RESCUEIT : sécuRisation dE la Chaîne logiStique orientée serviCe depUis le mondE des objets jusqu'à l'univers InformaTique

Laurent Gomez, Mehdi Khalfaoui, Elie El-Khoury, Cedric Ulmer, Jean-Pierre Deutsch, Ouarda Chettouh, Omar Gaci, Herve Mathieu, Ethmane El Moustaine, Maryline Laurent, et al.

▶ **To cite this version:**

Laurent Gomez, Mehdi Khalfaoui, Elie El-Khoury, Cedric Ulmer, Jean-Pierre Deutsch, et al.. RESCUEIT : sécuRisation dE la Chaîne logiStique orientée serviCe depUis le mondE des objets jusqu'à l'univers InformaTique. WISG '11 : Workshop Interdisciplinaire sur la Sécurité Globale, Jan 2011, Troyes, France. hal-00727624

HAL Id: hal-00727624
https://hal.science/hal-00727624v1

Submitted on 31 Jan 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

RESCUEIT : sécuRisation dE la Chaîne logiStique orientée serviCe depUis le mondE des objets jusqu'à l'univers InformaTique

Laurent GOMEZ[1], Mehdi KHALFAOUI[1], Elie El-Khoury[1], Cedric ULMER[1], Jean-Pierre DEUTSCH[2], Ouarda CHETTOUH[2], Omar GACI[3], Herve MATHIEU[3], Ethmane EL MOUSTAINE[4], Maryline LAURENT[4], Herve SCHNEIDER[5], Claire DARAS[6], Andreas SCHAAD[1]

[1]SAP Research France, 805 Avenue Donat, 06250 MOUGINS

[2]LOGPRO Conseil

[3]ISEL

[4]Telecom Sud Paris

[5]SOGET

[6]Kuehne + Nagel

laurent.gomez@sap.com, mehdi.khalfaoui@sap.com, cedric.ulmer@sap.com, jpdeustch@logpro.fr, ochettouh@logpro.fr, omar.gaci@gmail.com, herve.schneider@soget.fr, herve.mathieu@gmail.com, ethmane.moustaine@yahoo.fr, Maryline.Laurent@it-sudparis.eu, claire.daras@kuehne-nagel.com, andreas.schaad@sap.com

Résumé – Dans les processus logistiques, de nombreuses organisations (publiques et privées) sont impliquées, et chacune a potentiellement son propre outil de gestion de chaîne logistique (Supply Chain Management). Cependant, elles sont amenées à travailler de pair sur le processus global; d'abord en terme de planification, puis en terme d'opération, avec une vue sur la gestion des interruptions et sur la gestion de la résilience. Du point de vue modélisation, RESCUEIT propose de représenter une chaîne logistique complète dans le domaine de la sécurité civile. Au niveau de la modélisation, le projet propose d'intégrer les requis de sécurité. Il propose également une base de données de risques et mesures de réductions spécifiques aux chaînes logistiques. D'un point de vue requis, le projet propose d'identifier les paramètres de sécurité adéquates, et qui nécessitent d'être surveillés et pris en charge. Du point de vue de l'Internet des Objets, le projet propose d'améliorer l'utilisation des réseaux de capteurs sans fils et des RFIDs pour répondre aux besoins spécifiques d'une chaîne logistique sécurisée. Dans cet article, nous présentons une modélisation d'un scénario orienté matières dangereuses de chaîne logistique. A travers ce scénario, nous motivons l'intégration de réseaux de capteurs dans une chaîne logistique. Nous démontrons également les enjeux techniques et de sécurité que soulève une telle intégration. Nous proposons enfin des directions de recherche pour le projet RESCUEIT afin de répondre de manière efficace à ces enjeux.

Abstract – In global supply chains, many organizations (be it public or private) are involved, and each may own its supply chain software. Therefore, they have to collaborate in a global process; first in terms of planning, second from an operational perspective, with a view on the management of attacks and on resilience. From a modeling perspective, RESCUEIT proposes to represent a complete supply chain in the public security area. From a modeling perspective, the project proposes to integrate security requirements. It also proposes a database about risks and mitigation procedures related to supply chains. From a requirements perspective, the project proposes to identify the relevant security parameters, which need to be monitored and controlled. From an Internet of Things perspective, the project will enhance the usage of wireless sensor networks and of RFID systems, tailored for the specific needs of a secured supply chain. In this article, we introduce and model a dangerous goods oriented scenario. Through this scenario, we motivate the integration of smart items in supply chain management system. We demonstrate that such integration raise several technical and security challenges. We propose some research directions for secure supply chain management system supported with smart items.

1. Contexte

Le projet franco-allemand RESCUEIT travaille sur le concept d'une plateforme logistique sécurisée. Dans le cadre de ce projet, nous adressons (i) la modélisation de chaîne logistique globale et l'identification des risques, puis (ii) les opérations sûres et sécurisées et enfin (iii) la résistance aux attaques. Le résultat du projet RESCUEIT sera une plateforme de gestion de la chaîne logistique sécurisée, compatible avec les contraintes économiques et réglementaires Allemandes et Françaises.

La partie Allemande du projet se focalise sur l'aspect monde « virtuel », c'est-à-dire qu'il se concentre sur le logiciel de logistique, sur une base de données de gestion des risques, sur son utilisation de services web, sur les attaques logicielles envisageables, et sur l'intégration des mesures de protections adéquates. La partie Française du projet met l'accent sur l'aspect monde « réel ». Elle travaille sur la connexion du logiciel de logistique vers la chaîne d'exécution réelle, que ce soit en termes de géo-localisation, de capteurs ou de balises RFID. Les attaques possibles seront également prises en comptes, ainsi que les mesures de protections correspondantes.

Les parties Allemande comme Française travaillent sur la notion centrale de base de données de risques et de méthodes de réduction. Ceci permet aux acteurs de la chaîne logistique d'identifier les points faibles et d'implémenter les contrôles appropriés. Plus particulièrement, les partenaires allemands se concentrent sur les attaques et mesures de réduction d'un point de vue logiciel, tandis que les partenaires français travaillent d'un point de vue Internet des Objets.

Les principaux objectifs du projet sont les suivants :

- La définition et le développement d'une plateforme logicielle de logistique sécurisée, sure et robuste ;
- La définition d'une base de données logistique sur les risques et les mesures de réduction, d'un point de vue logiciel et matériel;
- La visualisation des propriétés de sécurité et de sûreté dans une chaîne logistique globale ;
- La configuration automatisée de services lies aux capteurs ou au système informatique.
- Un service d'évaluation de la gestion de la vie privée, pour l'analyse commune des chaînes logistiques et des possibles causes et effets d'une attaque contre les outils logiciels et physiques.

Le projet contient un aspect transversal, car il aborde également les aspects réglementaires et légaux pour l'opération de sa plateforme.

