CeSi

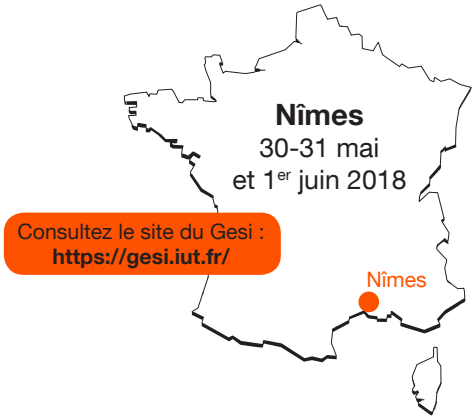
N°92 // DÉCEMBRE 2018 // 37e ANNÉE

Actes du colloque de Nîmes

NÎMES - Maison carrée

REVUE DES DÉPARTEMENTS DE GÉNIE ÉLECTRIQUE & INFORMATIQUE INDUSTRIELLE

édito



Pour tout savoir sur l'histoire de GeSi, consulter le site :
https://gesi.iut.fr/

Merci à l'équipe de Brive pour ce beau travail.

Chers amis, chers collègues,

Toute l'équipe d'organisation du colloque Nîmois vous présente ses meilleurs voeux pour cette année 2019.

Alors oui, je vous confirme aujourd'hui que l'organisation d'un tel colloque n'est pas une mince affaire ! Mais lorsque les retours sont positifs comme ils l'ont été, toute cette fatigue s'envole. J'espère que vous avez tous pu profiter de notre ville et surtout de nos trois commissions. Ce colloque fut très orienté industrie, à tel point qu'il y avait des industriels pendant les plénières et dans toutes les commissions. Cette décision a beaucoup plu à ces derniers qui ne demandent qu'à participer à cet événement afin de nous montrer ce qu'il se passe dans l'industrie.

*Je dois remercier pour cela les organisateurs de ces commissions : je pense à **Jean-Pierre Lenormand**, **Thierry Glaisner** et **David Glay** pour l'industrie du futur. Cette commission aurait pu durer 4 jours tant le nombre de participants augmentait à l'approche du colloque. Quel bonheur de travailler avec ces trois-là ! **Laurent Laval** et son énergie débordante, **Florent Bruguier** et **Joël Durand** (même les Nîmois étaient mis à contribution) pour la commission cybersécurité. **Marouane Alma** et **Alain Tinel**, qui ont dû contenir quelques conférenciers un peu long... pour la commission énergie et efficacité énergétique. Merci bien sûr **à vous tous** d'être venus voir le soleil qui est finalement apparu le dernier jour. Merci pour votre bonne humeur, ces moments de convivialité et cette belle ambiance.*

*Merci enfin **à toute l'équipe organisatrice, personnels du département et personnels de l'IUT** qui ont travaillé d'arrache pied pour la réussite de ce moment important pour les départements GEII.*

*C'est donc tout à fait détendu et serein que je passe le relais (l'enclume) à mon ami **Marouane Alma et l'IUT de Longwy**. Quel bonheur d'aller participer à un colloque organisé ailleurs !*

Le département GEII de Longwy est déjà très investi dans l'organisation et je ne doute pas qu'ils nous offriront à tous un très beau et très intéressant Colloque.

Nîmes 2018, 45e colloque pédagogique national a bien vécu vive Longwy 2019.

Patrick Effantin et toute l'équipe organisatrice du département GEII de Nîmes

GeSi

Revue des départements Génie Électrique & Informatique Industrielle des Instituts Universitaires de Technologie
Directeur de la publication : Philippe Lavallée - Responsable du comité de rédaction : Gino Gramaccia - gino.gramaccia@u-bordeaux.fr
Comptabilité : Monique Thomas
Comité de rédaction : Christian Pécoste - IUT Bordeaux, Florence Hénon IUT de Chartres
Impression : Imprimerie Laplante - 3, impasse Jules Hetzel - 33700 Mérignac - Téléphone : 05 56 97 15 05 - e-mail : pao@laplante.fr
Crédit photos : GettyImages - Dépôt légal : Décembre 2018 - ISSN : 1156-0681

sommaire

• **Édito de Patrick EFFANTIN** p 2

ACTES DU COLLOQUE DE NÎMES

• **Commission 1 : Cyber-sécurité** p 4
Laurent LAVAL *(IUT de Villetaneuse)*

• **Commission 2 : Énergie et efficacité énergétique** p 8
Marouane ALMA *(IUT de Longwy)* **/** ***Alain TINEL*** *(IUT du Havre)*

• **Commission 3 : Systèmes technologiques de l'Industrie du Futur** p 12
Thierry GLAISNER *(IUT de Ville d'Avray)* **/** ***David GLAY*** *(IUT de Lille)*
Jean-Pierre LE NORMAND *(IUT de Haguenau)*

• **Retour en images sur le Colloque de Nîmes** p 16

SCIENCES & TECHNOLOGIES

• **CyberEdu à la Commission 1 Cybersécurité** p 17
Philippe WERLE *(Vice-Président Outils de CyberEdu et Responsable du Management de la Sécurité des Systèmes d'Information de l'Université de Bordeaux)*

• **Localisation et identification de ressources industrielles par l'Internet des objets** p 19
Eddy BAJIC *(IUT Nancy Brabois)*

HORIZON SCIENCES HUMAINES

• **Le DUT GEII par apprentissage à l'IUT de Nancy-Brabois** p 28
Franck Joly *(IUT Nancy-Brabois)*

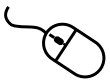
• **Projets tuteurés : une opportunité pour tisser du lien socio-économique** p 31
Taha BOUKHOBZA *(IUT Nancy-Brabois, Université de Lorraine)*
Denis CRONEL *(Centre interarmées de la solde, Défense Nationale)*
Cédric JOIN *(IUT Nancy-Brabois, Université de Lorraine)*
Christophe SIMON *(IUT Nancy-Brabois, Université de Lorraine)*

ERRATUM

Page 4 du GeSi n°91, il fallait lire : Autour du colloque de Nîmes, et non Actes du colloque du Calais. Toutes nos excuses.

ACTES DU COLLOQUE DE NÎMES

Commission 1 Cybersécurité



Laurent LAVAL *(IUT de Villetaneuse)*

Préambule

Dans un passé encore récent, pour une grande partie de la population, les attaques des systèmes informatiques et de communication étaient généralement assimilées à des épiphénomènes sporadiques et aux impacts essentiellement limités à la corruption de données (effacement, altération), leur divulgation non consentie, des pertes d'accès à des services ou à des fonctionnalités (logicielles ou matérielles) et surtout du temps passé à opérer une maintenance curative des systèmes attaqués (incluant la récupération de données). Ces attaques apparaissaient souvent comme l'œuvre de *script-kiddies* en quête d'expériences transgressives ou de *hackers* isolés à la recherche d'exploits pour exhiber leurs compétences aux yeux de microcosmes d'initiés (*Black Hats, Grey Hats*…). Les principales motivations alors recensées étaient le challenge individuel (satisfaction personnelle ou comparaison avec autrui), le besoin de reconnaissance ou de notoriété (même dissimulée derrière un pseudonyme), l'envie de transgresser les interdits, etc. Dans tous ces contextes, les échelles de valeurs étaient essentiellement : le niveau de technicité déployé pour découvrir ou exploiter une faille de sécurité, ou encore la capacité de nuisance (qu'elle soit potentielle et non totalement mise en œuvre comme chez les *Grey Hats* / *White Hats* ou effective et exercée comme chez les *Black Hats*). Dans ce proche passé, la dimension économique des actes de malveillance paraissait également circonscrite aux actions des *phreakers* (désireux d'exploiter les réseaux téléphoniques sans payer), à des opérations ciblées à l'encontre de certaines entreprises (blocage temporaire du fonctionnement, détournement d'informations...), en passant par l'utilisation frauduleuse et/ou illicite de matériels personnels (cartes bleues, ressources des ordinateurs...). Or, suite à la multiplication d'évènements relatés dans les médias (Affaire « Stuxnet », piratage du téléphone et du PC de la Chancelière allemande, piratage de comptes Instagram de personnalités, prise de contrôle à distance de calculateurs de voitures...), la perception de la *cybercriminalité*[1] semble avoir évolué. Les périmètres des activités malveillantes et/ou frauduleuses à base d'outils informatiques apparaissent désormais, aux yeux du grand public, sans limites en termes de cibles matérielles (de l'ordinateur aux objets connectés, en passant par des automatismes de production et les systèmes embarqués) et, plus inquiétant encore, en termes de cibles humaines (de l'individu lambda jusqu'au dirigeant d'un pays, en passant par des groupes de population). De récentes études, également diffusées à grande échelle par les médias, ont également contribué à sensibiliser la population à la très forte augmentation de ces activités malveillantes - en quelques chiffres : onze fois plus de logiciels malveillants (*vers, virus, malware...*) circulaient en 2017 sur internet qu'en 2016, 57 % des entreprises ont déclaré avoir été victimes d'une cyberattaque en 2016 contre 32 % en 2015, CISCO évoque une augmentation de 268 %, depuis novembre 2016, du trafic d'éléments malveillants via des communications chiffrées (elles-mêmes en augmentation), +83 % de smartphones infectés au 2ème semestre 2016 par rapport au 1er semestre (source : Nokia), etc. Enfin, les médias (incluant les sites d'informations spécialisés ou non) ont également mis en évidence l'existence de forces de frappe considérables[2], déployées par des groupes de cybercriminels organisés, de plus en plus nombreux et aptes à mener des (cyber)attaques complexes et/ou de grandes ampleurs.

Le plus inquiétant est toutefois de constater que la principale motivation des pirates informatiques est devenue économique en orientant leurs activités malveillantes vers la récupération illicite de données personnelles valorisables et surtout des extorsions de fonds à partir de *ransomwares* (rançongiciels en Français) ou de mails d'intimidation. En quelques chiffres : les *ransomware* ont enregistré une augmentation de 36 % entre 2016 et 2017 et l'entreprise Symantec, spécialisée dans les antivirus et la sécurité informatique, annonçait avoir bloqué près de 320 000 ransomware au premier semestre 2017 (source : *FIGARO*, 5 septembre 2017).

Même si les institutions et les entreprises demeurent des cibles importantes (En France, 80 % des PME ont été victimes de cyberattaques : du *ransomware* (61 %) au *déni de service* (38 %) en passant par la défiguration de site web (23 %) ou encore le vol de données personnelles (18 %)), l'attention des cybercriminels, motivés par les enjeux économiques, se concentre de plus en plus sur des cibles à la fois plus nombreuses, accessibles et vulnérables que sont les individus lambda. Tout ceci repose

1 Cf. https://www.kaspersky.fr/resource-center/threats/cybercrime
2 au sens de la capacité à mettre à mal la sécurité d'un système informatique ou d'un réseau.

naturellement sur l'essor des systèmes informatisés en tous genres (ordinateurs, téléphones, tablettes, calculateurs, systèmes embarqués...) et de leur connectivité. Nous sommes ainsi passés, en très peu de temps et sans réel accompagnement de la population, du concept de l'informatique pour tout le monde à l'*informatique ubiquitaire* / *omniprésente* / *pervasive* : « Accès à l'information pour tout le monde, n'importe où et n'importe quand ». Il est alors aisé de comprendre que la multiplication des systèmes connectés et notre méconnaissance individuelle de leur technologie accroissent notre vulnérabilité. S'il est possible de déployer des solutions techniques pour se protéger plus ou moins efficacement, la principale faille de sécurité reste l'individu en lui-même par sa méconnaissance des risques (actions qui le mettent en danger) et des procédures pour les limiter. L'objectif de cette commission était ainsi de sensibiliser les participants, de manière accessible à tous, aux problèmes et enjeux liés à la sécurité informatique au sens large. Dans ce cadre, des intervenants industriels des entreprises CISCO et Schneider Electric ont apporté leur connaissance et leur vision de la problématique de sécurité dans les réseaux de communication et les systèmes automatisés. Ces interventions ont été complétées par un ensemble d'exposés et de démonstrations visant, à travers un subtil équilibre entre vulgarisation technique et technicité, à balayer un spectre étendu d'attaques, de vulnérabilités et de cibles : du logiciel à l'être humain en passant par le matériel jusqu'aux composants électroniques. Les sections suivantes tentent de résumer ces différentes interventions.

Principales vulnérabilités et principales techniques d'attaques (logicielles)

Intervenant : Yassin EL HILLALI - IUT de Valenciennes

Après un recensement des principales motivations des auteurs d'attaques (challenge, jeu, transgression des interdits...), de leurs conséquences techniques (fuite de données, augmentation de privilèges, vandalisme...) et économiques (perte de revenu, frais de maintenance préventive et curative...), cet exposé a présenté quelques exemples concrets de procédures d'attaques : du classique Deny of Service (DoS) susceptible de bloquer le fonctionnement de serveurs, à l'injection de code aboutissant à une intrusion dans un système informatique. Cet exposé a notamment permis de mettre en évidence qu'une simple instruction comme une requête à destination d'un logiciel de gestion de bases de données, quelques lignes de programmation comme celles nécessaires à la création d'un logiciel malveillant (*keylogger, Trojan Horses...*) ou encore un *rootkit* peuvent suffire à perpétrer des intrusions au sein d'applicatifs de notre quotidien (site web), à récupérer/étendre des droits d'accès, à la récupération illicite de données (bases de données) ou à leur modification (perte *d'intégrité*) jusqu'à la prise de contrôle de systèmes (*compromission*). Certes, comme évoqué dans les échanges autour de cet exposé, il existe des solutions techniques permettant de lutter contre ce type de failles : application des mises à jour de sécurité des logiciels, inhibition du démarrage/boot de l'ordinateur à partir d'une clé USB, mise en place de *pare-feu*, fermeture des ports de communication, etc. Néanmoins, comme souligné dans l'exposé et les débats, l'être humain demeure le principal vecteur de *vulnérabilité*. Cette vulnérabilité découle essentiellement de la méconnaissance des risques et des mesures de protection, mais aussi des caractéristiques psychologiques de l'individu cible (crédulité, insouciance, appât de la gratuité et même son aptitude à être apeuré) qui sont largement exploitées par les cybercriminels par du *phishing, du téléchargement gratuit piégé* ou autres. De fait, le développement et l'efficacité de la sécurité informatique impliquent nécessairement une éducation des utilisateurs et des concepteurs à grande échelle, tant pour l'acquisition de connaissances sur les risques que pour l'adoption de bonnes pratiques (mise en place de protections) / bons réflexes face aux attaques.

Les certificats (définition, rôle, utilité, mise en œuvre …)

Intervenant : Philippe WERLE - Vice-Président Outils CyberEdu - Responsable du Management de la Sécurité des Systèmes d'Information (Université de Bordeaux)

L'utilisation d'Internet est omniprésente dans notre quotidien pour la consultation/mise à jour directe ou indirecte de bases de données (saisie à distance de notes d'étudiants, consultation des comptes bancaires, achats en ligne...). Or, trop peu d'utilisateurs se posent des questions telles que : Est-ce que le serveur auquel je me connecte en cliquant sur un lien est le véritable serveur souhaité (et non pas un serveur mis en place par un pirate informatique pour leurrer les utilisateurs) ? Est-ce que le cadenas qui apparait à gauche de l'URL[3] ou le « s » qui vient compléter le nom du protocole HTTP (pour donner https) suffisent à garantir l'authenticité[4] du serveur contacté ?

Ainsi, comme expliqué et mis en évidence au travers de démonstrations par Philippe WERLE, Vice-Président Outils CyberEdu, des réponses aux questions précédentes reposent sur l'utilisation des *certificats électroniques ou certificats numériques* (sortes de carte d'identité numérique pour l'authentification) que les serveurs « présentent » aux navigateurs des postes clients comme preuve de leur identité. Malheureusement, de nombreux administrateurs de sites web (universités, enseignes d'e-commerce, associations…) n'utilisent pas des certificats émis et vérifiés par une Autorité de Certification. En effet, pour des raisons purement économiques, certains administrateurs sont tentés d'utiliser des certificats SSL auto-signés : certificats gratuits, créés et gérés par l'administrateur. La plupart des navigateurs Cyber déclenchent des alertes de sécurité (messages ou pop-up) face aux certificats auto-signés. Malheureusement, un simple clic par l'utilisateur (sans même lire le message…) permet de passer outre ces alertes et de continuer la navigation. Ceci constitue alors une véritable prise de risque avec des conséquences parfois très critiques. Aussi, comme le souligne Philippe WERLE, les utilisateurs d'Internet doivent être conscients des dangers de la navigation sur le web, être vigilants (voire méfiants) et acquérir le réflexe d'accorder leur confiance aux seuls certificats signés. Coté organismes administrant des serveurs web, une prise de conscience est également nécessaire pour abandonner les certificats auto-signés et, plus globalement, financer la sécurité informatique à hauteur des menaces potentielles. Dans le cas de l'enseignement supérieur recherche, Philippe WERLE précise qu'il existe un marché public permettant d'obtenir sans frais des certificats. RENATER, notre réseau national de l'enseignement supérieur recherche (NREN), bénéficie du contrat signé entre GEANT Association et le prestataire de certification commercial Digicert (cf. https://www.renater.fr/certificats-tcs).

3 Uniform Resource Locator, couramment appelé « adresse web ».
4 Nous ne parlons pas ici de garantie de l'intégrité des données transmises mais bien de l'authenticité de la source de données.

SCHNEIDER Electric :

Vulnérabilités et attaques des systèmes automatisés : Les solutions Schneider pour limiter les risques

Intervenant : Jimmy VABAGLIO - Schneider Electric

Pour la plupart des individus, la sécurité informatique concerne presque exclusivement les ordinateurs et les matériels de réseaux/communication. Cependant, depuis l'affaire du virus Stuxnet qui s'est attaqué aux alimentations électroniques des centrifugeuses nucléaires iraniennes[5] via des SCADA[6], une partie de la population a compris que les systèmes automatisés de pilotage ou de supervision des systèmes de production peuvent également être des cibles potentielles d'attaques. Ceci est d'autant plus vrai que les automates programmables industriels, les systèmes de supervision et autres éléments de base des systèmes automatisés, sont de plus en plus dotés de services/fonctionnalités logicielles pour s'intégrer dans des environnements à haute connectivité. Selon des chiffres présentés dans cet exposé, la vulnérabilité des Systèmes de Contrôle Commande est bien réelle avec, par exemple, une multiplication par 10 environ du nombre de failles découvertes sur des produits industriels entre 2010 et 2012. Ceci découle essentiellement d'une prise en compte insuffisante des risques (induisant un manque de sécurisation des produits) par les différents acteurs : constructeurs, éditeurs, intégrateurs, utilisateurs, etc. Or, comme souligné par Monsieur Jimmy VABAGLIO, spécialiste sécurité chez Schneider Electric, une seule défaillance dans un des maillons de cette chaine d'acteurs suffit à anéantir la sécurité du système complet. Ceci suppose donc, non seulement de définir une stratégie globale de cybersécurité mais aussi d'accompagner l'ensemble des acteurs dans la mise en œuvre de cette stratégie. Cet exposé a donc présenté l'expertise de Schneider Electric en matière de cybersécurité, de méthodologie de mise en place d'une cybersécurité industrielle et d'accompagnement des acteurs (formation, aide à la rédaction de cahier des charges, rédaction de politique de sécurité ...). Cet exposé a également permis d'aborder le durcissement des équipements de la marque Schneider (remplacement des protocoles non-sécurisés par leurs homologues sécurisés, l'activation des fonctions de sécurité embarquées ...) et les perspectives de développement de ce durcissement (sécurisation des communications, renforcement du contrôle d'accès logique...).

Communications sécurisées – VPN :

Confidentialité / intégrité des données transmises

Intervenant : Joël DURAND - IUT de Nîmes

Comme déjà évoqué, une des principales problématiques en matière de sécurité informatique concerne la transmission des données. Que ce soient la communication de données personnelles telles que les informations relatives à une carte bleue lors d'un paiement via Internet ou des données professionnelles sensibles (fichier client d'un agent commercial). L'objectif est de préserver à la fois la *confidentialité* (non-divulgation) et *l'intégrité* (non-altération ou non transformation par un tiers) des données transmises. Le problème est d'autant plus complexe que les informations circulent, la plupart du temps, via l'intermédiaire de réseaux publics. Une solution connue depuis l'antiquité est naturellement de chiffrer[7] les données. Cet exposé a donc été l'occasion de rappeler/présenter le principe des méthodes de chiffrements par clés publiques et privées, asymétriques vs symétriques, et de discuter de la fiabilité de certaines méthodes de chiffrement (Exemple : la vulnérabilité du chiffrement par clé WEP dans les transmissions par réseau Wifi). Après une présentation de la problématique liée la principale attaque logicielle dite de l'Homme au Milieu (Man in the middle), l'exposé s'est ensuite concentré sur l'exploitation de cette technique de sécurisation des communications par chiffrement, pour la mise en œuvre de cadres de travail à distance via des VPN (Réseaux Privés Virtuels).

