La Cybersécurité du Smart Grid

Le Déploiement du Smart Grid Nécessite une Nouvelle Approche en Termes de Cybersécurité

Contributeurs

Yves Aillerie, Intel Corporation
Said Kayal, Alstom Grid
Jean-Pierre Mennella, Alstom Grid
Raj Samani, McAfee
Sylvain Sauty, Intel Corporation
Laurent Schmitt, Alstom Grid

SYNTHESE

Alstom Grid, Intel et McAfee unissent leurs expertises pour donner leur point de vue sur la cybersécurité du Smart Grid:

- Qu'est-ce que le Smart Grid ?
- Le Paysage de la cybersécurité du Smart Grid
- Comment protéger le Smart Grid

Cette initiative met l'accent sur les défis associés à la migration vers un réseau électrique moderne, et les différentes approches permettant son élaboration, en prenant en compte les risques liés à la cybersécurité.

Qu'est-ce que le Smart Grid ?

Une Evolution Nécessaire

Les dernières projections de l'Agence internationale de l'Energie sont sans ambiguïté : les technologies Smart Grid sont devenues essentielles pour répondre aux changements radicaux qui interviendront dans le monde en matière d'énergie, à l'horizon 2030[1] :

- **La demande énergétique** mondiale devrait croître de 2,2 % par an, ce qui double la demande mondiale dans ce domaine.
- **Les émissions de CO2** dans le monde devraient connaître une accélération encore plus rapide, conduisant au premier choc critique en matière de changement climatique, et exposant le réseau à de nouvelles catastrophes environnementales. Dans le même temps, on observe un regain d'attention des populations à l'égard des défis environnementaux.
- **Les énergies renouvelables** intermittentes vont continuer à se développer, atteignant une moyenne de 25 % d'ici à 2050, et conduisant certains secteurs du réseau à absorber davantage d'énergies intermittentes que la consommation réelle à certains moments de la journée.

Le Smart Grid est une évolution du réseau électrique destinée à relever ces défis. Le Smart Grid est un réseau de transport et de distribution d'électricité que des capacités en termes de commande numérique, de surveillance et de télécommunications rendent plus performant. Il assure un échange bidirectionnel, en temps réel, d'énergie et d'information entre les différents acteurs de la chaîne de l'électricité, depuis le site de production jusqu'aux utilisateurs commerciaux, industriels et résidentiels.

Cette évolution est cruciale pour intégrer les ressources énergétiques renouvelables et distribuées, et améliorer l'efficacité et la durabilité du réseau électrique et des services associés. Mais le Smart Grid permettra d'autres contributions majeures :

- Infrastructures intelligentes et à énergie positive
- Meilleure gestion de la densité énergétique lors des pics de consommation

- Tarification en temps réel pour les consommateurs
- Services de mobilité intégrés
- Nouvelles centrales électriques virtuelles
- Micro-réseaux

Le Smart Grid aidera également les clients à mieux gérer leur consommation, et même à revendre sur le réseau l'électricité produite à domicile mais non utilisée. La figure 1 illustre l'éco-système spécifique au Smart Grid.

Le Smart Grid est plus qu'une infrastructure permettant la production, la distribution et la consommation plus intelligentes de l'électricité. Il aura un impact positif sur la société moderne, avec des avantages pour les individus et l'ensemble de la population.

Ce phénomène ressemble à bien des égards à la révolution de l'Internet. C'est un "Internet des Watts" qui peuvent provenir des sources d'énergie renouvelables, du stockage de l'énergie, des véhicules électriques ou des équipements des maison intelligentes.

Au-delà de ces ressources intelligentes connectées, le Smart Grid c'est également les écocitoyens, l'efficacité énergétique, les pratiques vertes, la mobilité, la sécurité nationale et la fiabilité.