Ce papier est organisé de la façon suivante : section **Erreur ! Source du renvoi introuvable.**~~2~~ est dédiée a la description et la modélisation d'un scénario illustrant le stockage de matières dangereuses. Ce scénario démontre l'intérêt de l'intégration de réseaux de capteurs et tags RFID pour la détection et prévention d'incident dans la chaîne logistique. Les défis techniques et sécurité de cette intégration sont détaillés dans la section 0~~4~~. Nous concluons ce papier avec des directions de recherche du projet RESCUEIT.

2. Scénario

2.1 Scénario

KUEHNE + NAGEL situé à Savigny le temple (77) est un prestataire logistique dont l'activité constitue à assure le stockage et la gestion des flux logistiques de produits destinés à l'approvisionnement des grandes surfaces : stocker, trier et préparer des livraisons de produits divers, généralement de grande consommation.

Les produits stockés dans cet entrepôt sont de natures très diverses, toutefois compte tenu du volume de stockage et de la réglementation, certains produits stockés sont dit dangereux (générateurs d'aérosols, liquides et solides inflammables, phytosanitaires, engrais...) ce qui classe le site de Savigny le temple, SEVESO II au titre des installations classées pour la protection de l'environnement.

Les activités du site de stockage de Savigny le Temple ne mettent pas en jeu de procédés industriels complexes. Il n'implique pas des activités de manutentions avec des chariots électriques.

Dans cet article, nous avons choisi de nous intéresser à un scénario de déversement de produits dangereux sur le site. Le déversement accidentel est lié à la présence de produits liquides sur le site. Les déversements peuvent entraîner l'épandage plus ou moins important d'une nappe de liquide dangereux. Un déversement de produit dangereux peut apparaître suite à la chute d'une ou plusieurs palettes d'un camion ou d'un rack mais également suite à la perte de confinement d'un contenant (flacon, bidon) ou d'une série de contenants.

Figure 1: Stockage en rack

Un déversement de produit dangereux peut avoir une incidence sur l'environnement et les personnes. Lors de la perte de confinement d'un contenant, le liquide s'écoule et forme une nappe. La taille de cette nappe est principalement fonction de la topographie, de la viscosité du produit et de sa quantité.

Le scénario choisi aura lieu au sein de la cellule de stockage A4. Un exemple de produit stocker dans cette

cellule est le Garlon qui est un herbicide. C'est un liquide inflammable qui est nocif et dangereux pour l'environnement. Si l'on se réfère a la Fiche de données de sécurité, ce produit fait l'objet de divers contraintes de manipulations (ne pas fumer, inhaler, ports de gants…), de transports et de stockage, en effet il ne doit être stocké en présence de produits comburants, toxique ou corrosif.

Dans le cadre de notre scénario, nous supposons ~~que~~ qu'une personne aurait intentionnellement stocké au sein de cette cellule un produit incompatible, Nous prendrons pour exemple un engrais qui est un solide comburant. Nous partons du fait que sur l'ensemble des racks (qui présente 6 niveaux de stockage) la personne malveillante aurait au préalable stocker sur les 3 niveaux les plus bas de l'engrais.

A plusieurs niveaux supérieurs, il aurait intentionnellement dégradé les palettes de Garlon (en les perçant avec les fourches de son chariot élévateur) avant de les disposer à plusieurs endroits sur les niveaux supérieurs de cette même cellule de stockage. Cette même personne aura au préalable endommagé à plusieurs endroits les pieds de racks. Nous pouvons imaginer que ce scénario ait lieu le vendredi soir. Les produits en hauteur (Garlon) commenceront par fuirent sur les produits plus bas (engrais).

Au bout d'un certain moment les racks commenceront à s'effondrer entrainant les risques suivants :

- Incendie, flux thermique qui peut, selon son intensité, avoir des effets plus ou moins graves pour les personnes (brûlures, mort). Les marchandises et leurs emballages sont combustibles et constituent donc un potentiel calorifique non négligeable pouvant favoriser un incendie. En cas d'incendie, la combustion des matières stockées dans les cellules de l'entrepôt va entraîner le rayonnement d'un flux thermique
- L'émission de gaz de combustion qui peuvent se charger de gaz toxiques en quantités plus ou moins importantes. Selon les concentrations de ces gaz, les effets sur les personnes peuvent être dangereux, En cas d'incendie, les marchandises vont se décomposer et entraîner la formation de gaz divers de combustion. Parmi ceux-ci, certains sous forme de traces peuvent être dangereux pour les personnes comme l'acide cyanhydrique, les oxydes de soufre.
- La dispersion d'eaux d'extinction. L'eau utilisée par les pompiers pour éteindre l'incendie va se charger de débris et produits divers qui sont des polluants. Elles ne peuvent pas être rejetées dans le milieu naturel ou les réseaux publics. En cas d'incendie, l'eau utilisée par les pompiers va se mélanger avec les produits stockés dans l'entrepôt. Ces produits ainsi que les produits de dégradation peuvent créer une pollution des eaux de surface, du sol ou du sous-sol. Il est donc très important de maîtriser l'écoulement des eaux d'extinction afin d'éviter leur déversement à l'extérieur du bâtiment.

2.2 Modélisation

Nous proposons dans cette section une modélisation par BPMN (Business Process Model Notation) [13] du scénario évoqué précédemment. Nous sommes notamment intéressés par l'identification des principales conséquences d'un tel accident de matières dangereuses et la manière dont la présence de moyens de détection (capteurs dans l'entrepôt) peut permettre d'évaluer en temps réel le déroulement et les conséquences de l'accident.

Nous considérons alors un entrepôt dans lequel les activités d'un cariste sur un rack provoquent la chute d'une palette de produit dangereux d'un type donné. Cette palette va alors s'écraser sur d'autres pour provoquer la rupture de la lisse, ou de tout autre élément, dont l'effondrement accélérera la chute et la collision des palettes de l'ensemble du rack.

Notre but est d'étudier les conséquences d'un accident afin de développer de meilleures stratégies de prévention et de détection. En effet, même si des politiques de classification de produits dangereux sont en vigueur dans les entrepôts, les collisions et tous les autres types d'accidents de manipulations peuvent créer des situations potentiellement très dangereuses. Le scénario que nous présentons doit alors décrire les causes d'un accident, permettre d'évaluer les conséquences qui en résultent et enfin établir une nouvelle stratégie de suivi en temps réel, par des capteurs, des différents événements.

2.2.1 Étude de scénarii

La manipulation de matières dangereuses est composée d'un ensemble de missions logistiques qui débutent depuis le lieu de production jusqu'au site d'exploitation. Ainsi, ces biens se retrouvent transportés par des moyens multimodaux (par voie maritime, terrestre ou aérienne) d'un entrepôt à un autre jusqu'à destination. Ici, pour étudier et évaluer les conséquences inhérentes à la manipulation de matières dangereuses, nous décrivons les possibilités d'accidents par des scénarii.