CISCO :

Sécurité dans les réseaux informatiques

Intervenant : Julien BERTON, France Technical Manager, Ile-de-France Area Academy Manager - INLEA at CISCO

Nul n'est besoin de présenter CISCO comme acteur international majeur dans le domaine des réseaux informatiques. Basé sur l'Annual Cybersecurity Report (2018) de cette entreprise, l'exposé de Monsieur Julien BERTON, Technical Manager chez INLEA at CISCO, a apporté un éclairage particulièrement instructif sur la quantification, à l'échelle internationale, de la menace inhérente à la propagation d'attaques via les réseaux informatiques. La principale contribution à cette menace est actuellement celle des *ransomware*. Or, comme présenté dans cet exposé, que ce soit à partir de la consultation de sites web, de la réception de mails ou autres, les infections par ransomware résultent, avant tout, d'une « erreur » humaine : click sur un lien vers un site diffusant des logiciels malveillants (*malvertising*), lecture d'une pièce jointe infectée, etc. Si les vecteurs de propagation sont les supports de stockage amovibles (clés USB, DVD) et la connexion à Internet, l'individu reste donc la principale source de vulnérabilité. Comme déjà évoqué dans d'autres exposés, cette vulnérabilité découle du manque de connaissance des risques, de l'omission volontaire ou non des mises à jour de protection contre les menaces connues, du non-respect des procédures et règles de mise en sécurité des systèmes, etc. L'acquisition de ces connaissances et de ces reflexes passe, avant tout, par la formation. La seconde partie de cet exposé a donc concerné différentes offres de formations dispensées par CISCO, en matière de sécurité des réseaux et de cybersécurité. Ces formations, telles que Cybersecurity Essentials, CCNA Security... (voir : https://www.netacad.com/fr/courses/), sont accessibles aux enseignants et/ou aux étudiants via différentes formes de partenariats, et permettent notamment d'obtenir des niveaux de certifications reconnus, tant au niveau national qu'international.

Attaques matérielles :

Principales attaques (canaux cachés, fautes…), confiance dans les circuits intégrés (chevaux de troie)

Intervenant : Florent BRUGUIER - IUT de Nîmes

Après plusieurs exposés sur les attaques logicielles dans les systèmes informatisés, les systèmes d'automatismes, les matériels de communication / réseau, l'exposé de Florent BRUGUIER a permis d'aborder une catégorie d'attaques encore peu connue du grand public et qui concerne directement les composants électroniques (circuits intégrés). À titre d'exemple, Florent BRUGUIER a présenté deux techniques de cassage de clés de chiffrement basées sur l'observation, respectivement, de la consommation d'énergie ou du temps de réaction des composants impliqués dans l'authentification des clés. De manière vulgarisée : Pour pouvoir comparer une clé transmise

5 1/3 du parc des centrifugeuses servant à l'enrichissement de l'uranium ont été détruites.
6 Supervisory Control And Data Acquisition (Système de contrôle et d'acquisition de données).
7 Le chiffrement est le procédé avec lequel on rend la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement.

avec la vraie clé de chiffrement, il faut que cette dernière soit chargée dans une mémoire. La zone de mémoire concernée subit donc des transitions de l'état bas à l'état haut et vice et versa, afin de matérialiser les états logiques 0 et 1. Or, ces transitions d'états ne consomment pas la même énergie (et ne correspondent pas aux mêmes temps de transitions). En observant « cellule par cellule » les consommations d'énergies (ou les temps de transition), il est alors possible d'en déduire la clé de chiffrement. Au-delà de ces aspects techniques, cet exposé a alors soulevé une importante question relative à la confiance que l'on peut accorder aux composants achetés auprès de certains fabricants. Autrement dit, quelle garantie a-t-on que le circuit intégré que nous implantons sur notre carte électronique ne cache pas un émetteur / « transmetteur » d'informations, un système de blocage du fonctionnement ou autre ? Là encore, une sensibilisation des étudiants de GEII à ce genre de risques apparait comme très importante en vue de leur insertion dans les secteurs industriels de l'électronique et des systèmes embarqués.

CyberEdu (http://www.cyberedu.fr/) CyberEdu Association et labellisation

Intervenant : Philippe WERLE - Vice-Président Outils CyberEdu - Responsable du Management de la Sécurité des Systèmes d'Information (Université de Bordeaux)

Au regard des différents exposés, il est clairement apparu que la formation était un élément clé de la lutte contre les différentes formes d'attaques informatiques (incluant les cyberattaques). Dans ce sens, l'objectif de l'association CyberEdu, soutenue par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), est d'inciter et d'accompagner l'intégration de la Sécurité des Systèmes Informatiques dans les formations de l'enseignement supérieur. Pour cela, CyberEdu met à la disposition des enseignants une mallette pédagogique contenant notamment : un guide pédagogique, un cours préparé d'environ 24 heures sur l'enseignement des bases de la sécurité informatique, ainsi que des éléments de cours sur la sécurité des réseaux, des systèmes d'exploitation et dans le cadre du développement de logiciels. Comme souligné par Philippe WERLE, Vice-Président Outils CyberEdu, les fiches de cette mallette s'adressent à un large public et sont telles que l'acquisition de compétences (en auto-formation) et l'exploitation de ces outils pédagogiques ne sont pas réservées aux seuls enseignants techniques. De plus, ces fiches balayent un spectre étendu de sujets/compétences : de la sensibilisation et initiation à la Cybersécurité à des aspects plus pointus comme la sécurité dans les composants électroniques. Enfin, signalons que la contribution de CyberEdu ne s'arrête pas à ce kit pédagogique puisqu'elle organise également des colloques à travers la France et vise à délivrer un label CyberEdu aux formations (et donc aux étudiants) référencées comme intégrant des contenus de sensibilisation à la sécurité informatique (pour plus d'informations : http://www.cyberedu.fr/).

Conclusion

Les différents exposés ont permis de mettre en exergue de nombreuses menaces, de nombreuses techniques d'attaques et une pluralité des cibles matérielles (de l'ordinateur à l'objet connecté en passant par les composants d'automatismes). Au-delà de la sophistication technique des attaques, le principal vecteur de vulnérabilité demeure l'être humain lui-même. La connaissance des risques et des méthodes de protection demeure donc la meilleure solution pour développer la sécurité informatique et contrecarrer la cybercriminalité. Il semble donc important pour nous, enseignants de toutes matières, d'acquérir des compétences en cybersécurité / sécurité des systèmes informatiques afin de sensibiliser ou, encore mieux, de former nos étudiants aux risques et menaces, ainsi qu'à l'adoption de bonnes pratiques.

Remerciements : Je tiens à remercier Philippe Werle et Chantal Faye pour leur relecture de cet article, ainsi que tous les intervenants de cette commission cybersécurité.

Arènes de Nîmes

Commission 2 Énergie et efficacité énergétique

Marouane ALMA *(IUT de Longwy)*
Alain TINEL *(IUT du Havre)*

L'épuisement à terme des ressources fossiles et fissiles et leur impact négatif sur l'environnement impose une application généralisée de l'efficacité énergétique afin de maitriser la consommation d'énergie tout en augmentant les sources renouvelables.

Cette efficacité énergétique représente le rendement énergétique complet d'un système : elle va donc dépendre de l'objectif du système. Elle découle du rendement, mais est fonction de ce à quoi l'énergie doit servir.

Le secteur du bâtiment est, parmi les secteurs économiques, le plus gros consommateur en énergie. Il représente plus de 44% des consommations énergétiques nationales et près de 20% des émissions de CO2. La France s'est engagée très tôt pour améliorer la performance énergétique des bâtiments et s'est dotée d'une réglementation thermique dès 1974, renforcée régulièrement depuis. Le gouvernement français a décidé en 2007 le lancement d'une large concertation désormais connue sous le nom de « Grenelle de l'environnement », qui a permis d'amorcer la transition écologique de la France.

Les lois Grenelle ont ainsi servi de base pour définir la politique énergétique de la France, et notamment les principes de la nouvelle réglementation thermique. Cette nouvelle réglementation, appelée « RT 2012 » vise à généraliser le Bâtiment Basse Consommation dans la construction neuve.

Les objectifs de cette commission ont été dans un premier temps de sensibiliser le public, de présenter quelques solutions de production d'énergie issues de sources renouvelables et leurs introductions dans l'enseignement GEII. Dans un deuxième temps des solutions technologiques de smartgrids nous ont été proposées ainsi que leurs déclinaisons pour l'enseignement en DUT ou en LP.

Des retours d'expériences pédagogiques sur ces thématiques nous ont également été rapportés.

Intervention de Mr Pascal Tigreat de la société Wago :

« Présentation des consommations dans un bâtiment smart »

Le bâtiment « smart » ou intelligent se définit comme un bâtiment à haute efficacité énergétique, intégrant dans sa gestion intelligente les équipements consommateurs, les équipements producteurs et les équipements de stockage, tels que les véhicules électriques.

La réglementation thermique RT 2012 impose de connaitre donc de mesurer la consommation en énergie et pour cela il faut repérer les différentes sources de consommation que peuvent être le chauffage, la climatisation, la ventilation, l'eau, l'éclairage et les équipements.

Dans un premier temps il convient de mesurer ces consommations et cela peut se faire à postériori avec les factures ou par le relevé des compteurs en place.

- **Identification des postes de consommations :**
  - Electricité : luminaires, centrale de traitement d'air, ventilation mécanique centralisée, pompes, moteurs, groupe froid, pompes à chaleur, ventilo-convecteur, ballon d'eau chaude sanitaire, serveurs, PC, etc.
  - Eau : points de livraison (robinet, douches, WC), points de consommation.
  - Gaz : chauffage, four, eau chaude sanitaire, laboratoire.

- **Synthétisation des données :**
  - Base de données : simulation des consommations en fonction des usages, des zones du bâtiment, de l'utilisation horaire des équipements (détection éventuelle de fuites).

- **Identification des éléments énergivores :**
  - Centrale de traitement d'air, chauffage électrique, compresseur…, la consommation due à l'éclairage peut être importante en fonction de la vétusté du matériel (si utilisation d'un ballast électronique gain de 20 à 30% et si utilisation de led cela implique un gain de 50 à 60%)
  - Mesurer sur chaque départ la consommation réelle et pour les gros postes faire un enregistrement régulier de la consommation journalière et hebdomadaire

- Analyser les consommations :
  - Proposer des améliorations (gestion de plages horaires, anticipation)
  - Proposer des changements (équipements, principe de fonctionnement)
  - Voir si les abonnements sont bien dimensionnés
- Adaptation de la consommation :
  - en fonction de la tarification ou équilibrage réseau,
  - avec des compteurs communicants,
  - en décalant sa consommation (load shifting),
  - en effaçant sa consommation (production autonome),
- Agrégateur (engagement d'un groupe d'entreprises de ne pas consommer en même temps et suivant certaines plages horaires)

• **Le grid** (équilibrage du réseau) : il faut que la consommation du réseau soit équilibrée avec la production.
- Stockage de l'énergie (chaleur, ballon d'eau chaude, frigo)
- Stockage de l'électricité (alimentation sans interruption (UPS), batteries ou véhicule électrique)

La société Wago propose entre autres des produits orientés efficacité énergétique.

Intervention de Mme Claire Basset de l'IUT de Ville d'Avray :

« retour d'expérience sur la gestion d'éclairage »

Dans le cadre du Concours Usage et Bâtiment Efficace (CUBE 2020 : https://cube2020.org/) auquel l'IUT de ville d'Avray participe, le service patrimoine de cet IUT mène une réflexion globale sur sa consommation d'énergie. L'objectif du projet est de mettre en œuvre des automatismes permettant de réduire la consommation d'énergie dans une salle témoin (atelier d'automatisme) qui permet de faire des mesures, de sensibiliser les étudiants et de communiquer lors des journées portes ouvertes.

Dans l'atelier d'automatisme d'une superficie de 60m², il y a eu modification de l'éclairage pour passer en technologie LED avec pilotage intelligent par bus DALI, il y a eu modification du chauffage en intégrant une vanne 3 voies commandée en fonction de l'occupation de la salle et il y a eu création d'une supervision. Les mesures de puissance sont obtenues à partir de 3 centrales de mesure connectées en réseau, le chauffage est géré par un automate programmable industriel qui prend en compte la consigne de température et l'état ouvert ou fermé des fenêtres. L'éclairage est pris en charge par un automate programmable industriel WAGO et une interface DALI. Ce projet est entré dans le cadre des projets tuteurés pour 10 étudiants de DUT en 2015/2016, 4 étudiants en 2016/2017 et 2 étudiants de DUT et 2 de LP en 2017/2018.

Les perspectives sont d'obtenir des données de commande pour le chauffage en fonction de la météo et de l'emploi du temps, d'avoir un affichage en temps réel de la consommation électrique, de créer une page web et d'étudier la cybersécurité du système.

Intervention de Mr Claude Bouchard de la société ACE Didactique

La société ACE Didactique est composée de 3 départements :
- Energies et environnement
- Industries
- Technologie

Leurs buts sont les :
- Développement de petites parties opératives pour l'éducation
- Développement de scénarios pour développer des automatismes

L'exemple présenté concerne le système Pelton-3E-Microcentrale hydroélectrique Tri-Énergie. Pour assurer l'optimisation de la gestion de l'énergie, Smartgrid, ce banc permet de contextualiser la transition énergétique d'une centrale thermique vers un mixte énergétique à base d'énergies renouvelables : éolien, solaire et hydro électrique.

Ce dispositif donne la possibilité d'aborder et d'étudier les différents thèmes suivants :

Energie : produire de l'électricité
• Energie hydraulique, chute d'eau
• Energie fluidique, éolienne
• Energie solaire, photovoltaïque

Stocker l'électricité
• Energie potentielle, eau de retenue
• Energie mécanique, volant d'inertie
• Chimique, batterie

Transporter et gérer l'énergie électrique
• Structure d'un réseau de transport
• Pertes dues au transport
• Gérer les besoins de 4 consommateurs (Usine, Habitat, Hôpital, Pompage) en fonction des énergies disponibles

Matière & structure : Etude de la turbine
• Choix d'un matériau en fonction des contraintes
• Prototypage (impression 3D)

Information
• Acquérir : Capteurs de pression, Débitmètre
• Traiter : Automate Siemens
• Communiquer les informations : Réseau Ethernet
• Gérer la consommation et la production « smartgrid »

Intervention de Mr Samuel Nguefeu de R&D RTE :

« Le futur de la distribution électrique et retour d'expérience Valise Soleis »

En première partie, Mr Nguefeu nous a parlé des aspects conventionnels des réseaux électriques, de la victoire du courant alternatif sur le courant continu :

• Transformation facile des niveaux de tension pour réduire les pertes de transport.
• Evolution facile de la structure du réseau
• Elimination facile des tronçons de réseaux en défaut (disjoncteurs)

Les missions de RTE sont de développer, exploiter et maintenir le réseau de distribution.

La deuxième partie concerne l'avènement des énergies renouvelables :
• Photovoltaïque, Thermique, Eolien, Hydraulique, Biomasse, Géothermie.

En 2018, les énergies renouvelables ont couvert 22,8% de la consommation d'électricité en France.

Le stockage de l'énergie électrique :
• Les Stations de Transfert d'Energie par Pompage (STEP) permettent d'éviter le gaspillage d'énergie pendant les heures creuses (nuit, week-end) et de pallier à l'intermittence de la production électrique du secteur éolien et solaire.
• Le projet RINGO (ligne virtuelle) : l'entreprise veut "construire le premier réseau qui conjugue électricité et digital". L'objectif est de répondre aux évolutions rapides des usages de l'électricité (arrivée des véhicules électriques et bâtiments intelligents, notamment) et à la multiplication des acteurs (nouveaux

producteurs, agrégateurs, opérateurs d'effacement, etc.). Pour y parvenir, l'entreprise entend privilégier des solutions "légères" dont les lignes virtuelles qui visent à renforcer le réseau sans créer de nouvelles lignes. Des batteries rendraient le même service que celui fourni par un renforcement des lignes saturées ou la création de nouvelles lignes physiques.

Bilan prévisionnel de RTE :
- Augmentation des énergies renouvelables
- Fermeture des réacteurs nucléaires
- Evolution de la consommation
- Augmentation du nombre de véhicule électrique.

Convergence des technologies de l'énergie électrique et du numérique (courant porteur en ligne, fibre optique).
Cybersécurité (IEC 61850) : les équipements de postes sont dotés d'une interface numérique leurs permettant de dialoguer avec les contrôle-commandes numériques : disjoncteurs, sectionneurs, interrupteurs, transformateur de puissance.

Concernant la valise Soleis présentée, celle-ci est utilisée en TP avec les étudiants de l'IUT de Villetanneuse. Elle permet de faire des branchements et de calculer la puissance de panneaux photovoltaïques. Le logiciel AGS permet lui de récupérer les données et de tracer les courbes de puissances en fonction de l'inclinaison essentiellement.

Intervention de Mr Gonzales de Schneider Electric :

« les smartgrids »

Pour faire face aux mutations du paysage énergétique, il est nécessaire de moderniser le système électrique. Le contexte français et européen, dans lequel se sont développés les réseaux électriques, conduit à privilégier le déploiement des technologies de Smartgrids plutôt que le remplacement et le renforcement massif des réseaux.

L'intégration des nouvelles technologies de l'information et de la communication aux réseaux les rendra communicants et permettra de prendre en compte les actions des acteurs du système électrique, tout en assurant une livraison d'électricité plus efficace, économiquement viable et sûre.

Les grands principes des smartgrids sont :
- Supervision et contrôle : transport, état du réseau, mesure et comptage,
- Optimisation : reconfiguration du réseau et gestion de la demande,
- Anticipation : maintenance et gestion prévisionnelle du stockage de l'énergie.

Le système électrique sera ainsi piloté de manière plus flexible pour gérer les contraintes telles que l'intermittence des énergies renouvelables et le développement de nouveaux usages tels que le véhicule électrique. Ces contraintes auront également pour effet de faire évoluer le système actuel, où l'équilibre en temps réel est assuré en adaptant la production à la consommation, vers un système où l'ajustement se fera davantage par la demande, faisant ainsi du consommateur un véritable acteur.

Les microgrids, appelé aussi mini smartgrids ou micro-réseaux intelligents, sont des réseaux électriques de petite taille, conçus pour optimiser la facture énergétique, fournir un approvisionnement électrique fiable (surmonter les blackouts) et de meilleure qualité à un petit nombre de consommateurs. Ils agrègent de multiples installations de production locales et diffuses (micro-turbines, piles à combustible, petits générateurs diesel, panneaux photovoltaïques, mini-éoliennes, petite hydraulique), des installations de consommation, des installations de stockage et des outils de supervision et de gestion de la demande. Ils peuvent être raccordés directement au réseau de distribution ou fonctionner en mode îloté. Le concept est en train de s'élargir aux réseaux de chaleur et de gaz. Le concept de microgrids peut ainsi être pensé de façon multi-fluides et il peut concerner différentes échelles du territoire (bâtiment, quartier, zone industrielle ou artisanale, village, etc.).

Intervention de Mr Di Pillo de l'IUT de Longwy :

« Retour d'expérience sur le Cyclo-grid de schneider »

L'efficacité énergétique a été introduite pour assurer une optimisation de l'utilisation de l'énergie tout en fournissant les mêmes services. Elle est définie par le rapport entre l'énergie fournie et l'énergie consommée. Ces enjeux ont été présentés pour 3 secteurs importants : Le bâtiment (RT2012), l'industrie (Norme CEI 60034-30-1) et le transport (Norme NF EN 16247-4). M. Di Pillo a défini les Smartgrids et leur contribution dans l'efficacité énergétique par l'adaptation de la distribution de l'énergie électrique, depuis sa production, en fonction de la demande, avec comme intérêt l'équilibrage entre la production et la demande.

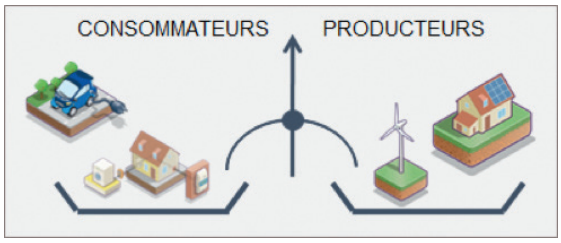


Image : Olivier Di Pillo – IUT de Longwy

Avantages des smartgrids :
- Pour le client : offres de services diversifiées et réduction des délais de prestations.
- Pour le producteur : intégration de sources d'énergie décentralisées, insertion de sources de stockage et possibilités de gérer de nouveaux usages avec maintenance et suivi simplifiés des sites décentralisés (gain économique).
- Pour le fournisseur : pas de déplacement sur site (intervention ou relevé) et pilotage à distance.

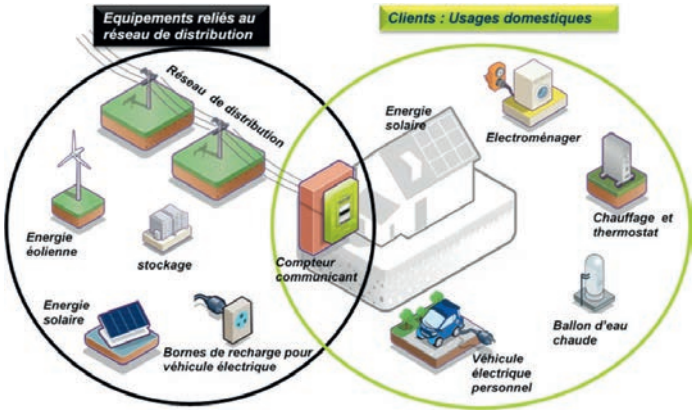


Image : Olivier Di Pillo – IUT de Longwy

Par la suite, le dispositif Cyclo-grid de Schneider a été présenté en détail avec ses chaines d'information et d'énergie, la possibilité d'inclure différentes sources d'énergie (éolien, photovoltaïque, stockage batterie ou réseau EDF), ainsi que les différents profils d'utilisation possibles (privilégier l'utilisation d'une source au détriment de la disponibilité de l'énergie ou l'inverse).
L'utilisation du dispositif Cyclo-grid en travaux pratiques de DUT GEII ou en LP dans les différentes matières liées à l'énergie (automatisme, réseaux locaux industriels, convertisseurs), a été présentée en fin d'exposé.

