... à la convergence du numérique, des entreprises et de l'enseignement supérieur.

Newsletter n°114 - Novembre 2018

SOMMAIRE :

- Le mot du Président
- Paiement sans contact : le danger ne suit pas forcément nos intuitions
- "L'identification des citoyens" : compte-rendu de l'intervention de Jean-Marc Lévy Dreyfus
- Notre système économique numérisé est devenu imprévisible : « Le numérique, c'est l'économique »
- Le cantique du quantique
- Actualité de l'atelier Estonie
- Cyber Sécurité vs Sécurité Numérique
- Article 7 La normalisation des smartgrids (Partie3 et Partie4)
- Blockchain privée vs blockchain publique (technique et juridique) expliqué en BD
- Construire une France innovante
- Agenda

Le mot du Président

Bonjour,

Depuis 2016, le fichier des fichiers des données des Français est autorisé (Titres Electroniques Sécurisés TES).
Cette surveillance centralisatrice, toujours refusée dans le passé, est maintenant active, incluant le fichage biométrique de l'ensemble des Français, et faisant craindre une surveillance sans retenue de la part de l'exécutif, celui d'aujourd'hui, mais aussi, et c'est là le plus inquiétant, celui de demain, quelque soit sa couleur.
Après les remarques très critiques de la CNIL et du CNNum, certaines associations, comme le Think Tank Génération libre, la Quadrature du Net et bien d'autres, avaient vertement critiqué cette centralisation des données, ce fichage généralisé. Le fichier TES est un réel danger, tant dans la difficulté qu'il y a à protéger une base centralisée, que de contrôler sérieusement le bien-fondé des requêtes qui pourraient y être faites. On peut craindre que cet outil, entre des mains maladroites, voire mal intentionnées, soit une atteinte grave à nos libertés individuelles.

À l'heure du RGPD, on peut s'étonner que l'état n'applique pas à lui même les principes qu'il entend imposer aux grandes entreprises du numérique.
Faut-il rappeler qu'en France, les lois Informatique et Libertés, la CNIL, et plus globalement ce mouvement de défense des données personnelles prend racine dans le projet "SAFARI" (1974, et oui !), qui avait pour objectif de créer un fichier central des Français, et qui avait été dénoncé par Philippe Boucher, ce qui avait entrainé son abandon, et la mise en place de la CNIL et des lois Informatique et Libertés .

La Quadrature du Net, avec le soutien des Exégètes amateurs, avait déposé une requête devant le Conseil d'État visant à faire invalider ces mesures, la requête vient d'être rejetée (octobre 2018). Le

ThinkTank Génération libre, vient de décider de faire appel de la décision devant la juridiction européenne, dans l'espoir d'endiguer la propagation d'une surveillance de masse dont la menace devient, à l'ère du numérique, de plus en plus tangible.

En me promenant ce soir dans Paris, je me suis souvenu de ma soirée, le lendemain des horribles attentats du 13 novembre 2015 : les terrasses étaient pleines de monde, les Parisiens étaient debout, fermement décidés à défendre leurs libertés, leurs modes de vie, contre la barbarie.
3 ans après, où en sommes-nous, comment l'État défend-il nos libertés ? En nous les retirant, ou les limitant ?

Une société évoluée se doit de se défendre, défendre ses citoyens, les libertés, mais avec discernement, mesure, retenue, contrôle et contre pouvoir. C'est le prix de notre liberté, notre bien le plus précieux.

Auteur:
Philippe RECOUPPÉ - Président Forum ATENA

Paiement sans contact : le danger ne suit pas forcément nos intuitions

Beau succès pour le paiement sans contact : les chiffres qui circulent évoquent 67 % de progression en dix ans et 27 % des transactions. Il est vrai que s'affranchir de la manipulation de pièces apporte une fluidité bienvenue dans les boulangeries comme dans beaucoup de petits commerces.

Est-ce anodin ? Quel est le prix à payer pour notre confort ? Penchons-nous sur les aspects sécurité du processus et disparition de la monnaie sonnante et trébuchante.

Sécurité

La sécurité demeure la crainte majeure inspirée par un mode de paiement qu'un simple effleurement permet de valider grâce à la technologie NFC (Near Field Communication). Munie d'une antenne passive, la carte bancaire bénéficie de l'énergie fournie par le lecteur lors de l'émission d'une requête pour moduler le signal incident au rythme des informations extraites d'une petite mémoire. Le lecteur peut alors récupérer ces informations.

Ainsi décrit, les transports en commun semblent bien menaçants pour ce type de carte.

Effectivement, la portée théorique de l'ensemble du système est de quelques centimètres. En pratique, le paramètre structurant pour cette valeur n'est pas au niveau de la carte qui est passive mais au niveau de l'émetteur. Seules les capacités du lecteur détenu par le pirate dictent les performances d'éloignement. Si nous sommes protégés des distances plus conséquentes par le coût et la taille des antennes, la densité d'usagers aux heures de pointe ne nous met pas à l'abri d'intrusions depuis un smartphone doté de la fonction NFC.

Dès lors deux inquiétudes percent : le détournement de fonds et la collecte de données personnelles.

La fraude

L'intuition nous pousse à nous méfier des cartes sans contact mais rassurons-nous toutefois avec le très faible taux de fraudes relevé par l'*Observatoire de la Sécurité des moyens de paiement* dans leur

rapport de 2016 : 0,02 %, clairement en deçà des 0,2 % des paiements en ligne. Ajoutons que l'utilisation frauduleuse des cartes sans contact perdues constitue le gros des troupes pour conclure que le détournement « par promiscuité » est marginal voire théorique. À quoi attribuer ce faible taux ?
Un élément d'explication physique peut être rattaché aux interférences entre antennes réceptrices passives. Une carte n'est que rarement le seul récepteur à portée d'émetteur, il faut compter avec d'autres cartes ou des antennes dans des vêtements par exemple. Ces éléments peuvent rendre délicate la lisibilité de la réponse du récepteur en brouillant les signaux.

La mise en œuvre du piratage quant à elle est particulièrement lourde : le paiement sans contact n'est accepté qu'après s'être dûment enregistré en tant que commerçant auprès d'un organisme bancaire, ce qui élimine les pirates amateurs. Le transfert entre particuliers n'est pas (encore) au catalogue.

D'autres scénarios comme le relai ont été imaginés. Un pirate auprès de vous se connecte à votre carte, un complice est relié par une connexion mobile auprès du terminal du commerçant. Lors du paiement les informations de votre carte sont utilisées. Mais le délai introduit par ce scénario théorique le rend détectable. De plus il nécessite une coordination pour accès à la carte de la victime et processus de piratage soient concomitants, ce qui relève de la gageure.

Le paiement par des applications mobiles ajoute un degré supplémentaire de sécurité grâce à l'utilisation de la carte SIM.

Ces efforts étant à déployer pour des gains limités à trente euros par capture, il n'est pas étonnant que l'activité n'attire que peu de candidats.

La collecte de données

Peut-être le détournement est-il rare, mais qu'en est-il du siphonage des données personnelles présentes sur la carte ? Le problème est réel et la CNIL a tôt fait de s'en émouvoir. À compter de 2013, seules ont droit de présence les informations de numéro de carte et de date de validité. Exit le nom du détenteur, l'historique des achats si précieux aux yeux des publicitaires. Et bien entendu absence du code imprimé au dos de la carte. Dès lors, difficile d'exploiter vos données pour dresser un profil de consommateur ou effectuer des achats sur Internet.

Si c'est en toute quiétude que j'use de ma carte pour repartir avec ma baguette, la perspective d'un monde sans pièces jaunes me laisse moins serein. Quelles conséquences à la disparition de la monnaie fiduciaire ?

La disparition de la monnaie fiduciaire

Des pays comme la Suède ou la Corée annoncent travailler sur le canevas d'une société sans cash. Depuis 2012, l'application suédoise « Swish » permet les transferts entre particuliers et est utilisée lors des offices religieux pour la quête voire par les SDF. Les trois quarts des suédois se sont quasiment passés de cash en 2017. À Pékin, c'est l'application de messagerie WeChat qui sied aux dépenses quotidiennes, du cinéma au « fast meal » ou au transport.

L'application M-Pesa, filiale de l'opérateur kenyan Safaricom est utilisée jusqu'en Afghanistan. Elle fait tout : règlement chez les commerçants, règlement de facture mais également recevoir son salaire ou un crédit.

Saluons en Europe pourtant frileuse l'application française Lydia qui s'approche de deux millions d'adeptes sur l'ensemble des pays.

Des avantages …

Pour les banques, les avantages sont nombreux : moins de braquages de fourgons, moins de distributeurs à charger et entretenir, suppression des processus de comptage et de tri de monnaie.

Pour les États, c'est avant tout la lutte contre le travail au noir et la fraude qui priment. Ajoutons que la production et la distribution de la monnaie fiduciaire pèsent pas loin de 1% du PIB en zone euro, ce qui est loin d'être négligeable.

