Vers l'utilisation des ontologies pour la formalisation des exigences de sécurité fondées sur la notion de situation de travail.

Yasmine SAADI[1], *Alain ETIENNE*[1], *Ali SIADAT*[1,] *Bruno DAILLE-LEFEVRE*[2]
1: LCFC. École Nationale Supérieure d'Arts & Métiers, 4 rue Augustin Fresnel, 57000 Metz, France
2: INRS. Institut National de Recherche et de Sécurité, Rue du Morvan, 54500 Vandoeuvre les Nancy
saadi_yasmine@hotmail.com, {alain.etienne, ali.siadat}@ensam.eu, bruno.daille-lefevre@inrs.fr

Résumé— *Les concepteurs peinent à formaliser le passage des besoins en sécurité aux exigences de sécurité lors de la conception d'un système de production. On y présente à travers cet article une approche méthodologique qui, à partir d'une situation de travail sur le système de production, les concepteurs font ressortir les critères d'usage qui ont une influence sur la santé et la sécurité des utilisateurs sous forme d'exigences de sécurité. La méthodologie s'appuie principalement sur l'emploi des ontologies connus pour être des sources riches en connaissances. Le but étant de mettre à la disposition des concepteurs un outil méthodologique d'aide à l'élicitation et la formalisation des exigences de sécurité.*

Mots clés— Conception sûre, ingénierie des exigences, situation de travail, formalisation, ontologie.

INTRODUCTION

Le constat habituellement fait en examinant les documents de spécification des exigences est que les exigences de sécurité, quand elles figurent, sont dans une section à part et recopiées à partir d'une liste générique de fonctions de sécurité, ce qui rend les mesures de sécurité prises par les concepteurs principalement correctives, pénalisant ainsi les coûts et les délais pour toute modification à posteriori [1].

Elles deviennent ainsi une obligation importante à inclure dès les premières étapes d'analyse des besoins en s'appuyant sur l'usage futur de l'équipement afin d'assurer la prise en compte des aspects de sécurité préventifs et non correctifs.

La notion de situation de travail définie dans [2] permet de prendre en compte les critères d'usage qui ont une influence sur la santé et la sécurité des utilisateurs sous forme d'activité future des opérateurs.

Aussi, bien que l'expression textuelle soit essentielle, elle n'est qu'une partie de l'ensemble des représentations nécessaires à une approche rigoureuse et efficace de spécification des exigences de sécurité. Se baser sur un processus bien défini, précis et adaptable pour l'expression des exigences, outillé de méthodes de modélisation simples, et fiables est l'un des secrets pour la conception d'un bon produit.

L'ingénierie des exigences (IE), vise à fournir ce type de cadre rigoureux permettant de décrire les systèmes à élaborer, et argumente même en faveur de l'intégration des aspects de prévention au plus tôt par la modélisation du contexte d'utilisation (situation de travail) de l'équipement à concevoir au moyen de modèles formels dont NIAM, une méthode de traduction des exigences textuelles en langage formel offrant une pédagogie plus attrayante en identifiant la connaissance (besoin) implicite via la modélisation des connaissances (besoin) explicites.

Et dans le but d'une spécification encore plus précise, les ontologies seront mobilisées, un langage de modélisation souvent utilisé en système d'information et rarement dans le domaine de la conception des équipements industriels, connues pour être des sources riches de connaissances et, étant structurées et dotées de mécanismes de raisonnement, elles forment un outil puissant pour guider l'analyse des exigences de sécurité.

Ainsi, l'objectif de l'étude se résume à tester quatre hypothèses principales

- La découverte des exigences de sécurité peut être effectuée en plusieurs étapes par analogie à l'ingénierie des exigences.
- Les contextes d'utilisation et le comportement futur du système et de l'utilisateur permettent-ils d'identifier les problèmes de sécurité.
- L'utilisation d'une méthode d'ingénierie de la connaissance permet-elle de structurer les exigences de sécurité exprimées en langage naturel.
- Recourir au domaine de représentation des connaissances est-il une première réponse à la spécification formelle des exigences de sécurité.

METHODOLOGIE

L'approche proposée se base sur l'interopérabilité des méthodes provenant du domaine de l'Ingénierie des Exigences et d'Ingénierie Connaissance (Fig 1).

Xème Conférence Internationale : Conception et Production Intégrées, CPI 2015, 2-4 Décembre 2015, Tanger - Maroc.

