Méta modèle de la sécurité des systèmes d'information : enrichissement par le contexte

Jacky Akoka, Nabil Laoufi, Nadira Lammari

Méta modèle de la sécurité des systèmes d'information

Enrichissement par le contexte

Jacky Akoka[1,2], Nabil Laoufi[3], Nadira Lammari[1]

1. CEDRIC-CNAM
292 Rue Saint-Martin, 75003 Paris, France
lammari@cnam.fr, jacky.akoka@lecnam.net

2. Institut Mines Télécom- TEM
9 rue Charles Fourier, 91011 Evry, France
jacky.akoka@telecom-em.eu

3. Ecole militaire polytechnique
BP 17, Bordj el Bahri ,16111, Alger, Algérie
nabil.laoufi@gmail.com

RESUME. Les entreprises sont confrontées de plus en plus aux problèmes induits par leur dépendance vis-à-vis des systèmes d'information. Elles se voient ainsi contraintes à mettre en œuvre un processus de dérivation des exigences de sécurité à partir de l'analyse des risques encourus. Ce processus requiert au préalable une analyse approfondie du contexte organisationnel. Le but de cet article est de proposer un méta modèle de sécurité enrichi par une ontologie du contexte. A cette fin, nous proposons (i) le développement d'une ontologie du contexte fondée sur la norme de sécurité ISO/CEI 27000 : 2018, (ii) une démarche d'enrichissement du méta modèle de sécurité par l'ontologie du contexte. Cet enrichissement est réalisé en deux phases. La première est relative à l'identification et à l'extraction des éléments du contexte de l'entreprise. La seconde concerne la détermination des critères de sécurité des actifs de l'organisation à protéger et (iii) l'application à un cas réel qui sert aussi de première étape dans la validation de notre démarche.

Mots-clés : Systèmes d'information, sécurité, ontologie, contexte, actifs, méta modèle

ABSTRACT. Companies are increasingly confronted with the problems caused by their reliance on information systems. They are thus forced to implement a process of security requirements derivation starting from risks analysis. This process requires a thorough analysis of the organizational context. The purpose of this article is to propose a security meta model enriched by an ontology of the context. To this end, we propose (i) the development of a context ontology based on the ISO / IEC 27000: 2018 security standard, (ii) an approach to enrich the security meta model with context ontology. This enrichment is carried out in two phases. The first is related to the identification and extraction of elements of the context of the enterprise. The second concerns the determination of the security criteria of the assets of the

organization to be protected and (iii) the application to a real case which also serves as a first step in the validation of our approach.

KEYWORDS: Information systems, security, ontology, context, assets, meta model.

1. Introduction

Les systèmes d'information (SI) doivent faire face à de nombreuses menaces susceptibles d'exploiter leurs vulnérabilités. Le but d'une politique de la sécurité est de limiter les impacts résultant de ces vulnérabilités. Cette politique est fondée sur la capacité des organisations à mettre en œuvre une procédure de dérivation des exigences de sécurité fondée sur l'analyse des risques qui ciblent le système d'information. Plusieurs méthodes permettent de dériver les exigences de sécurité à partir de l'analyse des risques (Lammari et al., 2011 ; Laoufi, 2017; Vasquez et al., 2012). Toutefois, la plupart n'intègre pas les contextes interne et externe des organisations.

Le concept de « contexte » ne fait pas l'objet d'une définition unanime. Cela est sans doute dû au fait qu'il n'existe pas un contexte déterminé par avance. (IFIP-IFAC Task Force, 2003) indique que « le contexte dépend des conditions interdépendantes dans lesquelles un événement, une action, etc. a lieu ». La définition la plus répandue est due à (Abowd et al., 1999) qui précisent que : « le contexte représente toute information qui peut être utilisée pour caractériser la situation d'une entité. Une entité est une personne, un objet ou un endroit considéré comme pertinent pour l'interaction entre un utilisateur et une application, y compris l'application et l'utilisateur ». En d'autres termes, le contexte peut être décrit comme étant constitué d'un ensemble d'attributs ayant un lien avec une finalité pour laquelle le contexte est utilisé.

Les linguistes et les chercheurs en langage naturel utilisent le concept de contexte pour interpréter le sens des phrases. Par exemple, la phrase « Je tiens à jouer avec ma sœur », indique que ma sœur et moi jouons ensemble et non qu'elle est un jouet. Autrement dit, le contexte social rétrécit l'interprétation correcte d'une expression (Leech, 1981).

Le contexte peut servir à limiter l'espace des solutions pour des problèmes liés au raisonnement automatique (Brézillon and Abu-Hakima, 1995). À titre d'exemple, les moteurs de recherche Web filtrent l'information en estimant sa pertinence dans des contextes déterminés d'interprétation, telle que la popularité des pages (Yahoo, Google), les catégories (recherches), les zones géographiques (France), etc.

