ordinateur doivent avoir reçu une formation sur les menaces que peut causer l'infection par les virus et comprendre leur responsabilité personnelle pour la protection de leur propre système.*

2.4.1.2 Normes BS 7799, ISO 17799 et ISO 27002

Plusieurs normes, méthodes et référentiels de bonnes pratiques en matière de sécurité des SI sont disponibles. Elles constituent des guides méthodologiques ainsi que le moyen de fournir l'assurance d'une démarche de sécurité cohérente. L'ISO a entrepris un vaste effort de rationalisation des travaux existants donnant naissance à la série ISO 27000. Certaines sont obligatoires pour obtenir une certification (27001 et 27006), les autres ne sont que des guides :

- ISO 27000 : vocabulaire.
- ISO 27001 : système de management de la sécurité de l'information (SMSI) (en vigueur).
- ISO 27002 : renumérotation de l'ISO 17799 (2007).
- ISO 27003 : implantation(en développement).
- ISO 27004 : métriques et mesures (en développement).
- ISO 2005 : management du risque (ISO 1335-2).
- ISO 2006 : conditions d'accréditation pour les organismes certificateurs de ISMS.
- ISO 27799 : ISO 17799 pour la sécurité 8 en développement).

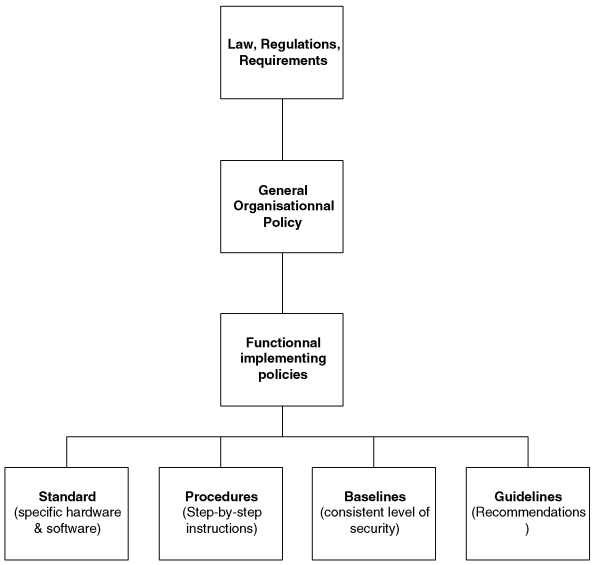

FIG. 2.2 – Vue générale d'une politique

Normes ISO 27001, BS 7799-2 : La norme ISO 27001, publiée en Novembre 2005, définit la politique du management de la sécurité des SI au sein d'une entreprise. Elle est issue de la BS 7799-2 :1999 *Specification for information security management systems* qui définit les exigences à respecter pour créer un System de management de la sécurité. Elle spécifie en annexe certains contrôles de sécurité, tirés de la norme ISO 17799, dont la mise en œuvre est obligatoire. La norme ISO 27001 comprend 6 domaines de processus :

- définir une PSSI
- définir le périmètre du Système de Management de la sécurité de l'information ;
- réaliser une évaluation des risques liés à la sécurité ;
- gérer les risques identifiés ;
- choisir et mettre en œuvre les contrôles.

Comme ISO 9000, l'ISO 27001 porte moins sur l'efficacité des dispositions mises en place, que sur leur existence, et la mise en place d'une boucle d'amélioration (PDCA).

Normes BS 7799, ISO 17799 et ISO 27002 : La norme ISO 17799 (2005), prochainement renommée 27002, est directement tirée de la BS 7799-1 (créée par le BSI British Standard Institute). Elle correspond à un niveau de détails plus fin que la 27001 et spécifie une PSSI. C'est une liste détaillée et commentée de mesures de sécurité. Cette norme est un guide de Bonnes Pratiques pour maîtriser la sécurité d'un SI. Plusieurs versions de la BS 7799 ont été élaborées depuis le début des années 1990 et la dernière est devenue la norme ISO/IEC 17799.

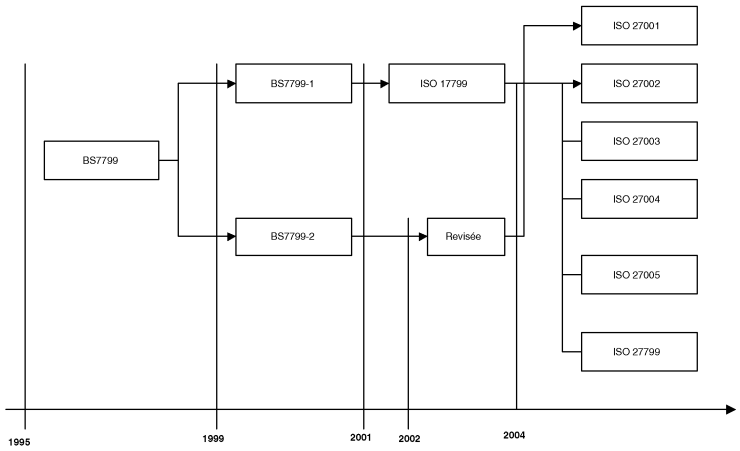

FIG. 2.3 – Evolution ISO27000

2.4.1.3 Liens entre ISO 27000 et les autres méthodes de sécurité

Nous avons vu plus haut l'analyse des risques faite avec la méthode MEHARI, nous venons de décrire ISO 27000 et sa suite. Le but de cette section est de donner le lien entre la norme et quelques méthodes. La norme ISO 17799 ne précise aucune obligation quant au choix de la méthode d'analyse de risques, chaque organisme ayant ses besoins et ses spécificités propres. Comme nous l'avons vu plus haut lors de la classification des méthodes, il en existe plusieurs dont le choix dépendra du contexte d'utilisation (application, type de résultat attendu, spécificité du domaine, compatibilité avec le référentiel de l'entité...). Les plus connues sont notamment MEHARI, EBIOS (et feu MARION). L'analyse de risques avec la méthode MEHARI permet de choisir des mesures de sécurité appropriées face au risque en vigueur. Ces mesures peuvent être issues de la base de connaissance de MEHARI ou de la norme ISO 17799. Quant à la méthode *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE) développée par l'université de Carnegie Melon, l'analyse de risques permet de choisir des mesures de sécurité issues de la base de connaissance Octave ou définies à partie d'ISO 17799. Il convient de confirmer que la norme est un document de référence basé sur un consensus couvrant un large intérêt industriel ou économique et établi par un processus volontaire. A la différence, une méthode est un moyen d'arriver efficacement à un résultat souhaité, précis. La méthode n'intègre pas la notion de document de référence, ni la notion de consensus. On ne peut donc pas opposer norme et méthode, mais plutôt les associer, une méthode sera l'outil utilisé pour satisfaire à une norme.

2.4.2 Autres contre-mesures

Il peut arriver des cas ou la PS peut être incomplète, i.e. ne couvre pas tous les aspects suite à une erreur de conception ou un choix délibéré de l'équipe en charge. On peut dans ce cas renforcer la sécurité par d'autres contre-mesures, telles que les mécanismes cryptographiques, la certification, etc.

2.4.2.1 Mécanismes cryptographiques

La cryptologie se compose de la cryptographie et de la cryptanalyse. La cyptographie est l'art d'écrire des secrets pour les rendre inintelligibles à des tiers. La cryptanalyse est l'art de retrouver les secrets cachés dans des informations inintelligibles. Il ne sera ici question que des éléments de cryptographie, qui sont à la base de nombreux mécanismes de sécurité : le chiffrement, le hachage et la signature. Le domaine de la cryptographie aborde les principes, les moyens et les méthodes permettant de garantir : l'intégrité, la confidentialité, l'authenticité, la non répudiation. La cryptographie est l'art de rédiger des secrets, elle permet de stocker et transmettre l'information sous une forme telle que seules les personnes concernées peuvent en prendre connaissance.

Chiffrement et déchiffrement Les fonctions de base de la cryptographie sont le chiffrement et le déchiffrement. Le chiffrement vise à assurer la confidentialité d'informations ; il consiste à transformer un texte en clair en un cryptogramme, à l'aide d'un chiffre (ou algorithme de chiffrement) et d'une clé de chiffrement. Le déchiffrement consiste à transformer le cryptogramme en un texte en clair identique à celui d'origine, à l'aide d'un algorithme de déchiffrement et d'une clé de déchiffrement.

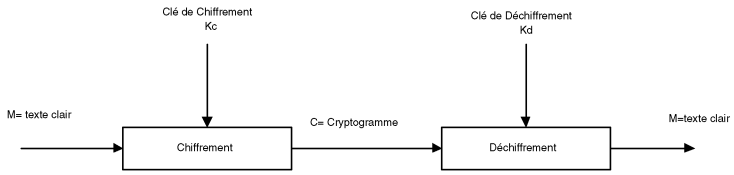

FIG. 2.4 – Chiffrement et Déchiffrement

Chiffrement en continu

Pour comprendre le cryptage en continu, il suffit de connaitre par exemple les vidéos au format RealVideo très répandues sur internet : on visualise l'image au fur et à mesure que les données sont reçues. Le principe est le même dans le cas de nos "Stream Ciphers" : le cryptage est effectué bit à bit sans attendre la réception complète des données à crypter. Un algorithme de chiffrement en continu doit présenter les caractéristiques suivantes :

Chiffrement par blocs

Quatre modes de chiffrement par bloc sont utilisés : *Electronic CodeBook* (ECB), *Cipher Block Chaining* (CBC), *Cipher FeedBack* (CFB) ou *Output FeedBack* (OFB). Le cryptage en blocs (block-cipher) est au contraire beaucoup plus utilisé et permet une meilleure sécurité. Les algorithmes concernés sont également plus connus (DES, AES, Skipjack...) ; leur nom vient du fait qu'ils s'appliquent à des blocs de données et non à des flux de bits (cf. stream-ciphers). Ces blocs sont habituellement de 64 bits mais cela dépend entièrement de l'algorithme utilisé et de son implantation. De même, la taille de la clé varie suivant l'algorithme et suivant le niveau de sécurité requis ; ainsi, un cryptage de 40 bits (c'est-à-dire utilisant une clé longue de 40 bits) pourra être déclaré faible puisque aisément cassable. Un cryptage de 56 bits (qui est le standard dans le cas du DES) sera qualifié de moyen puisque cassable mais nécessitant pas mal de moyens pour être exploitable

(vis-à-vis du temps requis et de la valeur des données). Enfin, un cryptage de 128 bits (valeur standard utilisée par Rijndael alias AES) est plutôt fort à l'heure actuelle. Le mode ECB est le plus simple des modes et s'applique aux blocks ciphers. Il revient à crypter un bloc indépendamment des autres ; cela permet entre autre de crypter suivant un ordre aléatoire (bases de données, etc.) mais en contrepartie, ce mode est très vulnérable aux attaques. Le mode CBC peut-être utilisé par les algorithmes en bloc. C'est d'ailleurs le mode le plus courant. Il permet d'introduire une complexité supplémentaire dans le processus de cryptage en créant une dépendance entre les blocs successifs ; autrement dit, le cryptage d'un bloc va être d'une manière ou d'une autre, lié à ou aux blocs/chiffrés précédents. Le mode CFB est un mode destiné aux blocks ciphers dans le but d'en autoriser une utilisation plus souple, qui s'apparente plus à celle des algorithmes en continu. On peut le considérer comme un intermédiaire entre les deux.

2.5 Intégration de données hétérogènes

La diversité des sources d'informations et leur hétérogénéité est une des principales difficultés rencontrées de nos jours. Cette difficulté se fait ressentir dans tous les domaines où les applications s'appuient sur d'énormes sources d'informations variées afin de traiter leurs opérations. L'intégration doit donner l'impression d'utiliser une source de données unique, homogène et centralisée. Il existe deux approches utilisées jusqu'à présent : une approche médiateur et une approche à entrepôts de données.

2.5.1 Approche médiateur

L'objectif est de donner l'impression d'interroger un système centralisé et homogène alors que les sources sont réparties, autonomes et hétérogènes. Un médiateur comme le montre la figure 2.5 comprend un schéma global, dont le rôle est central. C'est un modèle du domaine d'application du système. Cette approche présente un avantage de pouvoir construire un système d'interrogation de sources de données sans toucher aux données qui restent stockées dans leurs sources d'origine. Le médiateur ne peut pas évaluer directement les requêtes qui lui sont posées car il ne contient pas les données, ces dernières étant stockées dans leurs sources d'origine. L'interrogation des sources se fait à travers des adaptateurs, appelés aussi wrappers en anglais, qui traduisent les requêtes réécrites en termes de vues dans le langage de requêtes spécifiques acceptées par chaque source.

L'extraction est une opération très souvent effectuée par un outil appelé *Extract Transform Load* (ETL) qui consiste à aller chercher les données où elles se trouvent, les trier et les transformer éventuellement afin d'effectuer un prétraitement pour faciliter l'analyse. Dans cette phase, se font aussi le nettoyage des données, la suppression des doublons, et la détection des données non conformes. Ensuite, les données sont centralisées dans les bases de données du *DatawareHouse*. L'extraction et une partie de la transformation peuvent bien être groupées dans le même composant logiciel, tel qu'un wrapper ou un ETL. L'étape d'intégration peut être couplée avec des possibilités de transformation de données riches dans un même composant logiciel, qui habituellement, réalise le chargement dans l'entrepôt de données. Toutes les étapes de traitement peuvent aussi

être groupées dans un même logiciel. Si les étapes d'extraction et d'intégration sont séparées, les données nécessitent d'être stockées entre les deux. Ceci est possible en utilisant un media.

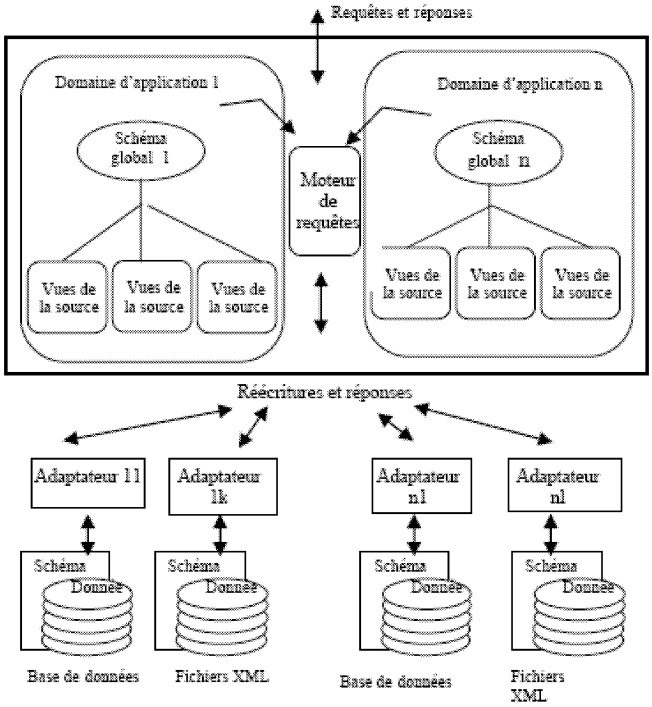

FIG. 2.5 – Architecture d'un système médiateur

2.5.2 Approche entrepôts de données

Un *data warehouse* répond aux problèmes de données surabondantes et localisées sur de multiples systèmes hétérogènes, c'est une architecture capable de servir de fondation aux applications décisionnelles. On distingue deux niveaux dans la construction des entrepôts de données. Le premier correspond à la construction des données opérationnelles, et de l'entrepôt global. Le second niveau englobe tous les entrepôts de données locaux.

2.6 Les tableaux de bord

2.6.1 Généralités

La conception des TB tend à occuper une place prédominante assez représentative des attentes insatisfaites des entreprises en matière de pilotage. Jusqu'à ces dernières décennies, la question de l'aide au pilotage était en effet moins présente. Lorsque le contexte était stable et la concurrence particulièrement faible, rechercher l'augmentation continue de la productivité, ainsi que la diminution des coûts de revient, était encore la meilleure

des stratégies. Les TB de cette époque, limités à des mesures exclusivement économiques et productivistes, étaient tout à fait adaptés. Aujourd'hui, le contexte a fortement changé, pour garantir une réelle rentabilité des capitaux investis, il faut élaborer des stratégies bien plus conséquentes. Il faut donc suivre plus précisément le progrès continu selon les axes choisis par l'équipe de direction lors de l'élaboration de la stratégie.

Les TB stratégiques et plus particulièrement, le modèle du « Balanced Scorecard» (BSC) développé par Kaplan et Norton dans [Kaplan1992], suscitent un intérêt croissant auprès des chercheurs comme des professionnels du contrôle de gestion. Outil de pilotage stratégique, ils apparaissent comme des instruments de prédilection au service des directions générales. Traduire la stratégie en termes opérationnels, mettre l'organisation en adéquation avec la stratégie, transformer la stratégie en un processus continu [Kaplan2001] comptent parmi les objectifs affichés par les concepteurs du BSC qui inscrivent ainsi leur modèle dans la problématique de l'alignement stratégique. Le BSC associe des mesures financières à des mesures non financières, toutes reliées à la performance globale de l'entreprise. Dans sa présentation générique, il est organisé autour de quatre axes principaux qui sont l'axe financier, l'axe clients, l'axe processus internes et enfin l'axe apprentissage et innovation. Une des hypothèses principales est qu'il existe des interdépendances entre chacun des axes, ce qui conduit à la construction de cartes stratégiques [Kaplan2000]. La méthode GIMSI est une méthode de conception du système de *Business Intelligence* (BI) et de TB orientés prise de décision. Structurée en dix étapes, elle s'inscrit dans un mode management moderne privilégiant la coopération, le partage de la connaissance et l'intégration performante des outils et techniques de la BI. C'est une méthode centrée sur l'homme, décideur en situation. Ce sont les hommes qui prennent les décisions. S'ils ignorent tout de la stratégie poursuivie, si le système n'est pas adapté à leurs besoins précis, ils ne prendront pas les décisions. A côté de ces TB stratégiques, sont aussi développées des démarches d'élaboration de TBS.

La SSI est une fonction stratégique. En ce sens, qu'elle est une fonction de direction, mais sans information à la prise de décisions, comment une direction peut-elle assumer ce rôle ? Comment peut-elle avoir une connaissance du niveau de sécurité globale du SI, suivre la qualité et mise en œuvre des PS, répartir efficacement les budgets alloués à la sécurité ? C'est le TBS qui, fournissant une information de synthèse, mettant en évidence des tendances, soulignant des vulnérabilités, des faiblesses ou des insuffisances, lui en donne les moyens. Ainsi le TBS n'est pas seulement un instrument de pilotage de la sécurité, il est aussi un outil de management indispensable.

Plusieurs démarches d'élaboration des TBS ont été développées. La méthode par "niveaux", développée par le CLUSIF présente les indicateurs sous forme d'un arbre à trois niveaux. Les indicateurs sont organisés sous forme d'arbre en trois niveaux : opérationnel, fonctionnel et stratégique. Au niveau opérationnel les indicateurs remontent les informations quantitatives (mesures techniques permettant d'affiner les réglages des alertes, des détecteurs d'incidents ou d'autres dispositifs techniques de sécurité) ; Au niveau fonctionnel les indicateurs remontent des informations sur l'efficacité de la politique de sécurité, la qualité des outils et méthodes utilisés, la conformité de ce qui est fait avec les objectifs stratégiques, etc. Les indicateurs opérationnels permettent

d'alimenter un ou plusieurs indicateurs fonctionnels voire stratégiques.

Le CNRS a développé une méthode reposant sur les évaluations de l'efficacité de la politique de sécurité et des moyens mis en œuvre par domaine de sécurité : prévention, détection, réaction. Dans le domaine de prévention, la politique mise en œuvre vise à dissuader les agressions, à diminuer la probabilité d'apparition d'un incident en minimisant les vulnérabilités tant techniques qu'organisationnelles et à limiter l'ampleur des dommages si une attaque a réussi. Dans le Domaine de détection, la politique de mise en œuvre vise à détecter un incident le plus tôt possible lorsqu'il se produit. Dans le domaine de la réaction, il s'agit de mettre en place l'ensemble des mesures palliatives lorsqu'un incident est survenu afin de minimiser l'impact de cet incident, faire cesser la malveillance et réunir les preuves pour lancer éventuellement des poursuites judiciaires. Nous reviendrons en détails sur ces méthodes dans la suite.

2.6.2 Les indicateurs

2.6.2.1 Le concept de performance

Qu'est-ce que la performance de l'entreprise ? D'après Philippe Lorino dans son article "Les Tableaux Bord révisés", si l'on admet que la performance de l'entreprise est fondamentalement d'essence économique, elle s'identifie à la création nette de richesse, car l'entreprise consomme des ressources (le temps des personnes, des capitaux, des matériaux, de l'espace...) pour produire des prestations. La performance apparaît donc comme un ratio, pas toujours mesurable, entre la valeur C des ressources détruites (les coûts liés au fonctionnement de l'entreprise) et la valeur V des prestations obtenues ([Lorino1995] [Lorino1997]).

2.6.2.2 Indicateurs de performance

Lorino définit un indicateur de performance (IP) comme une information devant aider un acteur, individuel ou plus généralement collectif, à conduire le cours d'une action vers l'atteinte d'un objectif ou devant lui permettre d'en évaluer le résultat. Cette définition montre d'emblée que l'IP n'est pas une mesure "objective ", attribut du phénomène mesuré indépendant de l'observateur, mais il est construit par l'acteur [Lorino1995], en relation avec le type d'action qu'il conduit et les objectifs qu'il poursuit. L'indicateur n'est pas nécessairement un chiffre mais l'IP peut prendre toute forme informationnelle répondant à l'une ou l'autre des deux fonctions évoquées dans la définition (conduite de l'action, évaluation de résultats) : jugement qualitatif, signe binaire oui/non, graphique... Par exemple, les indicateurs de pilotage jalonnent des actions dont les résultats sont mesurés par les indicateurs de résultat. Les indicateurs de résultat de certaines actions sont des indicateurs de pilotage pour d'autres actions inscrites sur un horizon de temps plus long.

2.6.2.3 La pertinence opérationnelle de l'indicateur

Il n'y a d'utilité que relativement à une action à piloter (à lancer, à ajuster, à évaluer), donc est étroitement lié à un processus d'action précis (par exemple, processus d'usinage, processus d'accueil des clients). Selon

Lorino la "pertinence opérationnelle " de l'indicateur, est loin d'être systématiquement assurée. Elle soulève notamment le vieux problème, délice des manuels de gestion depuis des décennies, de la "contrôlabilité" de la performance : le manager, ou l'entité concernée, ont-ils en mains les leviers d'action qui leur permettent d'influer de manière décisive sur le niveau de performance atteint et mesuré par l'indicateur ? Une chose à ne pas oublier, c'est la relation entre l'indicateur et l'action. L'idée de plusieurs auteurs à ce sujet est d'avoir une relation de l'action vers l'indicateur. Le choix de l'action doit fonder l'indicateur et non l'inverse (l'indicateur n'ayant d'utilité que pour piloter l'action et son résultat) cela implique que les indicateurs sont construits de manière contingente aux choix des modes d'action, et, à contrario, que les actions ne soient pas dictées par des indicateurs qui porteraient en eux-mêmes, de manière quasi-magique, le choix des actions pertinentes, comme semblent le penser Kaplan et Norton [Kaplan1996]. L'indicateur doit avoir une pertinence stratégique, il doit correspondre à un objectif, dont il mesure l'atteinte (indicateur de résultat) ou qu'il informe sur le bon déroulement d'une action visant à atteindre cet objectif (indicateur de pilotage).

2.6.2.4 L'indicateur doit avoir une efficacité cognitive

Lorino insiste sur cet aspect, car destiné à l'utilisation par des acteurs précis, généralement collectifs (équipes, y compris équipe de direction), qu'il doit aider à orienter leur action et à en comprendre les facteurs de réussite. Nous devons sans cesse nous poser la question suivante. L'indicateur est-il correctement associé à un acteur ? Cette condition, "l'efficacité cognitive" ou ergonomique de l'indicateur, signifie que celui-ci doit pouvoir être lu, compris et interprété aisément par l'acteur auquel il est destiné. Cette préoccupation n'est que marginalement présente dans les entreprises (sauf les rares exceptions où les enjeux, notamment de sécurité, ont justifié des efforts particuliers : citons les centrales nucléaire, les centres de production sensibles des grandes entreprises etc.). Elle est pourtant essentielle, et appelle le développement d'une véritable ergonomie cognitive des outils de gestion. L'indicateur se trouve en quelque sorte au centre d'un triangle (stratégie traduite en objectifs, processus d'action, acteur). En résumé nous sommes du même avis avec Lorino lorsqu'il relève que : l'IP

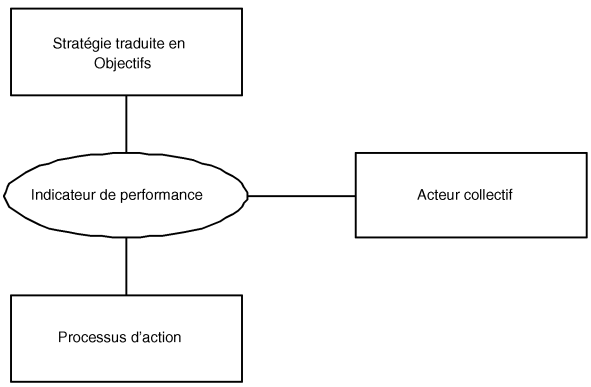

FIG. 2.6 – Le triangle de l'indicateur (stratégie, processus, acteur collectif)

résulte de deux jugements subjectifs portés sur les acteurs. (1) si l'IP est en place, c'est que certains acteurs

ont jugé qu'il constitue une mesure pertinente du déroulement ou du résultat d'une action. Or la mesure n'est jamais donnée par la réalité observée, elle est construite par l'acteur : elle résulte d'une interprétation. On a là un jugement "métrologique" fondant le choix de l'indicateur comme "indicatif" de ce qu'on veut suivre et mesurer. (2) Par ailleurs, le choix d'un indicateur de pilotage renvoie nécessairement au choix d'une action comme moyen pertinent d'atteindre un objectif. On a là un second jugement "subjectif", de type cause effet. Le lien de l'indicateur de pilotage avec un objectif stratégique n'est jamais direct. On ne choisit pas des indicateurs de pilotage pour poursuivre un objectif, on choisit des actions par rapport auxquelles on construit ensuite des indicateurs de pilotage. Le choix d'un indicateur de pilotage renvoie au choix préalable d'une action, donc à un jugement cause effet, réalisé ou ratifié par l'acteur. Le lien de l'indicateur avec l'objectif se fait donc à travers un double processus d'interprétation par les acteurs (figure 2.7), résumé par les deux questions suivantes : (1) pour atteindre cet objectif, quelle action faut-il engager (interprétation causes à effets) ? (2) pour évaluer le déroulement ou le résultat de cette action, quelle information faut-il utiliser (interprétation de type "mesure") ?

Le premier type d'interprétation s'appuie sur un modèle cause effet, proche de ce que les théoriciens de l'apprentissage organisationnel (Argyris, Schön) appellent "théorie de l'action" du type : "si nous faisons cela dans un tel contexte, nous obtenons tel type de résultat ; pour obtenir tel type de résultat, nous devons faire cela". L'indicateur repose sur une connaissance collective de l'action, mais, une fois en place, il doit contribuer à faire évoluer cette connaissance. Il constitue une base d'apprentissage sur les enchaînements causes à effet de l'action.

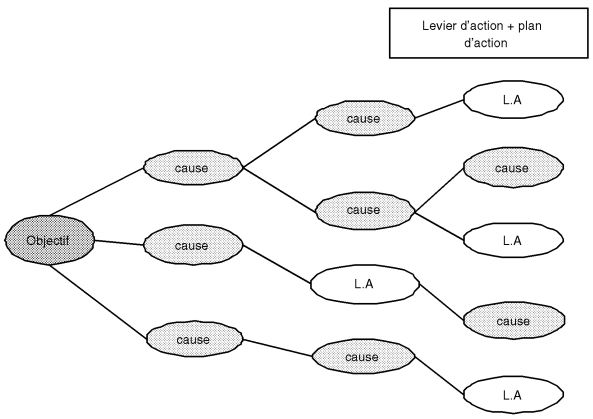

FIG. 2.7 – La structure cause - effet : Source Le Balanced ScoreCard revisé

2.6.2.5 La pertinence stratégique et opérationnelle des indicateurs

Un modèle causes à effets

Le système d'indicateurs devrait logiquement être l'image d'un modèle causes à effets portant sur l'action ; exemple qui pourrait s'appliquer au domaine de la sécurité. Le système d'indicateurs présente les étapes jugées

clés du modèle causes à effets "stratégicoopérationnel " (Quelles actions pour quels objectifs ?) d'indicateurs destinés à évaluer l'avancement des actions (réalisons-nous les actions décidées ?) et, à travers les résultats enregistrés, la validité du modèle causes à effets (les actions décidées et réalisées conduisent elles bien aux résultats attendus ?). Sur le modèle causes à effets, Kaplan et Norton semblent hésiter entre deux positions peut-être compatibles, mais clairement distinctes :(1) Le modèle causes à effets doit-il relier les mesures de performance à un chiffrage d'enjeux financiers équivalents, position dominante dans leur article de 1992 [Kaplan1992], (2) ou doit-il relier les mesures de performance à l'expression d'une stratégie multicritères, position dominante dans leur article de 1996 [Kaplan1996]. Dans sa forme logique la plus simple, le modèle causes à effets est arborescent, et fonde une structure d'indicateurs elle-même arborescente : un effet peut avoir plusieurs causes, bien identifiables, selon des niveaux successifs de causalité qui nous éloignent de l'objectif visé (lien de plus en plus indirect) mais nous rapprochent des potentiels d'actions pertinents (agir sur les causes amont et non sur des symptômes intermédiaires).

La relation de cause effet ne peut bien s'appliquer que si le problème posé par l'objectif est moins complexe et bien structuré dans un environnement certain. La construction d'une structure de causes à effets n'est pas aisée, c'est ce que Lorino essaie d'expliquer en disant qu'elle devient mal déterminée et non linéaire, plus proche d'interactions en boucle, avec des niveaux variables de corrélation entre phénomènes.

TAB. 2.1 – Exemple de système d'indicateurs

Objectifs	indicateurs résultats
Assurer la continuité de fonctionnement	Nbre de sauvegardes réalisées sur la période
Détecter et traiter les incidents	Pourcentage de résolution d'incidents
Assurer le fonctionnement du réseau	Temps moyen d'arrêt du réseau au cours de la période

2.7 Les méthodes de conception de tableaux de bord

2.7.1 Le Balanced ScoreCard

Le BSC est un instrument de contrôle de gestion apparu au début des années 1990 dans les écrits de Robert Kaplan et David Norton. Il vise la mesure et l'amélioration de la performance par la définition d'un ensemble d'indicateurs financiers et non financiers, directement liés à la stratégie de l'entreprise. Ces indicateurs sont regroupés autour de quatre axes préétablis : finances, clients, processus internes et apprentissage organisationnel. Le pilotage stratégique et le pilotage opérationnel sont imbriqués dans différents axes, grâce à une articulation entre les indicateurs stratégiques et des indicateurs historiques. Ces indicateurs sont choisis selon une vision de l'organisation comme un processus, et sont liés de ce fait, par une chaîne de causalité.

D'après Kaplan et Norton, il existerait un lien de causalité entre les différents axes du BSC : une bonne maîtrise du processus interne associé à un réel investissement de l'entreprise dans la recherche de l'innovation et dans

la promotion d'une logique d'apprentissage organisationnel, vont améliorer la satisfaction des clients, entraînant par là même l'atteinte des objectifs financiers de l'entreprise. Le BSC permet de suivre avec précision le progrès continu selon les axes choisis par le comité exécutif lors de l'élaboration de la stratégie. Il met à disposition plusieurs indicateurs auxquels les dirigeants sont sensibles. Ces indicateurs, qualitatifs et quantitatifs, sont distribués selon quatre perspectives : financier, client, processus interne, apprentissage organisationnel. On comprend donc que cette méthode propose d'élaborer la stratégie en respectant l'équilibre des quatre perspectives précédentes. Le BSC étant un outil de mesure de la stratégie, il est indispensable que ce dernier soit clairement explicitée. Pour cela, il est possible de dresser une carte de la stratégie déclinée selon les quatre perspectives citées ci-dessus.

La carte stratégique ou la vision stratégique est en effet le point central du système. Elle est l'expression des hypothèses stratégiques et définit les relations de cause à effet entre les mesures de résultats retenus et les déterminants de la performance. L'établissement de cette carte nécessite un travail de fond plus que conséquent. La qualité du système de pilotage est directement dépendante de la pertinence et de la vraisemblance de la carte stratégique.

L'équilibre des quatre perspectives est très important, il différencie le BSC des autres TB très souvent rencontrés. Un axe ne doit pas être privilégié par rapport aux autres. La tendance habituelle à se concentrer habituellement sur l'axe financier ne permet pas de piloter efficacement son entreprise dans un environnement dynamique comme le nôtre actuellement. Chaque perspective est ensuite déclinée en objectifs stratégiques auxquels sont associés des indicateurs, leurs valeurs cibles et les leviers d'action permettant de les atteindre. Selon Kaplan et Norton, chaque mesure sélectionnée pour le BSC doit être un élément d'une chaîne de relation de cause à effet exprimant l'orientation stratégique de l'entreprise. Avec l'approche BSC, piloter la performance d'une entreprise revient en fait, à faire en sorte que les actions soient conformes au plan stratégique des dirigeants.

2.7.1.1 Les limites du Balanced Score Card

En premier lieu, le BSC repose sur la notion d'un équilibre qui n'est pas facile à obtenir. Beaucoup d'entreprises commencent une démarche de mise en place de BSC, et obtiennent finalement un TB, avec un axe financier très développé, qui n'est pas du tout équilibré. De plus, le BSC n'est pas adapté à tous les types d'entreprises. Il soutend une structure d'entreprise de type anglo-saxon. Dans une entreprise latine, la mise en place stricte du BSC risque de créer chez les employés un sentiment de flicage et aboutira très certainement à une augmentation de la rétention d'information plutôt qu'un travail collaboratif.

Le TB est un ensemble dans lequel, on retrouve de grandes familles d'indicateurs, qui correspondent à des facteurs communs à deux ou plusieurs objectifs. Il n'y a aucune raison que la structure de causalité, et donc celle du TB, soit standard, quelle que soit l'entreprise, et permanente dans le temps. Elle est au contraire contingente à la stratégie comme le relève Lorino dans le "TB révisé". Il semble y avoir une certaine incohérence de la part

de Kaplan et Norton [Kaplan1992] [Kaplan1996], dans leurs travaux sur le "Balanced Scorecard ", à insister sur la nécessaire liaison causale du TB avec la stratégie, d'une part, et à prôner une structure standard en 4 parties ("finance " ou "point de vue de l'actionnaire ", "client ", "processus internes " et "savoir innovation"), d'autre part. Le TB n'apporterait rien de nouveau par rapport aux TB existants. Ces derniers comportaient déjà une association d'indicateurs financiers et non financiers. Le déploiement mécanique et descendant du BSC établit une discussion entre la phase de la formulation de la stratégie et la phase de sa mise en œuvre, et ne tient donc pas compte de la nature collective du processus d'élaboration de la stratégie. De plus, il ne prend pas en compte l'existence de marge de manœuvre aux niveaux inférieurs de l'organisation. Enfin, le système de rémunération fondé sur les performances, préconisé dans le BSC, pourrait créer ou aggraver les tensions au sein de l'entreprise.

Kaplan et Norton parlent de l'élaboration et de la mise en œuvre de la stratégie, ils ne se réfèrent à aucun modèle stratégique précis comme base de leur raisonnement. Par ailleurs, la vision, qui est la vocation de l'entreprise, est mise au même niveau que la stratégie, puis écartée dès que les auteurs traitent de l'application du BSC. En outre il y'a contradiction sur la primauté ou non de l'objectif financier sur les autres objectifs, d'autant plus que les fondements du modèle causal du BSC, ne sont pas explicites. L'universalité de ce modèle causal quelle que soit la stratégie peut être contestée. [Lorino2001], Atkinson, Waterhouse et Wells [1Wells 997], soulignent que le BSC en tant que système de mesure de la performance devrait davantage mettre l'accent sur les engagements de l'entreprise envers ses différentes parties prenantes et contrôler les variables qui matérialisent ses engagements contractuels. A leur avis, le BSC présente les deux inconvénients suivants : (1) il met trop l'accent sur le suivi de la contribution des collaborateurs et des fournisseurs et pas suffisamment sur l'importance des aspects intangibles. (2) Il exclut l'environnement externe comme dimension importante ayant un impact sur la performance de l'entreprise. Cependant, lorsque la performance des entreprises dépend davantage d'éléments exogènes qu'endogènes, on comprend le sens de la seconde critique formulée par Atkinson [Atkinson1996]. Certaines entreprises y ont remédié et l'on rencontre fréquemment des BSC comprenant une cinquième perspective appelée "Environnement". Cette perspective réunit les éléments clés hors contrôle qui influencent les variables d'actions et de résultats de l'entreprise. Cette adaptation est louable et permet à la fois de renforcer le processus de responsabilisation et d'accroître l'apprentissage organisationnel par l'ajout d'éléments clés dans le modèle d'entreprise.

2.7.2 La Méthode GIMSI

La démarche BSC est centrée sur la stratégie et son application, alors que, dans la méthode GIMSI, ce sont la motivation et l'implication des hommes de terrain qui sont au centre. Structurée en 10 étapes, elle s'inscrit dans un mode management moderne privilégiant la coopération, le partage de la connaissance. Ainsi, à la traditionnelle approche Top->Down, GIMSI greffe une dimension *Bottom->Up* et se focalise sur la question essentielle : comment maîtriser les risques en situation d'incertitude, pour prendre du mieux possible les décisions sur le terrain ? en proposant de suivre le chemin tracé par la méthode, son auteur Alain Fernandez veut inciter l'entreprise à réfléchir en termes de stratégie et objectifs avant de passer à l'implantation d'un sys-

tème de mesures de performance. De plus, les indicateurs doivent être construits et choisis en tenant compte, non seulement des objectifs de l'entreprise, mais également du contexte local et des hommes qui pilotent à ce niveau. Ce que le concepteur de la démarche peut éviter à tout prix, c'est la réduction du TB à un ensemble d'indicateurs synthétiques prédéterminés. L'objectif essentiel de cette méthode est la pertinence des indicateurs qui sont la base de tout projet de pilotage. C'est cette pertinence qui donne sa valeur ajoutée au pilotage. Il s'agit d'une démarche incrémentale : l'approche est progressive par projet, pour construire le système de pilotage global. La performance n'est plus perçue, comme dans le BSC, comme la conformité des actions aux plans venus d'en haut, mais comme la capacité à réagir, la pro-activité, sans pour autant négliger la cohérence. Les trois principaux facteurs de succès identifiés sont : la communication, la capacité locale à décider, et la coopération étendue. Elle place les acteurs au premier plan, avant la stratégie. Comme pour le BSC, une carte stratégique va être dressée, mais avec des perspectives suivantes :

- une perspective centrale "processus interne et SI ", qui relie les cinq autres perspectives ;
- une perspective clients ;
- une perspective actionnaires ;
- une perspective Partenaires ;
- une perspective Personnels ;
- une perspective Public .

Chacune de ces perspectives sera, comme dans la méthode BSC, déclinée en objectifs, indicateurs, valeurs cibles, leviers d'action. La disparition de la perspective financière en tant que perspective séparée permet de ne pas se focaliser sur elle. Elle se retrouvera déclinée sur les six perspectives citées ci-dessus.

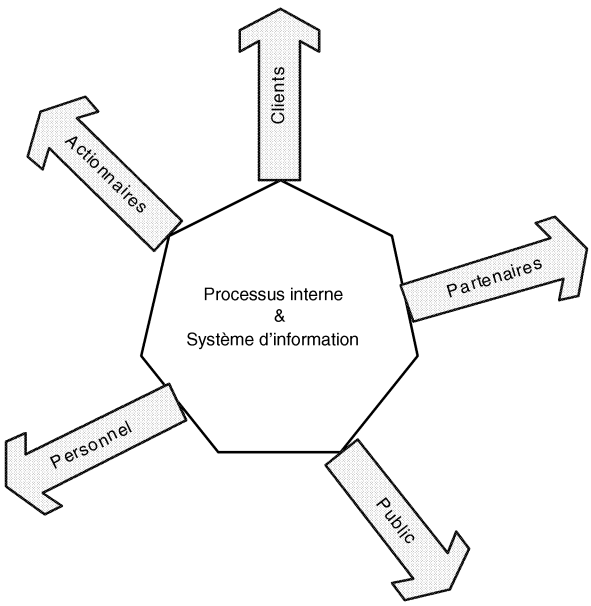

FIG. 2.8 – La démarche GIMSI

Cette méthode présente aussi comme le BSC des avantages significatifs. Par exemple, le fait de vouloir faire le lien entre la performance opérationnelle et la performance financière. Considéré aussi comme un support de communication entre les différents responsables, il permet de suivre le niveau d'atteinte des objectifs de performance et de lier la rémunération à la performance. Elle est très souple et offre la possibilité de réagir rapidement si une opportunité se présente car elle est centrée sur les personnes qui agissent et non sur l'élaboration à haut niveau d'une stratégie précédent à toute action corrective.

2.7.2.1 Les limites de GIMSI

La méthode GIMSI n'étant pas centrée sur la stratégie, elle peut manquer de cohérence si la stratégie n'est pas clairement définie par les dirigeants. Elle doit s'accompagner d'efforts importants d'expression et de communication de la stratégie. Enfin, cette méthode est basée sur une notion de bonne volonté des acteurs. Il faudra faire attention à animer et maintenir cette bonne volonté.

2.7.3 Méthode par niveaux

Cette méthode a été développée par le CLUSIF, les TBS peuvent être classé en trois niveaux selon la nature des indicateurs : stratégique, fonctionnel, opérationnel.

2.7.3.1 Niveau stratégique

Les indicateurs appartenant à ce type de TB sont intimement liés à la politique et à l'image de marque de l'entreprise. Ils sont généralement à caractère générique et on les appelle indicateurs de stratégie ou indicateurs de résultat. On peut définir un indicateur de stratégie comme celui qui décrit des résultats, obtenus du point de vue qualitatif, par rapport aux objectifs fixés par la politique de l'entreprise.

2.7.3.2 Niveau fonctionnel

Un indicateur fonctionnel décrit les résultats atteints en termes de qualité avec un double point de vue qui comporte à la fois la vision d'efficacité du fournisseur de service et la vision de satisfaction du client ou utilisateur du service. S'il s'agit d'une entreprise de vente par correspondance, la consolidation de certains indicateurs attachés aux critères de disponibilité et intégrité va permettre d'alimenter les indicateurs de niveau stratégique, les autres seront traités au niveau fonctionnel. C'est au niveau fonctionnel que l'élaboration des indicateurs est plus complexe, mais c'est aussi à ce niveau qu'on peut déceler la plupart des menaces et prendre les principales mesures de sécurité, car on peut agir rapidement par démultiplication.

2.7.3.3 Niveau opérationnel

Les indicateurs appartenant à ce type de TB sont de deux natures : *indicateurs d'efficacité* et *indicateurs de satisfaction*. Le niveau des indicateurs décrit le niveau auquel appartient le TBS. Un indicateur de pilotage ne peut servir que pour un TBS de pilotage et non opérationnel. L'architecture des indicateurs est faite en sorte

que les indicateurs d'un niveau inférieur peuvent alimenter les indicateurs d'un niveau supérieur, le niveau stratégique étant le plus élevé. Plusieurs indicateurs stratégiques peuvent alimenter un indicateur stratégique. Un indicateur stratégique peut être indépendant. Plusieurs indicateurs fonctionnels peuvent alimenter un indicateur fonctionnel ou stratégique. Un indicateur fonctionnel peut être indépendant. Plusieurs indicateurs opérationnels peuvent alimenter un indicateur opérationnel ou fonctionnel. Un indicateur opérationnel peut être indépendant. La figure 2.9 donne une vue des trois niveaux. On retrouve ici une forme pas très éloignée du modèle causes- effets développé par Kaplan et Northon. Une succession d'actions intermédiaires conduit à atteindre les objectifs. Ces actions intermédiaires sont évaluées grâce aux indicateurs intermédiaires qui sont les indicateurs fonctionnels ou opérationnels. Mais dans le cadre des TBS, les objectifs mesurés ne se situent pas seulement comme le but ultime à atteindre. C'est l'atteinte des objectifs intermédiaires qui permet d'atteindre les objectifs finaux. Ces objectifs étant stratégiques pour l'entreprise et la mesure de l'atteinte de ces objectifs se fait par des indicateurs stratégiques.

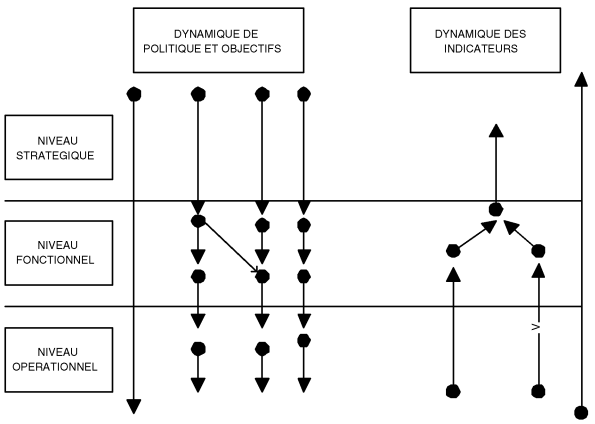

FIG. 2.9 – Dynamique indicateurs sources : CLUSIF 1997

2.7.4 Méthode par domaines

La méthode par domaines repose sur les évaluations de l'efficacité de la politique de sécurité et des moyens mis en œuvre par domaines de sécurité :

- domaine de prévention : la politique mise en œuvre vise à dissuader les agressions, à diminuer la probabilité d'apparition d'un incident en minimisant les vulnérabilités tant techniques qu'organisationnelles et à limiter l'ampleur des dommages si une attaque a réussi ;
- domaine de détection : la politique de mise en œuvre vise à détecter un incident le plus tôt possible lorsqu'il se produit ;
- domaine de la réaction : c'est l'ensemble des mesures palliatives réalisées lorsqu'un incident est survenu afin de minimiser l'impact de cet incident, faire cesser la malveillance et réunir les preuves pour lancer éventuellement des poursuites judiciaires ;

- domaine de la reprise après incident : c'est l'ensemble des procédures mises en œuvre afin de remettre le SI dans la configuration qu'était la sienne avant l'incident et dans sa capacité de fonctionnement nominale.

Dans cette démarche, pour connaître le niveau de sécurité d'un SI, il faut vérifier si la prévention, la détection, la réaction et la capacité de reprise sont suffisantes au vu des objectifs de sécurité qu'on s'est fixés. Cette segmentation en quatre domaines permet de déterminer les actions à réaliser en fonction des risques qu'on souhaite couvrir. La synthèse de ces réponses permet de connaître les points faibles nécessitant un complément d'attention. Dans cette approche les indicateurs sont élaborés domaine par domaine, parallèlement à la politique de sécurité. Ces indicateurs peuvent avoir une ou plusieurs composantes quantitatives (qui complètent la partie du TBS opérationnel) ou qualitatives (qui complète la partie du TBS fonctionnel). Contrairement à l'approche précédente, un indicateur peut être commun aux trois niveaux : stratégique, fonctionnel et opérationnel.

2.7.4.1 Méthode reposant sur la politique de sécurité

Cette méthode repose sur la politique de sécurité de l'entreprise. Elle est basée sur les objectifs stratégiques et les évolutions du contexte (du SI, des risques, des destinataires...). Elle se décompose en cinq étapes. Lors de la première itération, les étapes sont généralement réalisées successivement. Par la suite, les étapes d'exploitation et d'évolution des TBS peuvent donner lieu à des nouvelles itérations.

- **Etape 1 : Pré requis**. Cette étape consiste à rassembler des éléments préalables à l'élaboration de TBS : on peut citer : l'identification des destinataires des TB, la formalisation des utilisations prévues ou souhaitées, l'expression des objectifs de sécurité issus d'une analyse de risques SSI etc. Lors de cette première étape on retrouve la méthode de l'approche par politique de sécurité ou indirectement analyse de risques.

- **Etape 2 : Mise en place du projet**. La mise en place consiste à identifier et mobiliser les acteurs pour constituer les groupes de travail. Un groupe *utilisation* définit le besoin en TBS en partant de besoins fonctionnels identifiés. Un groupe *technique* valide la faisabilité des TBS ainsi que de leur pertinence par rapport aux réalités techniques du SI. un groupe *technique* valide la faisabilité des TBS ainsi que de leur pertinence par rapport aux réalités techniques du SI. Un groupe *pilotage* maîtrise les coûts et charges récurrents aux TB en phase de production etc.

- **Etape 3 : Elaboration des TBS**. Cette étape permet de construire les TBS en se basant sur les différents objectifs identifiés : la formalisation des objectifs mesurables, l'élaboration des indicateurs correspondants, l'élaboration des procédures d'alimentation des TBS etc.

- **Etape 4 : Exploitation du TBS**. La quatrième étape consiste à éditer et exploiter les TBS selon les périodicités prévues, il s'agira d'utiliser les TB dans le processus de décision.

- **Etape 5 : Evolution du TBS**. Le suivi du TB permet de vérifier s'il nécessite une évolution, du fait d'une observation parmi les suivantes : un défaut de qualité des indicateurs (cohérence, pertinence), une évolution du contexte, une évolution des objectifs de sécurité, une inadéquation des indicateurs par rapport aux objectifs de sécurité, un changement de destinataires etc.

2.7.4.2 Analyse des méthodes de conception des tableaux de bord de la sécurité

Les trois méthodes étudiées plus haut proposent pratiquement une démarche semblable. Cette démarche passe par une définition des objectifs de sécurité, la mise en place des mesures de sécurité et le calcul des indicateurs de sécurité. Elles s'appuient sur une politique de sécurité, sans prévoir le cas ou cette politique pourrait ne pas exister. La méthode par niveaux classifie les TBS en trois catégories ces mêmes catégories peuvent se retrouver lorsqu'on applique la méthode par domaine, tout dépend de l'indicateur choisit et la manière dont il se calcule. Dans la méthode par niveaux, on retrouve une organisation hiérarchique des indicateurs et le lien entre les différents niveaux, mais rien n'est dit sur l'organisation de ces indicateurs. On n'a l'impression que c'est selon le bon entendement de celui qui conçoit le TBS. Ces méthodes ne proposent pas une démarche formelle d'évolution du TBS. On ne sait pas la limite de validité d'un indicateur. Quand est ce que celui ci n'est plus significatif ? il n'existe pas un lien explicite entre objectifs fixés et les actions menées pour les atteindre. Cette limite cause un obstacle majeur au pilotage de la sécurité. Le TBS est vu dans ce cas pas comme un instrument de pilotage mais comme un instrument de mesure du niveau de sécurité. Il ne peut proposer aucun choix à prendre dans la stratégie compte tenu de l'évolution de l'environnement.

2.8 Analyse des offres des éditeurs en matière de tableaux de bord

Les TB sont très variables entre les différents établissements indépendamment du fait qu'ils soient utilisés pour la sécurité ou pas. Cette section a pour but de faire une analyse de quelques TB existants sur le marché. L'analyse est menée sur les outils les plus utilisés. Le marché des TB a été segmenté en deux grandes catégories. D'une part les TB basés sur des solutions décisionnelles dites "blanches" qui s'adressent à n'importe quel domaine d'activité pour lequel une modélisation spécifique des données de la compagnie est nécessaire. D'autre part, les TB basés sur des solutions décisionnelles dites "pré-packagées" pour un domaine précis permettant aux compagnies de ce domaine d'avoir un certain nombre de rapports prédéfinis. Il s'agit des solutions "clé en mains" proposées par des éditeurs dédiés à un domaine précis. Ces solutions comprennent un TB, un ensemble d'indicateurs "pré formatés", et des fonctionnalités diverses. Ces solutions sont déjà modélisées selon une logique choisie par l'éditeur, il ne reste plus qu'à les paramétrer et à les brancher sur le SI de l'entreprise.

2.8.1 Principaux composants et fonctionnalités

Ce paragraphe présente rapidement les fonctionnalités recensées dans la fiche de l'éditeur, seules les fonctionnalités déjà disponibles sont présentées. Pour mieux comprendre l'outil, on ne décrit pas seulement le TB, mais tout le processus depuis la récolte de données, en passant par le chargement et enfin d'aboutir à l'analyse.

2.8.1.1 L' alimentation

Le chargement des données permet de récupérer les données en provenance de sources diverses : SGBD, ERP, fichiers plats. Il peut s'agir d'un ETL. Pour des solutions ne comprenant pas d'ETL, le chargement est parfois possible mais nécessite des développements. Les solutions prévoient l'utilisation d'un outil ETL pour alimenter le *datawarehouse* et ou les *datamarts*. Le chargement de données externes par fichiers plats : permet de récupérer les objectifs fixés via les fichiers de type CVS.

2.8.1.2 Le Stockage

Le modèle de stockage de données est très souvent de type relationnel, mais cela n'exclut pas forcément les fonctionnalités de navigation multidimensionnelle mais celles-ci seront moins performantes que celles basées sur un cube.

Cube *On-line Analytical Processing* (OLAP) : le modèle de données permet nativement d'effectuer des analyses multidimensionnelles. Les deux solutions peuvent cohabiter, i.e. avoir une base relationnelle et les cubes selon les analyses à mener. On distingue plusieurs variantes.

- ROLAP (Relationnel OLAP) : la modélisation permettant des analyses multidimensionnelles est de type relationnel.
- MOLAP (Multidimensional OLAP) : la modélisation permettant des analyses multidimensionnelles est de type multidimensionnel.
- HOLAP (Hybrid OLAP) : la modélisation permettant des analyses multidimensionnelles combine multidimensionnel et relationnel.
- DOLAP (Desktop OLAP) : le cube est crée sur le poste de l'utilisateur.

Datamarts : il peut exister deux cas de figures, il existe un entrepôt de données pour certaines analyses (de niveau stratégique en particulier) et plusieurs *datamarts* crées à partir du *datawarehouse*. Le deuxième cas de figure se présente lorsqu'il n'existe pas de datawarehouse, mais il existe un ou plusieurs *datamarts*.

Sécurité et reprise après incident : l'accès aux données se fait via des comptes utilisateurs individuels. L'utilisateur ne voit que les données le concernant. En ce qui concerne la reprise après incident, dans le cadre de l'alimentation du SI, l'outil permet une reprise automatique des données lorsqu'un problème apparaît durant le chargement.

Après avoir décrit les principaux composants et les fonctionnalités, il est important de préciser que les TB peuvent être produits sous trois formes. Les TB standards, i.e. directement utilisables. Les TB personnalisables, sont des nouveaux TB produits ou les TB adaptés à partir de ceux fournis en standard. Dans la plus part de

cas, cette fonctionnalité permet de faire appel à l'éditeur de la solution. Enfin les TB interactifs, ils ne sont pas figés et permettent de naviguer dans les données.