Figure 1. L'éco-système du Smart Grid Source: Alstom Grid

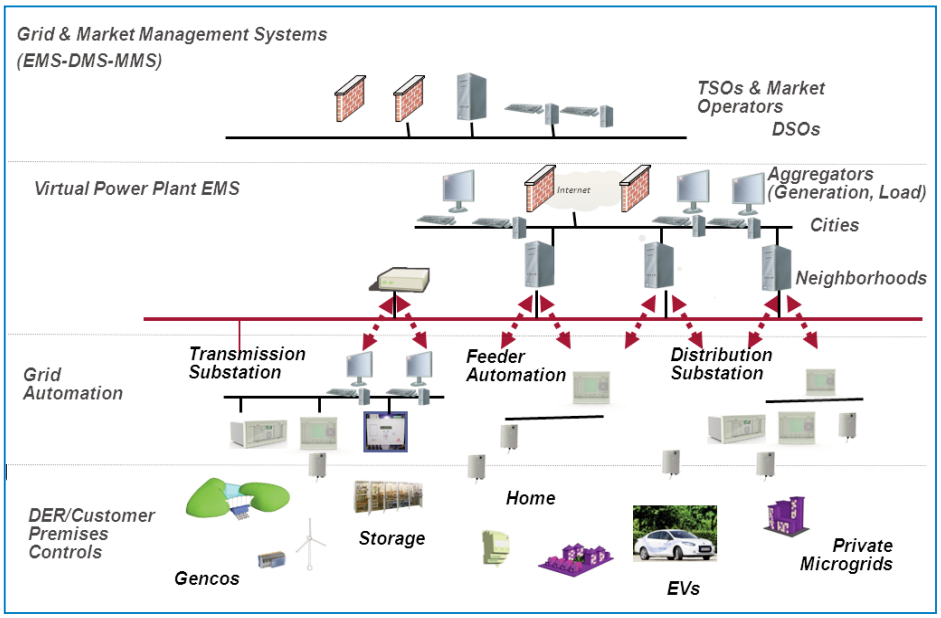


Figure 2. L'architecture en Couches du Smart Grid Source: Alstom Grid

Une Architecture en Couches

Les compagnies d'électricité du monde entier ont compris la nécessité de mettre en place de nouveaux systèmes Smart Grids, ajoutant ainsi une nouvelle couche d'équipements numériques à leurs infrastructures existantes pour interconnecter toutes leurs ressources—des super grids à ultra-haute tension jusqu'aux micro et pico réseaux à ultra-basse tension—aux immeubles et maisons.

Les technologies Smart Grid permettent d'améliorer les infrastructures actuelles—lignes électriques, postes électriques, salles de contrôle—en améliorant l'évaluation en temps réel de l'état du système. Les nouveaux équipements et dispositifs numériques peuvent être déployés de manière stratégique pour compléter l'existant. Utilisant une combinaison de systèmes IT centralisés et d'intelligence distribuée dans des noeuds de commande stratégiques — des commandes de centrales thermiques et des sites d'énergies renouvelables aux centres de contrôle de transmission et de distribution, en passant par les infrastructures commerciales et industrielles et les résidences individuelles— le Smart Grid peut apporter un niveau d'efficacité et de stabilité sans précédent au réseau électrique.

Les infrastructures d'Information et de communication joueront un rôle important dans la connexion et l'optimisation des couches disponibles.

La figure 2 montre l'architecture en couches du Smart Grid.

Un défi d'importance pour ces architectures nouvelles consiste à offrir une ouverture suffisante pour connecter des ressources historiquement cloisonnées tout en respectant les obligations de confidentialité et de respect de la vie privée et en réduisant les nouveaux risques associés à la cybersécurité.

Paysage de la Cybersécurité du Smart Grid

Les Normes de Cybersécurité

L'environnement Smart Grid s'appuie largement sur les normes, essentiellement pour garantir l'interopérabilité entre les systèmes. Les normes jouent également un rôle clé dans la cybersécurité de ce type de réseau.

Les normes permettant de développer la cybersécurité des Smart Grids sont déjà disponibles. Quelques améliorations, et des matériaux nouveaux, seront toutefois nécessaires pour refléter l'évolution du Smart Grid, ses technologies— et ses menaces. Certaines devront également être spécifiquement adaptées à l'environnement propre au Smart Grid.

Le défi consiste à maintenir ces normes dans le temps à un rythme approprié. Cela nécessitera des efforts substantiels, mais les avantages obtenus en contribuant au déploiement d'infrastructures Smart Grid sécurisées dès la conception en vaudront la peine.