En informatique, le contexte est généralement lié aux conditions dans lesquelles les utilisateurs sont immergés (poste de travail, réseau, communication, bande passante, sécurité). Dans le domaine de la sécurité des informations, le contexte joue un rôle primordial, qu'il soit un contexte interne ou un contexte externe. Le risque et les mesures de protection changent d'après le contexte. Ainsi, on ne protège pas un serveur de banque de la même façon qu'un simple serveur de messagerie d'une petite entreprise.

Le but de cet article est de proposer un méta modèle de la sécurité qui intègre le contexte des organisations. Le méta modèle de base repose sur des modèles ontologiques fondés sur les concepts relatifs à l'analyse des risques et à la dérivation des exigences de sécurité. Notre proposition permet l'enrichissement de ce méta modèle grâce à une ontologie du contexte. À cette fin, nous avons analysé les modèles de contexte existants. Les concepts sous-jacents permettent de peupler l'ontologie du contexte. Le reste de cet article est organisé comme suit. La section 2 présente un état de l'art sur les ontologies du contexte. La section suivante est précisément consacrée à la construction de l'ontologie de contexte. Nous présentons à la section 4 le méta modèle de la sécurité et son enrichissement par l'ontologie du contexte. A l'issue de cette phase nous obtenons un méta modèle de la sécurité qui intègre le contexte notamment dans sa relation avec les actifs à protéger. La section 5 est consacrée à l'illustration de notre démarche par une étude de cas réel. La conclusion et à la présentation de quelques voies de recherche future font l'objet de la dernière section.

2. Ontologie du contexte : un état de l'art

Le terme contexte, bien que présent dans une multitude de travaux de recherche, ne fait pas l'objet d'une définition consensuelle (Brazire and Brézillon, 2005). Son interprétation et son éventuelle formalisation dépend du domaine d'utilisation. A titre d'exemple, dans le « mobile-learning », le contexte peut aider et soutenir le processus d'apprentissage en fournissant des informations pertinentes ou des services dont l'apprenant peut avoir besoin. (Ardila, 2013). Dans ce contexte d'apprentissage, (Christopoulos, 2008) propose un modèle de contexte à cinq dimensions (information temporelle de l'utilisateur, lieu, artefact, temps et conditions physiques). Ce modèle a, par la suite, été enrichi dans (Gomez et al., 2014) par l'introduction de nouvelles dimensions et de nouveaux éléments de contexte caractérisant ces dimensions. Ces éléments sont décrits dans une taxonomie présentée dans (Ardila, 2013).

Dans le cadre de l'informatique orienté service, (Cabrera et al., 2014) adoptent la définition du contexte proposée dans (Dey, 2001) pour le développement d'applications sensibles au contexte. A l'issue d'un état de l'art sur la modélisation du contexte fondée sur les ontologies (Aguilar et al., 2017), ces auteurs proposent une description du contexte (sous forme d'une ontologie) à partir de onze éléments de contexte (concepts) identifiés : le temps, le lieu, l'activité, l'environnement, le facteur humain, la ressource, la politique, la préférence, le rôle, le profil et l'infrastructure). Des synonymes ont été associés aux différents concepts.

Dans le cadre de la modélisation d'applications sensibles au contexte dans les nuages (context-aware application in the cloud), (Aguilar et al., 2017) proposent une ontologie nommée CAMeOnto, associée à leur outil CARMiCLOC, dans l'objectif de construire un contexte et de le partager. L'ontologie proposée est fondée sur le principe des 5W (Who, When, What, Where et Why). Elle réutilise les deux ontologies CONON et MAont présentées respectivement dans (Guermah et al., 2014) et (Zhong-Jun et al., 2016). Cette ontologie regroupe six concepts, reliés entre

eux, et décrivant le contexte : l'utilisateur, l'activité, le temps, le lieu, le service et le dispositif.

Pour caractériser le contexte dans lequel une application d'entreprise doit fournir ses services, (Nadoveza et al., 2014) proposent de distinguer, dans leur ontologie, (1) les informations concernant les caractéristiques de l'application, (2) celles concernant le contexte métier telles que les activités en cours associées au métier (3) celles qui décrivent le contexte utilisateur tels que ses préférences et le dispositif qu'il utilise pour accéder.

A côté des travaux de recherche sur la description et la modélisation du contexte, on trouve aussi un certain nombre de normes faisant référence à ce terme et à ses composants sans pour autant offrir une modélisation correspondante. A titre d'exemple, pour la mise en place d'un système de management de la qualité (SMQ), la norme ISO 9001 :2015[1] exige des organisations, à travers la clause « Context of the organisation », la compréhension du contexte interne et externe à l'organisation. La compréhension du contexte externe, tel que le mentionne la norme, peut être facilitée par l'examen des problèmes pouvant découler des environnements juridiques, technologiques, concurrentiels, culturels, etc. La compréhension du contexte interne peut être facilitée par l'examen de questions liées aux valeurs, à la culture, aux connaissances et aux performances de l'organisation.