2.8.2 Cognos 8 BI

L'entreprise Cognos[6] propose des outils de la suite Cognos 8 BI qui sont de type solution "blanche". L'alimentation se fait par chargement de toutes sources de données, il existe un outil d'extraction (type ETL) appelé Data Manager, il existe également un module d'audit des erreurs et des rejets. Quant au stockage il existe quatre possibilités : base relationnelle, Cube(OLAP), entrepôts de données et *datamarts*. On trouve des TB interactifs (fonctionnalités multidimensionnelles), et une interface graphique pour la construction de TB personnalisés. On distingue en plus des fonctionnalités suivantes :

- tableaux et graphiques de tout type (possibilité de disposer des graphiques à échelles différents pour afficher plusieurs indicateurs en même temps),
- gestion avancée des alertes par envoi de "sms" ou de mail avec un commentaire et un rapport associé à chacune d'entre elle,

Toute compagnie peut personnaliser son portail Cognos en utilisant l'outil report studio. De plus Cognos BI 8 est une solution WEB totalement intégrée, basée sur une architecture orientée service permettant aux restitutions cognos d'être intégrées au sein de n'importe quel portail d'entreprise. Les TB peuvent également être disponibles sur mobile grâce à la solution Cognos 8 Go mobile.

Analyse : les outils d'analysis *Studio* et *Query Studio* permettent d'effectuer toute sorte de requêtes ad hoc sur les données : *analyse studio* est basée sur les analyses multidimensionnelles et *Query studio* permet de faire des requêtes simples (pour intégrer le résultat d'une requête dans le portail, il faut utiliser report studio). L'outil Office Connexion permet une intégration totale aux produits de la suite Microsoft Office - WORD, EXCEL, POWERPOINT, dans un environnement multi requêtes et multi sources.

Pilotage des performances : Cognos a une approche BSC complète permettant de dresser la carte stratégique de l'entreprise et de suivre ensuite les objectifs opérationnels au niveau de chaque pôle. Il est possible de définir des plans d'actions : tâche définie dans le temps à laquelle un responsable est associé.
Cognos fournit une offre qui semble intégrée, complète et qui devrait aider à répondre à beaucoup de besoin des entreprises à la fois en termes de *reporting* et de TB, mais également en termes d'analyse avancée de pilotage budgétaire et de gestion des performances (BSC).

2.8.3 Business Scorecard Manager

BSC Manager est un produit de Microsoft de type solution "blanche", qui offre toutes les fonctionnalités de *reporting* avec la possibilité pour les utilisateurs avancés de créer leurs propres rapports via le Report Builder.

[6] http ://www.cognos.com/fr/

Cet environnement de gestion de rapports met à la disposition des utilisateurs un large choix de sources de données, de formats de sortie (HTML, PDF, EXCEL, etc.). L'outil est capable d'attaquer des sources SQL server et non SQL server (base de données oracle etc.) Nous décrivons ci-dessous les principales fonctionnalités.

Alimentation et stockage : L'ETL de Microsoft SQL Server Integration Services(SSIS) permet d'alimenter le SI à partir de sources de données hétérogènes : bases de données (Oracle, DB2, Teradata), OLEDB ou ADOMD.NET, fichiers (plats, XML, Excel), SAP. L'entrepôt de données constitué doit être une base de données SQLServer. SSIS permet également d'alimenter des cubes et peut s'interfacer avec *reporting* services.

Analyse et pilotage de performance : le moteur Analysis services permet de gérer des cubes afin d'effectuer des analyses multidimensionnelles. L'outil Business Scorecard Manager est basé sur la méthode BSC et permet de disposer d'indicateurs clés en temps réel sous forme visuelle permettant d'identifier immédiatement les objectifs atteints ou les seuils critiques (feu tricolore, flèche etc.). Cet outil permet aux différentes équipes de partager des objectifs et de collaborer. L'intégration de documents non structurés favorise la communication entre les différents acteurs.

2.8.3.1 Dashboard Manager

Dashboard Manager est un outil conçu par Business Objects(BO) qui propose des outils de *reporting* en fonction des besoins et des budgets des entreprises. Elle est de type solution "blanche".

- Crystal report : cette solution permet de créer, gérer et distribuer des rapports sur le web. Plusieurs formules sont proposées selon les besoins des entreprises, un package particulier est disponible pour les PME/PMI.
- Crystal Vision : version améliorée de Cristal Report permettant en outre une interaction avec les outils Microsoft Office.
- Business Objects Entreprise : plateforme BI composée de plusieurs outils permettant d'effectuer du *reporting*, de l'interrogation, de l'analyse, etc.

Analyse et mesure de performance : il existe plusieurs outils dédiés à l'analyse :

- BO Web Intelligence : interface web de consultation de rapport : il permet également aux utilisateurs avancés de créer leurs propres requêtes ; certaines interrogations complexes nécessitant l'utilisation de Desktop Intelligence.
- BO intelligent : interface très conviviale pour le requêtage ad hoc.
- BO Desktop Intelligence : interface de type client lourd permettant d'élaborer des requêtes complexes qui peuvent ensuite être converties au format WEB pour une intégration au sein de WEB Intelligence
- BO OLAP Intelligence : outil d'analyse multidimensionnelle

Quant à la mesure de la performance, le portail de BO permet une approche BSC avec gestion d'une carte de pilotage stratégique. Nous venons de faire l'analyse de trois solutions de type boite "blanche" ; dans les développements qui suivent, nous allons décrire trois autres solutions de type "pré-packagée".

2.8.3.2 Cerner

Cerner[7] est une société qui propose plusieurs tableaux de bord de type "pré-packagée", on peut citer :

Discern Explorer : ce produit permet de lancer des requêtes automatiquement sur des données de production. Les utilisateurs peuvent disposer d'un état des lieux en temps réel. Les différents modules fonctionnels de Cerner fournissent aux utilisateurs des indicateurs opérationnels au travers de rapports réalisés avec le module Discern Explorer.

Power Vision : l'outil permet à des utilisateurs avancés de produire de nouveaux rapports ou des TB à partir d'une interface graphique.

Power Insight : la solution, basée sur la technologie BO, permet de faire des analyses avancées sur un entrepôt de données. Il permet un pilotage stratégique au niveau de l'établissement à partir de données centralisées. Les fonctionnalités ETL de l'outil (produit d'Informatica) permettent de constituer un *datawarehouse* à partir des données présentes dans les bases Cerner complétées éventuellement d'autres sources de données. C'est l'outil BO qui permet ensuite de produire des TB.

2.8.4 KEYRUS

KEYRUS[8] offre un outil de type "pré-packagée". Les utilisateurs accèdent aux indicateurs métiers et à une bibliothèque de rapports répondant aux interrogations avec plusieurs solutions techniques (Business Objects : environ 90 rapports disponibles, Oracle, et Microsoft : une dizaine de rapports). L'outil reste ouvert et permet de créer des rapports complémentaires. Il est même possible d'ajouter de nouveaux indicateurs au modèle de données. L'outil offre des restitutions variées issues des solutions standards du décisionnel : tableaux et graphiques de tous types, jauges, alertes, etc. Il est composé de *datamarts* logiques et/ou de cubes multidimensionnels dédiés aux composants fonctionnels pré-packagés. L'ensemble de ces composants est intégré dans un entrepôt de données centralisé (datawarehouse).

2.9 Les ontologies

La notion d'ontologie trouve son origine dans une branche de la philosophie traitant de la science de l'être. Cette discipline philosophique qui a été initiée par Aristote, essaie de définir l'être. Le terme lui même apparaît tardivement en 1962, emprunté au latin scientifique "ontologia".

En informatique, cette notion est apparue dans les années 90, depuis plusieurs définitions ont été proposées. La plus couramment utilisée est celle de Gruber [Gruber93], *an explicit specification of a conceptualization*.

[7] http ://www.cerner.fr
[8] www.keyrus.fr

Nous interprétons cette définition comme "une spécification formelle explicite de termes d'un domaine et de relations entre elles". Les ontologies sont devenues très courantes dans plusieurs domaines et particulièrement dans le World-Wide Web. Elles représentent un ensemble de concepts. Ces concepts peuvent être traités informatiquement et servir de base commune à un ensemble de personnes d'une communauté. Elles doivent être explicites, i.e. toute la connaissance nécessaire à leur compréhension doit être spécifiée. Les concepts définis dans une ontologie peuvent être classés en deux catégories [Gruber1995] :

- les concepts primitifs, dont une ontologie ne fournit pas les définitions complètes et s'appuient sur une documentation textuelle et un savoir préexistant partagé par le lecteur ;
- les concepts définis ; dont les conditions nécessaires et suffisantes de reconnaissance en termes de concepts primitifs sont fournis par une ontologie.

2.9.1 Représentation d'une ontologie

La conception d'une ontologie peut se faire en instanciant un modèle d'ontologies existantes.

- la connaissance structurelle : les objets du domaine d'étude sont regroupés en classes organisées par des relations ; la plus couramment utilisée est la relation de subsomption ;
- la connaissance descriptive : les objets des différentes classes sont regroupés parce qu'ils présentent des caractéristiques communes ; la définition de ces caractéristiques est faite en utilisant des propriétés ;
- la connaissance procédurale : les caractéristiques d'une classe peuvent être déduites à partir d'autres informations ; elles peuvent également être soumises à des contraintes.

2.9.2 Les composantes d'une ontologie

Une ontologie peut être vue comme un ensemble de concepts et de relations entre eux destinés à représenter les objets du monde sous une forme compréhensible, aussi bien par les hommes que par les machines. Si certaines divergences relative à la structure de l'ontologie ont été constatées, les composantes d'une ontologie sont les mêmes. Une ontologie est constituée des concepts et des relations ainsi que des propriétés et des axiomes [Djida2006] :

- les concepts sont des notions permettant la description d'une tâche, d'une fonction, d'une action, d'une stratégie ou d'un processus de raisonnement, etc. Ils peuvent être abstraits ou concrets, élémentaires ou composés, réels ou fictifs. Habituellement les concepts sont organisés en taxonomie. Une taxonomie est une hiérarchie de concepts reliés entre eux en fonction de critères sémantiques particuliers ;
- les relations sont des liens organisant les concepts de façon à représenter un type d'interaction entre les concepts d'un domaine. Elles sont définies comme tout sous ensemble d'un produit de n ensembles, c'est à dire R : $C1$ x $C2$ x.....x Cn. Des exemples de relations binaires sont : sous concepts-de, connecté-à, sorte-de, etc. ; .
- les propriétés(ou attributs) sont des restrictions des concepts ou des relations ;
- les fonctions sont des cas particuliers des relations dans lesquelles le nième élément de la relation est

unique pour les n-1 précédents. Formellement les fonctions sont définies ainsi : F : $C1$ x $C2$ x.....x $Cn-1, Cn$;

- les axiomes de l'ontologie permettent de définir la sémantique des termes (classes, relations), leurs propriétés et toutes contraintes quant à leur interprétation. Ils sont définis à l'aide de formules bien formées de la logique du premier ordre en utilisant les prédicats de l'ontologie ;
- les instances sont utilisées pour représenter les éléments.

2.9.3 Typologie des ontologies

Deux grandes classes d'ontologies sont à distinguer. La première est liée au type de la structure de la conceptualisation ; la deuxième au domaine à conceptualiser. Dans la première classe, l'ontologie se présente de façon différente selon le degré de formalisation, du langage utilisé pour définir la spécification des termes [Uschold1997]. Une ontologie est dite hautement informelle dans le cas d'utilisation du langage naturel sans aucune restriction, semi-formelle lorsque le langage est de type langage naturel, mais structuré avec un vocabulaire limité afin de restreindre les ambiguïtés. Si l'ontologie est représentée à l'aide d'un langage formel tel que "Ontolingua", l'ontologie est alors semi-formelle. Enfin lorsque les termes possèdent une sémantique formelle dans un système tel que le calcul des prédicats du premier ordre, l'ontologie est dite rigoureusement formelle.

Dans la deuxième classe, l'ontologie se définie selon le domaine étudié et le degré de généralité ou de précision des connaissances représentées. Les types d'ontologies les plus étudiées sont :

- les ontologies générales portent sur des concepts généraux qui se veulent indépendants d'un domaine ou d'un problème particulier ; tels que les concepts de temps, d'espace de notion mathématique. Parmi les ontologies générales il y'a (1) Cyc développée avec le modèle logique, en utilisant le langage CycL. (2) KR Ontology qui utilise le modèle de treillis et le FCA (Formal Concept Analysis) pour représenter l'ontologie.
- les ontologies du domaine expriment des conceptualisations spécifiques à des ontologies de domaines particuliers tout en étant générique pour ce domaine. Ces conceptualisations mettent des contraintes sur la structure et les contenus des connaissances de domaine. Il existe plusieurs ontologies de domaines qui ont été développées. *Enterprise ontology* et Tove dans le domaine medical.
- les ontologies d'application sont les plus spécifiques. Les concepts correspondent souvent aux rôles joués par les entités du domaine tout en exécutant une certaine activité [Maedche2002]. Elles contiennent toutes les définitions nécessaires pour décrire la connaissance requise pour une application particulière.

2.9.4 Construction d'ontologies

Il existe trois méthodes possibles de construction d'ontologies. Une ontologie peut être construite de manière manuelle, automatique ou mixte. Dans le mode manuel, les experts construisent l'ontologie en s'appuyant sur des techniques classiques de collecte et d'analyse de connaissances. La création d'une ontologie de manière

automatique se base sur des méthodes formelles et des techniques d'extraction des connaissances en s'appuyant sur des outils linguistiques et statistiques. Dans le mode mixte, les ontologies sont construites par les techniques automatiques tout en intégrant des méthodes permettant d'étendre l'ontologie, ayant été construite manuellement. Quelle que soit le mode choisi, l'élaboration d'une ontologie doit s'appuyer sur un certain nombre de règles qu'il est nécessaire de respecter et une méthodologie de construction d'ontologies.

2.9.4.1 Principes de construction d'ontologies

Le processus de construction d'ontologies doit respecter un certain nombre de principes de bases qui permetent d'obtenir un certain nombre d'ontologies répondant aux objectifs fixés. Th R Gruber[Gruber1993] propose ainsi un nombre de principes à respecter pour construire une ontologie :

- la clarté (les ambigüités doivent être réduites) : l'ontologie doit fournir le sens des termes définis en offrant des définitions objectives ainsi que de la documentation associée en langage naturel ;
- l'exhaustivité : une définition exprimée par une condition nécessaire et suffisante est préférable à une définition exprimée seulement par une condition nécessaire ou par une condition suffisante ;
- la cohérence, l'extensibilité (l'ontologie doit être construire de telle manière qu'on puisse l'étendre facilement), afin de pouvoir formuler des inférences cohérentes avec les définitions ;
- le biais d'encodage minimal : l'ontologie doit être conceptualisée indépendamment de tout langage d'implantation ;
- l'engagement ontologique minimal : il doit contenir un vocabulaire partagé mais ne doit pas être une base de connaissances comportant des connaissances supplémentaires à modéliser.

2.9.4.2 Méthodologies de construction d'ontologies

Plusieurs méthodologies ont été définies dans la littérature depuis quelques années. Elles peuvent être classifiées en fonction de l'utilisation ou non des connaissances ainsi que des techniques d'apprentissage. Les toutes premières qui servaient à construire des ontologies d'entreprises, le faisaient sans connaissance à priori, elles étaient manuelles. La retro conception des ontologies [Gomez1999] est basée sur le *mapping* d'un modèle conceptuel d'une ontologie implémentée avec un autre modèle plus valide pour le ré-implanter. Les méthodologies se distinguent selon les données en entrée : textes, dictionnaires, bases de connaissances, schémas relationnels, et semi-structurés, sources de données hétérogènes. Nous insisterons sur la construction à base des bases de connaissances, et sur l'évolution des ontologies. Ben Mustapha et autres [BenMustapha] ont travaillé sur cette classification et en ont fait une synthèse.

Les méthodologies de construction d'ontologies «from scratch » : Les méthodologies de construction des ontologies «from scratch » furent parmi les premières dans le domaine de l'ingénierie d'ontologie et visent à construire l'ontologie en l'absence de connaissances.
La méthodologie de Gruninger et Fox [Gruninger1995] consiste à construire un modèle logique des connais-

sances communes d'entreprise spécifié via l'ontologie en se basant sur les étapes suivantes :

1. la capture des «scénarios motivants» ;

2. la détermination des exigences de l'ontologie à construire sous la forme des questions informelles de compétences ;

3. la formalisation de la terminologie extraite antérieurement à l'aide d'un formalisme bien déterminé comme Knowledge Interchange Format (KIF) ou la logique du premier ordre ;

4. la spécification formelle des questions de compétence en utilisant la terminologie de l'ontologie et la spécification des axiomes et des définitions relatives aux termes de l'ontologie dans un langage formel comme la logique du premier ordre.

5. la spécification des théorèmes de complétude de l'ontologie qui vont représenter les conditions sous lesquelles les solutions des questions données seront complètes.

Fernandez [Fernandez1999] propose, dans la méthodologie METHONTOLOGY, de construire une ontologie en respectant des activités de gestion de projet (planification, assurance qualité), de développement (spécification, conceptualisation, formalisation, implantation, maintenance) et des activités de support (intégration, évaluation, documentation). On retrouve des problématiques de génie logiciel et de gestion de projet informatique qu'on a tout intérêt évidemment à voir s'appliquer à la construction de grandes ontologies, si on a une méthodologie réelle de construction. Natalya et Deborat dans [Natalya101] proposent une méthode simple pour la création d'une première ontologie. Ils abordent les points généraux qui doivent être pris en considération et offrent des procédures possibles pour développer une ontologie. Ils décrivent une approche itérative en commençant par aborder l'ontologie de façon frontale. Ensuite, ils reviennent sur l'ontologie, qu'ils considèrent comme processus d'évolution, en l'affinant et en la complétant par des détails. Tout au long de ce processus, ils discutent les décisions de modélisation à prendre par le concepteur, ainsi que les pour, les contres, et les implications des différentes solutions.

Les méthodologies d'apprentissage d'ontologies à partir de textes : Il s'agit ici de construire une ontologie sur la base de connaissances à priori. Celle-ci permet d'automatiser l'enrichissement de l'ontologie par des méthodes d'apprentissage. Selon Maedche et Sttab [Maedche2001], il existe autant d'approches d'apprentissage d'ontologie que d'entrées. Les approches à base de textes, de dictionnaires ([Hearst1992], [Jannink1999]), de bases de connaissances [Suyanto2001], de schémas semi structuré [Deitel2001], et de schéma relationnel ([Johannesson1994], [Kashyap1999] [Runin2002]). Parmi les méthodes d'apprentissage à partir de textes, on peut citer la méthode sur des techniques de traitement automatique du langage naturel. Hearst [Hearst1998]

a proposé une approche qui permet l'apprentissage automatique des relations d'hyponymie en extrayant l'ensemble des paires de concepts liés par une relation dans une ontologie existante pour construire des patrons lexico-syntaxiques. On parle aussi de l'apprentissage fondé sur les techniques de clustering. La méthodologie proposée par Khan et Luo [Khan2002] construit une ontologie du domaine à partir des documents textes en utilisant des techniques de clustering et WordNet. Enfin on peut citer l'apprentissage multi stratégies à partir de sources de données hétérogènes proposée par Mae dche et Staab[Maedche2001] ou l'apprentissage basé sur le calcul de fréquences proposé par Kietz [Kietz2000].

2.9.4.3 Les outils de construction d'ontologies

De nombreux outils permettent aujourd'hui d'éditer des ontologies. Parmi ceux-ci, quelques uns essaient de guider leur utilisateur dans l'élaboration de l'ontologie en suivant une méthodologie de conception plus ou moins complète, que ce soit en respectant les principes de cycle de vie et validation de logiciels d'un côté ou, de l'autre côté en outillant une réflexion épistémologique. Dans tous les cas, force est de constater qu'aucun de ces outils n'ont réussi à s'imposer et la réflexion sur l'outillage de la construction des ontologies reste ouverte.

Knowledge interchange Format(KIF) : KIF [NCITS1998] est un langage basé sur les prédicats de premier ordre avec des extensions pour représenter des définitions et des métas connaissances. Tant que la logique du premier ordre est un langage de bas niveau pour l'expression d'ontologies, l'outil Ontolingua [Farquhar1996] permet aux utilisateurs de construire des ontologies KIF à un niveau plus élevé de la description par l'importation des définitions des ontologies prédéfinies.

PROTEGE 2000 : est un environnement graphique de développement d'ontologies développé par le *Stanford Médical Informatics*. Dans le modèle des connaissances PROTEGE, les ontologies consistent en une hiérarchie de classes ayant des attributs (slots), qui peuvent eux-mêmes avoir certains attributs (facets). L'édition des listes de ces trois types d'objets se fait par l'intermédiaire de l'interface graphique, sans avoir besoin d'exprimer ce que l'on a à spécifier dans un langage formel : il suffit de remplir les différents formulaires correspondant à ce que l'on veut spécifier. Ce modèle autorise d'ailleurs la liberté de conception assez importante puisque le contenu des formulaires à remplir peut être modifié suivants les besoins via un système de méta classes, qui constituent des sortes de patrons de connaissances. L'interface très bien conçue et l'architecture logicielle permettant l'insertion de plugins pouvant apporter de nouvelles fonctionnalités (par exemple la possibilité d'importer et d'exporter les ontologies construites dans divers langages opérationnels de représentation ou encore la spécification d'axiomes) ont participé au succès de PROTEGE 2000 qui regroupe une communauté d'utilisateurs assez importante et constitue une référence pour beaucoup d'autres outils.

KL-ONE : est un langage basé sur la logique de description [Baget2003]. Il permet de représenter la connaissance à base de cadres. Ce système maintient la définition des concepts par un simple nommage, et l'indication de la correspondance des concepts dans une hiérarchie de généralisation/spécialisation. De nouveaux termes peuvent être définis par des opérations de conjonction des concepts. Par exemple l'opérateur

«and» peut être utilisé pour préciser qu'un nouveau concept est une spécialisation commune de plusieurs autres concepts. De nouveaux rôles peuvent être introduits pour représenter les relations qui peuvent exister entre des individus dans le domaine modélisé. Les définitions des concepts peuvent inclure des restrictions sur les valeurs possibles, sur les nombres de valeurs, ou sur le type de valeurs qu'un rôle peut avoir pour un concept.

RDF et RDF Schéma : c'est un formalisme graphique pour représenter des métas donnés. Il est basé sur la notion de triplet (sujet, prédicat, objet). Le sujet et l'objet sont des ressources liées par le prédicat. Le " RDF Schema " est alors un standard regroupant un ensemble d'informations indiquant les propriétés et les relations de classes régissant le système RDF. Les schémas RDF sont utilisés pour déterminer les vocabulaires qui représentent un ensemble de propriétés sémantiques propres à une communauté particulière, le terme communauté étant pris dans son sens large. Comprendre un schéma RDF particulier signifie comprendre la sémantique de chacune des propriétés présentées dans la description de la ressource.

DAML + OIL : est un langage construit sur des normes précédentes du W3C telles que RDF et RDF Schéma, et qui étend ces langages avec des primitives de modélisation plus riches. Contrairement aux outils précédents, Ontolingua [Ontolingua2002] est un serveur d'édition d'ontologie au niveau symbolique. Une ontologie est directement exprimée dans un formalisme également nommé Ontolingua, qui constitue en fait une extension du langage KIF. Ontolingua utilise des classes, des relations, des fonctions, des objets (instances) et des axiomes pour décrire une ontologie. Il propose un outil permettant d'inclure une ontologie dans celle en cours de construction. L'inclusion consiste à ajouter à l'ontologie courante les axiomes de l'ontologie à inclure, après traduction des axiomes [Farquhar1995]. La traduction consiste à établir une relation d'identité entre les termes des deux ontologies qui désignent les mêmes classes ou relations.

2.9.5 Opération de modification des ontologies

La réalisation d'une ontologie est une lourde tâche [Hoffman2006], et l'on cherchera donc souvent à réutiliser une ontologie existante, plutôt que de repartir de zéro ; il y'aura alors un travail d'adaptation à faire :

- Transformation : modification de l'ontologie afin de l'utiliser dans d'autres buts que l'original, pouvant porter sur la structuration de l'information, sur le formalisme de représentation choisi mais aussi (de façon moindre : « small, yet pervasive » [Fikes2000] McGuiness et al. 2000 sur la sémantique.

- Traduction : changement de formalisme de représentation (langage d'ontologie utilisé) qui cherche à préserver la sémantique de l'ontologie. [Chalupky2000] de Chalupsky utilise ce terme dans un autre sens, celui d'une « transformation de la connaissance », pour signifier une « réécriture syntaxique » puis « sémantique » (au niveau du langage de l'ontologie puis du contenu).

- Correspondances : relation entre les éléments de deux représentations (ontologies, schémas de bases de données, etc.), indiquant une similarité relative selon une mesure donnée [Klein2001] de Klein.

- Appariement : processus de définition d'un ensemble de fonctions permettant de spécifier des correspondances (qui peuvent être n-aires, voir p. ex. ([Embley2003], [Chang2003]) entre termes.

- Morphisme : établissement de correspondances entre ontologies sans toucher à leur structure. On trouvera plus de précisions sur le morphisme d'ontologie et de signature d'ontologie dans [Kalfoglou2003] de Kalfoglou et Schorlemmer.

- Alignement : établissement de correspondances binaires selon Kalfoglou et Schorlemmer dans [Kalfoglou2003] entre les concepts des deux ontologies afin de parvenir à un agrément. Il semble que [Klein2001] et [Noy2001] de Noy et Musen acceptent que les ontologies soient légèrement modifiées, en ce qu'ils demandent que l'alignement aboutisse à un ensemble « pertinent et cohérent» (ce qui est rarement possible sans modification, pour deux ontologies développées indépendamment).

- Fusion d'ontologies : création d'une nouvelle ontologie rassemblant la connaissance d'ontologies existantes.

- Articulation : ensemble des points d'ancrage des relations lors d'une mise en correspondance entre des ontologies [Klein2001]. Dans le cas où les ontologies sources ne doivent pas être modifiées, il s'agit d'une ontologie (« articulation ontology ») rassemblant l'ensemble des correspondances (cf. [Kalfoglou2003]). L'articulation fournit une mesure de la validité de l'opération effectuée. A ces opérations de modification, on peut ajouter des opérations plus formelles, telles que les ajouts ou les suppressions de concepts dans la hiérarchie des classes.

2.9.5.1 Ajout d'un nouveau concept

A titre d'exemple, considérons l'ontologie de représentation d'une certaine race ou tribu humaine. Pour représenter les parents d'une personne, faut-il créer une classe particulière pour chacune des pères, mères, etc. ? ou vaut-il mieux avoir une classe "Parents" avec des attributs pour le sexe. Si l'information sur le sexe que nous représentons dans l'ontologie diffère de manière significative, alors nous devons alors créer une classe pour chacun des parents. C'est-à-dire si nous voulons représenter la contiguïté des détails et l'information sur le sexe (qui est différent d'un parent à l'autre), aussi bien que des fonctions spécifiques pour chaque parent et le rôle qu'il joue pour l'enfant, nous aurons besoin de classes. Si nous voulons juste avoir l'information plate sur l'un des parents pour aider à retrouver une information plus précise, nous pourrions simplifier la hiérarchie et n'avoir que la classe **Parent** et un attribut **sexe**. Lammari [Lammari2004], a proposé un certain nombre

d'algorithmes que nous exposerons dans les sections suivantes.

Begin
Input: C l'ensemble des nouveaux concepts
H l'hiérarchie initiale
Output: H' : Hiérarchie résultant du merging de C avec H
$\Omega = \emptyset$
pour *chaque concept* Ci *de C* **faire**
  Déterminer la hiérarchie Hi associé au Concept Ci en appliquant la technique de normalisation
  $\Omega = \Omega \cup Hi$
fin
Fusion des hiérarchies contenues dans $\Omega \cup H$ en utilisant les techniques de fusion
end

Algorithm 1: Ajout d'un nouveau concept

2.9.5.2 Suppression d'un concept

Pendant la maintenance de l'ontologie, on peut décider qu'un concept ne présente plus d'importance pour l'ontologie. Nous considérons ici deux stratégies permettant de supprimer des concepts.

- Stratégie 1 : consiste à supprimer seulement le concept
- Stratégie 2 : consiste à supprimer le concept et ses descendants s'ils ne sont pas descendants d'un concept et qui ne sont pas ascendants du concept à supprimer

Plus formellement nous avons l'algorithme ci-dessous.

- C l'ensemble de concepts représentant une hiérarchie H dans l'ontologie
- $C1$ l'ensemble de concepts à supprimer de H, nous avons $C1 \subset C$
- $DR1$ l'ensemble de descendants de $C1$. $DC1 = \bigcup 1^n Dx$, $x \in 1...n$, $n = card(C1)$, Dx représente tous les descendants du concept c de
  $C1$
- $AR1$ l'ensemble des ascendants de $C1$, $AC1 = \bigcup 1^n Ax$, $x \in 1...n$, $n = card(C1)$, Ax représente tous les ascendants du concept c de $C1$
- $C2$ tous les concepts de H qui ne sont ni dans $C1$, ni $DC1$, ni dans $AC1$. $C2 = C - (C1 \cup DC1 \cup AC1)$
- $DC1$ tous les descendants de $C2$

Begin
Input: H : Hiérarchie initiale ; c : ensemble des concepts à supprimer de H
Output: H : Hiérarchie résultant
si *on choisit la stratégie 2* **alors**
  Déterminer DC_1 l'ensemble des descendants de C_1
  Déterminer C_2 l'ensemble de concepts de H qui ne sont pas dans C_1 ou dans DC_1
  Déterminer DC_2 l'ensemble de descendants of C_2
  Ajouter à C_1 l'ensemble $DC_1 - DC_2$
fin
pour *chaque concept c de C1* **faire**
  pour *chaque mot clé w de C* **faire**
    pour *chaque descendant direct d de r* **faire**
      Renommer w en w' tel que le nom de w'= nom de w ascendant de d Ajouter à d le mot clé w'
    fin
  fin
fin
pour *chaque descendant direct d de c* **faire**
  pour *chaque descendant direct a de c* **faire**
    ajoute un lien Is_a de d à a
  fin
fin
Effacer c de H
Remplacer le nom de chaque mot clé renommé par son nom initial
end

Algorithm 2: Suppression d'un concept

2.9.5.3 Suppression d'une hiérarchie de concepts

L'algorithme ci-dessous permet de supprimer des concepts de la hiérarchie. Une hiérarchie est vue comme un ensemble de concepts ; supprimer une hiérarchie peut être vu comme la suppression d'un ensemble de concepts. Si la stratégie choisie est la stratégie 1, alors rien que les concepts de la hiérarchie à supprimer seront supprimés. Quoique, le système supprimera chaque descendant de chaque concept de la hiérarchie qui n'est descendant d'aucun concept et qui n'est pas ascendant d'un concept à supprimer. Plus formellement, nous

avons l'algorithme ci dessous.

Begin
Input: H : Hiérarchie initiale ; $H1$ sous hiérarchie à supprimer de H
Output: H' : Hiérarchie résultante
Déterminer l'ensemble $C1$ de concepts de la hiérarchie $H1$
Supprimer $C1$ de H (en utilisant l'algorithme Suppression d'un concept)
end

Algorithm 3: Suppression d'une hiérarchie de concepts

2.9.6 Mise en correspondance entre ontologies

Le mapping consiste à mettre en correspondance les éléments d'un ou plusieurs ontologies entre elles. Il existe deux plus grands types de mapping. Le mapping entre les ontologies et l'information qu'elles décrivent, et le mapping entre les différentes ontologies utilisées dans un système. Dans le cadre de cette thèse, nous allons nous intéresser aux mappings entre ontologies. Le mapping inter-ontologies est bien connu dans la littérature sur les ontologies. On retrouve les approches suivantes :

- les *mappings* définis : une approche commune est de fournir la possibilité de définir les *mappings*. Cette approche est utilisée dans [Kraft1999] où les translations entre différentes ontologies sont réalisées par des agents médiateurs spéciaux qui peuvent être adaptés pour établir la traduction entre différentes ontologies et même entre différents langages. Il est important de préciser que dans cette approche, il y'a une grande liberté. L'utilisateur est libre de définir des *mappings* arbitraires, même s'ils n'ont pas de signification ou produisent des conflits ;

- Relations lexiques : elles étendent le modèle de la logique de description par des relations inter-ontologiques issues de la linguistique ; par exemple « synonyme », « disjoint », « hyponyme », et « hypernyme » qui sont utilisés dans le système [Observer1996].

- Connaissances de base haut niveau : afin d'éviter la perte de la sémantique, on doit rester dans le langage de la représentation formelle en définissant des *mappings* entre différentes ontologies. Une méthode directe pour rester dans le formalisme est de relier toutes les ontologies utilisées à une ontologie simple du haut niveau. Tant que cette approche permet d'établir des connections entre des concepts de différentes ontologies en termes des superclasses communes, elle ne permet pas la correspondance directe.

Pour surmonter l'ambiguïté causée par le *mapping* indirect (comme l'approche précédente), une solution est d'identifier des correspondances sémantiques entre les concepts des différentes ontologies. Ces approches comptent sur un vocabulaire commun pour la définition des concepts des différentes ontologies.

2.9.7 Méthodologie et méthode pour supporter l'évolution de l'ontologie

Plusieurs recherches mettent en évidence l'importance majeure de l'évolution de l'ontologie ainsi que le manque presque total des approches pour gérer cette évolution [charlet2003] ; [OntoWeb2002b] ; [WebOnt2004b].

Nous présentons deux approches qui traitent de l'évolution de l'ontologie sur le plan méthodologique : (1) l'approche développée par l'équipe de l' *Institute of Applied Informatics and Formal Description Methods* (AIFB) de l'université de Karlsruhe, et (2) l'approche développée par l'équipe du département de l' *Information Management and Software Engineering* (IMSE) de l'université d'Amsterdam.

2.9.7.1 Méthodologie de l'AIFB pour supporter l'évolution de l'ontologie

L'évolution de l'ontologie est définie par Maedche et al. [Maedche2003], Maedche, Motik, Stojanovic, Studer et Volz [Volz2003], Stojanovic et al. [Stojanovic2002], Stojanovic et Motik [Motik2002], comme étant : la modification appropriée de l'ontologie et la propagation consistante des changements dans les artefacts dépendants, c'est-à-dire dans les objets référencés, les ontologies dépendantes, et les applications logicielles utilisant l'ontologie. Pour supporter l'évolution de l'ontologie, les auteurs proposent alors une méthodologie composée de cinq étapes principales.

- Représentation des changements : cette étape vise l'édition des changements élémentaires ou complexes. Un **changement élémentaire** est un changement primitif et non décomposable. Les changements typiques étant l'ajout, l'effacement ou la modification des entités ontologiques. Un **changement complexe** est composé des plusieurs changements élémentaires qui forment ensemble une seule entité logique ; par exemple le déplacement, la fusion ou la séparation des entités ontologiques. Klein et Noy [Noy2003] mettent en évidence l'avantage d'utiliser des changements complexes : (1) ils sont plus facilement utilisables et compréhensibles car leur intention est explicite, contrairement à une suite de changements élémentaires ayant le même résultat, et (2) ils permettent l'évolution de l'ontologie avec moins de pertes des données[9].

- Sémantique des changements : l'ontologie doit évoluer d'un état consistant vers un autre état consistant, c'est-à-dire l'état où les contraintes du modèle ontologique sont respectées, afin de résoudre les inconsistances introduites par les changements. D'autres changements additionnels peuvent être nécessaires[10], la tâche de cette étape étant alors de permettre la résolution de tous les changements additionnels d'une manière systématique.

- Implantation : cette étape vise l'exécution des changements, une fois approuvés par les utilisateurs.

- Propagation des changements : le but de l'étape de la propagation des changements est de modifier automatiquement les instances et les ontologies dépendantes afin de préserver leur consistance avec l'ontologie évoluée. Pour cela, Maedche et al. [Maedche2003] proposent une approche de modification des ontologies dépendantes[11] par l'application récursive du processus d'évolution en fonction des chan-

[9] Déplacer_Concept préserve les instances, contrairement à la suite des changements Effacer et Ajouter_Concept.

[10] Sachant que chaque propriété doit avoir minimum un concept comme domaine et comme co-domaine, l'effacement d'un concept étant le seul domaine d'une propriété demande soit d'effacer la propriété elle-même, soit de définir un autre concept comme domaine de cette propriété.

[11] L'ontologie dépendante est celle qui utilise une partie de l'ontologie évolutive dans sa structure ontologique.

gements appliqués à l'ontologie évoluée.

- Validation : les utilisateurs évaluent le résultat de l'évolution et recommencent le processus, si nécessaire.

Cette méthode présente quelques limites. Premièrement, les auteurs ne proposent aucune étape d'analyse des effets des changements sur la relation de compatibilité entre l'ontologie évoluée et les artefacts dépendants. Ceci est une limite importante étant donné que l'évolution de l'ontologie peut provoquer la dégradation du référencement sémantique des objets ou la dégradation de l'interopérabilité avec d'autres ontologies ou encore celle du comportement des systèmes fondés sur l'ontologie (Heflin, Hendler, et Luke, 1999 ; Stuckenschmidt et Klein, 2003a).

2.9.7.2 Méthodologie de l'IMSE pour supporter le versionnage de l'ontologie

L'évolution de l'ontologie est définie par Klein ([Klein2002a],[Klein2002b]), Klein, Ding, Fensel et Omelayenko [Kleinn2002], Klein et Noy[Noy2003], Noy et Klein [Klein2003a], Noy et Musen [Musen2003a] comme étant : la capacité de gérer les changements de l'ontologie et leurs effets en créant et en maintenant différentes versions d'une ontologie. Cette capacité consiste à identifier et à différencier les versions, à modifier les versions, à spécifier des relations qui rendent explicites les changements effectués entre les versions et à utiliser des mécanismes d'accès pour les artefacts dépendants, c'est-à-dire les objets référencés, les ontologies et les applications dépendantes.

Contrairement à la définition faite dans la méthodologie AIFB, qui considère uniquement l'ontologie évoluée, l'accès aux artefacts s'effectuant par cette ontologie, cette définition considère l'utilisation de plusieurs versions de l'ontologie, l'accès aux artefacts s'effectuant au moyen de ces versions multiples. Les auteurs utilisent alors le terme versionnage pour décrire leur approche. Cette méthodologie présente quelques limites. Les auteurs ne proposent pas une approche pour supporter le processus d'évolution de l'ontologie, mais plutôt pour supporter la gestion des versions d'une ontologie après son évolution. Ils fournissent alors un modèle d'analyse de la relation entre les versions de l'ontologie, mais sans se préoccuper de la gestion de l'accès aux artefacts dépendants (i.e. objets référencés, ontologies, applications) au moyen de versions de l'ontologie. De plus, les auteurs ne développent aucun cadre fonctionnel pour intégrer la totalité des éléments méthodologiques qu'ils proposent.

2.9.8 Intégration des données par les ontologies

On distingue deux architectures pour l'intégration des données. L'approche médiateur [settouti2005] est fondée sur la définition de correspondances permettant la traduction des requêtes : une requête est formulée par un utilisateur dans les termes du schéma global et traduite en une ou plusieurs sous requêtes qui sont évaluées sur les données sources. Les réponses sont combinées et transformées afin d'être compatibles avec le schéma global et conforme à la requête de l'utilisateur. L'architecture d'un tel système est donnée en figure 2.10. L'ap-

proche entrepôt applique le principe de vues matérialisées et intègre les données en accord avec les schémas globaux. Le résultat est un entrepôt de données qui peuvent être directement interrogées à travers un langage adapté. L'architecture est montrée dans la figure 2.11.

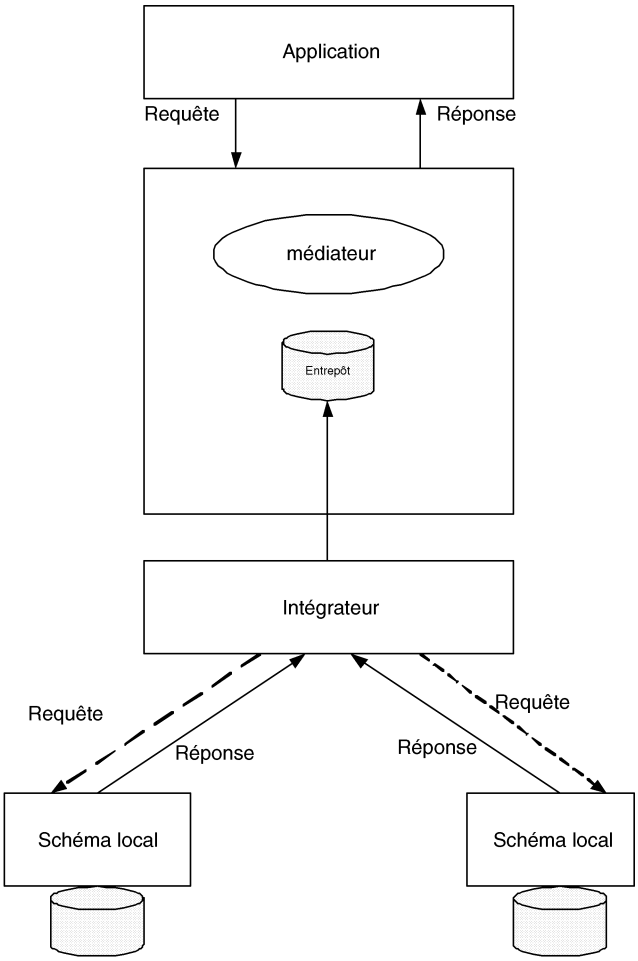

FIG. 2.10 – *Architecture médiateur*

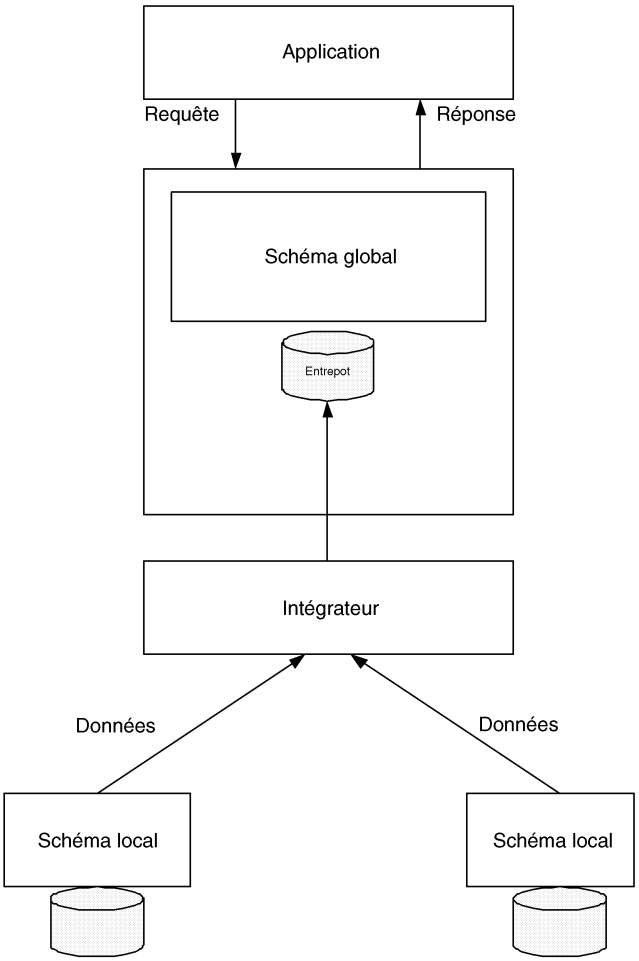

FIG. 2.11 – Architecture entrepôt

En principe les systèmes d'intégration doivent permettre à l'utilisateur de poser des requêtes plus complexes, que de simples mots clés, et être capables de donner des éléments de réponses provenant de sources de données différentes, afin de construire une réponse globale à l'utilisateur. Une ontologie peut être employée dans le processus d'intégration de données. On distingue plusieurs approches basées sur les ontologies, mais la manière d'utiliser les ontologies est différente. Wache dans [Wache2001] propose trois approches différentes : l'approche avec une simple ontologie, l'approche avec multiples ontologies, l'approche hybride.

2.9.8.1 Approche avec une ou plusieurs ontologies

Dans l'approche avec une seule ontologie, on utilise une ontologie globale qui fournit un vocabulaire partagé pour la spécification de la sémantique des sources de données. Toutes les sources de données sont reliées à une ontologie globale. une telle approche est visible sur la figure 2.12. Dans l'approche avec plusieurs ontologies, chaque source est décrite par sa propre ontologie, comme le montre la figure 2.13. L'avantage de cette approche est que l'ontologie n'a aucun besoin d'engagement commun et minimal envers l'ontologie globale[Favre2005]
.

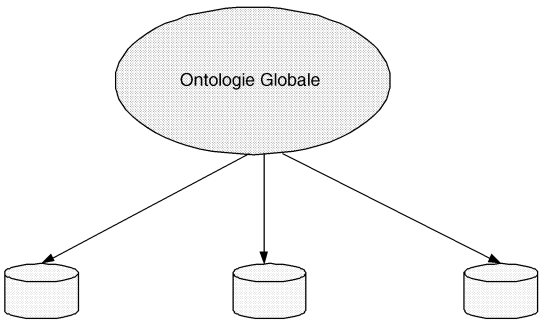

FIG. 2.12 – *Approche avec une ontologie*

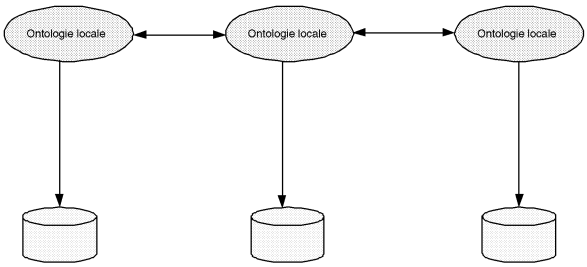

FIG. 2.13 – Approche avec plusieurs ontologies

2.9.8.2 Approche hybride

Pour surmonter les inconvénients des deux premières approches, les approches hybrides ont été développées comme indiquée à la figure 2.14. Cette approche décrit la sémantique de chaque source par sa propre ontologie comme avec l'approche à plusieurs ontologies. Les ontologies locales sont construites à partir d'un vocabulaire partagé. Le vocabulaire partagé contient les termes de base d'un domaine qui peuvent être combinées avec les ontologies locales afin de décrire une sémantique plus complexe[Wache2001]. L'avantage de cette approche réside sur le fait que les nouvelles sources peuvent facilement être ajoutées sans besoin de modification. Le vocabulaire partagé rend les ontologies de sources comparables et évite les inconvénients des approches avec multiples ontologies. L'inconvénient majeur de cette approche hybride réside sur le fait que les ontologies existantes ne peuvent pas facilement être réutilisées, mais doivent être reconstruites à partir de zéro [Wache2001].

2.10 Résumé

Dans ce chapitre nous avons étudié les bases de gestion de la SSI. Une bonne gestion de la sécurité vise à garantir les quatre conditions relatives à la confidentialité, la disponibilité, l'intégrité et la traçabilité. Pour atteindre nos objectifs, nous devons mener des actions susceptibles de nous aider à avancer dans ce sens. L'ensemble des indicateurs qui permettent de mesurer l'efficacité de ces actions constituent un TB. Les recherches sur les TB et de leur évolution durent déjà depuis quelques décennies. Il existe plusieurs méthodes qui diffèrent selon

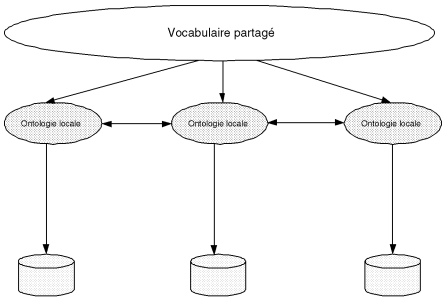

FIG. 2.14 – Approche hybride

les concepteurs, les destinataires, les utilisateurs et même l'environnement de l'entreprise. Nous avons énoncés deux méthodes de conception de TB de pilotage : la méthode BSC et la méthode GIMSI. Malgré le nombre restreint d'expériences effectuées avec le BSC, cet instrument semble présenter suffisamment d'avantages pour inciter le management à s'y intéresser. La mise en place d'un BSC n'est pas un problème ponctuel que l'on résoud, mais un système qui va vivre et qui doit se modifier en fonction des changements survenus dans l'entreprise et de son environnement. De plus, l'organisation en tant que telle apprend autant du processus que de l'instrument. Concevoir cet instrument est une chance unique de mettre sur pied des projets qui fédèrent, qui rassemblent. On ne peut pas s'approprier un instrument de réflexion stratégique de pilotage et de contrôle si l'on n'a pas participé à sa définition. La méthode GIMSI quant à elle est structurée en dix étapes successives, s'inscrivant ainsi dans un mode de management moderne, et privilégiant la coopération et le partage de la connaissance. Ainsi, la traditionnelle approche Top Down, GIMSI greffe une dimension *Bottom Up* et se focalise sur la question essentielle : comment se prennent réellement les décisions sur le terrain ? l'implication et l'appropriation sont au cœur de la méthode.

D'un autre côté nous avons analysé trois méthodes de conception des TB de la sécurité. La création et la gestion sont sensiblement identiques, quelle que soit l'approche utilisée. Il faut en règle générale s'assurer de sa cohérence et réaliser une mise à jour régulière avec une fréquence en fonction de la nature des indicateurs utilisés, définir les valeurs limites des différents indicateurs ; en dessous de la valeur minimale le niveau de sécurité n'est pas acceptable ; au-dessus de la valeur maximale, le niveau de sécurité est surdimensionné par rapport aux exigences de la PS. Enfin, il faut toujours sensibiliser les personnes chargées de la remontée des indicateurs de mesures. Nous avons en plus présenté une limite de toutes ces méthodes, que ce soit les méthodes de pilotage en général ou les méthodes pilotage de la sécurité en particulier. Nous avons terminé le chapitre en parlant des ontologies, qui sont des moyens très intéressantes et efficaces pour décrire des domaines vastes d'une façon permettant de traiter automatiquement l'information.

Dans les développements qui suivent, nous entendons nous inspirer des avantages et des limites des méthodes habituelles, nous servir des ontologies pour enfin concevoir un TB sécurité dynamique.

Chapitre 3

Construction d'une ontologie de la sécurité des systèmes d'information

3.1 Généralités

Plusieurs chercheurs travaillent actuellement sur la construction d'ontologies dans des domaines variés mais très peu travaillent sur la construction des ontologies dans le domaine de la SSI. A cause de la multitude de sources d'informations, la SSI devient de plus en plus difficile à implanter. L'information est variée et le concept qui y est attaché varie d'interprétation selon qu'on se trouve dans un contexte différent, même si on appartient à la même compagnie. Le financier ou le responsable des achats n'interprète pas de la même manière le risque de rupture de stock. Ceci dit, le savoir dans le domaine de la sécurité doit être analysé et interprété de manière uniforme, comme nous démontre Natalya [Natalya101] :

> "Analyser le savoir sur un domaine est possible dès que la spécification des termes du domaine est faite"

Pour permettre aux experts de la sécurité de parler le même langage, nous devons faire une analyse formelle et précieuse des termes utilisés, non seulement pour favoriser son utilisation mais aussi pour l'étendre à d'autres domaines. Cette approche nous laisse comprendre clairement que sans une spécification des termes dans le domaine de la sécurité, une analyse de l'information ne peut conduire qu'à une interprétation erronée. Le fait de développer une ontologie dans un domaine ou un sous domaine permettra de partager la compréhension commune de la structure de l'information entre les personnes travaillant dans le domaine, favorisant ainsi la réutilisation du savoir. Supposons par exemple qu'un certain nombre de sites Web contiennent de l'information sur la sécurité : si ces sites partagent et publient tous la même ontologie, celle étant à la base des termes qu'ils utilisent, alors les agents informatiques peuvent extraire et agréger l'information de ces différents sites. Les agents peuvent utiliser cette information agrégée soit pour pouvoir répondre aux interrogations des utilisateurs, soit comme données d'entrée pour d'autres applications.

La construction d'une ontologie pour la sécurité soulève la même problématique que celle du web sémantique ; toutefois les caractéristiques spécifiques à une ontologie de sécurité reflètent un manque de méthode et d'outils pour la conception. Le problème habituel reste d'actualité : celui de pertinence, de redondance, de contradiction, d'hétérogénéité de l'information. Notre approche dans la construction de l'ontologie consiste à accroître la capacité de cette dernière de manière qu'elle parvienne à spécifier et à extraire les connaissances à partir de plusieurs sources hétérogènes, construire une symbiose entre ces informations, et utiliser les techniques de traitement automatiques des informations.

3.2 Construction des ontologies locales

3.2.1 Présentation des corpus

Le développement des ontologies locales passe par la construction des corpus de textes. Dans le but de couvrir avec le plus d'exhaustivité possible l'ensemble de l'activité de la sécurité, nous avons utilisé la base de connaissances de MEHARI, la norme internationale ISO 17799 :2005, et les bases de connaissances de quelques compagnies. Ils se repartissent comme suit : MEHARI : 523, ISO 17799 : 2005 : 300, Experts : 200. Nous avons traités ces trois corpus manuellement car plusieurs outils de traitement automatique de texte traitent plus des mots. Nos corpus sont formés des phrases, ce qui nous a rendu la tâche très difficile. Les ressources constituant ces corpus nous parviennent sous format XLS (documents EXCEL), nous le traitons afin d'obtenir un format XML directement exploitable dans l'ontologie.

3.2.1.1 Outils

Pour construire les ontologies à partir de notre corpus nous nous sommes basés sur notre analyse propre de la syntaxe et de la sémantique des mots, faute de n'avoir pas trouvé une ontologie de la sécurité à partir de laquelle on pouvait travailler. Notre analyse nous a permis de déterminer les candidats termes qui ont permis la construction de l'ontologie. Le troisième corpus est composé de quelques cas pratiques et des interviews de quelques experts dans le domaine, nous a permis d'établir les relations entre les différents concepts.

3.2.2 La démarche

La méthodologie mise en œuvre permet de décrire tous les scénarios composés des termes communément utilisés dans le domaine de la sécurité. Ces scénarios peuvent être des risques, des contre-mesures de sécurité ou des indicateurs de sécurité. C'est la raison pour laquelle, malgré le fait que nous ayons deux corpus généralement connus dans le domaine (MEHARI et ISO 17799 :2000), cela n'a pas empêché qu'on se rapproche auprès des experts pour se familiariser avec le langage qu'ils utilisent tous les jours dans leur travail quotidien. Nous distinguerons quatre étapes successives dans notre démarche : 1) la constitution du corpus de connaissances et de son analyse, 2) l'engagement ontologique qui permet de formaliser les concepts et de définir les relations entre eux, 3) la classification et hiérarchisation des termes, 4) l'opérationnalisation de l'ontologie dans un langage de représentation des connaissances interprétables par l'ordinateur.