Pour les particuliers, la simplification des procédures est bénéfique. La souplesse des transactions diminue les files d'attentes. Dans certains pays où les salaires étaient réglés en liquide, l'enveloppe perdait de sa superbe à chaque niveau hiérarchique traversé. Le basculement vers des applications de transfert s'est traduit pour les salariés par une sensible augmentation.

Que du ciel bleu ? Hélas, il faudra faire également avec certaines conséquences.

… mais pas que

Quelques effets de bord à la disparition de la monnaie fiduciaire sont toutefois à surveiller.

Pour commencer, la monnaie dont nous disposons sur notre carte bancaire ou qui y est virée n'a qu'une garantie à la marge de l'État. Cette monnaie est un outil qui appartient à une banque commerciale. Un euro de la Société Générale n'a aucune valeur pour la BNP. Les virements entre les deux établissements passent par un intermédiaire en euros officiels de la banque centrale. En cas de faillite d'un établissement, les comptes ne valent plus rien. Vos économies s'envolent. Ce n'est pas un scénario d'école, chypriotes et grecs vous confirmeront que se heurter à des portes closes et à des distributeurs muets sont des choses qui arrivent tout comme l'évanouissement de l'établissement bancaire créé en 1850 par les frères Emanuel et Mayer Lehman. L'euro d'une banque commerciale est garanti par cette banque mais pas par la banque centrale. L'État apporte une assurance en garantissant à hauteur de cent mille euros chaque compte, mais la cagnotte prévue à cet usage résisterait-elle à un effet dominos ? C'est à confirmer.

Ensuite le passage par une banque commerciale de la totalité de nos transactions lui délivre de quoi dresser un profil très précis de notre consommation. Ce profil a une valeur marchande, c'est un produit qui a son marché. Ne croyons pas que le mal est déjà fait au prétexte que 90 % de notre consommation est d'ores et déjà entre les mains des banques commerciales. Les 10 % restant représentent tout sauf un tribut marginal pour notre profil car c'est là une part importante de notre consommation fortement révélatrice de notre mode de vie au quotidien. Est-il raisonnable de livrer 100 % de nos habitudes de consommation au Big Data ? Personnellement j'en doute.

Quand l'effet de bord est plus à surveiller que l'intuition

Eh oui, le paiement sans contact n'est pas si dangereux que ça, surtout dans sa version smartphone. Ce qui n'est pas intuitif.

En revanche, accepter la disparition de la monnaie fiduciaire ne nous offre pas d'autre solution que de passer par des banques commerciales à qui nous livrons nos secrets et dont nous ne pouvons qu'espérer crise après crise qu'elles résisteront. Ce qui me semble inquiétant.

Auteur:
Jacques BAUDRON - Secrétaire Forum ATENA - jacques.baudron@ixtel.fr

---

"L'identification des citoyens" : compte-rendu de l'intervention de Jean-Marc Lévy Dreyfus

Interview de Jean-Marc Lévy Dreyfus par Bernard Biedermann suite à sa conférence à **l'Atelier « Etat Plateforme »** du 12 novembre 2018 sur « L'identification des citoyens »

BB : Jean- Marc Lévy Dreyfus vous êtes entrepreneur dans l'informatique et le numérique depuis trois bonnes décennies. Vous êtes expert dans le domaine de l'internet dans lequel vous développez des techniques innovantes depuis 1994.Entre autres, vous travaillez sur des solutions de facilitations de l'inclusion financière et des transactions financières pour tous grâce à de simples coups de fil en Inde, en Afrique et en Amérique du Sud. Aujourd'hui, dans le cadre de l'Atelier sur l'Etat Plateforme, vous nous avez présenté une approche totalement nouvelle d'architecture de services publics de l'Internet basée sur une vision "droit de l'hommiste". Tout d'abord quel est le nom de ce produit et pouvez-vous nous dire en deux ou trois phrases ce qu'il fait ?
JMLD : Le nom de la nouvelle architecture que je propose est DNA, Domicile Numérique Attribué. DNA est une nouvelle manière d'organiser l'adressage, le nommage et par conséquent l'identification et la certification des individus et des entités dans les transactions et la gestion dans l'internet.
BB : Fondamentalement, quel est votre objectif ?
JMLD : Mon objectif est de valoriser les atouts de la France en lui permettant de reprendre le lead, de contribuer « à côté » du web un nouvel environnement d'échange et d'identification sécurisé et organisé et certifié par l'état régalien ou par une entité régalienne.
BB : Et pour quelle raison ?
JMLD : Aujourd'hui, nous vivons dans un monde globalement numérique très confus qui se caractérise par la fusion du web et de l'internet. Cette fusion est également sémantique ; Web et Internet désignant indifféremment les espaces que nous utilisons pour échanger à partir de nos pc, smartphones, tablettes. C'est une grosse erreur. En fait, le Web n'est qu'une des applications possibles exécutables sur le réseau internet. Ce dernier est en fait un réseau d'échanges de données numériques, entre des milliards de terminaux. Internet est structurellement agnostique et neutre par rapport aux usages qu'il supporte. Dans l'Internet, chaque nœud, chaque terminal et chaque paquet de données est identifié par des coordonnées binaires (des suites de 0 et de 1) sur 4 octets les adresses IP.
De par sa nature l'Internet ne peut être exploité par des humains qu'au travers de logiciels qui traduisent les adresses binaires en adresses décimales.

Ainsi l'adresse IP 172. 16.254.1 équivaut à 10101100 . 000100000 . 11111110 . 00000001

Les adresses IP étant extrêmement complexes à utiliser par monsieur tout le monde au quotidien (par exemple : http://172.16.254.1/mashpro/logindex/) les pères fondateurs californiens réfléchissent à une méthode pour gérer des adresses alphanumériques.
BB : Et quelle est la norme qui en est ressortie ?
JMLD : Pour permettre l'exploitation plus facile du réseau par les hommes (donc sans passer par les adresses IP numériques), en 1983 l'IETF, l'organisation des ingénieurs de l'internet, qui définit les règles du réseau, a délégué à Jon Postel, la responsabilité de créer un nouveau système d'adressage mnémonique et alphanumérique.
Avec l'aide de Paul Mockapétris, Jon Postel impose une solution de nommage et de résolution (comment identifier l'adresse IP de l'ordinateur qui contient le domaine) des adresses de l'Internet : le DNS, Domain Name System. (Système de Noms de Domaine)

Ce système est sous-jacent à toute l'organisation technique (et donc sociétale) des adresses que nous utilisons au quotidien sur Internet. Grâce au DNS il a été possible de sortir Internet des laboratoires et des universités californiennes et y déployer des solutions utilisables comme les emails et surtout le Web (www proposé par Tim Berners Lee en 1991). Pour fonctionner le Web utilise l'application HTTP (Hyper Texte Transfert Protocol) assujettie au navigateur laquelle interprète l'adresse DNS (de forme sous la forme www.nomdedomaine.tld/index.htm) en adresse numérique exécutable sur votre terminal. Il existe d'autres applications (SMTP, FTP, POP, IMAP, IRC...) qui fonctionnent sur Internet et qui ne sont pas dans le Web.
Dans le Web, pour exister l'individu (ou l'entreprise) doit impérativement disposer d'une (au moins une) adresse propre dans le DNS. Cette adresse nom de domaine ou adresse email est par construction unique - le DNS ne supporte pas les doublons - L'adresse est toujours déclarative : Il en résulte que le premier arrivé est le seul servi *

Un nom de domaine se déclare auprès d'un service d'enregistrement (Registrar) qui est affilié à l'organisation des noms de domaine (ICANN). Une adresse email auprès d'un fournisseur d'accès Internet ou d'un opérateur de messagerie.

BB : Et puis il y a eu Web2.0 en 2004 :
JMLD : C'est effectivement une révolution pour le Web qui désormais s'exonère du DNS. Le Web 2.0 généralise l'usage d'un moteur de recherche appuyé sur son annuaire propriétaire qui indexe à sa manière (avec ses algorithmes pour employer un terme à la mode) les adresses DNS. Ceci permet à l'utilisateur final d'accéder à la page qui lui convient sans être obliger de connaître ni de saisir l'adresse DNS.
Avec cette méthode, on trouve avec une simple recherche même approximative le lien et la bonne adresse cible ou la bonne personne dans un réseau social.

C'est cette capacité de simplifier et proposer une navigation fluide d'abord sur les PC et aujourd'hui sur les Smartphone par tous qui va permettre l'émergence de nouveaux services utilisés par des centaines de millions de gens parfaitement ignorant du DNS, de l'IPv4, des navigateurs.

Ainsi chaque offreur de solution peut organiser les contenus et les services qu'il souhaite proposer au consommateur et surtout lui proposer de s'enregistrer et donc enrichir son annuaire.

Il se constitue ainsi une couche fonctionnelle qui en tache de fond exploite IPv4 et le DNS mais de facto s'empare d'une valeur marchande que le Web n'a pas.

Et c'est ce qui a permis la captation de la valeur du Web par quelques immenses entreprises US : les GAFA qui nous aveugle aujourd'hui et nous masque toute la valeur sous jacente de l'Internet.