Aussi, une des lignes directrices relatives à la gestion des risques en sécurité de l'information mentionnées dans la norme ISO/IEC 27005:2011[2] est l'établissement du contexte de l'organisation. La norme ISO/CEI 27000 :2018[3] qui comprend les termes et les définitions d'usage courant dans la famille des normes SMSI (Systèmes de Management de la Sécurité de l'Information) dont fait partie la norme ISO/IEC 27005:2011, distingue le contexte interne du contexte externe. Elle définit ce dernier comme étant l'environnement extérieur dans lequel l'organisation cherche à atteindre ses objectifs. Cela peut inclure : (i) les aspects culturels, sociaux, politiques, juridiques, réglementaires, financiers, technologiques, économiques, naturels ainsi que l'environnement concurrentiel, qu'il soit international, national, régional ou local ; (ii) les principales tendances ayant un impact sur les objectifs de l'organisation ; (iii) les perceptions et les valeurs des parties prenantes externes. Le contexte interne, quant à lui, est défini, dans cette même norme, comme intégrant : (i) la gouvernance, la structure organisationnelle, les rôles et les responsabilités; (ii) les politiques, les objectifs et les stratégies qui sont en place pour les atteindre ; (iii) les capacités, exprimées en termes de ressources et de connaissances (par exemple le capital, le temps, les gens, les processus, les systèmes et les technologies); (iv) les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formel et informel) ; (v) les relations avec et les perceptions et les valeurs des parties prenantes internes ; (v) la culture de l'organisation ; (vi) les normes,

1 https://www.iso.org/fr/standard/62085.html
2 https://www.iso.org/standard/56742.html
3 https://www.iso.org/standard/73906.html

directives et modèles adoptés par l'organisation ; et (vii) la forme et l'étendue des relations contractuelles.

Des méthodes de gestion des risques informatiques, telles que EBIOS (ANSSI, 2010) et MAGERIT (Amutio et al., 2014) soulignent aussi l'importance de l'établissement du contexte et décrivent textuellement le contexte d'une organisation. La méthode EBIOS considère que le contexte est composé de deux catégories. L'une est externe et comprend l'environnement social, culturel, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, tant au niveau international, national, que régional ou local. Elle considère aussi les facteurs et les tendances ayant un impact déterminant sur les objectifs ainsi que les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs. L'autre catégorie, interne, comprend la description générale de l'organisme, les aptitudes en matière de gestion des ressources, les missions, les valeurs, les métiers, etc. La méthode MAGERIT fait la différence entre le contexte interne et les autres concepts qui constituent l'ensemble du contexte. Le contexte interne est composé des politiques internes ainsi que des intervenants internes et du management ou de ses représentants.

3. Construction de l'ontologie du contexte

Une ontologie est une relation de concepts permettant de partager un ensemble de connaissances d'un domaine donné. Exploitable par les systèmes informatiques, elle permet d'expliciter et d'interpréter les termes nécessaires pour partager la connaissance liée à ce domaine. Deux types de conception existent: la conception manuelle et celle fondée sur des apprentissages. Le premier type est coûteux et surtout pose des problèmes de maintenance et de mise à jour. La conception reposant sur des apprentissages utilise des procédés de construction plus automatiques qui mènent généralement à la conception d'ontologies dites légères. Dans (Maedche et al., 2001) différents types d'approches sont distingués. Les méthodologies de construction d'ontologies les plus connues sont : KACTUS (modelling Knowledge About Complex Technical systems for multiple USe) (Kactus, 1996) et METHONTOLOGY (Fernández-López et al., 1997) qui s'applique à clarifier les différentes phases de la construction en respectant les activités de gestion de projets, de développement et des activités de support. Les activités de gestion de projet correspondent aux activités qui initient et suivent le projet. Les activités de support assurent la réussite du projet. Parmi ces activités de support, on peut citer l'activité d'acquisition des connaissances des experts du domaine ou encore à partir de la documentation fournit par des experts du domaine. Dans les activités de développement, on retrouve les activités de spécification des besoins, de conceptualisation et de formalisation de l'ontologie. Citons aussi la méthode On-To-Knowledge (Staab, et al., 2001) qui tient compte du domaine d'application de l'ontologie en construction. Enfin, Neon (Suárez-Figueroa et al., 2012) propose un cadre méthodologique fondé sur neuf scénarios de construction d'ontologies.

Pour la construction de notre ontologie de contexte, nous avons choisi de mettre en œuvre les activités de développement décrits dans Methonthology. Dans ce cadre nous avons d'abord réuni l'ensemble des sources d'information utiles à sa construction (activité d'acquisition des connaissances) sachant que notre objectif est de l'utiliser pour récupérer le contexte d'une entreprise dans le cadre d'un processus de dérivation des exigences de sécurité fondée sur l'analyse des risques (spécification des besoins). De notre état de l'art, nous avons retenu comme source d'information les documents décrivant les méthodes d'analyse des risques informatiques (EBIOS et MAGERIT en font partie) et les normes ISO citées dans notre état de l'art.