Xth International Conference on Integrated Design and Production, CPI 2015, December 2-4, 2015, Tangier - Morocco.

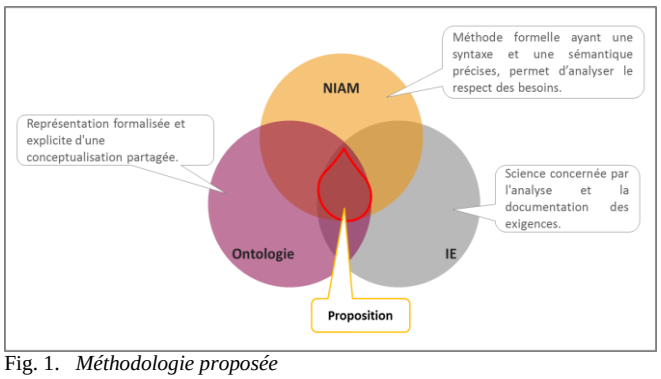

Fig. 1. *Méthodologie proposée*

Le principe est de s'appuyer sur l'ossature du processus de l'ingénierie des exigences (IE) (1ère hypothèse) (élucider, analyser, spécifier, vérifier) [3] auquel viendront s'associer -à différentes phases-, différentes méthodes pour assurer la découverte des besoins en sécurité comme suit :

1. Elucidation

L'IE fournit un vaste ensemble de techniques, de méthodes et d'outil pour l'identification, la collecte et retranscription des exigences. [4] présente quatre catégories de techniques d'élicitation : Techniques conversationnelles, Techniques observationnelles, Techniques analytiques, Techniques synthétiques.

La 2nd hypothèse de ce travail est l'identification des problèmes de sécurité à partir des contextes d'utilisation le comportement de l'équipement et de l'équipe de travail : Notion de Situation de travail.

L'élucidation est basée donc sur l'utilisation des techniques observationnelles [5] qui permettent d'enregistrer les comportements des personnes, de les visionner, de capter des scènes et générer des descriptions narratives des situations au moment où elles se produisent et ainsi identifier les menaces, les phénomènes dangereux, les zones dangereuses et les acteurs exposés au danger et anticiper certaines contre-mesures.

Le résultat est un ensemble de besoins de sécurité textuels à analyser et à modéliser dans les étapes qui suivent.

Une définition générique d'une situation de travail issue du recensement des différentes définitions [2] donne :

« Une situation de travail (Sdt) est entourée par un ensemble d'éléments physiques, chimiques, biologiques, organisationnels, sociaux et culturels dans lequel elle évolue, on y trouve un ou plusieurs systèmes sur lesquels exercent des équipes de travail une ou plusieurs tâches, qui peuvent également nécessiter des outillages (outils et des consommables). Un événement dangereux est susceptible de survenir fortuitement dans une situation de travail qui peut contenir plusieurs phénomènes dangereux et donc générer des zones dangereuses. La possibilité d'une interaction entre l'utilisateur et cette zone dangereuse permet d'identifier des risques ».

2. Analyse

Seule une partie de la connaissance initiale relative à la sécurité -formulée dans l'étape 1-est explicitement utilisée comme un besoin d'exigence [6].

Cette seconde étape consiste à épurer, réorganiser et compléter les besoins de sécurité recueillies au cours de l'étape précédente en identifiant des éléments du domaine et les interactions entre eux par l'élaboration de phrases élémentaires de type sujet verbe complément -principe de la méthode NIAM [7] - support de la connaissance recherchée ne faisant subir aucune perte d'information.

Afin d'avoir une compréhension claire de toutes les connaissances contenues dans le texte descriptif ci-dessus (Etape élucidation), les Sdt décrites sous forme textuelle sont analysées par la construction de phrases élémentaires et la définition des interactions entre les éléments du domaine selon l'approche NIAM. Ci-dessous une introduction au premier concept central « situation de travail » pour faciliter la compréhension de la méthodologie :

- Une situation de travail identifie aucun, un ou plusieurs risques.
- Une situation de travail a une ou plusieurs tâches de réalisation.
- Une situation de travail fait intervenir une ou plusieurs équipes de travail.
- Une situation de travail contient aucune, une ou plusieurs zones dangereuses.
- Une situation de travail est influencée par un ou plusieurs éléments d'environnement.
- Dans une situation de travail est utilisé aucun, un ou plusieurs auxiliaires.
- Dans une situation de travail n'évolue aucun, un ou plusieurs phénomènes dangereux.
- Une situation de travail concerne un ou plusieurs systèmes.
- Dans une situation de travail survient zéro, un ou plusieurs événements dangereux.