BB : Et c'est grave cet aveuglement ?
JMLD : Il faut comprendre que les GAFA en organisant les adresses et le nommage en lieu et place du DNS sont devenus incontournables dans le Web. Nous avons l'illusion que nous ne pouvons pas évoluer en dehors d'eux et par extension on a fini par penser que l'Internet doit nécessairement se conformer au modèle fonctionnel .
BB : Il existe pourtant des solutions ?
JMLD : Oui je propose une architecture de nommage radicalement nouvelle le DNA qui ne fonctionne pas sur le principe - très américain - du DNS lequel présume que chacun se débrouille pour créer son adresse .
Au contraire le DNA, Domicile Numérique Attribué, s'appuie sur le cadastre qui en repérant chaque foyer, entreprise service public, école, ... dans un répertoire nommé et géré par l'autorité permet d'organiser la fourniture de toutes sortes de services (eau, gaz, électricité, téléphone, égouts, enlèvement des ordures, voirie, poste, sécurité publique, liste électives, écoles, transport ...) et de les garantir à chaque résident du territoire cadastré.

Le DNA permet d'attribuer une adresse numérique sécurisée à chaque ayant droit du territoire sans que celui ci n'ait aucune action à entreprendre.

A partir de sa page DNA chacun bénéficie de services numériques de messagerie, de suivi administratif, de transactions sécurisés et garantis dans le réseau social de l'opérateur du DNA.

Le DNA constitue une réelle opportunité de faire levier sur les services publics et l'organisation administrative de la France et de transformer ce qui est un handicap dû au Web - dépendance aux GAFA, absence de sécurité, globalisation et la perte de repères - en un atout majeur : la constitution à coté du Web, d'un Internet de la Confiance et de la Sécurité garanti par l'Etat.

Un énorme potentiel de progrès pour notre Pays.

>>> Nb : Les slides de la conférence du 12 novembre sont disponibles **via ce lien**
>>> Prochaine réunion de l'Atelier "État Plateforme" de Forum ATENA : lundi 17 décembre

** ainsi qu'il n'y a qu'un seul et unique jacques.martin@gmail.com le second sera jacques-martin le troisième martin-jacques comment fait on pour le nième Jacques Martin? et comment communiquer avec votre ami Jacques Martin alors qu'il n'existe aucun service d'annuaire des emails (et heureusement imaginez la quantité de SPAM si votre adresse mail était publique.)*

Auteur:

Bernard BIEDERMANN, co-Président de l'Atelier Etat Plateforme

Notre système économique numérisé est devenu imprévisible : « Le numérique, c'est l'économique »

Pour une majorité d'observateurs, les économies développées ou en voie de développement, sont en train ou vont connaître la révolution du numérique. Définir et analyser cette révolution de façon précise nécessiterait un nombre conséquent de concepts et d'observations qui relèvent de plusieurs domaines : techniques, sociologique, psychologique, éthiques juridiques, et bien sûr économique.

Aujourd'hui, la proportion de biens et services de consommation ou de facteur de production qui intègrent et/ou dépendent du numérique est considérable, et ce, pour ce qui concerne leur conception, leur fabrication, leur contrat (vente, location), leur distribution, leur utilisation, leur maintenance et leur durée de vie.

Concernant le capital productif, je suggère (http://www.theoreco.com/,« Le numérique, c'est l'économique » C4 : Capital Libre et capital dédié) que les facteurs de productions numérisés, comme les robots soient qualifiés de « capital libre » parce qu'ils ne sont pas « dédiés » à une seule activité, comme par exemple le métier à tisser d'autrefois qui ne pouvait fabriquer que du tissu.
Le système économique numérisé se caractérise par, de l'interdépendance, de la complexité, des innovations continues avec effets de surprises, un environnement international avec ses contraintes de délais de décisions. Ces conditions constituent un système économique de plus en plus imprévisible malgré le flux continue d'informations économiques nécessaires aux prises de décisions des entrepreneurs et des consommateurs car la demande d'information demeure continuellement supérieure à l'offre.

L'auto-observation par un flux continue d'informations ne le rend pas plus prévisible car elle révèle le caractère infini des profils microéconomiques ainsi que leur changement continue. De plus, La diffusion cyclique de l'information alimente les modifications des besoins formatés par des produits innovants.

Nos économies se composent de sous-systèmes fonctionnant sur des applications numériques complexes. Cette complexité se caractérise par une fragilité intrinsèque susceptible de générer des crises, comme on en a déjà vécu, et que l'on a qualifiées ex post, d'imprévisibles malgré des investissements macroéconomiques dans la cybersécurité.

Toutes ces nouvelles tendances conduisent à se poser la question de savoir s'il ne faudrait pas revoir la théorie de la valeur, des biens et services, de consommation, de production et monétaires.

En poussant le raisonnement, on peut dire que notre système économique est devenu, imprévisible, truffé d'explosions de surprises, non probabilisable en raison de l'absence d'historiques, et donc indéterministe, mais sans véritable composante d'incertitude dans le sens Keynésien. A ce profil s'ajoute son caractère irréversible en raison du pouvoir qu'exerce le progrès technique sur les dirigeants.

Dans de telles conditions, la maxime « gouverner c'est prévoir » n'a plus vraiment de justifications. Des recommandations consisteraient plutôt à développer une analyse beaucoup plus fine et précise de la réalité avec pour objectif de prendre des décisions dans des délais très courts, sans se fonder sur des prévisions ou des extrapolations simplistes de tendances micro-économiques.

Sur http://theoreco.com :

1 : Approche globale
2 : L'information pour les décisions économiques
3 : La vie de l'entreprise
4 : Capital Libre et capital dédié
5 : Biens et services de consommation
6 : Marché du travail
7 : Marché monétaire
8 : La fin du travail ?
9 : Faut-il revoir la théorie de la valeur ?
10 : Quelles nouvelles attitudes adopter ?

Auteur:
Bernard BIEDERMANN, co-Président de l'Atelier Etat Plateforme

---

Le cantique du quantique

Cet article s'inspire librement à la base, et avec beaucoup de liberté et d'ajouts, d'une intervention dans une table ronde de Philippe Duluc, directeur technique Big Data et Sécurité d'ATOS et du professeur Jean-Jacques Quisquater, de l'UCL Crypto group à Louvain-la-Neuve, en Belgique. Cette table ronde a été tenue à l'occasion du colloque annuel de l'ARCSI, octobre 2018 à la Bibliothèque nationale de France. Ce colloque était aussi l'occasion de marquer les 100 ans de la victoire de 1918 et les 90 ans d'existence de l'ARCSI, (Association des Réservistes du Chiffre et de la Sécurité de l'Information).

Les ordinateurs vraiment quantiques, avec une capacité de milliers de qubits qui leur permettront d'effectuer des calculs très rapides et massivement parallèles, sont encore loin d'être une réalité aujourd'hui. Tout au plus existe-t-il des simulateurs de calculateurs quantiques qui en sont une première approche et permettent de développer les algorithmes et les programmes de demain, ou d'après-demain. Mais dès aujourd'hui, la physique quantique peut être utilisée pour générer des nombres aléatoires, indispensables pour créer des clés symétriques, avec lesquelles sont chiffrées et

déchiffrées les informations sensibles. Dans un chiffrement symétrique, on chiffre un message sensible avec une clé, on le déchiffre avec la même clé. Pourquoi est-ce important que cette clé soit créée avec un contenu aléatoire, ce que les ordinateurs d'aujourd'hui ne savent pas vraiment faire sans ajout d'un élément aléatoire extérieur ? Parce que si un prédateur peut prédire le contenu de cette clé durant sa génération, il peut alors déchiffrer le message chiffré avec cette clé devinée. Mais, avec la physique quantique si durant la distribution de ces clés, par exemple avec le protocole BB64, le prédateur tente une interception de la clé, les propriétés de la physique quantiques permetent de remarquer cette possible malveillance.

Voyons maintenant la dualité quantique. L'expérience des ondes lumineuses qui passent à travers deux fentes de Young, et créent des franges d'interférences sur un écran placé derrière les fentes, prouvent que la lumière est formée d'ondes, tout comme les vagues à la surface de l'océan. Mais les franges d'interférences peuvent aussi s'expliquer par la nature corpusculaire, de la lumière, qui peut être vue comme constituée de photons, particules de l'infiniment petit, sans masse mais avec une énergie : le quanta. Dans l'expérience des fentes de Young, un photon polarisé passe à la fois par une fente et en même temps par l'autre. Difficile de comprendre cette ubiquité avec le sens commun, mais c'est ainsi et le monde de l'infiniment petit a des comportement qui peuvent sembler bizzares mais ne sont pas moins bien réels et même prouvés mathématiquement. La particule interfère avec elle-même à la sortie des fentes de Young (!), et se renforce ou s'annule, ce qui produit les franges d'interférence. Cette théorie utilise la superposition d'états quantiques des particules, comme les photons. C'est difficile à admettre, mais avec l'aspect statistique du quantique, cela s'explique et des équations mathématiques sont là pour le démontrer. Rappelons ici que ces théories ne s'appliquent qu'aux particules à l'échelle sub atomique, donc ni à vous, ni à moi.