3.2.2.1 Traitement des ressources de base

Les trois corpus MEHARI, ISO177 :2005, Experts ont tous été traités manuellement. Les résultats de l'analyse de ces corpus nous ont permis de faire les rapprochements contextuels et de construire les groupes de candidats termes sémantiquement proches qui vont nous servir à bâtir les ontologies. Les termes contenus dans les deux corpus sont beaucoup plus proches, contrairement à ceux contenus dans le troisième. Le troisième corpus contient, en dehors des termes des deux premiers, d'autres termes utilisés dans le langage propre des compagnies. Tout dépend alors de la culture et de la politique de chaque compagnie.

3.2.2.2 Construction de l'ontologie, phase 1 : choix des candidats termes

Nous avons distingué deux étapes dans la sélection des candidats termes.

1. Nous notons ici une liste de tous les termes à traiter ou à expliquer à un utilisateur. Pour déterminer les propriétés de ces termes, nous établissons tout d'abord une liste sans nous soucier de l'éventuel chevauchement entre les termes. Il s'agit de rattacher des concepts à ces termes et de choisir ceux qui peuvent faire partie de l'ontologie. Rattacher les concepts aux termes revient à donner une description détaillée du terme ; si c'est un risque, on donnera l'impact de sa réalisation, sa cause ou son origine, sa potentialité. Si c'est une mesure, indépendamment du fait qu'elle soit dissuasive, préventive, de récupération, palliative ou de protection, on donne son objectif, le risque couvert. Si c'est un indicateur, on donne son seuil, le risque ou la mesure associée. On se pose par la suite une liste de questions appelées, questions de compétences. Cette liste permet de déterminer la portée de notre ontologie ; c'est une liste de questions auxquelles une base de connaissances fondée sur l'ontologie devrait pouvoir répondre [Gruninger1995]. Les questions servent à la fin de test pour savoir si l'ontologie contient assez d'informations. Si le terme choisi est un risque, on peut avoir les questions suivantes : 1) que souhaitez-vous éviter à votre ressource ? 2) quel est le risque résiduel si les contrôles potentiels sont mis en place ? 3) quel est l'impact ou la potentialité du risque ? si c'est une mesure, on peut avoir les questions suivantes : 1) est-ce que l'objectif est réalisable ? 2) est-ce que la mesure est associée à un risque ? 3) quelle est la robustesse ou l'efficacité de la mesure ? si c'est un indicateur, on peut se poser la question de savoir s'il mesure bien l'atteinte des objectifs etc.

2. Nous étudions les résultats obtenus à l'étape précédente et définissons les candidats termes sémantiquement proches les uns des autres pour structurer la hiérarchie de l'ontologie.

3.2.2.3 Construction de l'ontologie, phase 2 : formalisation des concepts

Toute classe représente un concept dans l'ontologie. Dans le domaine Risques, tous les risques de malveillances seront représentés par une classe appelée *Malveillances*. Dans la liste des termes créés dans la section précédente, nous sélectionnons les termes qui décrivent des objets ayant une existence indépendante plutôt que les termes qui décrivent ces objets. Ces termes constitueront les classes dans l'ontologie et deviendront des points d'ancrage dans la hiérarchie des classes. Si une classe A est superclasse d'une classe B, alors toute instance de

B est également, une instance de A. En d'autres termes, la classe B représente un concept qui est "une sorte" de A. Par exemple, tout risque lié à la destruction d'équipements est un risque accidentel. Par conséquent la classe *DestructionEquipement* est une sous-classe de la classe *Accident*.

Le mot concept est parfois utilisé à la place du mot classe. La classe est une représentation plus concrète (mathématique) d'un concept. Dans le domaine des risques, la classe *Risques* est le concept le plus général. *Malveillances*, *Erreurs* et *Accidents* sont des concepts généraux de niveau inférieur. Les classes *MaintenanceDeDonnees, DivulgationDeDonnees* sont plus spécifiques dans la hiérarchie (ou bien les concepts de niveau inférieur). Il est important de distinguer entre une classe et son nom : les classes représentent des concepts dans le domaine et non pas des mots désignant ces concepts. Le nom d'une classe varie suivant la terminologie choisie ; par exemple ; nous pouvons créer une classe *AccidentTelecom* et la rebaptiser après *TelecomAccident*. La classe représentera toujours le même concept. Dans le même ordre d'idées, un seul risque n'est pas une sous-classe de tous les risques. Ainsi, nous ne pouvons pas inclure, les deux versions au singulier et au pluriel du même concept dans l'ensemble des concepts, faisant ainsi de la première une sous-classe de la deuxième. Par exemple, il est faux de définir une classe *Erreurs* et une classe *Erreur* comme sous-classe d'*Erreurs*. L'erreur devient claire lorsqu'on pense à la hiérarchie comme un outil représentant la relation "une sorte de". Une erreur particulière n'est pas une sorte d'erreurs. Pour éviter cela nous avons choisi le pluriel dans la nomination de nos classes. Le même raisonnement s'applique dans le domaine des contre-mesures et celui des indicateurs.

3.2.2.4 Construction de l'ontologie, phase 3 : classification et hiérarchisation des termes

D'après [Gruninger1995], il existe plusieurs approches possibles pour développer une hiérarchie de classes. Dans notre cas nous avons opté pour un procédé de développement de haut en bas, en commençant par une définition des concepts plus généraux du domaine, ensuite poursuivre par la spécialisation des concepts.
Dans le domaine des risques, nous pouvons créer des classes pour les concepts généraux *Accidents*, *DestructionEquipements*, *IndisponibilitePassagereDesRessources*, *DestructionDeLogiciels*, *AlterationDeDonnees*, *Erreurs*, *Malveillances*, puis nous spécialiserons en créant quelques-unes de ses sous-classes : *ManipulationDesDonnees*, *DivulgationDesDonnees, DetournementDeFichiers, PerteDeFichiers, SinistreImmaterielTotal,* etc. Nous organisons les classes dans une taxonomie hiérarchique en nous demandant, si en étant instance d'une classe, un objet sera nécessairement (c'est à dire par définition) une instance d'une autre classe. Si une classe A est superclasse d'une classe B, alors toute instance de B est également, une instance de A. En d'autres termes, la classe B représente un concept qui est " une sorte " de A. Par exemple, tout risque lié à la destruction d'équipement est un risque accidentel. Par conséquent la classe *DestructionEquipements* est une sous-classe de la classe *Accidents*. La hiérarchie des risques est représentée par les figures : fig 3.1, fig 3.2, fig 3.3

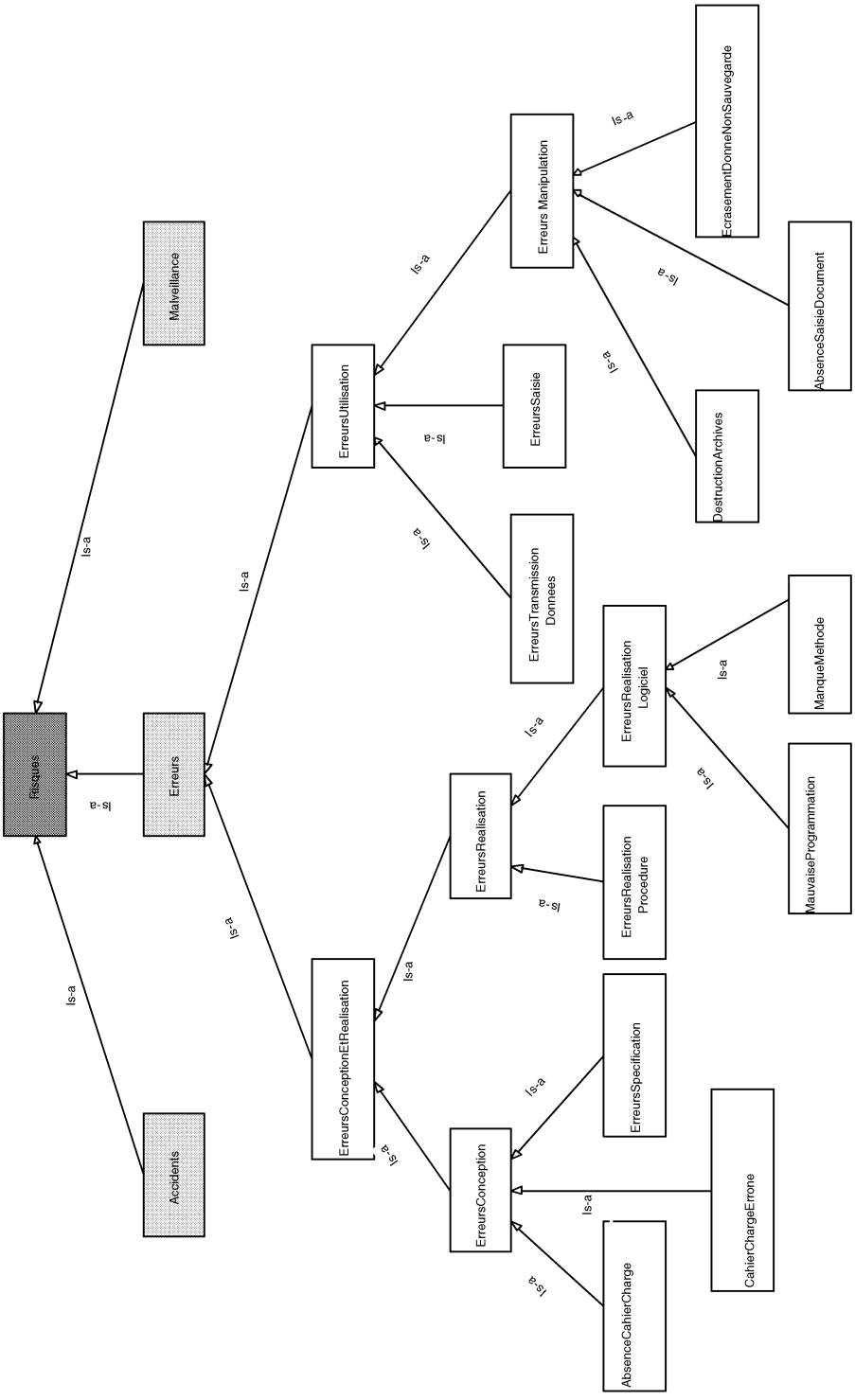

FIG. 3.1 – Hiérarchie des classes du concept Risques

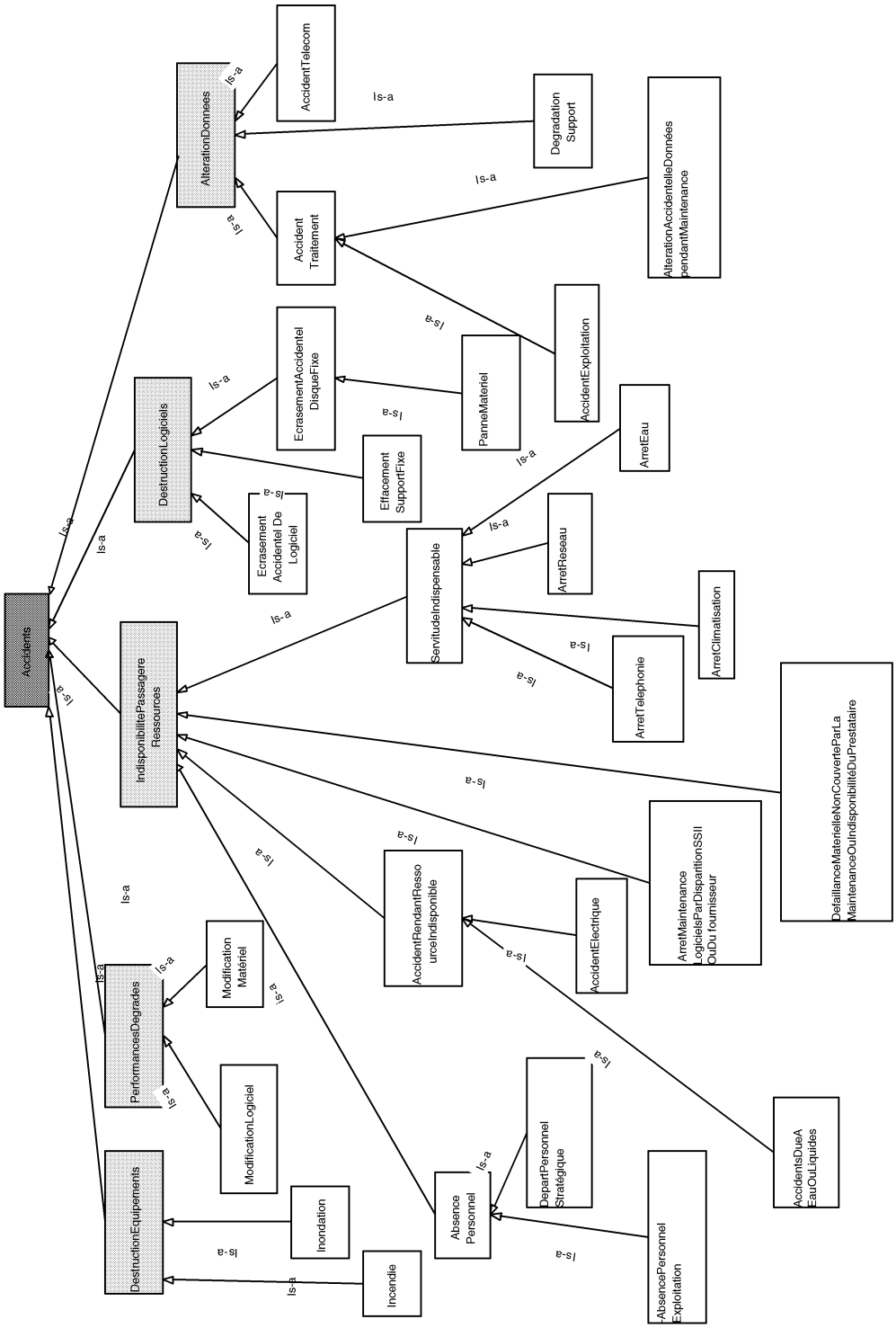

FIG. 3.2 – Hiérarchie des classes du concept Accidents

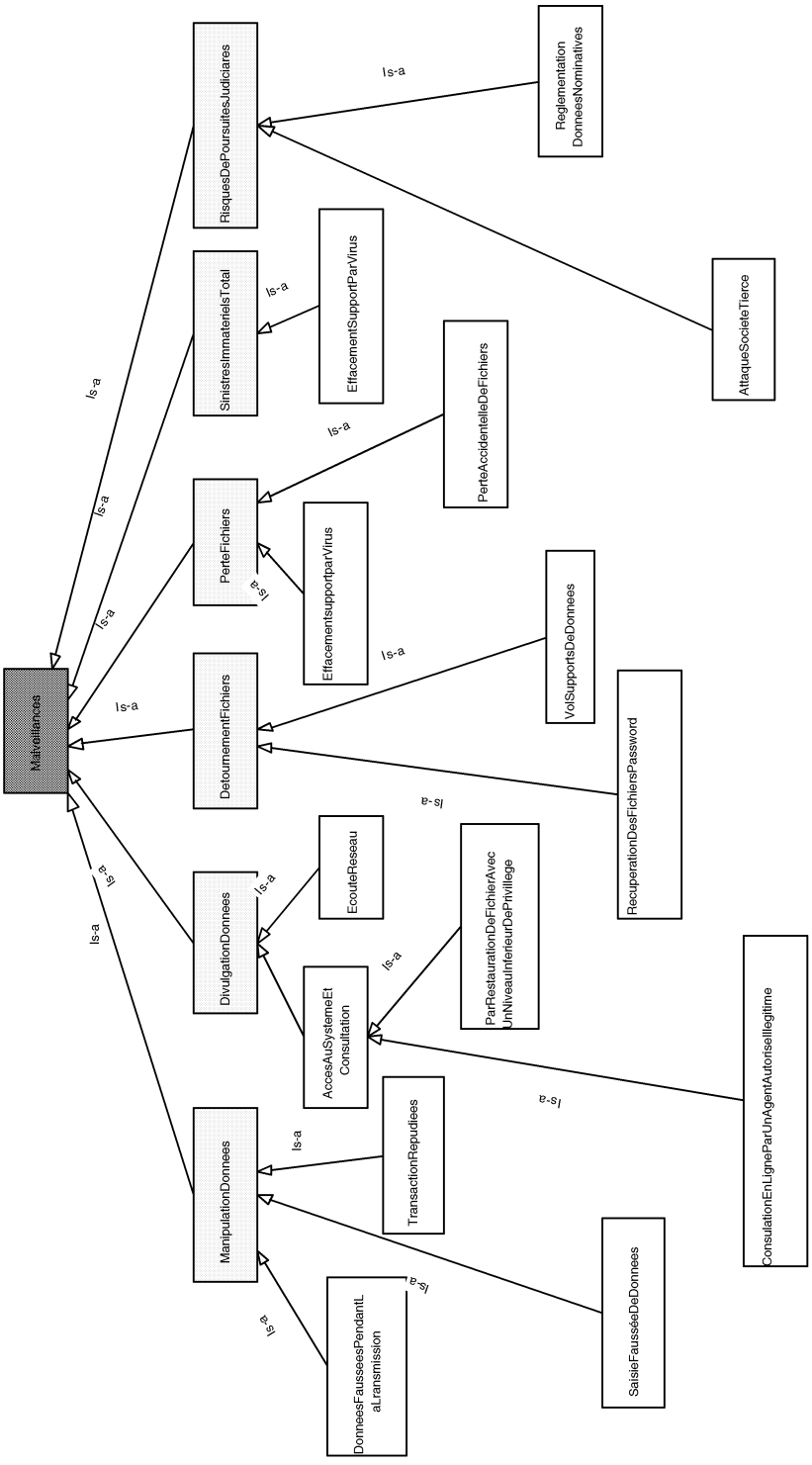

FIG. 3.3 – Hiérarchie des classes du concept Malveillance

Dans le domaine des contre-mesures, on distingue trois grandes classes : *MesuresTechniques, MesuresOrganisationnelles, MesuresPhysiques*. Ces classes principales sont divisées en sous classes : La protection de l'environnement du SI comporte l'ensemble des mesures classiques de protection physique d'un bien électronique de valeur : *ControleDesAccesAuxLocaux, DispositifsAnti-Intrusions, RegulationDeAlimentationElectriques, ProtectionContreIncendies*. La sécurité physique comme le montre la figure 3.6 se divise en deux grandes classes : *ZonesSecurisees, SecuriteDuMateriel*. L'objectif d'une Zone Sécurisée est d'empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux et les informations de l'organisme. Pour atteindre cet objectif, sept mesures peuvent être mises en place comme le montre la figure 3.6. Ces mesures représentent des classes différentes de l'ontologie des mesures. L'objectif de la sécurité du matériel est d'empêcher, l'endommagement, le vol ou la compromission des biens et l'interruption des activités de l'organisme. Il convient de protéger le matériel des menaces physiques et environnementales.
Les solutions techniques visent en priorité à la protection de l'environnement du SI, des supports de données et des transmissions. La protection du SI est assurée notamment par des contrôles d'accès logique, sur sites et à distance (identification, authentification et signature électronique), possibilité de contrôle de transactions qui y sont effectuées, la sauvegarde des données et des programmes, et la mise en œuvre des dispositifs antivirus. Cette classe se divise en plusieurs classes comme le montre la figure 3.6 : *ControleAcces*, *GestionEexploitationEtDesTelecommunications*, *Acquisitions*, *DeveloppementEtMaintenanceDesSI*, *GestionDesIncidentsSSI*. La classe *ControleAcces* possède plusieurs classes :

- la classe *Exigences métier relative au contrôle d'accès* permet de maîtriser l'accès à l'information. Il convient que l'accès à l'information, aux moyens de traitement de l'information et aux processus métier soit contrôlé sur la base des exigences d'exploitation et de sécurité ;

- la classe *Gestion de l'accès utilisateur* permet de maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux SI ;

- la classe *Responsabilités Utilisateurs* permet d'empêcher les accès utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de traitement de l'information ;

- la classe *Contrôle d'accès au réseau* permet d'empêcher les accès non autorisés aux services disponibles sur le réseau. Il convient de contrôler l'accès aux services à la fois en interne et en externe ;

- la Classe *Contrôle d'accès au Système d'Exploitation* a pour objectif d'empêcher les accès non autorisés aux systèmes d'exploitation. Il convient de mettre en place des dispositifs de sécurité pour restreindre l'accès aux systèmes d'exploitation aux seuls utilisateurs habilités. Cette classe possède six sous-classes représentant des mesures à mettre en place pour sécuriser le contrôle d'accès au système d'exploitation ;

- la classe*Contrôle d'accès aux applications et à l'information* permet d'empêcher les accès non autorisés aux informations stockées dans les applications. Il convient de mettre en place des dispositifs de sécurité

pour restreindre l'accès aux applications et à la navigation au sein des applications ;

- la classe *Informatique mobile et Télétravail* permet de garantir la sécurité de l'information lors de l'utilisation d'appareils informatique mobiles et d'équipements de télétravail ;

La classe *Gestion de l'exploitation et des télécommunications* possède plusieurs sous-classes ;

- la classe *Procédures et responsabilités liés à l'exploitation* permet d'assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information. Il convient d'établir les responsabilités et les procédures liées à la gestion et l'exploitation de l'ensemble des moyens de traitement de l'information. Elle comprend la mise au point des procédures d'exploitation appropriée ;

- la classe *Gestion de la prestation de service par un tiers* permet de mettre en œuvre et maintenir un niveau de sécurité de l'information et de service adéquat et conforme aux accords de prestation de service par un tiers ;

- la classe *Gestion Planification et acceptation du système* permet de réduire le plus possible le risque de pannes des systèmes ;

- la classe *Sauvegarde* permet de maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information. Il convient de dresser des procédures de routine pour mettre en œuvre la politique et la stratégie de sauvegarde convenues stipulant de réaliser des copies de sauvegarde des données et de procéder à des répétitions pour que leur restauration puisse être effectuée en temps voulu.

La classe *Acquisition, développement et systèmes d'information* possède les sous classes suivantes :

- la classe *Exigences de sécurité applicables aux SI* permet de veiller à ce que la sécurité fasse partie intégrante des SI. Les SI comprennent des systèmes d'exploitation, une infrastructure, des applications de gestion, des services et des applications mises au point par les utilisateurs ;

- la classe *Bon fonctionnement des applications* permet d'empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les applications ;

- la troisième classe *Mesures cryptographiques* permet de protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques. Il faut élaborer une politique d'utilisation des mesures cryptographiques. Il convient de créer une procédure de gestion des clés pour mettre en œuvre les techniques cryptographiques ;

- la classe *Sécurité des fichiers systèmes* permet de garantir la sécurité des fichiers systèmes. Il convient de contrôler l'accès aux fichiers systèmes et au code source du programme et de conduire les projets informatiques et les activités d'assistance conformément aux exigences de sécurité ;

- la classe *Sécurité en matière de développement et d'assistance technique* permet de garantir la sécurité du logiciel et des informations d'application. Il convient de mettre en place des mesures strictes pour l'environnement projet et l'environnement support.

La classe *Gestion des incidents liés à la sécurité de l'information* possède deux sous-classes :

- la classe *Signalement des événements et des failles liés à la sécurité de l'information* permet de garantir que le mode de notification des événements et failles liés à la sécurité de l'information permette la mise en œuvre d'une action corrective, dans les meilleurs délais.

- la classe *Gestion des améliorations et incidents liés à la sécurité de l'information* permet de garantir la mise en place d'une politique cohérente et efficace pour la gestion des incidents liés à la sécurité de l'information. On doit définir des responsabilités et des procédures permettant une gestion efficace des événements et failles de sécurité après leur signalement. Il convient d'appliquer un processus d'amélioration continue pour la surveillance, l'évaluation et la gestion globale des incidents liés à la sécurité de l'information, ainsi que pour les actions correctives mises en œuvre.

Contrairement aux mesures techniques et physiques, les mesures organisationnelles couvrent un domaine non technique. On distingue six grandes classes : *Politique de sécurité, Organisation de la sécurité, Gestion des biens, Sécurité des ressources rumaines, Gestion de la continuité du business, Conformité.*
La classe *politique de sécurité* permet d'apporter une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. La direction doit définir des dispositions générales claires en accord avec ses objectifs et qu'elle démontre son soutien et son engament vis-à-vis de la sécurité de l'information, en mettant en place et en maintenant une PS de l'information pour tout l'organisme. La figure 3.7 montre la hiérarchie des classes des mesures organisationnelles.

La classe *Organisation de la Sécurité* permet de gérer la sécurité de l'information au sein de l'organisme. Pour cela il faut établir un cadre de gestion pour initialiser, puis contrôler la mise en œuvre de la sécurité de l'information au sein de l'organisme. La direction doit approuver la PS de l'information, attribue les rôles liés à la sécurité, puis coordonne et réexamine la mise en œuvre de la sécurité à travers l'organisme.

La Classe *Gestion des Biens* permet de mettre en place et maintenir une protection appropriée des biens de l'organisme. La mise en œuvre de mesures spécifiques peut être déléguée par le propriétaire, mais ce dernier demeure responsable de la protection des biens.

La classe *Gestion des Ressources Humaines* permet de définir des mesures de sécurité avant le contrat, pendant le contrat et après le contrat. Les mesures de sécurité prises avant le recrutement ont pour objectif de garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils correspondent aux fonctions qui leur sont attribuées. Il convient de mentionner les responsabilités en matière de sécurité avant l'embauche, dans des descriptions de postes adéquats, puis dans le contrat de travail. Pour at-

teindre cet objectif la classe *Avant le Recrutement* possède trois sous-classes comme le montre la figure 3.7. Par contre les mesures de sécurité prise pendant le contrat ont pour objectifs de veiller à ce que les salariés, contractant et utilisateurs tiers soient conscients des menaces pesant sur la sécurité de l'information, de leurs responsabilités financières ou autres, et de la nécessité de disposer des éléments requis pour prendre en charge la PS de l'organisme dans le cadre de leur activité normale et de réduire le risque d'erreur humaine.

La classe *Gestion de la Continuité de l'Activité* permet de neutraliser les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les principales défaillances des SI ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

La classe conformité possède trois sous classes : *Conformité avec les exigences légales, conformité avec les politiques et les normes, prise en compte de l'audit du SI*. La classe *Conformité avec les exigences légales* a pour objectif d'éviter toute violation des obligations légales, statuaires, réglementaires ou contractuelles et des exigences de sécurité. La classe *Conformité avec les politiques et normes de sécurité* et *conformité technique* a pour objectif de s'assurer de la conformité des systèmes avec les politiques et normes de sécurité de l'organisme. Il convient de réexaminer régulièrement la sécurité des SI.

La classe *Prise en compte de l'audit du système d'information* permet d'optimiser l'efficacité et réduire le plus possible l'interférence avec le processus d'audit du SI. Il convient de prendre des mesures pour protéger les systèmes d'exploitation et les outils d'audit lors des audits du SI.

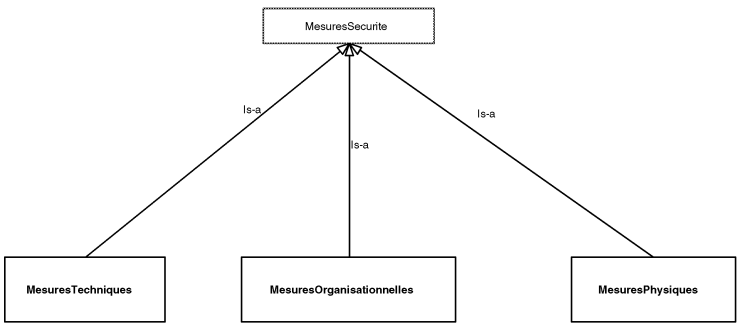

FIG. 3.4 – Hiérarchie des classes des mesures de sécurité

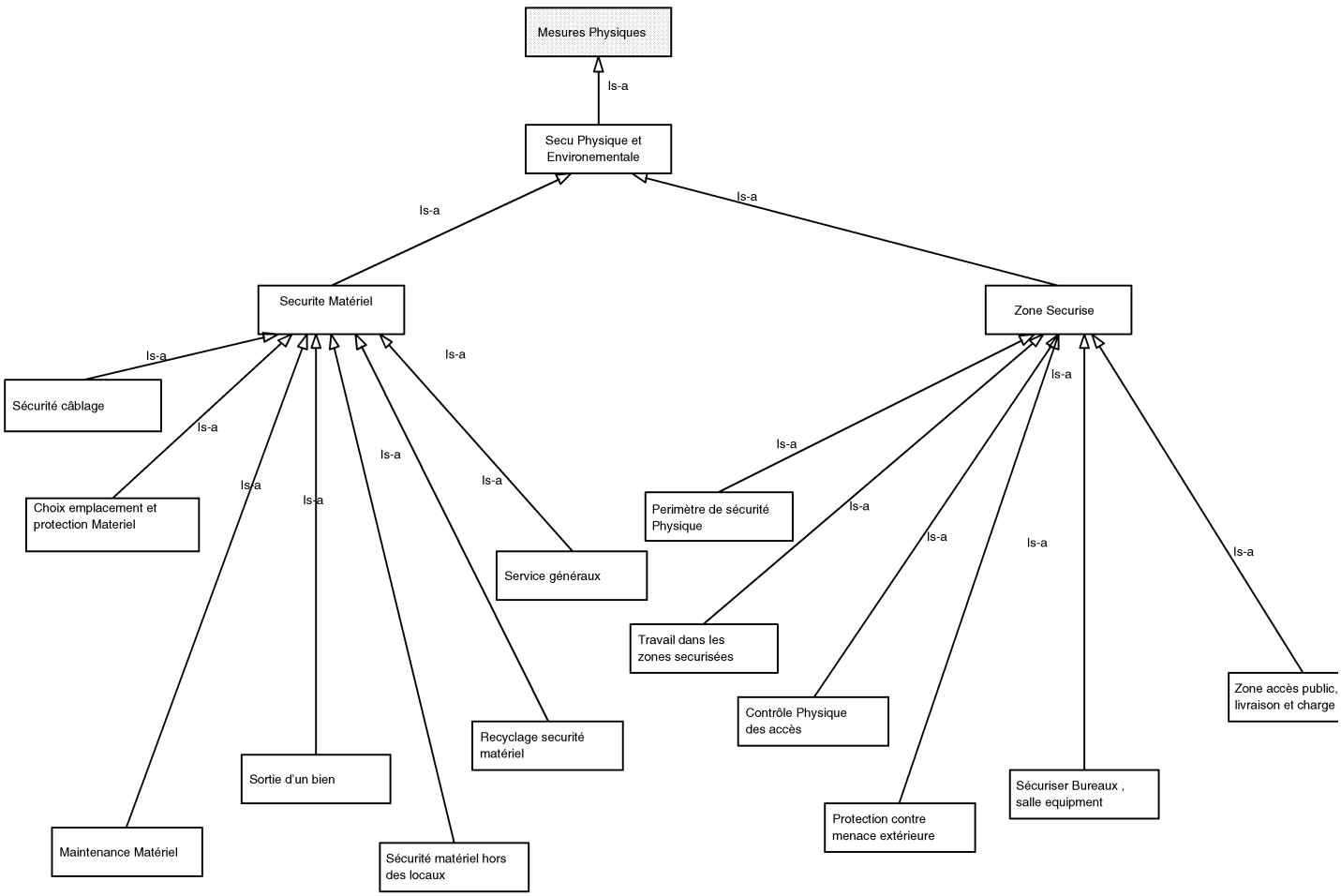

FIG. 3.5 – Hiérarchie des classes pour le concept mesures physiques

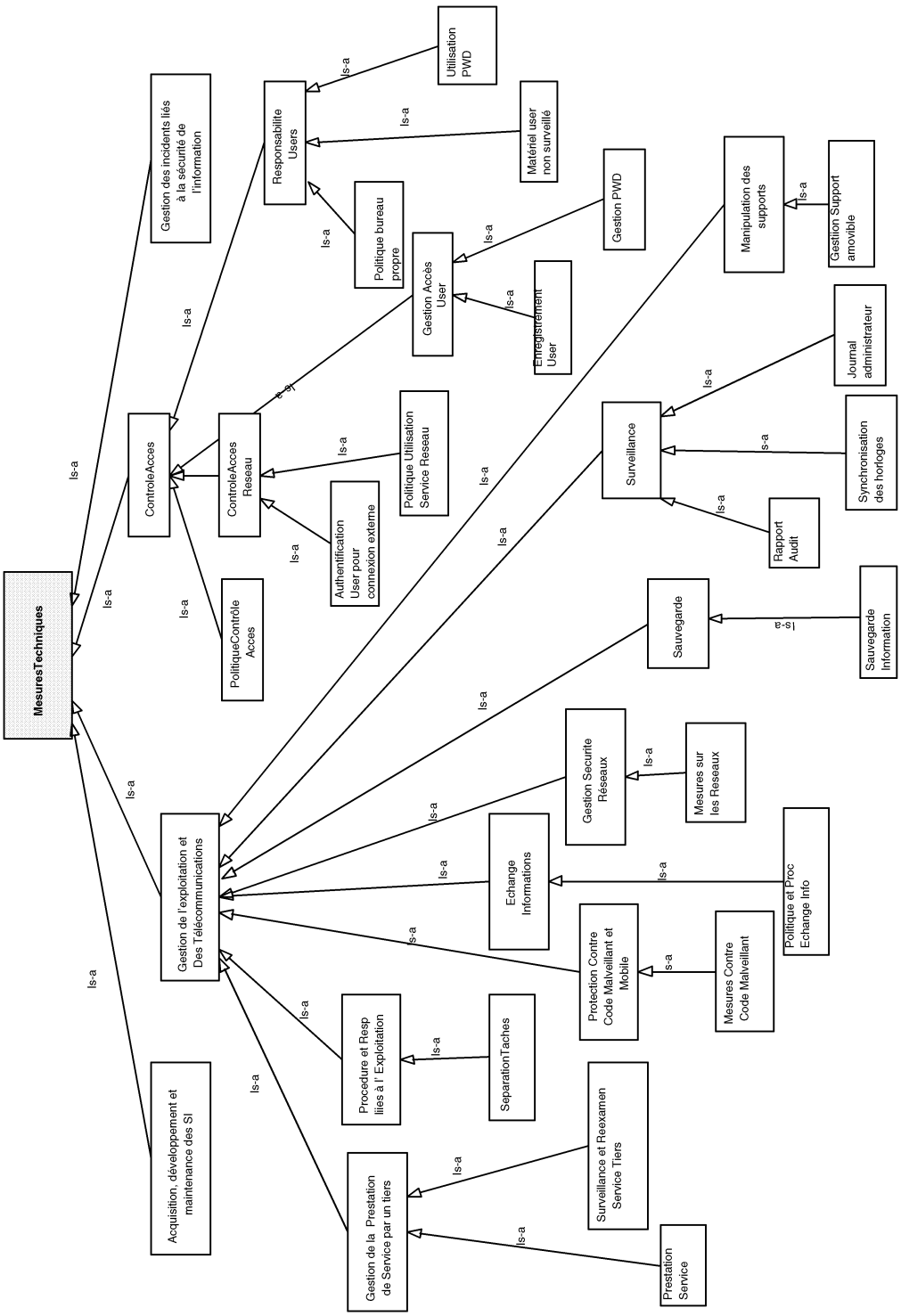

FIG. 3.6 – Hiérarchie des classes pour les mesures Techniques

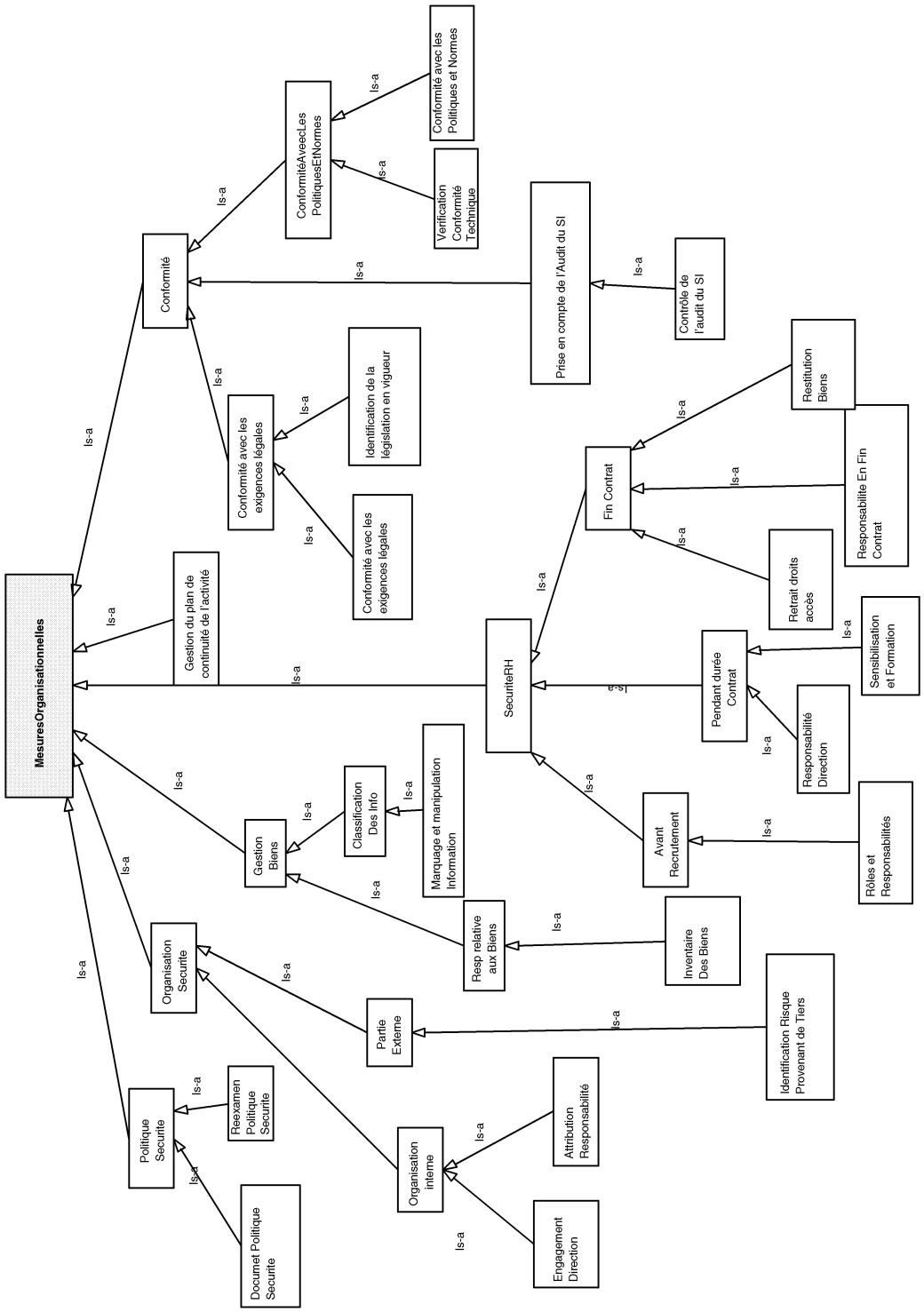

FIG. 3.7 – Hiérarchie des classes pour les mesures Organisationnelles

Dans le domaine des indicateurs, on distingue trois grandes classes : la classe *Stratégique*, la classe *Fonctionnel* et la classe *Opérationnel*.

Les indicateurs stratégiques sont de niveau 1. On peut citer les indicateurs liés à l'organisation de la sécurité, la protection des locaux, la sécurité applicative, la sécurité des projets et développement. Ils permettent de mesurer le niveau de sécurité sur un sous domaine précis, possède un ou plusieurs indicateurs fonctionnels et son interprétation dépend de celles des indicateurs fonctionnels qu'il possède. Pour qu'on juge le niveau de sécurité bon, il faut que les mesures de tous les indicateurs fonctionnels qui le composent aient des mesures qui jugent le niveau de sécurité bon. Il peut être indépendant, supposons qu'on ajoute un nouveau domaine qui n'était pas connu jusqu'à présent et que sa typologie ne permette pas d'introduire de sous domaine avant une certaine période, il reste indicateur indépendant.

Les indicateurs fonctionnels sont de niveau 2, ils peuvent alimenter un indicateur stratégique d'après le principe selon lequel, dans l'hiérarchie des classes, toute sous-classe est une forme de sa super classe. Un indicateur fonctionnel ne peut pas alimenter un indicateur fonctionnel. Il possède un ou plusieurs indicateurs opérationnels. Les indicateurs remontent des informations sur l'efficacité de la politique de sécurité, la qualité des outils et méthodes utilisées, la conformité de ce qui est fait avec les objectifs stratégiques, etc. Nous allons développer la hiérarchie de classes correspondant à l'indicateur "Sécurité des architecture réseaux et de communications".

Les indicateurs opérationnels sont de niveau 3, ils ne peuvent pas alimenter un indicateur opérationnel. Plusieurs indicateurs opérationnels peuvent alimenter un indicateur fonctionnel. Au niveau opérationnel, les indicateurs remontent les informations quantitatives (mesures techniques permettant d'affiner les réglages des alertes, des détecteurs d'incident ou d'autres dispositifs techniques de sécurité). Nous avons neuf grandes classes d'indicateurs. Chaque classe possède en moyenne une dizaine de sous-classes.

1. *OrganisationSecuriteInformation :* on distingue les indicateurs de sensibilisation et de formation à la sécurité, les indicateurs de gestion des RH etc. Les indicateurs de sensibilisation et de formation à la sécurité reflètent l'évolution de la sensibilisation de l'entreprise et la formation du personnel à la sécurité, tandis que les indicateurs de Gestion des RH doivent refléter la criticité des RH pour les postes stratégiques ou sensibles, l'évolution des responsabilités.

2. *SiteEtEtablissement :* nous retrouvons dans cette classe, les indicateurs d'implantation du site, les indicateurs de contrôle d'accès, et les indicateurs de gestion de la sécurité physique. Les indicateurs contrôle d'accès au site reflètent la fréquentation et la diversité des populations accédant au site, tandis que les indicateurs *Contrôle de la circulation* sur le site doivent refléter les incidents liés à la circulation tant du personnel interne qu'externe, à la circulation des visiteurs et à celle des fournisseurs, etc.

3. *ProtectionDesLocaux :* dans cette classe on retrouve :
   les indicateurs *ServicesGeneraux* ; qui reflètent l'évolution de la qualité de la fourniture des services ; les

indicateurs *ControleAccesBatimentsSensibles* ; qui reflètent l'évolution de la qualité du contrôle d'accès ; les indicateurs *ContrôleAccesLocauxSensibles* ; qui reflètent l'évolution de la sécurité des locaux sensibles ; les indicateurs *ControleAccesBureaux* ; reflètent l'évolution de la sécurité des bureaux .

4. *SecuriteDesArchitecturesReseauxEtTelecommunications :*
   les indicateurs reflètent l'évolution de la qualité du contrôle d'accès aux réseaux ; on retrouve les indicateurs *ControleConfidentialiteEchangesEtCommunications* ; ils doivent refléter l'évolution de la qualité du contrôle de la confidentialité et des communications ; les indicateurs *Contrôle de l'intégrité des échanges et des communications* ; qui reflètent l'évolution de la qualité du contrôle de l'intégrité des échanges et des communications ; les indicateurs *IntegriteElementsBaseReseau* ; reflètent l'évolution de la qualité de l'intégrité des éléments de base du réseau.

5. *ExploitationRéseauxTelecom :*
   Dans cette classe d'indicateurs on trouve les indicateurs *SecuriteProceduresExploitation*, reflètent la qualité du service rendu par l'exploitation des réseaux et des télécommunications.

6. *SecuriteSystemesArchitecture :*
   Les indicateurs permettront de renseigner sur l'utilisation des systèmes informatiques.

7. *ProductionInformatique :*
   dans cette classe nous avons les indicateurs " SécuritéProcéduresExploitation". Ils doivent refléter la sécurité des procédures d'exploitation. Les indicateurs *ContrôleConfigurationsMatériellesLogicielles*, doivent refléter le contrôle des configurations matérielles et logicielles.

8. *SécuriteApplicative :*
   Cette classe possède les indicateurs pertinents permettront de renseigner sur l'utilisation des applications.

9. *SecuriteProjetsDeveloppements :*
   Cette classe possède les indicateurs qui reflètent la sensibilité de l'équipe de développement, la disponibilité des ressources, la traçabilité et fiabilité de l'application.

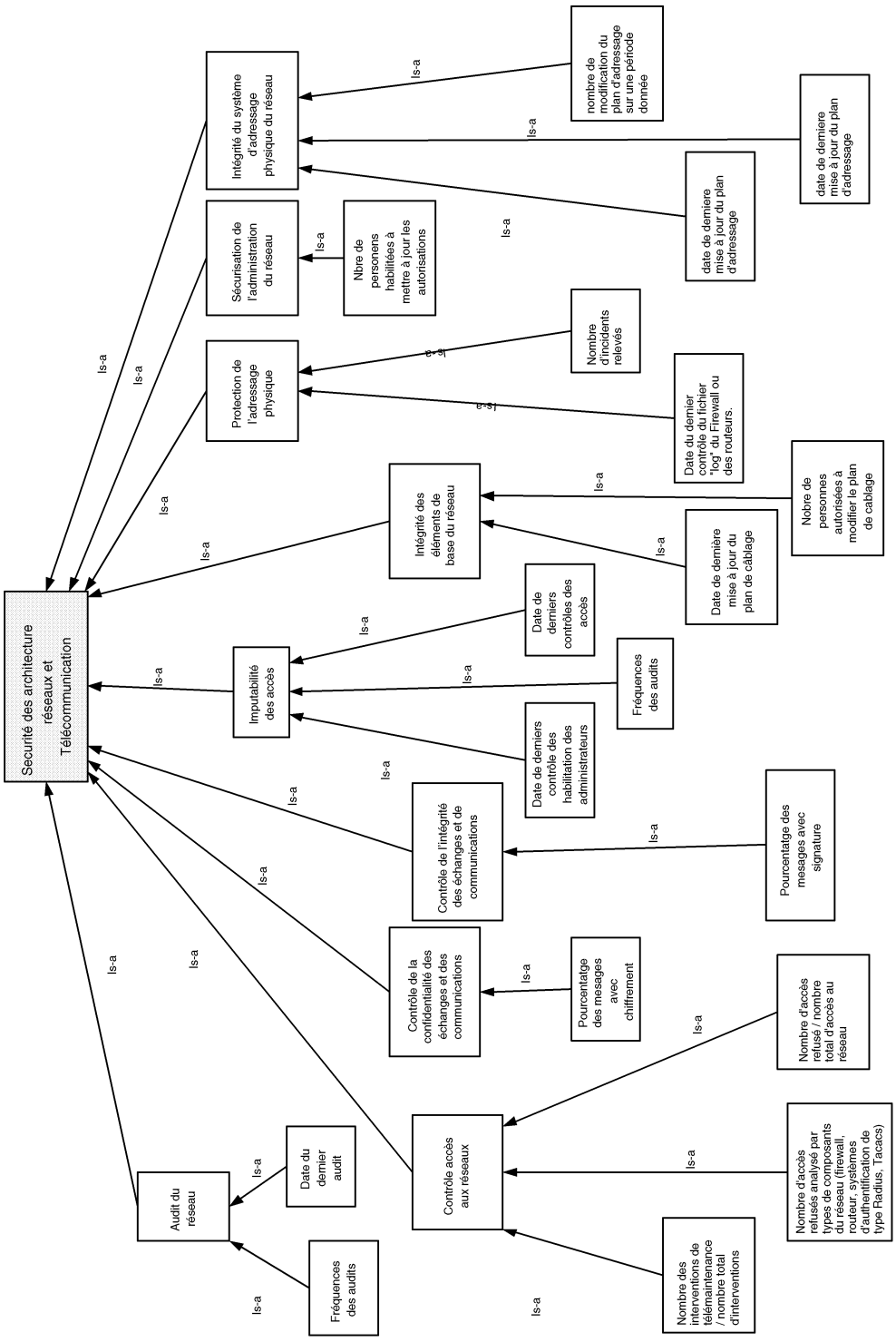

FIG. 3.8 – Hiérarchie de classes pour le sous concept Sécurité des architectures réseaux et Télécommunication

Les relations entre les classes

Sous-classe disjointe : les classes sont disjointes lorsqu'elles ne peuvent pas avoir d'instances en commun. Par exemple, les classes *AlterationDonnees* et *DestructionLogiciels* sont disjointes dans notre ontologie. On estime qu'un même risque ne peut pas être à la fois une altération de données et une sorte de destruction de logiciels. Par contre les classes *IndisponibilitePassagereRessource* et *DestructionLogiciels* ne sont pas disjointes. Certains risques sont à la fois instance de l'une et de l'autre. Spécifier que les classes sont disjointes permet au système de mieux valider l'ontologie. Si nous déclarons les classes *AltérationDonnées* et *DestructionLogiciels* comme étant disjointes, et qu'ensuite nous créons une classe à la fois sous-classe de l'une et de l'autre, le système signalera une erreur de modélisation.

Boucles : nous avons évité des boucles dans la hiérarchie de classe. On dit qu'il y a une boucle dans une hiérarchie quand une classe A a une sous-classe B et qu'en même temps B est une superclasse de A. Créer une telle boucle dans une hiérarchie revient à déclarer que les classes A et B sont équivalentes : toutes les instances de A sont des instances de B et toutes les instances de B sont aussi des instances de A. En fait, puisque B est une sous-classe de A, toutes les instances de B doivent être des instances de la classe A. Comme A est une sous-classe de B, toutes les instances de A doivent aussi être des instances de la classe B.

Héritage multiple : notre système, comme la plupart des systèmes de représentation de connaissances, permet l'héritage multiple dans la hiérarchie de classes. Une classe peut être une sous-classe de plusieurs classes. Supposons que, lors de l'évolution des classes, nous voulons créer une classe distincte pour les risques accidentels mais donc l'origine est intentionnelle. Appelons cette classe "Accidents Intentionnels", elle peut avoir trois super classes : *DestructionEquipements*, *DestructionDonnees*, *DestructionLogiciels*. Toutes les instances de la classe *AccidentsIntentionnels* seront aussi bien instances de la classe *DestructionEquipements* que de la classe *DestructionDonnees* et de *DestructionLogiciels*. Cette classe hérite les attributs et les facettes des attributs de ses deux classes parents.

Les propriétés des classes : les classes seules ne fournissent pas assez d'information pour répondre aux questions. Les propriétés permettent de décrire la structure interne des classes. La liste des termes sélectionnés pour les classes ne pouvant être exhaustive, les termes restant ont de fortes chances d'être des propriétés des classes. Les propriétés sont les relations binaires[1] sur les individus. Les propriétés lient deux individus ensemble. Ces termes comprennent par exemple : impact d'un risque, sa fréquence annuelle d'apparition, sa probabilité d'apparition. Pour chaque propriété nous devons donner la classe qu'elle décrit. Ces propriétés deviennent des attributs rattachés aux classes. Ainsi la classe Risques a les propriétés suivantes :

- hasImpactIntrinseque : décrit l'impact intrinsèque du risque
- hasExpositionNnaturelle : décrit l'exposition naturelle du risque
- hasMesuresDissuasives : décrit les mesures dissuasives

[1] Une relation binaire est une relation entre deux objets

- hasMesurePreventives : décrit les mesures préventives
- hasMesuresPalliatives : décrit les mesures palliatives
- hasMesuresRecupération : décrit les mesures de récupération
- hasCause : décrit la cause du risque
- hasOrigine : décrit l'origine du risque

Outre les propriétés citées plus haut, on peut ajouter les propriétés suivantes : nom du risque, niveau de profondeur dans notre arbre hiérarchique, description du risque etc. Toutes les sous-classes d'une classe héritent les attributs de cette classe. Par exemple tous les attributs de la classe *RisquesDeMalveillances* seront hérités par les sous-classes de Malveillances, y compris *DivulgationDonnees*, *PerteFichiers* et *DetournementFichiers*. Un attribut doit être rattaché à la classe la plus générale pouvant posséder cette propriété. Par exemple la fréquence d'apparition du risque, son impact, doivent être attaché à la classe *Risques*, puisque c'est la classe la plus générale dont les instances auront un attribut "hasImpact" "hasExpositionNaturelle" etc...

FIG. 3.9 – Hiérarchie des propriétés

Propriétés inverses chaque propriété possède une propriété inverse. Si une propriété lie un individu **a** à un individu **b**, alors son inverse lie l'individu b à l'individu a. Par exemple, l'inverse de hasInpactIntrinseque est IsImpactIntrinsequeOf, et hasExpositionNaturelle est IsexpositionNaturelleOf. Lorsqu'on définit des propriétés, il est très important de noter des détails supplémentaires dans l'ontologie. La valeur d'une propriété

peut dépendre de la valeur d'une autre propriété. Par exemple, si l'effacement de support fixe est produit (hasDone) par une altération accidentelle de données pendant la maintenance, alors on peut dire qu'une altération accidentelle de données pendant la maintenance produit l'effacement d'un support fixe. Ces deux relations producteur et produit sont des **relations inverses** d'après [Natalya101]. Il serait redondant de stocker l'information dans les deux sens. Si un effacement de support fixe a été produit par une altération accidentelle de données pendant la maintenance, une application utilisant la base de connaissances peut toujours déduire la valeur pour la relation inverse.

Transitivité des propriétés : dans le système, la propriété "Is-a" est transitive. Ainsi, si B est une sous-classe de A et C est une sous-classe de B, alors C est une sous-classe de A. La classe *AbsencePersonnelExploitation* est une sous-classe de *Absence du personnel* qui est une sous-classe de la classe *IndisponibilitePassagereRessources*, la transitivité des relations dans les sous-classes signifie que la classe *AbsencePersonnelExploitation* est une sous-classe de la classe *IndisponibilitePassagereRessources*. Nous distinguons ici les sous-classes directes[2] et les sous-classes indirectes. Il n'y a pas de classes entre une classe et sa sous-classe directe dans la hiérarchie. Dans notre exemple la classe Absence de personnel est une sous-classe directe de *IndisponibilitePassagereRessources*. ainsi, le risque qu'il y'ait un personnel d'exploitation absent est un risque d'indisponibilité passagère des ressources. Nous parlons aussi de transitivité des propriétés. La propriété "hasCause" est transitive.