Dans [12][~~10~~] et [12][~~11~~] nous trouvons des scénarii décrivant différents types d'accidents dont les causes sont par exemple, le feu, la pression ou une explosion. Ces scénarii constituent alors un moyen d'évaluation des conséquences d'accidents. D'une manière générale, le « Guidelines for Quantitative Risk Assessment » [12] nous renseigne sur les principes et les méthodes pour quantifier les différents effets des accidents impliquant des matières dangereuses.

Il apparaît alors que les conséquences d'un accident sont évaluées par plusieurs mesures notamment la superficie endommagée ou encore le nombre de personnes physiques présentes au moment de l'accident. Parmi ces différents moyens de quantifications, nous décrirons dans le scénario que nous présentons la nature des phénomènes

mis en jeu pendant un accident. Nous serons alors amenés à tenir compte des effets suivants :

- Diffusion de substances toxiques pour la santé et l'environnement ;
- Emission d'énergie thermique ;
- Libération de pression.

Nous modéliserons donc un scénario d'accident de matières dangereuses dont les conséquences dépendent des propriétés physico-chimiques des produits impliqués. Par une modélisation via BPMN, nous décrirons l'enchaînement des événements pour déduire une stratégie de suivi en temps réel grâce au déploiement d'un réseau de capteurs disséminés dans l'entrepôt.

2.2.2 Modélisation par BPMN

BPMN (Business Process Model Notation) [13] est une norme de représentation graphique pour la modélisation de processus. Cette norme constitue un cadre général de description de processus de telle sorte qu'elle s'adresse à différents types d'utilisateur, aussi bien des managers que des techniciens, tout en fournissant un niveau de description sémantique élevé. BPMN propose alors une base standard de modélisation indépendamment des outils d'implémentations.

La norme BPMN 1.1 s'appuie sur deux concepts pour organiser la modélisation de processus, à savoir les « orchestrations » et les « chorégraphies ». Les orchestrations concernent la manière dont les processus se déroulent dans le temps tandis que les chorégraphies sont relatives aux interactions inter-processus et décrivent leurs interdépendances.

La norme met en jeu un nombre d'objets fini parmi lesquels nous pouvons citer les activités qui décrivent les actions réalisées au sein d'un processus ou encore les événements qui marquent le début ou la fin d'une activité.

2.2.3 Étude de cas

Le scénario que nous modélisons ici a été défini par rapport à un historique d'accidents survenus dans des entrepôts de matières dangereuses.

Ce scénario concerne les activités de manutention de caristes sur un rack de l'entrepôt. En enlevant une palette et suite à un événement non identifié (vice caché) la lisse la supportant vacille et se rompt sous le poids de son chargement. Les autres palettes jusque-là entreposées chutent sur l'étage inférieure et provoquent des collisions de produits dangereux qui, avec le choc, explosent et provoquent des écoulements de liquides du fait de la perte du confinement. Par un effet domino, les lisses des étages inférieures sont endommagées jusqu'à ce qu'elles cèdent sous l'accumulation du poids des palettes ayant déjà chutées. Une fois que le rack est détruit et que les palettes se sont entrechoquées, leur contenu liquide se répand sur le sol tandis que des explosions de faible amplitude se produisent durant cette avalanche de palettes. Une fois libérés, les liquides se répandent et s'écoulent sur le sol de l'entrepôt. Leur rétention dépend alors de l'architecture de l'entrepôt comme le prévoit la législation.

Le scénario que nous venons de décrire est illustré par la Figure 2. Nous avons retenu deux types d'utilisateurs : le cariste et le personnel du site. Lorsque l'effondrement du rack est amorcé par la chute de la palette à décharger, le cariste est pris dans l'avalanche. Il faut alors prévenir le responsable sécurité ou tout autre personne faisant autorité en fournissant des informations quant à l'accident. Le personnel met alors en œuvre les procédures idoines pour le type d'accident rapporté par le cariste ou d'autres témoins.

L'utilisation de capteurs dans l'entrepôt à des fins de sécurisation peut se révéler efficace à plusieurs titres. D'abord, à la manière des sprinklers, des capteurs pourraient surveiller l'intégrité de la structure des racks. Dès qu'une défaillance est détectée, le déclenchement d'un système d'alarme et d'une procédure d'évacuation adaptée favoriseraient les réactions à ce type d'accident En effet, les témoins d'un accident ne décriront pas forcément de la manière ce qu'ils ont pu constater. Leurs témoignages n'est pas toujours fiable puisque ces témoins ont pu être choqués ou blessés.

Par ailleurs, sur le même modèle que les capteurs de détection de particules en suspension ou encore les capteurs de dégagements de chaleur ou de pression, nous pourrions intégrer un réseau de capteurs de détection de fuite de produits liquides inflammables. Ces capteurs fourniraient une description en temps réel de la nature d'un accident. En effet, nous pouvons facilement comprendre que les descriptions fournies par les témoins d'un accident ne sont pas toujours les mêmes du fait de l'interprétation de chacun. De même ce réseau de capteur favoriserait la localisation de l'accident, une telle information étant bénéfique notamment parce qu'il devient possible d'anticiper les conséquences de l'accident.

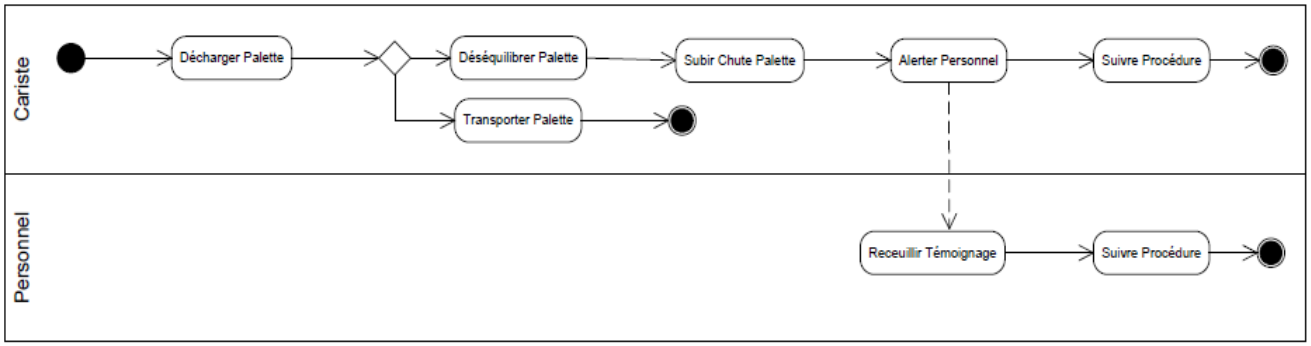

Figure 2 : Modélisation du scénario par un diagramme BPMN.