Ainsi la lumière a une existence ondulatoire, et en même temps une existence corpusculaire. On parle de dualité ondes – particules. En 1918, Max Planck reçut le prix Nobel pour ses recherches sur l'énergie des quantas. En 1921, Einstein recevait le prix Nobel pour ses travaux sur l'énergie photoélectrique qui établissait cette dualité ondes-particules. Comprendre cette dualité est indispensable pour expliquer certains phénomènes qui se produisent dans l'infiniment petit. D'ailleurs, avec la finesse des gravures des composants électoniques qui ne cesse de diminuer, obéissant à la loi de Moore, nous ne sommes pas loin de ne plus comprendre certains phénomènes qui se passent, sans le concours de la physique quantique.

Un qubit, version quantique du bit, obéit au principe de l'intrication et au principe de superposition des deux états |0> et |1>. Il subit une décorrélation quand on le mesure. Cette superposition des états, illustrée dans la littérature par l'expérience de pensée du chat de Schrodinger, enfermé dans sa boîte, mort et vivant à la fois, sera utilisée avec les algorithmes post quantiques, quand les ordinateurs quantiques seront vraiment utilisables. La décorrélation qui fait que quand on mesure un élément, ou quand il entre en collision avec un autre élément, cet élément perd ses propriétés de superposition, est ce qui frène l'existence des ordinateurs vraiment quantiques, mais peut résoudre le problème de la distribution des clés symétriques. Si on observe une clé avant sa réception, elle perd ses propriétés de superposition quantique et le destinataire, en fonction de la méthode utilisée, comme par exemple le protocole BB64, s'en aperçoit.

L'intrication quantique est un phénomène encore plus difficile à admettre, mais c'est un phénomène prouvé et même utilisé. Deux particules intriquées ne forment en réalité qu'un seul élément, quel que soit la distance qui sépare les deux particules. Si on fait subir une action sur une des particules, l'autre subit la même action. Un satellite chinois a utilisé l'intrication pour distribuer des clés symétriques en deux points de la terre. Une autre expérience, toujours chinoise sur un radar fait que, même si un avion est furtif, si les particules qui l'atteignent sont intriquées avec des particules sur la surface du radar, l'avion ne peut échapper à un répérage.

L'algorithme de Shor fait passer la complexité de la factorisation des grands nombres d'un problème exponentiel à un problème polynomial, bien plus simple à résoudre. Il facilite ainsi la difficulté de factoriser des grands nombres. Hors c'est grace à ce problème difficile à résoudre qu'est assurée la sécurité du chiffrement à clés publiques, typiquement le RSA. Pourquoi ? Parce qu'avec le chiffrement à clé publique, on distribue sa clé publique à tous ceux qui en ont besoin. L'utilisateur chiffre son message sensible avec la clé publique de celui à qui il veut le faire parvenir. Le destinataire, qui est le seul à posséder la clé privée liée mathématiquement à la clé publique qu'il a

distribuée à tous ceux qui la demande, déchiffre le message avec sa clé privée. Bien évidemment, s'il était possible de retrouver la clé privée à partir de la clé publique distribuée à qui veut l'utiliser, et qui n'est donc pas un secret, tous ceux qui retrouveraient la clé privée pourraient déchiffrer le message.

Mais même si l'algorithme de Shor permet de factoriser dans un temps raisonnable de grands nombres, il ne faut pas craindre l'obsolescence du chiffrement à clés publiques RSA avant de très nombreuses années. Les courbes elliptiques, utilisées aussi dans un chiffrement à clés publiques, seront menacées bien avant la factorisation des grands nombres qui toutefois deviendra un jour envisageable. L'angoisse qui rendra obsolète, par les ordinateurs quantiques, le chiffrement à clés publiques n'est pas pour demain. Mais peut-être cette factorisation se fera, dans un temps raisonnable, même par des ordinateurs classiques bien avant l'existence de vrais ordinateurs quantiques. C'est en tout cas ce que pense le professeur Jean-Jacques Quisquater et aussi Diffie Helmann.

Les algorithmes de tri de Roover, eux facilitent la recherche d'un élément parmi une multitude et donc le tri rapide de ces éléments. Les centres de recherches étudient de nouveaux algorithmes tenant compte des fonctionnalités des ordinateurs quantiques, quand ils existeront, on parle alors de cryptologie post-quantique.

Pour l'échange de clés de chiffrement symétriques, les Chinois auraient réalisé une expérience par satellite, qui utilise le principe de l'Intrication quantique de photons, mais cette expérience ne peut fonctionner que la nuit et sur une distance limitée. Elle exige, de plus, le passage d'un état quantique à un état classique puis à nouveau à un retour vers un état quantique.

Aujourd'hui, contrairement à l'ordinateur quantique qui n'existe pas encore, la physique quantique est une technologie en partie maitrisée et même utilisée par des banques pour la génération de nombres purement aléatoires. Côté simulateurs ou ordinateurs quantiques, Atos travaille dans son centre de recherche, de la Région parisienne, ouvert en 2016, sur quatre piliers : bâtir un simulateur quantique avec de plus en plus de qubits, y compris des qubits correcteurs d'erreurs, développer des algorithmes post quantiques, travailler sur une architecture quantique de nouvelle génération et enfin utiliser le quantique pour la cryptologie et la cybersécurité… quand les ordinateurs quantiques de puissance suffisante existeront. Philippe Duluc voit un simulateur quantique à 100 qubits à l'horizon de cinq ans.

Auteur:
Gérard Peliks, président de l'atelier sécurité et VP de Forum ATENA

Actualité de l'atelier e-gouvernement

Forum ATENA et l'Estonie ont été à l'honneur deux fois récemment. D'une part le 27 Septembre dernier, où sur la proposition de Madame Marie-José Taylor, du Club Rotary de Montfort-l'Amaury-Houdan, et en présence de Madame Nathalie Coupez, Présidente de ce club, j'ai eu le plaisir de faire une conférence sur l'e-gouvernance estonienne. L'assemblée, composée principalement de chefs d'entreprise et de cadres dirigeants, a été très intéressée par ce modèle. Les questions ont été nombreuses – et parfois incisives ! - et toujours pertinentes et de haut niveau.

Et le 19 Octobre, j'ai fait une présentation sur le modèle d'e-santé estonien à l'école d'ingénieurs Polytech de Marseille, lors d'un congrès organisé par le département Génie Biomédical et sous l'autorité de sa Directrice Madame Nadine Candoni. D'autres présentations lors de cette session ont été passionnantes, notamment celles portant sur les applications de l'IA en Imagerie médicale et de l'IoT en Réanimation. Les étudiants de l'assistance étaient un pur bonheur : quel plaisir de dialoguer avec des jeunes aussi ouverts sur l'avenir et sur le monde !

Et dans les deux cas, j'ai eu beaucoup de questions sur le Forum ATENA. Sans doute de futurs membres à l'horizon… En savoir plus et rejoindre l'Atelier e-gouvernement de Forum ATENA : https://www.forumatena.org/atelier-e-gouvernement

Auteur:
Pierre-François Laget, Président de l'Atelier e-gouvernement de Forum ATENA

Cyber Sécurité vs Sécurité Numérique

Dans le cadre du "**Lundi de l'IE**" de décembre, le **lundi 3 décembre 2018 de 18h30 à 20h30 à Télécom ParisTech**, amphi Thévenin, 46 rue Barrault – 75013 Paris Métro Corvisart, ligne 6, l'association Forum ATENA vous invite à l'évènement autour du thème : Cyber Sécurité vs Sécurité Numérique, le poids des mots - Le choc des nombres.
La participation à cet évènement est gratuite et ouverte à tous, dans la limite des places disponibles.

Dans un monde « cyber » où les mots doivent retrouver du sens, comment les nombres peuvent-ils aider à concilier fondamentaux et innovations, règlementation et organisation, intégration et professionnalisation ? La Bible comme Pythagore nous ont enseigné que *« Tout est nombre »* ! Quid de la cybersécurité et de la sécurité numérique, 20 ans après le big bang Internet, 40 ans après le PC, 80 ans après Turing ?
Partant du mythe du « risque zéro » et des attaques « zero day », nous analyserons, entre autres, la transformation du point focal qu'est le RSSI, les limites du binaire, les 3 axes de gouvernance, les 4 familles de risque, les 5 clés de l'acculturation, les 7 plateformes de pilotage, les 10 critères d'équilibre, les 12 métiers, mais tenterons aussi une exploration au sein de « l'infiniment petit » et de « l'infiniment grand » …

L'intervenant est **Pierre-Luc REFALO**, Vice-Président en charge des activités de Conseil « *cybersécurité et protection des données* » de Capgemini-Sogeti. Ses équipes accompagnent les dirigeants et les professionnels dans leur gestion des risques numériques, en particulier pour la protection des données sensibles / personnelles et la résilience des infrastructures critiques.
Il a également défini et lancé les services RGPD du Groupe Capgemini.

