ANR programme ARPEGE 2008

Systèmes Embarqués et Grandes Infrastructures

Projet SELKIS : Une méthode de développement de systèmes d'information médicaux sécurisés : de l'analyse des besoins à l'implémentation.

ANR-08-SEGI-018

Décembre 2008 – Août 2012

UPDATE OF L2.2: A UML PROFILE FOR SECURITY CONCEPTS

Livrable n° 2.3 bis

Jacky Akoka (ISID CEDRIC CNAM Paris)
Isabelle Comyn-Wattiau (ISID CEDRIC CNAM Paris)
Akram Idani (VASCO LiG Grenoble)
Mohamed Amine Labiadh (VASCO LiG Grenoble)
Nadira Lammari (ISID CEDRIC CNAM Paris)
Yves Ledru (VASCO LiG Grenoble)
Jean-Luc Richier (VASCO LiG Grenoble)

Février 2012

SOMMAIRE

1. Introduction

Le projet SELKIS a pour objectif de développer une méthode, fondée sur MDA (Model Driven Architecture), d'analyse et de conception de systèmes d'information (SI) sécurisés intégrant les propriétés de sécurité de base, à savoir la Disponibilité, l'Intégrité, la Confidentialité et la Traçabilité (DICT), dans les différentes phases du cycle de développement d'une application depuis la spécification des besoins jusqu'à l'implémentation.

Dans nos précédents livrable 2.1 et 2.2, nous avions présenté :

- notre approche, nommée MoSIS (Modélisation des Systèmes d'Information Sécurisés) pour la prise en compte des propriétés DICT depuis l'étape de spécification des besoins jusqu'à l'implémentation. C'est une approche dirigée par les modèles fondée sur MDA,
- le méta-modèle CIM utilisé par MOSIS pour la description d'un système d'information sécurisé qui englobe la vision métier et qui représente, à un grain très fin, les liens entre les exigences fonctionnelles et non fonctionnelles (notamment la sécurité). Ce modèle prend en compte les dimensions les dimensions organisationnelle, comportementale, informationnelle et structurelle des processus métiers,
- un profil UML de niveau PIM (méta-modèle des cas d'utilisation) pour la description des fonctionnalités d'un système sécurisé construit à partir de stréréotypes proposés pour la description de concepts liés à la sécurité des SI.
- un profil UML de niveau PIM (méta-modèle des classes) pour la description de la structure statique d'un SI sécurisé construit à partir de stréréotypes proposés pour la description de concepts liés à la sécurité des SI.
- le processus de MoSIS pour la transformation d'une instance du méta-modèle CIM en une instance du méta-modèle des cas d'utilisation; ces derniers servant à la description des fonctionnalités d'un système d'information sécurisé. Il est de niveau PIM

Les deux résultats de recherche que nous présentons dans ce livrable vont dans la continuité de ceux obtenus dans les précédents livrables. Le premier concerne la transformation d'une instance du méta-modèle CIM en une instance du méta-modèle des classes. Ce dernier constitue une composante de niveau PIM et contribue à la description de la structure statique d'un SI sécurisé. Le second résultat de recherche a trait à l'instanciation semi-automatique d'une partie du méta-modèle CIM. Cette instanciation concerne les besoins de sécurité. Nous proposons de les dériver à partir d'une analyse des risques de sécurité.

Le reste de ce livrable est organisé de la façon suivante. La section 2 rappelle le méta-modèle CIM et le profil UML de niveau PIM décrivant la structure statique du SI sécurisé (diagramme des classes) et présente quelques règles de transformation d'une instance du CIM en une instance du diagramme des classes. La section 3 est dédiée à l'approche de dérivation de besoins de sécurité à partir d'une analyse des risques. La section 4 conclut ce livrable.

2. D'un modèle de niveau CIM vers un diagramme des classes

A l'aide de MoSIS, notre approche de développement de SI, nous construisons un système d'information sécurisé selon trois étapes (livrable 2.1). Chacune d'elles correspond à un niveau d'abstraction MDA. La première étape a pour but la description du système d'information et de son environnement. C'est dans cette étape que s'effectue l'analyse de l'environnement organisationnel dans lequel le futur système va opérer. Cette analyse contient, d'une certaine manière, la justification («pourquoi») du choix des mécanismes de sécurité préconisés et fournit la réponse au «comment» et «quand» les utiliser. Le résultat de cette étape est une instance du méta-modèle CIM. La seconde étape correspond à l'analyse et la conception abstraite du système d'information. De cette analyse découlent les modèles UML d'analyse. Parmi ces modèles, on peut citer le diagramme des cas d'utilisation pour la description des fonctionnalités du système et le diagramme des classes pour la description de la structure statique du système. Ces modèles constituent le niveau PIM du système d'information sécurisé. Ils doivent prendre en compte aussi bien les concepts fonctionnels intrinsèques à l'application que les politiques de sécurité entreprises pour la sécuriser. Ces modèles sont des instanciations de méta-modèles de niveau PIM qui, eux, sont des extensions des méta-modèles d'UML. Ces extensions sont fondées sur des profils.La troisième étape est dédiée à la conception détaillée dans laquelle la plateforme technologique, qui accueillera le système d'information, a été prise en compte.

Nous avions proposé dans le livrable 2.1 et revu dans le livrable 2.1 : 1) le méta-modèle CIM de MoSIS, 2) le profil UML des cas d'utilisation pour la description des fonctionnalités d'un SI ainsi que 2) celui des classes pour la description de la structure statique du SI. Afin de faciliter la compréhension des règles de transformation d'une instance du méta-modèle CIM en une instance du diagramme des classes, les paragraphes qui suivent rappellent ces deux méta-modèles.