L'activité de conceptualisation a été menée de façon incrémentale. Le premier incrément a consisté à extraire de la norme ISO/CEI 27000 : 2018, tous les termes décrivant le contexte ainsi que les liens pouvant exister entre eux et d'en faire une abstraction sous forme de digramme des classes UML. Chaque incrément qui a suivi a permis de traiter une source d'information parmi celles sélectionnées dans la phase d'acquisition des connaissances. Ce traitement a consisté à extraire les termes relatifs au contexte afin d'enrichir, si besoin est, le modèle conceptuel issu de l'incrément précédent. Ceci nous a permis d'obtenir le modèle conceptuel de l'ontologie du contexte ci-dessous (Figure 1).

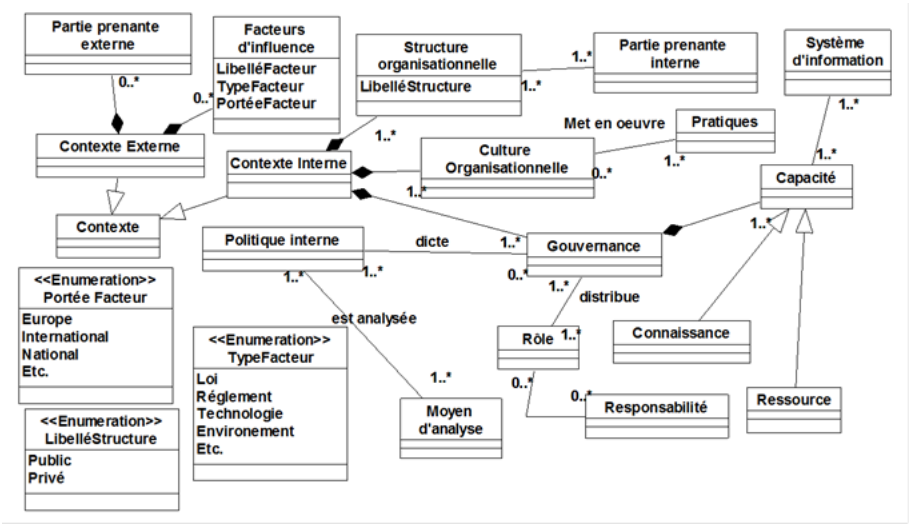

Figure 1. Ontologie du contexte

4. Processus d'enrichissement du méta modèle de la sécurité

Nous présentons ci-dessous (Figure 2) une démarche en deux phases qui permet d'instancier le méta modèle de sécurité (Figure 3) qui sert de base au processus de dérivation des objectifs de sécurité fondée sur l'analyse des risques.

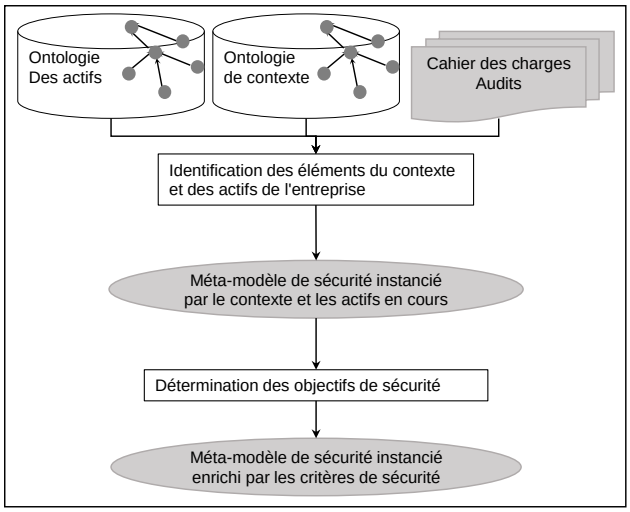

Figure 2. Processus d'enrichissement du méta modèle de la sécurité.

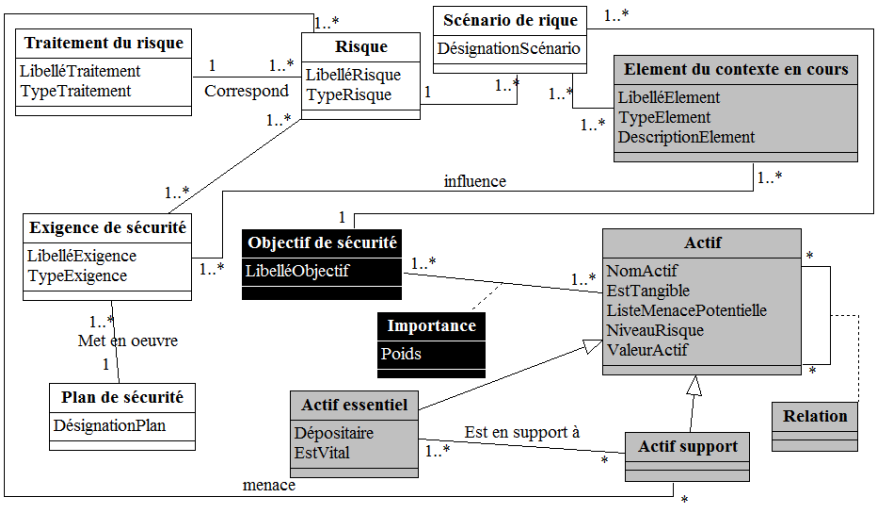

Figure 3 : Méta modèle de la sécurité.

