d'implémenter de nouveaux mécanismes de gestion de la demande.
La thèse de doctorat de José Horta expose que l'Internet des Objets permettra la mise en place de nouvelles applications avancées pour le contrôle de la production, le stockage et la consommation d'énergie, à la fois dans des contextes résidentiels et professionnels. Cependant, la conception de tels systèmes doit faire face à plusieurs contraintes en termes d'interopérabilité, adaptabilité à l'échelle, fiabilité, sécurité et coûts d'investissements et de maintenance.
Changer le profil de consommation de l'électricité de l'usager, pour répondre aux besoins du réseau de distribution, est l'une des principales solutions pour maintenir l'équilibre entre la production et la consommation de l'énergie électrique. La réponse à la demande (Demand Response, DR) désigne de manière générale tous les moyens mis en place pour changer le profil de consommation électrique de l'usager. Deux catégories de mécanismes d'ajustement de la demande sont envisageables, à savoir des mécanismes incitatifs (ex. signal de prix) et des mécanismes intrusifs (ex. contrôle direct de la demande). C'est l'objet de la thèse de doctorat de Rim Kaddah.

Différents scénarios et endroits pour le rechargement

Optimisation locale et mobilité électrique

Le nombre de véhicule électrique (VE) devrait continuer à croître dans les prochaines années, entraînant ainsi une forte augmentation des points et stations de recharge. Par ailleurs, l'Internet des Objets va transformer l'habitation en Smart Home disposant de services communicants dont certains prendront en charge le VE.

À partir d'un certain seuil, le fort appel en puissance pourra localement augmenter les pics de consommation et avoir ainsi un impact significatif sur les réseaux de production et de distribution électriques. Le développement des véhicules électriques ne pourra se faire sans une gestion adaptée de sa recharge.
Il sera donc opportun de disposer de communications radios entre les VE en recherche de bornes de recharge publiques ou privées. Concernant ce dernier type de bornes, un travail en commun avec le département MIRE d'EDF R&D permet de développer un simulateur d'approche de véhicule en WIFI sur un site multi-bornes.
Le gestionnaire d'énergie conçu dans le cadre de cette thématique est réalisé sous forme de simulateur logiciel développé sous Matlab. Ce simulateur est illustré par des scénarios de la Smart Home élaborés à partir du simulateur SMACH.
Le procédé permet d'optimiser la consommation électrique d'une Smart Home (Smart Building, Smart Factory). Il a été illustré au travers du stage de Lionel Capo-Chichi qui a réalisé, dans le cadre d'une maison type, une dizaine d'usages de consommation électrique et le choix des courbes de charge, un type de VE avec sa courbe de charge spécifique, des familles type, pour prévoir un simulateur étendu au quartier disposant de variabilité au niveau des occupants et de leurs consommations électriques.
L'objectif du stage de Nassim Baakel est de mettre en œuvre un dispositif matériel pour simuler l'approche d'un VE et l'affectation d'une borne de recharge sur un site multi-bornes via une communication radio en s'appuyant sur la norme ISO/IEC 15118 : spécification des messages échangés entre le VE et le gestionnaire d'énergie du site, implémentation du protocole de communication préconisé, mise en œuvre de la plateforme de test. ■

Bilan du Seido Lab

CONSTITUER UN PÔLE DE COMPÉTENCES DE RÉFÉRENCE
Le activités de SEIDO ont un début de reconnaissance au niveau international (à travers la publication d'articles de conférences et de revues internationales dont deux revues ayant un facteur d'impact (IF) de 3.45 et 2.4) et une reconnaissance au niveau national.
Cette reconnaissance a permis de nouer des contacts avec des partenaires externes, notamment Airbus DS dans le cadre de la Chaire cyber sécurité des systèmes de contrôle industriel et du dépôt du projet H2020 SPICE.
Par ailleurs, la revue « Génie Logicielle » a émis une sollicitation de publication d'un numéro spécial consacré aux résultats de SEIDO.

➜ S'inscrire dans un système de subvention
Le résultat est partiel toutefois plusieurs projets subventionnés ont été déposés (H2020 SPICE, PIVOINE FUI21, FUI22).

↗ Constitution d'une filière de formation
Une formation IdO destinée aux ingénieurs du corps des mines a été mise en place en 2015-2016. Elle sera proposé en 2016-2017 conjointement avec HEC. De plus, une gamme de formation continué dédiée au domaine IdO a été mise en place en 2016 à l'Institut Mines-Télécom.