Devant les différentes possibilités d'utilisation d'un réseau de capteurs pour mettre au point de nouvelles stratégies de prévention et de gestion d'accidents de matières dangereuses, il est important d'évaluer la faisabilité de telles options. Le projet Rescue-IT représente cette opportunité puisque, entre autres, notre objectif est d'intégrer une traçabilité des matières dangereuses dans la chaîne logistique et ainsi optimiser la gestion du risque inhérent à ce type de marchandises.

3. Intégration des WSANs et RFIDS dans une chaîne logistique

Comme démontré dans la section **Erreur ! Source du renvoi introuvable.**2, il apparait que les capteurs et les tags RFID présentent un intérêt certain en vue de la sécurisation des chaînes logistiques. Une des raisons principale de cette attrait réside dan la capacité de contrôler et de surveiller des larges espaces de ce type d'appareillage. Mais l'intégration de ce type de technologie avec des systèmes industriels soulève de nombreux défis techniques (ex., traitement, routage de données), et de sécurité (ex., confidentialité, intégrité des informations).

Dans cette section, nous nous concentrons sur les solutions techniques et de sécurité existantes pour l'intégration des tags RFID et de capteurs dans une chaîne logistique.

3.1 Défis techniques

Afin de faciliter l'intégration des capteurs et RFID dans des applications industrielles, de nombreuses couches logicielles ont été proposées, Leur objectif est d'agir étant couche de médiation, pour l'acquisition et le traitement des informations en provenance des WSANs et RFIDS, ainsi en tant que fournisseur de service.

Concernant la surveillance du monde réel, la couche de médiation a pour rôle la collection d'information en provenance des RFID et capteurs, du traitement de cette information, et leur mise à disposition auprès des applications industrielles. D'autre part, concernant la mise a disposition de service par les RFID et capteurs, les applications industrielles peuvent prendre le contrôle du monde réel en assignant des tâches spécifique (ex. bloquer un container, activer un alarme).

3.1.1 Intégration des RFIDs

Les RFIDs (Radio Frequency IDentification) sont considérés comme une révolution dans le domaine de la logistique car ils permettent de gérer et de réduire considérablement les coûts. Ils offrent la possibilité de synchroniser toute une chaîne logistique et de tracer les produits tout au long de la chaîne. Ainsi le gestionnaire de la chaîne dispose d'une meilleure visibilité, d'une meilleure réactivité et a la possibilité de récapituler en bout de chaîne toutes les étapes par lesquelles un produit est passé.

L'avantage des RFID vs les codes barres est de permettre la lecture du RFID sans nécessiter de visibilité directe entre l'objet à identifier et le lecteur. De plus, ils permettent d'automatiser certaines tâches fastidieuses comme le contrôle d'expédition, le contrôle de réception et la prise d'inventaire. Les RFID peuvent aussi être servir à lutter contre la contre façon de produits, comme par exemple les produits pharmaceutiques, grâce à l'authentification et la traçabilité des médicaments. Le consommateur peut en effet consulter toutes les informations relatives à un produit en tapant simplement son code.

C'est dans le but d'uniformiser et d'internationaliser les solutions RFID bas coût destinés à la logistique, que le consortium GS1 a approuvé le standard international EPCglobal [1] en 2004. S'y trouve défini un système d'identification EPC (Electronic Product Code) des étiquettes RFID.

Le réseau EPCglobal est construit sur le modèle de l'Internet et est dédié aux chaînes logistiques. Il a pour objectif de fournir un cadre standard permettant à des partenaires d'une chaîne logistique d'échanger des informations / des évènements relatifs à des produits. Pour interagir avec le réseau EPCglobal, chaque partenaire doit disposer d'un système d'information dédié à la gestion de produits tagués (EPCIS, EPC Information Services). Les consommateurs ont également la possibilité de consulter, via Internet, des informations relatives aux produits tout simplement en tapant leurs codes.

Le réseau EPCglobal nécessite pour sa mise en œuvre une ensemble de composants, à savoir : un sous-système RFID (ensemble de lecteurs), un middleware EPC, l'Object Naming service (ONS), l'EPCIS et l'EPC Discovery Service (EPCDS). Chaque composante joue un rôle unique et important au sein du réseau EPCglobal.

L'ONS utilise le service DNS (Domain Name System) déjà existant pour chercher des informations sur un EPC.

ONS et EPCIS aident les utilisateurs à trouver des informations sur l'objet demandé depuis le réseau EPCglobal. EPCDS fonctionne comme un moteur de recherche pour les données liées à l'EPC.

Cependant, la technologie RFID souffre d'un manque critique de sécurité qui peut aboutir au non respect de la vie privée des utilisateurs. Notons que les systèmes RFID ont des ressources extrêmement limitées, ce qui rend les solutions classiques conçues pour les réseaux filaires ou sans fil inappropriées. Notons que les étiquettes (tags) EPC de deuxième génération intègrent uniquement un générateur pseudo aléatoire de 16 bits et un contrôle de redondance cyclique sur 16 bits. De plus, de part l'architecture de communication retenue, les solutions RFID ne peuvent pas s'appuyer sur des tiers de confiance dans le réseau.

Il est clair que l'adoption de la technologie RFID simplifierait beaucoup les traitements logistiques. Cependant, cela nécessite de la part des industriels, un gros travail de réingénierie de l'ensemble des processus logistiques et de bâtir de nouvelles méthodes de travail inter-organisations.

3.1.2 Intégration des réseaux de capteurs

Les WSANs intéressent bon nombre de domaines métiers (ex. militaire, santé) [9], Communiquant a travers un réseau sans fil, les WSANs peuvent être déployés aisément dans de larges environnements physiques. WSANs sont considérés comme des réseaux auto-organises, intégrant des capteurs hétérogènes, capable de mesurer, traiter, router, et disséminer des informations vers des entités centralisantes, ou gateway.

Ainsi les WSANs améliorent la connaissance de leur contexte aux applications. Ils les supportent quant a leur adaptation, et la prise de décision. De plus, les WSANs augmentent la flexibilité des applications, et permettent d'optimiser leur fonctionnement et leur sécurité.

A l'instar des RFIDs, les capteurs sont réputés pour être des appareillages restreints en termes de ressource (ex. CPU, mémoire, batterie). L'intégration de réseaux de capteurs avec des applications industrielles, et plus précisément avec des systèmes de gestion de chaînes logistiques, soulèvent de nombreux défis techniques. Considérant le monitoring à travers les WSANS, nous avons identifie les besoins suivants : interopérabilité, traitement de l'information, livraison de l'information aux applications.