Notre méta modèle a été construit sur la base de nos travaux antérieurs (Vasquez et al., 2012), (Laoufi, 2017). Il est composé de trois groupes de concepts. Le premier groupe (en noir) est constitué des concepts relatifs aux objectifs de sécurité. Le second groupe (en blanc) est relatif aux concepts utilisés dans la phase de dérivation des exigences de sécurité. Le dernier groupe (en gris) est composé des concepts relatif au contexte qui comporte aussi ceux des actifs. Les vulnérabilités sont des propriétés de ces derniers. Toutefois, il faut noter que les vulnérabilités sont une des

composantes du risque. Il y a une relation entre le concept de risque et le concept d'actif support qu'on dénomme menace. Les critères de sécurité sont proposés pour les actifs de l'organisation, comme le propose le modèle des actifs de la méthode ISSRM (Naudet, 2016). Chaque relation possède un poids défini d'après la situation d'exploitation de l'actif. Cette valeur est tirée des méthodes utilisées généralement pour la construction de l'ontologie des actifs (Laoufi, 2017). Nous considérons que les actifs font partie du contexte. L'ensemble des actifs sont inclus dans l'ensemble du contexte, si tous les éléments des actifs sont aussi éléments du contexte.

Le contexte joue un rôle prépondérant dans la proposition des exigences de sécurité. Il existe un lien et une certaine interdépendance entre le contexte et les exigences de sécurité. Du fait que ces deux concepts sont rarement formalisés dans les démarches orientées sécurité et afin de formaliser le lien entre le contexte et les exigences de sécurité, nous rajoutons deux concepts du contexte (ressources, connaissances) et nous proposons une association dénommée "influence" dans le méta-modèle de la sécurité.

4.1. Identification des éléments du contexte et des actifs de l'entreprise

Cette phase requiert en entrée des informations concernant l'entreprise (cahiers des charges pour la conception du SI et/ou des audits s'ils existent) et les ontologies du contexte et des actifs. L'ontologie des actifs est décrite dans (Laoufi, 2017).

L'identification des éléments du contexte de l'entreprise requiert le recours à l'ontologie du contexte présentée dans la section 3. A cette fin, nous faisons appel à une technique d'extraction d'information pour capturer, comparer et identifier les éléments du contexte contenus dans les sources fournies par l'entreprise. Rappelons que l'extraction d'informations est un processus par lequel un système automatique est capable de traiter des documents par une approche linguistique (Turenne, 2010). Nous avons choisi les logiciels AutoMap (Carley et al, 2013a) et ORA (Carley et al, 2013b) pour réaliser les opérations d'extraction des informations et de visualisation des résultats. Automap est un outil dédié à l'exploration des textes. Il permet l'extraction d'informations à partir des textes en utilisant des méthodes d'analyse de texte. Il soutient l'extraction de plusieurs types de données, de documents non structurés. L'information qui peut être extraite comprend : le contenu des données analytiques (mots et fréquences), les données du réseau sémantique (réseau de concepts), les données méta réseau (la classification croisée des concepts dans leur catégorie ontologique comme les gens, les lieux et les choses et les liens entre ces concepts classés), et les données de sentiment (attitudes, croyances). Le logiciel ORA sert, quant à lui, à visualiser les données. À noter que cette phase s'exécute automatiquement en utilisant un logiciel d'exploration de texte fondé sur les approches syntaxiques. La mise en œuvre s'appuie pour son application sur un filtrage que nous avons conçu en utilisant les connaissances qui peuplent l'ontologie du contexte.

Cette ontologie contribue à la détection des éléments de contexte se trouvant dans les documents en entrée du processus (cahiers des charges et/ou rapports

d'audit) ainsi que qu'à leur regroupement en concepts génériques. Elle permet aussi de repérer les actifs.

A l'issue de l'identification des éléments du contexte et des actifs de l'entreprise, nous instancions notre modèle de la sécurité (Figure 3). Cette instanciation concerne la partie grisée de notre méta modèle.

4.2. Détermination des objectifs de sécurité

Cette deuxième phase de notre démarche consiste à déterminer les objectifs de sécurité des actifs de l'organisation en vue de leur instanciation dans le méta modèle de la sécurité. Ces objectifs de sécurité sont là pour garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Chaque actif peut avoir un ou plusieurs objectifs de sécurité selon le contexte d'utilisation et un niveau de gravité selon le scénario de risque. Pour cela, nous avons rajouté comme guidage à l'utilisateur un concept (poids) dans le méta modèle de sécurité qui possède comme attribut le niveau de gravité d'utilisation d'un des quatre objectifs de sécurité qui sont (ISO/IEC 2700:2018) :

- La confidentialité : propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus (3.54) non autorisés ;
- La disponibilité : propriété selon laquelle l'information est accessible et utilisable à la demande par une entité autorisée ;
- L'intégrité : propriété selon laquelle l'information est exacte et complète ;

Le résultat de cette étape est l'enrichissement du méta modèle de la sécurité avec les objectifs de sécurité des actifs de l'entreprise en précisant le poids de réalisation de chacun (Figure 5).