Intervention de Mr Luconi du lycée Dhuoda de Nîmes :

« Etat de l'art de l'évolution de l'éolien industriel »

Le développement du parc éolien français répond aux enjeux énergétiques ainsi qu'aux directives européennes en matière d'environnement et d'énergie renouvelables. Dans la loi relative à la transition énergétique, la France se donne l'objectif d'atteindre une part d'énergie renouvelable de 32% de sa consommation finale en 2030, dont une capacité installée de 30GW d'éolien. Aujourd'hui parmi les énergies renouvelables, l'éolien occupe la deuxième place (après l'hydroélectricité) dans la production d'électricité française. C'est aussi la source d'énergie renouvelable qui a le plus progressé avec le solaire.

M. Luconi a présenté des chiffres et des cartes sur les parcs éoliens français et européens, ainsi que les déploiements actuels et futurs de nouvelles éoliennes en parcs offshore (Seine Maritime, Calvados, Loire Atlantique, Vendée, etc.). Les besoins technologiques et industriels dans la production et la maintenance de plusieurs types d'éoliennes ont été présentés, d'où l'intérêt pour la communauté GEII de s'intéresser à ces techniques et de les inclure dans les différentes offres de formations (DUT + LP).

Intervention de Mr Guilbert de l'IUT de Longwy :

« Retour d'expérience sur l'utilisation de maquettes d'éoliennes en GEII »

La présentation a commencé par quelques chiffres récents sur le contexte environnemental actuel. Ces chiffres montrent la durée de vie limitée des ressources fossiles, la part très faible des énergies renouvelables (EnR) dans la consommation énergétique, ainsi que les capacités installées des EnR qui restent faibles malgré une forte évolution lors de la dernière décennie.
Trois maquettes pédagogiques consacrées aux éoliennes ont été présentées. La première est le fruit d'un projet tuteuré des étudiants du DUT. Elle concerne la production d'hydrogène propre à partir d'une éolienne par le principe de l'électrolyse de l'eau. L'hydrogène peut par la suite être utilisé avec une pile à combustible pour générer de l'électricité qui alimente, dans le cas de cette maquette, un servomoteur.
La seconde est une éolienne à taille réelle installée à l'IUT de Longwy et qui alimente le réseau, d'une puissance nominale de 5kW, un diamètre de pâles de 5m et une vitesse de vent nominale à 17m/s. Les mesures des vitesses du vent et électriques de chaque étage de conversion peuvent être visualisées et exploitées au moyen d'un logiciel. Ces mesures sont utilisées par les étudiants pour développer un modèle (mécanique et électrique) de l'éolienne.
La troisième est une éolienne didactique s'intéressant à la partie électrotechnique par l'étude de la machine asynchrone, et la partie automatique par pilotage de la position angulaire de l'éolienne avec des régulateurs de type P, PI et PID.

Intervention de Mr Glaisner de l'IUT de Ville d'avray :

« Projet étudiants : Installation solaire en Casamance au Sénégal »

Le projet « Niankitte 2016 » qui tire son nom du village sénégalais dans lequel s'est déroulée cette action, est un projet de 4 étudiants de 2e année DUT GEII de l'IUT de Ville d'Avray dans le but de dimensionner et d'installer un système photovoltaïque autonome de petite puissance, pour permettre l'accès à l'énergie électrique à la population. Le projet a été essentiellement financé par l'université de Paris Ouest Nanterre, l'IUT de Ville d'Avray ainsi que par l'ONG KASSOUMAI78. Le système photovoltaïque, quant à lui a été entièrement financé par la société de distribution d'électricité des Yvelines (SICAE-ELY).
Le déroulement du projet nous a été présenté. En premier lieu, l'étude et le dimensionnement ont été réalisés à l'IUT et validés par le tuteur du projet. Par la suite les étudiants se sont déplacés sur place ou ils ont eu droit à un accueil chaleureux de la population locale ainsi qu'à différentes rencontres avec les politiques locaux pour les interroger sur la politique énergétique du pays (Sénégal) et sur l'accès à l'électricité par la population. Les étudiants ont par la suite procédé à l'installation du système avec l'aide des locaux liés au projet. Une fois l'installation terminée, les étudiants ont procédé à une large sensibilisation à l'utilisation de ce genre de système complexe. M. Glaisner a encouragé ce type d'initiatives riches professionnellement et humainement.

Intervention de Mr Colin de ENEDIS Gard :

« Les smartgrids »

ENEDIS est le gestionnaire du réseau de distribution de l'électricité en France. Elle a pour obligation d'assurer l'accès au réseau électrique et sa maintenance quel que soit le fournisseur. Dans le cadre de l'application de la loi sur la transition énergétique, ENEDIS a ouvert une plateforme open-data contenant les données sur la consommation électrique par secteur d'activité. Dans cette présentation, M. Colin a parlé des enjeux de l'intégration des énergies renouvelables qui reste une clé de réussite pour la transition énergétique. Ces sources d'énergies renouvelables seront intégrées à de nombreux endroits du réseau avec une gestion intelligente en introduisant la notion de smartgrids.

À l'origine, le réseau a été créé pour amener l'électricité d'un site de production au client final, et ce modèle n'est plus le même aujourd'hui. L'exemple de l'intégration d'éoliennes au réseau, en l'adaptant à l'intermittence de la production a été présenté, avec une obligation donc d'avoir une régulation de la tension en fonction de nombreux paramètres. Dans le but de prendre en compte la production décentralisée et intermittente des éoliennes, de l'intelligence numérique a été utilisée ainsi que des capteurs communicants sur les lignes de raccordement des éoliennes. Cela permet une connaissance et une prise en compte de l'état réel de la production. D'autres exemples de smartgrids ont été présentés pour montrer à la communauté GEII l'intérêt de leurs utilisations dans l'optimisation de la distribution de l'énergie électrique.

Commission 3 Systèmes technologiques de l'Industrie du Futur

Thierry GLAISNER *(IUT de Ville d'Avray)*
David GLAY *(IUT de Lille)*
Jean-Pierre LE NORMAND *(IUT de Haguenau)*

Le poids grandissant et incontournable du numérique a placé le monde industriel en pleine mutation. La fabrication additive, le Big Data, la robotique avancée et l'Intelligence Artificielle engendrent un fort bouleversement industriel. Ces concepts technologiques offrent de nouvelles possibilités dans la manière de produire. On passe de l'ère de la production de masse à celle de la « personnalisation de masse ». L'état français souhaite rénover le secteur industriel par les apports du numérique à travers le projet **« Industrie du Futur » (Industrie 4.0 en Allemagne)**. Aujourd'hui, la révolution numérique vient succéder à celle de la mécanisation, de l'industrialisation et de l'automatisation. Nous allons vers une nouvelle industrie automatisée, connectée, intelligente et respectueuse de l'environnement. La transformation industrielle opérée par le numérique et les nouvelles technologies va conduire à de profondes évolutions des métiers et des qualifications.

Le développement et la combinaison de nouvelles technologies constituent un levier majeur pour proposer des solutions plus compétitives, plus flexibles, plus fiables, plus sûres et plus agiles. Les principaux enjeux concernent à la fois les technologies (principes physiques, modélisation et simulation, applications) en tant que telles mais également leur conception, leur mise en oeuvre et leur interaction avec les utilisateurs.

Les outils de production 4.0 nécessitent de nouvelles compétences, techniques et culturelles : fabrication additive, réalité virtuelle, réalité augmentée, prototypage virtuel, efficacité énergétique, robotique collaborative, transitique du futur, mise en service virtuelle / jumeau numérique, internet industriel des objets (IIOT) et des services, internet mobile, traitement et analyse de données massives (Big Data et Data Analytics), cybersécurité, cloud, interopérabilité des équipements et des systèmes, systèmes cyberphysiques, lean 4.0, technologies de production avancées, usines et lignes/ilots connectés, machines intelligentes et connectées, organisation et managements innovants, personnalisation de produits, etc.

Des usines construites sur ce modèle de l'industrie 4.0 existent déjà en France. A titre d'exemple, l'usine SEW-USOCOME de Brumath (Bas-Rhin) s'inscrit dans la double démarche d'excellence industrielle et technologique de l'entreprise. Elle y met en oeuvre de nouveaux processus d'assemblage de ses produits, intégrés dans un concept de mobilité intra-logistique innovant. Tous ces processus intègrent la gestion numérique des flux et la robotique.

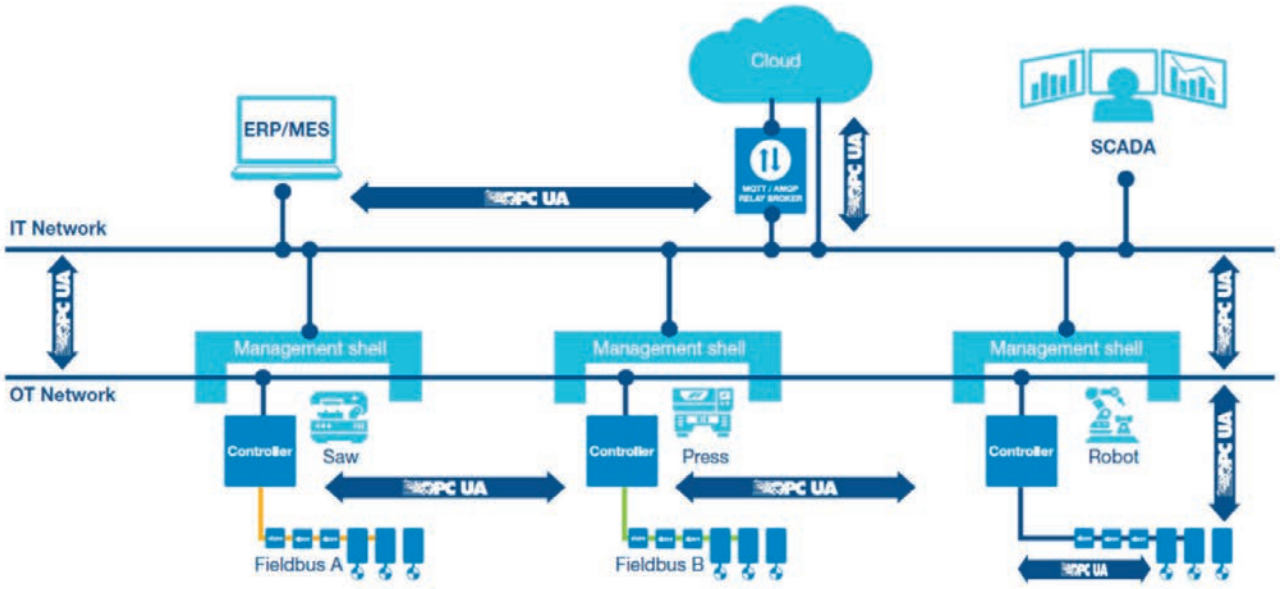
Cette commission avait pour objectif de sensibiliser la communauté GEII à cette transformation digitale de l'industrie. Ne pouvant pas traiter l'ensemble des technologies sur une journée et demie du colloque, la commission a centré les présentations autour de cinq thèmes technologiques de l'industrie du futur. N'ayant actuellement que peu de retour d'expérience pédagogique dans ce domaine provenant des départements GEII, nous avons fait appel à dix intervenants industriels pour présenter cette mutation de l'industrie.

Thème 1 : Réseau 4.0 - OPC-UA

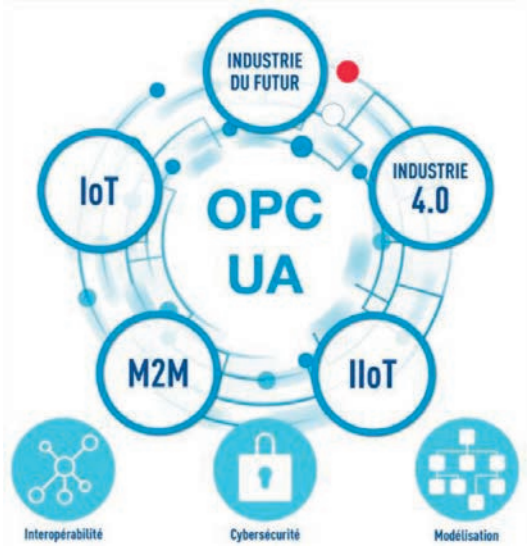
Stéphane Potier, *société B&R*

OPC UA (Open Connectivity Unified Architecture) est un standard ouvert indépendant des fabricants qui unifie les échanges de données dans la communication industrielle : accès aux données de production, gestion des alarmes et des évènements, données collectées et calculées. C'est la Norme d'interopérabilité pour l'industrie du futur. OPC UA est basé sur le principe client-serveur et permet une communication transparente, des capteurs-actionneurs aux systèmes ERP ou au Cloud. Le protocole est indépendant de la plateforme et intègre de façon native les mécanismes de sécurité : contrôle d'accès, identification et chiffrement. OPC UA fonctionne sur différents systèmes d'exploitation : Windows, Linux, Mac et Androïd.

OPC UA permet le passage entre le monde de l'IT (Information Technology) et celui de la production ou OT (Operational Technology). OPC UA permet le transfert de toutes les données du processus de production à travers un seul et unique protocole, aussi bien à l'intérieur d'une machine qu'entre machines, ou encore entre une machine et une base de données dans le Cloud. Sa grande flexibilité lui a permis d'être adapté à tous les domaines de l'industrie : Automobile, Agro-Alimentaire, Industrie du Pétrole et du Gaz, Energie, Services Publics, Conditionnement, Automatisation des Bâtiments…



OPC UA est considéré aujourd'hui dans l'Industrie du Futur comme LE protocole de communication idéal. Associé à la norme Ethernet TSN (Time Sensitive Networking), il ajoute la synchronisation temporelle sur réseau et les communications déterministes pour le contrôle/commande des processus et des machines (OPC UA TSN).



Il sera donc nécessaire de prendre en compte cette évolution importante de l'Informatique Industrielle lors de nos réflexions pour la construction du nouveau PPN. Il sera important également de laisser la possibilité de pouvoir modifier rapidement le contenu du PPN en fonction des évolutions attendues des prochains bouleversements technologiques.

https://opcfoundation.org

https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN.pdf

Thème 2 : Cobotique industrielle

Loïc Wanlin, *société Fanuc*
Adrien Poinssot, *société Universal Robots*
Maxence Thévenin, *société Stäubli*

Depuis le premier robot industriel Unimate dans les années 60, la robotique industrielle n'a cessé de se perfectionner en faisant la course à la vitesse et à la précision. Une nouvelle vision de l'industrie se dessine depuis quelques années pour offrir plus de complémentarité entre les tâches de l'homme et celles du robot ainsi que plus de flexibilité et d'agilité dans les processus de fabrication. Une industrie fondée sur la robotique collaborative. Les robots sont libérés de leurs cages pour amener une réelle interaction entre l'homme et le robot sur un seul et même espace de travail. La mise en place d'un espace de travail collaboratif Homme-Robot permet de garder la polyvalence du robot tout en conservant ou réintroduisant le facteur humain dans les chaînes de production. Le robot collaboratif, appelé aussi cobot, apporte précision, endurance et effort, là où l'opérateur offre son expertise, son intelligence et sa capacité de décision. Cette notion de collaboration (ou coactivité) Homme-Robot varie selon l'environnement de travail et le degré d'interaction entre l'opérateur et le robot.

Les trois intervenants industriels ont présenté les généralités sur la cobotique, leur gamme de robots collaboratifs et leurs spécificités ainsi que les trois niveaux de collaboration qui sont la collaboration directe, la collaboration indirecte et le partage d'espace de travail. La collaboration peut prendre la forme d'une simple coexistence sans interaction de l'homme avec le robot dans un processus global (partage d'espace où chacun travaille sur une tâche différente) ou elle peut mettre en oeuvre des modes opératoires dans lesquels l'homme et le robot interviennent de manière complémentaire et interdépendante (travail sur une même pièce par actions simultanées ou alternées) en vue de la réalisation des différentes étapes de production. La collaboration peut également mettre en oeuvre diverses formes d'assistance physique à la manutention pour aider l'opérateur à accomplir sa tâche en guidant ses mouvements, en démultipliant l'effort exercé, ou en compensant le poids d'un objet ou d'un outil. Quel que soit le degré d'interaction, la vitesse des robots est limitée à 250 mm/s en mode collaboratif. La programmation par démonstration (positionnement dynamique par guidage manuel) du robot est la plus intuitive et révolutionne la rapidité avec laquelle les robots sont déployés en usine.

Les intervenants ont également présenté les principes de sécurité inhérente à la collaboration Homme-Robot en s'appuyant sur différents scénarios de contact liés au robot et à l'application. Le robot collaboratif possède nativement des fonctions intelligentes pour la gestion de la sensibilité et la force appliquée afin de se bloquer ou s'éloigner de l'opérateur en cas de contact avec

le bras du robot, l'outillage ou les objets transportés, mais également se rétracter en cas de pincement. L'analyse de risque demande une certaine expertise pour identifier et évaluer, selon les échelles SIL et PL, les différentes sources de risques pouvant être liées au robot et à son intégration dans le poste de travail. Les caractéristiques des éléments de sécurité varient selon le niveau d'interactivité nécessaire entre l'homme et le robot. Depuis 2016, il existe une norme internationale ISO/TS 15066 qui décrit les différents concepts collaboratifs et leurs exigences, mais elle n'est pas harmonisée à l'échelle européenne. Pour aider les industriels à bien concevoir les phases d'analyse des risques, le ministère du Travail a publié en 2017 un guide de prévention pour la mise en oeuvre des applications collaboratives robotisées.

Plus simples, plus légers, plus maniables, plus intuitifs et surtout plus flexibles, les robots collaboratifs s'adaptent à la vie de l'entreprise, aux exigences de production, aux équipes de travail et aux processus de production. Aisés à programmer, rapidement configurables, facile à redéployer, accessibles aux TPE et PME et aux applications multiples dans de nombreux secteurs, les robots collaboratifs seront au coeur de l'usine du futur. D'après deux études de 2015, 50% des robots industriels vendus en 2020 seront des robots collaboratifs.

Thème 3 : Virtualisation – Jumeau numérique

Alexis Fremin du Sartel, *société Siemens*
Hervé Labarge, *société Fealinx*

Le concept de jumeau numérique

Les exigences du marché industriel évoluent de façon importante aujourd'hui. L'industrie du futur introduit des exigences accrues en matière de Rapidité (Cycles d'innovation raccourcis avec des produits plus complexes, de plus gros volumes de données), de Flexibilité (Production de masse individualisée, marchés volatiles et productivité élevée), de Qualité (Process de qualité en boucle fermée, Traçabilité des produits, Mesure de données volumineuse pour assurer la qualité) et d'Efficacité (Efficacité énergétique et des ressources). Le tout soumis à la nécessaire sécurisation des données.

Pour les industriels, la clé de la compétitivité est l'intégration et la digitalisation de l'ensemble de la chaine de valeur. C'est ainsi qu'est née l'idée de la création d'un jumeau numérique de l'ensemble de la chaîne de valeur (par exemple chez Siemens) : Jumeau numérique du produit, Jumeau numérique du process de production, Jumeau numérique de l'appareil de production.

Siemens et d'autres industriels se dirigent vers une approche globale pour les clients et les concepteurs de machines en mettant sur le marché des progiciels de virtualisation intégrant l'ensemble des besoins.

https://www.plm.automation.siemens.com/media/global/fr/factory-automation-domain-640x360_tcm55-21424.jpg

Cette vision globale numérique peut être présentée de la manière suivante :

Conception du produit : Conception, Simulation, Validation et Test du produit sans construire de prototype physique permettant de visualiser des impacts externes : température, vibrations…

Planification de la production : Validation de la faisabilité d'assemblage du produit, Validation de la cadence en fonction des équipements de production disponibles, Validation et optimisation de l'espace de travail, Simulation humaine pour analyser et améliorer les opérations, Optimisation du flux de production (Identification des goulots d'étranglement, Détermination de la taille des zones de buffers), Simulation de la consommation énergétique de l'usine, Prise de décision sûre pour des futurs investissements d'extension de l'usine.

Ingénierie de la Production : Automatisation de l'ingénierie de la production, Génération automatique du code automate directement depuis le jumeau numérique, Validation du programme avec simulation de l'automate et de la partie opérative.

Exécution de la production : Intégration de tous les composants d'automatisme. Ingénierie facile, rapide et efficace.

Services : Accès à des plateformes cloud ouvertes pour l'Internet Industriel des objets et l'analyse des données, Optimisation des opérations, maintenance préventive, nouveaux business models basés sur les services.

Jumeaux numériques et processus de production physique se « nourriront » des mêmes données provenant des capteurs intelligents et de tous les IIoTs présents sur les systèmes. Le jumeau numérique permettra, par exemple, d'accélérer un processus d'usure et de permettre une intervention de maintenance sur le système réel avec le bon timing. Il permettra de prévoir une modification de production en simulant à l'avance les effets d'un changement d'outil ou de séquence….

Les techniciens supérieurs de demain devront être capables de dialoguer et de comprendre aussi bien le système réel que son jumeau numérique sur des opérations de maintenance, de modification ou changement de programmation, d'évolution de procédé de fabrication….