3.1.2.1 *Interopérabilité*

Cette intégration doit se faire de manière la plus transparente et aisée possible. L'idée est de faciliter l'utilisation de l'information en provenance des capteurs par les applications industrielles. En effet, les applications industrielles ont pour objectif d'utiliser les informations contextuelles pour l'adaptation fonctionnelle ou de leur sécurité. Ce besoin d'interopérabilité s'exprime a la fois a l'acquisition des informations auprès des WSANs, mais également a leur mise a disposition auprès des applications.

3.1.2.2 *Traitement de l'information*

Le traitement de l'information est requis par les applications afin de réduire le flot d'information livre aux applications. En effet, les WSANs fournissent un grand nombre d'information, qui ne sont pas toujours intéressant pour les applications. Ainsi, il y a un besoin très clair de fournir à la demande de l'information prétraitée aux applications. Ce traitement peut s'effectuer à la fois dans les réseaux WSANs, et également dans la couche de médiation.

3.1.2.3 *Livraison d'information aux applications*

Un aspect important de la couche de médiation est la livraison de l'information pertinente aux applications. Il est nécessaire pour les applications de pouvoir accéder à l'information des WSANs de deux manières : à la demande, ou bien de manière automatisée, en fonction de leur besoins. A la demande, une application médicale peut avoir besoin des dernières mesures physiologiques d'un patient. L'application dans ce cas sollicite auprès de la couche de médiation des informations contextuelles. Dans ce cas, l'application peut avoir besoin d'un type d'information précise (ex. rythme cardiaque pour une application de sante). Il suffit pour l'application de filtrer et de choisir le type d'information qui lui sera notifié.

En ce qui concerne le contrôle des WSANs, les applications ont besoin de pouvoir communiquer et envoyer des commandes aux capteurs de manière standardisée. Dans ce cas, l'utilisation de protocoles de communication standardisés comme les WebService [11~~9~~] ou REST [11~~9~~] est nécessaire et permet une intégration plus aisée qu'à travers des protocoles propriétaires.

De nombreuses couches de médiation ont été proposées dans la littérature. [14], [16], [17], [18], [19], [20], [21].

Dans la table Table 3.1-1~~Table 4.1-1~~, nous avons repris leur intégration avec les RFID et les WSANs, distinguant les couches de médiation qui permettent le contrôle et la surveillance.

	Couche de mediation		Mise à la disposition de service	
	RFID support	WSN support	RFID support	WSN support
WASP		X		
CoBIS		X		X
PROMISE		X		
RWIP	X	X	X	X
SAP Auto-ID	X		X	

Table 3.1-1: Plateforme de couche de médiation

Il apparait que la plateforme RWIP développée par SAP Research est un bon candidat pour le projet RESCUEIT. Elle implémente à la fois une couche de médiation et la mise à disposition de service sur les capteurs et tags RFID. La flexibilité de cette plateforme nous permet de répondre aux attentes des applications, et plus précisément à celle d'un système de gestion de chaîne logistique.

3.2 Défis sécurité

3.2.1 RFID

Cependant, la technologie RFID souffre d'un manque critique de sécurité qui peut aboutir au non respect de la vie privée des utilisateurs. Notons que les systèmes RFID ont des ressources extrêmement limitées, ce qui rend les solutions classiques conçues pour les réseaux filaires ou sans fil inappropriées. Notons que les étiquettes (tags) EPC de deuxième génération intègrent uniquement un générateur pseudo aléatoire de 16 bits et un contrôle de redondance cyclique sur 16 bits. De plus, de part l'architecture de communication retenue, les solutions RFID ne peuvent pas s'appuyer sur des tiers de confiance dans le réseau.

Il est clair que l'adoption de la technologie RFID simplifierait beaucoup les traitements logistiques. Cependant, cela nécessite de la part des industriels, un gros travail de réingénierie de l'ensemble des processus logistiques et de bâtir de nouvelles méthodes de travail inter-organisations.

Le peu de robustesse des solutions RFID et l'absence de protection de la vie privée représentent un véritable défi pour les chercheurs. Mark Weiser [2] avait déjà identifié en 1991 que le respect de la vie privée serait l'un des problèmes majeurs de l'informatique ubiquitaire. Aujourd'hui, les travaux en cours tendent à adapter les solutions cryptographiques existantes aux RFID ou d'en définir de nouvelles. Les deux problèmes mentionnés sont le principal obstacle à l'adoption de la technologie RFID, car les ressources très limitées des étiquettes empêchent l'implémentation de solutions de sécurité classiques.

Les principales attaques portant sur les RFID sont les attaques par rejeu, les attaques en déni de services, les attaques physiques et le clonage des étiquettes, ces dernières attaques étant rendues possibles sur les étiquettes RFID bas coût (par exemple, EPC de deuxième génération) du fait de l'absence de mémoire sécurisée.

Les principaux problèmes remettant en cause la vie privée sont les suivants : la fuite d'informations et la traçabilité malveillante des utilisateurs et des objets.

La fuite d'information se produit dans les chaînes logistiques (et dans tous les systèmes RFID) lorsque les informations échangées entre l'étiquette et le lecteur révèlent des informations sensibles sur les objets. Il peut s'agir de l'identité de l'objet, ou des objets attachés à l'étiquette.

Quant à la traçabilité malveillante des utilisateurs et des objets, l'étiquette RFID répond à chaque demande d'authentification, ce qui donne aux attaquants la possibilité de la tracer. Pour éviter toute traçabilité malveillante, il est nécessaire que chaque échange soit assimilé par l'attaquant comme des échanges aléatoires. Pour cela, l'étiquette doit réaliser un chiffrement aléatoire à chaque tentative d'authentification. La plupart des protocoles de sécurité adaptés aux systèmes RFID sont de type défi-réponse. A la différence des solutions de sécurité traditionnelles, le vérificateur (serveur) ne connait pas l'identité de l'objet à identifier (étiquette). Cela se traduit du côté du serveur par une recherche exhaustive qu'il doit effectuer sur sa base de données afin d'identifier l'étiquette RFID. Cette solution est aujourd'hui la seule à garantir la protection de la vie privée et à considérer un modèle réaliste de l'attaquant. Notons toutefois que cette solution ne permet pas le passage à l'échelle (dans le cas d'un grand nombre d'étiquettes).

3.2.2 Réseaux de capteurs

Dans ce contexte, WSAN peut être considéré comme un médiateur sécurisé d'échange d'informations. Les partenaires peuvent stocker des informations, qui sont accessibles à un sous-ensemble des acteurs de la chaîne logistique, dans les capteurs. Le capteur, lui-même, peut interagir avec tous les partenaires de la chaîne, mais il ne peut dévoiler ce contenu qu'aux acteurs authentifiés.