5. Cas d'application

L'étude de cas porte sur le système d'information d'une organisation chargée de gérer les dossiers de demandes de pension d'invalidité. Toute demande donne lieu à une étude par une commission chargée de décider, le cas échéant, du taux d'invalidité. Cette décision est alors transmise au centre payeur le plus proche de l'adresse du demandeur. Le traitement des demandes des pensions d'invalidité nécessite l'intervention de plusieurs acteurs, notamment du demandeur, du gestionnaire, de la commission d'attribution des taux et du centre payeur. Le nombre de bénéficiaires est estimé à 300.000 personnes par an. Le délai moyen d'examen d'un dossier et de l'attribution éventuelle d'une pension est d'un an. Le système d'information souffre aussi de graves lacunes relatives à la sécurité. Pour améliorer ce système, l'entreprise a déclenché un audit du système d'information ainsi que de la procédure d'attribution du taux d'invalidité. Cet audit donne lieu à des recommandations quant au fonctionnement du service et à des mesures de sécurité informatique.

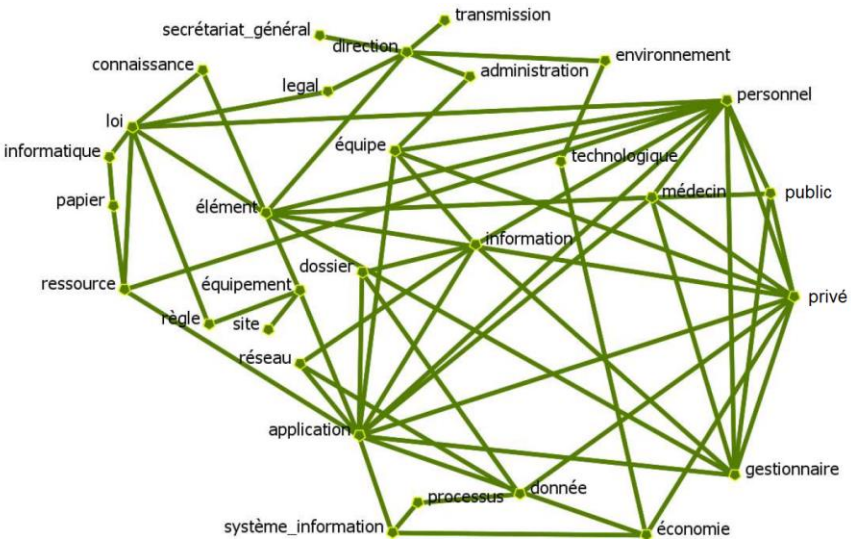

Figure 6. Réseau sémantique des concepts du contexte et des actifs.

Dans une première étape, nous procédons à l'extraction des concepts du contexte liés à l'organisme en utilisant le rapport d'audit. A cette fin, nous utilisons le logiciel Automap pour l'extraction et le logiciel ORA pour la visualisation du résultat. On obtient ainsi un réseau sémantique qui représente les relations existantes entre les concepts du contexte de l'organisation concernée (Figure 6). Dans cette figure, la fréquence des concepts ontologiques correspond à l'épaisseur du trait, ici peu visible.

Puis nous procédons à l'enrichissement du méta modèle de la sécurité avec les résultats obtenus lors de l'extraction précédente. Cet enrichissement est facilité par la mise en correspondance des éléments du contexte avec les concepts génériques de l'ontologie du contexte (Tableau 1).

Elément de contexte de l'organisation	**Concepts de l'ontologie du contexte**
Environnement, Technologique, Loi, Légal	Contexte externe
Direction, Secrétariat général, Règle, Administration, Informatique	Gouvernance
Donnée, Equipe, Dossier, Equipement, Information Réseau, Transmission, Application, Personnel Médecin, Gestionnaire, Public, Civil, Elément Papier, Connaissance, Processus, Ressource	Ressources
Système information	Système information
Site	Site
Donnée, Equipe, Dossier, Equipement, Information Réseau, Transmission, Application, Personnel Médecin, Gestionnaire, Public, Civil, Elément, Papier Connaissance, Processus, Ressource, Système information	Contexte interne

Site, Direction, Secrétariat général, Règle, Administration Informatique	

Tableau 1. Eléments de contexte de l'organisation et concepts de l'ontologie du contexte

Nous procédons de la même façon pour les actifs de l'organisation en les mettant en correspondance avec les concepts génériques de l'ontologie des actifs qui font partie de l'ontologie du contexte.