Thème 4 : IIoT – Internet industriel des objets

Olivier Durand, *société IFM*
Marion Bru, *société SICK*
Yacine Addou, *société National Instruments*
Frédéric Imbert et Jean Ferry, *IUT de Haguenau*

L'internet des objets (IoT) représente une extension d'internet à des éléments physiques qui ne possèdent pas de moyen de connexion. Les objets connectés permettent alors de remonter des informations vers le réseau, qui n'étaient jusqu'à présent connues que par des actions manuelles humaines. L'IoT comprend donc à la fois des objets ainsi que l'ensemble des éléments (réseaux, passerelles …) qui leurs permettent de se connecter entre eux et de se connecter à internet. L'internet des objets industriels (IIoT) est une sous-catégorie de l'IoT et se caractérise par une multitude de systèmes industriels connectés qui communiquent et coordonnent leurs données et leurs actions dans le but d'améliorer les performances industrielles et augmenter ainsi les bénéfices des entreprises.

Ces systèmes industriels connectés ont pour but de résoudre les problèmes de contrôle complexes et relient le monde du numérique au monde physique par l'intermédiaire de capteurs jusqu'à des robots industriels complexes. La prolifération d'objets intelligents et connectés dans l'IIoT offre d'énormes possibilités d'amélioration des performances et de réduction des coûts.

Olivier Durand de la société IFM a présenté IO-Link qui est une technologie normalisée d'entrées/sorties (selon la norme IEC 61131-9) dédiée à la communication avec des capteurs et des actionneurs. Le standard IO-Link est une liaison point-à-point qui fournit aux capteurs et actionneurs la capacité de dialoguer avec les systèmes de commandes. Automates et capteurs échangent ainsi des données de paramétrage, de diagnostic, ainsi que des informations supplémentaires liées au process.

La présentation de Marion Bru de la société SICK (Sensor Intelligence) a montré l'intérêt d'utiliser l'IIoT pour faire évoluer l'industrie vers davantage de flexibilité (production personnalisée), de réactivité (temps réel), d'efficacité (souplesse et fiabilité des process), de prédictivité (anticipation des consommations) et d'économie (optimisation et efficacité énergétique).

Yacine Addou de National Instruments (NI) a mis en avant dans sa présentation certains avantages de l'IIoT comme la maintenance prédictive, l'augmentation des performances par l'optimisation du temps, l'amélioration de la conception et de la fabrication de produits par l'intermédiaire de données des capteurs mondialement connectées.

Frédéric Imbert (GEII) et Jean Ferry (MMI), de l'IUT de Haguenau, ont fait un retour d'une expérimentation IIoT menée dans le cadre d'une collaboration inter département GEII-MMI. Le département MMI souhaitait réceptionner des données et les exploiter au format Web afin de réaliser un site permettant d'afficher et d'exploiter les données enregistrées dans une base de données. Pour être plus concret, les données devaient être issues de vraies grandeurs physiques enregistrées continuellement. La base de données devait être accessible à tout moment par un nombre d'utilisateurs quelconque. Des logiciels standards libres devaient être utilisés. Le GEII s'est concentré sur la réalisation de l'objet connecté, soit une centrale de mesure comprenant différents capteurs (température, luminosité, hygrométrie…). Le coeur du projet est basé sur un module ESP32 Wroom pour gérer l'acquisition et l'envoi des données. Une Raspberry pi, intégrant un point d'accès wifi et un serveur Web Apache (PHP-MySQL), a été utilisée pour la diffusion et l'archivage des données. La transmission des données avec l'ESP est effectuée par une requête GET. Les données sont envoyées au format JSON. La trame est composée de l'identifiant du capteur IIOT, suivi de couples de données (identifiant grandeur physique, valeur grandeur physique). Pour poursuivre ce projet en GEII, le protocole MQTT avec le « broker » Mosquito, l'affichage direct des données et l'accès à la base de données avec WinDev et WinDev mobile sont à l'étude. La sécurisation par chiffrement des données fait partie d'un autre projet en collaboration avec le MMI.

Thème 5 : Dispositifs pédagogiques pour la formation à l'industrie du futur

Cédric Vandermeersch, *société Festo*
Jean-Pierre Le Normand, *IUT de Haguenau*

Cédric Vandermeersch nous a présenté des dispositifs didactiques de production flexible et modulaire ciblés i4.0 tels que MPS 203, CP Lab, AFB Factory, CP Factory. Le pouvoir est maintenant donné au produit et non plus à la ligne pour aller vers la production personnalisée de masse. La production en réseau permet au produit de communiquer avec la machine contrairement à une ligne traditionnelle où le produit est passif. Les compétences nécessaires à un technicien de maintenance i4.0 ont également été décrites au cours de la présentation.

Jean-Pierre Le Normand, chef du département GEII de l'IUT de Haguenau, a présenté en fin de séance une plateforme d'apprentissage à l'industrie du futur. En effet, son département s'est lancé depuis 2015 dans cette transition numérique de l'industrie en développant une pédagogie autour d'une mini-chaîne de production industrielle modulaire de type AFB (société FESTO) orientée industrie 4.0 (i4.0) (http://iuthaguenau.unistra.fr/entreprises-et-innovation/smart-prod-industrie-du-futur/). Le projet, financé dans le cadre d'un investissement IDEX à hauteur de 145k€ et porté par Laurent Thoraval, a pour objectif de former et préparer les étudiants dans les meilleures conditions à l'usine intelligente (smart-factory) et à ses différentes briques technologiques (continuité numérique, cobotique, jumeau numérique, big data, cybersécurité, robotique mobile (AGV), etc.). Les principaux enjeux de l'industrie 4.0 et les bénéfices de la transformation numérique dans toute la chaîne de valeur sont abordés dans un module complémentaire au semestre 4 du DUT et les aspects plus technologiques sont traités dans le nouveau parcours « Industrie du futur » de la Licence Professionnelle SARI qui a démarré à la rentrée 2018. Des collègues du département QLIO interviennent également dans cette formation pour amener des connaissances transversales en LEAN 4.0 (coopération MES (Manufacturing Execution System) et ERP (Enterprise Resource Planning)). À l'issue de la présentation, deux vidéos (disponibles sur le site) ont permis d'identifier cette plateforme et ses activités pédagogiques.

Conclusion

Dans ce contexte de l'industrie digitale, les champs d'activité de nos diplômés GEII s'élargissent de plus en plus et très rapidement. L'arrivée de l'intelligence artificielle modifiera également ce paysage dans les prochaines années. De nouveaux thèmes doivent être abordés dès à présent dans nos formations de DUT et LP pour anticiper l'avenir des jeunes aux nouveaux métiers du secteur industriel de demain. Le métier de technicien de maintenance est l'un des métiers qui va fortement changer dans les prochaines années.

Les exposés de cette commission ont permis de présenter de manière générale de nouveaux concepts technologiques en lien avec l'industrie du futur, mais ces sujets doivent être traités plus en profondeur lors des prochains colloques pédagogiques GEII pour mieux partager nos expériences dans ce domaine qui devraient émerger de plus en plus chaque année dans nos formations. Les axes IIOT ou jumeau numérique pourraient être développés très rapidement.

Les compétences du GEII doivent évoluer dans ce nouveau contexte et la commission propose de prendre en ligne de mire trois piliers du projet « Industrie du futur » pour mener à bien la réflexion sur le futur PPN :

1. Le développement de l'offre technologique par les objets connectés intelligents, la réalité virtuelle...

2. La formation des nouvelles générations avec une montée en compétences sur le numérique et la robotisation

3. L'accompagnement des entreprises dans leur transformation digitale

Liens

Plans Industrie du futur / Industrie 4.0 :

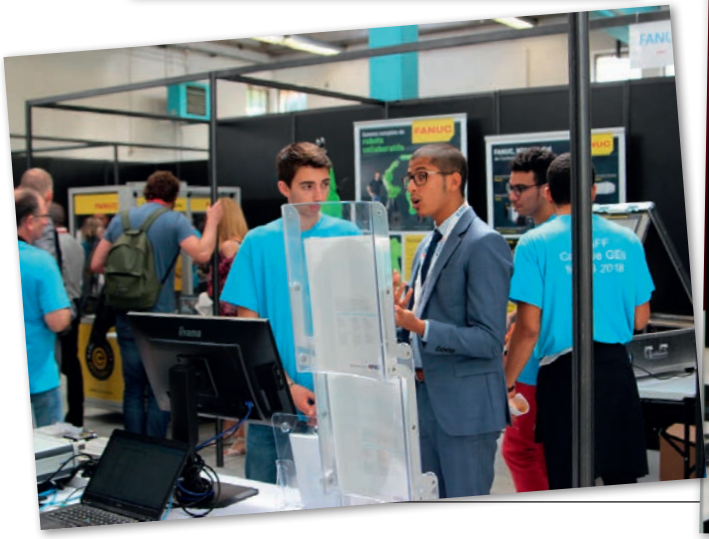
- http://industriedufutur.fim.net/
- http://www.industrie-dufutur.org/
- https://www.plattform-i40.de

Chaînes TV :

- http://smart-industries.lachaineindustrie.fr/
- http://www.industrie-du-futur.tv/

Retour en images sur le Colloque de Nîmes

Photos Thierry Fiol & Stéphane Sanchez



SCIENCES & TECHNOLOGIES

CyberEdu à la Commission 1 Cybersécurité

Philippe Werle, *Vice-Président Outils de CyberEdu et Responsable du Management de la Sécurité des Systèmes d'Information de l'Université de Bordeaux*

Octobre est le mois de la cyber sécurité dans toute l'Europe. De nombreuses manifestations sont organisées au travers du territoire français. C'est pour l'association CyberEdu une excellente occasion d'aborder le sujet dans ce numéro de GESI. CyberEdu est ravie de sa participation à la Commission Cybersécurité lors du 45e Colloque Pédagogique National des départements GEII qui s'est déroulé à l'IUT de Nîmes du 30 Mai au 1 Juin 2018.

Nous tenons à remercier Laurent Laval, chef du Département GEII de l'IUT de Villetaneuse, d'avoir donné l'opportunité à CyberEdu d'intervenir dans cette commission qu'il a créée, aidé dans sa tâche par Joël Durand et Florent Bruguier de l'IUT de Nîmes. Nous tenons également à remercier Gino Gramaccia, secrétaire de l'association GESI, qui nous a sollicités pour écrire un article pour la revue.

L'idée de la commission est le fruit de nombreux échanges autour de la sécurité des systèmes d'exploitation et de celle du développement de code, et surtout de la nécessité de multiplier le nombre des acteurs initiés à ces problématiques dans l'enseignement supérieur, les IUTs et notamment dans les départements GEII. En effet, en GEII, des enseignants de diverses matières (informatique industrielle, automatismes, électronique numérique, culture et communication …) et les étudiants sont amenés à utiliser différentes cibles potentielles d'attaques (de l'ordinateur au système embarqué en passant par les Automates Programmables Industriels), et à développer des programmes pour ces cibles.

L'incident de sécurité informatique, numérique ou cyber est la concrétisation la plus manifeste de l'irruption du virtuel dans le monde réel. Grâce à sa médiatisation, il peut apparaître comme effrayant et dévastateur dans tous les secteurs des activités humaines. Au sein des techniques et technologies du champ d'enseignement, de recherche et de professionnalisation du Génie Electrique et Informatique Industrielle, un incident peut prendre des proportions gigantesques dans le milieu industriel et l'on

n'aimerait pas devoir un jour devoir le qualifier de « cyber catastrophe industrielle ».

L'arrêt du réseau de diffusion de TV5 Monde[1], la paralysie de tous les services en Estonie, l'attaque Stuxnet visant les automates programmables[2] contrôlant la vitesse de rotation des centrifugeuses du site d'enrichissement nucléaire en Iran, la prolifération de codes malveillant dans le système de production électrique d'Enron en Californie et la paralysie de l'ensemble du système « UK Hospitals » touché par Wannacry, le ralentissement des services d'OVH victime d'une attaque de déni distribué de service (DDoS) avec un flux record de 1 Tb/s provenant d'un « botnet » de 145 000 caméras infectées[3] ne sont que quelques exemples de ce qui semble devenir une banalité dans le paysage des catastrophes numériques. Les objets connectés apparus sous le sapin de Noël par le dernier effet de mode consumériste se sont révélés d'une fragilité déconcertante entre les « ondes » de personnes mal intentionnées rodant autour de chez nous et n'hésitant pas à manipuler les plus jeunes enfants. Il est temps de rappeler une parole de sagesse d'un de nos confrères *« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique »* (A. Einstein).

Comme l'histoire l'a montré de manière spectaculaire pour d'autres technologies comme le train, l'automobile et l'aviation, de la conception au paramétrage en passant par l'usage et la formation ou l'enseignement, les acteurs et les usagers des technologies numériques doivent être formés, impliqués et se sentir concernés par la sécurité du numérique. Chacun, dans son domaine d'usage, d'activité, d'expertise professionnelle ou de responsabilité, doit devenir un acteur de sa sécurité numérique et, interconnexion oblige, de la sécurité du numérique de tous.

En 2013, la loi de programmation militaire de l'Etat français a pour la première fois mis un accent particulier sur la cyber sécurité et la nécessité d'en multiplier les savoirs et les compétences dans le monde de l'enseignement supérieur qui concoure à l'avenir de la nation. Il a été demandé à l'Agence Nationale de la Sécurité des Systèmes d'Information[4] de porter l'initiative CyberEdu.

L'ANSSI a organisé dans les locaux de son centre de formation parisien cinq colloques de sensibilisation à destination du monde de l'enseignement supérieur. L'agence a lancé un appel d'offres afin de constituer un ensemble de contenus pédagogiques réutilisables et modulables, la mallette pédagogique CyberEdu. En 2014, l'ANSSI a passé un marché avec l'Université européenne de Bretagne (qui regroupe 28 établissements d'enseignement supérieur et de recherche) et Orange pour sa réalisation. À partir de la rentrée universitaire 2015, l'ANSSI a mis à disposition cette mallette pédagogique sur son site web.

Aujourd'hui, il est évident que nos gouvernants portent une politique de sécurité routière, aérienne et des énergies. Il est également naturel d'avoir une politique de la cyber sécurité. Le 16 Octobre 2015, le Premier Ministre présente la « Stratégie Nationale pour la Sécurité du Numérique[5] » et positionne clairement l'initiative CyberEdu. L'objectif stratégique n°3 est l'enseignement de la sécurité du numérique en formation initiale et continue. L'initiative CyberEdu est identifiée comme étant le vecteur permettant d'atteindre cet objectif, avec le soutien de la CPU et de la CGE.

Le 17 mai 2016, l'initiative CyberEdu devient une association d'enseignants œuvrant à accompagner leurs pairs dans la montée en compétences en sécurité du numérique dans leur champ d'enseignement (informatique, télécommunication, juridique, communication, linguistique, gestion des organisations,…) pour qu'ils puissent ensuite enseigner ces disciplines. Une semaine après les festivités pour les 50 ans des IUTs à la Cité des Sciences et de l'Industrie, l'association CyberEdu est présente à l'AG de l'ADIUT du 16 décembre 2016. Depuis, l'association a pu diffuser son message dans différentes Assemblée de Chefs de Département.

En Commission Cybersécurité, il a été présenté la genèse de CyberEdu et ses objectifs, son réseau sur le territoire national, ses différents colloques organisés dans les régions sur des thématiques variés ; « Intégration de la sécurité dans le développement logiciel », « Intégrer la cyber sécurité dans les enseignements en réseaux », « Cryptographie et développement ». Un point particulièrement important a été souligné concernant l'association et il va être rappelé ici : CyberEdu est une association d'enseignants bénévoles ayant pour objectif l'intégration de la sécurité du numérique dans les cursus d'enseignement supérieur. Novice, amateur éclairé ou expert en sécurité, concepteur ou adaptant un support de cours, si vous êtes volontaires pour intégrer, adapter, accompagner ou conseiller, cette association est la vôtre.

Egalement présenté, le label « CyberEdu » permet de référencer et de rendre visibles aux étudiants et aux entreprises des formations longues incluant des contenus pédagogiques de sécurité du numérique. Les contenus peuvent être librement adaptés depuis la mallette pédagogique CyberEdu ou construits depuis d'autres sources et aborder des notions similaires.

La mallette sous licence CC-BY a été succinctement présentée avec son contenu totalisant 24 heures de cours structurés en modules et accompagnés d'un guide pédagogique. Afin de montrer la variété des contenus plus ou moins spécifiques de ces modules, une présentation a été faite du plan de cours pour les modules « notions de base », « hygiène informatique » et « réseau et applicatifs » montrant que l'appropriation est aisée avec ou sans un accompagnement par l'association.

Non présenté faute de temps, mais cependant fort utile, le support de présentation cite en dernière partie la présentation faite par Xavier Roirand, Vice-Président Grand Ouest et PAST à l'IUT de Vannes, « Exemple d'intégration de la sécurité numérique dans une formation ». Xavier Roirand nous montre comment ses collègues et lui se sont appropriés le contenu de la mallette pour l'adapter aux besoins de leurs enseignements.

CyberEdu est également doté d'un site[6] qui référence ses différents contenus, colloques, présentations, communications événementielles et la mallette pédagogique. Pour tout renseignement, vous pouvez écrire à **contact « @robase » cyberedu.fr**

1 https://fr.wikipedia.org/wiki/Cyberattaque_contre_TV5_Monde et https://www.sstic.org/2017/presentation/2017_cloture/
2 https://fr.wikipedia.org/wiki/Stuxnet - https://www.automation-sense.com/blog/automatisme/stuxnet-siemens-quand-les-virus-s-attaquent-aux-automates-programmables.html
3 https://www.objetconnecte.com/ovh-camera-connectees-ddos-260916/
4 Agence Nationale de la Sécurité des Systèmes d'Information
5 https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/
6 www.cyberedu.fr

Localisation et identification de ressources industrielles par l'Internet des Objets

Eddy BAJIC *(Université de Lorraine, IUT Nancy Brabois)*

Durant cette dernière décennie, de nombreuses entreprises ont investi massivement dans la recherche sur les objets connectés. Le concept d'usine du futur ou Industrie 4.0 est actuellement un des axes majeurs de recherche d'amélioration des processus et des services dans les entreprises, qui s'appuie fortement sur le déploiement d'objets connectés industriels dans une approche Internet des Objets (IdO), appelé communément Internet of Things (IoT). Dans cette perspective, le suivi et la localisation de ressources physiques sur un site industriel constituent un enjeu important dans la recherche de performance et d'efficacité des entreprises. Cette problématique provient du fait que, de plus en plus, les ressources sont mobiles et partagées au sein d'une entreprise ou d'un ensemble d'entreprises. Les ressources industrielles allant d'un gabarit de contrôle à un chariot élévateur, sont amenées à se déplacer et à être utilisé et demandé par de nombreuses personnes au sein de l'entreprise. Une problématique majeure est alors de localiser, en temps réel, ces ressources dans un périmètre donné, de reconstruire le trajet effectué, et de plus d'associer des informations et des services directement au pied de ces ressources pour leur mode d'emploi, maintenance, qualification, signalement, ... Cet article a pour objectif de présenter les différentes utilisations des objets connectés industriels, appelés aussi objets communicants, ainsi que les différentes technologies et plates-formes de services IoT existantes. Nous étudions ensuite la faisabilité d'un système de géolocalisation de ressources industrielles en utilisant des objets communicants de type beacon bluetooth low energy (BLE), et nous détaillerons l'infrastructure et les produits connectés IoT de la société Kontakt.io.

Mots-clefs : IoT; objets communicants; géolocalisation; trilatéralisation; BLE; Beacon; MQTT; plateforme de services.

I. Introduction

Nous sommes entourés d'objets au quotidien, de la tasse de thé que nous utilisons le matin, au stylo qui nous sert à écrire, en passant par notre smartphone qui nous permet de rester connecté au monde et d'effectuer une multitude de tâches avec un seul appareil. Depuis que l'Homme crée des objets, il n'a cessé de les faire évoluer. Le bol en bois a été remplacé par des assiettes en porcelaine ou encore le gramophone par des lecteurs numériques et des haut-parleurs, le télégramme par le SMS. Ces améliorations sont consécutives à l'évolution des technologies dans notre société ainsi qu'à la manière de développer et de rechercher des innovations.

Quelle est alors la prochaine étape ? L'évolution des interactions depuis l'interconnexion entre les hommes et les machines, se tourne désormais vers les interactions entre les machines, voire entre les objets eux-mêmes. Ainsi les objets sont connectés et communiquent sur Internet, amenant au concept Internet des Objets (IdO) ou *Internet of Things* (IoT). Les nouvelles technologies de communication ont transformé nos relations et le monde, bien au-delà de l'apport de simples solutions techniques car "*Le but d'une technologie n'est pas que de résoudre des problèmes. Elle crée aussi des concepts et une philosophie*" comme l'a bien exprimé Howard Rheingold dans [1].

Le concept IoT est simple : prendre un objet et y apporter des fonctionnalités technologiques sensitives et communicantes pour ajouter des caractéristiques étendues à son utilisation de base, afin d'apporter des informations riches et spontanées sur l'objet, son utilisation, son environnement. On peut ajouter une caméra à un stylo pour récupérer nos écrits sur notre ordinateur ; ajouter une connexion internet à une balance pour suivre l'évolution de notre poids sur une application ou encore connecter un détecteur de fumée au réseau internet pour nous avertir en cas de danger. L'IoT ouvre de nombreuses perspectives d'innovation dans différents domaines. Le domaine industriel est un secteur important d'application de l'IoT. Les entreprises connectées ont émergé ces dernières années. La recherche de profit, de performance, de productivité et d'efficacité incite les industriels à

connaître en permanence l'état, la position ou la disponibilité d'une ressource partagée au sein de l'entreprise. Cela permet de réduire les coûts de maintenance en cas d'arrêt ou d'adapter au mieux la production. Notre sujet est d'étudier comment l'IoT peut répondre à une problématique industrielle majeure, concernant la localisation des ressources (matériels, produits, outils,...) appelées communément *Physical Assets* au sein d'un site industriel.