Dans son rapport, le groupe de travail CEN-CENELEC-ETSI SG-CG/SGIS a choisi un scénario Européen pour illustrer la stabilité du réseau électrique, servant de référence à la définition de niveaux de sécurité (Tableau 1).[2]

La définition de ces niveaux contribue à jeter un pont entre l'exploitation du réseau électrique et la cybersécurité. Elle offre des directives pour aider à identifier les zones critiques où la sécurité compte le plus du point de vue de la stabilité globale du réseau électrique, depuis les super grids pan-Européens, jusqu'aux micro réseaux de quartiers.

Tableau 1. Niveaux de sécurité M/490 SG-CG/SGIS

Source: CEN-CENELEC-ETSI

Niveau de Sécurité	Scénario de Stabilité du Réseau Européen Exemples de Niveau de Sécurité
5 - Très Critique	▪ Ressources dont la défaillance peut engendrer une perte de puissance > 10 GW ▪ Incident pan-Européen
4 - Critique	▪ Ressources dont la défaillance peut engendrer une perte de puissance de plus de 1 GW à 10 GW ▪ Incident pays/Européen
3 - Elevé	▪ Ressources dont la défaillance peut engendrer une perte de puissance de plus de 100 MW à 1 GW ▪ Incident pays/régional
2 - Moyen	▪ Ressources dont la défaillance peut engendrer une perte de puissance de 1 MW à 100 MW ▪ Incident régional/ville
1 - Faible	▪ Ressources dont la défaillance peut engendrer une perte de puissance < 1 MW ▪ Incident ville/quartier

Des Cyber Menaces en Rapide Evolution

Le paysage des cyber menaces évolue rapidement et ces dernières années ont vu une croissance exponentielle de celles-ci. Dans son rapport du 4e trimestre 2012 sur les menaces, McAfee indique : « Les découvertes de nouveaux malwares ont cette année augmenté de 50 %, avec plus de 120 millions d'échantillons figurant dans le labo McAfee. ».[3]

Les figures 3 et 4 montrent les échantillons de malwares (logiciels malveillants) figurant dans la base de données du laboratoire McAfee, et les nouveaux échantillons de malwares.[4]

Les cyber menaces évoluent et deviennent hautement sophistiquées. Les menaces avancées persistantes (advanced persistent threats [APT] en Anglais) illustrent parfaitement cette mutation. De surcroît, les attaquants ne sont plus aujourd'hui des amateurs mais des professionnels compétents et organisés, capables de lancer des attaques complexes et coordonnées à l'aide d'outils sophistiqués.

De nombreux types de cyber menaces sont aujourd'hui bien connues :

- Hackers
- Malwares (logiciels malveillants)
- Zero days (attaques 0-day)
- Botnets
- Dénis de service
- Dénis de service distribués

Autant de menaces que nous côtoyons depuis de nombreuses années.

Les systèmes d'Information ont toujours été la cible des cyber-attaquants. Ce qui est relativement nouveau c'est la prise de conscience, depuis la découverte en 2010 de Stuxnet[5], le premier malware découvert ciblant les systèmes de contrôle industriels, que ces derniers sont également vulnérables aux cyber-attaques.

Les réseaux électriques sont des cibles stratégiques de choix qui doivent être protégées des cyber menaces.

L'architecture du Smart Grid
Les couches Smart Grids nécessitent une approche système de systèmes, avec des besoins différenciés en termes de sécurité.

Le Smart Grid inclut différents domaines :

- Production d'électricité
- Transport
- Distribution
- Sources d'énergie distribuées
- Villes intelligentes
- Consommateurs finaux

Il s'appuie sur une multitude d'acteurs et d'intervenants, ayant chacun un rôle et des activités spécifiques dans un domaine donné.

L'architecture Smart Grid est un système de systèmes: un système vaste et complexe comprenant des systèmes plus petits et plus simples, distribués et interconnectés. Chacune des entités plus petites a un impact systémique différent sur la stabilité de l'ensemble, qui nécessite une évaluation appropriée.