(le reste des éléments Système, Principe de solution, Tâche, Phénomène dangereux, Risque, Auxiliaire, Mesure de sécurité, Zone dangereuse, Environnement, Equipe de travail, Evénement dangereux sont présents dans [8].)

3. Spécification

La démarche de formalisation et de spécification consiste dans un premier temps à transformer les phrases élémentaires issues de la phase d'analyse en une représentation dans le formalisme proposé par NIAM. Puis dans un second temps à introduire des ontologies relatives aux aspects de prévention et de sécurité dans le domaine sécurité équipements.

A. Etape 1:

Chacune des idées présentes dans les phrases élémentaires est représentées par des concepts ainsi que par les relations entre concepts qui contribuent à limiter les possibilités d'interprétation du texte.

La figure 2 présente une vue globale de la formalisation proposée réalisée par la méthode NIAM qui permet de mettre en évidence les frontières de la notion situation de travail et les différentes aspects relatives à la sécurité identifiable à partir de cette situation de travail.

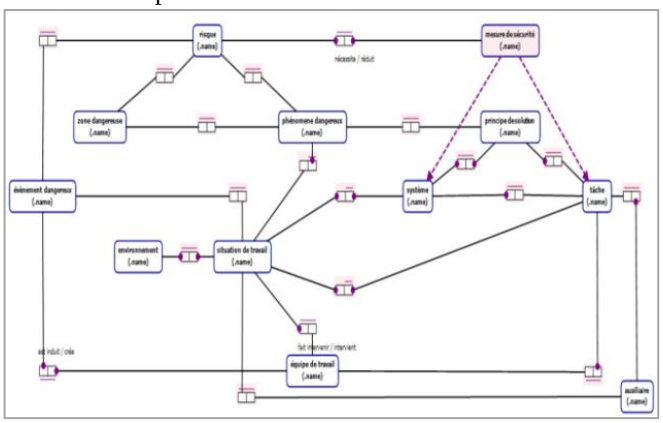

Fig. 2. *Une vue globale du modèle NIAM générique de la situation de travail.*

B. Etape 2 :

L'objectif est de s'initier à la construction d'une partie d'ontologie couvrant les aspects sécurités concernés par les situations de travail qui fournit la structure nécessaire permettant une capitalisation des connaissances à des fins de préservation et de transmission.

1) Spécification

Le développement débute par la phase de spécification qui consiste à établir un document de spécification des besoins où l'ontologie à construire est dérivée à travers cinq aspects :

- Domaine de connaissance: l'ontologie s'inscrit dans le cadre de la sécurité des opérateurs lors de l'utilisation d'une machine. Elle prend ses concepts dans le domaine de sécurité machine, et le domaine de situation de travail.
- Objectif: l'objectif majeur de l'incorporation des ontologies au sein d'un processus de spécification des exigences de sécurité est de formaliser et de normaliser des connaissances expertes permettant d'améliorer la cohérence et l'utilisabilité de ces exigences.
- Utilisateurs: présente l'ensemble des utilisateurs pouvant exploiter l'ontologie. Dans ce cas, ils représentent les concepteurs et les clients qui doivent exploiter les ontologies afin d'atteindre l'objectif visé qui est la spécification des exigences de sécurité.
- Sources d'informations: sur lesquelles est basée la construction de l'ontologie d'applications, elles peuvent être des documents techniques de la sécurité des machines, des standards, des réglementations et des référentiels de sécurité.
- Portée de l'ontologie : cet aspect consiste à déterminer à priori la liste des termes qui composent l'ontologie du domaine à spécifier, les concepts de situations de travail décrit dans le point 2.2 cconstitueront les principaux termes à apparaitre au centre de l'ontologie: événement dangereux, équipe de travail, principe de solution...