Le premier point que nous étudierons est relatif aux domaines d'applications IoT. Ensuite, nous nous pencherons sur les technologies et protocoles existants puis vers les plates-formes proposant des services pour objet connectés. Nous détaillerons la plateforme Kontakt.io qui connecte des objets en Bluetooth Low Energy (BLE) à Internet. Enfin, nous étudierons les éléments et la faisabilité d'un système de géolocalisation utilisant une telle infrastructure.

Ce travail a été abordé dans le cadre d'un projet d'initiation à la recherche avec des étudiants ingénieurs, et il trouve sa réalisation pédagogique en formation Master Ingénierie des Systèmes Complexes à la Faculté des Sciences et Technologies de Nancy, ainsi que dans le cadre d'une Unité d'Enseignement "Internet des Objets" de la Licence Professionnelle Automatisme et Informatique Industrielle - Systèmes Automatisés et Réseaux Industriels (LP AII-SARI) à l'IUT de Nancy Brabois.

II. Les domaines d'application

Les domaines d'application des concepts et technologies de l'Internet des Objets sont nombreux parmi lesquels les plus avancés sont la ville intelligente (*smart city*), l'usine du future (*Industry 4.0*), le e-santé (*smart health et assistant living*) [2].

Le concept de ville intelligente prône une ville connectée, où des capteurs connectés à internet (IoT) collecte des informations en temps réel afin de permettre un meilleur suivi, analyse et compréhension des flux urbains et des conditions ambiantes telles que le trafic, l'occupation des parkings afin de créer des services aux usagers et aux gestionnaires permettant des économies d'énergie et offrant plus de sécurité et confort dans la ville.

L'industrie connectée via le déploiement de capteurs et objets industriels connectés, devra permettre une meilleure connaissance des systèmes industriels et entrainer une plus grande productivité via une maintenance préventive plus efficace par exemple, et une plus grande réactivité ainsi que la réduction des coûts.

Dans le domaine de la santé, les capteurs connectés permettent un meilleur suivi des personnes médical au quotidien. On peut ainsi envisager la prévention de nombreux accidents médicaux, et la réduction du délai d'attente des secours en cas d'urgence. La montre connectée participe ainsi à suivre les progrès des sportifs ou des activités quotidiennes en embarquant un capteur de rythme cardiaque, de comptage de pas. L'assistance aux personnes handicapées ou âgées dans leur vie quotidienne, à domicile est un grand enjeu de e-santé.

III. Architecture IOT

Généralement, les systèmes IoT disposent d'une architecture en 6 niveaux [3] comme suit :

a. **Périphérique** (*device*) : IL constitue l'objet connecté doté de capteurs qui récupèrent et transmet les informations du monde physique.

b. **Passerelle** (*gateway*) : la passerelle permet de récupérer les informations des capteurs provenant des différents périphériques.

c. **Fog**: (*ou Egde*) Équipement communicant de type passerelle, procédant à des prétraitements et agrégations des données afin de réduire la taille des requêtes et de décharger le trafic réseau montant vers Internet.

d. **Cloud** : Serveurs informatiques accessibles sur Internet et récupérant les informations provenant des capteurs depuis les passerelles, pour les stocker dans des bases de données.

La nature et les caractéristiques des objets IoT sont nombreuses et variées (capteur de température, qualité de l'air, consommation eau, bouton satisfaction client,...), qui impactent sur leurs composants technologiques (microprocesseur, mémoire, E/S, batterie) et leur mode de communication en réseau [4]. De façon générique, nous pouvons définir un modèle d'architecture fonctionnelle pour l'Internet des Objets à 6 niveaux (Figure 1). Ce modèle peut s'appliquer à toutes les infrastructures IoT et montre le niveau Fog / Egde caractérisé par les passerelles dotées de fonctionnalités de traitement sophistiqué de données, afin prendre des décisions ou d'offrir des services rapidement et localement en limitant le flux de données vers Internet, et la latence associée.

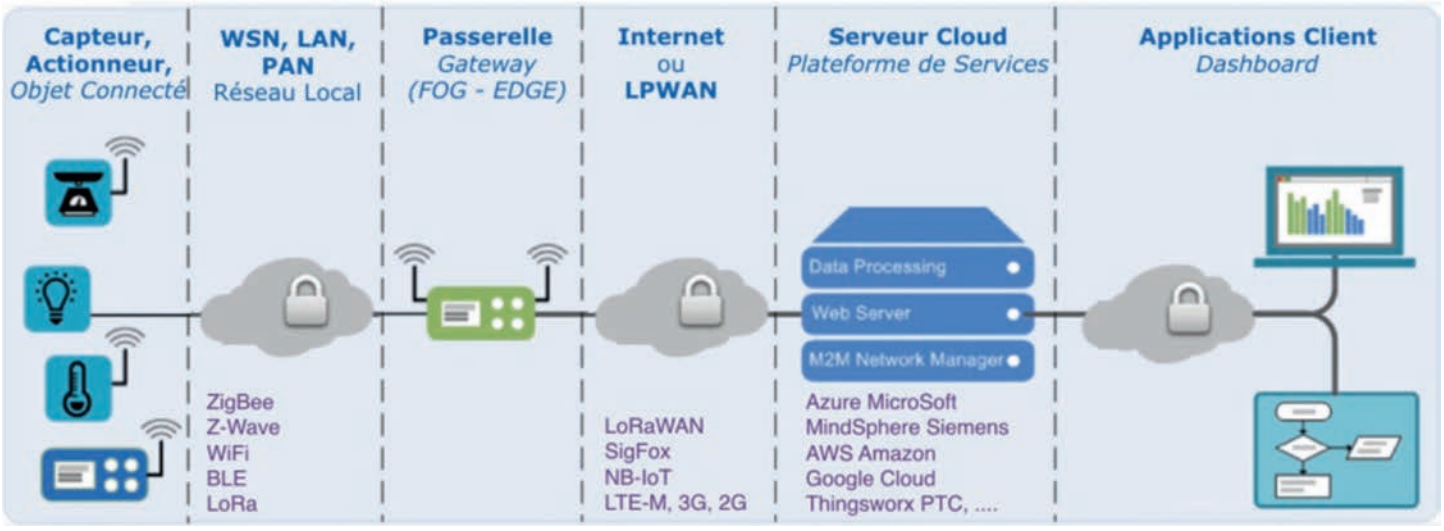


Figure 1 : Modèle d'architecture IoT à 6 niveaux

VI. Plate-forme materielle KONTAKT.IO

De nombreuses solutions matérielles de suivi (tracking) d'objets industriels sont disponibles sur le marché [5] [6] [7] [8]. Nous allons détailler la plateforme proposée par la société Polonaise Kontakt.io, et s'appuyant sur les technologies BLE, WiFi, MQTT et API RESTFul [9].

A. Architecture

Kontakt.io propose une architecture composée des 4 couches vues précédemment. Les capteurs se présentent sous la forme de différents boîtiers, appelés beacons, adaptés à différents usages. Ces boîtiers contiennent chacun différents capteurs, une ou plusieurs batteries, une mémoire ainsi qu'une unité de traitement et de communication. La communication entre les beacons et les passerelles, appelés gateways, est effectuée en utilisant la technologie Bluetooth BLE. Les passerelles sont connectées en Wifi au réseau internet et transmettent leurs données agrégées à une période fixe au cloud Kontakt.io.

B. Gateways

Une passerelle ou gateway, dont un exemple est présenté dans la Figure 2 est l'élément central du réseau IoT. Il s'agit d'une passerelle qui récupère via BLE les données des beacons à sa portée, les centralise puis les transfère via WiFi dans le cloud de Kontakt à intervalle régulier. Le déploiement des plusieurs gateways permet ainsi de couvrir une large zone, le BLE ayant une portée d'une cinquantaine de mètres. On peut ainsi suivre le déplacement des beacons à partir des différentes gateways qui vont capter son signal.
Il est important de noter que les gateways Kontakt.io jouent aussi un rôle important dans l'architecture du réseau. En effet, même si elles ne procèdent à aucun calcul ou traitement de données les gateways centralisent les informations. Celles-ci sont conservées une courte période puis envoyées au serveur. Il s'agit de la partie "Fog" de l'architecture (aussi appelé Edge Computing). Cela permet de limiter la charge du réseau. Un beacon pouvant émettre à une période allant de 20 ms à 10240 ms, si les informations étaient retransmises par la passerelle au fur et à mesure, le réseau serait vite surchargé, surtout dans une configuration multi beacons émettant de façon asynchrone.
Pour fonctionner, les passerelles Kontakt sont alimentées par un port USB, et doivent disposer d'une connexion WiFi (sécurisé WPA2), configurable via une application mobile d'administration du fabricant.
Chaque passerelle dispose d'un identifiant unique non modifiable défini par le fabricant. Des tags peuvent leurs être associés afin d'apporter une personnalisation à leur identification.

*Figure 2 : Gateway Kontakt.io 88*88*38mm [6]*

Au niveau matériel, les gateways sont équipées d'un processeur Dual Core ARM Cortex-A1 cadencé à 1GHZ, d'une mémoire RAM de 512MB et de 4GB de mémoire flash. Les communications sont gérées par un microcontrôleur Bluetooth ARM Cortex cadencé à 16MHz. La gateway supporte plusieurs technologies de communication, tel que le Bluetooth Low Energy, le Wifi (IEEE802.11a/b/g/n/ac) avec les protocoles de sécurité WPA-Personal et WPA-Entreprise (PEAPv0) et ZigBee (IEEE802.15.4).

C. Beacons

Le beacon (ou balise) est l'équipement communicant élémentaire de notre infrastructure IoT. Équipé d'une batterie, de capteurs et de moyens de transmission, il est placé dans l'environnement et permet de recueillir des données caoteurs et positionnement. Il existe une grande variété de beacons en fonction des besoins et des capteurs supportés. Chaque type de beacon dispose de ses spécificités et de ses usages.
Les beacons utilisent la technologie Bluetooth Low Energy pour communiquer avec les gateways. Ils peuvent émettre à une période configurable comprise entre 100 et 10240 millisecondes. La puissance d'émission du signal est aussi réglable. Ces deux réglages sont importants car ils impactent directement la durée de vie de la batterie du beacon. Une transmission rapide et puissante consommera plus d'énergie et réduira la durée de vie de la batterie.
D'autres paramètres sont configurables comme les protocoles d'application au-dessus de BLE pour la transmission de données (iBeacon, Eddystone ou Propriétaire), et leurs paramètres : données de télémétrie (accéléromètre, luminosité, température), et les identifiant des balises (UUID, Minor, Major, etc.). Nous détaillerons avec trois types de beacons.

1) Card Beacon : Au format carte de crédit, il permet généralement d'identifier une personne (Figure 3). Il peut communiquer via Bluetooth (sur la bande 2.4Ghz), via RFID en lecture seule (sur la bande 125 KHz) ou via NFC de type 2. La portée du Bluetooth peut atteindre 50 mètres théoriquement. Les Cards beacons sont équipés d'une batterie au Lithium de 320mAh pouvant tenir 8 mois avec une période d'émission de 350ms, et une puissance de transmission de -20dBm.

*Figure 3 : Card Beacon Kontakt.io 86*54*2mm [6]*

2) Beacon Pro : Équipé d'un microcontrôleur 32 bits ARM à 64MHz, de 64kB RAM et 512kB flash, avec un accéléromètre, un capteur température, et luminosité, et une LED. La communication s'effectue par Bluetooth 4.0 sur une distance théorique maximale de 80m. Trois batteries remplaçables, lithium CR2477 de 1000mAh chacune, permettent de proposer une durée de vie de 60 mois (Figure 4).

*Figure 4: Beacon Pro Kontakt.io 69*69*21mm [6]*

3) Beacon : Les beacons sont équipés d'un microcontrôleur 32bit ARM (Figure 5). La communication s'effectue par BLE en utilisant la bande des 2.4GHz. Équipés de deux batteries CR2477 de 1000mAh chacun, ces beacons peuvent fonctionner 4 ans avec une période de transfert de 625ms (Figure 5).

*Figure 5: Beacon ouvert Kontakt.io 55*55*15mm [6]*

D. Protocoles iBeacon et EddyStone

Deux protocoles sont couramment utilisés pour la remontée d'information par des Beacons en BLE, qui sont IBeacon et EddyStone. Ces protocoles sont les pivots de l'implémentation du concept de Web physique *(Physical Web)* dont l'objet est de générer des interactions sans contact entre des objets physiques dans une localisation géographique donnée, avec des équipements informatiques de type smartphone. Le principe du *Physical Web* est simple : un beacon émet spontanément et régulièrement une trame BLE, tel un phare signalant sa présence. Le smartphone qui scanne son environnement détecte ce signal lorsqu'il est dans la zone d'action du Beacon. Le message peut contenir des valeurs d'identification de la borne Beacon ou une URL. L'application ouvre l'URL à son utilisateur sous forme de notification, lui permettant d'accéder à la page web. Les deux protocoles d'application iBeacon et Eddystone disposent de différents formats de données présentés Figure 6.

1) iBeacon est le protocole de transfert de données mis en place par Apple en 2013 (non libre de droit). Il transmet notamment les données d'identification uinque du Beacon sur 3 paramètres libres UUID, Major, Minor, et le niveau RSSI à l'émission.

- Proximity UUID (Universal Unique IDentifier sur 16 Octets en hexadécimal)
- Major (2 Octets hexadécimal)
- Minor (2 Octets hexadécimal)
- TxPower (1 Octet) : Puissance du signal à 1 m, permet d'estimer la distance du beacon par le récepteur

2) Eddystone est un protocole de transfert de données développé par Google en 2015, sous licence libre, support du concept de Web Physique avancé par la société. Il permet l'échange de données entre un beacon et un récepteur :

- Namespace (10 Octets Hexadécimal): Équivalent à Proximity UUID de iBeacon (peut être enregistré dans la base Google)
- Instance (6 Octets en Hexadécimal): Équivalent à Major / Minor de iBeacon.

Le protocole EddyStone peut aussi émettre 3 autres types de trames :

- EID (Ephemeral Identifiers): transmet un identifiant crypté temporaire et tournant afin de sécuriser les échanges. Nécessite une connexion à un solver Google dans le Cloud pour décryptage.
- TLM (TeLeMetry) : transmet les informations de télémétrie du beacon (luminosité, température, accéléromètre, batterie).
- URL : transmet une URL de redirection vers un site Web (anciennement supporté par Chrome et Physical Web Browser sur Android) pour les récepteurs à proximité.

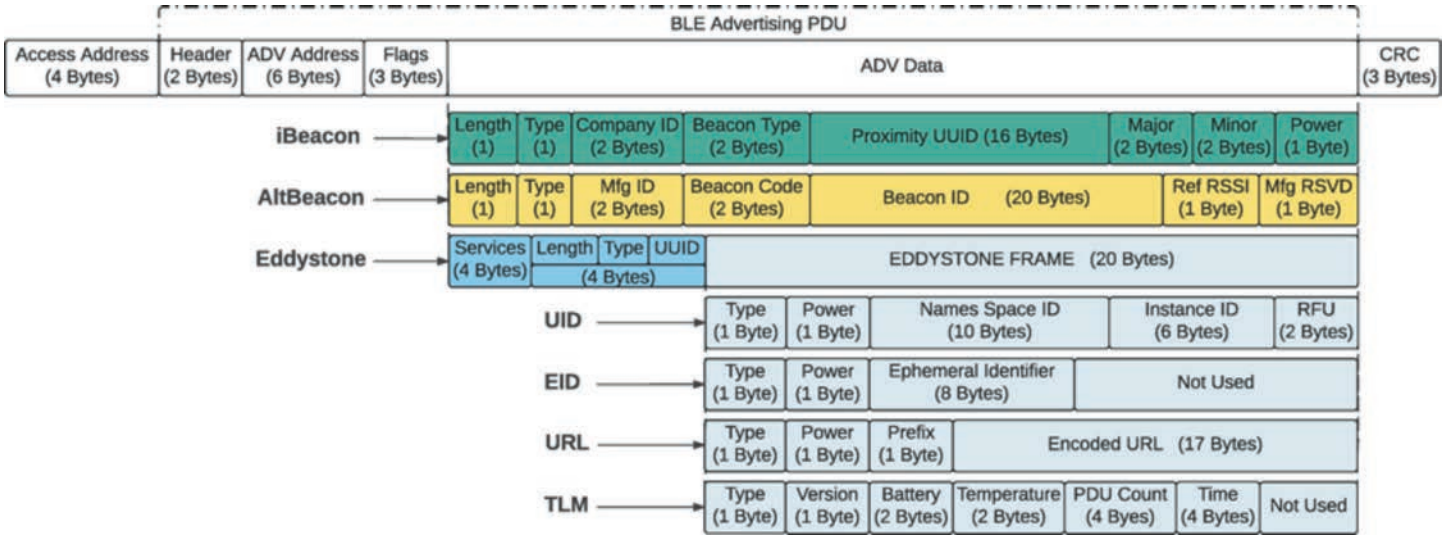


Figure 6: Format des trames iBeacon et EddyStone [5]

F. Application mobile

Kontakt.io propose une application mobile permettant de gérer les beacons et gateways. Il s'agit d'une application d'administration permettant, notamment, d'éditer les configurations des périphériques avec une connexion BLE. Il est important de noter que l'application ne communique pas avec les serveurs de Kontakt pour récupérer les périphériques à proximité mais utilise une connexion BLE locale.

G. API

Comme la grande majorité des plates-formes Cloud, Kontakt.io propose une API (Application Programming Interface ou interface de programmation applicative) permettant de récupérer les informations provenant des beacons et gateways ainsi que diverses informations statistiques. Il est aussi possible de récupérer les informations de télémétrie en utilisant l'API. Les services proposés sont disponibles sur deux adresses différentes : api.Kontakt.io et ovs.Kontakt.io.

L'API proposée par Kontakt.io est une API au format REST *(Representational State Transfer)* créé par Roy Fielding dans les années 2000. Basé sur le protocole HTTP, il permet de standardiser le format d'échange de données entre un client et un serveur. Le client envoie une requête et le serveur, envoie, si la requête est valide, une réponse. Les réponses sont émises sous divers formats, XML, CSS ou, dans notre cas, JSON *(JavaScript Object Notation)*.

Pour sécuriser l'accès à la plateforme de service dans le Cloud, Kontakt.io fournit une clé privée API. La Figure 8 présente une requête curl *(client URL request library)* pour interrogation API en ligne de commande, du service Cloud Kontakt, pour récupérer les données des Devices (Beacons et Gateways) scannés sur un site (place). Trois champs sont requis : URL (Identification serveur Cloud et paramètres d'interrogation), APIKey (Clef privée d'accès), et Accept (format retour).

```
curl "https://api.kontakt.io/device?deviceType=BEACON"
-H 'Api-Key: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
-H 'Accept: application/vnd.com.kontakt+json; version=10'
```

Figure 7: Requête d'identification des Devices en proximité

La Figure 8 montre la réponse fournie par le Cloud Kontakt.io, volontairement limité en taille aux données d'un seul Beacon_Pro car les données JSON retourné peuvent faire plusieurs kilo-octets selon le nombre de beacons et gateways visibles. Des filtres peuvent limiter l'ampleur de la requête. On y perçoit les caractéristiques suivantes : tag vfay, BEACON_PRO, "batteryLevel": 94%, et pour la partie protocole iBeacon "proximity":"00000000-0000-0000-1111-000000000000", "minor": 3, ,"major": 0 et pour le protocole Eddystone, instanceId":"000000000003, "minor": 3, "major": 0, et url": "036269742e6c792f3270507a704a71"(une URL en ASCII raccourcie codée au format bit.ly)

"devices": [{"venue": null,"metadata": {},"access": "SUPERVISOR","-**minor**": **3**,"orderId": "xxxxx","rssi0m": [0,-43,-40,-54,-31,-28,-24,-18], "ownerId":"3f3029e1-8c02-4a57-99d7-2f5cc8c30ac7","mac": "E8:3D:67:0C:5B:6C", "packets":["EDDYSTONE_URL","IBEACON","KONTAKT_TLM","KONTAKT"], "shares": [{"access": "EDITOR","managerMail":"eddy.bajic@univ-lorraine.fr","expirationDate": null}],"txPower":3,"**instanceId**":"**000000000003**","temperatureOffset": 0,"**major**": **0**,"accelerometer": {"doubleTap": {"timeLimit": 0,"timeWindow": 0,"detectionFlags": [],"threshold": 0,"timeLatency": 0},"features": ["Z_AXIS","Y_AXIS", "MOVE_DETECTION","ACCELEROMETER","X_AXIS"],"move":{"duration":160,"detectionFlags":["X_POSITIVE","Z_POSITIVE","Y_POSITIVE"], "detectionFlagsJunction": "OR", "threshold" : 240},"highPass": {"mode": "NORMAL","reference":0,"accelerometerData": false,"-moveDetection":true, "cutOffFrequency": 0.05,"doubleTapDetection":false},"sensitivity": 16,"preset": "MOVEMENT"},"actionsCount": 0,"**alias**": "**Chariot 3**","model": "**BEACON_PRO**","id": "59c6331e-10c2-40ec-9020-39d4a6b78cd4","powerSaving": {"moveSuspendTimeout":null,"features": ["LIGHT_SENSOR","RTC"], "powerSaverAdvertiseInterval":3500,"lightSensorHysteresis":5,"lightSensorThreshold": 30},"firmware": "1.12","customConfiguration": null,"lat": 48.6637443,"**batteryLevel**": **94**,"deviceType": "BEACON","rssi1m": [0,-84, -81, -82, -72, -69, -65, -59],"lng": 6.1569563,"shuffled": false,"profiles": ["IBEACON","EDDYSTONE"],"specification": "STANDARD","managerId":"3f3029e1-8c02-4a57-99d7-2f5cc8c30ac7", "**url**": "**036269742e6c792f3270507a704a71**","**tags**": ["**chariot**"],"secureNamespace": "11111111111111111111","deployedLat": 48.66367362398187, "secureProximity":"00000000-0000-0000-1111-000000000000","lastSeen": 1539686700,"deployedLng": 6.1567358672618875,"**proximity**":"**00000000-0000-0000-1111-000000000000**", "futureId": {"EDDYSTONE": [],"IBEACON": []},"name": "**chariot_3**","-namespace": "11111111111111111111","interval": 1000,"queriedBy": "vfay", "eidRotationPeriodExponent": 15,"uniqueId": "**vfay**"},

Figure 8: Réponse JSON à l'identification des Devices d'un site

Il est nécessaire de désérialiser (parser) la chaine de caractères de la réponse JSON selon des classes d'objets structurés pour retrouver les champs ou attributs pertinents et les reformater en numérique pour certains, et permettre in-fine leur exploitation logicielle.