Utilisant les niveaux de sécurité M/490 SG-CG/SGIS (Tableau 1), la figure 5 montre comment cela peut être transposé à l'architecture du Smart Grid.

Chaque sous-système, avec ses ressources associées, nécessite des fonctions et des solutions de sécurité spécifiques. Par exemple, la solution pour sécuriser un poste électrique n'est pas la même que la solution destinée à sécuriser les systèmes d'effacement et de gestion d'énergie domestique.

Cela ne signifie pas pour autant que les sous-systèmes dont le niveau de criticité est "moins important" ne doivent pas être sécurisés. A chaque niveau, les mesures de sécurité doivent être suffisantes pour réduire les risques. Pour protéger efficacement l'ensemble du réseau, les différents sous-systèmes ne doivent pas nécessairement être alignés sur le sous-système présentant les exigences de sécurités les plus élevées, chacun ayant un rôle spécifique à jouer au sein de l'éco-système.

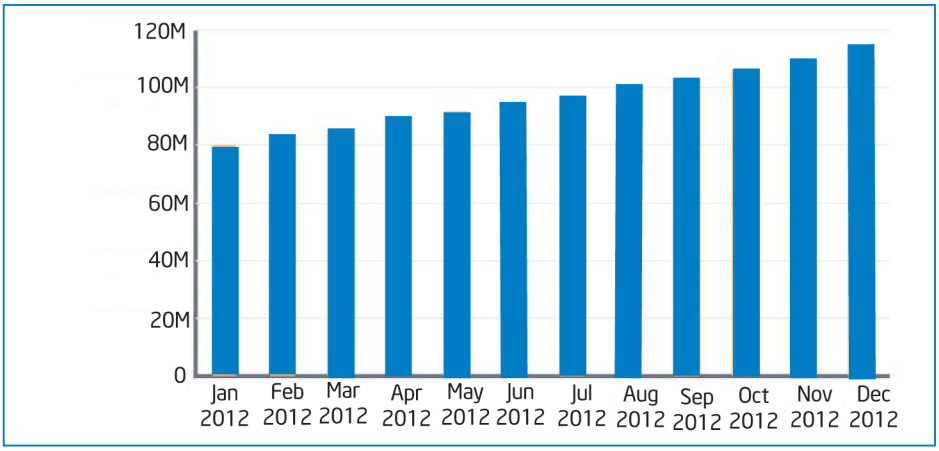


Figure 3. Totalité des échantillons de Malwares dans la Base de Données McAfee Labs Source: McAfee

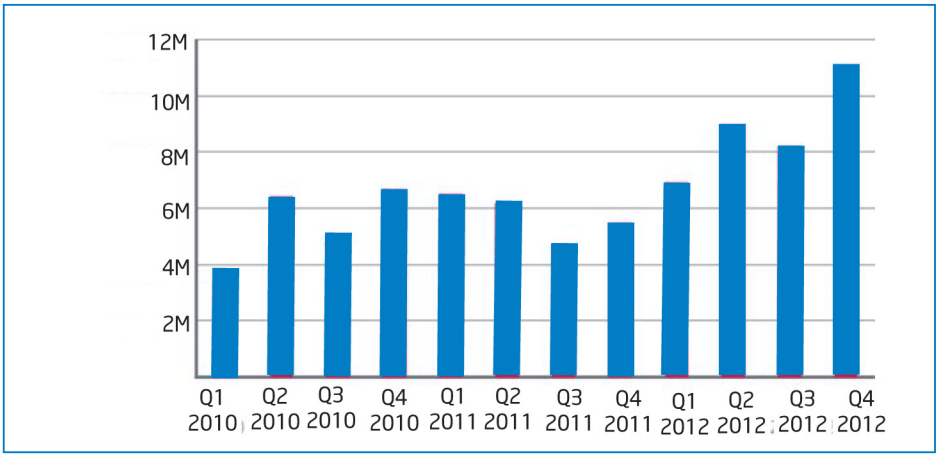


Figure 4. Echantillons de Nouveaux Malwares Source: McAfee

Les acteurs du Smart Grid doivent analyser les niveaux de sécurité, dans la perspective d'une évaluation globale des risques pour chaque type d'utilisation du Smart Grid, et pour les sous-systèmes considérés au sein de l'architecture globale.