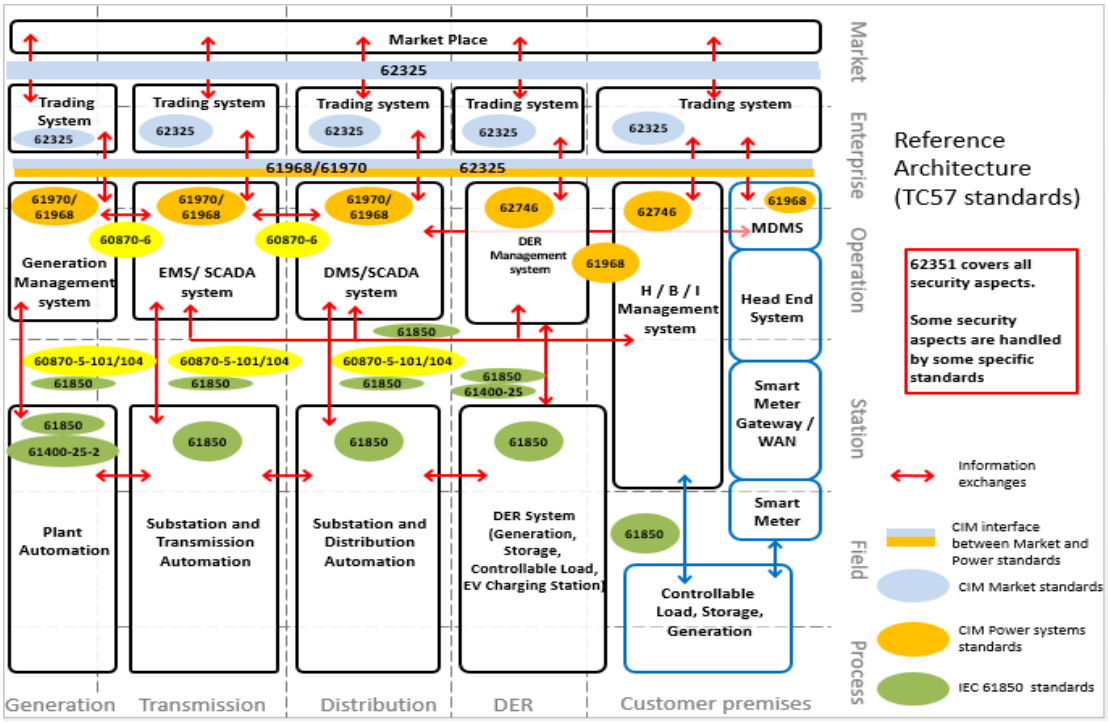
Il est aussi conférencier international et formateur dans plusieurs Mastères Cybersécurité. Il a publié 2 ouvrages de référence, « *Sécuriser l'entreprise connectée* » (2002) et « *La Sécurité Numérique de l'entreprise* » (2012), primé au Forum International de la Cybersécurité en 2013.
Une partie du temps sera consacrée à approfondir certains points abordés comme aux questions / réponses.

Les inscriptions obligatoires se font **par mail** à **beatricelaurent.CDE@gmail.com** avec « **Inscription 03/12** » dans l'objet. Mettez optionnellement ce que vous souhaitez sur vous dans le corps du message. Mettez-moi en copie : gerard.peliks@noos.fr

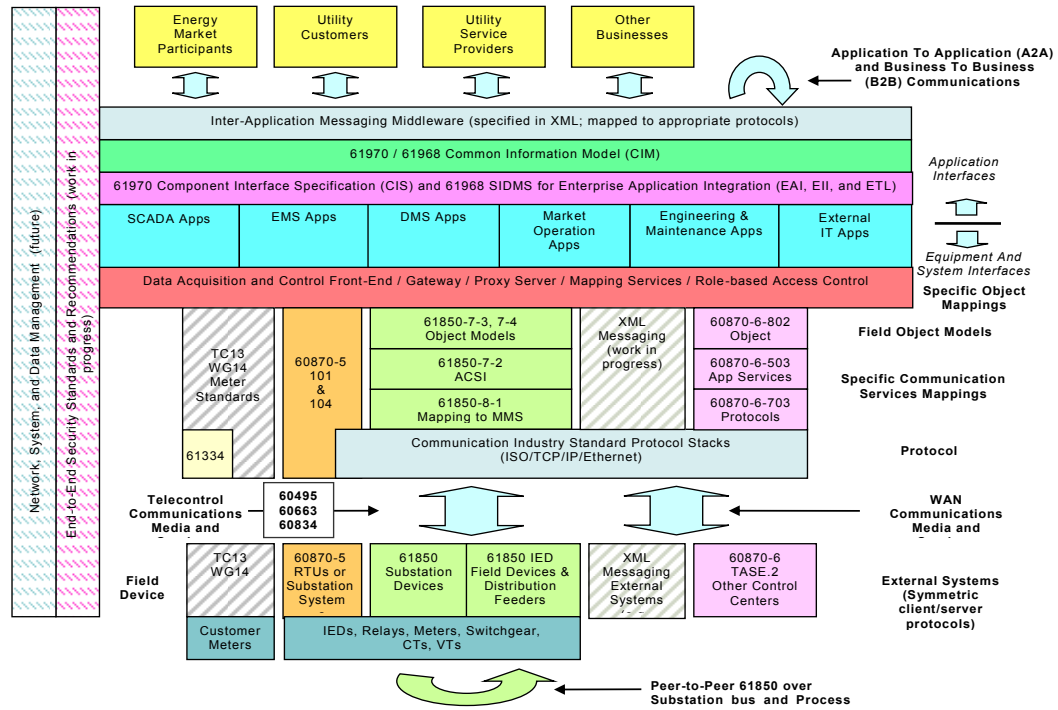
Auteur:
Gérard Peliks, directeur de l'atelier sécurité et VP de Forum ATENA

La normalisation des smartgrids : architecture de référence et normes pour la cyber sécurité

L'article de ce mois-ci sur « la normalisation des Smartgrids » concerne la **partie 3 «architecture de référence»** et **la partie 4 «normes pour la cyber sécurité».** L'intégration « amont-aval » doit s'appuyer sur une architecture de référence. La figure suivante décrit l'architecture de références des systèmes de conduite d'énergie Smartgrids (**IEC TR 62357-1**) où les normes CIM et 61850 sont incontournables :

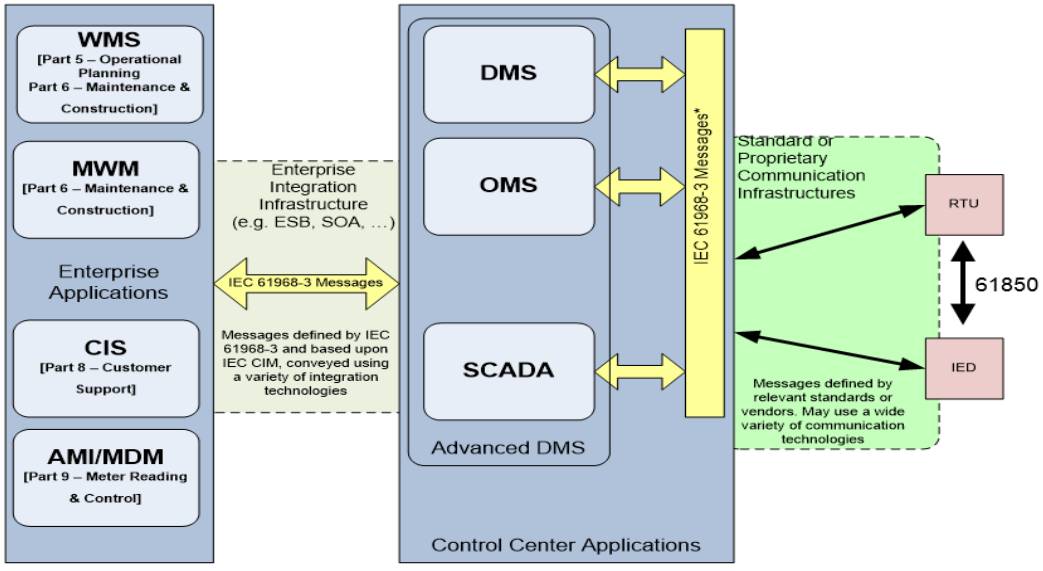


Si l'on se focalise au niveau de l'architecture d'un système Smartgrid d'une utility, par exemple un système SCADA (Supervisory Control and Data Acquisition) et des fonctions avancées de gestion d'énergie (Energy Management System) alors on disposera d'une architecture se rapprochant de la figure suivante :



*Notes: 1) Solid colors correlate different parts of protocols within the architecture.
2) Non-solid patterns represent areas that are future work, or work in progress, or related work provided by another IEC TC.