↗ Concevoir une architecture de référence
Bien que la thèse de José Horta ait pris du retard, elle représente un travail de référence solide qui laisse présager des résultats de propriété industrielle.

↗ Modèle cyber sécurité
Les résultats obtenus proposent des approches innovantes prometteuses.

↗ Propriété intellectuelle
Le dépôt d'un brevet a été réalisé en commun sur un procédé de gestionnaire d'énergie évolué associant trois inventeurs, un TPT et deux EDF Lab des départements MIRE et ICAME.

seido LAB est une publication du **Laboratoire Seido**. 7, boulevard Gaspard Monge - 91120 Palaiseau. Site internet : **www.seidolab.fr**. Directeur de la publication : **Ange Caruso.** Ont participé à ce numéro : **les membres du comité exécutif SEIDO**. Conception et réalisation : **Particule**.
Crédit photographique **© Philippe Forestier**.

Activités 2012-2016

mercredi 1er juin 2016

www.seidolab.fr

Directoire SEIDO Lab / Cyber sécurité / Internet Des Objets

« En ouvrant la voie à des services de plus en plus innovants, l'Internet des Objets marque pour la plupart des observateurs une nouvelle révolution industrielle. Estimé à 500 millions il y a dix ans, le nombre de périphériques connectés à Internet s'élève aujourd'hui à 11 millions environ et atteindra les 26 milliards d'ici 2020 d'après la société d'analyse Gartner, voire 50 milliards selon l'estimation de Cisco.
Si le développement de l'IdO ne fait plus de doute pour les analystes, il n'en va pas de même pour sa sécurisation. Dans une étude publiée le 25 avril dernier, Gartner prédit que plus de 25% des attaques identifiées à l'horizon 2020, impliquera l'IdO alors que la sécurité de l'IdO pèsera mois de 10% des budgets de la sécurité informatique. Selon cette étude, la sécurité de l'IdO représentera un marché de 348 millions $ en 2016, soit une hausse de 23,7% par rapport à 2015, une tendance qui se poursuivrait en 2017 et 2018. Une croissance modérée qui s'accélérait après 2020, toujours d'après l'étude de Gartner.
Cela conforte dans leur vision Télécom ParisTech et EDF Lab, qui ont mis en place en 2012 un laboratoire commun consacré à des travaux de recherche portant sur l'IdO associé à la cyber sécurité. L'enjeu pour EDF est de préparer et faciliter le déploiement de services de gestion de la demande et d'efficacité énergétique s'appuyant sur l'interopérabilité d'objets consommateurs d'énergie, mais aussi d'assurer la cohérence de l'ensemble du système et sa sûreté (sécurité, confidentialité, etc.).
Avec la création du SEIDO Lab, Télécom ParisTech et EDF se donnent comme ambitions de :

- Constituer un pôle de compétences dans le domaine de l'IdO, appliqué aux domaines énergétiques et les problématiques de sécurité informatique des systèmes électriques, faisant référence aux niveaux national et international ;
- Concourir à l'obtention de nouveaux concepts, de nouveaux standards, et à la définition de nouveaux équipements, de nouveaux logiciels et de développer ainsi un patrimoine de propriété commun ;
- Promouvoir en France la constitution d'une filière de formation et d'expertise dans ce domaine, d'ingénieurs et de doctorants de haut niveau ;

S'inscrire dans les financements publics de la recherche en France et en Europe. ■

- Publication dans deux revenues internationales dont l'IF est de 3.45 et 2.4
- Création de la formation PESTO à Télécom ParisTech, destinée aux ingénieurs du corps des mines
- Création en 2016 d'une gamme de formation continue dédiée au domaine de l'Internet des Objets à l'Institut Mines-Télécom
- Dépôt conjoint d'un premier brevet de PI fin 2015

ACTIONS TRANSVERSES

La mise en place du Laboratoire a consisté dans un premier temps à décliner les décisions de la convention de partenariat : création des directoires et des comités exécutifs du Laboratoire, puis la mise en place des moyens de communication au sein des équipes mixtes TPT et EDF Lab.