Propriétés et restrictions : nous avons utilisé des propriétés pour créer des restrictions. Les restrictions sont utilisées pour restreindre les objets qui doivent appartenir à une classe. En OWL, il existe trois types de restrictions : le quantificateur existentiel, le quantificateur universel et la restriction sur une valeur. Dans le cadre de cette étude, nous avons utilisé juste les quantificateurs. Ce type de restriction est composé d'un quantificateur, d'une propriété et d'un filtre. Par exemple la restriction $\exists$ hasCause Inondation. Cette restriction décrit l'ensemble ou la classe des objets qui ont au moins une cause qui soit un individu de la classe Inondation. Cette restriction est décrite par la figure 3.11. Nous avons donc la classe des objets qui remplissent cette restriction. Le quantificateur existentiel est le plus utilisé. Pour un ensemble d'objets, une restriction existentielle spécifie l'existence (au moins un) d'une relation pour une propriété donnée des éléments d'une certaine classe. Cette restriction définie la classe des objets qui ont au moins une cause qui trouve son origine dans l'inondation

3.2.2.5 Construction de l'ontologie, phase 4 : formalisation dans un langage de représentation de connaissances

Notre ontologie contient actuellement plus de 500 concepts primitifs issus d'une première analyse des candidats termes faite dans les phases précédentes. Les phases de constructions 1) et 2) étant itératives, nous augmenterons très rapidement la représentation en examinant les candidats termes qui n'ont pas été retenu et qui pourrait apparaitre lors de l'examen d'un autre corpus. La base de connaissances. Après avoir éditer les

[2]Une sous-classe directe est la sous-classe la plus proche de la classe

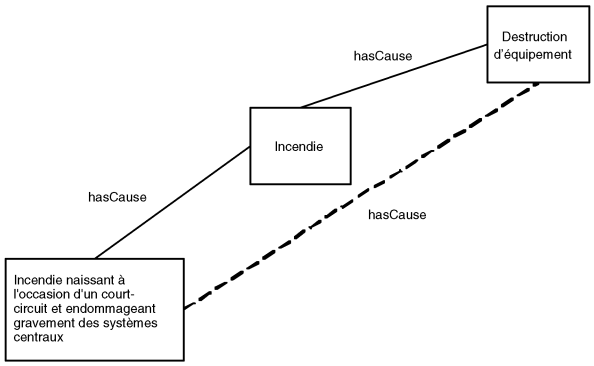

FIG. 3.10 – Un exemple de propriété transitive : hasCause

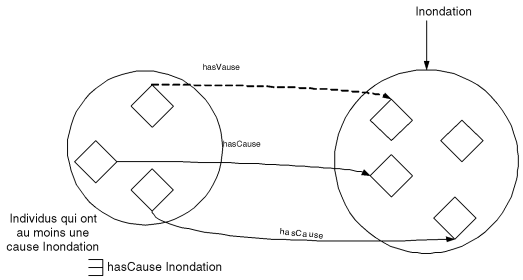

FIG. 3.11 – Restriction " ∃ hasCause Inondation "

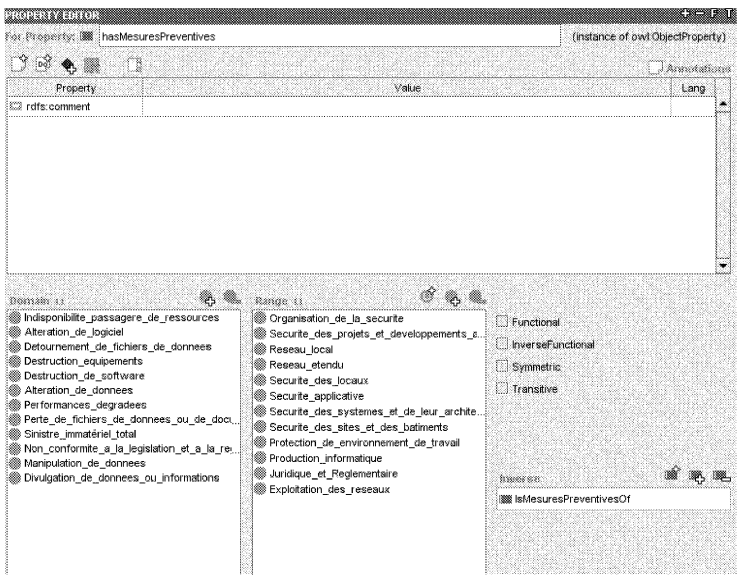

FIG. 3.12 – Propriété "hasMesurepreventive"

classes, on peut les exporter en OWL. La liste des classes de l'ontologie et de leurs propriétés figurent en annexe J.

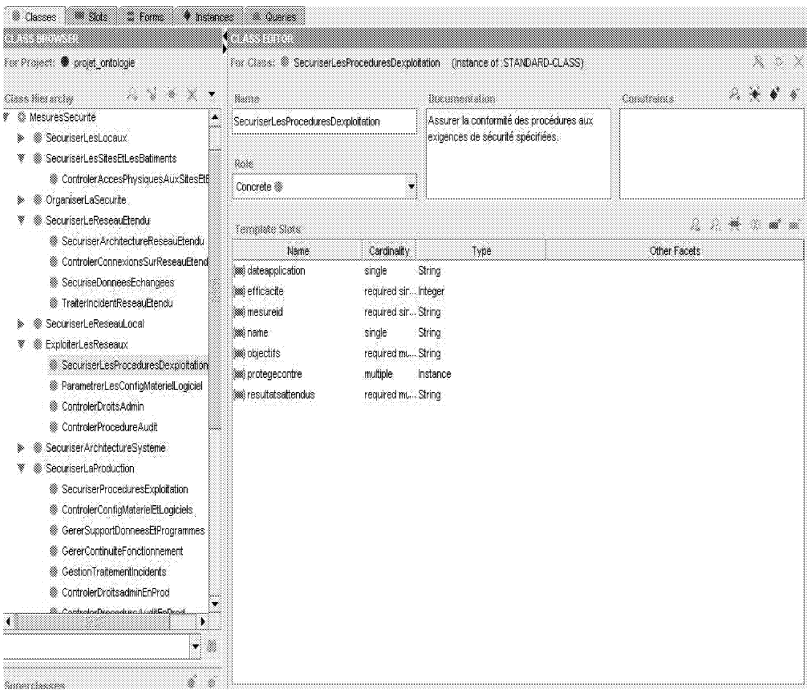

FIG. 3.13 – Extrait de l'ontologie des contre-mesures visualisable avec l'éditeur d'ontologie PROTEGE 2000

Création d'une instance supposons que lors de l'évolution des classes nous voulons créer une classe distincte pour les risques accidentels mais à l'origine intentionnelle. Reprenons l'exemple de l'ontologie des risques, nous devons créer les instances des classes. Définir une instance individuelle d'une classe exige : (1) choisir une classe, (2) créer une instance individuelle de cette classe, (3) la renseigner avec les valeurs des attributs. Par exemple nous avons crée une instance individuelle" accident de nature électrique (court-circuit), mettant hors service un équipement du réseau étendu " est une instance de la classe "accident ou panne mettant hors service une ou plusieurs ressources matérielles" qui à son tour représente tous les risques dus à une Indisponibilité passagère de ressources.

Selon Natalya [Natalya101], décider si un concept particulier est une classe ou une instance individuelle dans une ontologie dépend des applications potentielles de l'ontologie. Autrement dit, le problème est de retrouver les entités les plus spécifiques qui seront représentés dans la base de connaissance. Dans le cadre de notre travail, nous avons fait appel aux questions de compétences définies plus haut, les concepts les plus spécifiques qui constituent les réponses à ces questions sont des candidats pour devenir des individus dans notre base. Les instances individuelles sont les concepts les plus spécifiques représentés dans une base de connais-

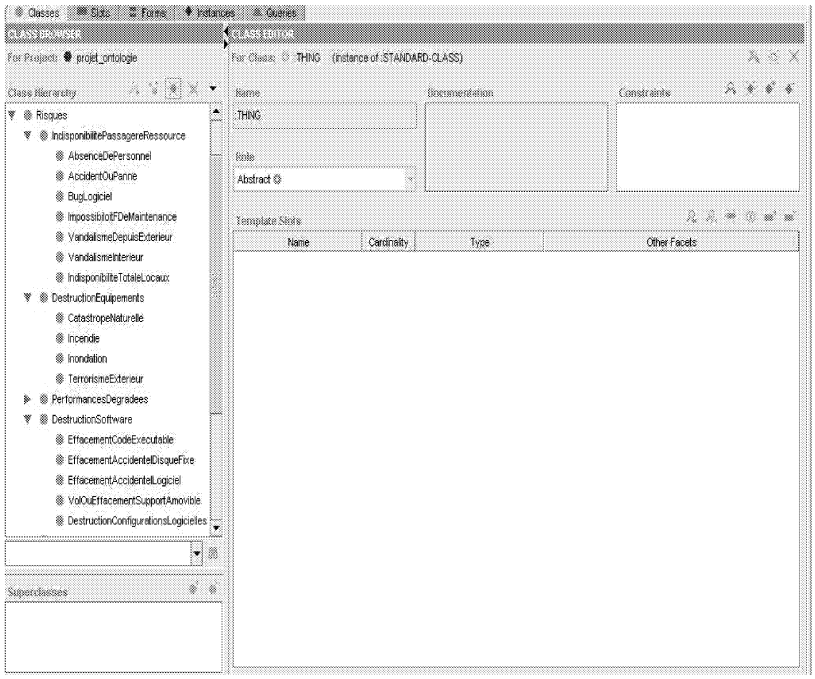

FIG. 3.14 – Extrait de l'ontologie des risques visualisable avec l'éditeur d'ontologie PROTEGE 2000

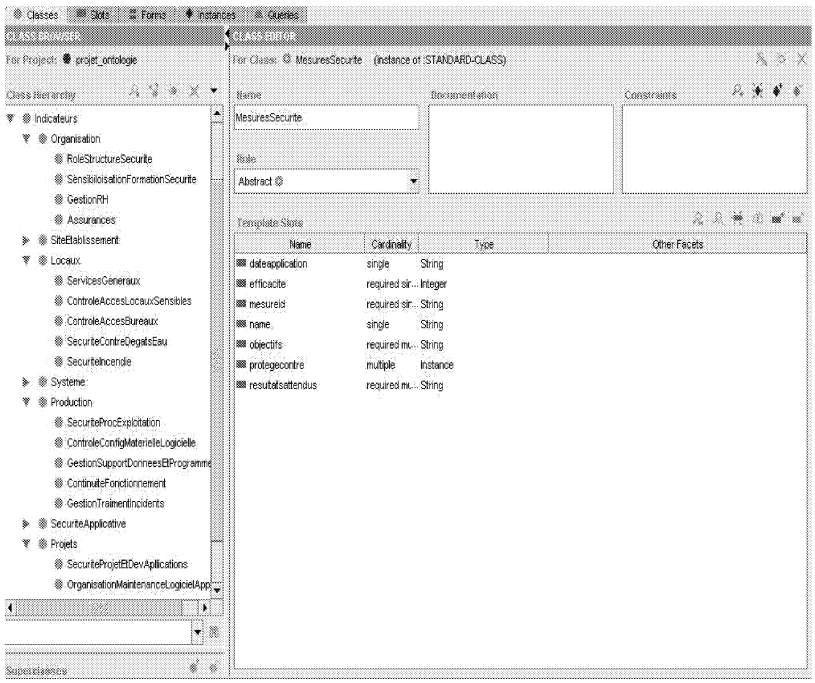

FIG. 3.15 – Extrait de l'ontologie des indicateurs visualisable avec l'éditeur d'ontologie PROTEGE 2000

sance. Il est souvent très difficile de distinguer entre une classe et les instances d'une classe. Protégé nous a permis de spécifier quelques classes comme abstraites, signifiant que la classe ne peut pas avoir d'instances directes. Dans notre cas, toutes les classes représentant les différents types de malveillances sont abstraites. L'agencement des classes dans la hiérarchie nous paraît très logique. La classe *ManipulationDonnees* ou *Détournement Fichier* est bien **une sorte** de Malveillance. La figure 3.18 montre une instance "Accident de nature électrique (court-circuit), mettant hors service un équipement du réseau étendu". Cette instance a pour mesure de récupération "Assurance des dommages matériels" et pour mesure préventive "MIN(03A01 ;03A04)" et pour mesure palliative "MAX(04A01 ;04A07 ;01E02)", en remplaçant les codes des mesures par leurs libellés, nous avons comme mesure préventive "MIN(Qualité de la fourniture de l'énergie ; Qualité du câblage) et pour mesure palliative "MAX(Sûreté de fonctionnement des éléments d'architecture du réseau étendu ; Plan de Reprise d'Activité (PRA) du réseau étendu ; Plans de continuité de l'activité). La fonction MIN signifie que les services appelés en arguments sont complémentaires et que si l'un d'eux est faible, l'ensemble sera faible. La fonction MAX signifie que les services appelés sont alternatifs : Si l'un d'eux est de bonne qualité, l'ensemble le sera. La figure 3.16 nous montre l'instance "Assurer les dommages matériels " de la classe Assurer.

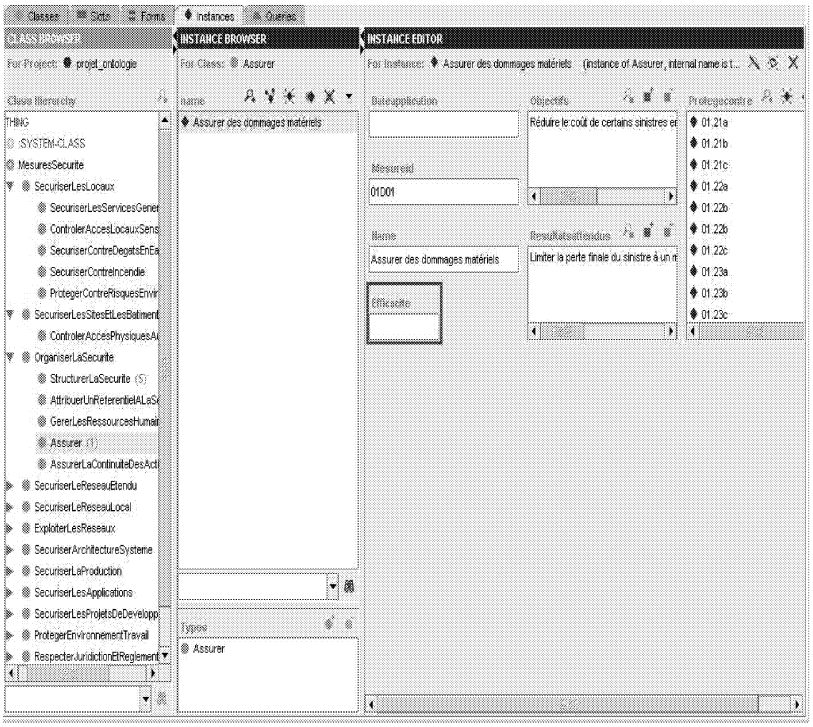

FIG. 3.16 – Extrait de l'intance "Assurer les dommage matériels"

3.3 Fusion des ontologies locales en une ontologie globale

La construction du vocabulaire partagé contient deux étapes principales : 1) l'analyse des ontologies locales ; 2) la sélection de tous les concepts et la résolution des problèmes d'hétérogénéité sémantique. Nous faisons une analyse complète des trois ontologies déjà construites. Cette analyse est facile dans la mesure où la sémantique des concepts a déjà été définie dans les ontologies locales. Après la sélection des concepts, nous avons localisé les problèmes d'hétérogénéité sémantique, dans ce cas précis, nous avons eu moins de problèmes car les ontologies locales ont des concepts très différents. Lorsque nous avons rencontrés des conflits de noms, nous avons utilisé les techniques suivantes pour les traiter :

- homonymes : lorsque nous avons trouvé deux concepts identiques mais sémantiquement différents, nous avons renommé les deux concepts au niveau de l'ontologie globale. Par exemple on peut trouver le concept *Erreur de réalisation* qui représente les erreurs commises lors de la réalisation d'une application métier et un autre concept *Erreur de réalisation* qui représente les erreurs commises lors de la réalisation d'un composant matériel. Nous différencions les deux concepts en les renommant en *ErreurRealisationApplication* et *ErreurRealisationMatériel* et ils peuvent être généralisés par le concept *ErreurRealisation* qui aura comme sous classe ces deux classes.
- synonymes : on peut trouver deux Concepts différents mais sémantiquement identiques. Dans l'ontologie globale on exprime une équivalence entre ces deux concepts. Par exemple *ErreurDeManipulation* dans une source locale a le même sens que *ErreurDeSaisie*. Dans ONTOSEC, un même concept ne peut exister dans plus d'une ontologie locale. Dans le cas ou cela se produirait, On spécialise ce concept dans l'ontologie dans ONTOSEC.

La figure 3.17 nous donne les relations entre les trois ontologies.

3.3.1 Réécriture des requêtes

Nous avons utilisé une architecture hybride, le schéma global et les schémas locaux correspondent respectivement à l'ontologie globale et les ontologies locales. Il existe plusieurs manières d'établir la correspondance entre le schéma global et les schémas des sources de données à intégrer. Nous avons opté pour l'approche **GLAV**. Cette approche fait correspondre à chaque concept ConceptG de l'ontologie globale un concept ConceptL sur l'ontologie locale. Si la requête est exprimée en termes de l'ontologie globale et locale alors on peut obtenir les résultats de cette requête par simple dépliement. On pourra poser des requêtes directement à ONTOSEC et éventuellement aux ontologies locales. ONTOSEC est un ensemble de termes classifiés en une hiérarchie. Elle ne contient pas de propriétés reliant les différents concepts. Ces propriétés existent chacune dans leur ontologie locale. L'utilisateur peut donc créer une requête qui contient des concepts de ONTOSEC et éventuellement des propriétés des ontologies locales. La requête exprimée en termes de concepts et propriétés doit être réécrite de manière à obtenir des résultats qu'on peut agréger. Tout concept qui ne garantit pas la combinaison des données obtenues est exclu. Du point de vue sémantique, cette exclusion tend à rendre une requête cohérente. Une requête cohérente est une requête decomposable en sous requêtes exécutables et dont les résultats est composables. Cette réécriture peut être vue comme une correspondance entre l'ontologie

globale et les ontologies locales, puisqu'elle permet de rendre le traitement de la requête utilisateur direct de l'ontologie globale vers les ontologies locales.

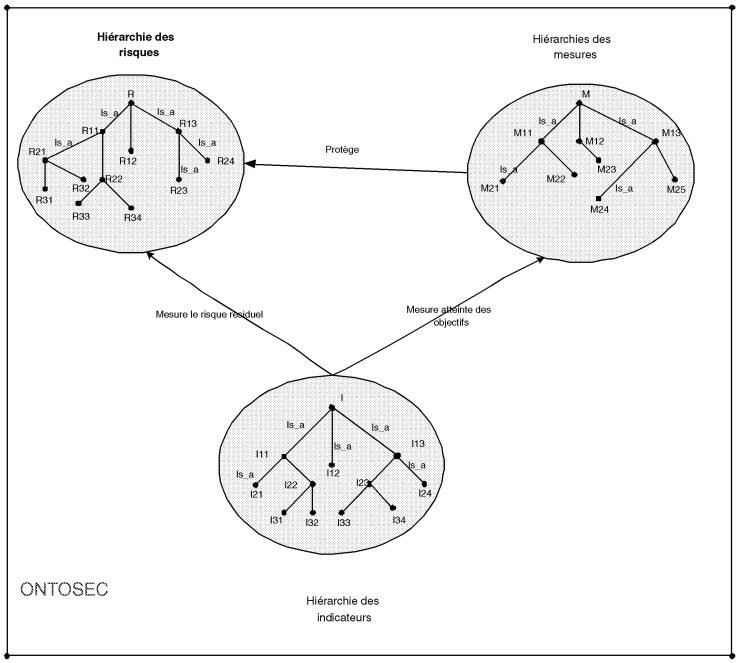

FIG. 3.17 – Composants ontologiques

3.4 Evolution de l'ontologie des ontologies

Le but de cette section est de présenter une démarche d'évolution d'ONTOSEC. Pour y arriver, voici quelques définitions nécessaires.

Rôle d'ONTOSEC : son rôle est de pouvoir mettre à la disposition des utilisateurs et de manière automatique tous les risques auxquels sont soumises les informations, et de proposer un certain nombre de mesures pour couvrir ces risques. Fournir à ces utilisateurs une liste d'indicateurs permettant de mesurer l'atteinte des objectifs prévus dans les mesures.

Changement dans ONTOSEC : un changement exécuté permet de passer d'une version Vn à une version Vn+1. Nous nommons changement, tout changement affectant une ontologie locale.

Consistance d'ONTOSEC : toutes les contraintes concernant le modèle et les axiomes doivent être respectées ; en plus, tout changement dans l'une des ontologies doit se répercuter dans les autres et de manière automatique.

Développeur d'ONTOSEC : tout acteur impliqué dans le processus d'évolution de l'ontologie.

Nous avons conçu le processus d'évolution d'ONTOSEC en sept étapes. Dans cette section nous présentons brièvement ces étapes. Le processus d'évolution d'ONTOSEC a pour but d'accroître la stabilité et la consis-

tance de l'ontologie en contrôlant les changements qui peuvent avoir lieu, soit dans l'environnement du SI, soit dans l'une des ontologies du système. On peut ajouter comme objectifs, le fait d'identifier un changement, de documenter son impact, de s'assurer que les méthodes standards et procédures sont utilisées de manière efficace afin de prendre en considération tous les changements, dans le but de minimiser l'impact d'un changement sur l'ontologie. Les phases du processus d'évolution sont : identification et téléchargement de l'ontologie,

- Evolution de l'ontologie, étape 1 : identification. Il s'agit d'accéder, d'identifier et de télécharger la version d'ONTOSEC à modifier.

- Evolution de l'ontologie, étape 2 : identifier les changements. Il existe deux approches : l'approche ascendante et l'approche descente. Dans l'approche descendante, les développeurs apportent des changements à partir des modifications faites dans le domaine de l'ontologie ou ses sous domaines. Dans l'approche ascendante les développeurs apportent des changements à partir des modifications faites après analyse de l'ontologie elle-même. Il s'agit ici de recueillir toutes les informations relatives au changement. On doit avoir entre autre la catégorie ou la sous catégorie du change, son type, son titre, sa description

- Evolution de l'ontologie, étape 3 : évaluer le changement. L'évaluation du changement est la phase la plus critique du processus d'évolution. Une mauvaise évaluation peut causer du retard dans le processus d'évolution car peut entrainer de réévaluation. Elle a pour objectif de filtrer et de rejeter les changements invalides. Elle donne l'approche à utiliser, ascendante ou descendante. Dans cette phase, on détermine la catégorie du changement. Cette catégorie est déterminée à partir de son risque et de son impact. Le risque est déterminé comme le risque d'échec pendant la phase d'implantation. L'impact est définit comme l'impact du changement sur l'ontologie.

- Evolution de l'ontologie, étape 4 : éditer les changements. Dans cette étape on édite les changements évalués dans la phase précédente. On distingue plusieurs opérations : l'introduction d'un nouveau concept, la suppression d'un nouveau concept, l'ajout ou la suppression d'un ensemble de concepts. L'ajout ou la suppression des attributs à des concepts, l'ajout ou la suppression des propriétés à ces concepts. En ce qui concerne les fonctionnalités pour permettre l'édition des changements, Natalya F. Noy et Deborah L. McGuinness dans [Natalya101] proposent une taxinomie de changements élémentaires spécifiant l'ajout, l'effacement et la modification des entités ontologiques définies à l'aide de protégé 2000. Nous envisageons alors d'adapter cette taxinomie dans le cadre de la sécurité des informations et de développer une taxonomie des changements complexes précisant par exemple le traitement d'un groupe de concepts ou l'ajout ou la suppression des éléments complexes. Pour chaque changement ontologique il est possible de générer différents changements additionnels conduisant chacun à des états finaux différents [Maedche2002]. Par exemple si un concept à l'intérieur est supprimé de la hiérarchie des concepts, ses sous concepts peuvent être soit supprimés, soit rattachés au concept parent, soit rattaché au concept racine de la hiérarchie.

- Evolution de l'ontologie, étape 5 : approbation. Cette étape permet de savoir si le changement sera développé et implémenté. Le but est de s'assurer que tous les changements sont revus et approuvés avec évaluation. Son but est de mettre à jour l'ontologie avec les informations juste liées au changement. Si cette validation n'est pas possible en raison du caractère distribué de l'environnement d'occurrence du processus d'évolution, alors des mécanismes de gestion des conflits doivent être prévus Pinto [Pinto2004]

- Evolution de l'ontologie, étape 6 : implanter le changement. Cette étape vise l'implantation des changements avec une sauvegarde de la trace de toutes les opérations faites. Au besoin, il y'a toujours possibilité de retourner à la version précédente. Elle ne fait pas vraiment partie intégrante du processus d'évolution

- Evolution de l'ontologie, étape 7 : validation de la nouvelle version. Les développeurs approuvent ou désapprouvent collectivement la nouvelle version de l'ontologie avant de la rendre opérationnelle.

3.4.1 Evolution de la hiérarchie de classes

3.4.1.1 Introduction d'une nouvelle classe

L'introduction d'une nouvelle classe est l'une des décisions les plus difficiles à prendre lors de la modélisation : quand faut-il introduire une nouvelle classe ?, ou bien quand faut-il représenter une distinction par des valeurs différentes de propriété ? Il est aussi difficile de naviguer dans une hiérarchie comportant plusieurs niveaux d'emboîtements de classes superflues que dans une hiérarchie très plate avec un nombre réduit de classes et comportant trop d'informations codées dans les attributs. Trouver le juste milieu comme dans notre cas n'est pas chose facile. Comme définit dans [Natalya101], les principes de base permettant de décider à quel moment il faut introduire une nouvelle classe dans la hiérarchie : les sous-classes d'une classe (1) possèdent habituellement des propriétés complémentaires que ne possède pas la superclasse, ou (2) des restrictions différentes de celles de la superclasse, ou (3) entretiennent des relations différentes de celles que les superclasses peuvent entretenir.

Dans l'exemple de l'ontologie des risques, la classe *EffacementSupportFixe* peut avoir des auteurs différents alors que cette propriété n'est pas utilisée pour décrire les risques en général. En d'autre termes, nous introduisons une nouvelle classe dans la hiérarchie, seulement quand il y'a quelque chose à dire de cette classe qu'on ne peut pas dire de sa superclasse. Concrètement, chaque sous-classe doit : soit avoir de nouveaux attributs rattachés, soit de nouvelles valeurs d'attributs définies, soit outrepasser certaines facettes concernant les attributs hérités.

Lors de la modélisation de notre domaine, nous devons souvent décider si la modélisation d'une distinction spécifique (comme *ErreursManipulationDonnees, ErreursSaisieDonnees, ErreursTransmissionDonnees* etc.), en tant que valeur de propriété ou en tant qu'ensemble de classes, dépend de nouveau des contours du domaine

et de la tâche fixée. On peut se poser la question de savoir si nous devons créer une classe *ErreursManipulationDonnées, ErreursSaisieDonnées, ErreursTransmissionsDonnées* ou tout simplement une classe *Erreurs* et renseigner les différentes valeurs de l'attribut mode (manipulation, transmission, saisie). La réponse est non. Dans notre ontologie des risques, le concept mode d'erreur a une importance capitale. Nous avons introduit ces classes distinctes parce que le concept mode a une implication particulière pour les relations d'un risque avec d'autres objets. De la même façon, le mode d'erreur est important pour une base de connaissances sur les risques et qui peut être employée pour déterminer un ordre d'éléments à respecter dans une procédure de prise de décision, quant aux mesures préventives ou curatives à prendre pour les gérer. C'est l'une des raisons qui nous ont permis de créer des classes distinctes. Ceci peut aussi se justifier par cette phrase Natalya [Natalya101] : si des concepts ayant des valeurs distinctes d'attributs deviennent des restrictions pour des attributs distincts dans d'autres classes, alors nous devons créer une nouvelle classe pour représenter la distinction. Sinon, il faut représenter la distinction dans une valeur d'attribut.

De même, notre ontologie a des classes sur les risques et des classes telles que *ErreursRealisationLogiciels, ErreursRealisationProcedure* plutôt qu'une classe unique pour toutes les erreurs de réalisation : *ErreursRealisationLogiciel, ErreursRealisationProcedure* sont des erreurs réellement différentes. Cette distinction vaut la peine, dans la mesure où notre ontologie de risques est détaillée. Natalya [Natalya101] illustre assez bien ces propos en ces termes :

> "Si une distinction est importante dans le domaine et que nous traitons les objets ayant des valeurs différentes pour cette distinction comme des objets de types différents, alors nous devons créer une nouvelle classe pour la distinction".

Imaginons maintenant que, consécutivement à de récents vols de biens personnels ainsi qu'à la découverte d'informations confidentielles non protégées, dans les bureaux, nous devions mettre en place une nouvelle classe de risques *VolPetitsMateriels* et la mesure associée appelée *Clean Desk*. Un Clean Desk est un bureau où les objets de valeur et les documents classifiés sont gardés dans une armoire ou un tiroir verrouillé. Cela s'applique aux dictaphones, téléphones mobiles, agendas électroniques, ainsi qu'aux PC portables etc., qui en fin de chaque journée, doivent être retirés de la station de base et rangés sous clé. Durant les heures de travail, quand un bureau est laissé déverrouillé et inoccupé pour une période prolongée, les documents sensibles et les objets de valeur doivent être mis sous clé. Les clés des meubles ne doivent pas être déposées dans un endroit non verrouillé de la même pièce. Les écrans de PC doivent être verrouillés si l'utilisateur s'absente du bureau pour plus de cinq minutes (Presser : "Ctrl+Alt+Delete + Lock Computer"). Afin de s'assurer que la mesure "Clean Desk" soit bien observée, des contrôles des bureaux doivent être entrepris. Tout objet ayant une valeur significative (PC portable, téléphone mobile, etc.) et/ou les documents classifiés, seront pris en charge et déposés dans un endroit sûr. Une feuille explicative, est déposée sur le bureau afin d'en informer l'utilisateur.

3.4.1.2 Suppression d'une classe

Pendant le pilotage de la stratégie, on peut décider qu'un risque ne présente plus un danger sévère pour l'entreprise. Nous ne pouvons le laisser en l'état et continuer à tenir compte lors de notre stratégie ; il faut donc

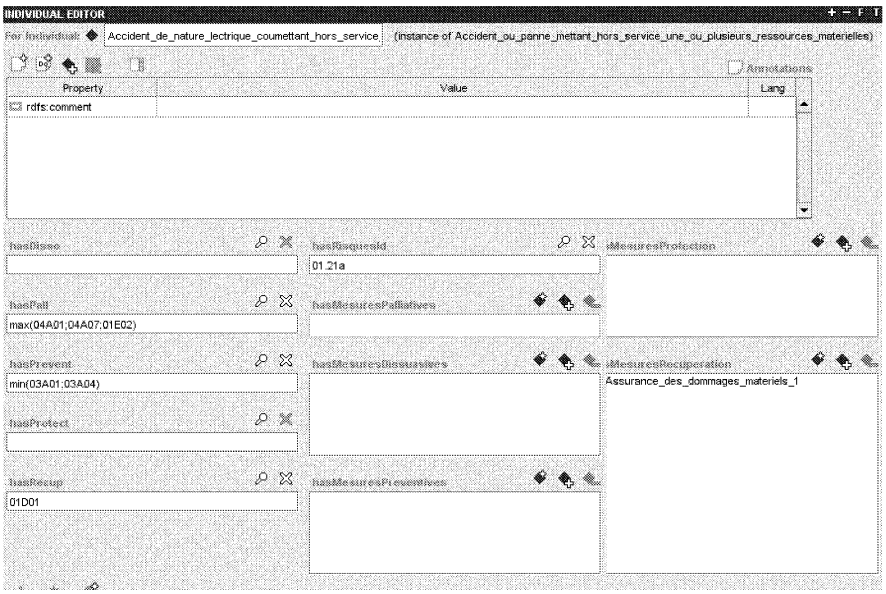

FIG. 3.18 – L'instance Accident de nature électrique, mettant hors service un équipement. du réseau étendu

mettre le système à jour. Nous envisageons ici deux stratégies permettant de supprimer des risques.

- Stratégie 1 : consiste à supprimer seulement le risque
- Stratégie 2 : consiste à supprimer le risque et ses descendants s'ils ne sont pas descendants d'un risque qui n'est pas ascendants du risque à supprimer

Par exemple, si nous décidons de supprimer le risque$R3$, de la hiérarchie de la figure 3.19a, en appliquant la stratégie 1 nous obtenons la hiérarchie de la figure 3.19b, mais par contre si nous appliquons la stratégie 2 nous obtenons la hiérarchie de figure 3.19c.

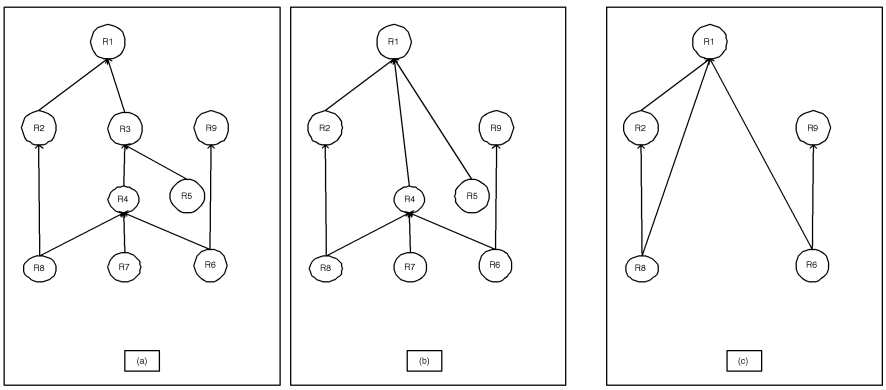

FIG. 3.19 – Résultat de la hiérarchie après suppression de risques

3.4.1.3 Suppression d'une hiérarchie de classes

Une hiérarchie est vue comme un ensemble de risques : supprimer une hiérarchie peut être vu comme la suppression d'un ensemble de risques. Si la stratégie choisie est la stratégie 1 alors rien que les risques de la hiérarchie à supprimer seront supprimés. Quoique, le système supprimera chaque descendant de chaque risque de la hiérarchie qui n'est descendant d'aucun risque qui n'est pas ascendant d'un risque à supprimer. Par exemple : supposons qu'on veuille supprimer de la hiérarchie de la figure 3.19 a, la sous hiérarchie composée de $R1$, $R2$, $R3$. Si nous choisissons la stratégie 1 alots le résultat est celui de la figure 3.20a, par contre si nous choisissons la stratégie 2 alors le résultat est celui de la figure 3.20b. La figure 3.21 résume les étapes

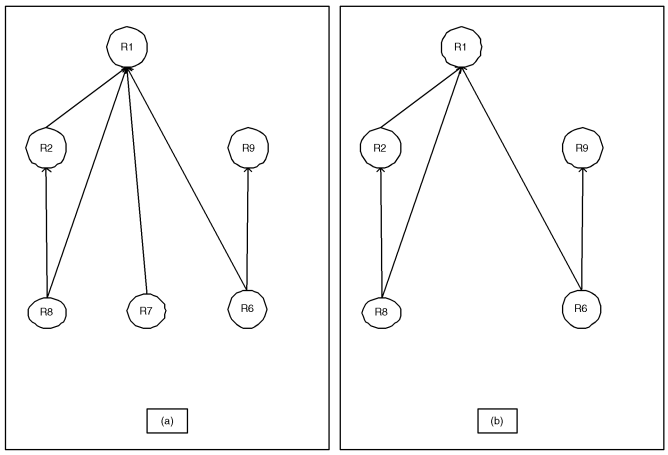

FIG. 3.20 – Suppression d'une hiérarchie selon la stratégie choisie

d'évolution des ontologies.

3.5 Développement du tableau de bord dynamique de la sécurité

Dans cette section nous nous decrivons le prototype developpé. il a été developpé sur le domaine de la sécurité applicative, mais peut très bien se generalisé sur l'ensemble des domaines presents dans ONTOSEC. La figure 3.22 présente le positionnement du TBDS par rapport à ONTOSEC. A partir d'un indicateur, on peut savoir les mesure et les risques qui sont en jeu. A partir des mesures ou des vulnérabilités, on peut connaitre les risques associés. Les informations sont liés au niveau de l'ontologie global, d'ou le mot dynamisme. Nous y reviendrons dans les sections suivantes.

3.5.1 Carte stratégique

La carte stratégique est la représentation graphique de l'interaction entre les objets de nos trois domaines, et schématise le furur tableau de bord dynamique. A l'initialisation du TBDS, on crée la carte stratégique à l'image de ce qu'est la stratégie de sécurité à ce moment précis. En cas d'évolution de la stratégie ou lors de la

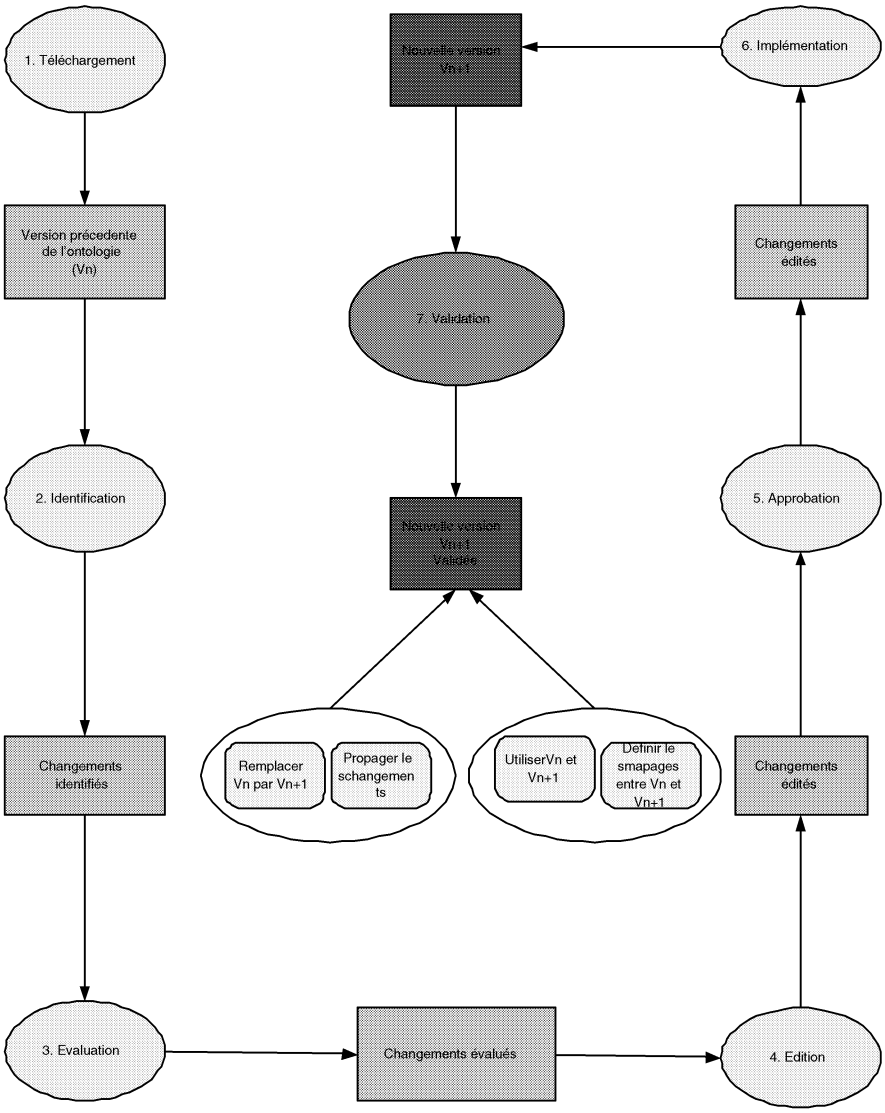

FIG. 3.21 – Etapes d'évolution de l'ontologie

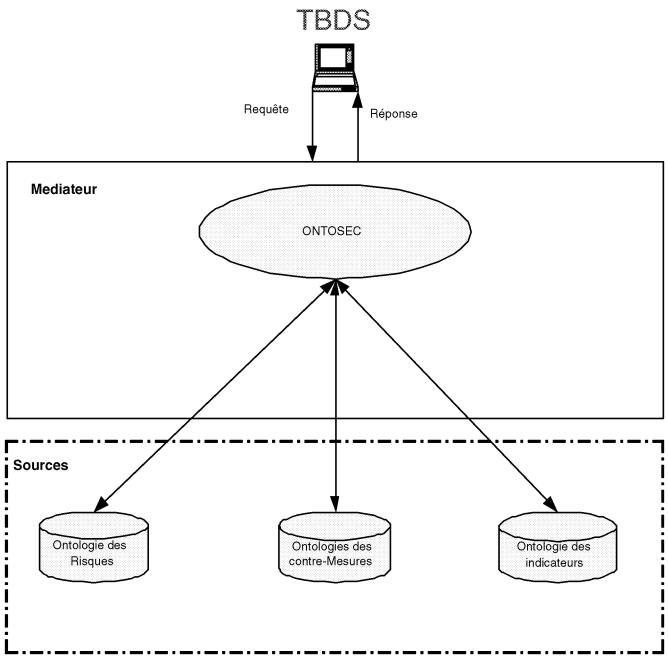

FIG. 3.22 – Tableau de bord dynamique

prise en compte d'un nouveau élément non prévu initialement, c'est le TBDS et sa carte stratégique qui servent de référence. Contrairement à la démarche BSC calsssique, elle est divisée en 3 niveaux qui sont ici :

- le niveau des risques ;
- le niveau Profil de Sécurité de l'information ;
- le niveau processus internes ;

Elle peut se representer de la manière suivante :

Couverture des risques métiers	opérationnels, fonctionnels, stratégiques...
Profil de Sécurité de l'information	contre-mesures, disponibilité, intégrité, confidentialité, objectifs
Indicateurs	indicateur d'objectif, indicateurs de performance

Le niveau des risques

Ce niveau représente les exigences de l'entreprise en termes de maîtrise des risques métiers. Il est en général renseigné à partir d'une analyse de risques préalablement menée. Il transcrit les préoccupations qui sont celles de la direction en termes de risques à maîtriser. Comme le montre la figure 3.23. Une menace exploite une vulnérabilité pour causer un risque. L'impact d'un risque est l'évaluation des conséquences de l'occurrence de ce risque, indépendamment de toute mesure de sécurité. Pour chaque risque, il existe une cible pour ce risque, c'est-à-dire une ressource impliquée ou détériorée. Il peut s'agir d'un type de données ou d'informations dérobées, d'un type de ressource rendues indisponibles, ou d'un type de ressources altérées, selon qu'il s'agisse d'un risque mettant en cause la confidentialité, la disponibilité ou l'intégrité de la ressource. Du côté

des "actifs business", on retrouve les informations fonctionnelles, alors que du côté ses "actifs systèmes", on retrouve les éléments techniques tels les matériels, les logiciels et les réseaux, mais aussi l'environnement du système informatique, comme les utilisateurs ou les bâtiments.

Les mesures servent à réduire les risques. Une mesure peut être dissuasive, protectrice, préventive ou palliative. Pour chaque risque et pour chaque type de mesure, on définit un indicateur d'efficacité. Ces indicateurs sont calculés par le biais de formules faisant référence à des services de sécurité. Les processus sont les suites d'actions de sécurité menées dans le but d'atteindre les objectifs. La mesure de l'atteinte de ces objectifs ou de l'efficacité des mesures prises est faite par les indicateurs d'objectifs et les indicateurs de performances.

Le niveau Profil de Sécurité de l'information

Le profile de sécurité de l'information définit les caractéristiques auxquelles l'information doit se conformer pour répondre aux exigences fixées par les métiers de l'entreprise pour la couverture des risques. Il traduit les objectifs fixés en termes de couverture des risques en exigences sur le SI et lie ainsi les attributs des risques avec les contre-mesures. Il est exprimé sous la forme de caractéristiques de l'information : disponibilité, intégrité, confidentialité. Ces caractéristiques doivent être garanties par les contre-mesures. Il représente le lien entre les objectifs de couvertures de risques et les actions mises en place pour couvrir les risques.

Le niveau Processus interne

Ici sont pris en compte les processus de l'entreprise mis en œuvre en vue d'atteindre les objectifs prévus dans le profile de sécurité. Pour mesurer l'atteinte des objectifs, on aura un indicateur d'objectif (IO). Prenons un exemple simple, la lutte anti-virale, le processus a pour but d'éviter la contamination du SI par les virus. Il a un impact direct sur les caractéristiques disponibilité (D), et intégrité (I) du PSI. Son résultat est mesuré par un IO qui est, par exemple, le taux de machines infectées. Ici les facteurs de succès sont les actions à mener pour atteindre les objectifs, ils sont mesurée par les indicateurs de performanc (IP).

3.5.1.1 Liens de causes à effets

La carte stratégique intègre les liens de causes à effets entre les différents indicateurs et entre les différents niveaux. Prenons un autre exemple de lutte contre le vol de petits matériels. Lorsque les objectifs sont atteints sur les IP de contrôle réguliers des bureaux, ou de la mise en place d'un système anti-vol, que seront obtenus de bon résultats sur les processus mesurés par l'IO : taux de vols. L'impact sera positif sur la disponibilité du matériel du profile de sécurité. Ces liens de causes à effets assurent la cohérence et l'articulation des différents éléments de la carte stratégique et donc du TBDS.

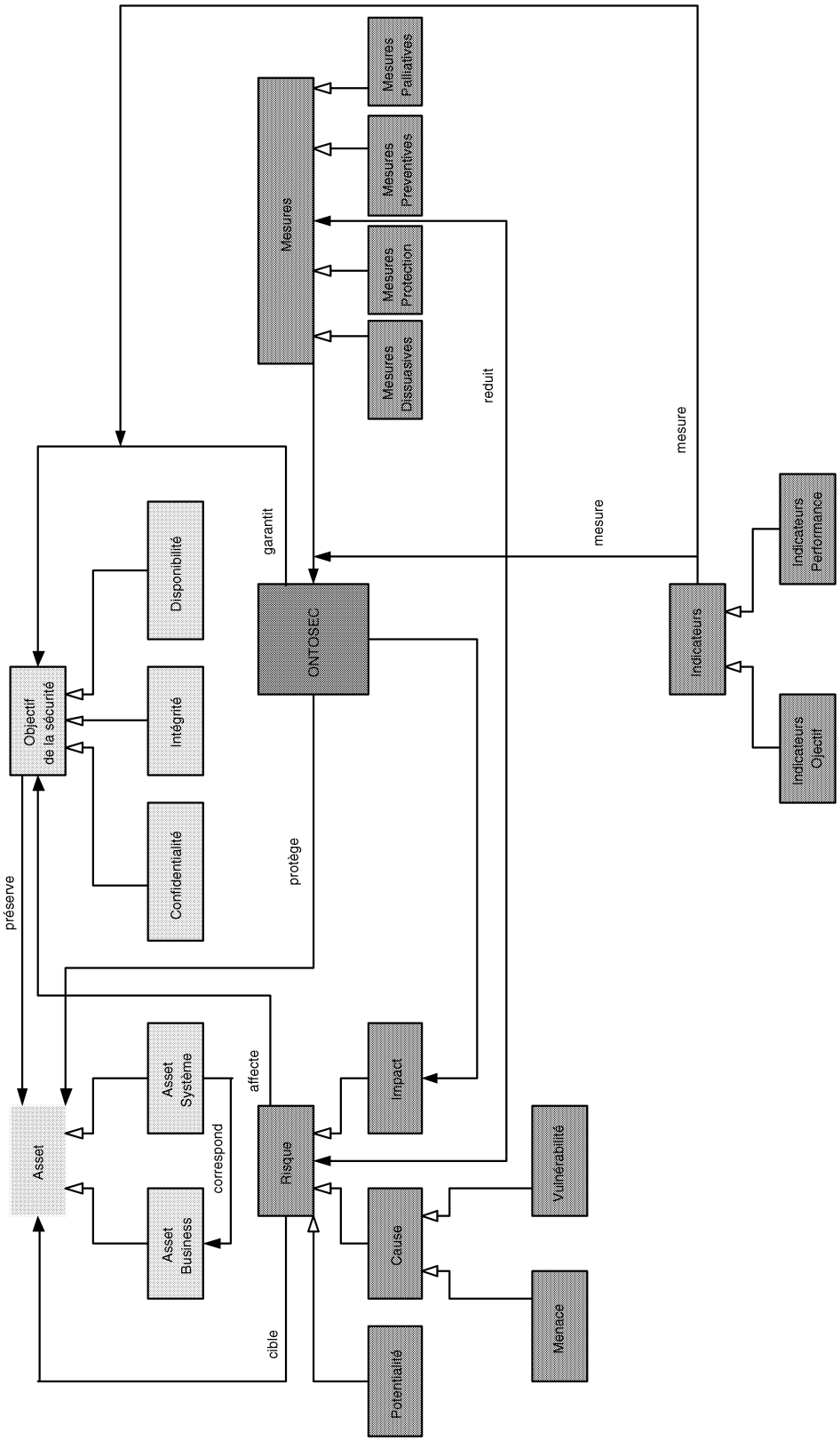

FIG. 3.23 – Carte stratégique

3.5.2 Schéma conceptuel

Cette partie est une traduction en UML de la carte stratégique. La figure 3.24 montre une vue du schéma conceptuel du TBDS. Nous avons trois principales classes : *Risques, Mesures, Indicateurs*. Les classes secondaires : *Menaces, Vulnérabilités, AssetBusiness, AssetSystèmes, Assets, Mesurespreventives, Mesurespalliatives, MesuresRecuperation, MesureDissuasives, MesureProtection*. Nous donnons ci-dessous plus de détails sur les classes principales.

3.5.2.1 Liste des indicateurs retenus

Ils mesurent l'atteinte des objectifs fixés dans les mesures. Ici nous avons considérer juste une partie de nos indicateurs. Nous avons défini deux types d'indicateurs : les indicateurs d'objectifs (IO) et les indicateurs de performance (IP). Un IO mesure le niveau atteint par les contre-mesures dans l'atteinte de leurs objectifs. Un IP mesure les facteurs de performance. Nous nous sommes limités à un domaine, celui de la sécurité applicative. Il peut facilement être appliqué aux autres domaines. Les six indicateurs de niveau 2 sont des indicateurs opérationnels qui servent au pilotage de la sécurité au quotidien. Les trois indicateurs de niveau 1 sont les indicateurs fonctionnels qui servent à mesurer l'avancement de la sécurité par domaine ou par axe (confidentialité des données, intégrité des données, etc...). Les indicateurs de niveau 0 sont les indicateurs stratégiques pour un reporting vers la DSI ou la direction générale. Ils permettent de mesurer l'état d'avancement de la politique de sécurité ou l'évolution des incidents liés à la SSI. Nous avons donc un total de 10 indicateurs comme le montre la figure 3.25.

- Indicateurs stratégiques : sécurité applicative. Il permet de renseigner sur l'utilisation des applications, l'intégrité des données utilisées et la confidentialité de ces données.
- Indicateurs fonctionnels :
    1. contrôle accès applicatifs : permet de renseigner sur l'utilisation des applications
    2. contrôle intégrité des données : permet de mesurer la qualité de l'intégrité des données confiées au SI
    3. contrôle confidentialité des données : permet de mesurer la qualité de la confidentialité et leur risque de perte
- Indicareurs opérationnels :
    1. authentification des accédants : mesure le nombre de personnes accédants avec succès ou non au système
    2. profils accès données applicatives : contrôle et gère les profils d'accès aux données
    3. contrôle de saisie de données : mesure le taux d'erreur lors de la saisie des sonnées
    4. intégrité des données échangées : contrôle le pourcentage de données échangées
    5. accusé de réception : contrôle le pourcentage de message avec accusé de réception
    6. signature électronique : contrôle le pourcentage de signature électronique

Les indicateurs ci-dessus sont en majorité des IO. Pour simplifier la lecture du document, ces mesurent possèdent des noms très similaires aux indicateurs. Toute mesure permet de couvrir un ou plusieurs risques. C'est une réponse à un besoin de sécurité, généralement en référence à certains types de menaces. Une mesure peut être constituée de plusieurs autres mesures pour répondre à un besoin déterminé. Une menace est la cause d'un risque. Chaque risque a un impact, une potentialité et une exposition standard. L' impact intrinsèque est l'évaluation des conséquences de l'occurrence du risque, indépendamment de toute mesure de sécurité. L'impact se déduit donc de l'impact intrinsèque par la formule :

I= MIN (IMPACT INTRINSEQUE, 5- STATUS RI),

où les STATUS - RI sont les facteurs de réduction de risques. Ce qui signifie que les facteurs de réduction de risques ont un effet de plafonnement sur l'impact. Pour chaque risque, il existe une cible, c'est-à-dire une ressource impliquée ou détériorée. Il peut s'agir d'un type de données ou d'informations dérobées, d'un type de ressources rendues indisponibles ou d'un type de ressources altérées, selon qu'il s'agit d'un risque mettant en cause la confidentialité, la disponibilité, l'intégrité ou la traçabilité d'une ressource. La gravité du risque, qui sera une valeur calculée, se déduira en fonction de la potentialité et de l'impact, comme le montre le tableau ci-dessous. Les mesures nécessaires pour couvrir un risque peuvent être dissuasive, préventive, protectrice ou récupératrice.
.

3.5.2.2 Fréquence de collecte

La fréquence de collecte des données est variable, elle est fonction des données présentes dans ONTOSEC. Elle se fait de manière instantanée par simple requête sur ONTOSEC. Le système accède à ONTOSEC et collecte les informations qui se trouvent dans l'ontologie des indicateurs. Si la requête est faite pour un indicateur quelconque, le système cherche à travers l'ontologie globale, l'indicateur de même nom dans l'ontologie des indicateurs. Les informations contenues dans l'ontologie peuvent être chargées en temps réel, tout dépend de l'outil utilisé dans l'entreprise, pour la collecte et le chargement de l'information.