2.1 Le méta-modèle CIM de MoSIS

La représentation des propriétés de sécurité, à différents niveaux d'abstraction, nécessite avant tout la description du SI au niveau métier. Cette description doit intégrer :1) les processus de gestion pour lesquels les SI servent de support, 2) les besoins fonctionnels et non fonctionnels que les SI vont prendre en charge et enfin 3) la structure de l'organisation dans laquelle le SI est exploité. Ces trois aspects ont été décrits, dans la version 1.0 du méta-modèle CIM de MoSIS (livrable 2.1) et revus dans la version 1.1 de ce même méta-modèle (livrable 2.2) suite à son instanciation à deux cas. Le premier cas nommé «Bibliothèque» et décrit en annexe 4 du livrable 2.1 est relatif à la gestion d'une bibliothèque. La seconde instanciation a concerné le système d'information pré-hospitalier d'IFREMMONT, un de nos partenaires dans le projet.

Pour des raisons de lisibilité, nous avions représenté notre méta-modèle CIM en trois méta-modèles : un méta-modèle des processus, un méta-modèle des besoins et un méta-modèle organisationnel. La fusion de ces trois méta-modèles constitue le méta-modèle CIM associé à un SI. Les figures 1, 2 et 3 décrivent respectivement chacun des méta-modèles constituant le méta-modèle CIM de MoSIS. A noter que dans ces derniers, figurent les concepts d'ancrage avec les autres méta-modèles (en gris clair les concepts d'ancrage du méta-modèle des processus avec celui des besoins et en gris foncé ceux liant le méta-modèle

des processus au méta-modèle organisationnel). Une description détaillée de ces méta-modèles est fournie dans les livrable 2.1 et 2.2.