2) Conceptualisation

Une fois la majorité des connaissances acquise, il convient de les organiser et de les structurer en utilisant des représentations formelles et faciles à comprendre. La représentation formalisée avec NIAM illustré dans la Fig 2 constitue le modèle conceptuel sur lequel est basée l'ontologie proposée.

a) Organisation

L'ontologie doit couvrir (à terme) le domaine de la sécurité machine : l'ensemble des standards réglementaires et les éléments du domaine d'usage de la machine (situation de travail), la figure 3 propose une réorganisation des éléments de situation de travail représentant les concepts centraux qui doivent apparaitre dans l'ontologie

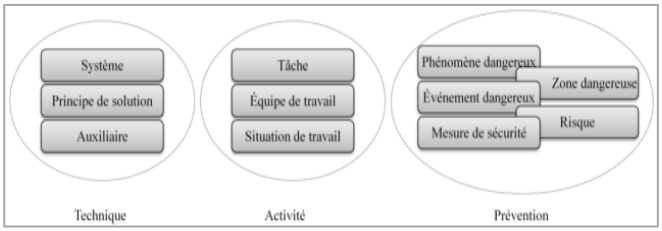

Fig. 3. *Organisation des concepts du modèle NIAM de situation de travail en classes.*

- La classe « Technique » identifie les éléments pertinents à l'analyse d'un système constitué d'un regroupement de principes de solution, engendrant et/ou soumis à des événements potentiellement dangereux en exerçant une activité.
- La classe « Activité » comprend les acteurs ayant à gérer le déroulement de tâches pour obtenir un résultat fixé par la situation de travail.
- La classe « Prévention » permet pour chaque situation de travail d'expliciter tout phénomène dangereux, réel ou possible évoluant dans une zone dangereuse et pouvant causer un risque d'atteinte à la santé de l'opérateur suite à l'apparition d'un événement dangereux.

b) Structure

Dans une première étape d'initiation expérimentale à la mobilisation des ontologies, seule les sous classes « Phénomène dangereux », « Risque » et « Mesure de sécurité » de la classe « Prévention » ont été spécifiées et instanciées. La bibliographie [9] [10] [11] [12] [13] [14] indique qu'il n'existe pas d'approche en cours qui ait pour but d'exploiter

les ontologies dans le processus de développement des exigences de sécurité machine.