Une vue plus simplifiée d'un système de Téléconduite Contrôle Commande est représentée ci-après :

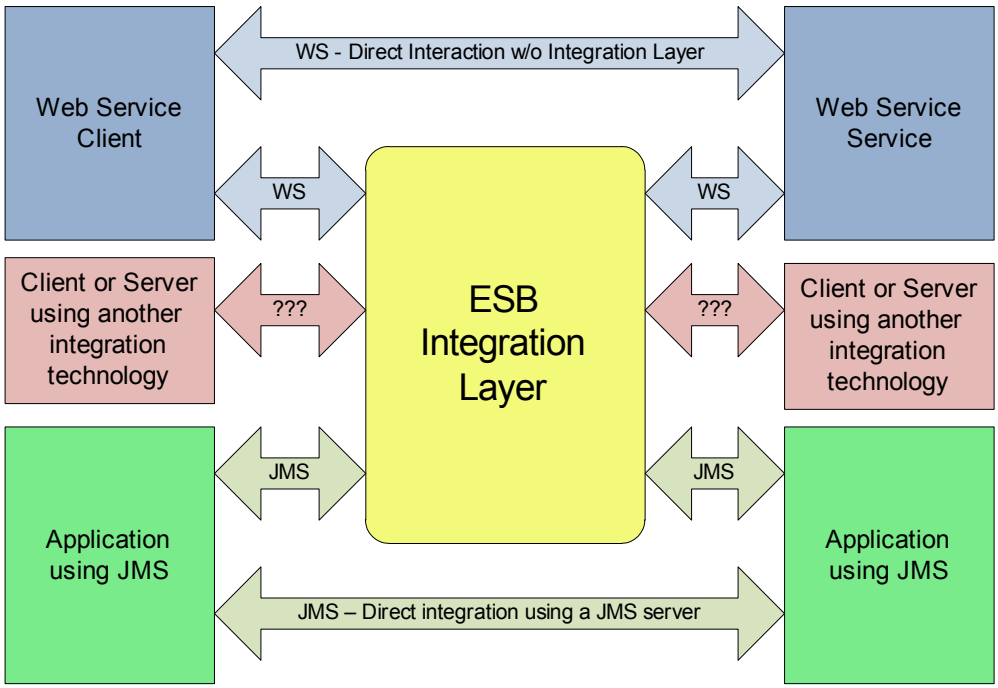


* Note, that depending on the system configuration, these can also be proprietary interfaces (E.g. a system that covers DMS and SCADA in one product).

Le système de téléconduite (utilisant un système SCADA), acquiert des données issues du process en 61850, convertit ces données en CIM et sera en interaction avec des applications de gestion des coupures (OMS : outage Management Service), de gestion avancée de la Distribution (Distribution Management System), de gestion des travaux (WMS : Work Management System), de gestion de la clientèle (CIS : Customer Information System), de gestion des compteurs communicants (AMI/MDM : Advanced Metering Information, Meter Daata Management).

Les parties 61968 du CIM sont alors mises en œuvre pour assurer l'interopérabilité inter-applicative via l'échange de messages.

La façon de véhiculer des messages utilise différentes technologies comme présenté ci-après :

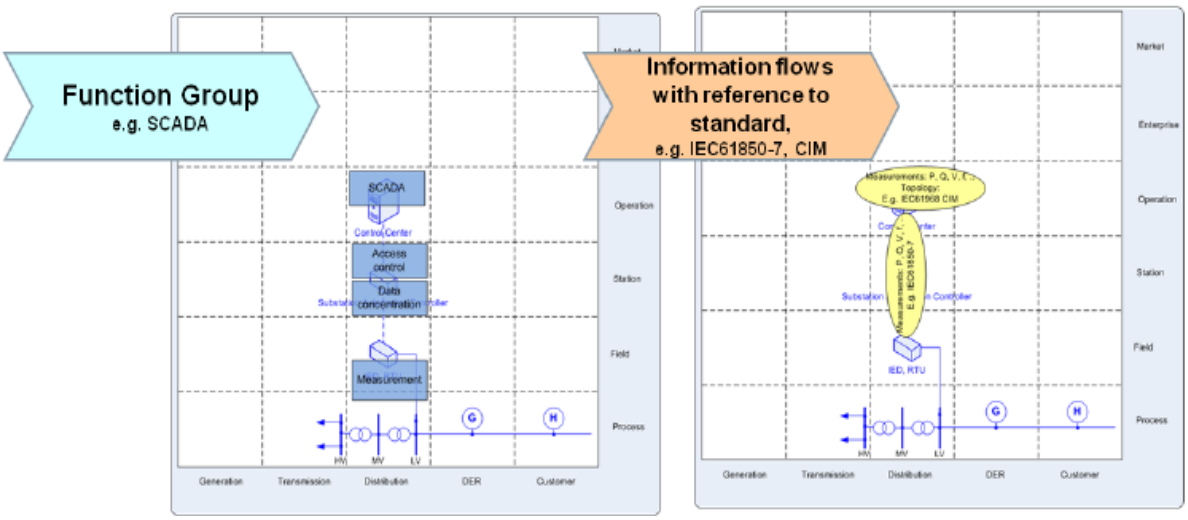


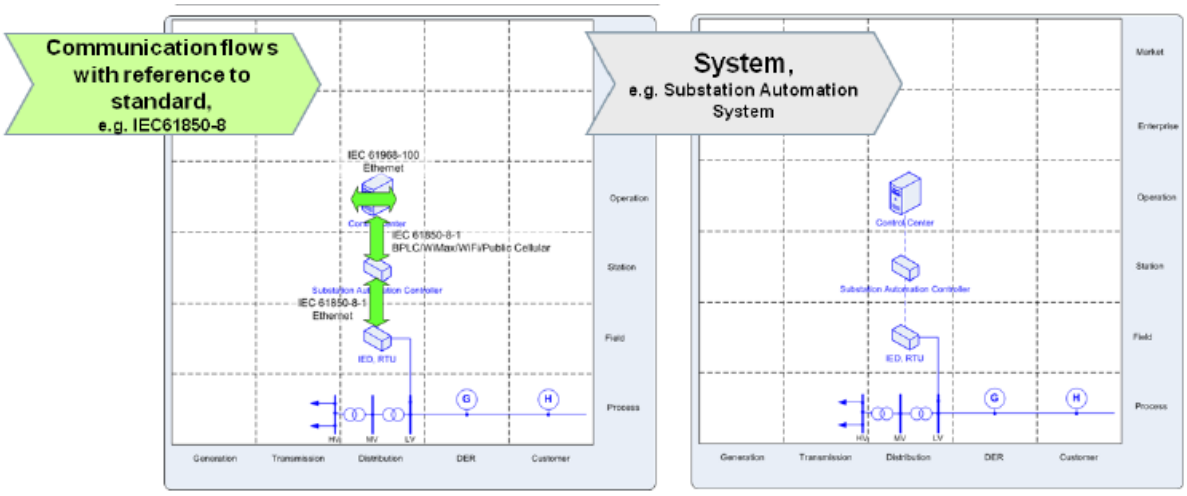
Les standards proposés par des organismes tels que le W3C, l'IETF ou par d'autres organismes sont donc valorisés par les groupes de normalisation IEC.

Une vision plus conceptuelle d'un système de téléconduite est offerte en utilisant le SGAM.

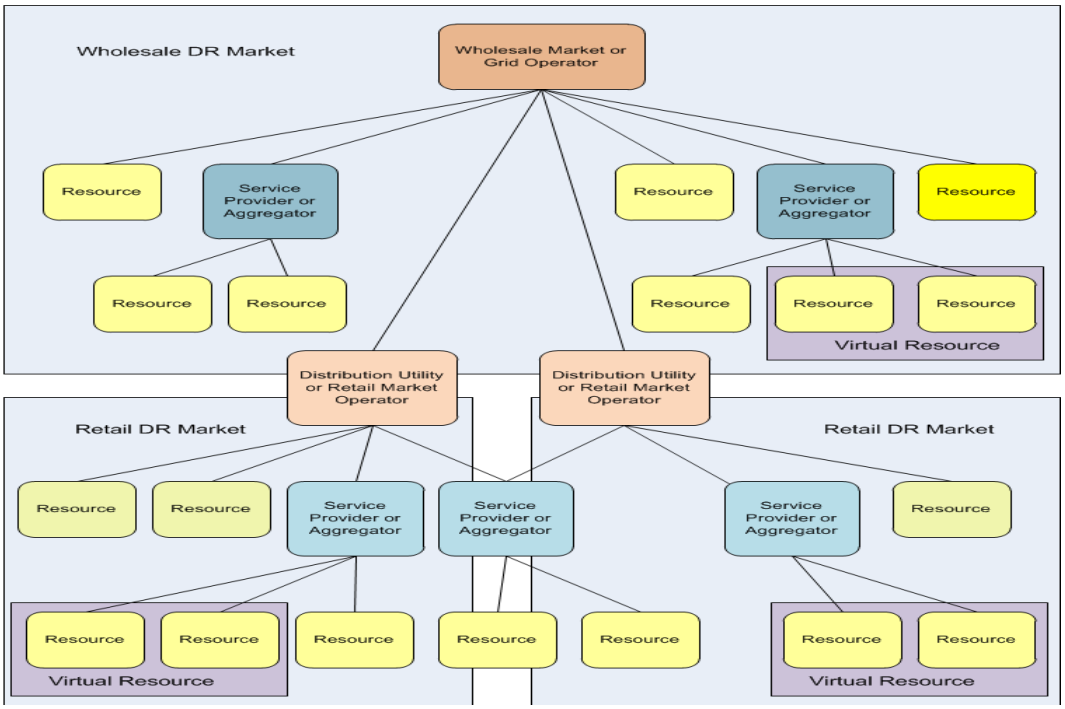
Une utilisation du SGAM est effectuée dans la feuille de route systèmes Smartgrid de l'IEC 63097 et a été adoptée dans de nombreux projets de R&D financés par la Commission Européenne.