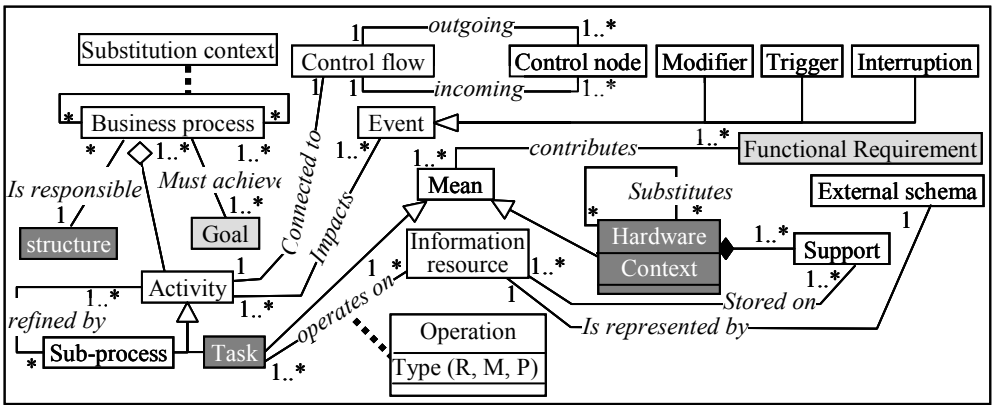

Fig. 1 : Méta-modèle des processus - version 1.0 du méta-modèle CIM de MoSIS

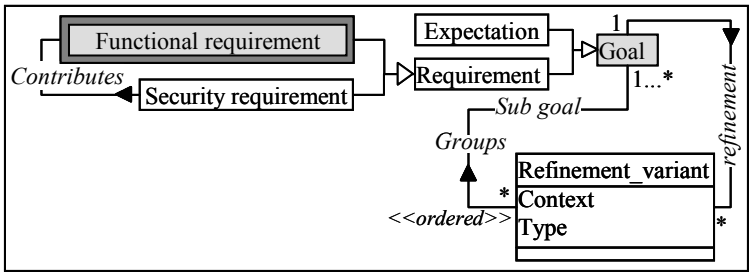

Fig. 2 : Méta-modèle des besoins - version 1.0 du méta-modèle CIM de MoSIS

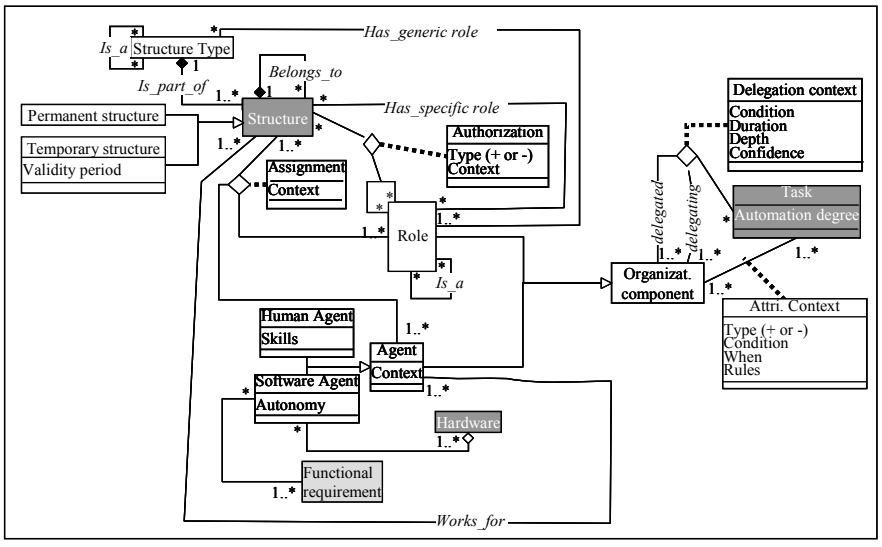

Fig. 3 : Méta-modèle organisationnel - version 1.0 du méta-modèle CIM de MoSIS

2.2 Profil UML pour la description de la structure statique

La description de la structure statique du SI au niveau PIM a été faite à l'aide d'un diagramme des classes. Ce dernier est présenté dans la figure 4. Il intègre les concepts de sécurité couverts à un niveau conceptuel indépendant des plates-formes (PIM). Outre les concepts de base de Role Based Access Control (RBAC), pris en compte par l'approche SecureUML, nous avions intégré les notions d'organisation, d'affectation et de délégation évoquées lors de la modélisation des exigences de sécurité au moyen des modèles CIM.

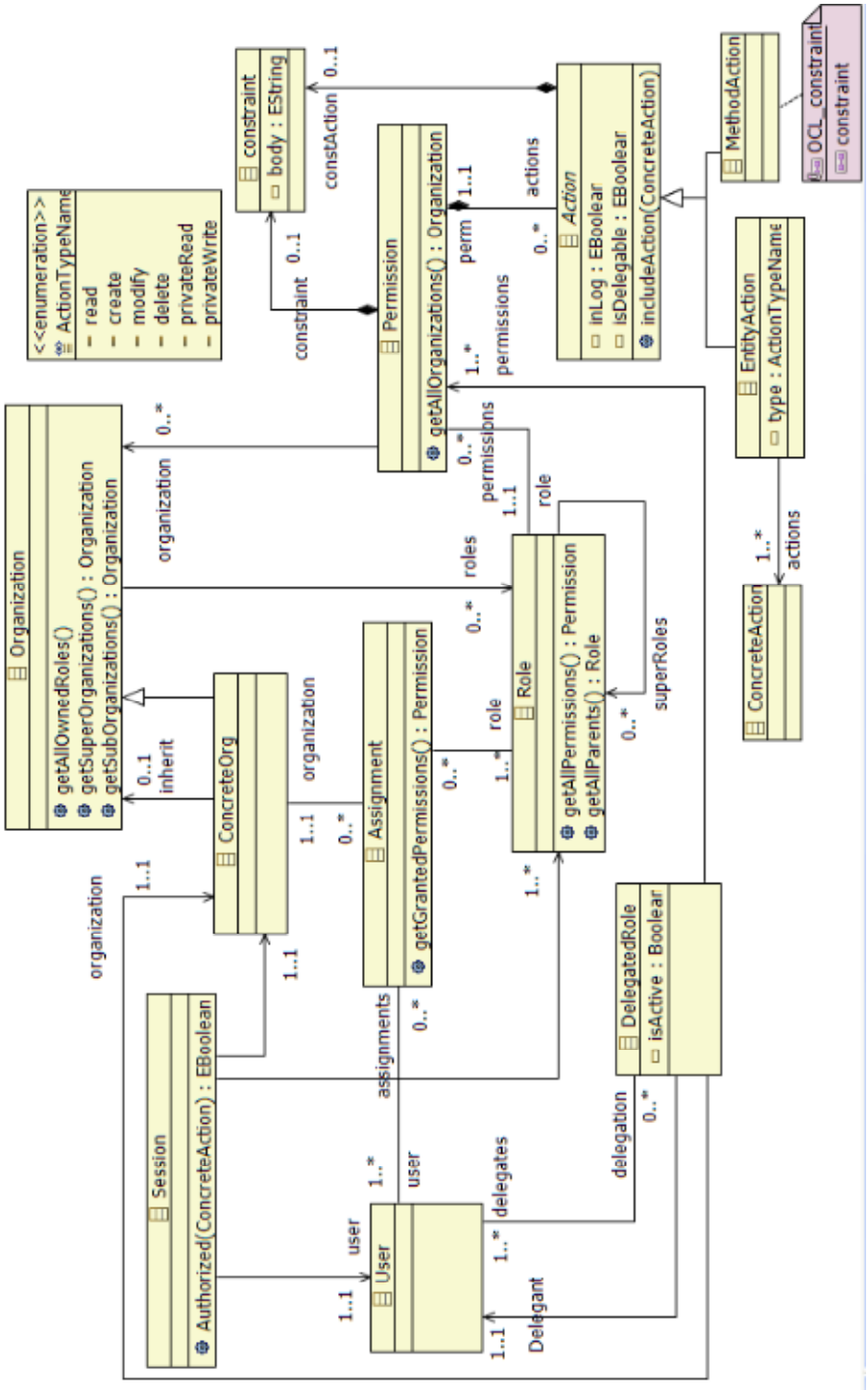

Fig. 4 : Profil UML pour la description statique d'un système d'information sécurisé

4. Règle de transformation d'un modèle de niveau CIM vers un diagramme des cas

Il existe plusieurs chemins de passage du niveau CIM vers le niveau PIM. Nous nous intéressons dans ce livrable à la transition consistant à utiliser le diagramme des classes.

La génération d'un diagramme des classes (de niveau analyse) d'une application sécurisée à partir de sa description au niveau CIM s'effectue moyennant des règles de transformation.