V. Acces aux données IOT par BROKER MQTT

Le protocole MQTT (Message Queuing Telemetry Transport www.mqtt.org) a été inventé en 1999 par Andy Stanford-Clark (IBM) et Arlen Nipper (Cirrus Link), pour des besoins de connexion de pipelines à des satellites, sous contraintes d'énergie minimale sur batterie, et de faible bande passante. Libre de droit depuis 2010, il est devenu le standard émergeant pour la gestion du flux de données IoT, permettant de remonter et mettre à disposition des informations, avec une consommation de bande passante réseau faible. MQTT est reconnu par OASIS [13] (Organization for the Advancement of Structured Information Standards). Ses caractéristiques sont :

- Modèle Publisher / Subscriber (Pub/Sub)
- Modèle Client Serveur TCP-IP (Routable et Fiable)
- Qualité de Service (Garantie d'acheminement)
- Code léger (client léger embarquable)

A. Modèle publieur/souscripteur

MQTT implémente un modèle d'échange de données de type Publieur/souscripteur (Publisher/Subscriber) selon une communication TCP-IP client-serveur (Figure 10). Un équipement communicant ou plus généralement une passerelle gérant un réseau d'équipements communicants, établit une connexion TCP (port 1883 ou 8083) vers un serveur MQTT appelé "Broker". La connexion peut être sécurisée (cryptage) et authentifiée (login/Password) à partir de la version MQTT 3.1.1 en intégrant le protocole TLS (Transport Layer Security) de cryptage de transport.

Figure 10: Infrastructure de gestion de données par MQTT (inspiré de Source www.HiveMQ.com)

Le broker MQTT enregistre les données publiées (*publish*) par ses clients, chacune étant identifiée par un nom (Topic), une valeur (suite libre de caractères ASCII souvent au format JSON Java Script Object Notation www.json.org) et un horodatage.

Ensuite, un autre client, voire de multiples clients peuvent se connecter au Broker, sous authentification, et s'abonner (*subscribe*) aux données identifiées par leurs Topics. Le broker enverra alors à chaque client abonné, les valeurs des topics auxquels il s'est abonné, dès qu'il y aura eu une nouvelle publication de topic, même si la valeur n'a pas changé. C'est donc un processus asynchrone qui occupe au minimum la bande passante réseau, et ne surcharge pas le client par des requêtes d'interrogation de topic, car il sera informé spontanément par le broker (fonction *Callback*).

B. Données transportées par MQTT et Qualité de Service

Un message MQTT est généralement encapsulé dans une trame Ethernet-TCP-IP et contient la valeur des données communiquées par un device IoT avec 4 attributs *(Topic, Value, QoS, retain value):*

TOPIC : /stream/vfay/health
Nom de la donnée publiée, avec possibilité d'arborescence

VALUE : Contenu de la donnée transmise en JSON.

```
{
 "batteryLevel": 97,
 "deviceUtcTime": 1528201219,
 "externalPower": false,
 "sourceId": "xujQT"
}
```

Le Beacon "vfay" est dans la proximité de la gateway "xuJQT" et dispose d'un niveau de batterie de 95%. La valeur de son horloge Temps réel interne est donnée au format epoch time unix.

QoS (Quality of Service) : Il caractérise le niveau d'agrément entre l'émetteur et le récepteur définissant la garantie de livraison du message entre le client et le broker (le protocole gère les retransmissions pour faire face aux problèmes de fiabilité de réseau). Les Figures 11, 12 et 13 illustrent les 3 niveaux de QoS.

Figure 11: QoS 0 Au plus une fois (Fire and Forget)
(Source www.HiveMQ.com)

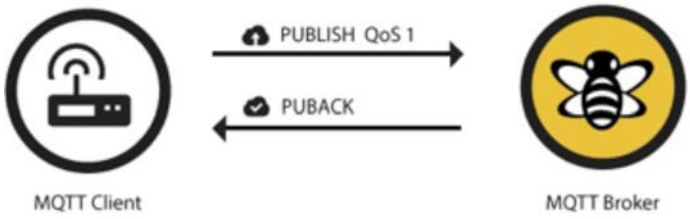


Figure 12: QoS 1 Au moins une fois (Acknowledged Delivery)
(Source www.HiveMQ.com)

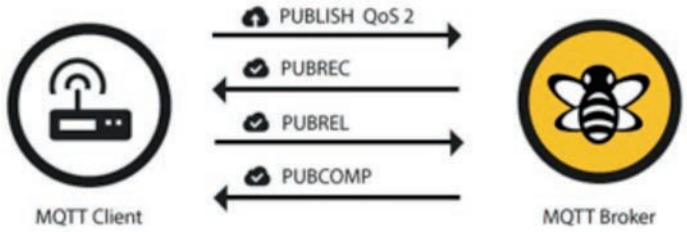


Figure 13: QoS 2 Exactement une fois (Assured Delivery)
(Source www.HiveMQ.com)

RETAIN VALUE : Si vrai, le Broker stocke la dernière valeur du Topic publié et sa QoS. Un client qui s'abonne à un Topic conservé *(retain)* recevra la dernière valeur immédiatement après l'abonnement, sans attendre la prochaine publication.

C. Avantages de MQTT

Le protocole MQTT par sa nature asynchrone, se démarque du traditionnel mode de communication question-réponse, qui opère de façon synchrone, et consomme beaucoup de bande passante réseau. Le mécanisme question-réponse nécessite d'interroger régulièrement le serveur pour disposer de la dernière valeur, alors que MQTT permet d'être informé de celle-ci sans l'avoir requise explicitement à chaque fois, ce qui génère beaucoup moins de trafic réseau.

La méthode publieur/souscripteur de MQTT permet de réduire le trafic au strict minimum qui est :

- la publication d'un *Topic* d'un client vers le Broker *(publish)*, réalisée une fois ;
- la souscription d'un client à un *Topic* d'un Broker, réalisée une fois ;
- l'annoncement du rafraichissement d'un *Topic* du Broker vers le client souscripteur, réalisée à chaque nouvelle publication du *Topic* par le client publieur;

Ainsi, le protocole MQTT permet de gérer un environnement de messagerie de type *Message Oriented Middleware* (MoM) qui permet de découpler les équipements producteurs de données, des applications qui utilisent ces données, avec l'intermédiaire d'un serveur appelé Broker. Citons parmi les brokers MQTT les plus usités, Mosquitto, RabbitMQ (logiciel libre) et HiveMQ (Publique).

Les données utilisateurs transportées par MQQT sont au format libre (ASCII, JSON, XML,...) mais le plus souvent au format JSON, et de taille pouvant aller jusqu'à plusieurs kilo-octets par topic. Cette liberté donne une grande souplesse et versatilité à l'utilisation de Topic MQTT. Tout comme l'interrogation par API, il est nécessaire de désérialiser *(parser)* la chaine de caractères de réponse selon des classes d'objets prédéfinis pour retrouver les champs pertinents et les reformater en numérique pour certains.

VIII. Données MQTT des balises BEACON

Les accès par WebSocket aux données produites par les beacons ne sont pas toujours la meilleure solution pour permettre l'analyse en temps réel de ces données de par l'aspect synchrone des requêtes. La plate-forme de services offre aussi l'accès aux données du moteur de localisation via MQTT de façon asynchrone. Pour recevoir les informations des périphériques beacons ou leurs données de télémétrie, le client MQTT doit se connecter au serveur identifié par :

- Host : ovs.kontakt.io
- Port : 8083 (non habituel pour MQTT-TLS)
- Protocol : MQTTS (TLS 1.2)
- User : .....
- Password : API Key
- Client ID : .....

Les données accessibles via MQTT permettent de connaître toutes les données statiques et dynamiques d'une balise Beacon.

a) Suivi des capteurs internes d'un Beacon :
Topic: /stream/vfay/sensor
Valeur de retour :

```
{"lightLevel":63,
"temperature":25,
"sourceId":"xujQT"}
```

Le Beacon vfay détecté par la gateway "xuJQT" voit une luminosité de 63 lu et une température de 25°C. Ce topic est émis par le Beacon à la période d'émission choisie sur le Beacon lors de sa configuration.

b) Suivi de l'accélèromètre d'un Beacon :
Topic:/stream/vfay/accelerometer"
Valeur de retour:

```
{"sourceId":"KIg18",
"lastDoubleTap":null,
"lastThreshold":140,
"x":1,"y":-1,"z":61,
"sensitivity":16}
```

Les valeurs d'accéléromètre du Beacon vfay sont X, Y et Z, avec une sensibilité configurée à 16 (en mg). Elles permettent de déterminer si la ressource est en mouvement, et de façon statique dans quel sens elle est positionnée (retournée ou non) dans chacune des 3 directions. lastThreshold est le temps (s) depuis son dernier mouvement. lastDoubleTap est le temps depuis le dernier

double appui sur le bouton du beacon. Il a été détecté par la passerelle Klg18.

c) Suivi du niveau de batterie d'un Beacon :
Topic: /stream/vfay/health
Valeur de retour:

{"batteryLevel":100,
"deviceUtcTime":1527602504,
"externalPower":false,
"sourceId":"LXWBF"}

Le Beacon vfay, détecté par la passerelle LXWBF, a un niveau de batterie de 100%, et une horloge interne RTC de valeur définie dans deviceUtcTime au format Unix Epoch.

d) Suivi du bouton d'un Beacon :
Topic:/stream/vfay/button
Valeur de retour :

{"sourceId":"Klg18",,
"lastSingleClick":26}

Il s'est passé 26 secondes depuis le dernier appui sur le bouton du Beacon vfay détecté par la passerelle Klg18.

IX. Données MQTT des passerelles

Chaque passerelle (gateway) Kontakt.io reçoit les messages iBeacon ou EddyStone des Beacons en proximité BLE, et renvoie les données agrégées de tous les beacons en un *Topic* vers le Broker Kontakt.io en utilisant MQTT. La liste ci-dessous montre le message reçu par un abonné (subscriber) au suivi de la passerelle xujQT.
Topic :
/presence/stream/xujQT
Value de retour:

[
{"timestamp":1527601113,
"sourceId":"xujQT",
"trackingId":"**vfay**",
"rssi":-86,
"proximity":"**FAR**",
"scanType":"BLE",
"deviceAddress":"e2:02:00:a0:a6:40"
},
{"timestamp":1527601113,
"sourceId":"xujQT",
"trackingId":"**47:6c:8b:9b:d9:55**",
"rssi":-66,
"proximity":"**IMMEDIATE**",
"scanType":"BLE",
"deviceAddress":"47:6c:8b:9b:d9:55"}]

La passerelle xujQT a détecté 2 équipements BLE aux temps donnés au format Unix Epoch *(timestamp)*. L'une est identifiée **vfay**, avec son adresse bluetooth et niveau de RSSI en réception. Le second équipement bluetooth n'est identifié que par son adresse MAC. C'est un équipement non Kontakt.io, en l'occurence un téléphone portable en mode Bluetooth activé.

Le niveau proximity indique la zone de proximité de l'équipement par rapport à la passerelle, zone estimée par cette dernière avec le RSSI selon 3 catégories IMMEDIATE, NEAR, FAR (Figure 13). Ces 3 valeurs correspondent à des cercles concentriques d'environ 3 mètres de rayon, centrés théoriquement sur le Beacon émetteur. Chacun de ces cercles défini une zone très proche *(Immediate)* à moins d'1 m environ, proche (Near) à moins de 3 m environ, ou éloigné *(Far)* à plus de 3 mètres du Beacon émetteur. Cette méthode d'évaluation de la distance constitue une méthode de géolocalisation grossière - due à la grande variabilité de la mesure de puissance du signal Bluetooth reçu (RSSI) -, appelée Zonage ou *Geofencing*. Cette méthode demeure toutefois d'un grand intérêt pour une grande majorité d'applications de localisation de ressources matérielles.

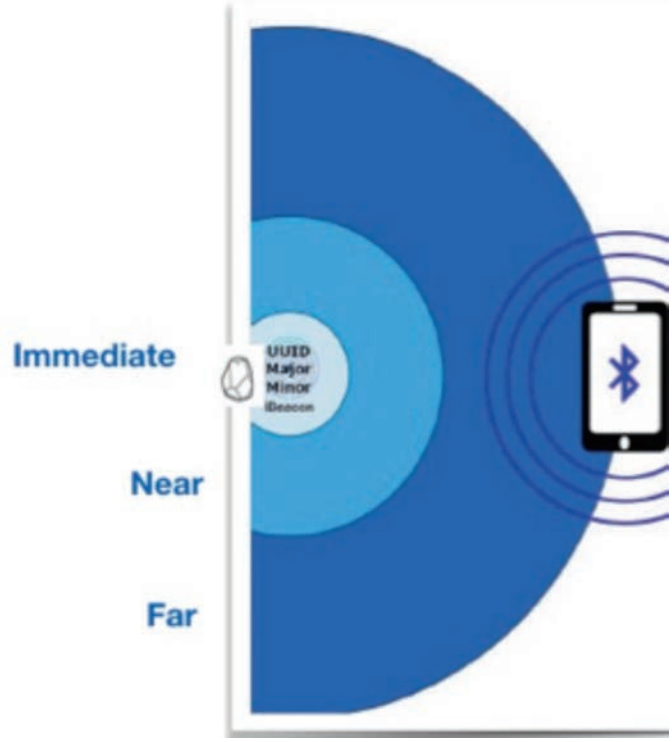


Figure 13 : Approximation de la distance d'un Beacon BLE.

X. Application à la géolocalisation des ressources avec KONTAKT.IO

A. API Application Programming Interface

L'interface API de Kontakt.io fournit toutes les informations concernant l'identification, l'état, les données capteurs et batterie, et la localisation des beacons.

B. Location Engine

La location Engine est fournie par Kontakt.io afin de récupérer des informations sur la présence de périphériques BLE à proximité des récepteurs (gateways). Pour utiliser cette fonctionnalité, il faut disposer d'un abonnement actif à Kontakt.io ainsi que d'un abonnement au *Location Engine*. Les services de *Location Engine* peuvent être utilisés selon 3 modes d'accès différents :
- HTTP (Hypertext Transfer Protocol).
- Web Sockets.
- MQTT (Message Queuing Telemetry Transport).

Tous ces services fonctionnent sur le serveur ovs.kontakt.io, et permettent de récupérer toutes les informations associées aux Beacons dont les coordonnées latitude et longitude de l'objet des gateways. Il est aussi possible de récupérer la puissance du signal reçu par les gateways pour chaque Beacon *(RSSI Radio Signal Strength Indicator)*.

C. RSSI

Le RSSI (Received Signal Strength Indicator) représente la puissance de réception d'un signal d'un beacon depuis une gateway. La valeur du RSSI dépend de deux facteurs, premièrement, la puissance d'émission initiale et deuxièmement, la distance de la source du signal à la gateway Le RSSI mesuré en réception est "globalement" proportionnel à la distance en valeur absolue. Pour une puissance d'émission fixée à +4dBm, le RSSI mesuré varie entre -26dB (distance de quelques centimètres) et -100dB (au-delà de 50 mètres).

Le RSSI est utilisé pour approximer la distance séparant un beacon d'une gateway. On utilise dans ce cas la formule suivante [4] :

$$RSSI = - \alpha \log(d) + K$$

soit :

$$d = 10^{\frac{RSSI - K}{\alpha}}$$

Avec α le facteur de perte, K une constante de signal à 1m, et d la distance en mètre. Il est important de savoir que l'environnement a une grande influence sur les valeurs de RSSI. Les perturbations électromagnétiques, l'absorption ou la diffraction des ondes, la présence d'obstacle quelconque et la distance vont faire fluctuer les mesures de RSSI.

D. RSSI à 1 mètre

Un étalonnage des mesures RSSI est nécessaire. Le RSSI à 1 mètre est une valeur étalon à mesurer expérimentalement à 1 mètre du beacon avec un scanner Bluetooth sur smartphone. À partir du RSSI à 1 mètre on calcule la distance selon la formule [10] :

$$d = 10^{\frac{RSSI1m - RSSI}{10*N}}$$

Avec RSSI1m, le niveau de signal reçu à 1m pour la puissance d'émission donnée, RSSI le RSSI mesuré, N une constante dépendant de l'environnement et d la distance en mètre.

E. Géolocalisation par tri-latéralisation

Il s'agit d'une méthode mathématique permettant de déterminer la position relative d'un objet en utilisant la géométrie des triangles, des cercles ou des sphères [11]. Il s'agit d'une méthode différente de la triangulation qui utilise des angles. Dans le cas de la tri-latéralisation, il est nécessaire de connaître au moins deux points de références.

Notre cas d'étude utilise trois récepteurs gateways, placés à des endroits précis et connus, en bleu sur la Figure 14. Le plan est mis à l'échelle ce qui permet de connaître la distance séparant chaque gateway. Les points verts sont les Beacons dont les positions ne sont ici pas réalistes.

Figure 14: Carte de placement des gateways

Kontakt.io permet aussi de placer le plan de la salle sur une carte satellite pour un rendu réaliste. Cela permet de connaître l'emplacement géographique physique des gateways (latitude et longitude), et par conséquent d'estimer ceux des beacons captés par les gateways.

La Figure 15 présente un exemple [12] permettant de localiser l'intersection des trois cercles.

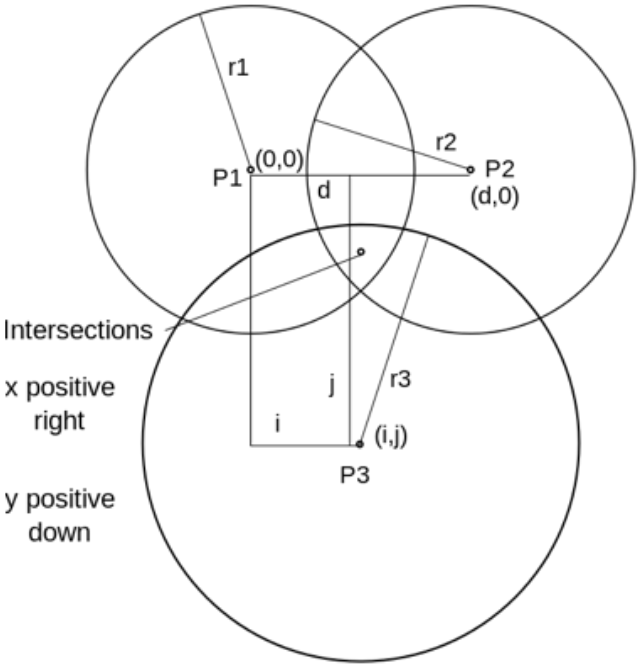


Figure 15: Exemple simple de trilatéralisation

Compte tenu des données précédentes on peut obtenir les trois équations de cercles suivantes :

$$r1^2 = x^2 + y^2$$
$$r2^2 = (x - d)^2 + y^2$$
$$r3^2 = (x - i)^2 + (y - j)^2$$

Ou utilise les deux premières équations pour isoler x :

$$r_1^2 - r_2^2 = x^2 - (x - d)^2$$
$$r_1^2 - r_2^2 = x^2 - (x^2 - 2xd + d^2)$$
$$r_1^2 - r_2^2 + d^2$$
$$x = \frac{r_1^2 - r_2^2 + d^2}{2d}$$

On remplace x dans la première équation pour trouver y :

$$y^2 = r_1^2 - \frac{(r_1^2 - r_2^2 + d^2)^2}{4d^2}$$

$$y = \frac{r_1^2 - r_3^2 + i^2 + j^2}{2j} - \frac{i}{j}x$$

Nous avons une solution [x , y] satisfaisant les trois équations. Dans notre cas (pour localiser un beacon), il faut modifier ces équations en prenant en compte le calcul de la distance par le RSSI. De plus, dans notre cas, les distances sont exprimées de centre à centre.