3.5.2.3 Méthode de calcul

La méthode de calcul est simple, Il dépend directement du niveau de l'indicateur dans la hiérarchie. Un indicateur opérationnel est fonction de l'efficacité de la mesure associée et de la gravité du risque couvert. Un indicateur fonctionnel est fonction des indicateurs opérationnels qui le composent. Il prend la tendance de la majorité de ses indicateurs opérationnels. Cela veut tout simplement dire qu'en dehors du fait qu'il puisse gérer les menaces existantes, aussi les menaces potentielles. Il peut être au rouge pas parce que l'objectif n'est pas atteint mais parce que les indicateurs opérationnels qui le composent sont déjà au rouge. Il existe donc une approche proactive dans la gestion des risques. Les indicateurs stratégiques se calculent avec le même principe que les indicateurs opérationnels, en se basant sur les indicateurs de niveau directement supérieur. Nous avons

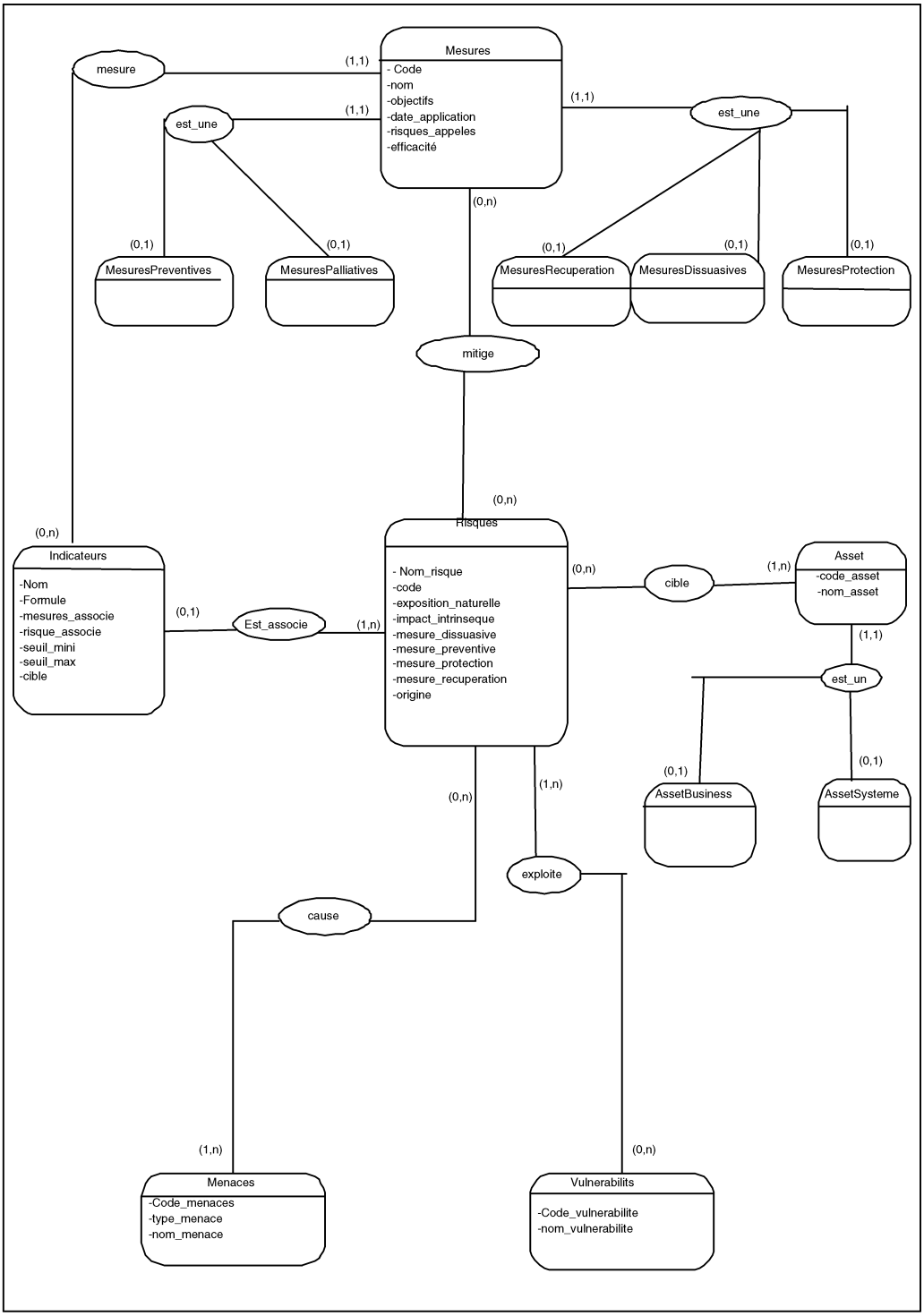

FIG. 3.24 – Modélisation TBDS

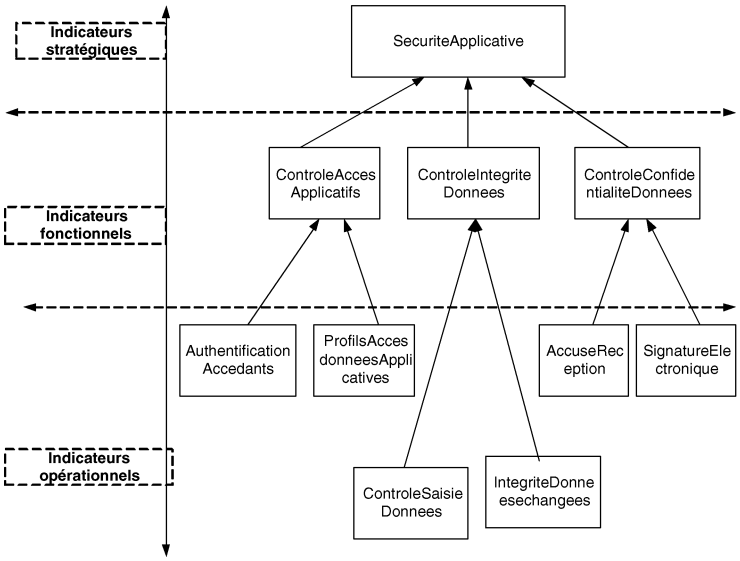

FIG. 3.25 – hiérarchie des indicateurs du TBDS

choisi de représenter ces indicateurs sous forme de graphique de bâtons, mais toute autre représentation est possible. Quant aux IP, ils se calculent sur la base d'une formule précise. Pour un IO opérationnel, une valeur de 3 montre que l'objectif est atteint, une valeur de 2 montre que l'objectif n'est pas atteint mais est en voie, une valeur de 1 montre que l'objectif est loin d'être atteint. Le code source du programme se trouve en "annexe H".

Grille de calcul d'un indicateur d'objectif opérationnel				
Efficacité de la mesure Gravité du risque	1	2	3	4
1	3	3	3	3
2	2	3	3	3
3	1	2	3	3
4	1	1	2	3

3.5.3 Un système dynamique

Nous avons dans ce travail beaucoup parlé du dynamisme. Il est important de préciser en quelques mots les raisons qui nous ont permis de parler de tableau de bord dynamique.

3.5.3.1 Evaluateur dynamique des attributs des risques

Le TBDS est un système qui évalue de manière dynamique l'efficacité et la robustesse des contre-mesures en fonction des attributs sur les risques. Si ces attributs changent, les modifications sont directement chargées dans ONTOSEC de manière instantanée. Les données sont directement mises à jour dans l'ontologie des

contre-mesures et celui des indicateurs. Pour toute nouvelle attaque, le système va dynamiquement adapter la politique de sécurité en utilisant les techniques d'ajout de nouvelles classes. De même si un risque devient insignifiant pour l'organisme, le système utilise les techniques de suppression de nouvelle classe pour mettre à jour la hiérarchie des classes. Ces deux modifications mettent à jour de manière dynamique la politique de sécurité.

3.5.3.2 Générateur dynamique des contre-mesures de sécurité

Le système propose une classification et une taxonomie des contre-mesures de sécurité de l'organisme. Cette taxonomie est liée de manière directe à une taxonomie des risques. Le système implémente les contre-mesures de sécurité en accord avec la norme ISO /IEC 17799 : 2005 et la méthode MEHARI. La politique de sécurité est donc mise à jour de manière dynamique. Pour toute mesure non incluse dans la norme ISO /IEC 17799 : 2005 et la méthode MEHARI, le système se réfèrent aux bonnes pratiques de quelques entreprises.

3.5.3.3 Générateur dynamique des indicateurs de sécurité

Le système propose de manière dynamique des indicateurs de sécurité. Ces indicateurs proviennent de l'ontologie des indicateurs et sont directement liés aux contre-mesures et aux risques associés. On distingue plusieurs types d'indicateurs. Les indicateurs opérationnels, les indicateurs fonctionnels et les indicateurs stratégiques. Les indicateurs peuvent être générés à tous les niveaux. Les indicateurs fonctionnels sont déduits dynamiquement des indicateurs opérationnels. Les indicateurs stratégiques sont déduits dynamiquement des indicateurs fonctionnels. Dans la section sur l'évolution d'ONTOSEC, nous avons démontré la transitivité des relations hiérarchiques. Nous pouvons donc déduire que les indicateurs stratégiques peuvent se déduire dynamiquement des indicateurs opérationnels. Tout ensemble d'indicateurs générés par le système constitue un tableau de bord.

3.6 Résumé

Nous pouvons résumer ce chapitre par trois étapes de construction. Nous avons construits de trois arbres hiérarchiques différents, celui des risques, des mesures et des indicateurs. Les concepts de ces trois arbres sont reliés par des relations bien précises, permettant ainsi à notre ontologie d'être vue comme un ensemble cohérent de concepts. Nous avons abordé les propriétés complexes de définition d'une hiérarchie de classes, des propriétés de classes et des instances. Toutefois, malgré toute la démarche suivi comme stipulé dans [Noy2001], il est important de retenir qu'il n'y a pas qu'une seule ontologie correcte de référence pour un domaine précis ; la conception d'une ontologie étant un domaine créatif il ne peut y avoir d'ontologies identiques faites par des personnes différentes.

Dans notre démarche, nous avons essayé au maximum de ressortir l'information nécessaire pour les applications pouvant utiliser ONTOSEC. Très souvent l'ontologie ne doit pas contenir toute l'information possible dans le domaine. On ne doit pas spécialiser (ou généraliser) plus que de besoin pour notre application. De

façon similaire Natalya F. Noy et Deborah L dans [Noy2001] relèvent que l'ontologie ne doit pas contenir toutes les propriétés possibles des classes et toutes les distinctions entre les classes dans la hiérarchie. Chaque ontologie est une arborescence correspondant aux schémas UML décrivant l'organisation des objets entre eux. Chaque risque a deux attributs principaux, son impact et sa potentialité. La potentialité du risque, représente en quelque sorte sa probabilité d'occurrence. Cette occurrence n'est pas modélisable en termes de probabilité. Elle est fonction du contexte et des mesures de sécurité mises en place. L'impact du risque sur l'entreprise, représente la gravité des conséquences directes et indirectes qui découleraient de l'occurrence du risqué. Chaque risque est relié à une ou plusieurs mesures de sécurité par une relation du type « estCouvert », ces mesures peuvent être dissuasives, préventives, protection, récupération.

Quant aux mesures de sécurité, chacune a deux principaux attributs : l'efficacité et la robustesse. L'efficacité mesure la capacité à assurer effectivement la fonction demandée face à des acteurs ayant des compétences plus ou moins fortes ou des circonstances plus ou moins courantes. Par exemple l'efficacité d'une mesure contrôlant des actions humaines est ainsi la mesure des compétences nécessaires pour qu'un acteur puisse passer au travers des contrôles mis en place. La robustesse de la mesure est sa capacité à résister à une action visant à la court-circuiter ou à l'inhiber. La robustesse ne concerne que les mesures dites techniques.

Le TBS quant à lui est un ensemble d'indicateurs issus de l'ontologie des indicateurs. Son but est de suivre la qualité des services de sécurité, de suivre la politique de sécurité, de remonter les alertes afin de prévenir les dysfonctionnements. On distingue les indicateurs stratégiques, les indicateurs fonctionnels et les indicateurs opérationnels. Plusieurs indicateurs stratégiques peuvent alimenter un indicateur stratégique. Un indicateur stratégique peut être indépendant. Plusieurs indicateurs fonctionnels peuvent alimenter un indicateur stratégique. Plusieurs indicateurs fonctionnels peuvent alimenter un indicateur fonctionnel. Un indicateur fonctionnel peut être indépendant. Plusieurs indicateurs opérationnels peuvent alimenter un indicateur opérationnel. Plusieurs indicateurs opérationnels peuvent alimenter un indicateur fonctionnel. Un indicateur opérationnel peut être indépendant. L'ensemble des classes de l'ontologie peuvent être exportées sous différents formats : OWL, CLIPS, RDF, HTML. En annexe I nous avons l'ensemble des classes de l'ontologie en OWL.

Chapitre 4

Validation

De nos jours, il existe une vaste palette d'approches pour la construction des TB sécurité. La plupart de ces approches décrivent la construction d'un TB à partir de la politique de sécurité et des règles qui y sont définies. D'autres approches décrivent la construction d'un TB en s'inspirant des méthodes ou des normes de sécurité existantes. Nous avions développé dans le chapitre précédent un TBDS sur le sous domaine de la sécurité applicative. Dans ce chapitre, nous allons appliquer cette démarche sur un cas concret simple d'une entreprise de distribution d'accès internet par satellite. Les solutions présentées ici ne sont pas exhaustives, mais ont pour but de donner un aperçu de ce nouvel outil d'aide à la décision dans la sécurité des SI.

4.1 Présentation de l'entreprise

Le dossier de présentation donne les informations relatives à l'entreprise TELKOM SA. Ces informations ont été rassemblées suite à un entretien avec les responsables de l'entreprise. TELKOM est une société de vente du matériel de télécommunication et fournisseur d'accès internet par satellite basée à Vevey et comprenant 12 collaborateurs avec plus d'un de chiffre d'affaire.

4.1.1 Prestations fournies

4.1.1.1 Accès Internet par RTC

Très connu par le public, l'accès Internet par RTC permet aux clients TELKOM de se connecter de n'importe quel endroit en utilisant leur ligne téléphonique. Le débit théorique est de 56kbps mais en pratique la moyenne obtenue est de 33600bps. Il permet aussi aux clients possédant des passerelles VoIP dial-up (exemple SPEEDIP) de passer des appels IP ou internationaux moins chers.

4.1.1.2 Accès Internet par GSM

Pas très différent de l'accès internet par RTC, il permet aux clients de TELKOM d'accéder à internet en connectant leur PC sur leur téléphone portable. Le débit maximum est de 9600bps. Le client paie le prix d'une

communication téléphonique normale en plus du forfait de connexion. Cette solution est très pratique pour les personnes utilisant Internet comme outils de travail et voulant se connecter à n'importe quel endroit.

4.1.1.3 Accès internet sans fil

C'est une solution qui est devenue très courante de nos jours. Elle permet aux PME-PMI et grandes entreprises de connecter leur réseau à Internet. Il suffit au client d'installer une antenne pour se connecter à Internet et de bénéficier de tous les services à valeurs ajoutées. En moyenne, le coût d'installation est de l'ordre de 800 euros ;

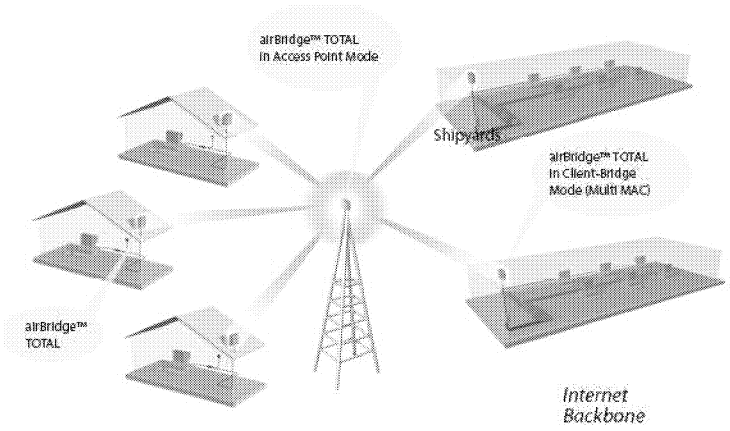

FIG. 4.1 – Accès sans fil sur un relais de TELKOM SA

4.1.1.4 La Voix sur IP

C'est l'ensemble des procédés qui permettent à la voix et à la parole d'être transportées sur le réseau internet. TELKOM SA offre plusieurs services :

- les chaînes de radio en direct ou en différé sur internet. Elle propose deux technologies dominantes sur le marché : la technologie Real Network et Windows média. Cette activité ne nécessite pas un matériel très sophistiqué.

- les appels téléphoniques gratuits : Deux solutions existent : PC-to-PC et Téléphone IP-Téléphone IP. La première n'est plus très utilisée car nécessite l'immobilisation de plusieurs matériels. La deuxième est celle qui permet à deux personnes disposants de téléphones IP de passer des appels entre eux gratuitement.

- les appels internationaux meilleurs marché. Cette solution permet aux personnes connectées sur Internet et possédant des téléphones IP ou des passerelles IP de passer des appels internationaux vers des réseaux fixes ou mobiles à des prix très faibles.

- routage d'appels : il permet à un client ne disposant pas de passerelles IP de passer des appels de n'importe quel poste fixe ou portable. Le client doit composer le numéro du centre serveur ensuite il est pris en charge par le serveur vocal qui vérifie l'identification et l'authentification. Si tout est correct, le client compose le numéro de son correspondant. Le matériel qui effectue ce routage est IP1000 ou IP2000.

Afin d'apporter un meilleur service à ses clients, TELKOM SA a décidé de créer un site web sur lequel les clients pourront consulter le catalogue et commander en ligne leurs produits. Ce site comprend les fonctionnalités suivantes :

- le catalogue de présentation des produits de télécommunication
- un module d'achat en ligne
- une base de données stockant les informations sur le client (coordonnées, modes de paiement, suggestions pour l'amélioration du site etc.)
- un couplage avec le SI de l'entreprise pour mettre à jour le catalogue
- un outil d'analyse statistique du comportement des visiteurs
- hébergement dans un local sécurisé.

4.1.2 Structure informatique

4.1.2.1 Le matériel

L'infrastructure du SI est constituée d'équipements homogènes. Elle se fait à l'aide d'un VSAT pouvant supporter un débit croissant jusqu'au moins 30Mbps. soit 20Mbps en montée et 10 Mbps en descente

- Les switchs sont de types Ethernet 100mbps 32 ports
- Les routeurs sont de type CISCO 2600
- Les serveurs DNS et Proxy Cache sont des PC de configuration PIV 1Go RAM, 2*40Go DD,. de type UNIX
- Les ordinateurs de bureau et portables sont de type PC.

4.1.2.2 Les logiciels

Tous les logiciels ont été acquis légalement et possèdent un numéro de licence officielle. L'entreprise a acquis le logiciel Bandwith Manager pour la gestion de la bande passante de ses différents clients. Le logiciel Saari pour la gestion commerciale, la gestion du personnel, la comptabilité et la paie. Un logiciel de monitoring pour le suivi des différents serveurs. La bureautique est traitée sur les ordinateurs de bureau à partir des logiciels installés sur des serveurs. Le système d'exploitation utilisé est Win 2000.

4.1.3 Sécurité

4.1.4 Schéma du réseau de TELKOM SA

Le schéma4.2 ci-dessous représente l'architecture générale du réseau. On remarque qu'il est divisé en quatre grandes parties :

- le réseau sans fil : il permet l'interconnexion de plusieurs sites distants au site central
- le réseau « voix et fax» : il gère les appels locaux « voix et fax » (sur le réseau IP) et le re routage de certains appels vers le réseau PSTN international
- les serveurs : ils gèrent toutes les communications, la facturation et le contrôle du réseau
- le réseau d'accès au satellite : il s'occupe de la communication avec le satellite

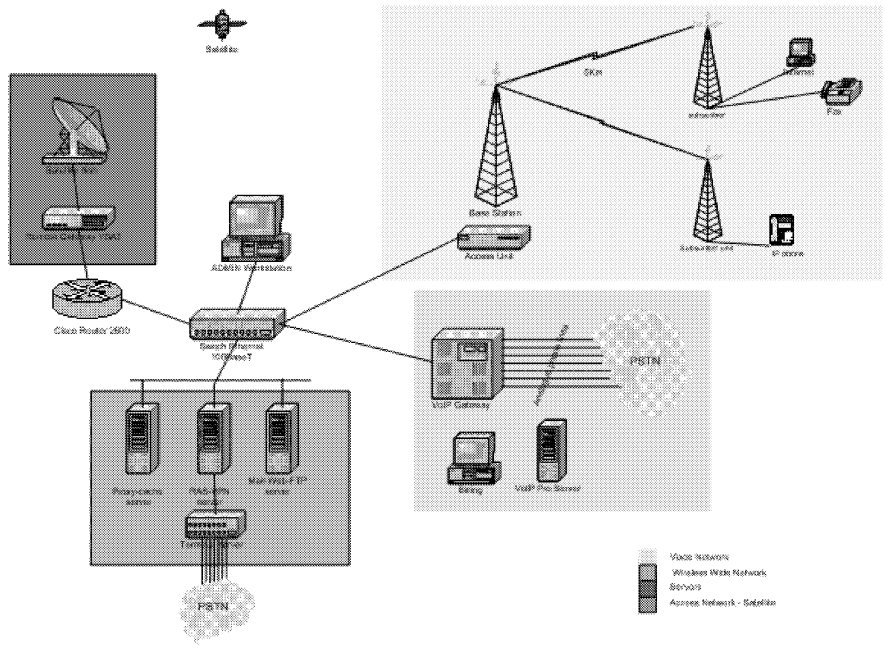

FIG. 4.2 – Schéma du réseau de TELKOM

4.1.4.1 Sécurité du système d'information

Il existe une PS, elle fait partie de la politique globale de sécurité de l'entreprise. Une charte d'utilisation des ressources informatiques et des services internet a été élaborée et diffusée à l'ensemble du personnel. Cette charte précise les droits et les devoirs de chaque utilisateur. Des affiches de sensibilisation sont posées sur des panneaux d'affichage, et contienent les règles suivantes :

- le contrôle d'accès se fait par identification ;
- principe de sauvegarde de tout fichier ;

- chaque utilisateur est responsable de son travail, le travail est sauvegardé sur des serveurs. Parallèlement les documents papiers sont rangés dans une armoire fermée ;
- chaque utilisateur est responsable des ressources informatiques mises à sa disposition dans le cadre de ses activité ;
- chaque utilisateur doit strictement respecter la politique clean desk(bureau propre) ;
- chaque utilisateur doit signaler toute anomalie dans le meilleur délai au support utilisateur ;

4.2 Tableau de bord dynamique de la sécurité de TELKOM

4.2.1 Création de la carte stratégique

La démarche TBDS est modulaire. Il est possible de mettre en place un TBDS sur une vue macroscopique (l'entreprise toute entière par exemple) ou sur un sous-ensemble de l'entreprise : une direction, un service, une application, ou sur un domaine de l'activité. Elle s'applique ainsi sur un périmètre sur lequel une analyse de risques a été menée. Sur ce périmètre, on récence les ressources IT à prendre en compte : le personnel, les applications, le matériel, les données (externes et internes), les informations, les bâtiments.

Analyse de l'existant : Nous prenons en compte les travaux existants en matière de sécurité informatique :

- analyse des risques et enjeux ;
- politique de sécurité ;
- objectifs fixés sur la couverture des risques ;
- equipments / Infrastructures

L'analyse des risques et la politique de sécurité permettent de renseigner le niveau " Risques " de la carte stratégique. Les autres documents seront pris en compte dans l'étape de processus internes de sécurité.

Profil Sécurité de l'information : il s'agit ici de modéliser avec l'administrateur de TELKOM, un profil d'exigence de sécurité qui permet d'élaborer le PSI. Lors de cette étape, on déterminera les valeurs cibles à atteindre pour que les objectifs de couverture de risque soiront atteints. Il s'agira de mettre en place toutes les contre-mesures nécessaires.

Processus interne de sécurité : D'après les principes de la carte stratégique, on sélectionne ici les indicateurs (indicateurs d'objectifs et indicateurs de performance) ayant un impact sur le périmètre considéré et les risques à couvrir. Les indicateurs d'objectifs mesureront l'atteinte des objectifs prévus dans les contre-mesure alors que les indicateurs de performance mesureront le niveau des actions menées.

4.2.2 Instanciation Carte Stratégique

Il s'agit de définir les éléments quantitatifs permettant de mesurer l'avancement des objectifs de sécurité. On se pose un certains nombre de questions, les réponses à ces questions nous permettent de fixer les objectifs de l'entreprise. Ces objectifs nous permettront de mieux sélectionner les risques sur lesquels nous devons

travailler. Pour les risques sélectionnés nous devons en principe calculer leur potentialité, qui représente leur probabilité d'occurrence, et leur impact, qui représente la gravité des conséquences directes ou indirectes qui découleraient de l'occurrence du risque. Une fois ces informations obtenues nous devons les charger dans l'ontologie, mais puisque le but de ce travail est un gain de temps, les risques sélectionnés peuvent éventuellement déjà exister dans ONTOSEC, il faudra juste aller chercher ces informations, afin de les rendre utilisables par le TBDS.

La définition des objectifs de sécurité s'est fait à un niveau très élevé de l'entreprise. Cette définition concrétise les choix stratégiques en matière de sécurité. Il est utopique de penser supprimer tous les risques. Il s'agit de fixer les niveaux de risque que l'entreprise jugera acceptables, inadmissibles, bien que supportables ou insupportables parce que n'ayant pas les moyens de faire face à ses conséquences. L'objectif sera de ramener, par de mesures de sécurité appropriées tous les risques à un niveau acceptable. La direction générale de TELKOM se fixe les objectifs suivants :

- mise en œuvre d'un système de un suivi des accès de télémaintenance ;
- définition des règles d'accès sur le pare-feu ;
- contrôles et des audits réguliers sur le pare-feu ;
- un suivi régulier des activités de contrôle des traces doit être assuré ;
- le système doit garantir une indisponibilité maximale de quelques heures ;
- la disponibilité des moyens de communication du siège vers les agences ;
- la disponibilité de la messagerie ;
- les utilisateurs doivent être sensibilisés sur la politique de sécurité etc...

Nous avons identifié les risques suivants :

Risques liés au catalogue de produits : le catalogue présente les informations sur les produits, l'internaute qui consulte le catalogue doit s'assurer que les informations sont correctes. Les menaces portant sur le catalogue sont :

- le remplacement du catalogue par une page placée par un pirate
- les modifications du contenu (prix, référence, descriptif etc.)
- le "spoofing" de site (mise en ligne d'un site similaire que les internautes consultent en pensant être sur le site de TELKOM, mais présentant des informations fallacieuses).

Risques liés à l'achat en ligne : les clients font leurs achats et leur paiement par internet, mais ceci ne peut se faire sans risque. Nous mentionnons ici les principaux risques et présentons par la suite les mesures nécessaires pour parer ces risques.

- Ecoute passive et rejeu : l'écoute passive suivie d'un rejet est une technique permettant de s'authentifier sur un serveur en réutilisant les paramètres d'authentification d'un tiers. Cette attaque consiste à écouter les communications réseaux par un moyen passif, c'est à dire n'agissant pas sur les communications.

Le but est généralement d'en extraire les identifiants et authentifiant utilisés. Il peut s'agir des mots de passe transmis en clair , mais aussi d'autres techniques.

- Vol d'information et répudiation : la répudiation consiste à nier avoir participé à une transaction. Le client, le vendeur (et éventuellement un intermédiaire de paiement) peut nier sa participation à l'une ou à l'ensemble des étapes de l'achat : la commande, le paiement ou la livraison.

Risques associés à la liaison entre le système d'achat en ligne et le système de gestion : afin d'assurer une meilleure réactivité et assurer un meilleur service après vente, le système d'achat en ligne a été lié au système de production de l'entreprise, ainsi qu'à ces systèmes de gestion comptables et de suivi de stock. On peut citer l'accès illicite aux systèmes de gestion de l'entreprise. Ce couplage entraîne de risque pour TELKOM, qu'un pirate qui obtient un accès illicite aux systèmes de l'entreprise, pourrait les mettre en déni de service.

Risques liés au système en général :

- Accès illicite à l'interface de mise à jour du site : si un tiers arrive à utiliser l'interface de mise à jour du site de TELKOM il est en mesure d'y faire des modifications profondes.

- Chevaux de Troie : un cheval de troie peut être utilisé pour récupérer des mots de passe, voire pour prendre le contrôle à distance d'une machine. Il existe aujourd'hui de nombreux programmes de piratage fonctionnant selon le principe de cheval de troie. Ce programme pourra permettre au pirate de prendre à distance le contrôle du serveur Web de TELKOM SA, ou encore utiliser la machine comme relais pour une attaque élaborée contre une machine cible secondaire.

- Déni de service (accidentel ou malveillant) : le déni de service consiste à rendre le serveur web de TELKOM indisponible. Ici nous voyons beaucoup plus le déni de service malveillant. Il consiste à envoyer au serveur un message plus grand que la capacité de réception du serveur.

- Spamming : il consiste à l'envoi des courriers non désirés à caractère commercial ou pseudo commercial. Supposons qu'un pirate récupère le fichier client de TELKOM en piratant le serveur web. Un autre risque possible, TELKOM gère une liste de diffusion pour informer ses clients sur les nouveautés ou des promotions

Considérons le risque d'indisponibilité des ressources, ce risque comprend l'absence du personnel technique. Il existe un seul expert pour le réseau sans fil, son absence peut causer de préjudice à l'entreprise en cas de problème touchant le réseau sans fil. Il n'existe pas de groupe électrique, ni de plaque électrique solaire, en cas de panne grave électrique, le réseau est *down*. Les risques identifiés nous allons nous baser sur l'ontologie des risques pour identifiés les scénarios correspondants. L'ontologie nous donne les scénarios ainsi que les formules indiquant les sous services utilisés pour chaque type de mesure(structurelle, dissuasive, préventive, de protection, palliative, de récupération).

Considérons le risque associé à la liaison entre le système d'achat en ligne et le système de gestion : On retrouve le risque « Modification de l'interface de mise à jour du site ». Cette rubrique peut se retrouve dans l'ontologie correspondant au scénario "Altération de données" et "Indisponibilité passagère des ressources" comme le montre la figure 4.3. Pour le scénario "Indisponibilité de ressources" le risque de "court-circuit" est de min(03A01 ;03A04). Il est composé des services 03A01(Qualité de la fourniture de l'énergie) et 03A04 (Qualité du câblage). Cela signifie que ces sous services sont impliqués dans la quantification des mesures préventives. Le calcul de l'efficacité revient à calculer pour chaque mesure l'efficacité de celle-ci EFF DISS,

Altération de logiciel						
Modification volontaire des fonctionnalités prévues d'une application informatique		Dissuasives	Preventive	Protection	Palliative	Recuperation
	Modification volontaire des fonctionnalités prévues de l' application de gestion du site par les équipes de developpement	10A02	10A02		max(min(08D05;09D03);09D02)	01D02
	Modification volontaire des fonctionnalités prévues de l' application de gestion du site par la maintenance	10B01	10B01		min(08D04;max(min(08D05;09D03);09D02))	01D02
	Modification volontaire des fonctionnalités prévues de l' application de gestion du site par le personnel d'exploitation	max(07C02;08F03)	min(08B02;08B03)	09B04	min(08D04;max(min(08D05;09D03);09D02))	01D02
Indisponibilité passagère de ressources						
Absence de personnel						
	Absence de personnel d'exploitation				09E03	
Accident ou panne mettant hors service une ou plusieurs ressources matérielles						
	Accident de nature électrique (court-circuit), mettant hors service un équipement du réseau étendu		min(03A01;03A04)		max(04A01;04A07;09E03)	01D01
	Accident de nature électrique (court-circuit), mettant hors service un équipement du réseau local		min(03A01;03A04)		max(05A02;05A08;09E03)	01D01

FIG. 4.3 – Risques extraits de ONTOSEC pour le cas TELKOM SA

EFF PREV, EFF PROT, EFF PALL, EFF RECUP. La valeur de chaque efficacité est ajustée pour obtenir les STATUS : STATUS EXPO, STATUS DISS, STATUS PREV, STATUS PROT, STATUS PALL, STATUS RECUP.

On déduit STATUS-P à partir des trois STATUS de potentialité (STATUS-EXPO, STATUS-DISS, STATUS-PREV) en utilisant la grille correspondant au type de scénario (P-MALVEILLANCE, P-ERREUR, P-ACCIDENT).

Prenons le scénario suivant : "Modification volontaire des fonctionnalités prévues d'une application par le personnel d'exploitation" est de type Malveillance.
La réduction d'impact STATUS-RI se calcule à partir des trois STATUS d'impact (STATUS-PROT, STATUS-

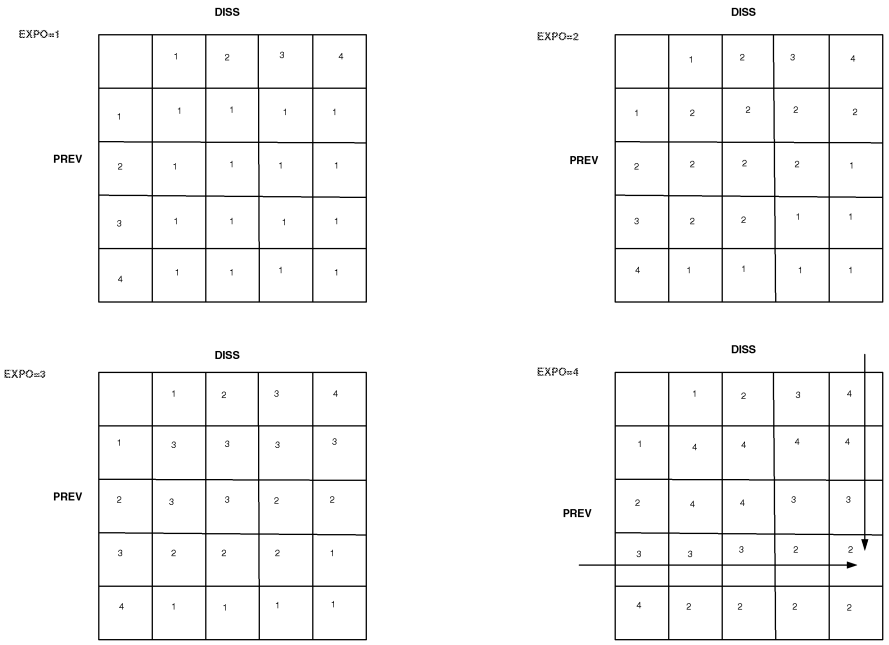

FIG. 4.4 – Potentialité pour un scénario de type malveillance : Source KB MEHARI

PALL, STATUS-RECUP) en utilisant la grille correspondant à la nature du scénario (RI-DISPONIBILITE, RI-INTEGRITE, RI-CONFIDENTIALITE). Prenons le scénario suivant : "Modification volontaire des fonctionnalités prévues d'une application par le personnel d'exploitation" est de type Intégrité.
On obtient STATTUS-PROT =2
STATTUS-PALL =2
STATTUS-RECUP =4
La réduction d'impact est donc égal à 3.

On détermine ensuite l'impact STATUS-I à partir de STATUS-RI et de la classification (valeur) de la ressource en utilisant les informations provenant de la direction générale. Sachant que STATUS-RI =3 et que la ressource application de gestion du site a une valeur égale à 2, on obtient un impact égal à 2, on déduit la valeur de la gravité du sinistre en fonction du STATUS-P et STATUS-I, en utilisant la grille d'aversion au risque. Sachant que STATUS-I=2 et STATUS-P=2, on obtient une gravité égale à 2 pour le scénario "Modification volontaire des fonctionnalités prévues de l'application de gestion du site par le personnel d'exploitation".

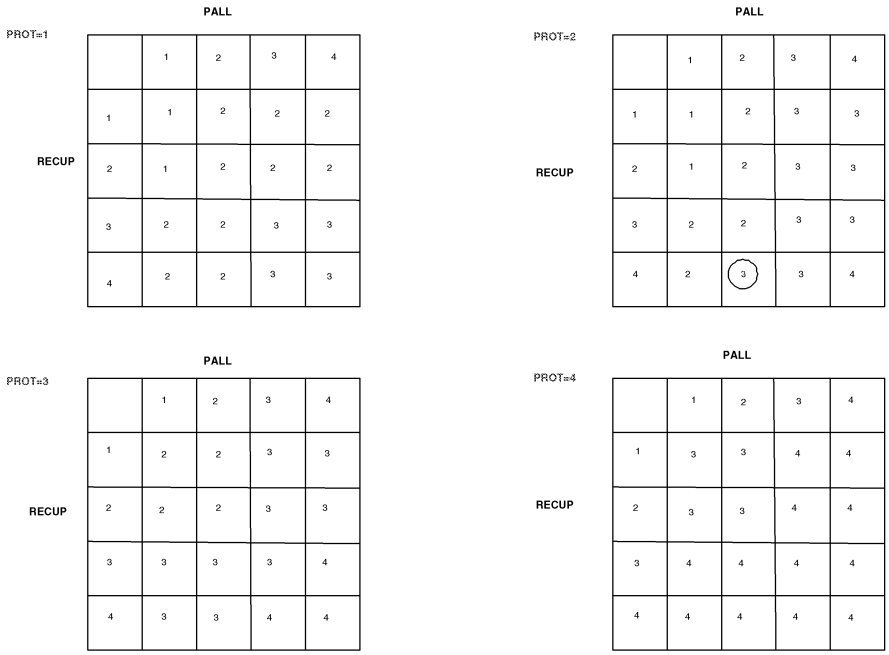

FIG. 4.5 – Potentialité pour un scénario de type Intégrité : Source KB MEHARI

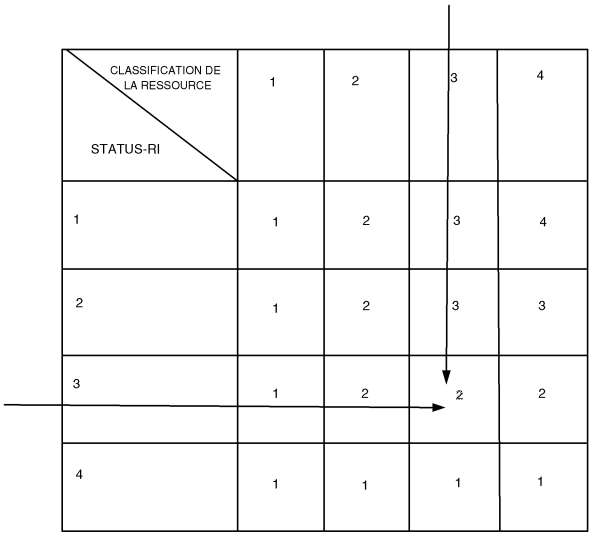

FIG. 4.6 – Calcul de l'impact

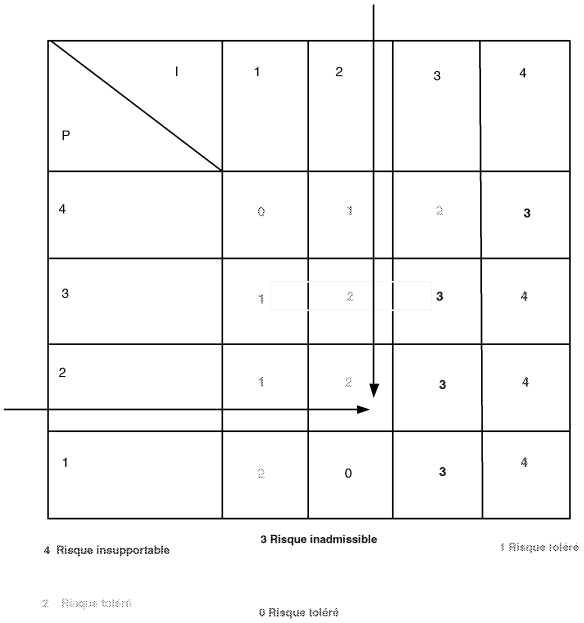

FIG. 4.7 – Gravite du risque "Modification volontaire des fonctionnalités ... "

Analyse des mesures de sécurité : après avoir fait une analyse de risques le système nous permet de déterminer les mesures associées. Prenons l'exemple du risque "Modification volontaire des fonctionnalités prévues de l'application de gestion du site par le personnel d'exploitation", ONTOSEC nous permet d'identifier les mesures suivantes :

- mesures palliatives et préventives : la classe *GestionDesChangements* qui est une sous-classe de *OrganisationDesDeveloppements*.
- mesures palliatives : max(min(08D05 ;09D03) ;09D02)= max (min(SauvegardeDesDonnees applicatives ; ReconstitutionDesTraitements) ; Reconstitution des données)
- mesures de récupération : la classe *AssuranceDesDommagesImmatériels* sous-classe de *Assurances*, qui elle même est une sous-classe de *OrganisationDeLaSecurite*.

Choix des indicateurs représentatifs en fonction des objectifs fixés et du risque exemple "Modification volontaire des fonctionnalités prévues de l'application de gestion du site par le personnel d'exploitation", ONTOSEC nous fournit les indicateurs suivants :

1. nombre de personnes habilitées à changer les règles et autorisations de l'application de gestion du site / Nombre de profils attribués à cette application choisie ;
2. nombre de modifications de programmes, en exploitation, contenant des contrôles / Nombre total de programmes contenant des contrôles ;
3. taux de satisfaction des utilisateurs sur les interventions de maintenance.

Chaque indicateur se voit attribué des objectifs correspondant à des seuils :

- insuffisant
- acceptable
- optimal

ONTOSEC nous fournit les objectifs de chaque indicateur qui sont transmis à chaque responsable et par rapport auxquels sont comparés les valeurs obtenues pour chaque indicateur. Chaque responsable identifié connaît ses objectifs ainsi que la façon dont il contribue à l'atteinte des objectifs globaux. Toutes ces informations sont disponibles dans ONTOSEC. Le résultat d'un indicateur peut être :

- une mesure ;
- un calcul qui intègre une pondération prédéfinie ;
- un rapport à un ou plusieurs seuil ;

4.2.2.1 Interface du tableau de bord

Il s'agit ici de l'interface initiale du TBDS. A gauche de l'écran se trouve la légende, à droite, l'arbre hiérarchique des indicateurs. L'utilisateur peut choisir les indicateurs qui l'intéressent en fonction de ses droits d'accès. Voir figure 4.8.

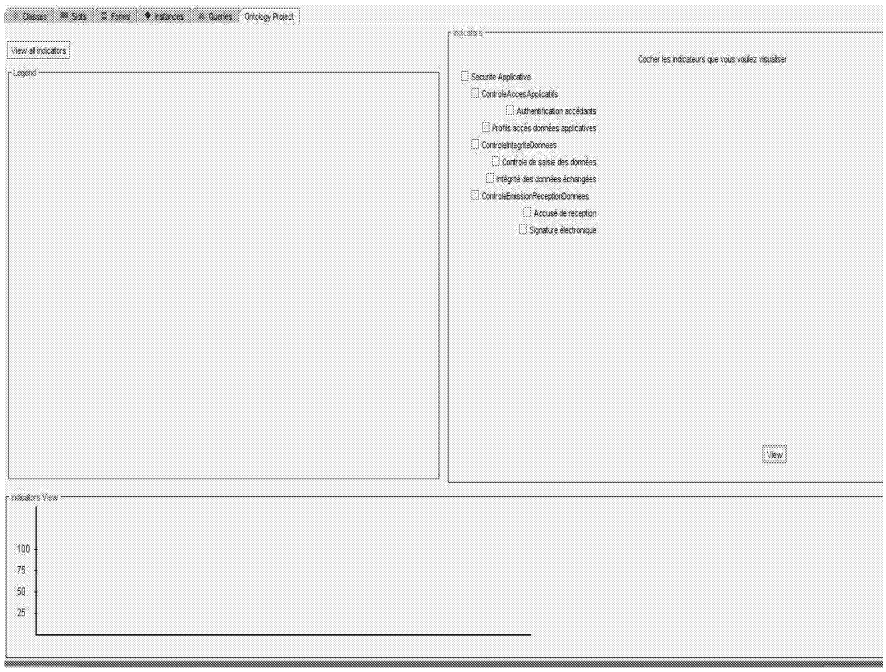

FIG. 4.8 – Vue préliminaire

Vue sur les indicateurs stratégiques : nous avons un seul indicateur stratégique (niveau 0). Il est calculé en fonction des indicateurs fonctionnels et opérationnels. Si l'utilisateur est juste intéressé par la sécurité applicative, il doit cocher cet indicateur, après validation, le tableau de bord s'affiche dans la partie inférieure comme le montre la figure 4.9

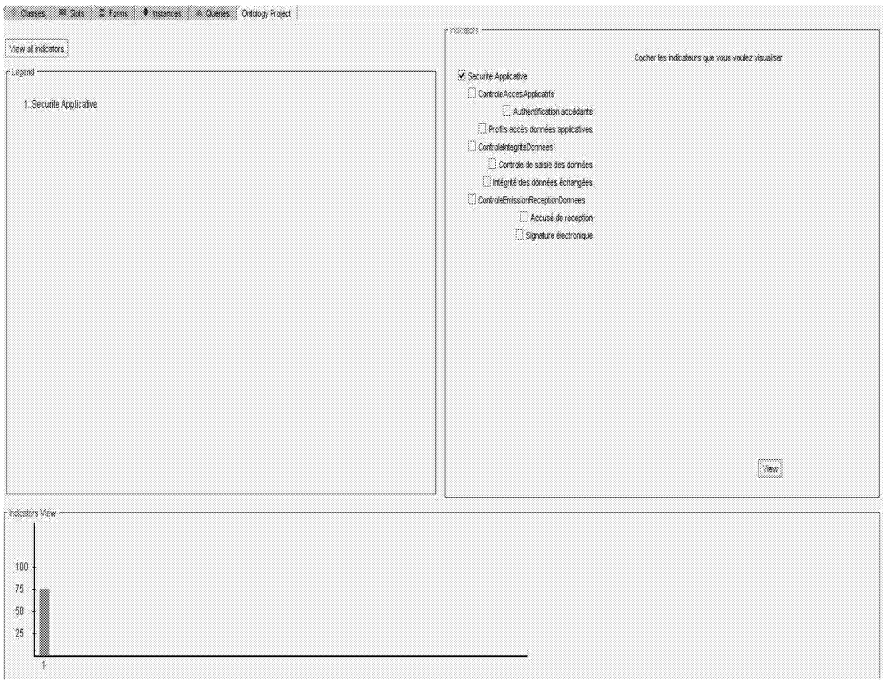

FIG. 4.9 – Vue sur tous les indicateurs stratégiques

Vue sur les indicateurs fonctionnels : nous avons trois indicateurs de fonctionnels (niveau 1). Ils sont calculés en fonction des indicateursopérationnels (niveau 2). L'utilisateur en cochant ces indicateurs et après validation, il verra le TBDS s'afficher comme le montre la figure 4.10

Vue sur les indicateurs opérationnels : nous avons six indicateurs opérationnels (niveau 3). Ils mesurent l'atteinte des objectifs des mesures de sécurité. Ils sont calculés en fonction de l'efficacité de la mesure, de l'impact et de la potentialité du risque associé. En les choisissant, nous avons le tableau de bord comme le montre la figure 4.11.

Vue sur tous les indicateurs nous avons dix indicateurs, ces dix indicateurs permettent d'avoir une vue globale de la sécurité sur le domaine étudié. Il suffit juste de cliquer sur *view all indicators* ou de tous les cocher dans l'arbre hiérarchique. On verra s'afficher les informations comme dans la figure 4.12.

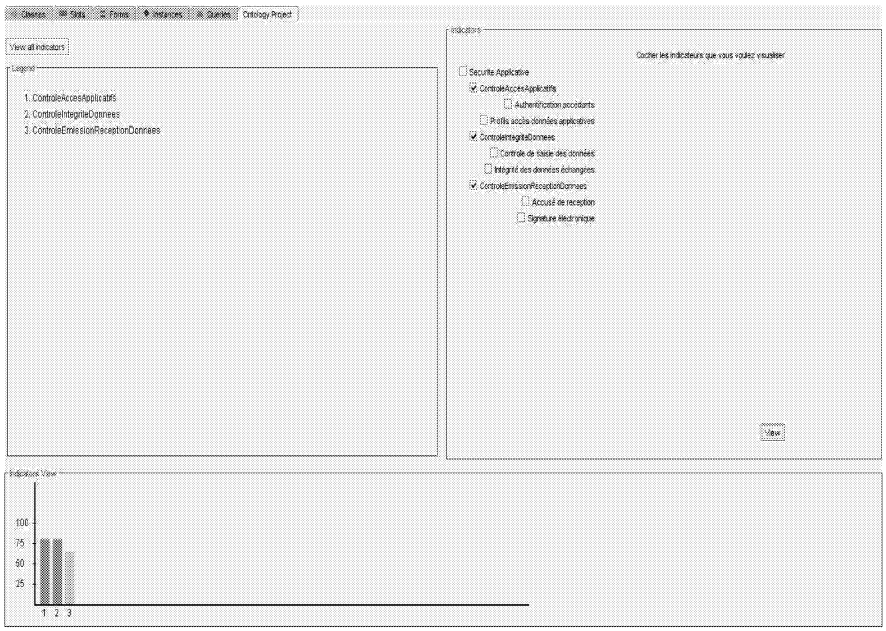

FIG. 4.10 – Vue sur tous les indicateurs fonctionnels

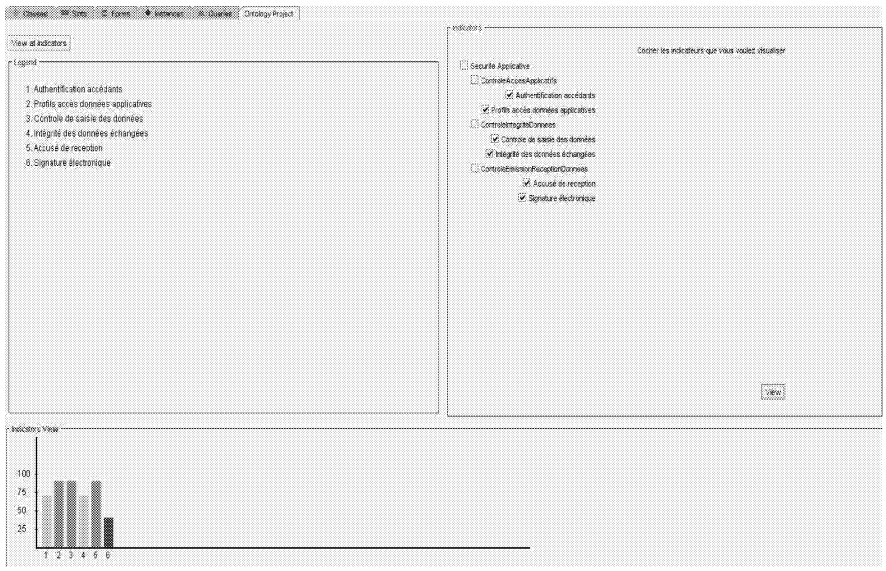

FIG. 4.11 – Vue sur tous les indicateurs opérationnels

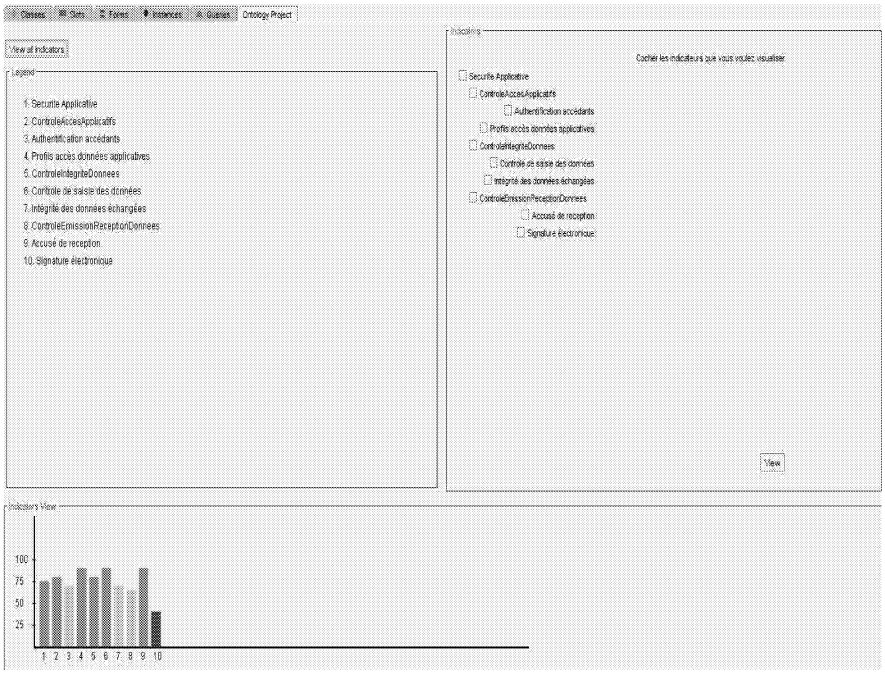

FIG. 4.12 – Vue globale de la sécurité applicative de TELKOM

4.3 Apports de la démarche TBDS dans la gestion de la sécurité de TELKOM

Suite à l'application de la démarche TBDS dans l'entreprise TELKOM, nous avons tenu à avoir le point de vu d'un responsable de la boîte. Dans les lignes suivantes, nous disons ce qu'il pense.

L'utilisation d'ONTOSEC au sein de notre entreprise nous a donné beaucoup d'avantages. L'un des apports les plus importants est la communication rendue possible autour de la stratégie de sécurité. Elle a permis de faire en sorte que la sécurité devienne l'affaire de tous. que le business et l'informatique puisse mieux se comprendre. Tout d'abord, vis-à-vis de la direction, le TBDS a fournit une justification de la stratégie sécurité en reliant par des liens de causalité clairs les actions engagées par la stratégie et les risques à couvrir.

La gestion de la sécurité avec ONTOSEC est modulaire et peut se faire de manière proactive, elle est adaptée à tous les secteurs de l'entreprise. Le champ d'application est variable, la démarche peut se faire sur l'entreprise entière ou seulement sur un domaine. Nous avions de problèmes pour la mise en place de solutions de sécurisation des accès internet, de l'accès au réseau interne et de la conformité avec la politique de sécurité. ONTOSEC nous propose par des requêtes simples la liste de nos vulnérabilités et nous propose les solutions à mettre en place. Si les nouvelles menacent appartient à une catégorie existante dans l'ontologie alors il suffit juste de prendre les solutions proposées par ONTOSEC. Sinon, il faut trouver les contre-mesures appropriées et de mettre ONTOSEC à jour.

Pour résumer ONTOSEC en une phrase, nous dirons que c'est un système, qui nous a permis de gérer de façon globale la sécurité en faisant intervenir les risques, les contre-mesures et les indicateurs. Maintenant nous pouvons passer de la politique de sécurité aux contre-mesures de sécurité en quelques minutes. Il est important de préciser que, ONTOSEC propose des solutions, mais sans dire comment les implanter.