Spécificités de la Cybersécurité
La Commission Européenne a exprimé son intérêt à propos de mesures destinées à assurer un niveau de sécurité commun des réseaux et de l'information au sein de l'Union.[6] La Maison Blanche a elle aussi montré sa préoccupation à propos de la cybersécurité et de la protection des infrastructures critiques.[7]

Etant par nature un vaste système de systèmes distribués et interconnectés, le Smart Grid offre une surface d'attaque exceptionnellement large. Chacune de ses ressources- passerelles domestiques, compteurs intelligents, postes électriques, salles de contrôle—constitue une cible potentielle pour une cyber attaque. De fait, une attaque affectant un noeud critique peut mettre en danger la sécurité du réseau et entraîner par effet systémique une panne complète du réseau électrique.

Le défi en matière de cybersécurité du Smart Grid consiste à protéger le nombre sans-cesse croissant de ressources du Smart Grid et leurs voies de communication des cyber menaces qui évoluent en permanence.

Protéger l'Architecture de Bout en Bout

Pas de Solution Miracle

Pour maintenir la stabilité de l'ensemble du réseau, la plupart des sous-systèmes du Smart Grid doivent pouvoir continuer à fonctionner en toutes circonstances—même en cas d'attaque de l'une des ressources, ou si l'une d'entre elles est compromise.

Les technologies et les bonnes pratiques actuelles en matière de cybersécurité—antivirus, pare-feux, systèmes de prévention d'intrusions, architecture sécurité, défense en profondeur et durcissement de système—sont nécessaires pour protéger le Smart Grid. Pour autant, l'histoire nous montre qu'elles ne sont qu'une partie de la solution.

Contrer des menaces évoluées et hautement sophistiquées, comme les menaces avancées persistantes, nécessite des technologies de cybersécurité elles aussi avancées, comprenant entre autres, les solutions de gestion des événements et des informations de sécurité, en anglais security information and event management (SIEM), les solutions de liste blanche d'applications et les fonctionnalités de sécurité intégrées au niveau du processeur.

Sécuriser le Smart Grid nécessite donc la combinaison de technologies de cybersécurité standard et avancées.

Sécurité dès la conception

Avec l'évolution constante des menaces, des technologies avancées en matière de cybersécurité sont nécessaires pour assurer une protection efficace.

En fournissant des informations complètes et en temps réel sur les menaces, les solutions de cybersécurité sont à même de protéger les réseaux contre les cyber menaces provenant de multiples vecteurs. Destinées à collecter des données à partir des équipements, réseaux et applications, les solutions de gestion des événements et des informations de sécurité (SIEM) ciblent les événements sécurité afin d'identifier les risques et les menaces basés sur l'analyse des données internes et externes. Ces systèmes sont déployés dans des zones sécurisées et isolées, ou dans de larges zones distribuées, ce qui s'avère très important pour obtenir une appréciation adéquate de la situation entre les zones. Les systèmes SIEM collectent et agrègent les informations provenant des cyber systèmes, et fournissent ensuite des informations sur les risques et menaces, via un processus automatisé qui aide à la prise de décision.