La figure suivante illustre l'usage du SGAM pour projeter sur les différentes couches les composants fonctionnels, les normes associées aux échanges d'informations, aux protocoles de communication et aux systèmes physiques associés à la supervision d'un réseau de distribution.





La figure suivante illustre de façon macroscopique une architecture combinant marché de gros et marché de détail avec utilisation de ressources distribuées, pouvant être regroupées et mises à disposition par des agrégateurs.



L'aval compteur a ses problématiques propres, mais doit travailler à une harmonisation des flux d'informations avec l'amont compteur, pour un pilotage harmonieux du système électrique.

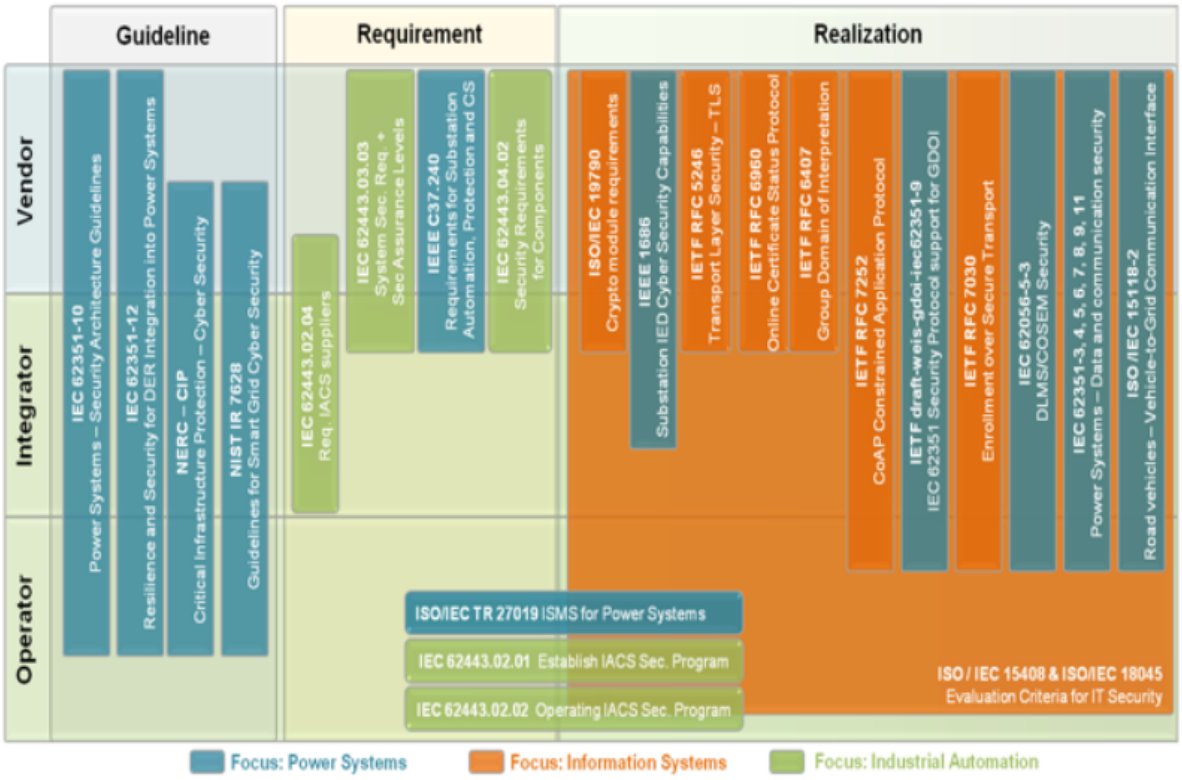
C'est l'objectif du groupe de travail TC 205 du CENELEC, qui traite des systèmes électroniques pour les foyers domestiques et les bâtiments, en coopération avec les experts « amont compteur » du TC 57 de l'IEC, mais aussi avec des associations généralement positionnées sur l'aval compteur.

Ces associations développent des modèles de données en dehors de toute architecture de référence existante, et doivent donc assurer les coûts d'adaptation du logiciel pour intégrer les langages du TC 57 (CIM, 61850).

Les normes pour la cyber sécurité

Mais interopérabilité ne veut pas dire vulnérabilité : tout doit être mis en œuvre pour que la cybersécurité soit de mise sur un système ouvert. Et là aussi, les normes volontaires peuvent aider à faire les choses avec rigueur et méthode.

Le groupe « **Cybersecurity** » du mandat M490 a produit un document sur les aspects cyber-sécurité qui a aussi alimenté les travaux de l'IEC.
La figure suivante illustre le panorama des normes de cyber-sécurité qui concernent les smartgrids :



La série des normes ISO/CEI 2700x :

. ISO/CEI 27000 : Introduction et vue globale de la famille des normes

. ISO/CEI 27001 : Norme d'exigences des SMSI

. ISO/CEI 27002 : Guide des bonnes pratiques en SMSI

. ISO/CEI 27003 : Guide d'implémentation d'un SMSI

. ISO/CEI 27004 : Norme de mesures de management de la sécurité de l'information

. ISO/CEI 27005 : Analyse des risques

. ISO/CEI 27006 : Guide de processus de certification et d'enregistrement

. ISO/CEI 27007 : Guide directeur pour l'audit des SMSI

. ISO/CEI 27008 : Lignes directrices de vérification en matière de mesures de sécurité

. ISO/CEI 27010 : Gestion de la sécurité de l'information des communications intersectorielles

. ISO/CEI 27011 : Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie des télécommunications

. ISO/CEI 27013 : Guide sur la mise en œuvre intégrée de l'ISO/CEI 27001 et de l'ISO/CEI 20000-1

. ISO/CEI 27014 : Gouvernance de la sécurité de l'information

. ISO/CEI 27016 : Management de la sécurité de l'information

. ISO/CEI 27019 : Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie

. ISO/CEI 27032 : Lignes directrices pour la cybersécurité

. ISO/CEI 27035 : Gestion des incidents

. ISO/CEI 27039 : Sélection, déploiement et opérations des systèmes de détection d'intrusion

. ISO/CEI 27040 : Sécurité de stockage

Norme ISO/CEI 27019 :

L'objectif de la norme ISO 27019 (version 2017) est de permettre aux différents acteurs de l'énergie (producteur, transporteur, distributeur, agrégateur) de mettre en œuvre un système de management de la sécurité de l'information (SMSI) dédié à cette industrie. Par rapport à la norme ISO 27002, qui est adaptée au SI « entreprise», la norme 27019 reprend la structure de cette dernière et fournit en plus des recommandations et des ajouts dédiés pour le SI « industriel » des énergéticiens.

La série des normes ISO/CEI 62443 :

La norme IEC 62443 issu des travaux de l'ISA 99) est une norme plus générique :

- IEC 62443-1-X : introduction à la norme
- IEC 62443-2-X : exigences de sécurité liées à l'organisation
- IEC 62443-3-X : exigences de sécurité liées aux systèmes et à l'architecture
- IEC 62443-4-X : exigences de sécurité liées au développement des composants industriels
- ...

Elle constitue un référentiel normatif à matière de cyber sécurité pour les SI des systèmes industriels (automate, Scada, IoT, Réseaux locaux industriels, capteur, actionneur). La norme IEC 62443 introduit des notions de « zone » et de « conduit » dans un SI industriel.

Un SI industriel est organisé en plusieurs zones indépendantes les unes des autres :

- Une zone regroupe un ensemble de sous-systèmes
- Un conduit est un canal de communication entre deux zones

La norme définit 5 niveaux de sécurité pour chaque zone : La Security Level 4 est la plus élevée (protection contre des violations intentionnelles utilisant des moyens illimités).