Chapitre 5

Conclusion

5.1 Bilan et contributions

Le développement d'un TBS dans un environnement dynamique est l'un des principaux défis que les chercheurs dans le domaine de la sécurité souhaitent relever. Un défi apparu du fait de la montée croissante des nouvelles techniques d'attaques. Ces techniques croissent pratiquement au même rythme voire plus que la recherche dans ce domaine. Face à ces techniques d'attaques, nous avons une montée sensible des méthodes d'élaboration de TB. Les TB représentent de plus en plus un enchaînement logique des différentes composantes d'une stratégie globale de sécurité. L'objectif ultime de la stratégie de sécurité n'est plus seulement la couverture des risques, mais aussi la prévention de risques non encore identifiés. Toute modification de la stratégie globale de sécurité doit avoir des répercutions sur le TB. La stratégie doit pouvoir se modifier de manière dynamique face aux nouvelles attaques. Les indicateurs du TB ne mesurent plus toujours les valeurs réelles, mais ils doivent pourvoir en fonction des indicateurs de bas niveau et de la PS nous renseigner sur les menaces qui pourront survenir. Comment gérer donc quelque chose qui n'existe pas encore ? quelque chose dont on ne connait pas le moment ou les chances de son apparition ? la difficulté de gérer quelque chose qui n'existe pas montre bien qu'il n'est pas aussi facile le mesurer. Les TB classiques deviennent impuissants face à tout ceci. Les entreprises qui les utilisent sont confrontées à plusieurs problèmes. Le temps d'analyse des données devient assez élevé à cause de la masse importante des informations à gérer. Les informations proviennent des sources variées, il se pose donc un problème d'hétérogénéité. Les accès concurrentiels aux bases contenant ces informations deviennent problématiques par leurs interférences avec d'autres transactions en cours. En tenant compte de tous ces problèmes, comment les responsables de la sécurité parviennent-ils à mettre à disposition des décideurs et des opérateurs les informations leur permettant de mesurer l'état réel de la sécurité de l'entreprise ? telle est la question à laquelle nous avons essayé de trouver des éléments de réponse le long de ce travail de thèse.

Dans ce travail de thèse, un TBDS est un TB qui est conçu avec la stratégie globale de sécurité. Les deux sont étroitement et dynamiquement liés. Toute variation de la stratégie est répercutée directement sur le TB. Tout

part de la définition de la stratégie de sécurité à un niveau très élevé de l'organisation, ensuite de la carte stratégique. Cette stratégie peut être mise en place de plusieurs manières. Dans le cadre de ce travail, cette stratégie est implantée au niveau fonctionnel en utilisant la norme ISO 27001 : 2005 ou la version 4 de COBIT pour les entreprises qui le souhaitent. Les directives fonctionnelles sont ensuite implantées au niveau opérationnel avec des normes telles que ITIL version 3 ou COBIT version 4. Le TBDS est un ensemble d'indicateurs qui mesurent l'état d'avancement de la PS. Les indicateurs opérationnels sont générés dynamiquement en fonction des données sur les contre-mesures et les menaces. Les indicateurs de niveau supérieur sont calculés à partir des indicateurs de niveau inférieur (indicateurs opérationnels, indicateurs fonctionnels) en utilisant des techniques statistiques. Les informations sur les indicateurs sont ainsi remontées depuis le niveau opérationnel jusqu'au niveau stratégique, permettant ainsi de générer les TB de façon dynamique à tous les niveaux de l'organisation.

Dans notre approche, nous avons dans un premier temps travaillé sur les ontologies en faisant une analyse comparative des différentes méthodes de construction d'ontologies. La méthodologie de construction d'ontologies *from scratch* était l'une des premières. Elle vise à construire l'ontologie en l'absence de connaissances. La méthode *methontology*[Fernandez1999] construit une ontologie en respectant des activités de gestion des projets (planification, assurance qualité), de développement (spécification, conceptualisation, implantation, maintenance) et des activités de supports (intégration, évaluation, documentation). Natalya et Deborah [Natalya101] proposent une méthode simple de construction d'une première ontologie. Elles décrivent une approche itérative en commençant par aborder l'ontologie de façon frontale. Ensuite elles reviennent sur l'ontologie, qu'elles considèrent en processus d'évolution, en l'affinant et en la complétant par des détails. Tout au long de ce processus, elles discutent les décisions de modélisation à prendre par le concepteur, ainsi que les pour, les contre et les implications des différentes solutions. Les méthodologies d'apprentissage à partir de textes permettent de construire une ontologie sur une base de connaissance à priori. Cette base de connaissance permet d'automatiser l'enrichissement de l'ontologie par des méthodes d'apprentissage.

A côté de ces méthodes, nous avons proposé une méthode de construction d'une ontologie dans le domaine de la sécurité des informations, que nous avons appelé démarche TBSD. Notre approche en quatre étapes permet de construire une ontologie globale de la sécurité à partie de trois ontologies locales. La première étape qui consiste à choisir les termes candidats de l'ontologie, s'appuie sur la base de connaissance de MEHARI, la norme ISO 17799 : 2005 et un troisième corpus qui est issu des bonnes pratiques de quelques entreprises. Après avoir choisi les termes, on rattache un concept à ces termes en leur donnant une description détaillée. La deuxième étape on définit les propriétés et les relations entre les concepts ; la relation la plus utilisée étant la relation *Is-a* qui permet de spécifier les termes. La troisième étape consiste à créer une hiérarchie des classes. Nous avons opté pour un procédé de développement de haut en bas, en commençant par une définition des concepts plus généraux du domaine, et avons poursuivi par la spécialisation des concepts. La quatrième étape nous a permis de développer l'ontologie dans un langage de représentation des connaissances. Cette démarche a été appliquée pour les trois ontologies locales : ontologie des risques, ontologie des contre-mesures et ontologie des indicateurs. Nous avons ensuite fusionné ces trois ontologies pour avoir ONTOSEC.

ONTOSEC est un ensemble de concepts classifiés en une hiérarchie. Cette ontologie ne contient pas de propriétés reliant les différents concepts. Ces propriétés existent chacune dans leur ontologie locale. L'utilisateur peut donc créer une requête qui contient des concepts d'ONTOSEC et éventuellement des propriétés des ontologies locales.

Nous avons proposé par la suite une démarche pour l'évolution d'ONTOSEC. Cette démarche en sept étapes, permet de donner le chemin à suivre pour passer d'une version consistante de l'ontologie à une autre. Elle commence par l'identification de l'ontologie à modifier, ensuite l'identification du changement à apporter. Le changement est fait en fonction de l'approche choisie par le développeur (ascendante ou descendante). Après avoir identifié le changement, on l'évalue afin de savoir son impact sur l'ontologie, on l'édite, on l'approuve et on l'implante.

L'ontologie globale a servie de médiateur pour mettre en place le TBSD. Le TBDS utilise ONTOSEC afin de répondre aux questions posées par les utilisateurs. Cette approche, qui lie de manière étroite le TBSD et la stratégie globale de sécurité, tient compte de l'évolution de la stratégie. Tout changement de la stratégie est directement répertorié sur une ontologie locale. Le changement est directement répercuté de manière dynamique dans ONTOSEC et par conséquent dans le TBSD. Notre démarche unifie dans un cadre cohérent les approches existantes dans la littérature, en proposant une approche à base des ontologies. Elle apporte aux organisations la cohésion des processus autour de la stratégie de sécurité.

Quant à l'originalité de nos travaux, elle réside principalement dans l'interaction entre les trois ontologies et le TBSD, tout se fait de manière dynamique. A partir des menaces, le système peut retrouver les risques associés avec les attributs, et de manière dynamique, proposer les contre-mesures à mettre en place pour couvrir le risque dont il est question. Le couple (risque, contre-mesure) est lié de manière directe à un indicateur de performance ou à un indicateur d'objectif. L'indicateur étant un concept utilisé par l'ontologie des indicateurs, il sera directement exploité par le TBSD. Malgré son originalité, cette démarche possède des points communs avec la plupart des méthodes étudiées. Avec sa carte stratégique, elle se rapproche du BSC. La carte stratégique est le point central du système ; elle est l'expression des hypothèses stratégiques et elle définit les relations de causes à effets entre les mesures des résultats avec les indicateurs d'objectifs, et les actions menées pour atteindre ces objectifs qui sont quant à elle mesurées par les indicateurs de performance. Le système des indicateurs est l'image d'un modèle de causes à effets portant sur l'action. Le choix de l'action fonde l'indicateur et non l'inverse. Sur ce point, nous abondons dans le même sens que Kaplan car l'ontologie des indicateurs de sécurité est construite avec celle des mesures. Kaplan dans le BSC parle des indicateurs de pilotage. Dans notre démarche, nous parlons des indicateurs de performance qui jouent le même rôle. Ensuite Kaplan parle des indicateurs d'objectifs qui jouent le même que les indicateurs de même nom dans notre démarche : la démarche TBSD.

La méthode se rapproche de celle de la DCSSI qui repose sur la PS de l'entreprise. Elle est étroitement liée à la PS, et toute modification de la PS se répercute sur le TBSD. Elle se rapproche de la méthode par domaine du CNRS. Les domaines ici sont les supports de nos ontologies locales : risques, mesures et indicateurs. Le domaine de la réaction est équivalent à celui des mesures de sécurité puisqu'elle recense l'ensemble des mesures nécessaires au cas où il surviendrait un incident. Le domaine de la détection qui consiste à détecter un incident le plus tôt possible lorsqu'il se produit peut être mis en œuvre par un module qui consisterait à mapper l'ontologie des risques à l'ontologie des contre-mesures de sécurité. Ce *mapping* ferait ressortir les risques les plus probables et associerait aussi les actions à prendre pour les couvrir. Pour le moment des simples requêtes permettent d'avoir ces mesures. Le domaine de la prévention, qui consiste à limiter les dégâts au cas où surviendrait une attaque réussie, et le domaine de la réaction qui est l'ensemble des mesures palliatives réalisées lorsqu'un incident survient, peuvent ici être comparés au domaine des contre-mesures de sécurité.

La méthode se rapproche de la méthode par niveau du CLUSIF, les taxonomies de l'ontologie des indicateurs se retrouvant sur trois niveaux. Par exemple pour l'OR, le niveau 1 correspond aux douze domaines de sécurité ; soit de MEHARI, soit d'ISO 17799 : 2005. En prenant l'exemple de l'ontologie des indicateurs, on distingue trois niveaux : les indicateurs de pilotage, les indicateurs fonctionnels et les indicateurs opérationnels.

L'objectif de notre démarche étant de faciliter la mise sur pied d'une politique globale de sécurité, nous avons définit la carte stratégique. La carte stratégique de la démarche TBSD schématise le futur TB. Elle est découpée en trois niveaux : niveau des risques, niveau profile de sécurité de l'information, niveau processus interne. Elle intègre les liens de causes à effets entre les différents indicateurs et entre les différents niveaux. Suite à cette carte stratégique, nous avons développé un tableau de bord dynamique de la sécurité. Ce tableau a été développé dans le sous domaine de la sécurité applicative mais peut très bien être implanté dans les autres domaines de l'organisme. Toutes les requêtes des utilisateurs sont faites sur le tableau de bord, lequel se base sur ONTOSEC en utilisant les de réécritures des requêtes afin d'apporter une réponse à l'utilisateur.

5.2 Perspectives

L'utilisation des ontologies pour la mise sur pied d'un TBSD peut s'étendre dans toutes les entreprises, quelle que soit leur taille, qu'elles aient ou pas une stratégie de sécurité. Pour celles qui ont déjà une stratégie de sécurité, la démarche permettra d'améliorer cette stratégie. Pour celles qui n'en ont pas, la démarche permetra d'élaborer une stratégie globale de sécurité. Les travaux sur les TBSD sont loin d'être terminés. La fusion des trois ontologies ou la mise en correspondance pourra donner un autre aspect au dynamisme, permettant ainsi de naviguer entre les ontologies de manière transparente. Une possibilité future serait de proposer un algorithme de réécriture des requêtes dans un cadre plus formel. Cette réécriture pourrait résoudre le problème de traitement de requêtes dans le cadre d'une architecture de médiation avec plusieurs ontologies modélisée, selon l'approche **GLAV**. Afin de valider ONTOSEC sur d'autres approches, une possibilité serait de proposer des algorithmes de réécriture pour les approches *GAV* et **LAV**. A titre de rappel, l'approche GAV fait correspondre

à chaque concept de l'ontologie globale une vue sur l'ontologie locale. Une requête exprimer en termes de l'ontologie globale peut être reformulé en une vue sur l'ontologie locale. L'approche LAV fait correspondre à chaque concept de l'ontologie locale une vue sur l'ontologie globale. Une requête exprimée en termes de l'ontologie globale peut être réécrite en vue.

Bibliographie

[Akoka1999] Akoka. J Comyn-Wattiau I. Lammari N. , Relational Database Reverse Engineering : Elicitation of Generalization Hierachies, Proceedings of workshop REIS 99 of ER99, LNCS 1727, Paris 1999.

[Baget 2003] Jean-François Baget, Étienne Canaud, Jérôme Euzenat, Mohand Saïd-Hacid."Les langages du web sémantique", in : Action spécifique " Web sémantique ", Jean Charlet, Philippe Laublet, Chantal Reynaud, editors

[Beneventano2000] Beneventano D. and Bergamaschi S. and Castano S. and Corni A. and Guidetti R. and Malzevezzi G. and Melchiori M. and Vincini M. (2000). Information integration : The MOMIS project demonstration. In VLDB 2000 proceedings of 26th International Conference on Very large Data Bases. September 10-14. Cairo Egypte. p. 611-614.

[Bessire2000] Bessire D et le CRI (2000), Du TB au pilotage : l'entreprise au risque de se perdre, Acte du 21 congrès de l'A.F.C

[BenMustapha2006] ers une approche de construction de composants Ontologiques pour le Web sémantique synthèse et discussion

[Baader2003] Franz Baader, Diego Calvanese, Deborah McGuinness, Daniele Nardi, Peter Patel-Schneider, editors. The Description Logic Handbook. Cambridge University Press, 2003 ;

[Brachman1985] R. J. Brachman and J. G. Schmolze. An overview of the KL-ONE knowledge Representation System. Cognitive Science, 9(2) :171 216, April 1985.
[Brisaboa2003]. Buccella A., Cechich A. and Brisaboa N.R. An Ontology Approach to Data Integration. Journal of Computer Science and Technology. Vol.3(2). Available at http ://journal.info.unlp.edu.ar/default.html, 2003, (pp. 62-68).

[Chalupsky2000] H CHALUPSKY. OntoMorph : A Translation System for Symbolic Knowledge. In : Anthony G. COHN, Fausto GIUNCHIGLIA, Bart SELMAN. KR 2000, Principles of Knowledge

Representation and Reasoning, Seventh International Conference, Breckenridge, Colorado, USA, April 11-15, 2000 [en ligne]. Breckenridge : Morgan Kaufmann Publishers, 2000, pp 471-482. Disponible sur : <http ://citeseer.ist.psu.edu/chalupsky00ontomorph.html> (consulté le 22/05/04)

[Charlet2003] Web sémantique, Jean Charlet, Philippe Laublet and Chantal Reynaud octobre 2003

[Chang2003] Bin HE, Kevin Chen-Chuan CHANG, Jiawei HAN. Automatic Complex schéma Matching across Web Query Interfaces : A Correlation Mining Approach. Technical Report UIUCDCS-R-2003-2388, Department of Computer Science, UIUC, December 2003.

[Cigref2002] Sécurité des systèmes d'information, Quelle politique globale de gestion des risques, Cigref 2002

[CISSP] Official Guide to the CISSP EXAM, Susan Hansche CISSP, John Berti CISSP, Chris Hare CISSP

[CLUSIF1997a] Démarche de conception d'un TB qualité : Comission des méthodes Club de la sécurité des systèmes d'informtions Français , juin 1997

[CLUSIF1997b] Evaluation des consequences Economiques des incendies et sinistres relatifs aux systèmes Informatiques CLUSIF Février 1997

[CLUSIF1996] Rapports 1996, 2000 et 2001 du CLUSIF sur la sinistralité informatique en France

[CNRS2003] Le TB de la sécurité du système d'information CNRS juin 2003

[CNRS1990] Guide de la sécurité des systèmes d'information à l'usage des directeurs - CNRS (Robert Longeon, Jean-Luc Archimbaud 1999)

[Dan2004] Dan Brickley and R. V. Guha, Editors. RDF Vocabulary Description Language 1.0 : RDF schéma, W3C Recommendation, 10 February 2004.http ://www.w3.org/TR/rdf-schéma/

[Dacier 1994] M. Dacier, Vers une évaluation quantitative de la sécurité informatique, Thèse de doctorat, Institut National Polytechnique de Toulouse, N° 971, 154 pp., 20 décembre 1994 (Rapport LAAS 94488).

[Deswarte 2003] Y. Deswarte, La sécurité des systèmes d'information et de communication,in Sécurité des réseaux et des systèmes répartis, (Yves Deswarte et Ludovic Mé, eds), Traité IC2, Hermès, ISBN :

02-7462-0770-2, 264 pp, octobre 2003

[Dekker2001] Auditing Computer and Management Information Systems. in Kent, A. (ed) Encyclopedia of Library and Information Science, Volume 68 Marcel Dekker, 2001

[DCSSI2003] Elaboration de TB SSI : Premier minitre secrétariat général de la défense nationale, direction centrale de la sécurité des systèmes d'information sous la direction des opérations Bureau Conseil.

[DCSSI1994] Guide pour l'élaboration d'une politique de sécurité interne (PSI) à l'usage du responsable de la sécurité du système d'information 15 septembre 1994 DISI/DCSSI/DIS

[Ding2001] ing, Y., et Fensel, D. (2001). Ontology Library Systems : The key for successful Ontology Reuse. Paper présented at the First Semantic Web Working Symposium (SWWS'1), Stanford, USA.

[Djida2006] ne approche hybride de gestion des connaissances basée sur les ontologies : applications aux incidents informatiques, Djida Bahoul, 2006

[Dubois1996] Dubois, J.-C., L'analyse du risque : une approche conceptuelle et systémique, Chènevière-McGrawHill, 1996. ISBN : 2-89461-066-1

[Embley2003] Li XU, David EMBLEY. Using Domain Ontologies to Discover Direct and Indirect Matches for schéma Elements. In : Second International Semantic Web Conference (ISWC- 03), October 20, 2003, Sanibel Island, Florida. CEUR, 2003. Disponible sur : <http ://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS//Vol-82/>

[Favre2005] Cécile Favre, Fadila Bentayeb, Omar Boussaid, Nicolas Nicoloyannis. Entreposage virtuel de demandes marketing : de l'acquisition des objets complexes à la capitalisation des connaissances, EGC'05, paris, 2005.

[Ferrante2002] Fondements d'une politique de sécurité ou sûreté globale des systèmes d'informations au sein d'une grande entreprise. Communication sur la gestion des risques par Fabrice Ferrante, Octobre 2002

[Fernandez1999] Fernandez M., Gomez-Perez A, Pazos J et Pazoz A (1999) Building a chemical ontolgy using methonlogy and the ontology design environment. IEEE Intelligent System and their applications, 37-45

[Farquhar1996] A. Farquhar, R. Fikes, and J. Rice The Ontolingua Server a tool for collaborative ontology construction In Proceedings of the 10 th Knowledge Acquisition for Knowledge Based Systems Workshop (KAW'96), 1996

[Fikes2000] Richard Fikes, Deborah L. McGuinness, James Rice, et al. . An Environment for Merging and Testing Large Ontologies. In : Proceedings of the Seventh International Conference on Principles of Knowledge Representation and Reasoning (KR2000), 12-15 April 2000, Breckenridge, Colorado, USA

[Ghenaouti2000] S. Ghernaouti-Hélie : "Stratégie et protection des systèmes d'information". Flash Informatique - Numéro spécial été 2000, EPFL.

[Ghernaouti2001] S. Ghernaouti - Hélie : " Sécurité informatique et protection des systèmes d'information ". Revue Informatique professionnelle - Gartner group. Septembre 2001.

[Ghernaouti2000] Sécurité Internet. Stratégies et Technologies, S. Ghernaouti-Hélie. Dunod 200o. Page 45 .

[GMSIH2007] ystèmes d'information Décisionnels dans les établissements de santé : analyse de l'offre éditeur au 31/07/2007.

[Gomez1999] òmez-Pérez, A. et M.D. Rojas (1999). Ontological Reengineering and Reuse. European Knowledge Acquisition Workshop (EKAW).]

[Gomez,2000] GOMEZ-PEREZ A. (2000), Développements résents en matière de conception, de maintenance et d'utilisation d'ontologies. Terminologies nouvelles, (19), 9-20 Traduit de l'anglais par S. Descotte

[Gruninger1996] Uschold, M. and Gruninger, M. (1996). Ontologies : Principles, Methods and Applications. Knowledge Engineering Review 11(2).

[Gruber1993] Gruber T. A translation approach to portable ontology specification , knowledge Acquisition, 7, 1993

[Gruber1995] Gruber T. Toward Principles for the Design of Ontologies Used for Knowledge Sharing , In formal ontology in Conceptual Analysis and Knowledge Representation, Guarino N. and Poli R Rds Kluwer cademic Publishers, 1995

[Gruninger1995] Gruninger, M. and Fox, M.S. (1995). Methodology for the Design and Evaluation of Ontologies. In : Proceedings of the Workshop on Basic Ontological Issues in Knowledge Sharing,

Montreal.

[Heflin2000] Heflin, J., et Hendler, J. (2000). Dynamic Ontology on the Web. Paper présented at the AAAI, 17th National Conference on artificial Intelligence.

[Heflin2001] Heflin, J. (2001). Towards the Semantic Web : Knowledge and representation in a dynamic, distributed environment. Faculty of the Graduate School of the University of Maryland.

[Heflin1999] Heflin, J., Hendler, J., et Luke, S. (1999). Coping with Changing Ontologies in a Distributed Environment. Ontology Management. Papers from the AAAI Workshop, 74-79.

[Hendler2001] Hendler, J. (2001). Agents and the Semantic Web. IEEE Intelligent systems, March/April 2001, 30-37.

[Hoffman2006] Appariement Contextuel d'ontologies, Patrick Hoffman Laboratoire d'informatique en images et système d'information , Université Claude Bernard Lyon 1

[Infosec2002] Méthodes publiques de gestion de la sécurité des systèmes d'information infosécurité conseil 24 avril 2002

[ISO17799] Norme Internationale ISO/CEI 17799 Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information

[IEEE1990] IEEE. (1990). IEEE Standard Glossary of Software Engineering Terminology. (No. Std. 610.12-1990). New York (USA) : IEEE Computer Society.

[IEEE1995] IEEE Guide for Software Quality Assurance Planning (No. Std. 730.1-1995). New York (USA). IEEE Computer Society.

[ITSEC1991] ITSEC , Information Technology Security Evaluation Criteria, v 1.2, 136 pp., ISBN 92-826-3005-6, Office des publications officielles des Communautés Européennes, Luxembourg, 1991.

[ISO 15408] Technologies de l'information, Techniques de sécurité, Critères d'évaluation pour la sécurité TI ISO/IEC, 1999

[Kaplan1992] Kaplan R.S. et Norton D.P. (1992), « The balanced scorecard, measures that drive performance », Harvard Business Review. Juanuary-February, pp. 71-79.

[Kaplan1993] Kaplan R.S. et Norton D.P. (1993), « Putting the balanced scorecard to work », Harvard Business Review, septembre-octobre, pp. 134-147.

[Kaplan1996] Kaplan R.S. et Norton D.P. (1996), « Using the balanced scorecard as a strategic management system », Harvard Business Review, juanuary-february, pp.76-85.

[Kaplan1998] Kaplan R.S. et Norton D.P. (1998), Le TB prospectif, les Editions d'Organisation.

[Klein2002a] Klein, M. (2002a). Supporting evolving ontologies on the internet. Paper présented at the Proceedings of the EDBT 2002 PhD Workshop, Prague, Czech Republic.

[Klein2002b] Klein, M. (2002b). Versioning of distributed ontologies (No. Deliverable D20 V1.1, EU/IST Project WonderWeb).

[Klein2002] Klein, M., Ding, Y., Fensel, D., et Omelayenko, B. (2002). Ontology management - Storing, aligning and maintaining ontologies. In J. Davids, D. Fensel et F. vanHarmele (Eds.), Towards the Semantic Web : Ontology-Driven Knowledge Management (pp. 47-69) : Wiley.

[Klein2001] KLEIN M. . Combining and relating ontologies : an analysis of problems and solutions. In : GÓMEZ-PÉREZ A., GRUNINGER M., STUCKENSCHMIDT H. IJCAI-01 Workshop on Ontologies and Information Sharing, August 4-5, 2001. Seattle, USA [en ligne]. Seattle : CEUR, 2001, pp53-62. Disponible sur : <http ://sunsite.informatik.rwth-aachen.de/Publications/CEURWS// Vol-47/>

[Kalfoglou2003] Yannis KALFOGLOU, Marco SCHORLEMMER. Ontology mapping : the state of the art. Knowledge Engineering Review, 2003, issue 2, volume 18, pp 1-31.

[Kraft1999] .D. Preece, K.-J. Hui, W.A. Gray, P. Marti, T.J.M. Bench-Capon, D.M. Jones, and Z.

[Kraft0999] ui. The kraft architecture for knowledge fusion and transformation. In Proceedings of the 19th SGES International Conference on Knowledge-Based Systems and Applied Artificial Intelligence (ES'99). Springer, 1999.

[Lammari2003] Nadira Lammari, Elisabeth Métais(2003) Building and Maintaining Ontologies : a Set of Algorithms - Revue Data and Knowledge Engineering(DKvol.0(0),2003.

[Lamere1991] Lamère JM. Sécurité des systèmes d'information. Paris : Dunod, 1991.

[Lamnari2004] Building and Maintening Ontologies : a set of Algorithms Nadira Lammari, Elisabeth Métais Laboratoire CEDRIC, CNAM, 292 rue Saint Martin 75141 Paris Cedesx 03 France

[Lorens2003] TB de la sécurité réseau , Cédric Lorens , Laurent Levrier octobre 2003

[Lorino2000] Lorino P. (2000), « Le balanced scorecard revisité : dynamique stratégique et pilotage de performance, exemple d'une entreprise énergétique », Congrès de l'Association Française de Comptabilité, Metz, 2000.

[Maedche2001a] aedche, A. and S. Staab (2001). Ontology Learning for the Semantic Web. IEEE Intelligent Systems,Special Issue on the Semantic Web, 16(2) :72 à 79.

[Maedche2001b] aedche, A. and R. Volz (2001). The Text-To-Onto Ontology Extraction and Maintenance Environment.Proceedings of the ICDM Workshop on integrating data mining and knowledge management, San Jose, California, USA.

[MEHARI2004] Méthode Harmonisée d'Analyse de Risques (MEHARI), Principes et mécanismes, CLUSIF, Version 3, Octobre 2004. http ://www.CLUSIF.asso.fr/

[MEHARI2007] MEHARI 2007, Principes et mécanismes, CLUSIF http ://www.CLUSIF.asso.fr/.

[Natalya101] Natalya F. Noy and Deborah L. McGuinness. "Ontology Development 101 : A Guide to Creating Your First Ontology". Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001.

[Noy2001] N. F. Noy, M. A. Musen. Anchor-PROMPT : Using Non-Local Context for Semantic Matching. In : Proceedings of workshop on Ontologies and Information Sharing at the International Joint Conference on Artificial Intelligence (IJCAI), août 2001, Seattle, WA.

[NLDB02] Ontology-Based Data cleaning Zoubida dedad, Elisabeth Métais Conference NLDB'02

[Norreklit2000] Bourguinion A, Malleret V. et Norreklit H (2002) , l'irréductible dimenssion culturelle des instruiments de gestion : l'exemple du TB et du balanced scorecard, comptabilité-contrôle-audit , numéro spécial mai , pp 7-32

[NCITS1998] National Committee for Information Technology Standards, Technical Commettee T2(Information Iterchange and Interpretation), Draft proposed American national standard for knowledege IOnetrchange Format . http :// logic.stanford.edu/kif/dpans.html, 1998

[Observer1996] E. Mena, V. Kashyap, A. Sheth, and A. Illarramendi. Observer : An approach for query processing in global information systems based on interoperability between pre-existing ontologies. In Proceedings 1st IFCIS International Conference on Cooperative Information Systems (CoopIS '96). Brussels, 1996.

[OntoWeb2002a] EC project IST-OntoWeb, from http ://www.ontoweb.org

[OntoWeb2002b] A survey on methodologies for developing, maintaining, evaluating and reengineering ontologies (No. IST-2000-29243 - Deliverable 1.4).

[PSSI2004] Guide pour l'élaboration d'une politique de sécurité de système d'information PSSI version du 3 mars 2004

[Pierra 02] . Pierra, Un modèle formel d'ontologie pour l'ingénierie, le commerce électronique et le Web sémantique : Le modèle de dictionnaire sémantique PLIB , Journées Scientifiques WEB SEMANTIQUE, mParis, 10-11/10/2002.

[Pierra 03] . Pierra, Context-Explication in Conceptual Ontologies : The PLIB Approach , In Proceedings of CE'2003 : Special track on Data Integration in Engineering, 2003.

[Pierra et al. 04] . Pierra, H. Dehainsala, Y. Ait ameur, L. Bellatreche, J. Chochon, M. El-hadj Mimoune, Base de Données à Base Ontologique : le modèle OntoDB , A paraître dans : 20-èmes Journées, Bases de Données Avancées (BDA 2004).

[Pinto2004] into, S., Staab, S., et Tempich, C. (2004). DILIGENT : Towards a fine-grained methodology for Distributed Loosely-controllled and evolvInG Engineering of oNTologies. I. Paper présented at the 16th European Conference on Artificial Intelligence ECAI-2004, Valencia.

[Rogozan2003] Gestion de l'évolution d'une ontologie : méthodes et outils pour un référencement sémantique évolutif fondé sur une analyse des changements entre versions de l'ontologie. Proposition de recherche doctorale en informatique cognitive. Dedia Codruta Rogozan. Télé Université du Quebec

[Reynaud2006] Mapping pour l'intégration de documents XML, Chantal Reynaud, Brigitte Safar Université Paris-Sud XI, CNRS (L.R.I.) and INRIA (Futurs) 91405 Orsay cedex Chantal.Reynaud, safar@lri.fr , http ://www.lri.fr/cr

[Sides2007] Système d'information décisionnels dans les établissements de santé : analyse de l'offre éditeur au 31/07/2007

[Settouti2005] Un système de médiation basé sur les ontologies, Lotfi Sofiane Settouti, 23 juin 2005

[Studer2003] Studer, R. (2003). The Semantic Web : Methods, Applications and Future Trends. Paper présented at the IFIP Conference on commerce, business and government, I3E 2003, Sao Paulo, Brazil.

[Stojanovic2002] Stojanovic, L., et Motik, B. (2002). Ontology Evolution within Ontology Editors. Paper présented at the Knowledge Acquisition, Modeling and Management (EKAW), Siguenza, Spain.

[Subrahmanian1995] Subrahmanian V.S. and Adali S. and Brink A. and Emery R. and Lu J. J. and Rajput A. and Rogers T. J. and Ross R. and Ward C. (1995). HERMES : A heterogeneous reasoning and mediator system. Technical Report. Univ. of Maryland

[Trouessin 2000] G. Trouessin, Towards Trustworthy Security for Healthcare Information Systems, Report N°GT/2000.03, CESSI/CNAM, juin 2000.

[Wache2001] H.Wache, T. Vogele, U. Visser, H. Stuckenschmidt, G. Schuster, H. Neumann, S. Hubner. Ontology-Based Integration A Survey of existing Approches, in proceeding of IJCAI-01 Workshop : Ontologies and information Sharing, Seattle, WA, pp 108-117, 2001.

[WebOnt.2001] OWL Ontology Web Language, from http ://www.w3.org//sw/WebOnt/

[WebOnt2004a] OWL Web Ontology Language Guide and Reference, from

[Wiederhold1992] Wiederhold G. (1992). Mediators in the architecture of future information systems, Computer, Vol. 25(3). p.38-49.

[Ysosecure] Gestion des risques et Organisation de la sécurité, Ysosecure 2003/2005

Annexe A

Grille d'exposition naturelle standard

Evaluation de l'exposition naturelle standard Evaluation de la potentialité des evenements suivants		P=1 Très im probable	P=2 Plutôt im probable	P=3 Plutôt probable	P=4 Très probable	Status- Expo
Accidents						
AC01	Court-circuit au niveau du câblage ou d'un équip		x			2
AC02	Chute de la foudre		x			2
AC03	Incendie naissant ds les locaux : corbeille		x			2
AC04	Accidents du à l'eau ou a des liquide		x			2
AC05	Inondation causée par une canaliosation percée		x			2
AC06	Inondation causée par la crue d'1 rivière		x			2
AC07	Inondation causée par l'extinction d'1 incend. voisin		x			2
AC08	Coupure d'énergie de longue durée		x			2
AC09	Indisponibilité totale des locaux		x			2
Actes malveillants volontaires						
MA01	Vandalisme depuis l'extérieur		x			2
MA02	Vandalisme intérieur		x			2
MA03	Terrorisme sabotage par des agents ext	x				1
MA04	Saturation des moyens informatiques		x			2
MA05	Saturation du réseau par un ver		x			2
MA06	Effacement volontaire de support logiciel		x			3
MA07	Altération malveillante de logiciel			x		3
MA08	Entrée de données fausses			x		3
MA09	Indisponibilité totale des locaux			x		3
Actes volontaires non malveillants						
AV01	Absence de personnel d'exploitation : grève		x			2
AV02	Départ vde personnel stratégique			x		3
AV03	Pénétration du SI d'une tierce société			x		3
Erreurs						
ER01	Dégradation involontaire de performance		x			2
ER02	Effacement acc. de logiciel par erreur humaine			x		2

Annexe B

Définition des niveaux d'exposition naturelle

- **Niveau 1 : L'exposition est très faible** Indépendamment de toute mesure de sécurité, la probabilité d'occurrence d'un tel scénario est extrêmement faible et pratiquement négligeable.

- **Niveau 2 : L'exposition est faible** l'unité est peu exposée. Même en l'absence de toute mesure de sécurité, l'environnement (culturel, humain, géographique) et le contexte (stratégique, concurrentiel, social) font que la probabilité d'occurrence d'un tel scénario, à court ou moyen terme, est faible.

- **Niveau 3 : L'exposition est moyenne** l'unité n'est pas particulièrement exposée, L'environnement et le contexte de l'entreprise font que, si rien n'est fait pour l'empêcher, un tel scénario devrait se produire, à plus ou moins court terme.

- **Niveau 4 : L'exposition est forte** l'unité est particulièrement exposée. L'environnement ou le contexte font que si rien n'est fait, un tel scénario se réalisera sûrement, vraisemblablement à court terme.

Annexe C

Tableau d'impact intrinsèque

Tableau d'impact intrinsèque				
Classification des données , informations et éléments d'infrastructure				
Données et informations		D	I	C
D01	Fichiers de données ou base de données applicatives			
D02	Fichiers bureautiques stockés sur serveur à accès partagés			
D03	Fichiers bureautiques stockés sur postes personnels fixes			
D04	informations écrites ou imprimées détenues par les utilisateurs, archives personnelles		X	
D05	Listings ou états imprimés des applications informatiques	X	X	
Infrastructure informatique et télécom		D	I	C
R01	Équipements et câblage du réseau étendu (systèmes réseau avec leurs logiciels)			X
R02	Équipements et câblage des réseaux locaux (systèmes réseau avec leurs logiciels)			X
R03	Données de configuration du réseau étendu			
R04	Données de configuration des réseaux locaux			
S01	Systèmes centraux, serveurs applicatifs et équipements périphériques centraux,			
S02	Fichiers de configuration des systèmes et serveurs			
S03	Systèmes terminaux mis à la disposition des utilisateurs (PC, imprimantes locales)		X	X
A01	Application logicielle ou progicielle, middleware (code exécutable)			
A02	Code source			
A03	Fichiers de configuration applicatives			
Infrastructure générale		D	I	C
E01	Environnement de travail des utilisateurs			
E02	Équipements de télécommunication orale ou analogique			
Impacts intrinsèques ne dépendant pas de la classification d'une ressource				
Indisponibilité du personnel		D	I	C
P01	Équipes de spécialistes métiers			
P02	Personnel d'exploitation			
Non conformité à la loi ou à la réglementation		D	I	C
C01	Non conformité à la loi ou à la réglementation relatives à la protection de la vie privée			
C02	Non conformité à la loi ou à la réglementation relatives aux contrôles financiers			

Annexe D

Grille d'évaluation standard

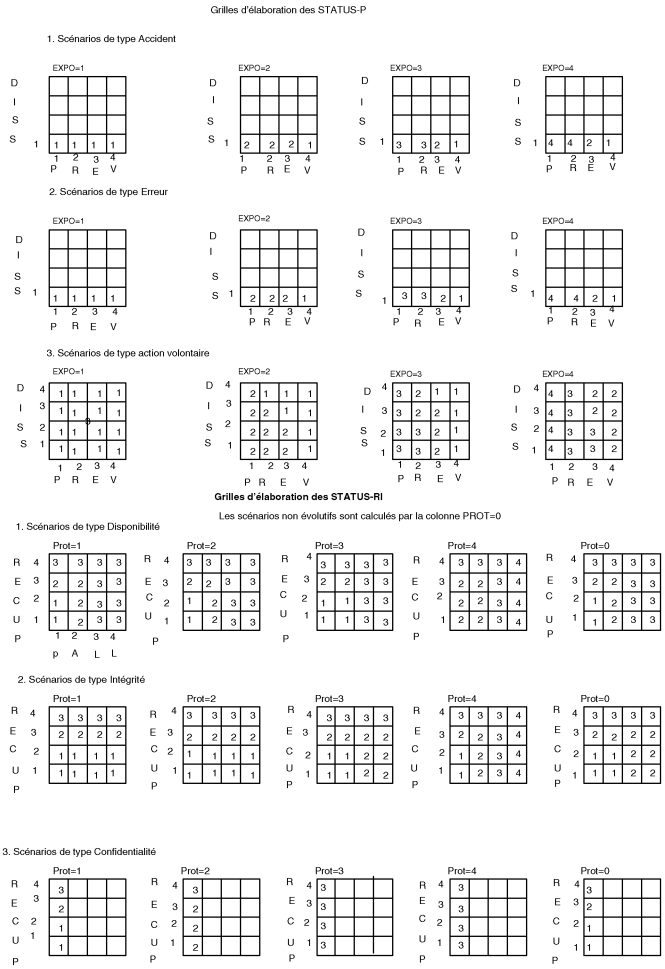

FIG. D.1 – Grille d'évaluation standard

Annexe E

Définition des niveaux de facteurs de réduction de risque

Dissuasion

- Niveau 1 : L'effet dissuasif est très faible ou nul. L'auteur peut logiquement penser qu'il n'encourrait aucun risque personnel : il peut penser qu'il ne serait pas identifié ou qu'il aurait de très sérieux arguments pour réfuter toute imputation de l'action ou que les sanctions seraient très faibles.

- Niveau 2 : L'effet dissuasif est moyen. L'auteur peut logiquement penser qu'il encourrait un risque faible et qu'en tout état de cause les préjudices personnels qu'il aurait à subir resteraient supportables.

- Niveau 3 : L'effet dissuasif est important. Un auteur rationnel devrait logiquement penser qu'il encourt un risque important : il devrait savoir qu'il serait sans doute identifié et que les préjudices qu'il aurait à subir seraient graves.

- Niveau 4 : L'effet dissuasif est très important.

Un auteur rationnel devrait logiquement abandonner toute idée d'action. Il devrait savoir qu'il sera presque certainement démasqué et que les sanctions encourues sont hors de proportion avec le gain espéré.

Prevention

- Niveau 1 : L'effet préventif est très faible ou nul. Toute personne proche ou appartenant à l'entreprise ou tout initié la connaissant un minimum est capable de déclencher un tel scénario, avec des moyens qu'il est facile d'acquérir. Des circonstances tout à fait courantes (maladresse, erreur, conditions défavorables non exceptionnelles) peuvent être à l'origine d'un tel scénario.

- Niveau 2 : L'effet préventif est moyen. Le scénario peut être mis en œuvre par un professionnel sans autres moyens que ceux dont disposent les personnels de la profession. Des circonstances naturelles rares peuvent aboutir à ce résultat

- Niveau 3 : L'effet préventif est important. Seul un spécialiste, un professionnel doté de moyens très importants, ou une collusion entre plusieurs professionnels ayant des domaines différents peuvent aboutir. Concours de circonstances rares ou circonstances exceptionnelles exigées

- Niveau 4 : L'effet préventif est très important.

Protection ou confinement

- Niveau 1 : L'effet de confinement et de limitation des conséquences directes est très faible ou nul. Soit le sinistre ne peut être limité dans ses conséquences directes, soit il ne sera détecté qu'au bout d'un délai important. Les mesures qui peuvent alors être prises n'ont qu'une influence très limitée sur le niveau des conséquences directes.

- Niveau 2 : L'effet de confinement et de limitation des conséquences directes est moyen. Si le sinistre pouvait être limité dans ses conséquences directes, le délai de détection n'est pas rapide et/ou les réactions sont tardives. Les mesures qui peuvent alors être prises ont une influence réelle sur l'impact, mais l'ampleur des conséquences directes reste importante.

- Niveau 3 : L'effet de confinement et de limitation des conséquences directes est important. Le délai de détection est rapide et les réactions sont prises sans délai. Les mesures qui peuvent alors être prises ont une influence réelle sur l'impact direct, qui est réel mais limité et circonscrit.

- Niveau 4 : L'effet est très important. Le début de sinistre est détecté en temps réel et les mesures déclenchées immédiatement Les conséquences directes seront limitées aux détériorations immédiates dues à l'accident, l'erreur ou l'acte volontaire.

Palliation

- Niveau 1 : L'effet de limitation des conséquences indirectes est très faible ou nul. Les mesures seront totalement improvisées et/ou il est probable que leur effet en sera très faible.

- Niveau 2 : L'effet de limitation des conséquences indirectes est moyen. Les solutions de secours ou moyens palliatifs ont été prévus globalement et pour l'essentiel, mais l'organisation de détail n'a pas été faite. Il est probable qu'il résultera de ce manque de préparation un manque d'efficacité très net des

mesures prévues. Le délai de reprise du fonctionnement normal de l'activité ne peut être connu avec précision ou ne changera pas fondamentalement le niveau de gravité du sinistre.

- Niveau 3 : L'effet de limitation des conséquences indirectes est important. Les mesures ont été analysées et organisées dans le détail, puis validées. Le délai de reprise du fonctionnement normal de l'activité peut être estimé ou connu avec précision et est tel que cela réduira notablement la gravité des conséquences indirectes du scénario.

- Niveau 4 : L'effet de limitation des conséquences indirectes est très important. Le fonctionnement normal de l'activité est assuré sans discontinuité notable.

Recuperation

- Niveau 1 : L'effet de récupération est très faible ou nul. Ce que l'organisation peut espérer récupérer de l'assurance ou d'un recours en justice est négligeable comparé à l'impact global du scénario et de ses conséquences
- Niveau 2 : L'effet de récupération est moyen. Ce que l'organisation peut espérer récupérer n'est pas négligeable, mais la majeure partie de l'impact du scénario reste à la charge de l'entreprise. Il n'est pas sûr que pour un sinistre majeur, le transfert de risque soit suffisant pour permettre la poursuite de l'activité.
- Niveau 3 : L'effet de récupération est important. L'assurance et/ou le recours en justice permettront d'atténuer notablement l'impact du scénario et, en tout état de cause, de poursuivre l'activité. L'impact résiduel sera au maximum très grave, sans atteindre le niveau « Vital »
- Niveau 4 : L'effet de récupération est très important. Quelle que soit l'importance du sinistre, l'impact résiduel sera supportable (niveau 2).

Sources MEHARI 2007

Annexe F

Principes de construction des grilles d'évaluation des STATUS

Les principes ci-dessous sont ceux qui ont été retenus pour élaborer les grilles faisant passer des STATUS détaillés aux STATUS globaux, STATUS-P et STATUS-RI.

Grille d'évaluation du STATUS-P

Les rationnels suivants peuvent être avancés :

- L'exposition naturelle ayant été définie comme une évaluation de la potentialité intrinsèque, en dehors de toute autre mesure, STATUS-P vaut au plus STATUS-EXPO (en l'absence de toute autre mesure, c'est-à-dire si STATUS-DISS et STATUS-PREV valent tous les deux 1)

- Si STATUS-PREV vaut 3 ou 4, pour des accidents ou des erreurs ; alors STATUS-P vaut au plus 2 ou 1, respectivement

- Si STATUS-PREV vaut 4, pour un acte volontaire ; alors STATUS-P vaut au plus 2

- Si STATUS-PREV vaut 4, pour un acte volontaire ; et si l'exposition est inférieure ou égale à 3, alors STATUS-P vaut 1

Grille d'évaluation du STATUS-RI

Les rationnels suivants peuvent être avancés :

- Si STATUS-RECUP vaut 3, alors STATUS-RI vaut au moins 2

- Si STATUS-RECUP vaut 4, alors STATUS-RI vaut au moins 3

- Si STATUS-PALL vaut 3 ou 4, pour des scénarios de disponibilité, alors STATUS-RI vaut au moins 3 (les plans de secours étant bons, l'impact résultant ne peut être grave)

- Si STATUS-PROT vaut 4 dans un scénario d'intégrité, l'impact peut être fortement réduit s'il est possible de restaurer rapidement (la ressource altérée) et alors STATUS-RI est aligné sur le STATUS-PALL qui, dans ce cas traite de la restauration

- Si STATUS-PROT vaut 3 dans un scénario d'intégrité et s'il est possible de restaurer rapidement (STATUS-PALL = 3 ou 4), le pire aura sans doute été évité mais cela peut quand même être grave : STATUS-RI = 2, alors que, s'il n'est pas possible de restaurer rapidement (STATUS-PALL = 1 ou 2), rien n'est atténué : STATUS-RI = 1

- Si STATUS-PROT vaut 1 ou 2 pour un scénario d'intégrité, alors STATUS-RI vaut 1 sauf action du STATUS-RECUP (la protection est faible, il n'y a pas de mesure véritablement palliative, car celles-ci ne sont constituées que de mesures de restauration qui n'ont pas d'effet sur les conséquences indirectes, seules jouent donc les mesures de restauration).

Annexe G

Expression des besoins de sécurité

Il consiste à évaluer les besoins consolidés et à les classer après avoir évalué la gravité d'un ensemble de situations de risque en s'appuyant sur un diagnostic de l'état des services de sécurité. Cette approche est basée sur la définition de « besoins de service » décrite ci-dessous.

Besoins de services

Un besoin de service de sécurité est établi pour chaque scénario, en s'appuyant sur les principes suivants. Besoin de service relatif à un scénario donné Un service de sécurité donné peut avoir un effet sur la gravité d'un scénario. Si tel est le cas, il est considéré qu'il existe, pour ce service, et du fait de ce scénario, un besoin de service. Quantitativement, ce besoin de service sera d'autant plus important que :

- son influence (traduite par son coefficient d'influence), pour ce scénario, sera forte ;
- la gravité du scénario considéré sera élevée ;
- la qualité actuelle du service sera faible.

Ainsi, pour un service i face à un scénario k, le besoin de service sera calculé par la formule :
$BSik = eik.b^{Gk}.(4 - \sigma i)$
dans laquelle $BSik$= besoin de service pour le service i face au scénario k
eik = coefficient d'influence du service i pour le scénario k
b= base générale paramétrable
Gk= gravité du scénario k
σi= qualité du service i, $(4 - \sigma i$en étant donc le complément à 4)
Le coefficient d'influence « e », de valeur comprise entre 0 et 16 traduit le degré d'influence du service sur le scénario.

$eik = \alpha ik.\beta ik$ Détermination de αik si le service n'est appelé que par un type de mesure :
Si le service est le seul appelé pour le type de mesure considéré $\alpha ik = 2$
Si le service est appelé par une formule de type min($servA$;$servB$), $\alpha ik = 2$
Si le service est appelé par une formule de type max. ($servA$;$servB$), $\alpha ik = 1$
Dans le cas d'une formule complexe, seule est prise en compte la fonction (« min » ou « max. ») ayant comme argument direct le numéro de service considéré. Détermination des βik
Si le service i est appelé comme :
mesure dissuasive pour le scénario k, $\beta ik = 4$
mesure préventive pour le scénario k, $\beta ik = 8$
mesure de protection pour le scénario k, $\beta ik = 4$
mesure palliative pour le scénario k , $\beta ik = 8$
mesure de récupération pour le scénario k, $\beta ik = 2$
$BSi = \sum k = 1BSik$
Si le service est appelé par plusieurs types de mesures, un coefficient d'influence sera calculé pour chaque type de mesure et le coefficient d'influence le plus élevé sera retenu. Le paramètre b qui sert de base pour tenir compte de la gravité de chaque scénario a une grande influence sur le résultat :

- une valeur de 2 minimise l'effet de la gravité des scénarios

- il est généralement considéré qu'une valeur de 8 est une bonne option

La synthèse des besoins de service
La synthèse des besoins de service BSi , pour un service i donné, sera évaluée par simple sommation :
$BSi = \sum k = 1BSik$
Le besoin de service BSi ainsi obtenu est d'autant plus important que le service a été demandé par de nombreux scénarios, que ces scénarios étaient graves et que le service peut avoir une influence directe sur la gravité des scénarios.