3.2.2.1 *Contrôle d'accès*

Dans la chaîne logistique, plusieurs organisations ont compris que le partage d'informations avec d'autres partenaires de la chaîne peut conduire à une réduction significative des coûts. Par exemple, La planification collaborée et la prévision sont des approches visant à réaliser des prévisions précises de la demande et améliorer les opérations de la chaîne logistique. En partageant des informations pertinentes sur la demande entre des partenaires commerciaux dans la chaîne, les prévisions deviennent plus précises, ce qui a un effet positif sur la performance de la chaîne logistique. Par conséquent, il y a un besoin évident de mécanismes préservant les

informations sensibles de chaque partenaire, afin de conserver leurs avantages compétitifs [26].

Le composant de contrôle d'accès dans les WSAN est responsable d'autoriser et d'accorder aux utilisateurs le droit d'accéder au réseau et aux données stockées par les capteurs. Un réseau de capteurs rassemble une variété de données partagées par les utilisateurs du réseau. Afin de respecter la confidentialité de ces données, les utilisateurs doivent avoir des droits différents selon leur rôle. La gestion de la liste de contrôle d'accès, avec des rôles différents pour chaque utilisateur peut être difficile, surtout avec la contrainte de la mémoire limitée dans les capteurs.

La révocation c.-à-d. la capacité de l'annulation de certains comptes d'utilisateurs ou des droits d'accès qui ont été faits auparavant, doit être possible. Un mécanisme simple et facile doit être met en place, afin de parvenir à un contrôle d'accès simple avec une révocation.

Il y a des techniques de contrôle d'accès qui peuvent réaliser des contrôles d'accès avec révocation [24][24][25]. Cependant, elles ne sont pas adaptées à notre problème. Elles ont été conçues spécialement pour un WSAN fixe, et non pour un WSAN mobile, avec l'interaction de nombreux partenaires.

La sécurité d'un réseau des capteurs mobile est encore un domaine de recherche ouvert, avec plusieurs défis à résoudre. Par exemple, le contrôle d'accès pour un nœud mobile est plus difficile que statique, car on doit faire face au transfert d'une passerelle à une autre passerelle[27], en plus des autres problématiques de confidentialité, et d'intégrité.

3.2.2.2 *La responsabilité*

La responsabilité peut être définie par l'obligation de fournir une justification de son action si une autorité l'a demandé. Dans un contexte de chaîne logistique, cela signifie la définition de la responsabilité d'une erreur ou une détérioration de la marchandise entre les partenaires de la chaîne logistique. La collaboration croissante, entre différents acteurs hétérogènes, exige ce genre de mesure visant à protéger les acteurs de la chaîne logistique. Par exemple, la responsabilité peut aider à identifier qui a éteint la climatisation pendant un certain temps dans un champ de fleurs, afin d'optimiser ses gains.

WSAN peut aider à atteindre cet objectif, car il suit la marchandise dans toute la chaîne, et il est capable de surveiller différents paramètres de l'environnement physique. Par conséquent, il peut être utilisé par les autorités afin de trouver facilement l'entité coupable[28].

Cependant, la recherche dans ce domaine doit encore être approfondie. Jusqu'aujourd'hui, il n'existe aucun moyen automatique pour décider le rôle de l'autorité (la police). En outre, tout coupable peut facilement détruire physiquement le capteur, ce qui empêche toute récupération des informations dans les capteurs pour les examiner.

3.2.2.3 Le suivi de la marchandise

Les WSANs permettent également de suivre la marchandise en temps réel, en intégrant un GPS au capteur, puis reporter la localisation au système de la SCM. La fiabilité de cette information est très importante, car un partenaire peut avoir besoin de suivre la marchandise afin de minimiser le coût du stockage. En plus, le fait que les capteurs ne sont pas normalisés avec le réseau EPCglobal rend le suivi encore plus difficile. Ce dernier permet aux entreprises d'utiliser la norme Electronic Product Code (EPC) afin de suivi des marchandises dans la chaîne logistique, dont des étiquettes RFID passives ont été collées. Malheureusement, il n'y a pas des normes parallèles pour les capteurs [27][~~27~~].

Mis

Certaines solutions existent déjà [30][31], pour suivre les marchandises. Toutefois, on ne peut pas être les intégrées ou les étendu pour résoudre les autres problèmes de sécurité. Donc, nous devons prendre en compte cette question, lors de la construction de notre système.

Suivre la marchandise dans une chaîne logistique, tout en protégeant la vie privée des acteurs de la chaîne logistique est l'un des enjeux du projet RESCUEIT. Le responsable de la chaîne logistique doit être le seul capable de retracer le chemin parcouru par la marchandise, et identifier les différents acteurs qui ont été sur le chemin. Un acteur, qui n'a pas les droits nécessaires, doit être incapable d'identifier les acteurs qui ont été avant lui dans la chaîne logistique. Les attaques par usurpation et par rejeux doivent être prises en compte.

3.2.2.4 *Evaluation de performance de la chaîne logistique*

Dans la gestion de la chaîne logistique, il est crucial d'assurer un certain niveau de performance afin de répondre aux attentes des clients. Plusieurs méthodologies ont été proposées. Elles visent toutes à améliorer la performance de la SCM. L'évaluation des performances peut être réalisée par différents indicateurs de performance. De la production de matières premières, à la distribution de produits finis au client final, y compris la transformation, le transport des produits, la chaîne logistique implique plusieurs acteurs et contient plusieurs opérations. Chacun d'eux doit être évalué sur la base des indicateurs de performance bien identifiés.

4. Directions de recherche

4.1 Sécurité des RFIDs

Comme identifié dans [3], un protocole d'authentification mutuelle entre lecteur et étiquette est sécurisé s'il satisfait les conditions suivantes :

- Aucune information sur les clés secrètes/identifiants de l'étiquette n'est révélée par l'observation des messages échangés lors de l'exécution du protocole.
- L'authentification n'a lieu que si le protocole exécuté est légitime, autrement dit :

- Le succès de l'authentification est assuré avec la probabilité 1 en cas d'exécution légitime

- La probabilité de succès est négligeable du point de vue de la sécurité en cas d'exécution illégitime.

La sécurité et la protection de la vie privée des systèmes RFID font l'objet de nombreux travaux de recherches [4, 5, 6], mais aucun ne satisfait les exigences de sécurité et de protection de la vie privée dans un contexte de RFID bas coût.