Ces règles de transformation peuvent être catégorisées selon les concepts qu'elles permettent de générer. Parmi ces règles, certaines permettent de déduire les classes d'analyse décrivant les organisations, les rôles (acteurs UML) et les utilisateurs du SI sécurisé (qui peuvent correspondre à des agents humain ou software), d'autres de procéder à l'affectation des rôles aux utilisateurs. D'autres règles encore vont permettre déduire les attributions de tâche de lecture, écriture et modification sur les objets du SI sécurisé. Enfin, d'autres règles concernent la définition des règles d'autorisations/interdiction et délégations. A titre d'exemple, nous pouvons citer les règles de déduction des organisations.

R1: Toute instance TS de «Structure Type» TS donne naissance à une instance O de «Organization»

R2 : Toute instance S de «Temporary Structure» donne naissance à une instance CO de «Concrete Organization»

R3 : Toute instance S de «Permanent Structure» donne naissance à une instance CO de «Concrete Organization» ayant pour «validity period» la valeur nulle.

R4 : SI deux instances TS1 et TS2 de «Structure Type» sont liées par le lien «Is_A»
Et SI TS1 est la «sous» structure type de TS2
Alors créer le lien « Is_A » entre l'instance O1 de «organisation» correspondante à TS1 et l'instance O2 de «organization » correspondante à TS2 tel que O1 soit «sous» organisation de O2.

R5 : SI une instance TS de «Structure Type» est liée par le lien «Is_part_of» à une instance S de «Permanent Structure»
Et SI S compose TS
Alors créer un lien «Is_part_of» entre l'instance O de «Organisation» correspondante à TS et l'instance CO correspondante à S tel que CO compose O.

R6 : SI une instance TS de «Structure Type» est liée par le lien «Is_part_of» à une instance S de «Temporary Structure»
Et SI S compose TS
Alors créer un lien «Is_part_of» entre l'instance O de «Organisation» correspondante à TS et l'instance CO correspondante à S tel que CO compose O.

R7 : SI deux instances S1 et S2 de «Permanent Structure» / «Temporary Structure» sont liées par le lien «Belongs_to»
ET SI S1 compose S2
Alors créer le lien «Belongs_to» entre l'instance «Concrete Organization» O1 correspondante à S1 et l'instance «Concrete Organization» O2 correspondante à S2 tel que O1 compose O2.

Ces règles concernent les portions de méta-modèle CIM et PIM représentées par la figure 5.

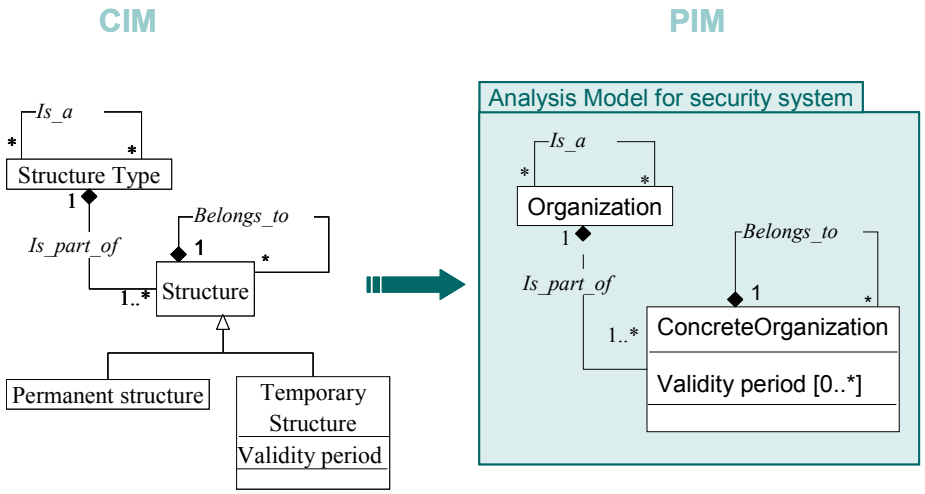

Fig. 5 : Portion de passage du CIM au PIM

3. Instanciation d'une partie du méta-modèle CIM à partir de l'analyse des risques

La dérivation d'une instance d'un des méta-modèles PIM de MoSIS est effectuée en appliquant des règles de transformation sur une instance du méta-modèle CIM. Cette dernière décrit les processus métiers du SI, la structure de l'organisation où il est exploité ainsi que les besoins fonctionnels et non fonctionnels qu'il prend en charge. Parmi les besoins non fonctionnels, nous nous intéressons, dans le cadre du projet SELKIS, aux besoins de sécurité. Ces derniers sont généralement déduits suite à une analyse des risques.

Nous proposons dans le cadre du projet SELKIS de procéder à une instanciation semi-automatique de la partie du CIM relative aux besoins de sécurité à l'aide d'un processus guidé de dérivation des besoins de sécurité à partir de l'analyse des risques que nous intégrons dans MoSIS. Notre processus repose sur l'utilisation de deux ontologies que nous avons élaborées dans le cadre du projet SELKIS: 1) une ontologie des risques fondée sur les concepts inhérents aux différentes méthodes d'identification et d'analyse des risques faisant référence et 2) une ontologie des exigences de sécurité obtenue en capitalisant sur les concepts constitutifs des méthodes de l'ingénierie des exigences analysées.

Après une présentation synthétique de notre état de l'art sur l'analyse des risques et les besoins de sécurité, nous décrivant dans la section 3.2 notre approche de guidage.