Annexe H

Code source tableau de bord sécurité dynamique

```
import java.awt.* ;
import java.awt.event.* ;
import java.util.* ;
import javax.swing.* ;
import test.GraphPanel ;
import test.Indicator ;
import test.IndicatorPanel ;
import test.LegendPanel ;
import test.TestBox ;
import edu.stanford.smi.protege.model.* ;
import edu.stanford.smi.protege.widget.* ;
import edu.stanford.smi.protege.resource.* ;
/*Classe de base permettant de tout mettre ensemble et de se connecter avec ONTOSEC */
public class FrameCounter extends AbstractTabWidget implements ActionListener
private static final int MAX_FRAMES = 200 ;
private JTextField field ;
private JButton allIndicators ;
private IndicatorPanel indicatorPanel ;
private GraphPanel graphPanel ;
private LegendPanel legendPanel ;
public void initialize()
setLabel("Ontology Project") ;
System.out.println("je suis le meilleur") ;
initComponents() ;
button.addActionListener(new ActionListener()
public void actionPerformed(ActionEvent event)
// update text field
int count = getKnowledgeBase().getClsCount() ;
field.setText(String.valueOf(count)) ;
Collection col = getKnowledgeBase().getClses() ;
Iterator it = col.iterator() ;
while(it.hasNext())
System.out.println(((Cls)it.next()).getName())  ) ;
// create the output text field
field = new JTextField(10) ;
field.setEnabled(false) ;
field.setHorizontalAlignment(SwingConstants.RIGHT) ;
// add the components to the tab widget
setLayout(new FlowLayout()) ;
add(button) ;
add(field) ;
add(new JButton("Fenomene")) ;
Collection col = getKnowledgeBase().getClses() ;
Cls cls = null ;
Iterator it = col.iterator() ;
while(it.hasNext())
```

```
cls = (Cls)it.next() ;
if(cls.getName().equals("Library"))
System.out.println("trouve") ;
break ;
System.out.println("LA CLASSE :–+ cls.getName()")
Cls ins = getKnowledgeBase().getCls("Library") ;
Collection
colInstance = getKnowledgeBase().getInstances(ins) ;
Iterator it2 = colInstance.iterator() ;
while(it2.hasNext())
Instance instance = (Instance)it2.next() ;
System.out.println(",,,"+instance+" ; ; ;"+this) ;
Collection colSlot = instance.getOwnSlots() ;
Iterator it3 = colSlot.iterator() ;
while(it3.hasNext())
Slot slot = (Slot)it3.next() ;
System.out.println(slot.getName()) ;
if(slot.getName().equals("issues"))
Collection list = instance.getDirectOwnSlotValues(slot) ;
Object slotValue = instance.getDirectOwnSlotValue(slot) ;
System.out.println("LA VRAI VALEUR"+slotValue) ;
Iterator itValue = list.iterator() ;
while(itValue.hasNext())
//String value = (String)itValue.next() ;
System.out.println("LA VALEUR : "+itValue.next()) ;*/
Cls ins = getKnowledgeBase().getCls("Library") ;
System.out.println(" : : :"+ ins.getName())
/*public static boolean isSuitable(Project project, Col-
lection errors)
boolean isSuitable ;
if (project.getKnowledgeBase().getFrameCount() > MAX-
FRAMES)
isSuitable = false ;
String text = "Project too big, max=" + MAXFRAMES
+ " frames" ;
errors.add(text) ;
else
isSuitable = true ;
return isSuitable ;*/
/*This method is called from within the constructor to
initialize the form */.
<editor-fold defaultstate="collapsed" desc=" Genera-
ted Code ">
private void initComponents()
Définit une taille pour celle-ci ; ici, 400 px de large et
500 px de haut
this.setSize(400, 500) ;
/* Nous allons maintenant dire à notre objet de se po-
sitionner au centre */
allIndicators = new JButton("View all indicators") ;
allIndicators.addActionListener(this) ;
allIndicators.setPreferredSize(new Dimension(20, 20)) ;
allIndicators.setMargin(new Insets(6, 6, 6, 6)) ;
graphPanel = new GraphPanel() ;
graphPanel.setLayout(new BorderLayout(6, 6)) ;
legendPanel = new LegendPanel() ;
graphPanel.setIndicatorPanel(indicatorPanel) ;
indicatorPanel = new IndicatorPanel(graphPanel, le-
gendPanel) ;
Indicator.setFrame(this) ;
addComponents() ;
setVisible(true) ; </editor-fold>


public void addComponents()
JPanel conten = new JPanel() ;
conten.setLayout(new BorderLayout(6, 6)) ;
JPanel panNord = new JPanel() ;
panNord.setLayout(new GridLayout(1, 2, 6, 6)) ;
JPanel panNordOuest = new JPanel() ;
panNordOuest.setLayout(new BorderLayout(6, 6)) ;
panNordOuest.setBorder(BorderFactory.createTitledBorder(
BorderFactory.createEmptyBorder())) ;
JPanel panIndButton = new JPanel(new BorderLayout(6,
6)) ;
panIndButton.add(allIndicators, BorderLayout.WEST) ;
```

```
panNordOuest.add(panIndButton, "North") ;
panNordOuest.add(legendPanel) ;
panNord.add(panNordOuest) ;
panNord.add(indicatorPanel) ;
conten.add(panNord) ;
conten.add(graphPanel, "South") ;
this.add(conten) ;

// this method is useful for debugging
public static void main(String[] args)
edu.stanford.smi.protege.Application.main(args) ;
public void actionPerformed(ActionEvent arg0)
// TODO Auto-generated method stub
graphPanel.setAllIndicators(true) ;
graphPanel.setSomeIndicators(false) ;
graphPanel.repaint() ;
legendPanel.setPaintAll(true) ;
legendPanel.setSomethingToPaint(false) ;
legendPanel.repaint() ;

package test ;
import java.awt.BorderLayout ;
import java.awt.Color ;
import java.awt.Dimension ;
import java.awt.Font ;
import java.awt.Graphics ;
import java.util.Collection ;
import java.util.Iterator ;
import edu.stanford.smi.protege.model.* ;
import edu.stanford.smi.protege.widget.* ;


    import javax.swing.BorderFactory ;
import javax.swing.JCheckBox ;
import javax.swing.JPanel ;


    import edu.stanford.smi.protege.model.Cls ;
import examples.tabwidget.FrameCounter ;
/* Panneau permettant representer graphiquement les
indicateurs par des diagrammes la taille
et la couleur de ceux-ci dependent de leur valeur */
public class GraphPanel extends JPanel
private Boolean allIndicators ;
private boolean someIndicators ;
public GraphPanel()
allIndicators = false ;
someIndicators = false ;
setLayout(new BorderLayout(6, 6)) ;
setPreferredSize(new Dimension(400, 200)) ;
setBorder(BorderFactory.createCompoundBorder(
BorderFactory.createTitledBorder(
BorderFactory.createLineBorder(Color.darkGray),
" Indicators View "),
BorderFactory.createEmptyBorder(0, 6, 6, 6))) ;
/*Permet de representer graphiquement les indicateur
selon que c'est tous les indicateurs que l'on veut voir
ou une partie d'entre eux */
public void paintComponent(Graphics g)
int rank = 1 ;
int begin = 60 ;
g.setColor(this.getBackground()) ;
g.fillRect(18, 20, 1000, 170) ;
g.setColor(Color.BLACK) ;
drawRepere(g) ;
if(allIndicators)
//paint the graph according to the array of indicators
we have
for(int i = 0 ; i < Utilities.indicators.length ; ++i)
System.out.println("L'ind : "+Utilities.indicators[i].getName()) ;
int valeur = Utilities.indicators[i].calculerValeur() ;
System.out.println("LA VALEUR ind : "+valeur ) ;
paintIndicator(g, begin, valeur, rank) ;
rank++ ;
begin += 20 ;
someIndicators = false ;
if(someIndicators)
for(int i = 0 ; i < Utilities.indicators.length ; ++i)
```

```
if(Utilities.indicators[i].getBox().isSelected())
System.out.println("L'ind : "+Utilities.indicators[i].getLevel()
) ;
int valeur = Utilities.indicators[i].calculerValeur() ;
paintIndicator(g, begin, valeur, rank) ;
System.out.println("LA VALEUR ind : "+valeur ) ;
rank++ ;
begin += 20 ;
allIndicators = false ;
/*methode dessinant le repere du graph @param g */
public void drawRepere(Graphics g)
g.fillRect(50, 20, 2, 150) ;
g.fillRect(50,170, 800, 2) ;
g.drawString("25", 20, 149) ;
g.drawLine(48, 145, 52, 145) ;
g.drawString("50", 20, 124) ;
g.drawLine(48, 120, 52, 120) ;
g.drawString("75", 20, 99) ;
g.drawLine(48, 95, 52, 95) ;
g.drawString("100", 20, 74) ;
g.drawLine(48, 70, 52, 70) ;


    /* Méthode de dessiner l'indicateur sur le graph
selon sa valeur
@param g
@param begin
@param valeur
@param rank */
public void paintIndicator(Graphics g, int begin, int
valeur, int rank)
setColor(g, valeur) ;
g.fillRect(begin, 170-(int)valeur, 15, (int)valeur) ;
g.setColor(Color.BLACK) ;
g.drawString(""+rank, begin+3 , 185) ;
/** changer la couleur courant pour dessiner
@param g
@param value */
public void setColor(Graphics g, double value)
if(0< value and value < 50) g.setColor(Color.RED) ;
if(50<= value and value <= 70) g.setColor(Color.ORANGE) ;
if(value >70) g.setColor(Color.GREEN) ;
public Boolean getAllIndicators()
return allIndicators ;
public void setAllIndicators(Boolean allIndicators)
this.allIndicators = allIndicators ;
public boolean isSomeIndicators()
return someIndicators ;
public void setSomeIndicators(boolean someIndicators)
this.someIndicators = someIndicators ;
package test ;
import java.util.Collection ;
import java.util.Iterator ;
import javax.swing.JCheckBox ;
import edu.stanford.smi.protege.model.Cls ;
import edu.stanford.smi.protege.model.Instance ;
import edu.stanford.smi.protege.model.Slot ;
import examples.tabwidget.FrameCounter ;
/** @author Lambert SONNA MOMO
Classe permettant d'instancier les indicateurs, les in-
dicateurs sont de trois niveaux,1, 2 et 3 */
public class Indicator
//Nom de l'indicateur
private String name ;
//Nom interne
private String internalName ;
//Menace liée à l'indicateur
private Instance risque ;
//Mesure contre la menace
private Instance mesure ;
//Niveau de l'indicateur, trois niveaux possible, 0, 1, 2
private int level ;
//Valeur de l'indicateur, determine le niveau de secu-
rité de l'indicateur
private int valeur ;
//chaque indicateur a un checkbox
private JCheckBox box ;
```

```
//indicateurs associés
private String []children ;
//indicateur parent
private String parent ;
//une instance du frameCounter, permettant d'appeler
les methode de la librairie protege
private static FrameCounter frame ;
/*Constructeur
@param menace
@param mesure
@param level*/
public Indicator(String name, String internalName, int
level, String parent, String [] children)
this.name = name ;
this.internalName = internalName ;
this.level = level ;
this.parent = parent ;
this.children = children ;
box = new JCheckBox(name) ;
public int getLevel()
return level ;
public void setLevel(int level)
this.level = level ;
public Instance getRisque()
return risque ;
public void setRisque(Instance risque)
this.risque = risque ;
public Instance getMesure()
return mesure ;
public void setMesure(Instance mesure)
this.mesure = mesure ;
public int getValeur()
return valeur ;
public void setValeur(int valeur)
this.valeur = valeur ;
public String getName()
return name ;
public void setName(String name)
this.name = name ;
public JCheckBox getBox()
return box ;
public void setBox(JCheckBox box)
this.box = box ;
public String[] getChildren()
return children ;
public void setChildren(String[] children)
this.children = children ;
public FrameCounter getFrame()
return frame ;
public static void setFrame(FrameCounter frameC)
frame = frameC ;
/* methode recursive permettant de calculer la valeur
d'un indicateur, en pourcent
@return */
public int calculerValeur()
int valeur = 0 ;
//Condition d'arret de la recursion
if(level == 2)
//indicateur de niveau 2, on recupere la classe liée à
l'indicateur pere
Cls cls = frame.getKnowledgeBase().getCls(parent) ;
Collection colInstance = frame.getKnowledgeBase().getInstances(cls) ;
Iterator it2 = colInstance.iterator() ;
while(it2.hasNext())
//System.out.println("c bon !"+((Instance)it2.next()).getName()) ;
//System.out.println("ca marche !"+((Instance)it2.next()).getName()) ;
Instance instance = (Instance)it2.next() ;
//On recupere l'instance liée l'indicateur
if(instance.getName().equals(internalName))
Collection colSlot = instance.getOwnSlots() ;
Iterator it3 = colSlot.iterator() ;
System.out.println("c bon : "+((Slot)it3.next()).getName()) ;
while(it3.hasNext())
Slot slot = (Slot)it3.next() ;
//On recupère la mesure associée à l'indicateur
if(slot.getName().equals("mesureassocie"))
```

```
System.out.println("ca marchesd") ;
Collection list=instance.getDirectOwnSlotValues(slot) ;
mesure = (Instance)instance.getDirectOwnSlotValue(slot) ;
Iterator itValue = list.iterator() ;
while(itValue.hasNext())
//String value = (String)itValue.next() ;
System.out.println("La val : "+itValue.next()) ;
//On recupère la risque associée à l'indicateur
if(slot.getName().equals("risqueassocie"))
System.out.println("ca marche") ;
Collection list = instance.getDirectOwnSlotValues(slot) ;
risque = (Instance)instance.getDirectOwnSlotValue(slot) ;
Iterator itValue = list.iterator() ;
while(itValue.hasNext())
//String value = (String)itValue.next() ;
System.out.println("La val : "+itValue.next()) ;
elsecontinue ;
//calcul de la valeur en fonction du risque et de la mesure liés à l'indicateur
valeur = calculerValeur(risque, mesure) ;
//si pas condition d'arret
if(level == 1 || level == 0)
Indicator ind = null ;
for(int i = 0 ; i < children.length ; ++i)
System.out.println(children[i]) ;
ind = getIndicator(children[i]) ;
valeur += ind.calculerValeur() ;
System.out.println("- "+valeur) ;
valeur = (int)Math.ceil(valeur/children.length) ;
return valeur ;
/*methode permettant de la calculer la valeur effective de l'indicateur
en fonction du risque et de la mesure associés.
@param risque
@param mesure
@return*/
public int calculerValeur(Instance risque, Instance mesure)
int[] risqueValues = getAttribute(risque, 2) ;
int[] mesureValue = getAttribute(mesure, 1) ;
System.out.println("»"+risqueValues[0]+" : "+ risqueValues[1]+" : "+mesureValue[0]) ;
int gravite = gravity(risqueValues[0], risqueValues[1]) ;
int valeur = getPourcentageValeur(mesureValue[0], gravite) ;
return valeur ;
/* Méthode permettant de recuperer les attributs d'une instance dans le projet protege
en l'occurence l'efficacité pour une mesure, et l'impact et la potentialité pour un risque
@param instance
@param len
@return*/
public int[] getAttribute(Instance instance, int len)
int [] values = new int[len] ;
System.out.println("ca marchehhjj !"+instance.getName()) ;
Collection colSlot = instance.getOwnSlots() ;
Iterator it2 = colSlot.iterator() ;
while(it2.hasNext())
Slot slot = (Slot)it2.next() ;
System.out.println(slot.getName()) ;
if(slot.getName().equals("impact"))
Collection list = instance.getDirectOwnSlotValues(slot) ;
values[0] =
Integer.parseInt(instance.getDirectOwnSlotValue(slot).toString()) ;
System.out.println("LA VALEUR sur : "+instance.getDirectOwnSlotV
Iterator itValue = list.iterator() ;
while(itValue.hasNext())
//String value = (String)itValue.next() ;
System.out.println("LA VALEUR sur : "+itValue.next()) ;

if(slot.getName().equals("potentialite"))
Collection list = instance.getDirectOwnSlotValues(slot) ;
values[1] = Integer.parseInt(instance.getDirectOwnSlotValue(slot).toS
Iterator itValue = list.iterator() ;
while(itValue.hasNext())
```

```
String value = (String)itValue.next() ;
System.out.println("LA VALEUR : "+itValue.next()) ;

if(slot.getName().equals("efficacite"))
Collection list = instance.getDirectOwnSlotValues(slot) ;
values[0] = Integer.
parseInt(instance.getDirectOwnSlotValue(slot).toString()) ;
Iterator itValue = list.iterator() ;
while(itValue.hasNext())
String value = (String)itValue.next() ;
System.out.println("LA VALEUR : "+itValue.next()) ;
return values ;
/* Méthode permettant de calculer la gravité d'un risque
en focntion de son impact
et de sa potentialité
@param impact
@param poten
@return*/
public int gravity(int impact, int poten)
int gravity = 0 ;
if(impact == 1) {
if(poten ==4)
gravity = 3
else gravity = 1
if(impact == 2)
if(poten == 1)gravity = 1
if(poten == 2)gravity = 2
if(poten == 3 || poten == 4)gravity = 3
if(impact == 3)
if(poten == 1)
gravity = 2 ;
if(poten == 2 || poten == 3)
gravity = 3 ;
if(poten == 4)gravity = 4 ;
if(impact == 4)
if(poten == 1 || poten == 2)
gravity = 3 ;
if(poten == 3 || poten == 4)
gravity = 4 ;
return gravity ;
/* Méthode permettant de calculer la valeur d'un indi-
cateur en pourcent, en fonction
de l'efficacité de la mesure et de la gravité du risque
@param effic
@param gravite
@return
*/
public int getPourcentageValeur(int effic, int gravite)
int value = 0 ;
if(effic < gravite)value = 40 ;
else
if(effic > gravite)
value = 90 ;
elsevalue = 70 ;
return value ;
/* Retourne un indicateur en fonction de son nom
@param name
@return */ public Indicator getIndicator(String name)
Indicator ind = null ;
for(int i = 0 ; i < Utilities.indicators.length ; ++i)
if(Utilities.indicators[i].getName().equals(name))
ind = Utilities.indicators[i] ;
return ind ;
/* NewJPanel.java
Created on 28 août 2008, 01 :40 */
package test ;
import java.awt.Color ;
import java.awt.event.ActionEvent ;
import java.awt.event.ActionListener ;
import javax.swing.BorderFactory ;
import javax.swing.JButton ;
import javax.swing.JCheckBox ;


    /* Panneau content tous les checkbox pourles in-
    dicateurs et un bouton permettant
    de vusualiser ceux que l'on aura selectionnés */
```

```
public class IndicatorPanel extends javax.swing.JPanel
implements ActionListener
/** Creates new form NewJPanel */ public Indicator-
Panel(GraphPanel graphPanel, LegendPanel legendPa-
nel)
setBorder(BorderFactory.createCompoundBorder(
BorderFactory.createTitledBorder(
BorderFactory.createLineBorder(Color.darkGray),
" Indicators "),
BorderFactory.createEmptyBorder(0, 6, 6, 6))) ;
this.graphPanel = graphPanel ;
this.legendPanel = legendPanel ;
initComponents() ;
/* This method is called from within the constructor
to
initialize the form.
WARNING : Do NOT modify this code. The content
of this method is
always regenerated by the Form Editor. */
<editor-fold defaultstate="collapsed" desc=" Genera-
ted Code ">
private void initComponents()
jLabel1 = new javax.swing.JLabel() ;
view = new JButton() ;
view.addActionListener(this) ;
for(int i = 0 ; i < 10 ; ++i)
boxes[i] = Utilities.indicators[i].getBox() ;
boxes[0].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[0].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[1].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[1].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[2].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[2].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[3].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[3].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[4].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[4].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[5].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[5].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[6].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[6].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[7].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[7].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[8].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[8].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
boxes[9].setBorder(javax.swing.BorderFactory.
createEmptyBorder(0, 0, 0, 0)) ;
boxes[9].setMargin(new java.awt.Insets(0, 0, 0, 0)) ;
view.setText("View") ;
jLabel1.setText("Cocher les indicateurs que vous vou-
lez visualiser") ;
javax.swing.GroupLayout layout = new javax.swing.
GroupLayout(this) ;
this.setLayout(layout) ;
layout.setHorizontalGroup(
layout.createParallelGroup(javax.swing.
GroupLayout.Alignment.LEADING)
.addGroup(javax.swing.GroupLayout.Alignment.
TRAILING, layout.createSequentialGroup()
.addContainerGap()
.addGroup(layout.createParallelGroup(javax.swing.
GroupLayout.Alignment.TRAILING)
.addComponent(view)
.addComponent(jLabel1))
.addGap(147, 147, 147))
.addGroup(layout.createSequentialGroup()
.addContainerGap()
```

```
.addGroup(layout.createParallelGroup(javax.swing.
GroupLayout.Alignment.LEADING)
.addGroup(layout.createSequentialGroup()
.addGap(17, 17, 17)
.addGroup(layout.createParallelGroup(javax.swing.
GroupLayout.Alignment.LEADING)
.addGroup(layout.createSequentialGroup()
.addGap(17, 17, 17)
.addGroup(layout.createParallelGroup(javax.swing.
GroupLayout.Alignment.TRAILING)
.addComponent(boxes[3])
.addComponent(boxes[2])
.addComponent(boxes[5])
.addComponent(boxes[6])
.addComponent(boxes[8])
.addComponent(boxes[9])))
.addGroup(layout.createSequentialGroup()
.addGroup(layout.createParallelGroup(javax.swing.
GroupLayout.Alignment.LEADING)
.addComponent(boxes[1])
.addComponent(boxes[7])
.addComponent(boxes[4]))
.addPreferredGap(javax.swing.LayoutStyle.
ComponentPlacement.
RELATED, 17, javax.swing.GroupLayout.
PREFERREDSIZE))))
.addGroup(layout.createSequentialGroup()
.addComponent(boxes[0])
.addPreferredGap(javax.swing.LayoutStyle.
ComponentPlacement.
RELATED, 34, javax.swing.GroupLayout.PREFERREDSIZE))
.addContainerGap(273, Short.MAXVALUE))
) ;
layout.setVerticalGroup(
layout.createParallelGroup(
(javax.swing.GroupLayout.Alignment.
LEADING).addGroup(layout.createSequentialGroup()
.addContainerGap()
.addComponent(jLabel1)
.addPreferredGap(javax.swing.LayoutStyle.(
ComponentPlacement.
RELATED).addComponent(boxes[0])
.addPreferredGap(javax.swing.LayoutStyle.(
ComponentPlacement.
RELATED).addComponent(boxes[1])
.addPreferredGap(javax.swing.LayoutStyle.
ComponentPlacement.
RELATED).addComponent(boxes[2])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED).addComponent(boxes[3])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED).addComponent(boxes[4])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED).addComponent(boxes[5])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED).addComponent(boxes[6])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED).addComponent(boxes[7])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED).addComponent(boxes[8])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED).addComponent(boxes[9])
.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.
RELATED, 30, Short.MAXVALUE).addComponent(view)
.addGap(13, 13, 13))) ; // </editor-fold>
// Variables declaration - do not modify private ja-
vax.swing.JButton view ;
private javax.swing.JLabel jLabel1 ;
// End of variables declaration
private JCheckBox[] boxes = new JCheckBox[10] ;
private GraphPanel graphPanel ;
private LegendPanel legendPanel ;


    public void actionPerformed(ActionEvent arg0)
graphPanel.setSomeIndicators(true) ;
graphPanel.setAllIndicators(false) ;
```

```
graphPanel.repaint() ;
legendPanel.setSomethingToPaint(true) ;
legendPanel.setPaintAll(false) ;
legendPanel.repaint() ;
public void setGraphPanel(GraphPanel graphPanel)
this.graphPanel = graphPanel ;
public JCheckBox[] getBoxes()
return boxes ;
package test ;
import java.awt.Color ;
import java.awt.Graphics ;
import javax.swing.BorderFactory ;
import javax.swing.JPanel ;
public class LegendPanel extends JPanel
private boolean somethingToPaint ;
private boolean paintAll = false ;
public LegendPanel()
somethingToPaint = false ;
setBorder(BorderFactory.createCompoundBorder(
BorderFactory.createTitledBorder(
BorderFactory.createLineBorder(Color.darkGray),
" Legend "),
BorderFactory.createEmptyBorder(0, 6, 6, 6))) ;

public void paintComponent(Graphics g)
int count = 1 ;
int beginX = 30 ;
int beginY = 50 ;
g.setColor(this.getBackground()) ;
g.fillRect(20, 20, 600, 400) ;
g.setColor(Color.BLACK) ;
if(somethingToPaint)


    for(int i = 0 ; i < Utilities.indicators.length ; ++i)
if(Utilities.indicators[i].getBox().isSelected())
g.drawString(count+". "+Utilities.indicators[i].
getName(),beginX , beginY) ;
count++ ;
beginY += 20 ;

paintAll = false ;

if(paintAll)
for(int i = 0 ; i < Utilities.indicators.length ; ++i)
g.drawString(count+". "+Utilities.indicators[i].getName(),beginX
, beginY) ;
count++ ;
beginY += 20 ;

somethingToPaint = false ;
public boolean isSomethingToPaint()
return somethingToPaint ;
public void setSomethingToPaint(boolean something-
ToPaint)
this.somethingToPaint = somethingToPaint ;
public boolean isPaintAll()
return paintAll ;
public void setPaintAll(boolean paintAll)
this.paintAll = paintAll ;
package test ;
import java.util.HashMap ;
import javax.swing.JPanel ;
public class Utilities
static String [] ind1Children = "ControleAccesAppli-
catifs", "ControleIntegriteDonnees", "ControleEmission-
ReceptionDonnees" ;
static String [] ind2Children = "Authentification accé-
dants", "Profils accès données applicatives" ;
static String [] ind3Children = "Controle de saisie des
données", "Intégrité des données échangées" ;
static String [] ind4Children = "Accusé de reception",
"Signature électronique" ;
static String [] ind5Children = ;
static String [] ind6Children = ;
static String [] ind7Children = ;
static String [] ind8Children = ;
```

```
static String [] ind9Children = ;
static String [] ind10Children = ;
public static Indicator [] indicators = new Indicator("Securite
Applicative", "", 0, "", ind1Children),
new Indicator("ControleAccesApplicatifs", "", 1, "Se-
curite Applicatice", ind2Children),
new Indicator("Authentification accédants", "theseon-
tologieInstance", 2, "ControleAccesApplicatifs", ind5Children),
new Indicator("Profils accès données applicatives", "the-
seontologieInstance", 2, "ControleAccesApplicatifs",
ind6Children),
new Indicator("ControleIntegriteDonnees", "", 1, "Se-
curite Applicatice", ind3Children),
new Indicator("Controle de saisie des données", "the-
seontologieInstance", 2, "ControleIntegriteDonnees",
ind7Children),
new Indicator("Intégrité des données échangées", "the-
seontologieInstance", 2, "ControleIntegriteDonnees",
ind8Children),
new Indicator("ControleEmissionReceptionDonnees",
"", 1, "Securite Applicatice", ind4Children),
new Indicator("Accusé de reception", "theseontologieInst",
2, "ControleEmissionReceptionDonnees", ind9Children),
new Indicator("Signature électronique", "theseontolo-
gieInst", 2, "ControleEmissionReceptionDonnees", ind10Children) ;
```

Annexe I

Liste des classes de ONTOSEC

< ?xml version="1.0" ?>
<rdf :RDF
xmlns :rdf="http ://www.w3.org/99/02/22-rdf-syntax-ns"
xmlns :xsd
xmlns :rdfs="http ://www.w3.org/2000/01/rdf-schema"
xmlns :owl="http ://www.w3.org/owl"
xmlns="http ://www.owl-ontologies.com/unnamed.owl"
<owl :Ontology rdf :about=""/>
<owl :Class rdf :ID="GererLesIncidentsApplicatifs">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserLesApplications"/>
</rdfs :subClassOf>
Détecter et gérer les incidents et anomalies applicatifs</rdfs :comment>
</owl :Class>
<owl :Class rdf :ID="SinistreImmaterielTotal">
<rdfs :subClassOf>
<owl :Class rdf :ID="Risques"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="IntegriteElementsBasesReseau">
Les indicateurs doivent refléter l'évolution de la qualité de l'intégrité des elts de base du rés</rdfs :comment>
<rdfs :subClassOf>
<owl :Class rdf :ID="ArchitectureReseauTel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="GestionTraimentIncidents">
Les indicateurs doivent refléter la gestion et traitement des incidents :</rdfs :comment>
<rdfs :subClassOf>
<owl :Class rdf :ID="Production"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="GererContinuiteServiceEnvTravail">
<rdfs :subClassOf>
<owl :Class rdf :ID="ProtegerEnvTravail"/>
</rdfs :subClassOf>
Assurer la continuité de service de l'environnement de travail</rdfs :comment>
</owl :Class>
<owl :Class rdf :ID="TraiterIncidentReseauLocal">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserLeReseauLocal"/>
</rdfs :subClassOf>
Détecter les anomalies de fonctionnement ou des intrusions sur les réseaux locaux pour intervenir
au mieux et dans les meilleurs délais.</rdfs :comment>
</owl :Class>
<owl :Class rdf :ID="TransmissionFausseDonnees">
<rdfs :subClassOf>
<owl :Class rdf :ID="ManipulationDonnees"/>
</rdfs :subClassOf>
</owl :Class>

<owl :Class rdf :ID="DestructionConfigLogicielles">
<rdfs :subClassOf>
<owl :Class rdf :ID="DestructionSoftware"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="AuditReseau">
Les ind reflètent l'évolution de la qualité du respect des règles de sécurité définies</rdfs :comment>
<rdfs :subClassOf>
<owl :Class rdf :about="ArchitectureReseauTel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriserArchitecture">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserArchitectureSysteme"/>
</rdfs :subClassOf>
Mettre en place une architecture globale des systèmes garantissantune continuité de fonctionnement
conforme aux attentes des utilisateurs.
</rdfs :comment>
</owl :Class>
<owl :Class rdf :ID="ContunuerLeFonctionnement">
Assurer la continuité de fonctionnement des services applicatifs.
</rdfs :comment>
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesApplications"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriteProjetEtDevApllications">
<rdfs :subClassOf>
<owl :Class rdf :ID="Projets"/>
</rdfs :subClassOf>
Les indicateurs doivent refléter la sensibilité de l'équipe de développement, la disponibilité des ressources,
la traçabilité et fiabilité de l'application
etc.</rdfs :comment>
</owl :Class>
<owl :Class rdf :ID="SensibiloisationFormationSecurite">
<rdfs :subClassOf>
<owl :Class rdf :ID="Organisation"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="AbsenceDePersonnel">
<rdfs :subClassOf>
<owl :Class rdf :ID="IndisponibilitePassagereRessource"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriteProcExploitation">
Les indicateurs doivent refléter la sécurité des procédures d'exploitation, ils mesuront par exemple</rdfs :comment>
<rdfs :subClassOf>
<owl :Class rdf :about="Production"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControlerConnexionsSurResEtendu">
Faire en sorte que seules les entités autorisées aient accès au réseau étendu et puisse se connecter aux
autres entités.</rdfs :comment>
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserLeResEtendu"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControlerDroitsadminEnProd">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserLaProduction"/>
</rdfs :subClassOf>
Gérer avec rigueur l'attribution et l'utilisation de droits privilégiés sur les systèmes et
applications</rdfs :comment>
</owl :Class>
<owl :Class rdf :ID="DetournementInfoTemporaires GeneresParLesSystemes">
<rdfs :subClassOf>
<owl :Class rdf :ID="DivulgationDonnees"/>

</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriserArchitectureResLocal">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLeReseauLocal"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="GererContinuiteFonctionnement">
Assurer la continuité de fonctionnement des systèmes et applications.
</rdfs :comment>
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLaProduction"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="IntegriteSystAdressagePhyReseau">
<rdfs :subClassOf>
<owl :Class rdf :about="ArchitectureReseauTel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="OrganiserLaSecurite">
<rdfs :subClassOf>
<owl :Class rdf :ID="MesuresSecurite"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControlerAccesLocauxSensibles">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserLesLocaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="AccesSystemeEtConsultation">
<rdfs :subClassOf>
<owl :Class rdf :about="DivulgationDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ConfinerEnvironnement">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserArchitectureSysteme"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ModificationMateriel">
<rdfs :subClassOf>
<owl :Class rdf :ID="PerformancesDegradees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControlerDroitsAdmin">
<rdfs :subClassOf>
<owl :Class rdf :ID="ExploiterLesReseaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="EffacementAccidentelLogiciel">
<rdfs :subClassOf>
<owl :Class rdf :about="DestructionSoftware"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControleAccesLocauxSensibles">
<rdfs :subClassOf>
<owl :Class rdf :ID="Locaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ServicesGeneraux">
<rdfs :subClassOf>
<owl :Class rdf :about="Locaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="AterationDonnes"> <rdfs :subClassOf rdf :resource="Risques"/> </owl :Class>
<owl :Class rdf :ID="ControleConfigMaterielleLog">
<rdfs :subClassOf>
<owl :Class rdf :about="Production"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="Inondation">
<rdfs :subClassOf>
<owl :Class rdf :ID="DestructionEquipements"/>
</rdfs :subClassOf>

```
</owl :Class>
<owl :Class rdf :ID="GererLesRessourcesHumaines">
<rdfs :subClassOf rdf :resource="OrganiserLaSecurite"/>
</owl :Class>
<owl :Class rdf :ID="ProtegerPostesTravail">
<rdfs :subClassOf>
<owl :Class rdf :about="ProtegerEnvTravail"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="FasificationMessage">
<rdfs :subClassOf>
<owl :Class rdf :about="ManipulationDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="Production">
<rdfs :subClassOf>
<owl :Class rdf :ID="Indicateurs"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="Locaux">
<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="AssurerLaContinuiteDesActivites">
<rdfs :subClassOf rdf :resource="OrganiserLaSecurite"/>
</owl :Class>
<owl :Class rdf :ID="ProtegerInfoEcriteEchangee">
<rdfs :subClassOf>
<owl :Class rdf :about="ProtegerEnvTravail"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="DestructionEquipements">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="GererSupportDonneesEtProg">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLaProduction"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="PerteAccidentelleDocument">
<rdfs :subClassOf>
<owl :Class rdf :ID="PerteFichiersDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="CatastropeNaturelle">
<rdfs :subClassOf rdf :resource="DestructionEquipements"/>
</owl :Class>
<owl :Class rdf :ID="AccesSystCopieFichDonnees">
<rdfs :subClassOf>
<owl :Class rdf :ID="DetournementFichiersDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="IndisponibilitePassagereRessource">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="AcceesServeursCopieFichiers">
<rdfs :subClassOf>
<owl :Class rdf :about="DetournementFichiersDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="DestructionSoftware">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="ControlerAccesSystemes">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserArchitectureSysteme"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="ManipulationDonnees">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="GererEnregistrerLesTraces">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserArchitectureSysteme"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="Systeme">
```

<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="SecurisationAdministrationReseau">
<rdfs :subClassOf>
<owl :Class rdf :about="ArchitectureReseauTel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="EffacementCodeExecutable">
<rdfs :subClassOf rdf :resource="DestructionSoftware"/>
</owl :Class>
<owl :Class rdf :ID="EffacementParBombeLogique">
<rdfs :subClassOf>
<owl :Class rdf :about="PerteFichiersDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriserContreDegatsEnEau">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesLocaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ContinuiteFonctReseauTelecom">
<rdfs :subClassOf>
<owl :Class rdf :ID="ExploitationReseauTelecom"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SurutilisationMalveillRessInfor">
<rdfs :subClassOf>
<owl :Class rdf :about="PerformancesDegradees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="PerteAccidentelleFichiers">
<rdfs :subClassOf>
<owl :Class rdf :about="PerteFichiersDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriseDonneesEchangees">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLeResEtendu"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="Incendie">
<rdfs :subClassOf rdf :resource="DestructionEquipements"/>
</owl :Class>
<owl :Class rdf :about="SecuriserLeResEtendu">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="ControleDetectionTraimentIncidReseaux">
<rdfs :subClassOf>
<owl :Class rdf :about="ExploitationReseauTelecom"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="GestionEtEnregistrementsTraces">
<rdfs :subClassOf rdf :resource="Systeme"/>
</owl :Class>
<owl :Class rdf :ID="ModificationVolontaireFonctionnaliteAppl">
<rdfs :subClassOf>
<owl :Class rdf :ID="AlterationLogiciel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControlerConfidentialiteDonnees">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesApplications"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="TerrorismeExterieur">
<rdfs :subClassOf rdf :resource="DestructionEquipements"/>
</owl :Class>
<owl :Class rdf :ID="SubtitutionVolontaireSupport">
<rdfs :subClassOf rdf :resource="ManipulationDonnees"/>
</owl :Class>
<owl :Class rdf :ID="SecuriteProcedureExploitation">
<rdfs :subClassOf>
<owl :Class rdf :about="ExploitationReseauTelecom"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="OrganisationMaintenanceLogicielApplicatif">

```
<rdfs :subClassOf>
<owl :Class rdf :about="Projets"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="GestionSecuritePhysique">
<rdfs :subClassOf>
<owl :Class rdf :ID="SiteEtablissement"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ModifVolontairesFonctAppl">
<rdfs :subClassOf>
<owl :Class rdf :about="AlterationLogiciel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ProtegerContreRisqEnvironnement">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesLocaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="StructurerLaSecurite">
<rdfs :subClassOf rdf :resource="OrganiserLaSecurite"/>
</owl :Class>
<owl :Class rdf :ID="SurutilisationAccidRessInfor">
<rdfs :subClassOf>
<owl :Class rdf :about="PerformancesDegradees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="Projets">
<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="ControlerConfigMatEtLogiciels">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLaProduction"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="SecuriserLaProduction">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="GestionSupportDonneesEtProg">
<rdfs :subClassOf rdf :resource="Production"/>
</owl :Class>
<owl :Class rdf :ID="RendreLesDonnesDisponibles">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesApplications"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="IndisponibiliteTotaleLocaux">
<rdfs :subClassOf rdf :resource="IndispPassagereRessource"/>
</owl :Class>
<owl :Class rdf :ID="ContinuiteFonctionnementApplications">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriteApplicative"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="RoleStructureSecurite">
<rdfs :subClassOf>
<owl :Class rdf :about="Organisation"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="Organisation">
<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="SecuriserLesServicesGeneraux">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesLocaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControleCirculationSite">
<rdfs :subClassOf>
<owl :Class rdf :about="SiteEtablissement"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="EffacementAccidDisqueFixe">
<rdfs :subClassOf rdf :resource="DestructionSoftware"/>
</owl :Class>
<owl :Class rdf :ID="RespLegislationVerifComptaInformatisee">
```

<rdfs :subClassOf>
<owl :Class rdf :ID="RespJuridictionReglementaire"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="TraiterIncidentResEtendu">
<rdfs :subClassOf rdf :resource="SecuriserLeResEtendu"/>
</owl :Class>
<owl :Class rdf :about="PerformancesDegradees">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="DetournementInfosEnTransit">
<rdfs :subClassOf>
<owl :Class rdf :about="DivulgationDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="GestionTraitementIncidents">
<rdfs :subClassOf rdf :resource="SecuriserLaProduction"/>
</owl :Class>
<owl :Class rdf :ID="RespLegislationRappAvPersonnels">
<rdfs :subClassOf>
<owl :Class rdf :about="RespecterJuridiction"/>
</rdfs :subClassOf>
Communiquer au personnel la réglementation et la législation
</owl :Class>
<owl :Class rdf :ID="ControlerIntegriteDonnees">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesApplications"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ViolationDroitsDePropIndustrielle">
<rdfs :subClassOf>
<owl :Class rdf :ID="NonConformiteALaLegislation"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="ProtegerEnvTravail">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="RespLegislationConcernantUsageCryptographie">
<rdfs :subClassOf>
<owl :Class rdf :about="RespecterJuridiction"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="RejeuTransaction">
<rdfs :subClassOf rdf :resource="ManipulationDonnees"/>
</owl :Class>
<owl :Class rdf :ID="ControleConfidentialiteDonnees">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriteApplicative"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControleIntegriteDonnees">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriteApplicative"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="VolSupport">
<rdfs :subClassOf>
<owl :Class rdf :about="PerteFichiersDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriteIncendie">
<rdfs :subClassOf rdf :resource="Locaux"/>
</owl :Class>
<owl :Class rdf :ID="AccidentOuPanne">
<rdfs :subClassOf rdf :resource="IndisponibiliteRess"/>
</owl :Class>
<owl :Class rdf :ID="SecuriserLesProceduresDexploitation">
<rdfs :subClassOf>
<owl :Class rdf :about="ExploiterLesReseaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="PerteFichiersDonnees">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="ProtegerProprieteIntellectuelle">

```
<rdfs :subClassOf>
<owl :Class rdf :about="RespecterJuridiction"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="VandalismeDepuisExterieur">
<rdfs :subClassOf rdf :resource="IndisponibiliteRess"/>
</owl :Class>
<owl :Class rdf :ID="ControlerAccesAuxApplications">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesApplications"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="SecuriserContreIncendie">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesLocaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ImputabiliteAcces">
<rdfs :subClassOf>
<owl :Class rdf :about="ArchitectureReseauTel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="SiteEtablissement">
<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="ControleIntegEchEtCommunication">
<rdfs :comment rdf :datatype >
<rdfs :subClassOf>
<owl :Class rdf :about="ArchitectureReseauTel"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="AttribuerUnReferentielALaSec">
<rdfs :subClassOf rdf :resource="OrganiserLaSecurite"/>
</owl :Class>
<owl :Class rdf :about="ArchitectureReseauTel">
<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="ManipulationFichiers">
<rdfs :subClassOf rdf :resource="ManipulationDonnees"/>
</owl :Class>
<owl :Class rdf :ID="GererLesChangements">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserLesProjetsDeDev"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ModificationLogiciel">
<rdfs :subClassOf rdf :resource="PerformancesDegradees"/>
</owl :Class>
<owl :Class rdf :about="RespecterJuridiction">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="ConfinementEnvironnements">
<rdfs :comment rdf :datatype >
<rdfs :subClassOf rdf :resource="Systeme"/>
</owl :Class>
<owl :Class rdf :ID="VandalismeInterieur">
<rdfs :subClassOf rdf :resource="IndisponibiliteRess"/>
</owl :Class>
<owl :Class rdf :about="SecuriserLesLocaux">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="SecuriserReseauLocal">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLeReseauLocal"/>
</rdfs :subClassOf>
<rdfs :comment rdf :datatype >
</owl :Class>
<owl :Class rdf :about="AlterationLogiciel">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :about="SecuriserLesProjetsDeDev">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="ControlerAccesZonesDeBureau">
<rdfs :subClassOf rdf :resource="ProtegerEnvTravail"/>
<rdfs :comment rdf :datatype >
```

</owl :Class>
<owl :Class rdf :ID="ControlerProcedureAuditEnProd">
<rdfs :subClassOf rdf :resource="SecuriserLaProduction"/>
</owl :Class>
<owl :Class rdf :ID="SecuriserProceduresExploitation">
<rdfs :subClassOf rdf :resource="SecuriserLaProduction"/>
</owl :Class>
<owl :Class rdf :ID="ControleAccesApplicatifs">
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriteApplicative"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="DetournementCodeSource">
<rdfs :subClassOf>
<owl :Class rdf :about="DetournementFichiersDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="EffacementFichParBombeLogique">
<rdfs :subClassOf rdf :resource="SinistreImmatTotal"/>
</owl :Class>
<owl :Class rdf :ID="SecuriteContreDegatsEau">
<rdfs :subClassOf rdf :resource="Locaux"/>
</owl :Class>
<owl :Class rdf :about="SecuriteApplicative">
<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="BugLogiciel">
<rdfs :subClassOf rdf :resource="IndisponibiliteRess"/>
</owl :Class>
<owl :Class rdf :ID="SecuriteMaintenanceApplicative">
<rdfs :subClassOf rdf :resource="Projets"/>
</owl :Class>
<owl :Class rdf :ID="ImpossibiliteDeMaintenance">
<rdfs :subClassOf rdf :resource="IndisponibiliteRess"/>
</owl :Class>
<owl :Class rdf :ID="ControlerEmisEtRecepDonnees">
<rdfs :comment rdf :datatype >
<rdfs :subClassOf>
<owl :Class rdf :about="SecuriserLesApplications"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="VolOuEffacementSuppAmovible">
<rdfs :subClassOf rdf :resource="DestructionSoft"/>
</owl :Class>
<owl :Class rdf :ID="AlterationMalveillFonctionnaliteAppl">
<rdfs :subClassOf rdf :resource="AlterationLogiciel"/>
</owl :Class>
<owl :Class rdf :about="SecuriserArchitectureSysteme">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="ControlerAccesPhyAuxSitesEtBatiments">
<rdfs :subClassOf>
<owl :Class rdf :ID="SecuriserLesSitesEtLesBatiments"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="GestionRH">
<rdfs :subClassOf rdf :resource="Organisation"/>
</owl :Class>
<owl :Class rdf :ID="AttaqueSocieteTierce">
<rdfs :subClassOf>
<owl :Class rdf :about="NonConformiteALaLegislation"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="RespectLegislationCommFinanciere">
<rdfs :subClassOf rdf :resource="RespecterJuridiction"/>
</owl :Class>
<owl :Class rdf :ID="AccidentTraitement">
<rdfs :subClassOf rdf :resource="AterationDonnes"/>
</owl :Class>
<owl :Class rdf :about="SecuriserLeReseauLocal">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="VolsSupportDonneesAppl">
<rdfs :subClassOf>
<owl :Class rdf :about="DetournementFichiersDonnees"/>
</rdfs :subClassOf>

```
</owl :Class>
<owl :Class rdf :ID="VolDocumentEcrit">
<rdfs :subClassOf>
<owl :Class rdf :about="DivulgationDonnees"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :about="ExploitationReseauTelecom">
<rdfs :subClassOf rdf :resource="Indicateurs"/>
</owl :Class>
<owl :Class rdf :ID="SaisieFausseDonnees">
<rdfs :subClassOf rdf :resource="ManipulationDonnees"/>
</owl :Class>
<owl :Class rdf :ID="ControleDisponibiliteDonnees">
<rdfs :subClassOf rdf :resource="SecuriteApplicative"/>
<rdfs :comment rdf :datatype >
</owl :Class>
<owl :Class rdf :ID="ParametrerLesConfigMaterielLog">
<rdfs :subClassOf>
<owl :Class rdf :about="ExploiterLesReseaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="EffacementMalveillantSupport">
<rdfs :subClassOf rdf :resource="SinistreImmatTotal"/>
</owl :Class>
<owl :Class rdf :ID="ContinuiteFonctionnement">
<rdfs :subClassOf rdf :resource="Production"/>
</owl :Class>
<owl :Class rdf :ID="ProtectionAdressagePhysique">
<rdfs :subClassOf rdf :resource="ArchitectureReseauTel"/>
</owl :Class>
<owl :Class rdf :about="DivulgationDonnees">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="ControleConfigMatEtLogiciels">
<rdfs :subClassOf rdf :resource="ExploitResTelecom"/>
</owl :Class>
<owl :Class rdf :ID="ControleAccesReseau">
<rdfs :subClassOf rdf :resource="ArchitectureResTel"/>
</owl :Class>
<owl :Class rdf :about="NonConformiteALaLegislation">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :about="SecuriserLesApplications">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="ControlerProcedureAudit">
<rdfs :subClassOf>
<owl :Class rdf :about="ExploiterLesReseaux"/>
</rdfs :subClassOf>
</owl :Class>
<owl :Class rdf :ID="ControleAccesBureaux">
<rdfs :subClassOf rdf :resource="Locaux"/>
</owl :Class>
<owl :Class rdf :ID="ControleconfidEchEtCommunication">
<rdfs :comment rdf :datatype >
<rdfs :subClassOf rdf :resource="ArchitectureReseauTel"/>
</owl :Class>
<owl :Class rdf :ID="CaptationIformationFugitives">
<rdfs :subClassOf rdf :resource="DivulgationDonnees"/>
</owl :Class>
<owl :Class rdf :about="DetournementFichDonnees">
<rdfs :subClassOf rdf :resource="Risques"/>
</owl :Class>
<owl :Class rdf :ID="ContAcceesDonneesReseauLocal">
<rdfs :subClassOf rdf :resource="SecuriserLeReseauLocal"/>
</owl :Class>
<owl :Class rdf :ID="ConAccèsSystemesEtAppl>
<rdfs :subClassOf rdf :resource="Systeme"/>
</owl :Class>
<owl :Class rdf :ID="TraitementIncidents">
<rdfs :subClassOf rdf :resource="ExploitResTelecom"/>
</owl :Class>
<owl :Class rdf :ID="EffacementMalveillantDeSupp">
<rdfs :subClassOf rdf :resource="PerteFichDonnees"/>
</owl :Class>
<owl :Class rdf :ID="SecuriserArchitectureResEtendu">
```

<rdfs :subClassOf rdf :resource="SecuriserLeResEtendu"/>
<rdfs :comment rdf :datatype >
</owl :Class>
<owl :Class rdf :ID="ContEmissionReceptionDonnees">
<rdfs :subClassOf rdf :resource="SecuriteApplicative"/>
</owl :Class>
<owl :Class rdf :ID="Assurances">
<rdfs :subClassOf rdf :resource="Organisation"/>
</owl :Class>
<owl :Class rdf :about="ExploiterLesReseaux">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :Class rdf :ID="SecuriserECommerce">
<rdfs :subClassOf rdf :resource="SecuriserLesAppl"/>
</owl :Class>
<owl :Class rdf :ID="EffacementSupportParVirus">
<rdfs :subClassOf rdf :resource="PerteFichiersDonnees"/>
</owl :Class>
<owl :Class rdf :ID="ControleAccesSite">
<rdfs :subClassOf rdf :resource="SiteEtablissement"/>
</owl :Class>
<owl :Class rdf :ID="ErreurSaisie">
<rdfs :subClassOf rdf :resource="AterationDonnes"/>
</owl :Class>
<owl :Class rdf :ID="ImplantationDuSite">
<rdfs :subClassOf rdf :resource="SiteEtablissement"/>
</owl :Class>
<owl :Class rdf :ID="SecuriserLesProcessusDevev">
<rdfs :subClassOf rdf :resource="SecuriserProjetsDeDev"/>
</owl :Class>
<owl :Class rdf :ID="Assurer">
<rdfs :subClassOf rdf :resource="OrganiserLaSecurite"/>
</owl :Class>
<owl :Class rdf :about="SecuriserLesSitesEtLesBatiments">
<rdfs :subClassOf rdf :resource="MesuresSecurite"/>
</owl :Class>
<owl :ObjectProperty rdf :ID="mesureassocie">
<rdfs :domain rdf :resource="Indicateurs"/>
</owl :ObjectProperty>
<owl :ObjectProperty rdf :ID="protegecontre">
<rdfs :domain rdf :resource="MesuresSecurite"/>
</owl :ObjectProperty>
<owl :DatatypeProperty rdf :ID="objectifs">
<rdfs :domain rdf :resource="MesuresSecurite"/>
</owl :DatatypeProperty>
<owl :DatatypeProperty rdf :ID="resultatsattendus">
<rdfs :domain rdf :resource="MesuresSecurite"/>
</owl :DatatypeProperty>
<owl :FunctionalProperty rdf :ID="mesurerecuperation">
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="AbsenceDePersonnel"/>
<owl :Class rdf :about="AccidentOuPanne"/>
<owl :Class rdf :about="BugLogiciel"/>
<owl :Class rdf :about="ImpossDeMaintenance"/>
<owl :Class rdf :about="VandalismeDepuisExterieur"/>
<owl :Class rdf :about="VandalismeInterieur"/>
<owl :Class rdf :about="IndisponibiliteTotaleLocaux"/>
<owl :Class rdf :about="CatastropeNaturelle"/>
<owl :Class rdf :about="Incendie"/>
<owl :Class rdf :about="Inondation"/>
<owl :Class rdf :about="TerrorismeExterieur"/>
<owl :Class rdf :about="ModificationLogiciel"/>
<owl :Class rdf :about="ModificationMateriel"/>
<owl :Class rdf :about="SurutilisationAccidRessInfor"/>
<owl :Class rdf :about="SurutilisationMalveillRessInfor"/>
<owl :Class rdf :about="EffacementCodeExecutable"/>
<owl :Class rdf :about="EffacementAccidDisqueFixe"/>
<owl :Class rdf :about="EffacementAccidentelLogiciel"/>
<owl :Class rdf :about="VolOuEffacementSuppAmovible"/>
<owl :Class rdf :about="DestructionConfigLogicielles"/>
<owl :Class rdf :about="ModifVolontairesFonctAppl"/>
<owl :Class rdf :about="AccidentTraitement"/>
<owl :Class rdf :about="ErreurSaisie"/>
<owl :Class rdf :about="TransmissionFausseDonnees"/>

```
<owl :Class rdf :about="RejeuTransaction"/>
<owl :Class rdf :about="SaisieFausseDonnees"/>
<owl :Class rdf :about="SubtitutionVolontaireSupport"/>
<owl :Class rdf :about="ManipulationFichiers"/>
<owl :Class rdf :about="FasificationMessage"/>
<owl :Class rdf :about="AccesSystemeEtConsultation"/>
<owl :Class rdf :about="CaptationIformationFugitives"/>
<owl :Class rdf :about="VolDocumentEcrit"/>
<owl :Class rdf :about="DetournementInfosEnTransit"/>
<owl :Class rdf :about="AccesCopieFichDonneesAppl"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="code">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="IndisponibilitePassagereRess"/>
<owl :Class rdf :about="DestructionEquipements"/>
<owl :Class rdf :about="PerformancesDegradees"/>
<owl :Class rdf :about="DestructionSoftware"/>
<owl :Class rdf :about="AlterationLogiciel"/>
<owl :Class rdf :about="AterationDonnes"/>
<owl :Class rdf :about="ManipulationDonnees"/>
<owl :Class rdf :about="DivulgationDonnees"/>
<owl :Class rdf :about="DetournementFichDonnees"/>
<owl :Class rdf :about="PerteFichiersDonnees"/>
<owl :Class rdf :about="SinistreImmaterielTotal"/>
<owl :Class rdf :about="NonConformiteALaLegislation"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="valeur">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain rdf :resource="Indicateurs"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="expositionnaturelle">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="AbsenceDePersonnel"/>
<owl :Class rdf :about="AccidentOuPanne"/>
<owl :Class rdf :about="BugLogiciel"/>
<owl :Class rdf :about="ImpossDeMaintenance"/>
<owl :Class rdf :about="VandalismeDepuisExterieur"/>
<owl :Class rdf :about="VandalismeInterieur"/>
<owl :Class rdf :about="IndisponibiliteTotaleLocaux"/>
<owl :Class rdf :about="CatastropeNaturelle"/>
<owl :Class rdf :about="Incendie"/>
<owl :Class rdf :about="Inondation"/>
<owl :Class rdf :about="TerrorismeExterieur"/>
<owl :Class rdf :about="ModificationLogiciel"/>
<owl :Class rdf :about="ModificationMateriel"/>
<owl :Class rdf :about="SurutilisationAccidRessInfor"/>
<owl :Class rdf :about="SurutilisationMalveillRessInfor"/>
<owl :Class rdf :about="EffacementCodeExecutable"/>
<owl :Class rdf :about="EffacementAccidDisqueFixe"/>
<owl :Class rdf :about="EffacementAccidentelLogiciel"/>
<owl :Class rdf :about="VolOuEffacementSuppAmovible"/>
<owl :Class rdf :about="DestructionConfigLogicielles"/>
<owl :Class rdf :about="ModifVolontairesFonctAppl"/>
<owl :Class rdf :about="AccidentTraitement"/>
<owl :Class rdf :about="ErreurSaisie"/>
<owl :Class rdf :about="TransmissionFausseDonnees"/>
<owl :Class rdf :about="RejeuTransaction"/>
<owl :Class rdf :about="SaisieFausseDonnees"/>
<owl :Class rdf :about="SubtitutionVolontaireSupport"/>
<owl :Class rdf :about="ManipulationFichiers"/>
<owl :Class rdf :about="FasificationMessage"/>
```

<owl :Class rdf :about="AccesSystemeEtConsultation"/>
<owl :Class rdf :about="CaptationIformationFugitives"/>
<owl :Class rdf :about="VolDocumentEcrit"/>
<owl :Class rdf :about="DetournementInfosEnTransit"/>
<owl :Class rdf :about="AccesSystCopieFichDonnees"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="impactintrinseque">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="AbsenceDePersonnel"/>
<owl :Class rdf :about="AccidentOuPanne"/>
<owl :Class rdf :about="BugLogiciel"/>
<owl :Class rdf :about="ImpossDeMaintenance"/>
<owl :Class rdf :about="VandalismeDepuisExterieur"/>
<owl :Class rdf :about="VandalismeInterieur"/>
<owl :Class rdf :about="IndisponibiliteTotaleLocaux"/>
<owl :Class rdf :about="CatastropeNaturelle"/>
<owl :Class rdf :about="Incendie"/>
<owl :Class rdf :about="Inondation"/>
<owl :Class rdf :about="TerrorismeExterieur"/>
<owl :Class rdf :about="ModificationLogiciel"/>
<owl :Class rdf :about="ModificationMateriel"/>
<owl :Class rdf :about="SurutilisationAccidRessInfor"/>
<owl :Class rdf :about="SurutilisationMalveilRessInfor"/>
<owl :Class rdf :about="EffacementCodeExecutable"/>
<owl :Class rdf :about="EffacementAccidDisqueFixe"/>
<owl :Class rdf :about="EffacementAccidentelLogiciel"/>
<owl :Class rdf :about="VolOuEffacementSuppAmovible"/>
<owl :Class rdf :about="DestructionConfigLogicielles"/>
<owl :Class rdf :about="ModifVolontairesFonctAppl"/>
<owl :Class rdf :about="AccidentTraitement"/>
<owl :Class rdf :about="ErreurSaisie"/>
<owl :Class rdf :about="TransmissionFausseDonnees"/>
<owl :Class rdf :about="RejeuTransaction"/>
<owl :Class rdf :about="SaisieFausseDonnees"/>
<owl :Class rdf :about="SubtitutionVolontaireSupport"/>
<owl :Class rdf :about="ManipulationFichiers"/>
<owl :Class rdf :about="FasificationMessage"/>
<owl :Class rdf :about="AccesSystemeEtConsultation"/>
<owl :Class rdf :about="CaptationIformationFugitives"/>
<owl :Class rdf :about="VolDocumentEcrit"/>
<owl :Class rdf :about="DetournementInfosEnTransit"/>
<owl :Class rdf :about="AccesSystCopieFichDonnees"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="nomindicateur">
<rdfs :domain rdf :resource="Indicateurs"/>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="mesurepalliative">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="AbsenceDePersonnel"/>
<owl :Class rdf :about="AccidentOuPanne"/>
<owl :Class rdf :about="BugLogiciel"/>
<owl :Class rdf :about="ImpossDeMaintenance"/>
<owl :Class rdf :about="VandalismeDepuisExterieur"/>
<owl :Class rdf :about="VandalismeInterieur"/>
<owl :Class rdf :about="IndisponibiliteTotaleLocaux"/>
<owl :Class rdf :about="CatastropeNaturelle"/>
<owl :Class rdf :about="Incendie"/>
<owl :Class rdf :about="Inondation"/>
<owl :Class rdf :about="TerrorismeExterieur"/>

```
<owl :Class rdf :about="ModificationLogiciel"/>
<owl :Class rdf :about="ModificationMateriel"/>
<owl :Class rdf :about="SurutilisationAccidRessInfor"/>
<owl :Class rdf :about="SurutilisationMalveilRessInfor"/>
<owl :Class rdf :about="EffacementCodeExecutable"/>
<owl :Class rdf :about="EffacementAccidDisqueFixe"/>
<owl :Class rdf :about="EffacementAccidentelLogiciel"/>
<owl :Class rdf :about="VolOuEffacementSuppAmovible"/>
<owl :Class rdf :about="DestructionConfigLogicielles"/>
<owl :Class rdf :about="ModifVolontairesFonctAppl"/>
<owl :Class rdf :about="AccidentTraitement"/>
<owl :Class rdf :about="ErreurSaisie"/>
<owl :Class rdf :about="TransmissionFausseDonnees"/>
<owl :Class rdf :about="RejeuTransaction"/>
<owl :Class rdf :about="SaisieFausseDonnees"/>
<owl :Class rdf :about="SubtitutionVolontaireSupport"/>
<owl :Class rdf :about="ManipulationFichiers"/>
<owl :Class rdf :about="FasificationMessage"/>
<owl :Class rdf :about="AccesSystemeEtConsultation"/>
<owl :Class rdf :about="CaptationIformationFugitives"/>
<owl :Class rdf :about="VolDocumentEcrit"/>
<owl :Class rdf :about="DetournementInfosEnTransit"/>
<owl :Class rdf :about="AccesCopieFichDonneesAppl"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="cible">
<rdfs :domain rdf :resource="Indicateurs"/>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="seuilmax">
<rdfs :domain rdf :resource="Indicateurs"/>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="description">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :range rdf :resource/>
<rdfs :domain rdf :resource="Indicateurs"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="seuilmini">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain rdf :resource="Indicateurs"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="mesurepreventive">
<rdfs :range rdf :resource/>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="AbsenceDePersonnel"/>
<owl :Class rdf :about="AccidentOuPanne"/>
<owl :Class rdf :about="BugLogiciel"/>
<owl :Class rdf :about="ImpossDeMaintenance"/>
<owl :Class rdf :about="VandalismeDepuisExterieur"/>
<owl :Class rdf :about="VandalismeInterieur"/>
<owl :Class rdf :about="IndisponibiliteTotaleLocaux"/>
<owl :Class rdf :about="CatastropeNaturelle"/>
<owl :Class rdf :about="Incendie"/>
<owl :Class rdf :about="Inondation"/>
<owl :Class rdf :about="TerrorismeExterieur"/>
<owl :Class rdf :about="ModificationLogiciel"/>
<owl :Class rdf :about="ModificationMateriel"/>
<owl :Class rdf :about="SurutilisationAccidRessInfor"/>
<owl :Class rdf :about="SurutilisationMalveillRessourecesInfor"/>
<owl :Class rdf :about="EffacementCodeExecutable"/>
<owl :Class rdf :about="EffacementAccidDisqueFixe"/>
<owl :Class rdf :about="EffacementAccidentelLogiciel"/>
<owl :Class rdf :about="VolOuEffacementSuppAmovible"/>
<owl :Class rdf :about="DestructionConfigLogicielles"/>
<owl :Class rdf :about="ModifVolontairesFonctAppl"/>
<owl :Class rdf :about="AccidentTraitement"/>
<owl :Class rdf :about="ErreurSaisie"/>
<owl :Class rdf :about="TransmissionFausseDonnees"/>
```