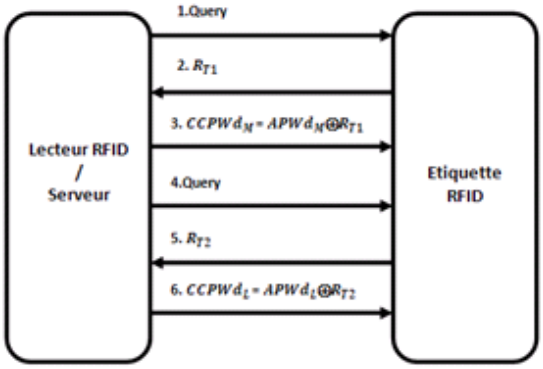

Figure 3: Le protocole d'authentification EPCGen2

Prenons par exemple le standard EPC Generation 2 [1]. Il définit le protocole d'authentification décrit à la Figure 3. Ce dernier repose sur le partage d'un mot de passe de 32 bits entre le lecteur et l'étiquette et ne permet que l'authentification du serveur (situé derrière le lecteur) auprès de l'étiquette. Le protocole se déroule en six étapes, à savoir :

- (1, 2) L'étiquette est interrogée par le lecteur et répond par une valeur pseudo aléatoire R_{T_1}.

- (3) Le lecteur répond par une valeur qui est le résultat de l'opération XOR effectuée sur les 16 bits (sous-clé) les plus significatifs du mot de passe et la valeur R_{T_1}.

- (4, 5, 6) Si la sous-clé transmise par le lecteur est valide, l'étiquette transmet au lecteur une nouvelle valeur pseudo aléatoire R_{T_2}. Le lecteur répond par les 16 bits les moins significatifs du mot de passe xorés avec R_{T_2}.

Si le processus d'authentification s'achève avec succès, l'étiquette peut alors transmettre au lecteur son identifiant EPC en clair. Le lecteur peut ensuite procéder à différentes opérations, comme la désactivation définitive de l'étiquette par un *kill password*.

Notez que le protocole EPCGen2 est vulnérable aux attaques par rejeu et aux attaques en déni de services. De plus, le standard EPCGen2 ne prend pas en compte le problème d'écoute des communications.

Une autre solution [7] est à mettre en avant car elle répond aux besoins des chaînes logistiques de sécuriser les interactions entre différentes organisations. Il est en effet important de permettre aux organisations de partager des informations relatives aux événements associés à un objet. Notons que cette information est fortement confidentielle et probablement concurrentielle. L'échange de ce genre de données exige donc un contrôle rigoureux dans le réseau EPCglobal. Dans [7], les auteurs présentent une solution pour sécuriser les interactions (traçabilité) entre les différents partenaires de la chaîne logistique. Cette solution repose sur la présence d'une entité tierce (broker) qui permet d'établir des relations de confiance entre les organisations en présence. Cependant, cette solution ne propose pas de mécanisme d'authentification entre l'étiquette et le lecteur, et elle ne résout pas les problèmes de confidentialité et de traçabilité.

4.1.1 Sécurité des WSANs

Dans cette section, nous introduisons plusieurs problèmes de sécurité liés à l'intégration des capteurs sans fil (WSAN) dans les systèmes de la gestion de la chaîne logistique (SCM). En raison de l'hétérogénéité des partenaires impliqués, dont les intérêts sont potentiellement différents, les SCM rencontrent des défis de sécurité spécifiques, qui sont généralement liée aux échanges d'informations avec le système de SCM. Dans cette section, nous identifions quelques-uns, nous discutons de la traçabilité sécurisée, évaluation dynamique du risque, et des performances de la chaîne logistique.

4.1.1.1 *Traçabilité sécurisée*

De nos jours, le suivi de la marchandise est une fonctionnalité obligatoire afin de vérifier le respect des réglementations, et la responsabilité des acteurs de la chaîne logistique en cas d'accident. WSN permet un suivi automatique des marchandises, grâce à ses capacités de surveillance. Toutefois, le suivi des marchandises peut conduire à des fuites des informations sensibles. Cette fuite met en danger l'avantage compétitif de chaque partenaire. Nous proposons d'adresser cette problématique, avec un mécanisme de traçabilité sécurisée de la marchandise. Plus précisément, ce mécanisme vise à valider d'une manière sécurisée le chemin parcouru par la marchandise en identifiant les différentes entités qui ont composés ce chemin. Ce mécanisme assure la protection de la vie privée, car un adversaire ne peut ni apprendre des détails sur un chemin, ni sur les partenaires de la chaîne. Il se base sur des techniques d'empreinte digitale [29][~~29~~], la confidentialité est assurée par un chiffrement homomorphique. Contrairement, aux travaux existants, ce mécanisme réduit la quantité de mémoire et de calculs utilisés par les capteurs.

4.1.1.2 *Evaluation dynamique de risque*

L'évaluation de risque dans la chaîne logistique est aborde généralement a la conception de cette dernière. Or durant l'exécution du processus logistique, il apparait difficile de maitriser l'évaluation du risque. Or, de part leur capacité à capturer leur environnement (ex, température,

présence de gaz, humidité de l'air, détecteur de fumée, position), les capteurs semblent être un très bon candidat pour une évaluation en temps réel du risque.

Notre approche consiste en effet à définir sur les capteurs un ensemble de conditions de rupture de chaîne logistique en fonction de critères d'évaluation de risques lies a l'environnement des produits. La rupture de chaîne de froid pour des produits pharmaceutique est ici un bon exemple. Avec un capteur de température, nous pouvons alors surveiller la température ambiante dans un camion transportant des médicaments, ou dans une zone de stockage. Cette information de température nous permet en temps réel d'évaluer le risque de rupture de la chaîne logistique, et de réagir le plus rapidement possible en cas d'incident.

En complément de cette approche, nous proposons d'aborder la problématique liée à la composition de risques inférés par les conditions environnementales.

4.1.1.3 *Evaluation sécurisée et de confiance de la performance de la chaîne logistique*

Parmi les indicateurs de performance, le taux de remplissage (par exemple, le pourcentage des marchandises livrées à temps), délai de réponse (par exemple, la durée entre le jour de livraison demandé et le jour négocié), actions (par exemple, le travail total en cours), le retard (par exemple, la durée entre le jour de la livraison réelle moins confirmés jour de livraison). L'évaluation générale de la performance de la chaîne logistique passe par une synthèse des indicateurs de performance sur la chaîne logistique.

Afin d'évaluer la performance globale de la chaîne logistique, la collecte de tous ces indicateurs est nécessaire. Deux raisons majeures peuvent dissuader la collecte de ces informations. Pour des raisons de confidentialité évidente, les acteurs impliqués dans le chaîne logistique serait refusent de fournir des indicateurs de performance. Une divulgation de ces informations sensibles liées au rendement d'un acteur à ses concurrents peut avoir un effet négatif sur son avantage compétitif. De plus, pour des raisons plutôt purement techniques, il semble très difficile de recueillir toutes les informations relatives aux indicateurs de performance tout au long de la chaîne logistique.

Les capteurs peuvent jouer un rôle très important en collectant ces indications de performances. Ils peuvent en premier lieu collecter tout au long de la chaîne logistique des informations liées à la performance. Basé sur ces indicateurs, les capteurs peuvent alors prendre un rôle plus actif dans l'optimisation de la chaîne logistique en temps réel.