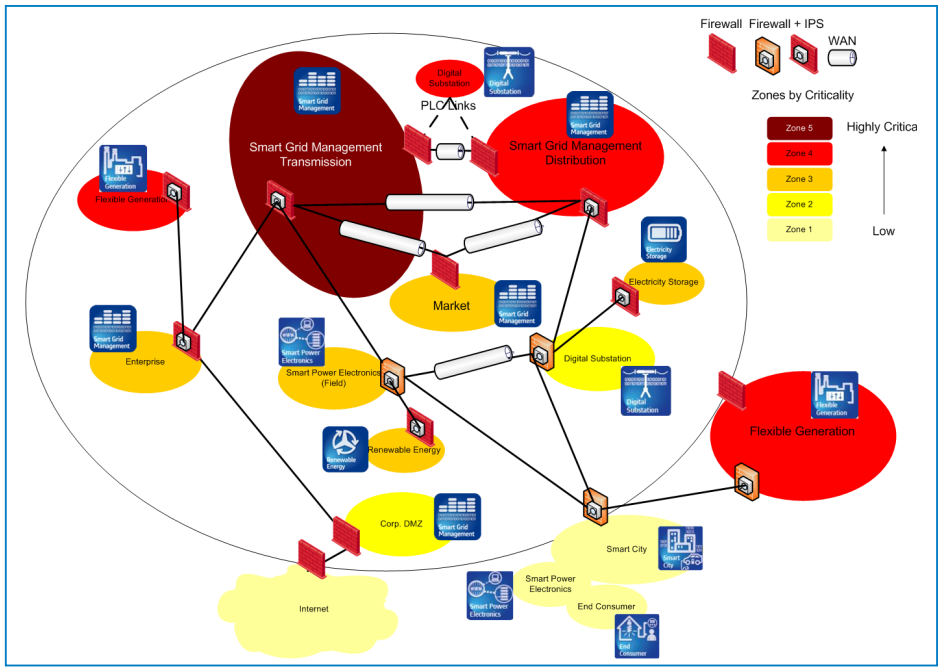


Figure 5. Architecture Smart Grid avec des besoins en sécurité différents Source: Alstom Grid

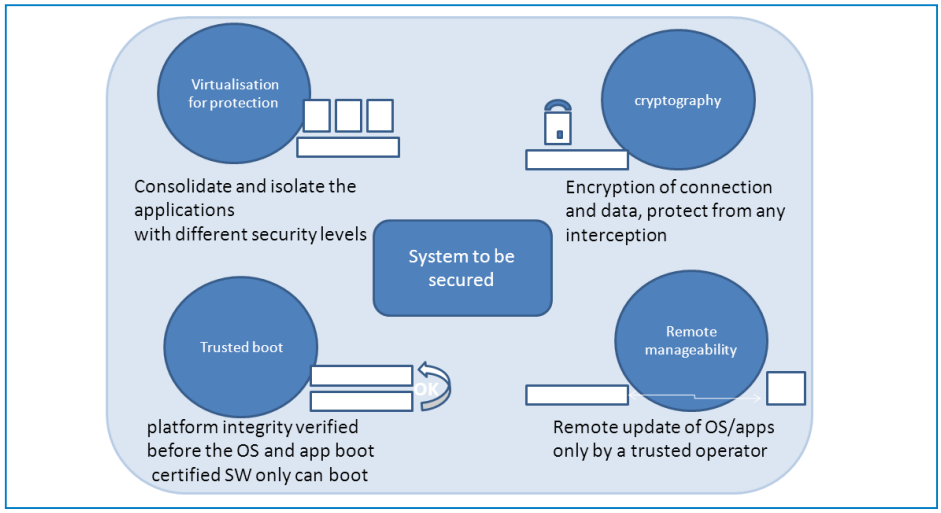


Figure 6. Fonctionnalités de sécurité Assistées par intégration dans le Matériel, (Processeur, Chipset) Source: Intel

Les solutions de liste blanche d'applications peuvent compléter les technologies classiques de protection contre les malwares comme les anti-virus, et s'avèrent être une alternative valable lorsque ces technologies traditionnelles ne peuvent être mises en oeuvre. Les solutions de liste blanche d'applications, via une liste de fichiers connus, permettent de s'assurer que seuls les fichiers autorisés seront exécutés. Les logiciels non autorisés (par ex. les malwares) ne peuvent être exécutés sur les systèmes qui bénéficient de cette technologie. Cette technologie est particulièrement bien adaptée aux environnements dans lesquels les systèmes utilisés sont stables.

Enfin, la sécurité assistée par matériel permet aux systèmes de se montrer plus résistants , et contribue à réduire le temps nécessaire à un retour en service normal en cas d'incident ou d'attaque (Figure 6).