Actifs de l'organisation	**Concepts de l'ontologie des actifs**
Personnel, Public, Médecin, Gestionnaire, Elément Civil	Personnel
Application, Donnée, Information, Dossier Système information	Application
Equipe, Electronique	Matériel
Réseau	Réseau
Site	Site
Réseau, Application, Donnée, Information, Dossier Système information, Equipe, Electronique	Actif support (technique)

Tableau 2. Eléments des actifs de l'organisation et concepts de l'ontologie des actifs

La dernière phase consiste à déterminer les objectifs de sécurité. A cet effet, nous associons à chaque concept des actifs un ou plusieurs objectif(s) de sécurité en appliquant notre démarche de construction des scénarios des risques (Vasquez et al., 2012). Nous obtenons le tableau ci-dessous (Tableau 3).

Actif	**Contexte**	**Scénarios des risques**	**Objectifs de sécurité**
Hardware Software Site	Contexte externe	Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, par un phénomène naturel majeur.	Disponibilité Intégrité Confidentialité
Software	Contexte externe	Traitement illicite des données personnelles, utilisation des données personnelles à d'autres fins que celles autorisées par la législation ou un règlement.	Confidentialité
Hardware	Gouvernance	Destruction ou altération d'un équipement ou d'un support de stockage d'une plate-forme du système, due à un accident ou une négligence ou encore à un acte délibéré, par une personne ayant accès à cet élément.	Disponibilité Intégrité Confidentialité
Hardware	Ressources	Arrêt ou dysfonctionnement de la climatisation dans les locaux d'une plate-forme, de ceux de support de stockage, de documents ou de d'équipements, suite à une panne ou un acte volontaire.	Disponibilité
Réseaux	Ressources	Au niveau des réseaux ou des supports de communication utilisés, interception des échanges entre un utilisateur et le système, entre deux plates-formes du système, entre deux équipements d'une même plate-forme.	Disponibilité Intégrité Confidentialité
Software	Site	Vol de documents du système, vol ou substitution	Confidentialité

Hardware		d'un support de stockage d'informations dans un site du système, dans un site de stockage.	
Software	Ressources	Personne interne à l'organisme qui, par negligence, diffuse de l'information à d'autres personnes de l'organisme ne devant pas à en connaître, ou à l'extérieur. Personne diffusant consciemment de l'information à d'autres personnes de l'organisme ne devant pas en connaître,	Confidentialité

Tableau 3. Détermination des critères de sécurité (Extrait)

Le résultat obtenu permet d'instancier, et donc d'enrichir, le méta modèle de la sécurité. A noter que nous avons attribué le même poids pour chaque objectif de sécurité.

6. Conclusion et future recherche

Les principales contributions de cet article sont :

- la proposition d'un méta modèle de sécurité qui sert de base à une démarche de dérivation des exigences de sécurité à partir d'une analyse des risques,
- le développement d'une ontologie du contexte fondée sur la norme de sécurité ISO/CEI 27000 : 2018,
- Une démarche d'enrichissement du méta modèle de sécurité par l'ontologie du contexte. Cet enrichissement est réalisé en deux phases. La première est relative à l'identification et à l'extraction des éléments du contexte de l'entreprise et des actifs. La seconde concerne la détermination des objectifs de sécurité des actifs de l'organisation à protéger.
- L'application à un cas réel, et qui sert d'une première étape dans la validation de notre démarche.

Plusieurs axes de recherche future sont possibles. Citons notamment l'enrichissement de l'ontologie du contexte et des règles de correspondance associées, l'application de la démarche à plusieurs exemples, l'exploitation de l'aspect « contexte externe » ainsi que des scénarios de risques associés, ainsi qu'une validation plus large des concepts et des relations ontologiques.

Bibliographie

Abowd G.D., Dey A.K., Brown P.J., Davies N., Smith M., Steggles P. (1999) *Towards a Better Understanding of Context and Context-Awareness*. HUC 1999 (Handheld and Ubiquitous Computing). LNCS 1707. Springer, Berlin, Heidelberg.

Aguilar, J., Jerez, M., Rodriguez, T. (2017). CAMeOnto: Context awareness meta ontology modeling, Applied Computing and Informatics, 2017,ISSN 2210-8327,https://doi.org/10.1016/j.aci.2017.08.001.

Amutio, M., Candau, J. (2014). *Magerit V3 : Methodology for Information Systems Risk Analysis and Management, Book I - The Method*. Ministerio de Hacienda y Administraciones Públicas . http://administracionelectronica.gob.es/.

ANSSI. (2010). https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf.

Ardila, S.E.G. (2013). Learning Design Implementaion in Context-Aware and Adaptive Mobile learning, Thèse Université de Girona, Catalonia, Spain, 2013.

Bazire, M., Brézillon, P. (2005). Understanding Context before Using It. CONTEXT 2005: 29-40.

Brézillon, P., Abu-Hakima, S. (1995). *Using knowledge in its context*: *Report on the IJCAI-93 Workshop*. The AI Magazine, 16(1) pp. 87-91.