- Sous classe : phénomène dangereux

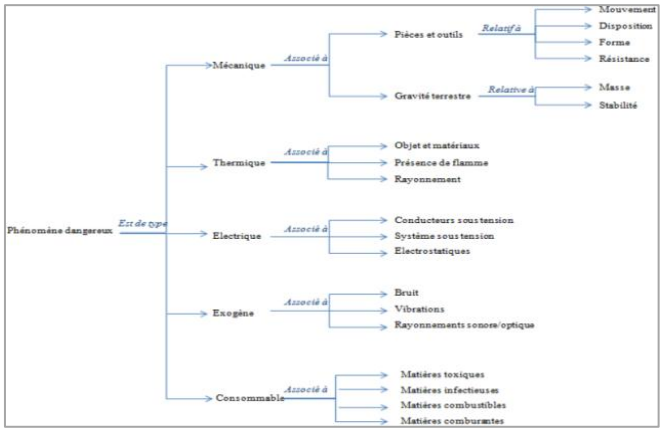

Fig. 4. *Structure de la sous classe phénomène dangereux.*

- Sous classe : Risque

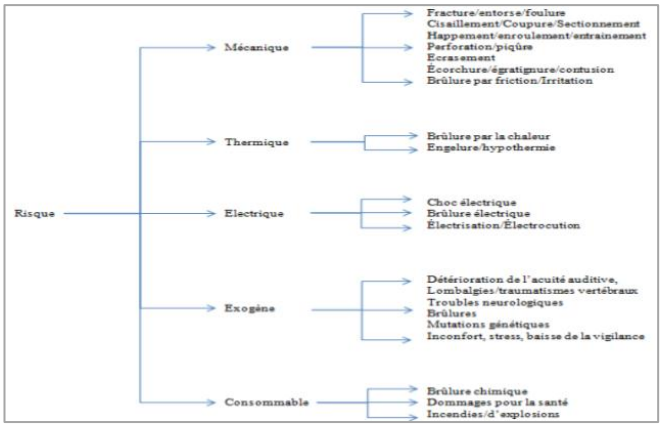

Fig. 5. *Structure de la sous classe risque.*

- Sous classe : Mesure de sécurité

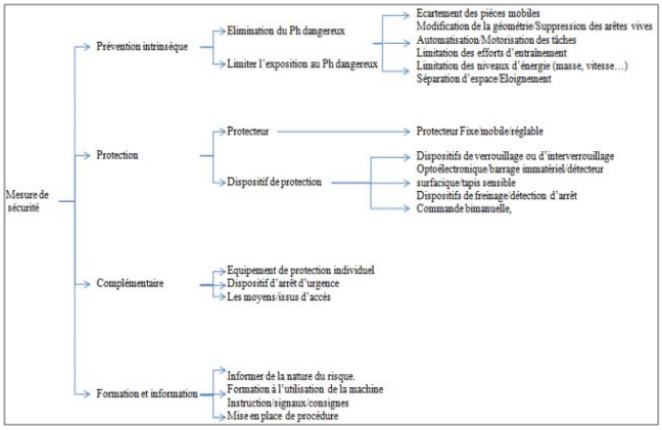

Fig. 6. *Structure de la sous classe mesure de sécurité*

c) Relations

Une fois les concepts du domaine explicités, ces derniers doivent être instanciés pour reproduire un récit relatif à une situation. Pour ce faire il faut définir des relations qui expriment la sémantique du domaine. Le tableau ci-dessous donne un aperçu des plus importantes relations entre ces concepts.

TABLEAU 1. LES RELATIONS ENTRE LES CONCEPTS DU DOMAINE D'ONTOLOGIE

Type de relation	Définition	Exemple
Sémantique	Apporte plus d'informations à la relation. Assiste les concepteurs à la compréhension du domaine. Elimine ambiguïtés et assure la cohérence.	Relation sorte_de, de généralisation-spécialisation exprime qu'un concept est un cas particulier d'un autre concept.
Spécifique	Forme un modèle conceptuel plus spécifique du domaine	Relation nécessite, indique qu'un élément est exposé à l'action d'un autre élément.
Logique	Constituée d'une ou plusieurs prémisses reliées à une ou plusieurs conclusions	Relation de prédiction Si…Alors, définis comme toute règle ayant son antécédent connu a priori, et son conséquent non connu.

4. Vérification :

Le but est de s'assurer de la bonne application des règles imposées par les méthodes utilisées.

Pour le formalisme NIAM le contrôle concerne la règle d'unicité, la cohérence syntaxique et la représentation ainsi que la cohérence des contraintes. Le résultat de ce contrôle produit une liste d'erreurs autrement dit le non-respect des règles. Ce processus de vérification est le plus souvent automatisé sur les outils logiciels support de NIAM.

Afin d'accroitre l'efficacité de cette démarche, un deuxième processus lui est associé plus orienté vers la validation, qui consiste en une transposition de ce schéma en une vue plus vulgarisée en langage naturel permettant de confronter le résultat de la formalisation et la modélisation avec la connaissance initiale sensée être unique. L'estimation de l'écart entre les deux formes de représentation relève de la subjectivité de l'expert du domaine qui estime que la représentation formelle est ou non suffisamment conforme à la connaissance initiale.

Et pour la vérification et la validation de la structure conceptuelle et sémantique de l'ontologie proposée, un expert du domaine doit intervenir. La validation peut se baser sur une terminologie du domaine ou sur un dictionnaire lexicographique. Cependant l'ontologie construite profite d'une certaine précision étant donné que sa structure est basée sur le modèle formalisé NIAM dont les résultats répondent aux critères de vérification et validation

RESULTATS

Ce projet a montré un nouvel axe de recherche possible sur l'interopérabilité des méthodes provenant les différents domaines d'ingénierie (système et connaissance) pour appuyer la spécification des exigences de sécurité dans le domaine équipement machine , en prenant les problèmes liés à l'utilisation d'équipement au plus tôt dans le processus de conception, via l'ossature de l'ingénierie des exigences.

L'originalité principale réside dans l'utilisation de la connaissance extraite des ontologies de sécurité. L'approche va guider l'analyste concepteur en lui fournissant des ontologies, un outil et des mécanismes pour en extraire des éléments pertinents de connaissance afin de les appliquer à son analyse des exigences de sécurité. Le résultat visé est une meilleure définition des exigences de sécurité.

DISCUSSION

Les nouvelles fonctionnalités demandées par les utilisateurs à l'ingénierie des exigences de sécurité nécessitent la conception de nouveaux outils et méthodes pour l'élicitation des besoins, le projet de recherche s'articule autour de la formalisation des concepts clefs de la situation de travail afin de pouvoir les traduire sous forme d'exigences.

Néanmoins si l'application de bonnes pratiques peut aider à atteindre cet objectif, elle ne garantit pas d'y arriver à coup sûr. En se basant sur de bonnes pratiques, le projet de recherche agit de même vu qu'à priori, aucun travail de recherche sur une méthode de passage des besoins aux exigences basée sur l'ontologie n'a été recensé dans le domaine de la conception des équipements industriels.