3.1 Risques et exigences de sécurité : état de l'art

Plusieurs normes internationales concernant la gestion de la sécurité de l'information ont été élaborées par l'Organisation Internationale de Normalisation (ISO). Certaines d'entre elles concernent la gestion des risques. Il s'agit des normes ISO/CEI 2700x. Notons aussi qu'il existe une multitude de méthodologies relatives à la gestion des risques : MEHARI (Clusif, 2010), EBIOS (ANSSI, 2010), ISRAM (Karabacak et al., 2005), COBIT (ISACA, 2012), ITIL (Hochstein et al. 2005), RMF (Alberts et al., 2010), FTA (Ericson, 2000), FMECA (Borgovini et al., 1993), HAZOP (Aagedal et al., 2002) (Winther et al., 2001), CRAMM (SS-UK, 2005), OCTAVE (Alberts, 2002). Faute d'espace, nous ne pouvons décrire les spécificités de toutes ces méthodes. Des comparaisons détaillées de la plupart d'entre elles sont fournies dans (Behnia1et al., 2012), (Lambert, 2011) et (Vorster, 2005). Cependant, nous retenons le fait que ces méthodes visent le respect des critères de sécurité DICT garantissant

un niveau de protection acceptable des actifs de l'organisation. Certaines de ces méthodes, telles que ISRAM, se focalisent sur la proposition de mesures de sécurité et sont, de ce fait, qualifiées de quantitatives. D'autres sont plutôt qualifiées de qualitatives dans la mesure où elles contribuent à l'identification des risques. Elles fournissent des recommandations générales concernant les mesures de sécurité à mettre en place. Parmi ces méthodes, nous pouvons citer EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) et MEHARI (Méthode Harmonisée d'Analyse de Risques). EBIOS est une approche orientée processus. Son principe général est d'identifier l'actif, d'évaluer l'impact d'un événement de sécurité sur l'actif, de rechercher les menaces et les vulnérabilités et finalement, à partir de cette information, d'en déduire les besoins de sécurité les plus appropriés relativement au contexte de l'entreprise. Une des caractéristiques d'EBIOS est l'utilisation d'une base de connaissances à laquelle se connecte le logiciel, lui donnant accès à la liste des vulnérabilités (techniques) connues, des contraintes de sécurité et des méthodes d'attaques (menaces). MEHARI, contrairement à EBIOS, est une approche orientée scénarios. Elle consiste en l'analyse des scénarios qui peuvent affecter la sécurité de l'information, par rapport aux critères DICT. Ces scénarios expriment les dysfonctionnements potentiels de l'entreprise.

En résumé, nous constatons que la plupart des méthodes de gestion des risques ainsi que quelque unes des normes ISO/CEI 2700x sont utiles pour développer notre ontologie des risques. Toutefois, elles sont insuffisantes pour l'identification des exigences de sécurité. Parallèlement, la recherche en ingénierie des exigences a fourni un large éventail d'approches contribuant à l'identification des exigences de sécurité. Une étude comparative de ces approches peut être trouvée dans (Salini et al., 2011) et (Fabian et al., 2010). Toutefois, notons que, parmi les travaux les plus récents, certains proposent une intégration de l'analyse des risques avec celle des besoins de sécurité. A titre d'exemple, nous pouvons citer les travaux (Asnar et al., 2011) et (Matulevicius et al., 2008). Asnar et al., 2011 proposent une extension de la modélisation des buts de TROPOS en introduisant des concepts associés à l'analyse des risques et cela à des fins d'analyse, d'évaluation et de sélection de risques pouvant être encourus pour satisfaire les buts fixés. Matulevicius et al. ont proposé une adaptation du processus de Secure Tropos et son modèle pour la gestion des risques. Bien qu'intéressantes, ces approches nécessitent la plupart du temps une maîtrise du langage qui leur est associé. Elles n'offrent pas de guidage dans la dérivation des besoins de sécurité à partir de l'analyse des risques.

Enfin, notre étude de l'état de l'art nous a permis de constater l'émergence d'approches d'identification des exigences de sécurité fondées sur l'analyse des risques. Cependant, malgré les tentatives d'intégration de l'analyse des risques dans l'identification des exigences de sécurité, ces deux processus demeurent indépendants. A notre connaissance, aucune démarche formelle permettant d'établir des liens entre ces deux processus n'est proposée dans la littérature. L'objet de notre recherche a été de proposer une liaison entre ces deux processus afin d'offrir un guide pour la dérivation des exigences de sécurité à partir d'une analyse des risques.

3.2 Notre approche de guidage

Comme énoncé précédemment, notre démarche repose sur l'utilisation de deux ontologies que nous avons élaborées : 1) une ontologie des risques et 2) une ontologie des exigences de sécurité. Pour servir le guidage, nous avons procédé à l'alignement de ces deux ontologies. Cet alignement est fondé sur les relations sémantiques existant entre les deux ontologies. Il est facilité par le recours à des bases de connaissances issues des méthodologies et des normes décrites précédemment.

La figure 6 décrit notre démarche.