XI. Conclusion

Comme nous l'avons présenté, l'Internet des Objets est un domaine en plein développement tant sur les applications grand public que dans le secteur industriel. L'IoT ouvre de nouveaux horizons pour les applications industrielles, et contribue à la réalisation de l'usine du futur : suivi de ressources, monitoring de machines, géolocalisation et traçabilité, maintenance préventive, sécurité, communication homme-ressource, etc... La problématique abordée dans cet article concerne la faisabilité d'un système de localisation de ressources industrielles en utilisant des objets communicants selon le standard Bluetooth Low Energy (BLE). Nous avons présenté les architectures IoT, les principales plateformes de services Cloud, et le fonctionnement pratique d'une infrastructure IoT exploitant des objets communicants de type Beacon Bluetooth Low Energy. Il est possible d'utiliser les services centralises de localisation (Location Engine) dans le Cloud, au travers de requêtes API Restful en mode question-réponse, ou par des connexions MQTT en mode publieur/souscripteur. La méthode permettant de localiser des Beacons associés à des ressources industrielles est d'utiliser le niveau de signal RSSI, et d'effectuer une trilatéralisation en utilisant les positions fixes connues des passerelles installées dans l'environnement. Le problème dans l'utilisation du RSSI est son irrégularité, qui entraîne une faible précision, étant soumis aux aléas des transmissions par ondes radio (réflexion, absorption, ...) en créant une forte variabilité de puissance des signaux mesurés en réception. Les ondes radio sont soumises à d'importantes perturbations provenant de leur environnement ce qui peut fausser les résultats. La géolocalisation se résume alors à la détermination de la présence de Beacon dans des zones selon 3 catégories : IMMEDIATE, NEAR, FAR selon la méthode dite de zonage (Geofencing). L'avantage des Beacons BLE est leur faible coût de déploiement mais ils n'offrent pas de géolocalisation précise. D'autres méthodes telles que Ultra Wide Band (UWB) permettent une géolocalisation très précise, en s'appuyant sur la mesure de temps de propagation (TDOA Time Difference Of Arrival) entre des beacons et les passerelles proches, qui doivent être synchronisées temporellement de façon très précise. La solution Beacon BLE apporte toutefois des services de localisation suffisant pour une grande majorité de cas d'applications industrielles, ne nécessitant généralement que la notification de présence ou absence de ressources dans une zone ou dans un environnement donné.

Comparé à l'accès aux services d'une plateforme dans le Cloud par requêtes HTTP API RESTful, le protocole MQTT, léger et rapide, constitue une solution d'accès aux données des objets, simple de mise en œuvre avec des clients légers, et suffisamment réactive sans consommer de bande passante importante du réseau. Le protocole MQTT s'impose de plus en plus comme le protocole privilégié pour l'accès distant aux données des objets connectés d'une infrastructure IoT.

Références

[1] H. Rheingold, "Foules Intelligents" , M21 Editions, ISBN : 2-9520514-2-9, 2005

[2] E. Bajic, B. Auriac, G. Koenig : "Objets Connectés Industriels : Identification et Géolocalisation dans une Infrastructure Internet des Objets » http://www.koenigguillaume.me/portfolio2/files/PIDR.pdf

[3] F. Samie, L. Bauer and J. Henkel, IoT Technologies for Embedded Computing : A Survey, IEEE International Conference on Hardware/Software Codesign and System Synthesis, 2-7 October 2016 Pitsburg, USA.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, Internet of Things : A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communications Surveys & Tutorials Journal, Vol. 17, No. 4, 2015, pp. 2347-2376.

[5] https://kontakt.io/

[6] https://aws.amazon.com/fr/iot/

[7] https://azure.microsoft.com/fr-fr/

[8] https://cloud.google.com/solutions/iot/?hl=fr

[9] L. Hernández-Rojas, M. Fernández-Caramés, P. Fraga-Lamas and Car- los. J. Escudero, Design and Practical Evaluation of a Family of Light-weight Protocols for Heterogeneous Sensing through BLE Beacons in IoT Telemetry App., Sensors Journal Vol.18, No.1, 2018.

[10]https://iotandelectronics.wordpress.com/2016/10/07/how-to-calculate-distance-from-the-rssi-value-of-the-ble-beacon/

[11] https://en.wikipedia.org/wiki/Trilateration

[12]https://en.wikipedia.org/wiki/Trilateration#/media/File:3spheres.svgs

[13]https://www.oasis-open.org/news/announcements/mqtt-version-3-1-1-becomes-an-oasis-standard

L'Esplanade Charles de Gaulle - Nîmes

HORIZON SCIENCES HUMAINES

Le DUT GEII par apprentissage à l'IUT de Nancy-Brabois

Franck Joly *(IUT Nancy-Brabois)*

La mise en place des licences professionnelles dans les départements d'IUT a constitué la première incursion de l'alternance dans nos formations, tout d'abord avec le contrat de professionnalisation, supplanté depuis quelques années, sous l'impulsion des politiques publiques, par le contrat d'alternance. Prévu dès le départ comme une modalité possible, les maquettes pédagogiques des 3 licences professionnelles portées par le Département GEII de l'IUT Nancy-Brabois ont d'emblée été construites pour permettre à l'alternance et à la formation initiale de cohabiter dans un unique dispositif, ce n'était pas le cas pour le DUT.

La possibilité de proposer le DUT GEII par apprentissage est apparue comme une opportunité dans un contexte favorable, qu'il fallait saisir, et ce dès 2012, lorsque Jean-Marie JEHL a été chargé d'évaluer la pertinence, puis de mettre en œuvre les cadres permettant le fonctionnement de cette nouvelle voie.

D'abord proposée en 2013 pour réaliser la 2e année de DUT, cette formation a accueilli en 2018 sa 3e promotion en 1re année de DUT. Un fonctionnement qui ne s'est pas fait sans rencontrer des difficultés dans le recrutement, mais aussi dans la mise en œuvre pédagogique, peut-être en passe d'atteindre aujourd'hui un régime stationnaire avant les modifications du DUT et son passage à 3 ans.

Quels sont les enjeux de cette proposition de formation ? Comment le département a-t-il géré la mise en place de la formation GEII par apprentissage ? Quelles sont les difficultés auxquelles se heurte le département ? Quelles orientations possibles sont envisageables pour pérenniser la formation par apprentissage ?

Construire un dispositif

Contrairement aux licences professionnelles, le DUT GEII n'a pas été pensé pour être proposé en alternance, la première conséquence est la nécessité d'un dispositif autonome et parallèle à la formation initiale. Cette modalité de par ses spécificités implique aussi des adaptations tant au niveau de son déroulement calendaire que dans son déroulement pédagogique. Comme pour le stage, un lien spécifique doit être mis en place entre l'équipe pédagogique et l'entreprise pour assurer le bon déroulement et un canal d'échange tout au long des deux années du diplôme.

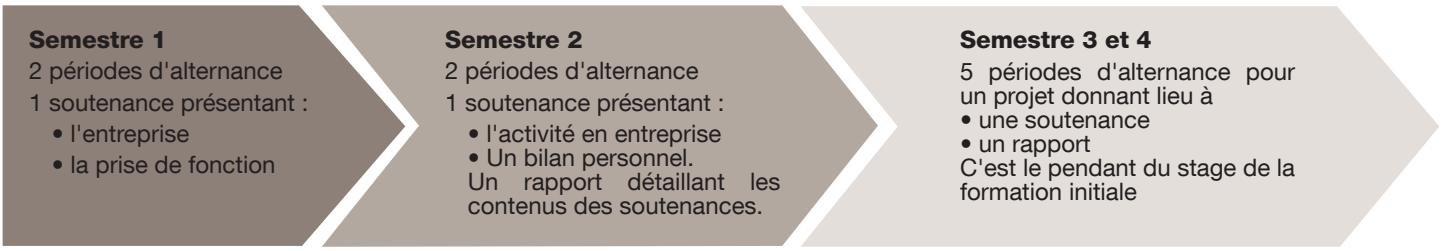
Le calendrier d'alternance

Un apprenti de 1re année passe 28 semaines à l'IUT et 24 semaines en entreprise alors que cette répartition est inversée pour un apprenti de 2e année, ce qui donne en moyenne une répartition équitable des temps alternés — il est à noter qu'en tant que salarié à part entière de l'entreprise, l'apprenti bénéficie de 5 semaines de congés payés par an qui sont pris sur le temps en entreprise. Les phases d'alternance en entreprise pendant l'année universitaire sont constituées de 3 à 4 semaines et recouvrent systématiquement les vacances scolaires. Ce découpage des semestres universitaires nécessite aussi un emploi du temps spécifique et un agencement de chaque module compatible avec les périodes de présence à l'IUT ; cette opération est bien évidemment transparente au regard du PPN et n'entame en rien l'intégrité des modules.

Le groupe d'alternants n'est mis en place qu'à la fin de la première période du début d'année ; les nouveaux étudiants constituent une unique promotion pour quelques semaines de formation. Il est ainsi possible aux candidats à l'alternance qui n'auraient pas encore signé un contrat de poursuivre leur recherche (voire à des étudiants inscrits en formation initiale de réaliser le passage en apprentissage) ou de finaliser la mise en place ; d'autre part, cette uniformisation temporaire permet la création de liens entre les étudiants des deux dispositifs. Un fonctionnement identique est mis en œuvre pour la 2e année.

La mise en œuvre du PPN

L'alternance demande un temps qui n'est pas entièrement dégagé par l'utilisation des vacances, aussi certains modules à caractère professionnel (projet tutoré, étude et réalisation, stage) ou en rapport direct avec le monde de l'entreprise (PPP, connaissance de l'entreprise) ont été « déportés » en partie dans l'entreprise en considérant que la compétence est acquise dans le cadre du travail en alternance. L'évaluation en est alors confiée au tuteur par le biais de certains des critères des évaluations semestrielles et aussi à travers les différentes soutenances et rapports demandés en fin de semestre.



Pour le PPP, la situation même de l'apprenti permet de supposer que la réflexion menée dans le cadre du PPP a été faite et que ce module est en grande partie sans utilité, c'est donc naturellement que ce module n'est évalué qu'à travers un travail d'écriture sur le projet post-DUT ; nous reviendrons sur ces considérations plus tard.

La simplicité de cet exposé cache en fait la complexité d'évaluer et de faire évaluer par les tuteurs de manière régulière et équitable, des activités loin des salles de TD/TP de l'IUT.

Le suivi

La désignation d'un enseignant qui suivra l'apprenti durant la formation de l'apprenti permet d'instaurer une relation de confiance et d'échange avec le tuteur, de pouvoir mener conjointement des évaluations semestrielles, faire des bilans sur les résultats académiques, pour conduire à un encadrement conjoint de l'apprenti. De plus des soutenances semestrielles sur des thèmes dédiés, dont le stage, auxquelles le tuteur assiste, constituent des étapes importantes dans le suivi et permettent des échanges profitables entre le monde de l'entreprise et le monde de la formation.

L'apprenti est aussi porteur d'un livret d'apprentissage qui présente les contenus et les jalons de la formation au tuteur et propose une interface traditionnelle ; son utilisation n'est pas systématique.

Le CFA, interne à l'université, assure quant à lui le suivi administratif. Pour l'instant, ces deux aspects du suivi sont dissociés, or certains points, comme la gestion des absences en formation, nécessiteraient une réelle intrication.

Construire des promotions

La mise en place de l'alternance passe par la création d'un groupe spécifique dont la taille maximale a été fixée pour chaque année à 14 places, soit un groupe de TP. La taille minimale est quant à elle dictée par la viabilité financière, soit 6 places (cette taille est aussi la masse critique nécessaire à la synergie et à l'activité pédagogique de groupe).

Une première expérience : la 2e année de DUT par apprentissage

Ce n'est pas sans difficulté que la formation GEII en apprentissage s'est mise en place au département de Nancy-Brabois. C'est tout d'abord le choix de la 2e année par apprentissage qui a été fait : les étudiants ayant validé la première année de DUT disposent alors d'un bagage intéressant pour pouvoir être intégrés dans une entreprise du secteur GEII. Ce point est un argument en faveur des candidats auprès des entreprises, puisqu'opérationnels et triés par le Département, mais ferme aussi la possibilité d'intéresser des grands groupes comme Orange ou RTE dont la politique de recrutement se focalise sur des contrats de 2 ans.

Le dispositif d'accompagnement à la recherche du stage de 2e année porté par l'enseignement de communication et une forte sollicitation des relations avec les secteurs professionnels et industriels locaux ont permis d'aboutir à un premier groupe de 9 étudiants pour la rentrée 2014. Cette première expérience a mis en évidence la difficulté de concilier les attentes des entreprises en matière de profils et de compétences d'une part, les souhaits et les contraintes des quelques candidats d'autre part.

La suite logique : des promotions sur deux ans

Ouvrir la formation par apprentissage dès la première année était un objectif à court terme d'autant plus évident que la conjoncture à tout point de vue est, depuis quelques années maintenant, favorable à l'apprentissage dès l'entrée dans le supérieur ; pour nous, l'ouverture des deux années permettrait d'intégrer verticalement la filière par apprentissage, d'offrir deux points d'accès, et ainsi pérenniser financièrement en augmentant le flux de candidats tout en répondant aux attentes de grands groupes mentionnés ci-dessus. La mise en place a donc commencé par le recrutement.

La sélection des dossiers des candidats à la 1re année de DUT met en jeu la crédibilité du département auprès des futures entreprises d'accueil. Il convient donc de redoubler d'attention dans la sélection ; aux critères standards pour un recrutement en formation initiale (implication, capacités et comportement), s'ajoutent la pertinence de la démarche et l'aptitude à évoluer dans une entreprise — il est assez aisé de comprendre que ces deux derniers points sont intangibles et relèvent d'une perception au-delà de la simple lecture. Aussi, après une étape de sélection, deux types de candidats se distinguent : ⅔ sélectionnés, ⅓ convoqué en entretien. Pour la rentrée 2018, 44 candidats ont été sélectionnés pour un projet d'ouverture de la section à 14 places.

Parallèlement la possibilité de passer de la 1re année en formation initiale à la 2e année en alternance est toujours offerte, sous condition.

Cette phase ne se limite cependant pas à cette sélection des candidats et leur capacité à trouver l'entreprise qui les accueillera alors que pour la plupart, ils sont dans la phase de préparation du BAC. Ainsi deux aides à la recherche leur sont proposées :

- Des pistes de recherche et des offres d'apprentissage gérées par le Département qui sont mises à disposition des candidats retenus ; ces offres ayant été soit obtenues par sollicitation des entreprises partenaires pour les stages, soit reçues par le biais de différents canaux (demande d'information directe, CFA, organisme de recrutement mandaté…), mais aussi à l'issue d'une campagne de collecte de la taxe d'apprentissage.
- Des conseils et des informations sur les différents dispositifs et l'organisation de la formation, une aide à la rédaction des documents de candidature ; cette dernière action permet en particulier de rencontrer les candidats et de leur démontrer un soutien dans une expérience nouvelle pour des jeunes lycéens en passe d'entrer dans la vie active.

On voit donc que mettre en place une formation par apprentissage demande de l'énergie à une équipe si elle veut voir la formation ouvrir : une gestion du calendrier pour contacter les entreprises au bon moment, une gestion des candidats qui doivent avoir les outils nécessaires pour candidater dans les entreprises, mais aussi suffisamment de motivation pour aller au bout de leur recherche, de la communication avec les entreprises pour proposer des candidats et encadrer la recherche des étudiants qui ne peut se faire, en réalité, sans un appui des formateurs et une bonne communication autour de la formation GEII.

Vers le régime stationnaire ?

Aussi, la formation en apprentissage en GEII a vu des fluctuations annuelles, de l'implication du département et du partenariat avec le CFA ; le bilan pour le département GEII de Nancy-Brabois est donc d'une promotion d'apprentis de 2e année en 2013, une promotion d'apprentis de première année en 2015, une promotion de 2e année en 2016, une promotion de première année en 2017. Pour la rentrée 2018, les deux années devraient enfin être ouvertes simultanément :

- la 2e année dans le prolongement de 1re année actuelle, augmentée de quelques transfuges de la formation initiale,
- une nouvelle 1re année avec plus de candidats (23 en 2017/44 en 2018), plus d'offres dont celles de groupes nationaux demandeurs d'alternants sur deux ans.

De l'origine des candidats

Avant de clore ce descriptif, il convient présenter quelques chiffres issus des 3 années de fonctionnement, avec une projection sur l'année 2018-2019 pour la promotion actuellement en 1re année et reposant sur les résultats obtenus.

	Série S	Série STI		Série S	Série STI
Inscrits en 1re année	7	11	Inscrits en 2e année ou dont la 1re année est en passe de validation	12	8
Échec ou en difficulté en fin de 1A	0	6	Ayant obtenu ou ayant de grandes chances d'obtenir le DUT	12	8
Avec une 1re expérience dans le supérieur	3	2	Avec une 1re expérience dans le supérieur	3	3

Il est difficile de mener une analyse consistante sur un ensemble de données aussi restreint, cependant elles semblent confirmer quelques évidences dont les explications peuvent être empruntées à la formation initiale ou tout simplement relever du bon sens.

- Avoir un BAC S offre de meilleures chances de réussite en fin de première année, mais n'est plus un avantage notable en 2e année : les apprentis issus de BAC STI qui n'adaptent pas leur attitude face au travail personnel se trouvent assez rapidement en situation d'échec, cette situation est d'autant plus critique que le comportement et le travail en entreprise peuvent être adaptés au regard du tuteur. Il convient donc de mettre en place des garde-fous à « déclenchement rapide » pour ne pas laisser une situation paradoxale se mettre en place en 1re année.
- Intégrer l'apprentissage en 2e année est une opération gagnante : l'étudiant qui passe la 1re année a une base technique solide qui peut séduire les entreprises attendant des apprentis quasi opérationnels pour un engagement moins important dans la durée, mais aussi l'accompagnement, à l'instar des apprentis de licence professionnelle qui gardent cependant l'avantage d'une première expérience professionnelle.
- Avoir eu une première expérience dans le supérieur est souvent synonyme de premier échec et de réflexion constructive sur sa réorientation : le choix de l'apprentissage s'appuie sur un projet et la poursuite d'un objectif, ce qui peut faire défaut aux néo-bacheliers ; ce point met en évidence l'intérêt d'appuyer le recrutement en première année sur des dispositifs universitaires de type « rebond » ayant pour objectif de préparer la réorientation à l'issue d'un échec en semestre 1 : les possibilités d'apprentissage sont présentées aux participants d'une formation, ceux qui s'orientent vers cette modalité sont soutenus et démontrent leur motivation à travers la recherche préalable d'un contrat.

Les deux derniers points démontrent l'intérêt d'entrer dans l'apprentissage « en pleine conscience », des solutions restent à mettre en place pour répondre à la situation évoquée dans le premier point.

En guise de conclusion

Mettre en place le DUT GEII par apprentissage est donc une expérience enrichissante qui doit maintenant entrer dans sa phase adulte. La maturation du dispositif est en passe d'atteindre son terme et les publics, étudiants et professionnels, sont circonscrits ; cependant, l'exigence de l'apprentissage, la gestion de l'alternance des périodes et des rôles (bien que connue) et la construction d'une « identité d'apprenti » se sont révélées, lors du fonctionnement du dispositif, comme des questions auxquelles nous allons devoir apporter des réponses adéquates en mettant en place, par exemple, un PPP spécifique proposant des interventions/activités propres à susciter une réflexion et une réaction des apprentis concernés ou encore une présence plus marquée du tuteur sur la supervision de la partie formation.

Franck JOLY, ***professeur agrégé de mathématiques, Département GEII, IUT Nancy-Brabois, Université de Lorraine***

Arènes de Nîmes

Projets tuteurés : une opportunité pour tisser du lien socio-économique

Taha BOUKHOBZA *(IUT Nancy-Brabois, Université de Lorraine)*
Denis CRONEL *(Centre interarmées de la solde, Défense Nationale)*
Cédric JOIN *(IUT Nancy-Brabois, Université de Lorraine)*
Christophe SIMON *(IUT Nancy-Brabois, Université de Lorraine)*

Depuis quelques années, au département Génie Electrique et Informatique Industrielle de l'IUT Nancy-Brabois, certains projets tuteurés se font en partenariat avec diverses institutions ou associations locales. Evidemment, cela est couteux en temps, en énergie et ne mobilise pas nécessairement l'ensemble de l'équipe pédagogique, mais l'espoir d'apporter une expérience intéressante et utile aux étudiants a permis de développer ces activités « concrètes ».
Dans cet article, nous allons relater cette expérience et essayer de partager nos conclusions. Les aspects techniques seront peu abordés mais, évidemment, nous restons à la disposition de la communauté pour toutes informations complémentaires.

I. Genèse

Un premier projet est né suite à une réflexion pédagogique sur le module de projet tuteuré en Licence Professionnelle Systèmes Automatisés et Réseaux Industriels (SARI), des besoins en technicité des étudiants venant d'horizons multiples et de la nécessité de concrétiser l'enseignement de la gestion de projets. L'idée de développer une flotte de drones 'from scratch' a été imaginée comme facteur de motivation et surtout parce que nous y retrouvons des domaines de compétences de la Licence Professionnelle : instrumentation, communication industrielle, informatique industrielle, automatique … Quelques premiers investissements ont permis de démarrer le prototypage de solutions à base de matériel arduino et de shields. La concomitance du lancement d'un appel à projets formation innovante par la région Lorraine et de l'Université de Lorraine en 2015 pour l'acquisition de matériel pédagogique a permis de démarrer un projet de plus grande ampleur. Il a été demandé dans le cadre de cette demande de subvention, 4 drones différents (Tricoptère, Quadricoptère, HexaCoptère, Octocoptère) ainsi que des tablettes et téléphones portables pour y développer des applications permettant la supervision et le contrôle. Deux personnes portaient le projet : Christophe SIMON (responsable de la licence professionnelle) et Denis CRONEL (vacataire professionnel, fonctionnaire du ministère des Armées, en charge des enseignements de gestion de projets en LP à l'époque). Le projet a été financé à hauteur de 16k€.