En effet afin d'améliorer le travail réalisé et mieux remplir les objectifs fixés, les recherches futures doivent porter sur les points ci-dessous :

- Enrichissement de l'ontologie par le recours à des experts et à partir des documents du domaine et des bases de données.
- Mise en place de règles d'association pour l'identification automatique des situations induisant le cadre des accidents.
- Programmation d'un raisonneur pour rechercher des situations de travail similaires et adapter les solutions trouvées à la situation de travail actuel.
- Renforcement du processus de vérification et validation.

CONCLUSION

Ce projet de recherche concerne les outils conceptuels dont disposent les acteurs pour spécifier et formaliser le passage des besoins en sécurité aux exigences de sécurité lors de la conception d'un système de production. Un système de production caractérisé par ses attributs humain, physique et informationnel. Exposant ses utilisateurs à des menaces qui exploitent des vulnérabilités dans le système. Autour duquel est proposée une approche méthodologique (Fig 7) qui part des acquis de l'ingénierie des exigences en reprenant ses 4 étapes, et argumente en faveur de l'intégration des aspects de prévention au moyen de modèles formels dont NIAM et mobilise l'ontologie : l'originalité de ce projet.

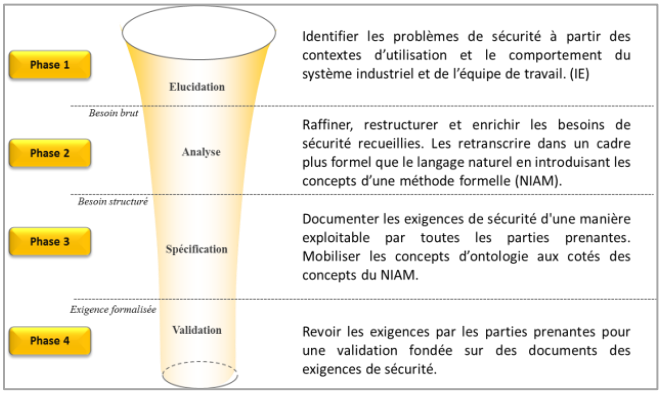

Fig. 7. *La démarche de la méthodologie proposée ainsi que les outils utilisés*

RÉFERENCES

[1] Fabian et al.,2010. A comparison of security requirements engineering methods. Requirements Engineering.

[2] HASAN R., 2002. Contribution à l'amélioration des performances des systèmes complexes par la prise en compte des aspects socio-économiques dès la conception Thèse de l'Université Henry Poincaré Nancy 1.

[3] Wiegers K. E.,2003. Software Requirements, Microsoft Press.

[4] Zheying Z.,2007. Effective Requirements Development - A Comparison of Requirements Elicitation Techniques, Software Quality Management journal, pp. 225-240.

[5] Coulin C. R., 2007.A situational approach and intelligent tool for collaborative requirements elicitation [Report] :Doctoral Thesis / Computing Sciences ; University of Technology and Université Paul Sabatier. - Sydney and Toulouse, 33 .

[6] Eljamal M. H.,2007. Contribution à l'évolution des exigences et son impact sur la sécurité [Report] : Doctoral Thesis /Systèmes Industriels ; Université Paul Sabatier. - Toulouse : [s.n.], 161.

[7] Habrias H., 1988. Le Modèle relationnel binaire : Méthode I. A. NIAM, Livre.

[8] Saadi Y., 2013. Contribution à l'amélioration de l'outillage conceptuel pour la formalisation des exigences de sécurité : Rapport d'études bibliographiques. Master Recherche Conception Industrialisation et Innovation. Ensam.ParisTech Metz

[9] Lodderstedt T., 2002. SecureUML: A UML-Based Modeling Language for Model-Driven Securit, Proceedings of the 5th International Conference on The Unified Modeling Language.

[10] Jürjens H., 2002. UMLsec: Extending UML for Secure Systems Development", Proceedings of the 5th International Conference on The Unified Modeling Language.

[11] McDermott J., 1999. Using Abuse Case Models for Security Requirements Analysis. In Proc. of ACSAC'99. IEEE Press, 55–66.

[12] Firesmith, Donald G., et Firesmith Consulting. 2003.Engineering Security Requirements . Journal of Object Technology 2, 53–68.

[13] Liu L.,J., 2003. Security and Privacy Requirements Analysis within a Social Setting, RE, Proceedings. 11th IEEE International, 2003