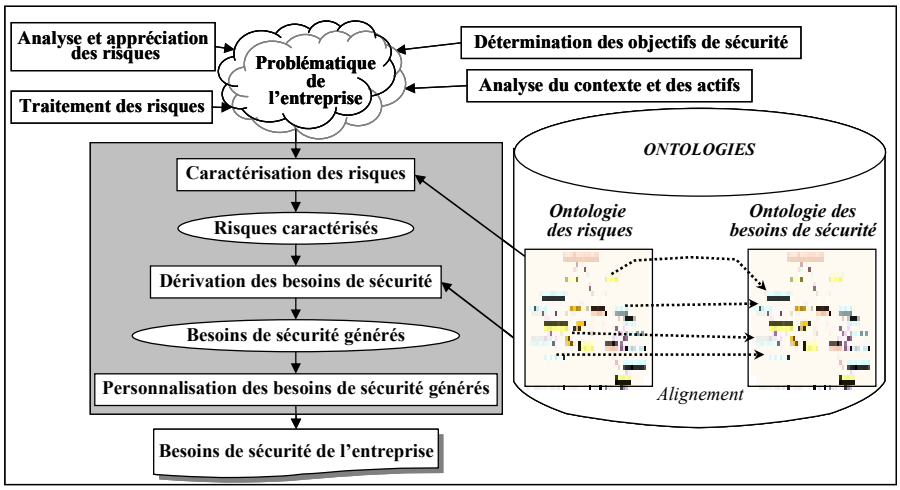

Fig. 6 : Architecture du schéma de dérivation des besoins de sécurité

Notre démarche nécessite, au préalable, une caractérisation de la problématique de l'entreprise. Cette caractérisation consiste à appliquer les quatre premières étapes du processus de Gestion des Risques de Sécurité des Systèmes d'Information (GRSSI) décrit dans (Mayer et al., 2008) et qui sont l'identification du contexte et des actifs, la détermination des objectifs de sécurité, l'analyse et l'appréciation du risque et enfin le traitement du risque.

Notre démarche de guidage se déroule en trois temps. Dans un premier temps, les risques potentiels, recensés suite à la définition de la problématique de l'entreprise, sont caractérisés sur la base de l'ontologie des risques. Dans un second temps, les exigences de sécurité, associées aux risques recensés et caractérisés, sont dérivées. Enfin, la liste des exigences obtenue par dérivation est personnalisée compte tenu du contexte de l'entreprise. La caractérisation des risques recensés est effectuée par leur mise en correspondance avec ceux de l'ontologie. Cette mise en correspondance est pour l'instant manuelle. Des techniques de traitement du langage naturel pourraient contribuer à son automatisation. Les exigences de sécurité, quant à elles sont dérivées de façon automatique moyennant les liens d'alignement établis entre les deux ontologies des risques et des besoins. Pour l'instant, la personnalisation des besoins générés est manuelle.

Le prototype associé à notre approche a été développé à l'aide du « pattern » Google, auquel nous avons ajouté la possibilité de recherche sélective via la plateforme SESAME. Cette dernière nous a permis de stocker en OWL et d'interroger en SeRQL via l'interface web native openRDFWorkbench l'ontologie englobant celle des risques et celle des exigences de sécurité.

3.3 Construction des ontologies des risques et exigences de sécurité

L'analyse des différentes normes, méthodes d'analyse des risques et d'identification des exigences de sécurité, nous a permis de regrouper, sélectionner, uniformiser et intégrer les concepts les plus utilisés. Ces derniers ont été par la suite utilisés pour la construction de nos deux ontologies. Dans notre démarche de construction des ontologies, nous avons commencé par l´étude des ontologies existantes (Lambert, 2011). Ensuite, nous avons complété la

structure conceptuelle avec les termes utilisés dans les méthodologies citées dans l'état de l'art. Cette démarche a permis d'enrichir les ontologies avec des concepts structurels organisés en hiérarchies. Les ontologies ainsi créées ont été, par la suite, liées en fonction de critères sémantiques pour représenter un type d´interaction entre les risques et les besoins de sécurité. L´alignement a été réalisé par l´établissement de correspondances pertinentes entre les concepts des deux ontologies.

La méthodologie mise en œuvre a permis de décrire les concepts communément utilisés dans le domaine de l´analyse de risque et des besoins de sécurité. Les étapes successives de la démarche ont été : 1) l´étude des méthodes, l'extraction et l'analyse des connaissances menant au choix de concepts, 2) la classification et la hiérarchisation des concepts, 3) l´interprétation des relations entre les concepts des ontologies pour la réalisation du processus d´alignement, 5) la mise en œuvre du schéma d'alignement.

Un extrait de l'ontologie des risques (respectivement celle des besoins de sécurité) est représenté à la figure 7 (respectivement 8).