Elle s'est poursuivi par le recrutement des premiers stagiaires qui, pour certains, devinrent des doctorants, puis la mise en place de réunions de partage d'expertises réciproques, d'une part, concernant la commercialisation et la distribution d'énergie électrique et ses différents usages, et, d'autre part, sur les technologies de télécommunication dont celles de l'idO. Ces échanges induisirent notamment l'inscription en commun à une formation de plusieurs jours des personnels TPT, doctorants et encadrants, à un stage interne EDF sur le marché de l'électricité qui fut complété par l'organisation de la visite d'un poste source de transformation haute tension classe B (réseau HT RTE) en haute tension classe A (Réseau HT ERDF) et la visite d'un poste publique de transformation haute tension classe A en basse tension.
Ce fut également, lors de la première année pleine, l'organisation de réunions *ad hoc* pour définir des cas d'utilisation Smart Home pour partager potentiellement ceux-ci dans les différents axes des deux domaines du Laboratoire.

Ce fut au fil du fonctionnement du Laboratoire l'organisation une fois par an d'un Workshop ouvert en partie à des contacts externes aux entités des partenaires pour communiquer sur les résultats du Laboratoire, soit trois à ce jour. Ce type d'action de communication a été complété par la réalisation d'une plaquette, d'une maquette de communication interne semestrielle (SEIDO LabNews) et d'une maquette de site web hébergé en dehors des SI des partenaires pour permettre des publications tel que cela était mentionné dans la convention du Laboratoire. Ce site permet également de faciliter la gestion des Workshops.

Ce fut enfin l'animation au quotidien de la coordination de fonctionnement du Laboratoire, gestion des prévisions d'activité et de budget, gestion des achats, notamment des transferts entre EDF et TPT, gestion des habilitations aux moyens communications, animation des réunions *ad hoc* sur des problématiques transverses, et gestion en générale de toute affaire courante (RH stage et thèse, etc). ■

Identifier des scénarios reposant sur des interactions sécurité/sûreté

Le travail sur l'axe Sûreté et Sécurité a donné lieu à un premier résultat concernant une proposition de profil UML permettant de raisonner sur l'identification de scénarios d'attaques ou de défaillances reposant sur des interactions entre mécanismes de sécurité et sûreté de fonctionnement. Ce travail a été poursuivi par deux réflexions : un travail de raffinement du profil offrant deux moyens de description des objectifs de sûreté aux ingénieurs ; une réflexion de fond sur l'arbitrage des conflits sûreté sécurité.

En particulier cette démarche a mis l'accent sur la possibilité de définir la notion de protection fournie qui permet de relier une fonction de sécurité, une propriété de sécurité et un bien support ou essentiel. Ce type d'information nous a semblé essentiel pour raisonner sur les incompatibilités entre mécanismes de sûreté et sécurité.

Le travail de stage de Sarah Nait, *Gestion des interactions entre la sécurité et l'ingénierie de la fiabilité*, s'est attaché à produire un état de l'art concernant les méthodes de description d'exigences de sécurité et sûreté mais aussi sur les moyens disponibles pour décrire les mécanismes garantissant ces propriétés. Suite à ce travail, un problème clé est apparu : de nombreux conflits entre sûreté et sécurité interviennent entre des exigences correspondant à des étapes différentes du processus de conception. Par exemple, l'exemple ultra classique du contrôle d'accès au bâtiment démontrant un conflit entre politique de sécurité et politique de sûreté est en fait un faux problème car le seul problème vient de la mise en œuvre du contrôle d'accès qui pourrait être réalisé sans avoir à modifier les exigences de haut niveau. Nous avons proposé un cadre de raisonnement pour identifier ces situations et si possible guider l'ingénieur vers une résolution du problème ou *a minima* indiquer la nature précise du conflit.

Les travaux menés jusqu'en 2016 sur la problématique ISS portent essentiellement sur l'amont de la conception de systèmes industriels, en se basant sur la formalisation des exigences de sûreté et de sécurité afin de détecter au plus tôt leurs interactions. Cet aspect théorique a été développé pendant le stage réalisé par Sofiane Heddar visant à appliquer une approche orientée modèle sur des exemples simples mais représentatifs de quelques contraintes de sécurité. L'application de concepts théoriques issus de l'ingénierie dirigée par les modèles sur des exemples industriels reste la cible des futurs travaux ISS.