L'évaluation de la performance soulève évidemment des problèmes de confidentialité des indicateurs de performance, mais également de confiance vis-à-vis des informations collectées. En effet la confiance de l'information fournie à WSAN doit être évaluée afin de filtrer les indicateurs falsifiés.

5. Conclusion

Dans cet article, nous avons présente les dernières activités du projet RESCUEIT. Nous avons démontré l'intérêt de l'intégration de réseaux de RFIDs et WSANs dans la chaîne logistique a travers un scénario élaboré en collaboration avec le site de stockage de Savigny le Temple de Kuehne + Nagel. Ce scénario se concentre sur le transport, manutention et stockage de matières dangereuses. Une modélisation de ce scénario nous permet de mettre en évidence un ensemble de risques.

De plus nous avons démontré de quelle manière, de part leur intégration, les objets intelligents (ex. RFIDs, capteurs) nous permettent d'atténuer les risques inhérents a la chaîne logistique. Cette intégration est bénéfique sous de nombreux aspects notamment quant au traçage des produits dangereux, l'identification de la responsabilité, atténuations des risques en temps réel, ou encore optimisation sécurisée de la chaîne logistique.

Nous prévoyons d'orienter nos activités de recherche dans les domaines cites en section 4, authentification mutuelle de RFIDs bas cout, et l'utilisation de capteurs pour la traçabilité, l'évaluation de risque dynamique ou encore de performance. Le résultat de ces activités de recherche donnera lieu à un premier prototype en collaboration entre les partenaires français fin 2011, puis un prototype franco-allemand pour mars 2013.

Références

[1] GS1/EPCglobal, ISO/IEC TR 24729-4:2009. *Information technology -- Radio frequency identification for item management -- Implementation guidelines -- Part 4: Tag data security*, 2009. http://www.epcglobalinc.org/home/

[2] M. Weiser. The computer for the 21st century. Scientific American, 265(3):94–104, September 1991.

[3] B. Alomair and R. Poovendran, Securing Low-cost RFID Systems: an Unconditionally Secure Approach. The 2010 RFID Security Workshop-RFIDsec'10 Asia, 2010.

[4] M.-H.-Y. Chien. Efficient time-bound hierarchical key assignment scheme. IEEE Transactions on Knowledge and Data Engineering, 16(10):1301–1304, 2004.

[5] M. J. Atallah, M. Blanton, and K. B. Frikken. Incorporating temporal capabilities in existing key management schemes. In ESORICS, pp. 515–530, 2007.

[6] A. Juels, P. Syverson, and D. Bailey. High-Power Proxies for Enhancing RFID Privacy and Utility. RSA Laboratories Bedford, MA 01730, USA.

[7] T. van Deursen , and S. Radomirovic. "Security of an RFID Protocol for Supply Chains". E-Business Engineering, 2008. ICEBE '08. 2008, pp. 568–573.

[8] A. Sorniotti, F. Kerschbaum. RFID-Based Supply Chain Partner Authentication and Key Agreement. Second ACM conference on Wireless network security, pp. 41-50, 2009.

[9] C.-Y. Chong and S. P. Kumar. “Sensor Networks : evolution, opportunities, and challenges”.Proceedings of the IEEE, 91(8) :1247_1256, 2003.

[10] A. Bernatik et M. Libisova. Loss prevention in heavy industry: risk assessment of large gasholders. Journal of Loss Prevention in the Process Industries., 17(4):271–278, 2004.

[11] V. Cozzani, S. Bonvicini, G. Spadoni, et Zanelli S. Hazardous transport: A methodological framework for the risk analysis of marshalling yards. Journal of Hazardous Materials., 147(2):412–423, 2007.

[12] Tno, guidelines for quantitative risk assessment, purple book., 1999.

[13] BPMN, http://bpmn.org

[14] WASP Project, http://www.wasp-project.org/

[15] L. Gomez, C. Ulmer, “Secure Sensor Network for Critical Infrastructure Protection”, in the proceedings of SensorComm’10, 2010.

[16] PROMISE Project, http://www.promise-plm.com

[17] J. Anke, B. Wolf, G. Hackenbroich, H.-H. Do, M. Neugebauer, A. Klein: PROMISE: Product Lifecycle Management and Information Tracking using Smart Embedded Systems. In: Ubiquitous Computing Technology for Real Time Enterprises, Max Mühlhäuser, Iryna Gurevych (Editors), Idea Group, Hershey, USA, 2007.

[18] CoBIs: Collaborative Business Items, Project Website, http://www.cobis-online.de/

[19] SAP AG, SAP Auto-ID Infrastructure, http://www.sap.com/platform/netweaver/autoidinfrastructure.epx

[20] J. Anke , J. Müller, P. Spieß, L. Weiss and F. Chaves, “A Service-Oriented Middleware for Integration and Management of Heterogeneous Smart Items Environments”, Proceedings of the 4th MiNEMA workshop in Sintra. 2006

[21]C. Bornhoevd, T. Lin, S. Haller and J. Schaper, Integrating Smart Items with Business Processes An Experience Report, Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences. 2005

[22] Web Service, http://www.w3.org/2002/ws/

[23] T. Roy, “Fielding, Architectural Styles and the Design of Network-based Software Architectures”, PhD dissertation, University of California, 200.

[24]Identity-Based Key Agreement and Encryption For Wireless Sensor Networks. Geng Yang, Chunming Rong, Christian Veigner, Jiangtao Wang, and Hongbing Cheng. 5B, May 2006, IJCSNS International Journal of Computer 182 Science and Network Security, Vol. 6.

[25]Efficient fine-grained data access control in wireless sensor networks. Wang, Qian, et al. 2009. Military Communications Conference, 2009. MILCOM 2009. IEEE . pp. 1-7.

[26]Schwarz, Mikhail J. Atallah and Vinayak Deshpande and E Keith B. Frikken and Leroy B. Secure Supply-Chain Collaboration. 2004.

[27]Wireless sensor networks: a survey. I. F. Akyilidiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. 2002, Computer Networks, pp. 393-422.

[28]Temporal Accountability and Anonymity in Medical Sensor Networks. Liu, Jing and Xiao, Yang. s.l. : Springer Netherlands, 2010, Mobile Networks and Applications.

[29]Anti-collusion fingerprinting for multimedia. Trappe, W., et al. 2003. s.l. : ieee, 2003. Signal Processing, IEEE Transactions on. pp. 1069-1087.

[30]IBM. IBM - Distribution supply chain and logistics solutions for sensors and actuators. www-01.ibm.com. [Online] http://www-01.ibm.com/software/solutions/sensors/distribution/.

[31]Army logistician. Enhanced Logistics Tracking and Monitoring Through Sensor Technology. [Online] http://www.almc.army.mil/alog/issues/JulAug08/enhancelog_w_sensortech.html.