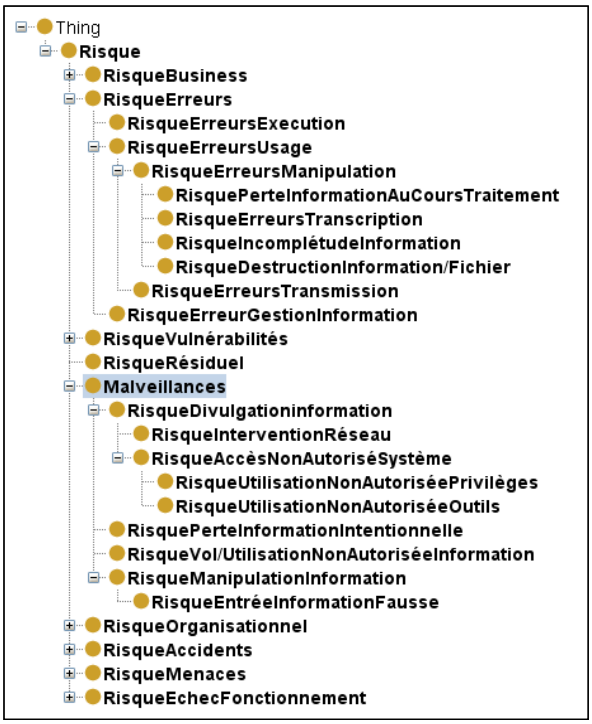

Fig. 7 : Un extrait de l'ontologie des risques

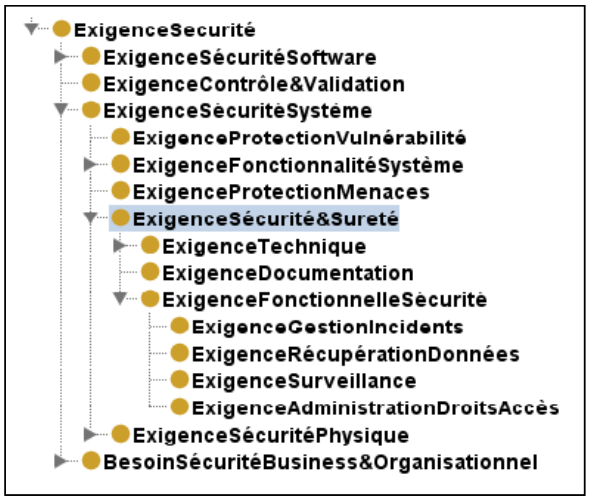

Fig. 8 : Un extrait de l'ontologie des besoins de sécurité

La mise en correspondance des concepts des deux ontologies permet de réduire l´implication directe des utilisateurs dans le processus de rapprochement des risques et des exigences de sécurité. Pour ce faire, nous avons adopté une démarche en cinq étapes (voir Figure 9). Dans un premier temps, nous avons récupéré toutes les bases de connaissances fournies par les méthodologies étudiées afin de les exploiter pour l'identification des scénarios potentiels. Pour tout scénario identifié on a aussi récupéré sa description détaillée ainsi que la liste des actions associées. Nous avons ensuite analysé chaque scénario recensé et l'avons mis en correspondance avec l'ontologie des risques afin de lui assigner les risques associés. Cette association peut être explicite (comme par exemple dans MEHARI) ou doit être déduite (comme par exemple dans CRAMM). Parallèlement à cela, nous avons mis en correspondance la liste des actions associées aux scénarios avec les concepts de l'ontologie des risques (Phase 4). Cette mise en correspondance nous a permis d'associer à chaque scénario une liste d'exigences de sécurité. Enfin, en exploitant les associations risques/scénarios obtenues de la phase 3 et les associations scénarios/exigences obtenues de la phase 4, nous avons déduit par transitivité les liens d'alignement entre les concepts des deux ontologies.

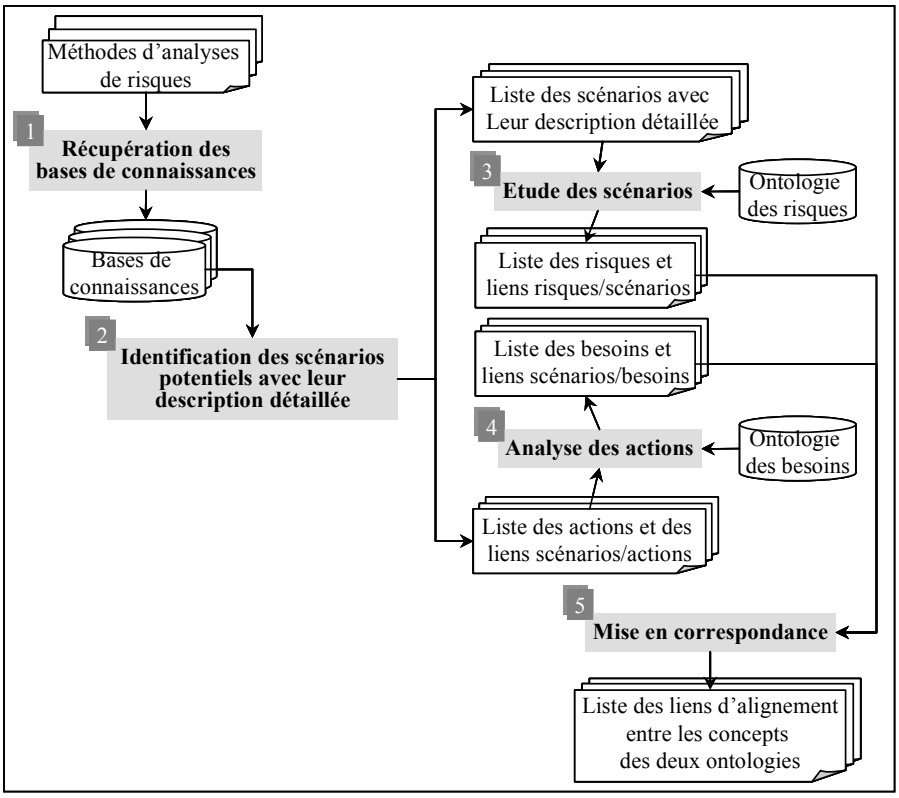

Fig. 9. Processus d´identification des liens d'alignement

Plus d'une dizaine de scénarios ont été testés avec des résultats satisfaisants. La table 1 présente quelques exemples de mise en correspondance entre les risques et les exigences de sécurité obtenus par application de notre démarche d'alignement à partir des bases de connaissances des méthodologies étudiées.