Une étude a été aussi entamée visant à clarifier les concepts utilisés lors d'études de sûreté et de sécurité. Nous pensons qu'une des raisons de conflits entre sûreté et sécurité provient d'un manque de compréhension mutuelle des exigences et des procédures du cycle de vie issues du monde de la sûreté.

Ainsi, la perspective majeure consiste à combiner et intégrer les travaux réalisés par Sarah Nait et Sofiane Heddar, en clarifiant les concepts dans un premier temps, puis en proposant une démarche orientée cas d'application dans le monde industriel. Plus généralement, il serait intéressant de voir comment cette approche pourrait être appliquée au cas concret de l'interaction entre un processus de maintenance informatique ou électronique du système, et une politique de sécurité de type contrôle d'accès et flux.

Défense optimale des systèmes embarqués

Les infrastructures industrielles s'appuient sur des composants numériques d'une grande diversité. Parmi eux, bon nombre sont des systèmes propriétaires et/ou figés mais dont la protection doit être assurée malgré tout. Il faut donc intégrer des mécanismes de sécurité dans un contexte technique très contraint, en limitant l'impact sur ces systèmes. Les approches classiques de la sécurité sont au mieux peu adaptées, sinon inopérantes.

Les travaux réalisés sur cette thématique ont pour objectif de fournir des méthodes et des outils d'aide à la décision permettant d'identifier les stratégies de défenses les mieux adaptées au contexte des Smart Grids, aussi bien lors de la phase de la définition de la politique de sécurité que lors de la réponse à des incidents. Les défis sous-jacents sont les suivants :

- la prise en compte des interactions entre attaquants et système de défense ;
- la recherche d'un compromis entre le niveau de sécurité du système et les autres contraintes non fonctionnelles ;
- la possibilité de comparer les impacts respectifs sur le niveau de sécurité du système de deux stratégies de sécurité distinctes.

Les travaux sur cette thématique ont été réalisés dans le cadre de la thèse de doctorat de Ziad Ismaïl, co-encadré par Jean Leneutre, David Bateman et Alia Fourati.

Les principales contributions sont les suivantes :

- la proposition d'une stratégie de configuration optimale des mécanismes de chiffrement des communications entre les équipements d'une infrastructure AMI (Advanced Metering Infrastructure) ;
- la proposition d'un modèle analytique pour l'étude de la propagation des risques de sécurité de l'infrastructure ICT (Information and Communication Technology) vers le réseau électrique ;
- la définition d'un modèle et prototypage d'outils pour la génération de politiques de sécurité optimales dans les systèmes de contrôles industriels.

Les doctorants, de gauche à droite, Rim Kaddah, José Horta et Rayhana Baghli avec Bruno Traverson, encadrant industriel de Rayhana

Ziad Ismaïl en plein exposé durant Workshop 2014

Les méthodes et outils obtenus dans la dernière contribution peuvent être utilisés comme aide à la décision soit pour fixer des priorités sur le déploiement de nouvelles mesures de sécurité, soit pour répondre à des intrusions de manière efficace.

Les résultats obtenus dans cette thèse proposent des approches innovantes de défense se basant sur une modélisation via la théorie des jeux. Néanmoins, ces résultats ne peuvent être utilisés dans l'immédiat dans un contexte industriel ; des travaux complémentaires sont nécessaires pour adapter ces résultats au contexte opérationnel.

Sécurité des réseaux de capteurs

Les principales contributions dans cette thématique consistent en une analyse de risques menée avec la méthode EBIOS d'une architecture idO se basant sur 5 cas d'utilisation définis par le COSEI ; les résultats de cette analyse de risques se résument en :