<owl :Class rdf :about="RejeuTransaction"/>
<owl :Class rdf :about="SaisieFausseDonnees"/>
<owl :Class rdf :about="SubtitutionVolontaireSupport"/>
<owl :Class rdf :about="ManipulationFichiers"/>
<owl :Class rdf :about="FasificationMessage"/>
<owl :Class rdf :about="AccesSystemeEtConsultation"/>
<owl :Class rdf :about="CaptationIformationFugitives"/>
<owl :Class rdf :about="VolDocumentEcrit"/>
<owl :Class rdf :about="DetournementInfosEnTransit"/>
<owl :Class rdf :about="AccesCopieFichDonneesAppl"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="mesureprotection">
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="AbsenceDePersonnel"/>
<owl :Class rdf :about="AccidentOuPanne"/>
<owl :Class rdf :about="BugLogiciel"/>
<owl :Class rdf :about="ImpossDeMaintenance"/>
<owl :Class rdf :about="VandalismeDepuisExterieur"/>
<owl :Class rdf :about="VandalismeInterieur"/>
<owl :Class rdf :about="IndisponibiliteTotaleLocaux"/>
<owl :Class rdf :about="CatastropeNaturelle"/>
<owl :Class rdf :about="Incendie"/>
<owl :Class rdf :about="Inondation"/>
<owl :Class rdf :about="TerrorismeExterieur"/>
<owl :Class rdf :about="ModificationLogiciel"/>
<owl :Class rdf :about="ModificationMateriel"/>
<owl :Class rdf :about="SurutilisationAccidRessInfor"/>
<owl :Class rdf :about="SurutilisationMalveilRessInfor"/>
<owl :Class rdf :about="EffacementCodeExecutable"/>
<owl :Class rdf :about="EffacementAccidDisqueFixe"/>
<owl :Class rdf :about="EffacementAccidentelLogiciel"/>
<owl :Class rdf :about="VolOuEffacementSuppAmovible"/>
<owl :Class rdf :about="DestructionConfigLogicielles"/>
<owl :Class rdf :about="ModifVolontairesFonctAppl"/>
<owl :Class rdf :about="AccidentTraitement"/>
<owl :Class rdf :about="ErreurSaisie"/>
<owl :Class rdf :about="TransmissionFausseDonnees"/>
<owl :Class rdf :about="RejeuTransaction"/>
<owl :Class rdf :about="SaisieFausseDonnees"/>
<owl :Class rdf :about="SubtitutionVolontaireSupport"/>
<owl :Class rdf :about="ManipulationFichiers"/>
<owl :Class rdf :about="FasificationMessage"/>
<owl :Class rdf :about="AccesSystemeEtConsultation"/>
<owl :Class rdf :about="CaptationIformationFugitives"/>
<owl :Class rdf :about="VolDocumentEcrit"/>
<owl :Class rdf :about="DetournementInfoEnTransit"/>
<owl :Class rdf :about="AccesSystCopieFichDonnees"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="potentialite">
<rdfs :domain rdf :resource="Risques"/>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="dateapplication">
Date à laquelle la mesure a été mise en application</rdfs :com-
ment>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain rdf :resource="MesuresSecurite"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="risqueassocie">
<rdf :type rdf :res="http ://www.w3.org/owlObjectProperty"/>
<rdfs :domain rdf :resource="Indicateurs"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="efficacite">

```
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain rdf :resource="MesuresSecurite"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="name">
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="MesuresSecurite"/>
<owl :Class rdf :about="IndisponibilitePassagereRessourceW1"/>
<owl :Class rdf :about="DestructionEquipements"/>
<owl :Class rdf :about="PerformancesDegradees"/>
<owl :Class rdf :about="DestructionSoftware"/>
<owl :Class rdf :about="AlterationLogiciel"/>
<owl :Class rdf :about="AterationDonnes"/>
<owl :Class rdf :about="ManipulationDonnees"/>
<owl :Class rdf :about="DivulgationDonnees"/>
<owl :Class rdf :about="AccesSystCopieFichDonnees"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
/owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="theseontologieSlot6">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
</owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="mesuredissuasive">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain>
<owl :Class>
<owl :unionOf rdf :parseType="Collection">
<owl :Class rdf :about="AbsenceDePersonnel"/>
<owl :Class rdf :about="AccidentOuPanne"/>
<owl :Class rdf :about="BugLogiciel"/>
<owl :Class rdf :about="ImpossDeMaintenance"/>
<owl :Class rdf :about="VandalismeDepuisExterieur"/>
<owl :Class rdf :about="VandalismeInterieur"/>
<owl :Class rdf :about="IndisponibiliteTotaleLocaux"/>
<owl :Class rdf :about="CatastropeNaturelle"/>
<owl :Class rdf :about="Incendie"/>
<owl :Class rdf :about="Inondation"/>
<owl :Class rdf :about="TerrorismeExterieur"/>
<owl :Class rdf :about="ModificationLogiciel"/>
<owl :Class rdf :about="ModificationMateriel"/>
<owl :Class rdf :about="SurutilisationAccidRessInfor"/>
<owl :Class rdf :about="SurutilisationMalveillResscesInfor"/>
<owl :Class rdf :about="EffacementCodeExecutable"/>
<owl :Class rdf :about="EffacementAccidDisqueFixe"/>
<owl :Class rdf :about="EffacementAccidentelLogiciel"/>
<owl :Class rdf :about="VolOuEffacementSuppAmovible"/>
<owl :Class rdf :about="DestructionConfigLogicielles"/>
<owl :Class rdf :about="ModifVolontairesFonctAppl"/>
<owl :Class rdf :about="AccidentTraitement"/>
<owl :Class rdf :about="ErreurSaisie"/>
<owl :Class rdf :about="TransmissionFausseDonnees"/>
<owl :Class rdf :about="RejeuTransaction"/>
<owl :Class rdf :about="SaisieFausseDonnees"/>
<owl :Class rdf :about="SubtitutionVolontaireSupport"/>
<owl :Class rdf :about="ManipulationFichiers"/>
<owl :Class rdf :about="FasificationMessage"/>
<owl :Class rdf :about="AccesSystemeEtConsultation"/>
<owl :Class rdf :about="CaptationIformationFugitives"/>
<owl :Class rdf :about="VolDocumentEcrit"/>
<owl :Class rdf :about="DetournementInfosEnTransit"/>
<owl :Class rdf :about="AccesSystCopieFichDonnees"/>
<owl :Class rdf :about="VolsSupportDonneesAppl"/>
<owl :Class rdf :about="AcceesServeursCopieFichiers"/>
</owl :unionOf>
</owl :Class>
</rdfs :domain>
/owl :FunctionalProperty>
<owl :FunctionalProperty rdf :ID="mesureid">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypePro"/>
<rdfs :domain rdf :resource="MesuresSecurite"/>
</owl :FunctionalProperty>
```

<owl :FunctionalProperty rdf :ID="impact">
<rdf :type rdf :res="http ://www.w3.org/owlDatatypeProp
<rdfs :domain rdf :resource="Risques"/>
</owl :FunctionalProperty>
<SaisieFausseDonnees rdf :ID="theseontologieInst">
2</potentialite>
07.32</code>
2</impact>
01D02</mesurerecuperation>
min(08F02 ;max(min(07A03 ;07A04) ;
min(09A03 ;09A04))) </mesurepreventive>
09B04</mesureprotection>
Saisie de fausses données par un membre du personnel
usurpant l'identité d'un utilisateur autorisé</name>
</SaisieFausseDonnees>
<AccidentOuPanne rdf :ID="theseontologieInst">
Accidents dus à l'eau ou à des liquides mettant hors
service un équipement du réseau local</name>
max(05A02 ;05A08 ;01E02)</mesurepalliative>
03C01</mesurepreventive>
01D01</mesurerecuperation>
01.22b</code>
</AccidentOuPanne>
<AccidentOuPanne rdf :ID="theseontologieInst">
<name rdf :datatype >
Inondation due à l'extinction d'un incendie voisin, met-
tant hors service
des équipements du réseau local</name>
05A08</mesurepalliative» 01D01</mesurerecuperation>
<code rdf :datatype >
02.33b</code>
</AccidentOuPanne>
<AccidentOuPanne rdf :ID="theseontologieInst">
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype> 01.24a</code>
<mesurepalliative rdf :datatype >
min(08D06 ;09E02)</mesurepalliative>
<name rdf :datatype >
Accident de nature électrique externe à l'entreprise
(court-circuit extérieur, coupure d'un câble, défaillance
extérieure, etc.)
empêchant de fonctionner les systèmes centraux.</name>
<mesurepreventive rdf :datatype>
03A02</mesurepreventive>
</AccidentOuPanne>
<AccidentOuPanne rdf :ID="theseontologieInst">
<mesurepalliative rdf :datatype>
04A07</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepreventive rdf :datatype >
03A05</mesurepreventive>
<code rdf :datatype >
02.11a</code>
Catastrophe naturelle ou acidentelle : Chute de la foudre
endommageant
gravement des équipements du réseau étendu</name>
</AccidentOuPanne>
<ControleEmissionReceptionDonnees rdf :ID="theseontologieInst">
<risqueassocie>
<RejeuTransaction rdf :ID="theseontologieInst">
2</impact>
09F03</mesureprotection>
<name rdf :datatype >
Rejeu de transaction</name>
2</potentialite>
<mesurepreventive rdf :datatype>
max(04C01 ;09C01 ;09F02)</mesurepreventive>
07.21</code>
01D02</mesurerecuperation>
</RejeuTransaction>
</risqueassocie>
<mesureassocie>
<ControlerEmisEtRecepDonnees rdf :ID="theseontologieInst">
<mesureid rdf :datatype>

09F01</mesureid>
<protegecontre rdf :resource="theseontologieInst"/>
3</efficacite>
<name rdf :datatype >
Accusé de réception</name>
</ControlerEmisEtRecepDonnees>
</mesureassocie>
Accuséderéception</nomindicateur»
Nombre d'Accusé - Réception adressés / Nombre de transmissions sensibles</cible>
</ControleEmissionRecepDonnees>
<StructurerLaSecurite rdf :ID="theseontologieInst">
01A02</mesureid>
Organisation du management et du pilotage de la sécurité des SI</name> Mettre en place
des processus de prise de décision concernant la sécurité des SI et de contrôle des actions
menées en conséquence</resultatsattendus>
<objectifs rdf :datatype>
Organiser le management et le pilotage de la sécurité des systèmes d'information</objectifs>
</StructurerLaSecurite>
<AccidentOuPanne rdf :ID="theseontologieInst">
<mesurepalliative rdf :datatype >
05A04</mesurepalliative>
<name rdf :datatype >
Tir d'armes légères ou lancement de projectiles depuis la rue, rendant indisponible des équipements du réseau local.</name>
<code rdf :datatype >
01.51b</code>
<mesurerecuperation >
01D01</mesurerecuperation>
</AccidentOuPanne>
<SurutilisationMalveillRessInfor rdf :ID="theseontologieInst">
<code rdf :datatype >
03.41</code>
<name rdf :datatype>
Dégradation des performances applicatives due à la saturation répétitive malveillante
de moyens informatiques par un groupe d'utilisateurs</name>
<mesuredissuasive >
min(07C01 ;07C02)</mesuredissuasive>
<mesurepreventive rdf :datatype>
08E01</mesurepreventive>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<mesureprotection rdf :datatype>
min(08E02 ;08E03)</mesureprotection>
</SurutilisationMalveillRessInfor>
<EffacementCodeExecutable rdf :ID="theseontologie">
<mesureprotection rdf :datatype>
08F03</mesureprotection>
<name rdf :datatype >
Ecrasement total ou pollution massive des configurations systèmes par un
membre du personnel (non administrateur)</name>
<mesurepreventive rdf :datatype>
min(08F01 ;08F02)</mesurepreventive>
<code rdf :datatype >
04.12c</code>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<mesurepalliative rdf :datatype>
08D04</mesurepalliative>
</EffacementCodeExecutable>
<TransmissionFausseDonnees rdf :ID="theseontologie">
1</potentialite>
<code rdf :datatype >
07.11</code>
<mesurepreventive rdf :datatype >
max(04C01 ;04C02 ;09B02 ;09C01)</mesurepreventive>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<impact rdf :datatype >
3</impact>

<name rdf :datatype >
Données applicatives faussées pendant la transmission sur le réseau étendu
par un pirate agissant de l'extérieur</name>
</TransmissionFausseDonnees>
<AccidentOuPanne rdf :ID="theseontologie">
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<name rdf :datatype >
Inondation due à une canalisation percée ou crevée et rendant indisponibles
des équipements du réseau local</name>
<mesureprotection rdf :datatype=>
min(03C02 ;03C03)</mesureprotection>
<code rdf :datatype>
01.31b</code>
<mesurepalliative rdf :datatype>
05A08</mesurepalliative>
<mesurepreventive rdf :datatype >
03C01</mesurepreventive>
</AccidentOuPanne>
<ModificationMateriel rdf :ID="theseontologie">
<name rdf :datatype >
Dégradation involontaire de performances, à l'occasion d'une opération de maintenance
matérielle évolutive d'un équipement du réseau local (hors télémaintenance)</name>
<mesurepalliative rdf :datatype >
05A04</mesurepalliative>
<mesurepreventive rdf :datatype >
06A03</mesurepreventive>
<mesurerecuperation rdf :datatype >
05A04</mesurerecuperation>
<code rdf :datatype >
03.21b</code>
</ModificationMateriel>
<ErreurSaisie rdf :ID="thontoInstance">
3</potentialite>
<mesureprotection rdf :datatype >
09B04</mesureprotection>
<mesurepreventive rdf :datatype >
09B03</mesurepreventive>
<code rdf :datatype >
06.21</code>
1</impact>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<name rdf :datatype >
Erreur pendant le processus de saisie,</name>
</ErreurSaisie>
<VolOuEffacementSuppAmovible rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
08D04</mesurepalliative>
<code rdf :datatype >
04.41</code>
<mesuredissuasive rdf :datatype >
03B06</mesuredissuasive>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<name rdf :datatype >
Vol ou effacement d'un support amovible contenant le code source d'un logiciel
dans les locaux informatiques, par une personne autorisée</name>
</VolOuEffacementSuppAmovible>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
max(05A02 ;05A04)</mesurepalliative>
<name rdf :datatype >
Panne rendant indisponible un équipement du réseau local</name>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<code rdf :datatype >
01.23b</code>
<mesurepreventive rdf :datatype >

05A02</mesurepreventive>
</AccidentOuPanne>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype>
02.41a</code>
<mesurepalliative rdf :datatype>
0 4A07</mesurepalliative>
<name rdf :datatype >
Terrorisme sabotage par des agents extérieurs : explosifs déposés à proximité
des locaux sensibles, mettant hors service des équipements du réseau étendu</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
</AccidentOuPanne>
<GererLesRessourcesHumaines rdf :ID="thontoInstance">
<name rdf :datatype>
Gestion des tierces parties</name>
<resultatsattendus rdf :datatype >
Limiter l'exposition à des erreurs ou accidents par manque d'attention, par inadvertance ou par
méconnaissance des mesures adéquates, de
la part de tierces parties.
</resultatsattendus>
<mesureid rdf :datatype >
01C05</mesureid>
<objectifs rdf :datatype>
Faire en sorte que les tierces parties pouvant avoir accès au système d'information
sachent quelle conduite tenir vis-à-vis de l'information ou des ressources spécifiques
auxquelles elles ont accès et s'engagent à respecter les règles de sécurité correspondantes.</objectifs>
</GererLesRessourcesHumaines>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesuredissuasive rdf :datatype>
03B06</mesuredissuasive>
<name rdf :datatype>
Vandalisme touchant l'ensemble d'une salle informatique et télécom, par des
personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.).</name>
<mesureprotection rdf :datatype>
max(03B02 ;03B04)</mesureprotection>
<mesurepreventive rdf :datatype >
min(03B01 ;03B02 ;03B03)</mesurepreventive>
<mesurepalliative rdf :datatype >
min(04A03 ;05A04 ;08D01)</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype >
01.61d</code>
</AccidentOuPanne>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
min(08D06 ;09E02)</mesurepalliative>
<name rdf :datatype>
Incendie : accident interne (corbeille à papier, cendrier, etc.) endommageant
gravement des systèmes centraux</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesureprotection rdf :datatype >
min(03D02 ;03D03)</mesureprotection>
<code rdf :datatype >
02.21c</code>
<mesurepreventive rdf :datatype >
03D01</mesurepreventive>
</AccidentOuPanne>
<AttribuerUnReferentielALaSec rdf :ID="thontoInstance">
<resultatsattendus rdf :datatype >
Permettre que le degré de protection apporté à chaque ressource soit
proportionné au degré de sensibilité de cette ressource.</resultatsattend
<mesureid rdf :datatype >
01B03</mesureid>

<objectifs rdf :datatype>
Expliciter et porter à la connaissance de l'ensemble du personnel concerné le degré de sensibilité des supports d'information ou de communication et des ressources du système d'information (données, applications, ressources de traitement et de communication) qu'ils gèrent et utilisent.</objectifs>
<name rdf :datatype>
Classification les ressources</name>
</AttribuerUnReferentielALaSecurite>
<StructurerLaSecurite rdf :ID="thontoInstance">
<objectifs rdf :datatype>
S'assurer que tous les domaines de sécurité ont un responsable et qu'il existe
une structure de coordination, à même de prendre toute décision transverse.</objectifs>
<mesureid rdf :datatype>
01A01</mesureid>
<resultatsattendus rdf :datatype>
Éviter des trous et des domaines non couverts qui pourraient représenter un risque
pour l'information et des incohérences entre domaines qui pourraient avoir un impact
négatif sur la sensibilisation des responsables et des utilisateurs.</resultatsattendus>
<name rdf :datatype>
Organisation du management et du pilotage de la sécurité générale</name>
</StructurerLaSecurite>
<AttribuerUnReferentielALaSecurite rdf :ID="thontoInstance">
<mesureid rdf :datatype>
01B04</mesureid>
<resultatsattendus rdf :datatype >
Permettre que chaque actif reçoive le niveau de protection approprié.</resultatsattendus>
<name rdf :datatype >
Gestion des actifs</name>
<objectifs rdf :datatype >
Assurer une gestion des actifs matériels ou immatériels telle que le niveau
de protection apporté à chacun soit décidé et contrôlé par la personne la mieux à même de le faire.</objectifs>
</AttribuerUnReferentielALaSecurite>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype >
02.33a</code>
<mesurepalliative rdf :datatype >
04A07</mesurepalliative>
<name rdf :datatype >
Inondation due à l'extinction d'un incendie voisin, mettant hors service
des équipements du réseau étendu</name>
</AccidentOuPanne>
<ControlerIntegriteDonnees rdf :ID="thontoInstance">
<name rdf :datatype>
Contrôle de la saisie des données</name>
<protegecontre rdf :resource="thontoInstance"/>
<mesureid rdf :datatype>
09B03</mesureid>
3</efficacite>
</ControlerIntegriteDonnees>
<GererLesRessourcesHumaines rdf :ID="thontoInstance">
<name rdf :datatype >
Engagement du personnel - clauses contractuelles</name>
<objectifs rdf :datatype >
Réduire l'occurrence d'actions néfastes ou potentiellement dangereuses en les interdisant.</objectifs>
<mesureid rdf :datatype>
01C01</mesureid>
<resultatsattendus rdf :datatype >
Limiter l'exposition à des erreurs, accidents ou malveillances
en interdisant, éventuellement en fonction de certaines circonstances, certaines pratiques ou actions à un cer-

tain
nombre de personnes.</resultatsattendus>
</GererLesRessourcesHumaines>
<ManipulationFichiers rdf :ID="thontoInstance">
<mesureprotection rdf :datatype >
09B04</mesureprotection>
3</impact>
<code rdf :datatype>
07.52</code>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<name rdf :datatype>

1</potentialite>
<mesurepreventive rdf :datatype >
min(08F01 ;max(min(07A01 ;07A02) ;
min(09A01 ;09A02)))
</mesurepreventive>
</ManipulationFichiers>
<GererLesRessourcesHumaines rdf :ID="thontoInstance">
<name rdf :datatype >
Procédure d'habilitation du personnel</name>
<objectifs rdf :datatype >
Vérifier, avant d'affecter une personne dans un poste sensible, que cela ne
risque pas de le mettre dans une situation de conflit d'intérêt ou dans une position
où il pourrait subir des pressions inacceptables</objectifs>
<mesureid rdf :datatype >
01C03</mesureid>
<resultatsattendus rdf :datatype >
Éviter que du personnel placé dans une position
de conflit difficile à gérer réagisse au détriment des intérêts de l'entreprise.</resultatsattendus>
</GererLesRessourcesHumaines>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype>
01.41c</code>
<name rdf :datatype >
Défaillance matérielle d'un système informatique central impossible à
résoudre par la maintenance, ou indisponibilité du prestataire</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
max(08D08) ;min(08D06 ;09E02))</mesurepalliative>
</AccidentOuPanne>
<VolOuEffacementSuppAmovible rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
08D09</mesurepalliative>
<name rdf :datatype >
Vol répété de bandes archives de programmes dans les locaux de stockage
des media, par une personne non autorisée</name>
<code rdf :datatype >
04.42</code>
<mesureprotection rdf :datatype >
08C03</mesureprotection>
<mesurepreventive rdf :datatype >
08C03</mesurepreventive>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<mesuredissuasive rdf :datatype >
08C03</mesuredissuasive>
</VolOuEffacementSuppAmovible>
<AccidentOuPanne rdf :ID="thontoInstance">
<name rdf :datatype >
Tir d'armes légères ou lancement de projectiles depuis la rue,
rendant indisponibles des systèmes informatiques centraux.</name>
<code rdf :datatype>
01.51c</code>
<mesurepalliative rdf :datatype>
08D01</mesurepalliative>

<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
</AccidentOuPanne>
<AbsenceDePersonnel rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D04</mesurerecuperation>
<mesurepalliative rdf :datatype >
01C02</mesurepalliative>
<code rdf :datatype >
01.13</code>
<name rdf :datatype >
Disparition de personnel stratégique</name>
</AbsenceDePersonnel>
<EffacementCodeExecutable rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype >
min(06C01 ;06C02)</mesurepreventive>
<code rdf :datatype >
04.12a</code>
<mesurepalliative rdf :datatype>
min(04A05 ;04A06)</mesurepalliative>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<name rdf :datatype>
Ecrasement total ou pollution massive des configurations
du réseau étendu, par un membre du personnel
(non administrateur)</name>
<mesureprotection rdf :datatype>
06C03</mesureprotection>
</EffacementCodeExecutable>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype>
04A07</mesurepalliative>
<mesurepreventive rdf :datatype>
03D01</mesurepreventive>
<code rdf :datatype >
02.21a</code>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesureprotection rdf :datatype>
min(03D02 ;03D03)</mesureprotection>
<name rdf :datatype>
Incendie : accident interne (corbeille à papier, cendrier, etc.) endommageant
gravement des équipements du réseau étendu</name>
</AccidentOuPanne>
<SurutilisationMalveillRessInfor rdf :ID="thontoInstance">
<name rdf :datatype >
Dégradation de performances du réseau étendu due à
la saturation du réseau par un ver</name>
<mesurepreventive rdf :datatype >
min(08D07 ;11D06)</mesurepreventive>
<mesurepalliative rdf :datatype >
04A04</mesurepalliative>
<mesureprotection rdf :datatype >
04D01</mesureprotection>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<code rdf :datatype >
03.42a</code>
</SurutilisationMalveillRessInfor>
<EffacementCodeExecutable rdf :ID="thontoInstance">
<mesureprotection rdf :datatype >
06C03</mesureprotection>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<name rdf :datatype >
Ecrasement total ou pollution massive des
configurations du réseau local par un membre
du personnel (non administrateur)</name>
<mesurepalliative rdf :datatype>
min(05A06 ;05A07)</mesurepalliative>
<code rdf :datatype >
04.12b</code>
<mesurepreventive rdf :datatype >
min(06C01 ;06C02)</mesurepreventive>

</EffacementCodeExecutable>
<ControlerEmisEtRecepDonnees rdf :ID="thontoInstance">
<protegecontre>
<FasificationMessage rdf :ID="thontoInstance">
<name rdf :datatype >
Faux message émis par un membre du personnel usurpant l'identité d'une personne accréditée avec falsification de signature</name>
1</potentialite>
<mesurepreventive rdf :datatype >
09F01</mesurepreventive>
3</impact>
<code rdf :datatype >
07.61</code>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
</FasificationMessage>
</protegecontre>
1</efficacite>
<name rdf :datatype>
Garantie d'origine, signature, électronique</name>
<mesureid rdf :datatype >
09F01</mesureid>
</ControlerEmisEtRecepDonnees>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype>
min(08D06 ;09E02)</mesurepalliative>
<code rdf :datatype>
02.33c</code>
<name rdf :datatype>
Inondation due à l'extinction d'un incendie voisin, mettant hors service des systèmes centraux</name>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
</AccidentOuPanne>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype>
03C01</mesurepreventive>
<mesurepalliative rdf :datatype>
04A07</mesurepalliative>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<code rdf :datatype>
01.31a</code>
<mesureprotection rdf :datatype>
min(03C02 ;03C03)</mesureprotection>
<name rdf :datatype>
Inondation due à une canalisation percée ou crevée et rendant indisponibles
des équipements du réseau étendu</name>
</AccidentOuPanne>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesureprotection rdf :datatype >
min(03D02 ;03D03)</mesureprotection>
<mesurepalliative rdf :datatype>
min(04A07 ;05A08 ;08D06 ;09E02)</mesurepalliative>
<mesurepreventive rdf :datatype>
03D01</mesurepreventive>
<code rdf :datatype>
02.21d</code>
<name rdf :datatype>
Incendie : accident interne (corbeille à papier, cendrier, etc.) endommageant gravement l'ensemble d'une salle informatique et télécom</name>
</AccidentOuPanne>
<AttribuerUnReferentielALaSecurite rdf :ID="thontoInstance">
<resultatsattendus rdf :datatype>
Faire en sorte que le management sache ce qu'il doit faire personnellement et ce qu'il doit exiger de son personnel, en termes de mesures de protection.
Éviter donc des défauts de protection par négligence ou méconnaissance et dissuader les actions volontaires nuisibles en ayant bien averti qu'elles étaient interdites.

</resultatsattendus>
<mesureid rdf :datatype>
01B02</mesureid>
<name rdf :datatype>
Directives générales relatives à la protection de l'information</name>
<objectifs rdf :datatype>
Expliciter et porter à la connaissance de l'ensemble du personnel les directives
et mesures à prendre concernant la protection de l'information.</objectifs>
</AttribuerUnReferentielALaSecurite>
<Assurer rdf :ID="thontoInstance">
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype>
03C01</mesurepreventive>
<name rdf :datatype >
Inondation due à une canalisation percée ou crevée et rendant
indisponibles des systèmes centraux</name>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype>
min(08D06 ;09E02)</mesurepalliative>
<code rdf :datatype>
01.31c</code>
<mesureprotection rdf :datatype >
min(03C02 ;03C03)</mesureprotection>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<name rdf :datatype>
Catastrophe naturelle telle que crue d'une rivière, remontée de la nappe phréatique,
débordement du réseau d'égouts, tornade avec destruction de la couverture, etc.
mettant hors service des systèmes centraux</name>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<code rdf :datatype>
02.32c</code>
<mesureprotection rdf :datatype>
min(03C02 ;03C03)</mesureprotection>
<mesurepalliative rdf :datatype>
min(08D06 ;09E02)</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype >
min(03A01 ;03A04)</mesurepreventive>
<code rdf :datatype >
01.22c</code>
<mesurepalliative rdf :datatype>
max(07D01 ;09E01 ;min(08D06 ;09E02) ;01E02)
</mesurepalliative>
<name rdf :datatype>
Accident de nature électrique (court-circuit), mettant hors service un système informatique central.</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesureprotection rdf :datatype >
03B04</mesureprotection>
<code rdf :datatype>
01.61b</code>
<mesurepreventive rdf :datatype>
min(03B01 ;03B02 ;03B03)</mesurepreventive>
<name rdf :datatype>

Petit vandalisme sur les équipements du réseau local, par des personnes
autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.).</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesuredissuasive rdf :datatype >
03B06</mesuredissuasive>
<mesurepalliative rdf :datatype >
05A04</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype>
min(08D06 ;09E02)</mesurepalliative>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<code rdf :datatype >
02.22c</code>
<name rdf :datatype>
Incendie naissant à l'occasion d'un court-circuit et endommageant
gravement des systèmes centraux</name>
<mesurepreventive rdf :datatype >
03D01</mesurepreventive>
<mesureprotection rdf :datatype >
min(03D02 ;03D03)</mesureprotection>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
min(08D06 ;09E02)</mesurepalliative>
<name rdf :datatype >
Catastrophe naturelle ou acidentelle : Chute de la foudre endommageant
gravement des systèmes centraux</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype>
02.11c</code>
<mesurepreventive rdf :datatype >
03A05</mesurepreventive>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<name rdf :datatype>
Terrorisme sabotage par des agents extérieurs : explosifs déposés à proximité
des locaux sensibles, mettant hors service des équipements du réseau local</name>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype>
05A08</mesurepalliative>
<code rdf :datatype >
02.41b</code>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<name rdf :datatype >
Petit vandalisme sur le câblage ou des baies de câblage du réseau étendu,
par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.).</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepreventive rdf :datatype >
03B07</mesurepreventive>
<code rdf :datatype >
01.62a</code>
</AccidentOuPanne>

</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
min(04A07 ;05A08 ;08D06 ;09E02)</mesurepalliative>
<code rdf :datatype >
01.31d</code>
<mesureprotection rdf :datatype>
min(03C02 ;03C03)</mesureprotection>
<mesurepreventive rdf :datatype>
03C01</mesurepreventive>
<name rdf :datatype >
Inondation due à une canalisation percée ou crevée et rendant indisponible
l'ensemble d'une salle informatique et télécom</name>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesureprotection rdf :datatype >
min(03D02 ;03D03)</mesureprotection>
<name rdf :datatype>
Incendie naissant à l'occasion d'un court-circuit et endommageant
gravement des équipements du réseau étendu</name>
<mesurepreventive rdf :datatype >
03D01</mesurepreventive>
<code rdf :datatype >
02.22a</code>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
04A07</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<ModificationMateriel rdf :ID="theseontologieInst>
<mesurepreventive rdf :datatype >
07D01</mesurepreventive>
<code rdf :datatype >
03.31c</code>
<name rdf :datatype >
Dégradation des performances applicatives due à une saturation accidentelle de ressources résultant d'un incident système</name>
<mesurepalliative rdf :datatype >
08D03</mesurepalliative>
<mesureprotection rdf :datatype>
08E01</mesureprotection>
</ModificationMateriel>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype >
02.41c</code>
<name rdf :datatype >
Terrorisme sabotage par des agents extérieurs : explosifs déposés
à proximité des locaux sensibles, mettant hors service des systèmes centraux</name>
<mesurepalliative rdf :datatype >
min(08D06 ;09E02)</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype>
01.51a</code>
<mesurepalliative rdf :datatype>

04A03</mesurepalliative>
<name rdf :datatype >
Tir d'armes légères ou lancement de projectiles depuis la rue,
rendant indisponible des équipements du réseau étendu.</name>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype>
09E01</mesurepreventive>
<name rdf :datatype >
Panne rendant indisponible un système informatique central</name>
<code rdf :datatype >
01.23c</code>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
max(07D01 ;08D01)</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<name rdf :datatype >
Assurer des dommages matériels</name>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesuredissuasive rdf :datatype>
03B06</mesuredissuasive>
<name rdf :datatype>
Petit vandalisme sur les systèmes informatiques centraux, par des
personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.).</name>
<mesurepreventive rdf :datatype>
min(03B01 ;03B02 ;03B03)</mesurepreventive>
<mesurepalliative rdf :datatype>
08D01</mesurepalliative>
<mesureprotection rdf :datatype>
03B04</mesureprotection>
<code rdf :datatype >
01.61c</code>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype>
03B07</mesurepreventive>
<code rdf :datatype>
01.62b</code>
<name rdf :datatype>
Petit vandalisme sur le câblage ou des baies de câblage du réseau local,
par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.).</name>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
</AccidentOuPanne>
</protegecontre>
<objectifs rdf :datatype >
Réduire le coût de certains sinistres en se couvrant par des assurances adaptées.</objectifs>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype >
01.23d</code>
<mesurepalliative rdf :datatype >
11D01</mesurepalliative>
<mesurerecuperation rdf :datatype >

01D01</mesurerecuperation>
<name rdf :datatype >
Panne rendant indisponible un système terminal mis à la disposition
des utilisateurs (PC, imprimante, périphérique spécifique, etc.)</name>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype>
01.21a</code>
<mesurepreventive rdf :datatype>
min(03A01 ;03A04)</mesurepreventive>
<name rdf :datatype>
Accident de nature électrique (court-circuit), mettant hors service un équipement du réseau étendu</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
max(04A01 ;04A07 ;01E02)</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<mesureid rdf :datatype >
01D01</mesureid>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype >
01.21c</code>
<mesurepreventive rdf :datatype >
min(03A01 ;03A04)</mesurepreventive>
<name rdf :datatype >
Accident de nature électrique (court-circuit), mettant hors service un système informatique central.</name>
<mesurepalliative rdf :datatype >
max(07D01 ;09E01 ;min(08D06 ;09E02) ;01E02)
</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<resultatsattendus rdf :datatype>
Limiter la perte finale du sinistre à un montant maximum en mutualisant les
pertes au dessus d'un certain seuil.</resultatsattendus>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype>
04A07</mesurepalliative>
<name rdf :datatype>
Catastrophe naturelle telle que crue d'une rivière, remontée de la nappe
phréatique, débordement du réseau d'égouts, tornade avec destruction
de la couverture, etc.mettant hors service des équipements du réseau étendu</name>
<code rdf :datatype>
02.32a</code>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesureprotection rdf :datatype >
min(03C02 ;03C03)</mesureprotection>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype>
01.23e</code>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype>
03A03</mesurepalliative>

<name rdf :datatype>
Servitude indispensable HS : arrêt de la climatisation entraînant l'arrêt
des équipements informatiques (panne grave ou rupture de canalisation d'eau)</name>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="theseontologieInst">
<name rdf :datatype>
Accident de nature électrique (court-circuit), mettant hors service
un équipement du réseau local</name>
<mesurepalliative rdf :datatype>
max(05A02 ;05A08 ;01E02)</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype >
01.21b</code>
<mesurepreventive rdf :datatype >
min(03A01 ;03A04)</mesurepreventive>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<ModificationMateriel rdf :ID="thontoInstance">
<name rdf :datatype>
Dégradation involontaire de performances, à l'occasion d'une opération
de maintenance matérielle évolutive d'un équipement du réseau étendu (hors télémaintenance)</name>
<mesurepreventive rdf :datatype>
06A03</mesurepreventive>
<code rdf :datatype >
03.21a</code>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
04A03</mesurepalliative>
</ModificationMateriel>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype >
01.41b</code>
<name rdf :datatype >
Défaillance matérielle d'un équipement du réseau local impossible à résoudre
par la maintenance, ou indisponibilité du prestataire</name>
<mesurepalliative rdf :datatype >
max(05A08 ;05A09)</mesurepalliative>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<name rdf :datatype >
Accidents dus à l'eau ou à des liquides (fuite d'une canalisation, liquides renversés accidentellement, etc.),
mettant hors service un équipement du réseau étendu</name>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepreventive rdf :datatype >
03C01</mesurepreventive>
<code rdf :datatype >
01.22a</code>
<mesurepalliative rdf :datatype >
max(04A01 ;04A07 ;01E02)</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
05A08</mesurepalliative>

<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<mesurepreventive rdf :datatype>
03A05</mesurepreventive>
<name rdf :datatype >
Catastrophe naturelle ou acidentelle : Chute de la foudre endommageant
gravement des équipements du réseau local</name>
<code rdf :datatype>
02.11b</code>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype>
02.32b</code>
<mesurepalliative rdf :datatype>
05A08</mesurepalliative>
<name rdf :datatype >
Catastrophe naturelle telle que crue d'une rivière, remontée de la nappe phréatique,
débordement du réseau d'égouts, tornade avec destruction de la couverture, etc.
mettant hors service des équipements du réseau local</name>
<mesurepreventive rdf :datatype >
min(03C02 ;03C03)</mesurepreventive>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype >
03C01</mesurepreventive>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype>
max(05A02 ;05A08 ;01E02)</mesurepalliative>
<code rdf :datatype>
01.22b</code>
<name rdf :datatype>
Accidents dus à l'eau ou à des liquides (fuite d'une canalisation, liquides renversés accidentellement, etc.),
mettant hors service un équipement du réseau local</name>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype >
01.23a</code>
<name rdf :datatype >
Panne rendant indisponible un équipement du réseau étendu</name>
<mesurepreventive rdf :datatype>
04A01</mesurepreventive>
<mesurepalliative rdf :datatype >
max(04A01 ;04A03)</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesureprotection rdf :datatype >
min(03D02 ;03D03)</mesureprotection>
03D01</mesurepreventive>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
05A08</mesurepalliative>
<code rdf :datatype>
02.22b</code>
<name rdf :datatype>
Incendie naissant à l'occasion d'un court-circuit et endommageant gravement

des équipements du réseau local</name>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype>
01.61a</code>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesureprotection rdf :datatype >
03B04</mesureprotection>
<mesurepreventive rdf :datatype >
min(03B01 ;03B02 ;03B03)</mesurepreventive>
<name rdf :datatype>
Petit vandalisme sur les équipements du réseau étendu, par des personnes
autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.).</name>
<mesuredissuasive rdf :datatype>
03B06</mesuredissuasive>
<mesurepalliative rdf :datatype >
04A03</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype >
01.24b</code>
<name rdf :datatype>
Accident de nature électrique externe à l'entreprise (court-circuit extérieur, coupure d'un câble, défaillance extérieure, etc.)
rendant indisponible l'environnement de travail des utilisateurs.</name>
<mesurerecuperation rdf :datatype>
01D01</mesurerecuperation>
<mesurepalliative rdf :datatype >
11D07</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<name rdf :datatype >
Incendie : accident interne (corbeille à papier, cendrier, etc.) endommageant
gravement des équipements du réseau local</name>
<mesurepreventive rdf :datatype >
03D01</mesurepreventive>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<code rdf :datatype >
02.21b</code>
<mesureprotection rdf :datatype>
min(03D02 ;03D03)</mesureprotection>
<mesurepalliative rdf :datatype>
05A08</mesurepalliative>
</AccidentOuPanne>
</protegecontre>
<protegecontre rdf :resource="thontoInstance"/>
<protegecontre>
<AccidentOuPanne rdf :ID="thontoInstance">
<code rdf :datatype>
01.41a</code>
<name rdf :datatype >
Défaillance matérielle d'un équipement du réseau étendu impossible à résoudre
par la maintenance, ou indisponibilité du prestataire</name>
<mesurepalliative rdf :datatype >
max(04A07 ;04A08)</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
</AccidentOuPanne>
</protegecontre>
</Assurer>
<AbsenceDePersonnel rdf :ID="thontoInstance">

<name rdf :datatype >
Départ de personnel stratégique</name>
<code rdf :datatype >
01.12</code>
<mesurepalliative rdf :datatype >
01C02</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D04</mesurerecuperation>
</AbsenceDePersonnel>
<GererLesRessourcesHumaines rdf :ID="theseontologie1">
<mesureid rdf :datatype >
01C06</mesureid>
<objectifs rdf :datatype >
Gérer les utilisateurs du système d'information de manière à pouvoir tracer
toute action et l'imputer à une personne physique</objectifs>
<resultatsattendus rdf :datatype >
Faire en sorte que tout utilisateur du système d'information puisse être identifié
de manière sûre et sans ambiguïté et cela dès l'attribution de droits généraux..</resultatsattendus>
<name rdf :datatype >
Enregistrement des personnes</name>
</GererLesRessourcesHumaines>
<ControleAccesApplicatifs rdf :ID="thontoInstance">
<mesureassocie>
<ControlerAccesAuxApplications rdf :ID="thontoInstance">
<protegecontre rdf :resource="thontoInstance"/>
<name rdf :datatype>
Authentificationdesaccédants</name>
<mesureid rdf :datatype>
09A03</mesureid>
2</efficacite>
</ControlerAccesAuxApplications>
</mesureassocie>
<nomindicateur rdf :datatype >
Authentificationaccédants</nomindicateur>
<risqueassocie rdf :resource="thontoInstance"/>
</ControleAccesApplicatifs>
<IndisponibiliteTotaleLocaux rdf :ID="thontoInstance">
<code rdf :datatype>
01.71c</code>
<mesurepalliative rdf :datatype >
11D07</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<name rdf :datatype >
Interdiction totale d'accès décrétée par les autorités empêchant les
utilisateurs d'accéder à leurs bureaux</name>
</IndisponibiliteTotaleLocaux>
<DestructionConfigLog rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype>
11D06</mesurepreventive>
<code rdf :datatype>
04.51a</code>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<mesurepalliative rdf :datatype >
11D03</mesurepalliative>
<name rdf :datatype >
Effacement de configurations utilisateurs par un virus</name>
</DestructionConfigLogicielles>
<ControleIntegriteDonnees rdf :ID="thontoInstance">
<mesureassocie rdf :resource="thontoInstance"/>
<risqueassocie rdf :resource="thontoInstance"/>
<nomindicateur rdf :datatype >
Contrôledesaisiedesdonnées</nomindicateur>
</ControleIntegriteDonnees>
<EffacementAccidDisqueFixe rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<mesurepalliative rdf :datatype>
08D04</mesurepalliative>
<code rdf :datatype>

04.21</code>
<name rdf :datatype >
Ecrasement accidentel d'un disque fixe contenant des programmes
exécutables dû à une panne de matériel</name>
</EffacementAccidDisqueFixe>
<StructurerLaSecurite rdf :ID="thontoInstance">
<name rdf :datatype >
Organisation des audits et du plan d'audit</name>
<mesureid rdf :datatype >
01A04</mesureid>
<resultatsattendus rdf :datatype >
Éviter que les recommandations ou directives exprimées ne soient pas suivies et que les comportements se dégradent au fil du temps.
La fonction sécurité de l'information est souvent placée en position de conseil et de diagnostic.
Il lui est donc difficile d'assumer simultanément une fonction véritable d'audit : il est alors souhaitable que cette fonction soit prise en charge par une structure dont c'est le métier et d'assurer les liaisons nécessaires avec elle.</resultatsattendus>
<objectifs rdf :datatype>
Exprimer les besoins d'audit de sécurité des SI et faire prendre en compte
ces besoins par une structure d'audit (interne ou externe).</objectifs>
</StructurerLaSecurite>
<SurutilisationMalveillRessInfor rdf :ID="thontoInstance">
<mesureprotection rdf :datatype>
05D01</mesureprotection>
<name rdf :datatype>
Dégradation de performances du réseau local due à la saturation du réseau par un ver</name>
<code rdf :datatype>
03.42b</code>
<mesurepalliative rdf :datatype >
05A05</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<mesurepreventive rdf :datatype>
min(08D07 ;11D06)</mesurepreventive>
</SurutilisationMalveillRessInfor>
<EffacementCodeExecutable rdf :ID="thontoInstance">
<mesuredissuasive rdf :datatype>
08F03</mesuredissuasive>
<name rdf :datatype>
Effacement direct de code exécutable par une personne autorisée
(exploitation, support informatique, maintenance, etc.)</name>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<code rdf :datatype >
04.11</code>
<mesurepalliative rdf :datatype>
08D04</mesurepalliative>
</EffacementCodeExecutable>
<ControlerIntegriteDonnees rdf :ID="thontoInstance">
<protegecontre rdf :resource="thontoInstance"/>
2</efficacite>
<name rdf :datatype>
Protection de l'intégrité des données échangées</name>
<mesureid rdf :datatype>
09B02</mesureid>
</ControlerIntegriteDonnees>
<ControlerAccesAuxApplications rdf :ID="thontoInstance">
<protegecontre rdf :resource="thontoInstance"/>
3</efficacite>
<mesureid rdf :datatype>
09A01</mesureid>
<name rdf :datatype>
Gestion des profils d'accès aux données applicatives</name>
</ControlerAccesAuxApplications>
<IndisponibiliteTotaleLocaux rdf :ID="thontoInstance">
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>

<mesurepalliative rdf :datatype>
max(04A02 ;04A07)</mesurepalliative>
<name rdf :datatype>
Interdiction totale d'accès décrétée par les autorités entraînant un arrêt du réseau étendu</name>
<code rdf :datatype>
01.71a</code>
</IndisponibiliteTotaleLocaux>
<ModificationLogiciel rdf :ID="thontoInstance">
<mesurepreventive rdf :datatype >
min(08A04 ;10B05)</mesurepreventive>
<code rdf :datatype >
03.11</code>
<mesurepalliative rdf :datatype>
08D04</mesurepalliative>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<name rdf :datatype>
Dégradation involontaire des performances applicatives, à l'occasion
d'une opération de maintenance corrective ou évolutive de logiciel ou de progiciel</name>
</ModificationLogiciel>
<GererLesRessourcesHumaines rdf :ID="thontoInstance">
<objectifs rdf :datatype>
Faire en sorte que tous les personnels (utilisateurs, managers et informaticiens) comprennent les enjeux de la sécurité et sachent quelle conduite tenir vis-à-vis de
l'information ou des ressources spécifiques qu'ils gèrent ou utilisent.</objectifs>
<resultatsattendus rdf :datatype>
Limiter l'exposition à des erreurs ou accidents par manque d'attention,
par inadvertance ou par méconnaissance des mesures adéquates.</resultatsattendus>
<mesureid rdf :datatype >
01C04</mesureid>
<name rdf :datatype>
Sensibilisation et formation à la sécurité</name>
</GererLesRessourcesHumaines>
<AccidentOuPanne rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
max(07D01 ;09E01 ;min(08D06 ;09E02) ;01E02)
</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D01</mesurerecuperation>
<name rdf :datatype>
Accidents dus à l'eau ou à des liquides mettant hors service un système informatique central.</name>
<mesurepreventive rdf :datatype>
03C01</mesurepreventive>
<code rdf :datatype >
01.22c</code>
</AccidentOuPanne>
<ControleEmissionRecepDonnees rdf :ID="thontoInstance">
<description rdf :datatype>
Les indicateurs mesureront l'évolution de la qualité des transactions automatisées</description>
<cible rdf :datatype >
Nombre d'accusés de réception non reçus sur une période</cible>
<nomindicateur rdf :datatype >
signanitureelectronique</nomindicateur>
<risqueassocie rdf :resource="thontoInstance"/>
<mesureassocie rdf :resource="thontoInstance"/>
</ControleEmissionRecepDonnees>
<StructurerLaSecurite rdf :ID="thontoInstance">
<mesureid rdf :datatype >
01A05</mesureid>
<resultatsattendus rdf :datatype >
Éviter qu'en cas d'accident grave touchant les systèmes d'information,
on perde un temps précieux pour réunir les personnes concernées par les décisions à prendre.</resultatsattendus>
<name rdf :datatype >

Gestion de crise liee a la securite de l information</name>
<objectifs rdf :datatype >
Faire en sorte qu'en cas d'accident ou de crise grave touchant les systèmes
d'information, une cellule de crise puisse être réunie rapidement avec les personnes
concernées, compétentes et habilitées à prendre et à faire appliquer les décisions nécessaires.</objectifs>
</StructurerLaSecurite>
<IndisponibiliteTotaleLocaux rdf :ID="thontoInstance">
<code rdf :datatype>
01.71b</code>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<mesurepalliative rdf :datatype >
max(min(05A03 ;08A03) ;min(08D06 ;09E02))
</mesurepalliative>
<name rdf :datatype >
Interdiction totale d'accès décrétée par les autorités entraînant un arrêt des systèmes centraux</name>
</IndisponibiliteTotaleLocaux>
<AbsenceDePersonnel rdf :ID="thontoInstance">
<code rdf :datatype >
01.11</code>
<expositionnaturelle rdf :datatype >
AV01</expositionnaturelle>
<name rdf :datatype>
absencepersonnelexploitation</name>
<mesurepalliative rdf :datatype>
09E03</mesurepalliative>
<impactintrinseque rdf :datatype>
P02</impactintrinseque>
</AbsenceDePersonnel>
<DestructionConfigLog rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype>
11D03</mesurepalliative>
<code rdf :datatype>
04.51b</code>
<mesurepreventive rdf :datatype>
11D06</mesurepreventive>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<name rdf :datatype>
Effacement de logiciels spécifiques utilisateurs par un virus</name>
</DestructionConfigLogicielles>
<ControleIntegriteDonnees rdf :ID="thontoInstance30020">
<nomindicateur rdf :datatype>
intégritédesdonnée echangées</nomindicateur>
<mesureassocie rdf :resource="thontoInstance30021"/>
<risqueassocie rdf :resource="thontoInstance30022"/>
</ControleIntegriteDonnees>
<GererLesRessourcesHumaines rdf :ID="thontoInstance19">
<name rdf :datatype >
Gestion du personnel stratégique</name>
<mesureid rdf :datatype >
01C02</mesureid>
<objectifs rdf :datatype>
Limiter, si possible les causes de départ ou d'absence de personnel stratégique.
Limiter les conséquences de tels départ ou absences, le cas échéant.</objectifs>
<protegecontre rdf :resource="thontoInstancee21"/>
<protegecontre rdf :resource="thontoInstance20"/>
<resultatsattendus rdf :datatype>
Réduire les risques liés à une indisponibilité ou à une absence
de personnel stratégique.</resultatsattendus>
</GererLesRessourcesHumaines>
<AttribuerUnReferentielALaSecurite rdf :ID="thontoInstance14">
<objectifs rdf :datatype>
Expliciter et porter à la connaissance du management les comportements
souhaités, admis et interdits, tant de la part du personnel que du management.</objectifs>
<resultatsattendus rdf :datatype>

Faire en sorte que le management sache ce qu'il doit faire personnellement et ce qu'il doit exiger de son personnel, en termes de comportement.</resultatsattendus>
<name rdf :datatype >
Devoirs et responsabilités du personnel et du management</name>
<mesureid rdf :datatype >
01B01</mesureid>
</AttribuerUnReferentielALaSecurite>
<IndisponibiliteTotaleLocaux rdf :ID="thontoInstance">
<mesurepalliative rdf :datatype >
max(04A02 ;04A07)</mesurepalliative>
<mesurerecuperation rdf :datatype>
01D02</mesurerecuperation>
<code rdf :datatype >
01.71a</code>
<name rdf :datatype >
Interdiction totale d'accès décrétée par les autorités entraînant un arrêt du réseau étendu</name>
</IndisponibiliteTotaleLocaux>
<StructurerLaSecurite rdf :ID="thontoInstance8">
<resultatsattendus rdf :datatype>
Les résultats attendus sont multiples : Détecter les évolutions lentes et permettre
une meilleure anticipation des mesures nécessaires , Favoriser une mise en commun
et une capitalisation des connaissances acquises à l'occasion de la gestion des
incidents et diffuser cette connaissance aux personnes intéressées
Participer à la formation et à la sensibilisation des opérationnels et des utilisateurs</resultatsattendus>
<objectifs rdf :datatype >
Avoir une vue globale, et une mise en perspective dans le temps, des incidents,
que ces incidents soient réels ou soupçonnés, que les tentatives aient abouti ou non.</objectifs>
<name rdf :datatype >
Systeme general de reporting et de gestion des incidents</name>
<mesureid rdf :datatype >
01A03</mesureid>
</StructurerLaSecurite>
<EffacementAccidentelLogiciel rdf :ID="thontoInstance20024">
<mesurepalliative rdf :datatype >
08D04</mesurepalliative>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<name rdf :datatype >
Effacement accidentel de logiciel exécutable par erreur humaine</name>
<code rdf :datatype >
04.31</code>
</EffacementAccidentelLogiciel>
<EffacementCodeExecutable rdf :ID="thontoInstance20022">
<code rdf :datatype >
04.12d</code>
<mesurerecuperation rdf :datatype >
01D02</mesurerecuperation>
<name rdf :datatype >
Ecrasement total ou pollution massive des configurations applicatives par
un membre du personnel (non administrateur)</name>
<mesureprotection rdf :datatype>
08F03</mesureprotection>
<mesurepalliative rdf :datatype>
08D04</mesurepalliative>
<mesurepreventive rdf :datatype >
min(08F01 ;08F02)</mesurepreventive>
</EffacementCodeExecutable>
<ControleAccesApplicatifs rdf :ID="thontoInstance30012">
<nomindicateur rdf :datatype >
profilsaccèsdonneesapplicatives</nomindicateur>
<mesureassocie rdf :resource="thontoInstance30013"/>
<risqueassocie rdf :resource="thontoInstance30016"/>
</ControleAccesApplicatifs>

</rdf :RDF>

< !– Created with Protege (with OWL Plugin 3.3.1,
Build 430) http ://protege.stanford.edu –>