Type de Risque	Exigence associé	Source
RisqueVol/UtilisationNonAutoriséeInformation	BesoinConfidentialité	Mehari/Ebios/CRAMM
RisquePerteIntentionnelleInformation	BesoinAdministrationDroitsAccès	Mehari/Ebios/CRAMM
RisqueUtilisationNonAutoriséeOutils	BesoinSurveillance	Mehari/Ebios/CRAMM
RisqueUtilisationNonAutoriséePrivilèges	BesoinAdministrationDroitsAccès	Mehari/Ebios/CRAMM
RisqueInterventionRéseaux	BesoinSurveillance	Mehari/Ebios/CRAMM
RisqueManipulationDonnées	BesoinConfidentialité	Mehari/CRAMM/MARION
RisqueDivulgationDonnées	BesoinsConfidentialité&Integrité	Mehari/Ebios/CRAMM

Table 1. Exemples d'alignement de concepts

La validation de notre approche et des ontologies associées est essentielle. En ce qui concerne les deux ontologies, nous avons procédé à une vérification qui a consisté à mesurer la pertinence des relations taxonomiques définies. Pour l'approche de guidage, nous avons effectué une validation via trois études de cas.

4. Conclusion

Nous avons présenté, dans ce livrable, les évolutions apportées à notre démarche MoSIS de **Mo**délisation des **S**ystèmes d'**I**nformation **S**écurisés. Ces évolutions concernent, d'une part, la déduction de la description statique d'un système d'information sécurisé par transformation d'une instance du méta-modèle CIM en une instance du méta-modèle des classes de niveau analyse (PIM) et d'autre part l'instanciation des besoins de sécurité représentés dans le méta-modèle CIM à partir d'une analyse des risques.

Il est prévu de procéder à la formalisation des règles de transformations permettant de déduire, à partir d'un modèle de niveau CIM, le diagramme des classes. Il est aussi prévu d'enrichir les deux ontologies produites en introduisant des liens d'association entre concepts qui nous permettront, par exemple, de détecter des conflits potentiels entre risques et/ou exigences de sécurité. Cette détection de conflits offrirait un meilleur guidage dans la spécification des risques et permettrait de proposer plusieurs scénarios d'exigences à satisfaire.

5. Bibliographie

Aagedal O. J., den Braber F., Dimitrakos T., Axel Gran B., Raptis D. Stolen K. «Model-based Risk Assessment to improve Entreprise Security». *6th IEEE International Entreprise Distributed Object Computing*, Lausanne, Switzerland, 2002.

Alberts C., Dorofee A., *Managing Information Security Risks: The OCTAVE (SM) Approach*, Addison-Wesley Professional, Software Engineering series, 2002

Alberts C., Dorofee A., Risk Management Framework, Rapport technique CMU/SEI-2010-TR-017, Software Engineering Institute, http://repository.cmu.edu/sei/5/, 2010

ANSSI, EBIOS : Méthode de gestion des risques, Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information, https://adullact.net/projects/ebios2010, Janvier 2010.

Asnar Y., Giorgini P., Mylopoulos J., «Goal-driven risk assessment in requirements engineering». *Requirements Engineering*, 16(2), pp. 101-116, 2011.

Behnia1 A., Abd Rashid R., Chaudhry J. A., «A Survey of Information Security Risk Analysis Methods», *Smart Computing Review*, 2(1), February 2012

Borgovini R., Pemberton S. et Rossi M., Failure Mode, Effects and Criticality Analysis (FMECA), Rapport technique, Reliability Analysis Center, 1993

Clusif, MEHARI 2010 : Manuel de référence des services de Sécurité, http://www.clusif.asso.fr/fr/production/mehari/, Mai 2010

Di Jorio L. Mise à Jour automatique basée sur les motifs fréquents. Mémoire de Stage de Master. Université de Montpellier II, 2007.

Ericson C.A.. «Fault Tree Analysis – A History», *17th International System Safety Conference*, 1999.

Fabian B., Gürses S., Heisel M., Santen T., Schmidt H., «A comparison of security requirements engineering methods». *Requirements Engineering Journal, 15*(1), pp. 7-40, 2010.

Gerber M., von Solms R. «From Risk Analysis to Security Requirements». *Computers & Security*, 20 (1), pp. 577-584, Octobre 2001.

Hochstein A., Zarnekow R., Brenner W. «ITIL as Common Practice Reference Model for IT Service Management: Formal Assessment and Implications for Practice». *IEEE International Conference on e-Technology, e-Commerce and e-Service* (EEE'05), 2005

ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, http://www.isaca.org/cobit/pages/default.aspx, 2012

ISO, PN ISO/IEC 17799:2003, 2003.

Karabacak B., Sogukpinar I., «ISRAM: information security risk analysis method», *Computers & Security*, 24(2), pp. 147-159, Mars 2005

Keeney, M. J. D et al., Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors in May 2005. Rapport cas d'étude. Université Carnegie Mellon Un, http://www.cert.org/insider_threat/insidercross.html, 2005

Lambert S. M., *Tableaux de bord Dynamiques : Une approche à base d'ontologies*. Éditions Universitaires Européennes, Décembre 2011.

Matulevicius R., Mayer N., Mouratidis H., Dubois E., Heymans P., Genon N., «Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development», *20th International Conference on Advanced Information Systems Engineering*, pp. 541-555, Montpellier, France, Juin 2008.

Mayer N., Dubois E., Heymans P., Matulevicius R., « Défis de la sécurité de l'information. Support à la gestion des risques de sécurité par les modèles » . *Ingénierie des Systèmes d'Information*, 13(1), pp. 37-74, 2008.

Salini P., Kanmani S., «A Survey on Security Requirements Engineering», *International Journal of Reviews in Computing*, 8(1), pp. 1-10, décembre 2011.

Stumme G., Hotho A., Berendt B. «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, Juin 2006.

SS-UK, CRAMM User Guide, Security Service of UK Government, Juillet 2005