Bulcao Neto, R. F., Pimentel, M. G. C. (2005). *Toward a domain-independent semantic model for context-aware computing*. In Proceedings of the 3rd Latin American Web Congress (LA-WEB'05), pages 61–70, Buenos Aires, Argentina, 2005.

Cabrera, O. Franch, X., Marco, J. (2014). *A Context Ontology for Service Provisioning and Consumption*. IEEE RCIS 2014.

Carley, K. M., (2013a). Dave Columbus, D., Landwehr, P. (2013). *AutoMap User's Guide 2013*. Technical Report CMU-ISR-13-105. Institute for Software Research. Carnegie Mellon University. http://www.casos.cs.cmu.edu/projects/automap/CMU-ISR-13-105.pdf.

Carley, K.M., (2013b). *ORA: Quick Start Guide*. http://netanomics.com/wp-content/uploads/2017/03/ORA-QuickStart-Guide-2016.pdf

Chen, H., Finin, T., Joshi, A. (2003). *Using OWL in a Pervasive Computing Broker*. Workshop on Ontologies in Open Agent Systems (AAMAS 2003).

Christopoulou, E. (2008). Context as a necessity in mobile applications. In: Klinger, K. (Ed.), User Interface Design and Evaluation for Mobile Technology, pp. 187–204, 2008.

Dey, A.K. (2001). Understanding and Using Context, Personal Ubiquitous Comput., vol. 5, pp. 4-7, 2001.

Ejigu, D., Scuturici, M., Brunie, L. (2007). *An Ontology-Based Approach to Context Modeling and Reasoning in Pervasive Computing*. CoMoRea Workshop de PerCom'07, White Plains, NY, 2007, pp. 14-19.

Fernández-López, M. and Gómez-Pérez, A. and Juristo, N. (1997). *METHONTOLOGY: From Ontological Art Towards Ontological Engineering*. Actes de AAAI-97, 1997, Stanford University.

Gomez S., Zervas, P., Sampson, D.G., Fabregat, R. (2014). Context-aware adaptive and personalized mobile learning delivery supported by UoLmP, Journal of King Saud University - Computer and Information Sciences, Volume 26, Issue 1, Supplement, 2014, Pages 47-61, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2013.10.008.

Guermah, H., Fissaa, T., Hafiddi, H. Nassar, M., Kriouile,A. (2014). An ontology oriented architecture for context aware services adaptation, Int. J. Comput. Sci. 11 (2) (2014).

IFIP-IFAC Task Force. (2003). *Geram: Generalized Enterprise Reference Architecture and Methodology*. Version 1.6.3, Handbook on Enterprise Architecture. Editeurs : Bernus, Peterand Nemes, Laszloand Schmidt. ISBN=978-3-540-24744-9

Kactus. (1996). *The KACTUS Booklet version 1.0*. Esprit Project 8145 KACTUS.

Lammari, N., Bucumi, J. S., Akoka, J., Comyn Wattiau, I. (2011). *A conceptual Meta, Model for Secured Information Systems*.ICSE´11. 2011. DOI: 10.1145/1988630.1988635.

Laoufi, N. (2017). Processus de dérivation des exigences de sécurité à partir de l'analyse des risques, Thèse de doctorat, Conservatoire National des Arts et Métiers, Mars 2017.

Leech, G. (1981). Semantics: The Study of Meaning. Harmondsworth, UK: Penguin, 1981.

Maedche, A., Staab, S. (2001). Ontology Learning for the Semantic Web. IEEE Intelligent Systems, Special Issue on the Semantic Web, 16(2), 2001.

Nadoveza, D., Kiritsis, D. (2014). Ontology-based approach for context modeling in enterprise applications. Computers in Industry 65(9): 1218-1231.

Naudet, Y., Mayer, N., Feltus, C. (2016). *Towards a Systemic Approach for Information Security Risk Management*. ARES 2016: 177-186

Staab, S., Schurr, H., Studer, P., Sure, Y. (2001). Knowledge processes and ontologies. IEEE Intelligent Systems 16(1):26-34.

Stumme, G., Hotho, A., Berendt, B. (2006). *Semantic web mining: State of the art and future directions*. Web Semantics: Science, Services and Agents on the World Wide Web, 4(2), pp.124–143.

Suárez-Figueroa, M.C., Gómez-Pérez, A., Fernández-López, M. (2012). *The NeOn Methodology for Ontology Engineering*, Book Chapter in Ontology Engineering in a Networked World, 2012, Publisher: Springer Berlin Heidelberg, pp. 9-34.

Turenne, N., (2010). *Apprentissage statique pour l'extraction de concepts à partir de textes*, Doctoral Thesis in Computer sciences.

Vasquez, M., Lammari, N., Comyn-Wattiau, I., Akoka, J. (2012). *De l´analyse des risques à l´expression des exigences de sécurité des systèmes d'information*, INFORSID 2012.

Zhong-Jun, L., Guan-Yu, P., Ying, A (2016*). Method of meta-context ontology modeling and uncertainty reasoning in SWoT*, Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (2016) 128–135.