En parallèle, entre 2014 et 2015, les départements GEII et Génie Mécanique et Productique (GMP) ont collaboré pour concevoir et réaliser un banc d'essai pour des revêtements multicouches aluminisés destinés à se protéger des conditions de chaleur extrême. Cette prestation, pour le compte de l'entreprise EDC Protection a essentiellement été menée par des enseignants et les personnels techniques des départements, même si l'interface de supervision et l'exploitation des mesures ont été proposées en tant que sujet d'Etudes et de Réalisations (ER) pour des étudiants de 2ème année de DUT GEII. La réussite de cette prestation, la satisfaction de l'entreprise mais aussi l'intérêt que cela a suscité auprès des étudiants qui se sont réellement engagés, a été au-delà de ce que nous attendions. Cela nous a encouragés à poursuivre dans cette voie. En effet, sans enlever le bénéfice financier que les départements ont retiré de cette prestation (EDC depuis nous verse toujours de la taxe d'apprentissage), il nous a semblé que ce type de projets pouvait motiver nos étudiants, les faire travailler sur des projets concrets avec une finalité sociétale et pour le département de tisser du lien socio-économique.

Le département s'est depuis lancé dans plusieurs aventures et continue à rechercher des projets et des partenaires.

Dans la section suivante, nous décrirons quatre de ces projets.

II. Les différents projets

Le projet Cycl@pe

C'est le tout premier projet tuteuré auquel participent les étudiants de licence professionnelle SARI. Le but est la surveillance de l'évolution de paramètres physico-chimique d'une parcelle de forêt en utilisant la flotte de drones acquise par le département. Il s'agit plus précisément de mettre en service quatre drones permettant de visualiser et(ou) sauvegarder les données suivantes : Pression, Température, Hygrométrie, Taux de CO2, Géolocalisation, Vitesse, Altitude. Le pilotage des drones se fait à vue via une Interface Homme-Machine conçue par les étudiants et compatible avec différents supports (tablette, smartphone ou ordinateur portable). Au vu des réglementations en vigueur, les drones devront voler à une altitude inférieure à 50 mètres. L'autonomie visée est de 30 minutes. Quatre drones constituent la flotte : deux quadricoptères et deux hexacoptères (depuis 2015, la flotte s'est étoffée). La commande se fait au travers d'une carte Arduino et l'expérience. Par ailleurs, la prise en compte de la réglementation par les étudiants a montré qu'il fallait équiper tous nos drones de parachutes et de systèmes type « boîte noire ». Enfin, le vol à vue

induit la diffusion d'un flux vidéo qui est peu compatible avec des composants de type arduino et de nouvelles solutions couplant arduino et raspberry PI ont été imaginées avec les étudiants.

Voici une liste non exhaustive des fonctionnalités proposées par l'interface :

- Récupération des paramètres de vol : Niveau de batterie ; Altitude approximative ; Position GPS (longitude, latitude) ; Récupération et affichage du flux vidéo provenant de la caméra ; Récupération et affichage de la position GPS du drone sur une carte dynamique ; Création et exécution d'une mission (composition d'actions) ; Sauvegarde des coordonnées de décollage ; Sauvegarde des coordonnées d'atterrissage, Récupération et réexécution des missions connues par le drone, analyse et archivage des mesures physico-chimique.

Le contexte du projet qui n'a pas de commanditaire extérieur à l'Université est lié aux activités de recherches prospectées par le Centre de Recherche en Automatique de Nancy sur la surveillance de la bio-diversité dans les forêts aux alentours de la zone d'enfouissement de déchets nucléaires de Bure dans la Meuse.

Evidemment, la description faite du projet relate le cahier des charges de l'année en cours. Cet état d'avancement a été obtenu après cinq années ou plutôt cinq promotions d'étudiants de LP qui ont fait évoluer le projet sous la tutelle d'un enseignant permettant le continuum entre les promotions. En effet, entre 8 et 12 étudiants de LP y consacrent chaque année leurs 150 heures de projets tuteurés. Aussi, non seulement l'aspect technique et technologique était important mais aussi la rigueur dans la gestion de projets permettant de ne pas redémarrer de zéro chaque année. Enfin, le coût financier, au-delà de l'implication d'un enseignant, est, une fois les drones achetés, assez faible et ne dépasse jamais 5 000€ par an. La figure 1 montre un des hexacoptères et un des quadricoptères pilotés par une interface homme-machine développée par les étudiants en Visual C#.

Figure 1 : Hexa et quadricoptère et leur IHM

Projet Chrys@lide

C'est une collaboration avec le Service Départemental d'Incendie et de Secours de Meurthe & Moselle (SDIS 54) qui s'étend entre 2016 et 2020. L'objectif étant, en plusieurs phases, d'équiper un robot mobile radioguidé (sur chenilles) de capteurs permettant aux pompiers d'évaluer la dangerosité d'une zone distante avant une éventuelle intervention. Deux éléments ont été le moteur de ce projet. D'une part, en avril 2012, un officier SDIS54 est décédé lors d'une reconnaissance sous protection respiratoire dans une installation classée « risques phytosanitaires » et, d'autre part le projet cycl@pe en adéquation avec l'attente des pompiers portant sur l'exploration de la zone d'intervention avant la présence des pompiers. L'analyse du problème par les étudiants, sous la conduite des enseignants, a montré qu'une solution à robots chenilles était plus adaptée. Ainsi, pour réduire le risque encouru par les personnels d'intervention, le SDIS54 a décidé de s'équiper de plusieurs robots permettant l'analyse de l'environnement préalable, afin de sécuriser les interventions de ses personnels sur différents terrains opérationnels. Pour l'achat du robot, différentes sources de financements ont été sollicitées : Université de Lorraine, ressources propres de l'IUT Nancy-Brabois mais aussi le ministère de l'intérieur. Une première partie du projet a été justement de rédiger un cahier des charges et de choisir le robot parmi ceux existant sur le marché avec les options garantissant son évolutivité et sa maintenabilité.

En 2017, la somme des subventions récoltées a permis d'acheter le robot (plus de 55k€) qui doit passer une partie de l'année en opération chez les pompiers et le reste de l'année (d'octobre à Mai) en développement à l'IUT. Le robot est visible à la figure 2. L'objectif est de toujours avoir une interaction entre le, SDIS et les étudiants pour améliorer le robot. A cette fin, deux revues officielles (une en septembre et l'autre en mai) sont organisées et un comité de pilotage du projet regroupant des membres du SDIS, l'équipe pédagogique et un chef de projet étudiant a été mis en place. Evidemment, durant les périodes de projets tuteurés, le point est fait régulièrement avec les étudiants.

Figure 2 : Robot Chrys@lide

Le choix des capteurs a déjà représenté une partie importante du projet. Il a demandé une expertise importante du SDIS 54. La détection de neurotoxiques, d'ammoniac, de divers gaz inflammables, de composants radioactifs, ou d'arsenic et de souffre est très importante pour le SDIS. Cependant, notre expérience dans le domaine est faible et les essais pour valider et calibrer les instruments et leurs conditionneurs sont relativement limités au sein de l'IUT. D'autres capteurs qui doivent équiper le robot sont plus classiques à mettre en œuvre tels que les pyromètres, détecteurs de COV mais la détection de gaz de combats est très compliquée. Aussi, l'INRS dont un de ses agents est expert auprès du SDIS a été sollicité. Pour le reste : placements de caméras, déplacements du robot sur divers types de terrains (sable, terrains humides, escaliers ….), communication… représentent des développements plus standards. Leurs tests sont donc effectués sur le site de l'IUT en autonomie.

Ce projet est complet et couvre beaucoup de champs disciplinaires qui vont évidemment au-delà des compétences demandées en GEII. Trois groupes de travail ont été mis en place pour couvrir les différents pans de ce projet. Il s'agit essentiellement d'étudiants de LP SARI mais aussi, pour les parties études, de DUT GEII 2A et de 1A en second semestre afin d'assurer une continuité dans ce projet sur les 4 années. Les aspects gestion de projet et interaction avec le client externe sont là aussi très importants.

Bien que le département n'ait pas tiré profit financièrement de cette coopération, l'acquisition du robot illustrant nos enseignements, le facteur motivationnel des étudiants, lié à l'objectif sociétal sont très positifs. Chaque année les étudiants sont très motivés pour travailler sur ce projet notamment pour l'intérêt humain du projet et cela nous permet de revenir sur des fondamentaux de l'instrumentation de ce robot.

Le projet @SCLEPIOS

En collaboration avec un médecin spécialisé en gériatrie, dont l'objectif est de fournir des solutions technologiques qui aident au maintien à domicile (quand cela ne présente aucun risque évidemment) des personnes âgées handicapées résidants dans des communes éloignées des grandes agglomérations. L'idée est de permettre à la personne âgée de vivre à son domicile dans les meilleures conditions possibles mais aussi de leur faire réaliser des économies, les frais d'hospitalisation (6000 euros par mois en moyenne) ou de maison de retraite (2500 euros en moyenne) qui sont aujourd'hui assez élevés. Ce projet concerne pour l'instant les étudiants de la LP Intelligence Technique et Energétique du Bâtiment (ITEB) mais tire ses fondamentaux dans de l'instrumentation partagée avec les autres formations sur le plan conceptuel.

Pour ce projet, le maître d'ouvrage est un médecin spécialisé en gériatrie. Les étudiants doivent proposer une réhabilitation des domiciles des personnes âgées, incluant des équipements de sécurité (la détection de chute par exemple étant le plus classique.), qui soient adaptés et qui facilitent la vie quotidienne de leurs usagers. Des relevés d'informations diverses (climatiques, intrusion, extinction automatique des plaques de cuisines….) sont transmis en temps réel soit à un centre de surveillance soit à des proches. Des relevés d'informations, de nature médicale, sont récoltés et transmis au médecin traitant. Des actionneurs télécommandés ou supervisés à distance permettant plus de sécurité et/ou plus de facilité (automatisation de plusieurs parties du domicile) font partie de la réhabilitation proposée. Un prototypage des interfaces patient, Médecin et la structure du logement patient est illustré à la figure 3.

Figure 3 : IHM Patient/Médecin et Structuration type d'un logement patient.

Une association d'aide aux personnes âgées handicapées (DOMEVRE-EN-AIDE) a été proposée par les étudiants, et devrait être créée d'ici 2020 en fonction des résultats des études par les étudiants.

Ce projet se poursuit aussi d'années en années et constitue le sujet de projet tuteuré d'étudiants de la LP ITEB en formation initiale. La rénovation effective de certains domiciles de patients demande encore plus de temps et surtout des solutions de financement non abouties à ce jour. L'association à ce projet d'autres départements d'IUT (Génie Biologique Santé par exemple) serait certainement un plus.

Projet HYDROS

Ce projet est développé depuis mars 2017 en lien avec l'association environnementale NEOMYS dont une des études concerne l'analyse et l'évolution des crapauds « Calamite» sur une zone pionnière d'Art-sur-Meurthe. L'objectif est d'analyser le milieu de vie des crapauds (jusqu'à 50 mares à analyser). Le crapaud calamite a besoin d'une certaine température pour pouvoir se reproduire et la proximité entre le site de reproduction et l'homme ne favorise pas la sauvegarde de l'espèce.

Il s'agit plus précisément de concevoir et réaliser des enregistreurs de données résistants aux fortes humidités, aux fortes chaleurs, aux gels, aux orages et aux vents forts, pluies acides corrosives. Outre la résistance à toutes ces contraintes environnementales, la structure conçue devra supporter l'ensemble de l'installation incluant des panneaux solaires. Afin de ne pas perturber la faune sauvage, la transmission des informations est sans fil car les réseaux filaires seraient trop invasifs pour le milieu, leurs durées de vies limitées et pourraient générer des déchets s'ils étaient endommagés.

Aussi, le dispositif doit soit se fondre dans le décor, et non aisément accessible pour éviter de subir les éventuels casseurs ou voleurs. Un mât en acier (totem) de 1500 mm de hauteur et 60 mm de diamètre, pouvant accueillir l'enregistreur de données et sa communication est en cours de réalisation, ainsi que sa gaine protectrice qui assurera une protection contre les détériorations par des visiteurs ou par les conditions climatiques.

Les données enregistrées sont la profondeur de la mare, la température de l'eau, son PH, sa qualité chimique et la pression atmosphérique. Une caméra permet aussi d'avoir des images de la mare et son évolution (périmètre, taille) de jour comme de nuit. Une interface Homme Machine permettant l'exploitation les données récoltées et le paramétrage des instruments est aussi développée par les étudiants. Nous revenons donc sur des éléments fondamentaux des projets précédents en instrumentation, informatique et communication industrielle. Le concept des totems instrumentés, de leur structuration en réseau et le test de mesures capteur via des prototypes arduino est illustré à la figure 4.

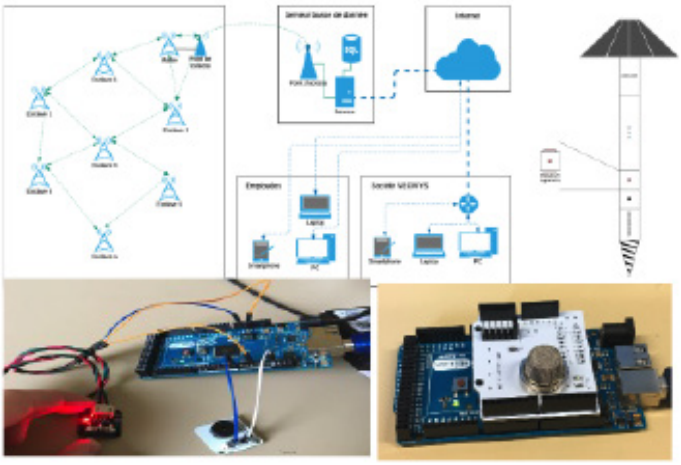


Figure 4 : Structuration réseau, Totem et prototypage d'instrument

Le financement du projet est en cours d'étude avec l'association NOEMYS. À l'instar du projet Chrys@lide, les totems passent une partie de l'année en développement et l'autre en exploitation afin d'avoir des retours de l'association et assurer des cycles d'améliorations itératifs. Les étudiants engagés pour la partie réalisation sont ceux de la LP SARI et pour la partie études, ceux du DUT GEII. L'installation et la livraison de 5 totems instrumentés est prévue pour 2019. Le projet essaime car la construction physique du totem sort du champ de compétences de nos étudiants et un partenariat avec le département de génie mécanique pour la conception physique du totem a été démarré en 2018.

III. Bilan, retombées et difficultés rencontrées

Avec ces projets tuteurés orientés vers des applications concrètes en lien avec le monde socio-économique, la motivation et l'investissement des étudiants ont été les points positifs les plus importants. Cela a permis aux étudiants de dépasser certaines difficultés technologiques par exemple. Le lien qui s'est formé avec les différents commanditaires a aussi été très apprécié par les étudiants qui l'ont pris à leur charge et ont fait preuve quelques fois d'un professionnalisme presque surprenant. Pour certains d'entre eux, cela a permis de découvrir des vocations et de s'intéresser à des domaines qui leur étaient complètement étrangers. C'est en faisant qu'on apprend à faire.

D'un point de vue pédagogique, ces projets ont permis de bien illustrer, appliquer et faire comprendre la nécessité des aspects de gestion de projets en grandeur réelle. De plus, les étudiants ont dû s'approprier des connaissances techniques (automatique, réseau, capteurs et instrumentation, électronique embarquée…) couvrant un large spectre du GEII mais aussi des compétences de communication, de rédaction voire de chimie et de biologie. Des projets pluridisciplinaires à l'image du champ de métiers dans lesquels ils pourraient exercer.

Ces projets ont aussi permis au département d'avoir plus de liens et plus de connexions avec son environnement proche. Cette ouverture, même si elle n'est pas toujours comptable, donne de l'envergure. À terme, que ce type de projets soit réalisable avec des étudiants peut être valorisé à divers niveaux et peut servir de support de communication au département et être un levier pour le recrutement, l'acquisition de nouveaux équipements ou la construction de nouvelles collaborations.

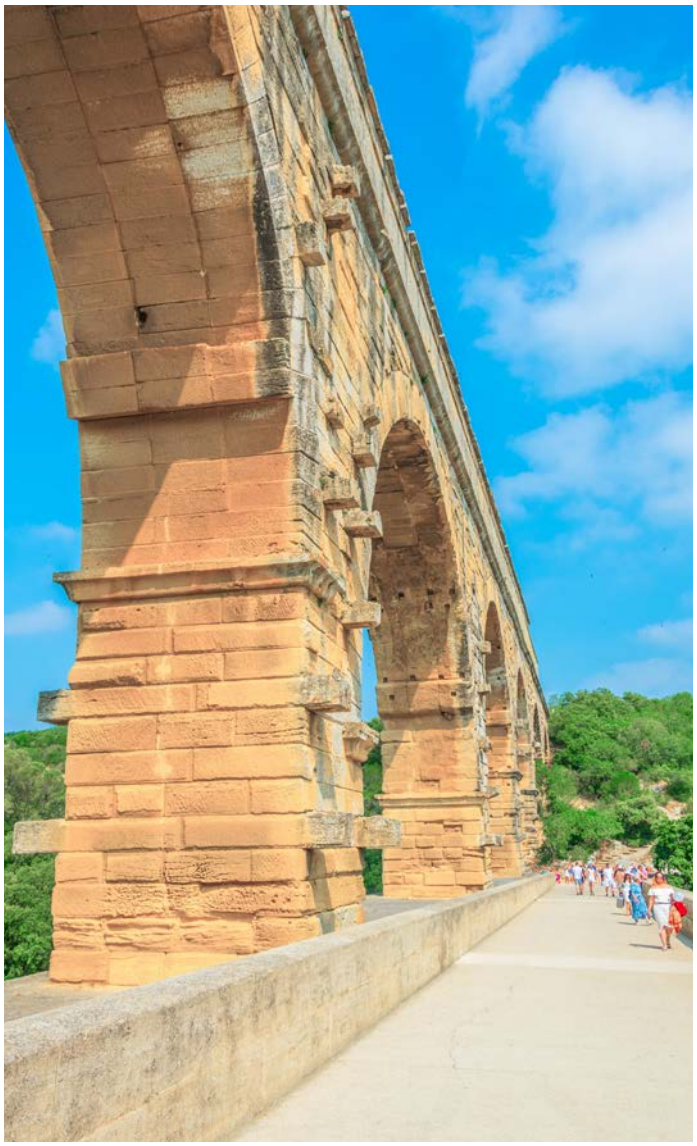
Néanmoins, la forte adhésion des étudiants n'a pas eu toujours d'équivalent de la part des collègues enseignants. En effet, peu de personnes se sont réellement embarquées dans les divers projets, pour des raisons de disponibilités mais pas seulement. Le fait que ce soit porté par un vacataire professionnel extérieur n'ayant pas les mêmes préjugés ni le même rapport académique avec la technologie a été un facteur essentiel de la réussite de ces projets. Enfin, l'argument financier : l'argument récurrent que le budget investi dans les drones et du robot par exemple, même subventionnés, aurait pu servir utilement à acheter des automates, des moteurs, des ordinateurs ou tout autre équipement de TP académique a été souvent rappelé lors des réunions de départements ou juste à la cafétéria du département. Malheureusement, ce type de projets exige un réel investissement humain et des compétences technologiques très diverses. Malheureusement, l'air du temps n'est pas toujours propice à ce genre d'implication pouvant être rédhibitoire à une évolution classique d'une carrière surtout que la rémunération n'est pas toujours à la hauteur. Par ailleurs, même si les connaissances techniques de nos étudiants peuvent sembler innovantes pour nos partenaires, de tels projets (de longue durée) ne peuvent être mis en concurrence avec le pragmatisme et la réactivité d'un bureau d'étude privé. Le projet innovant peut rapidement ne plus l'être quand il s'étale sur plusieurs années. .

Perspectives : Pour certains projets des compétences d'autres départements de l'IUT Nancy-Brabois seraient très utiles, que ce soit en biologie, en mécanique, en chimie ou en réseaux. Dans les prochaines années, surtout si le DUT en 3 ans voit le jour, ce type de projets serait un support pédagogique extraordinaire et permettrait le développement de compétences transverses. C'est la motivation et l'implication des étudiants, allant plus loin qu'en séances de séances de TP ou de TD classiques, qui permet une appropriation des savoirs (même si l'on peut constater un manque de méthode). C'est du vrai Apprendre Autrement, du learning by doing et un 'lieu' d'exercice professionnel où l'on peut se tromper mais avec l'obligation de résultat. C'est aussi un support thématique exportable dans des projets pédagogiques européens notamment avec le service des relations internationales et le développement de la Carrousel Week [1] en GEII. Reste à trouver les partenaires et monter les dossiers de financements. Notre environnement local où gravitent beaucoup d'associations, de petites entreprises, est demandeur de ce type de collaborations. Il faut juste que ce soit dans la même échelle temporelle que nos formations : un projet ne peut, avec les 32 à 35 heures de cours par semaine, se faire dans la même durée que s'il était réalisé par un bureau d'études professionnel. Certains partenaires peuvent se permettre ce temps d'exécution et comprendre qu'avec ces projets, ils investissent dans la formation et la créativité des techniciens de demain.

Enfin, outre l'investissement de l'équipe enseignante, et même si statutairement le département a seulement « obligation de moyen », les responsabilités, l'image et le sérieux sont toujours engagés.

Références

[1] https://iutnb.univ-lorraine.fr/fr/content/carousel-week-une-semaine-dechanges



Pont du Gard - Vers-Pont-du-Gard

Invitation au voyage...

Fortifications de Vauban - Longwy

Lac de Gérardmer - Lorraine

Invitation au voyage...