Des chipsets spécifiques permettent la sécurisation, la maintenance et le contrôle à distance des systèmes (système d'exploitation, BIOS, patchs d'applications) sur des réseaux eux-mêmes sécurisés. Parmi toutes leurs fonctions, ces chipsets intègrent des circuits dédiés aux traitements relatifs à la sécurité. Ces plates-formes peuvent également détecter les manipulations physiques du système, en enregistrant toute manipulation physique du système, et en détectant tout changement dans les composants matériels.

La virtualisation matérielle peut isoler les environnements d'exécution et séparer l'accès mémoire, confinant ainsi une attaque aux limites d'une machine virtuelle. Cette dernière peut être rechargée aisément à partir de sa dernière image stable connue.

Un processus de démarrage intégré, fiable et sécurisé, permet de vérifier l'intégrité de la plateforme avant d'installer l'hyperviseur et les machines virtuelles.

De plus, des circuits intégrés de chiffrement offrent des fonctionnalités performantes et rapides, telles que le standard de chiffrement avancé (AES, Advanced Encryption Standard) et les générateurs aléatoires, qui peuvent être utilisées pour le chiffrement des communications et du stockage. Ces circuits fournissent également des capacités de stockage sécurisées pour les clés cryptographiques.

Pour être véritablement efficaces, ces différentes technologies avancées doivent être adaptées aux modèles spécifiques des Smart Grids. Ce sont là des mesures nécessaires pour construire des architectures Smart Grid intrinsèquement sécurisées dès la conception.

Conclusion

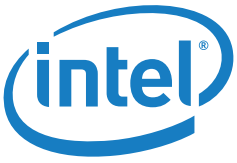
Les premières expériences acquises à l'occasion de démonstrateurs Smart Grids révèlent que les nouvelles architectures se développent sous la forme de combinaisons de nouveaux cas d'utilisation et d'acteurs, venant s'ajouter aux infrastructures existantes. Ce qui nécessite l'interconnexion des sous-systèmes existants avec les nouveaux éléments.

Cela induit intrinsèquement une augmentation de la surface d'attaque et nécessite donc de prendre de nouvelles mesures de réduction des risques en prenant en compte l'impact potentiel d'une attaque sur la stabilité du réseau électrique de bout en bout. Cela nécessite une nouvelle approche pour gérer les cyber-risques de manière consistante par rapport aux risques traditionnels liés à la gestion des réseaux électriques. Cela nécessite également de permettre aux opérateurs de réseaux électriques de pouvoir évaluer la situation en cas de cyber-attaque.

Ce n'est qu'en ayant une parfaite connaissance de ce qu'est le Smart Grid, de ses forces, de ses faiblesses et des menaces auxquelles il doit faire face qu'il sera possible de construire des architectures Smart Grid intrinsèquement sécurisées dès la conception.

Grand stratège militaire, Sun Tzu expliquait déjà au VIe siècle av. J-C : "Si tu connais ton ennemi et si tu te connais, tu n'auras pas à craindre le résultat de cent batailles. Si tu te connais toi-même sans connaître ton ennemi tes chances de victoires et de défaites seront égales. Si tu ne connais ni ton ennemi ni toi-même tu perdras toutes les batailles."[8]

La cybersécurité est un sujet de préoccupation croissant et un facteur de succès clé pour le déploiement du Smart Grid. Alstom, Intel et McAfee s'associent pour répondre aux opportunités Smart Grid de manière sure et efficace.



1 Agence internationale de l'Energie "Technology Roadmap: Smart Grids," http://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf (2011).

2 CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart Grid Information Security," ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf (Novembre 2012).

3 McAFee Labs, "McAfee Threats Report: Fourth Quarter 2012 Executive Summary," http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012-summary.pdf (2013).

4 McAFee Labs, "McAfee Threats Report: Fourth Quarter 2012," http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf (2013).

5 "Stuxnet," Wikipedia.org, http://fr.wikipedia.org/wiki/Stuxnet (Mai 2013).

6 Communiqué Union européenne "EU Cyber Security Plan," http://europa.eu/rapid/press-release_IP-13-94_en.htm?locale=en (7 février 2013).

7 Communiqué Maison Blanche "Executive Order: Improving Critical Infrastructure Cybersecurity," http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

8 Sun Tzu, "L'art de la Guerre," http://artdelaguerre.com/

0513/YA/SS