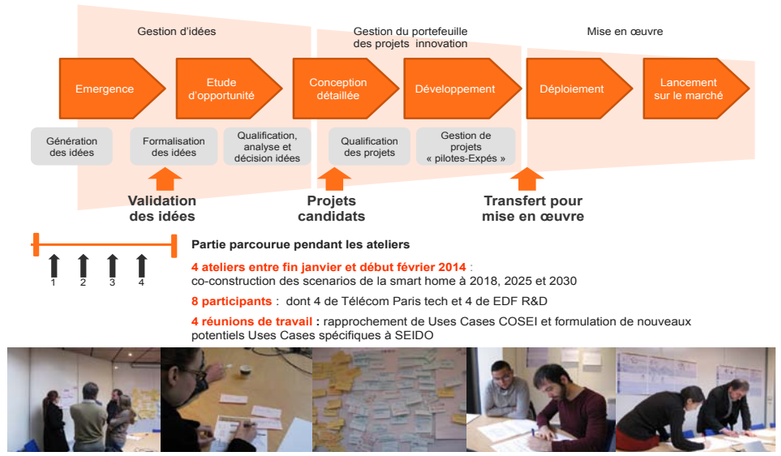
- étude des évènements redoutés ;
- étude des scénarios de menaces ;
- étude des risques de sécurité ;
- identification des objectifs de sécurité et identification des risques résiduels ;
- proposition de mesures de sécurité selon une approche de défense en profondeur.

Cette étude a été menée dans la cadre du stage de Hussein Samhat en se basant sur l'architecture étudiée dans la thèse de José Horta, ainsi que les use case du COSEI. La pertinence des résultats de l'étude est donc inhérente à cette architecture. D'autre part, les mesures de sécurité proposées sont génériques et les mécanismes de sécurité appropriés à mettre en place doivent être spécifiés et déclinés au regard de l'architecture. ■

Collecte des données et gestion des flux

Dans le cadre de la maison connectée, les démarches actuelles de composition de services sur le web doivent être adaptées car elles reposent essentiellement sur la connaissance préalable des services qui seront manipulés lors de la composition. Nous visons, dans le cadre de cette thématique, à rendre dynamique le processus de composition des services offerts par les objets connectés de la maison. Nous proposons une architecture qui adapte, de manière dynamique, les règles de composition en fonction des services disponibles et accessibles à un moment donné. L'architecture conçue dans le cadre de cette thématique sera réalisée sous forme d'un prototype logiciel et illustrée par des scénarios d'utilisation de la maison connectée qui ont été élaborés par le groupe de travail transverse « use cases » du Laboratoire SEIDO. Dans le cadre de la thèse de doctorat de Rayhana Baghli, elle propose une démarche qui vise à rendre dynamique le processus de composition de services. Nous définissons une stratégie qui, adapte de manière dynamique, les règles de composition en fonction des services disponibles et accessibles à un moment donné.

Dans le cadre de la composition de services liés et appliqués à la Smart Home, stage M2 de Meriam Charfi, REST (REpresentation State Transfer) est un style d'architecture qui reprend les principes fondamentaux du web en respectant quatre contraintes : identification universelle des ressources, interface uniforme, navigation par liens hypertextes et interactions sans état. Les Linked Data, ou données liées, visent à créer un web des données. Ces données sont disponibles dans un format standard, accessible et gérable par les humains et par les outils du Web sémantique (RDF). La combinaison de services Restful – conformes à l'architecture REST – et des données liées – les Linked Services – permet d'envisager la composition de services basée sur les informations relatives aux ressources et au modèle d'interaction avec ces ressources.



Processus proposé

L'objet du Stage M2 de Rayhana Baghli, est l'approche de modélisation dirigée par les faits connaît un regain d'intérêt actuellement comme le montre la publication récente de standards tels que ORM 2 (Object-Role Modeling version 2). Son utilisation pour modéliser les règles métier dans les systèmes d'information est notamment illustrée par le standard SBVR (Semantics of Business Vocabulary and Business Rules). L'intérêt de cette approche est qu'elle permet des descriptions de façon quasiment naturelle ce qui les rend accessibles aux experts non informaticiens (principe de verbalisation). De plus, ces descriptions peuvent être traduites sous forme de spécifications formelles ce qui en permet la validation.

Architecture de bout en bout

Nouveau paradigme, le consommateur devient un acteur de la grille, impliqué dans la production, le stockage, l'effacement et l'échange d'énergie. Ce changement dans le modèle économique entraîne le développement d'algorithmes avancés de contrôle, de stratégies de gestion et d'une architecture de communication nécessaires pour mettre en place ces services de gestion de l'énergie.

Nous proposons dans cet axe une architecture générale pour les services énergétiques de la Smart Home, basée sur l'Internet des Objets. Notre architecture hiérarchique repose sur le concept de la virtualisation des réseaux de distribution de l'électricité ; elle permettrait d'implémenter un marché d'échange d'énergie entre Smart Homes dans le but d'équilibrer la production locale et la demande, mais aussi