Les informations détaillées sont disponibles à l'adresse suivante : **http://www.isa-france.org/**

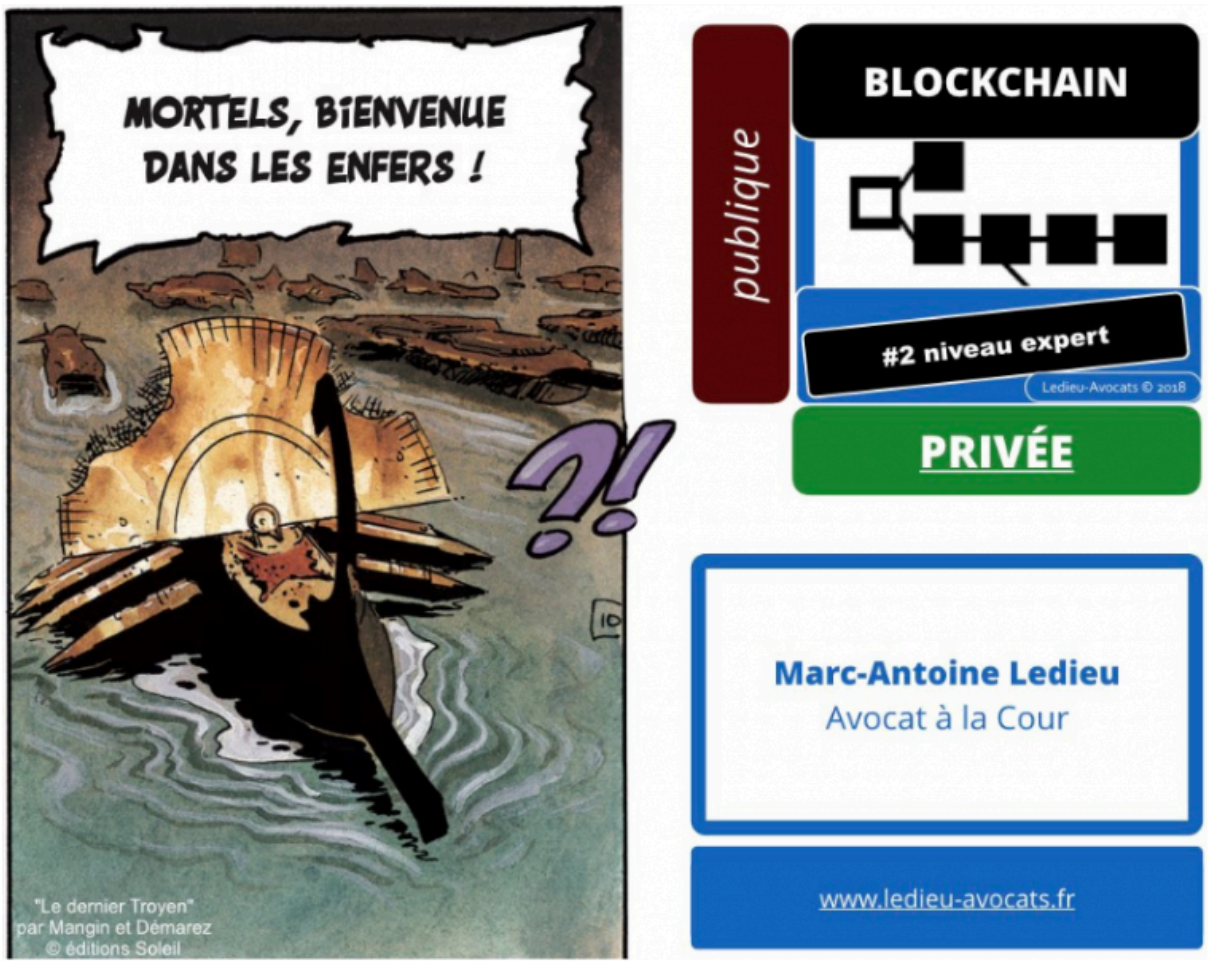
RDV donc dans les prochaines Newsletter et pour ceux qui s'intéressent au SMART GRID, rejoignez le Forum ATENA et **notre Atelier,** pour échanger et débattre avec nous sur ce sujet.
Pour mémoire, cet article 7 sur « la normalisation des Smartgrids » est organisé en 7 parties :

Partie1 : Introduction
Partie2 : L'émergence de normes pour les Smartgrids
Partie3 : L'architecture de référence
Partie4 : Les normes pour la cyber sécurité
Partie5 : L'utilisation concrète des normes
Partie6 : Les démonstrateurs
Partie7 : Les formations Smartgrids en France

Auteur:
Eric Lambert & Rolland Tran Van Lieu - Forum ATENA - Atelier SMART GRID

Blockchain privée vs blockchain publique (technique et juridique) expliqué en BD

Maintenant que vous êtes devenu(e)s des professionnel(le)s de la cryptographie, et parce que vous avez révisé les concepts techniques autours du protocole blockchain, vous êtes mûr(e)s pour faire un peu de droit. Dès à présent, faites vous à l'idée que le comparatif blockchain privée vs blockchain publique - pour ce qui est du droit - ne donne strictement aucun avantage aux blockchains publiques.



A part le droit pénal qui applique unilatéralement ses critères, si vous n'avez pas effectivement conclu de contrat, vous allez au devant de difficultés majeures. Tandis que si vous vous positionnez dans une blockchain privée, et que votre contrat est suffisamment détaillé, alors là, on peut discuter...

Lire / voir la suite >

Construire une France innovante

Le « Collectif Innovation » & la Société d'Encouragement pour l'Industrie Nationale, en partenariat avec Forum ATENA, des Ecoles & Universités (*CentraleSupelec, Telecom Paris Tech, Agro Paris Tech, Paris 1 Panthéon SorbonneMaster Management de l'innovation, Paris 4 Master Européen,SciencesPo Paris Ecole du Management et de l'Innovation)* vous invitent aux Assises 2018 de l'Innovation "Construire une France innovante" qui se tiendront Lundi 3 décembre 2018 de 15 à 22 heures à Hôtel de l'industrie 4 Place de St-Germain des Prés Paris 6°

Invitation gratuite. Inscription obligatoire

https://www.eventbrite.fr/e/billets-assises-de-linnovation-financement-gouvernance-51821752256

Ces Assises de l'Innovation constituent un premier rendez-vous annuel pour faire le point sur l'état de l'innovation en France. Elles réuniront une quarantaine d'experts : des dirigeants des plus grandes institutions, des responsables politiques, des investisseurs professionnels, des représentants de business angels, des économistes, des praticiens du droit et du chiffre, des étudiants.

Les Assises prévoient un regard détaillé sur l'écosystème de l'innovateur et ont l'ambition de mobiliser les leviers politiques, économiques, fiscaux, sociaux et culturels, qui permettront à la France de redevenir un leader de l'innovation dans le monde.

Notre dispositif pour l'innovation est stable depuis dix ans
Il est considéré par beaucoup comme suffisant. Il suffirait d'attendre un développement spontané sans ajout ni modification.

Pourtant si le dispositif juridico-fiscal est inchangé, son développement est hétérogène.

- la dépense pour le CIR (Crédit Impôt Recherche) est passée de quelques centaines de millions d'Euros à plus de 6 Milliards suite à la réforme de 2007 et ce décuplement constitue une réussite remarquable.

- inversement, le volume du financement des start-up en France est resté très « stable » autour de 1 Milliard par an. Ce phénomène se retrouve dans toute l'Europe. Cela conduit à une innovation entrepreneuriale très insuffisante.

Certes, il faudrait ajouter le financement des SATT et les fonds BPI en cours de création. Mais on reste loin du rythme de développement du CIR et cela n'est pas comparable à l'intensité de l'effort des USA en faveur de ses start-ups ; sans parler de l'efficacité du système américain. Cette année, les fonds US vont investir près de 120 Milliards $ en venture capital. L'intensité de l'effort est de 300 $/habitant alors que la France en est à 30 € environ, par habitant.

Le fossé ne se comblera pas seul ni sous l'impulsion d'un État omniprésent.

On peut faire mieux !... et pour y parvenir, le Collectif Innovation a sélectionné quatre domaines :
- le financement de l'amorçage et du décollage des start-ups, deux périodes cruciales de leur développement ; - la gouvernance de l'innovation, qui doit être à la fois plus souple, plus partenariale mais aussi plus structurée ; - un débat plus général sur les territoires d'innovation : la taille optimum pour fonder et accompagner le développement de l'écosystème de l'innovateur, et la répartition des pouvoirs entre ces niveaux.

Il faut étudier des solutions nouvelles sans dépenses publiques nouvelles.

Agenda

[03/12 - Assises de l'Innovation]
15:00 à 22:00 - Hôtel de l'industrie - 4 Place de St-Germain des Prés - 75006 Paris
En savoir + et s'inscrire

[03/12 - Lundi de l'IE : Cyber Sécurité vs Sécurité Numérique]
18:30 à 20:30 - Télécom ParisTech (Amphi Thévenin) - 46 Rue Barrault - 75013 Paris
En savoir + et s'inscrire

[06/12 - Jeudi de la Fibre (CREDO) : Le siècle du numérique, FTTH et 5G : les réseaux Télécoms de 2050]
18:30 à 21:00 - FNCCR - 20 boulevard La Tour Maubourg - 75015 Paris
En savoir + et s'inscrire

[09/12 - Conférence IREST : Comment l'humain va-t-il s'adapter aux Intelligences Artificielles ?]
18:00 à 20:00 - Télécom ParisTech (Amphi Emeraude) - 46 Rue Barrault - 75013 Paris
En savoir + et s'inscrire

[17/12 - Atelier Etat Plateforme]
18:30 à 20:00 - Télécom Evolution (salle DB 0005) - 39 rue Dareau - 75014 Paris
En savoir + et s'inscrire

[22 et 23/01 - Forum International de la Cybersécurité : Security and Privacy by Design]
Lille Grand Palais
En savoir + et s'inscrire

[12 & 13/02 - Conférences GO2S]
(guided optics &sensors Systems) par l'ARUFOG
Plus d'infos : http://arufog.org/