

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la recherche scientifique
Université A.MIRA BEJAIA
Faculté de la Technologie
Département de Génie Electrique



Mémoire de fin d'études
En vue de l'obtention de diplôme
Master en électrotechnique
Option : Réseaux Electriques

Thème

***Aspects économiques et sécurité informatique
dans les projets Smart Grids : Etude de cas.***

Présenté par :

ZEMOURI Yassine

REMILI Karim

Encadré par :

M^r. MEDJOU DJ Rabah

M^{elle} IBERRAKEN Fairouz

Promotion 2012/2013.

Remerciements

Nous tenons à adresser nos plus vifs remerciements à Monsieur **Rabah MEDJOUDJ**, Maître de conférences au département Génie Electrique, pour nous avoir confié ce sujet d'actualité. Il nous a dirigés avec beaucoup d'efforts et de patience, son soutien moral, sa compréhension et ses encouragements constants, non seulement dans ce travail, mais aussi durant notre cursus universitaire. Ses idées et son dynamisme nous ont beaucoup inspirés.

Nous exprimons également notre profonde gratitude à Mr **Med. BOUTEBEL** et **Mme AOUZELLAGUE**, enseignants chercheurs au département génie électrique, nous tenons à leur exprimer notre plus profonde reconnaissance pour leur suivi pédagogique et leurs conseils aussi bien en Licence qu'en Master, et d'avoir accepté de faire partie du jury et examiner le présent travail.

Nous tenons très sincèrement à témoigner toute notre reconnaissance à **Melle IBERRAKEN Faïrouz**, doctorante au niveau du même département qui travaille sur les smart grids, pour les conseils et commentaires qui ont été très instructifs. Nos remerciements vont également à **Mr MEDJDOUB**, adjoint chef du département, pour son écoute et ses conseils dans les moments difficiles.

Évidemment nous ne saurions oublier **Mme N. TAHAKOURT**, du département informatique, pour son aide et ses conseils.

Dédicace

*A mon père et ma très chère maman, qui m'ont éclairés
Le chemin en me donnant la main tout au long de mes années
d'études*

<< Que dieu me les gardes >>.

A mes frères (Riad, Mourad).

A mes sœurs (Katia, Samira, Nawal, Ferial).

A toutes ma famille.

A tous mes amis de la promotion.

A tous mes amis sans exception.

Yassine

-
- ✚ *A mes chers parents qui ont beaucoup sacrifié pour nous, et faire de moi leur 8ème et dernier diplômés, Dieu les bénisse ;*
 - ✚ *A mes frères et sœurs ;*
 - ✚ *A tous mes amis, particulièrement **Massi** le fidèle depuis ma première classe 1995.*
 - ✚ *A mes cousins et cousines, particulièrement **Hamid**.*
 - ✚ *A la mémoire de **Zi Lahlou Anki**, le maçon du village qui nous a quittés récemment. Il a beaucoup estimé les étudiants.*
 - ✚ *A la mémoire de mon grand père **Md Amokrane**, qui vient de nous quittés en rédigeant même ses dédicaces, une semaine avant le dépôt de ce mémoire.*

Je dédie ce modeste travail.

Karim

Sommaire

Introduction Générale.....	1
Croissance de l'industrie des smart grids	
Introduction	3
<u>I.1</u> Historique du développement des smart grids	3
<u>I.2</u> Les visages des smart grids dans le monde.....	4
I.2.1 Cas des pays de l'Europe	4
I.2.2 Cas des USA	5
I.2.3 Cas de la Chine	6
I.2.4 Cas de l'Inde	6
<u>I.3</u> Croissance du marché des smart grids	7
I.3.1 Les grands projets smart grids dans le monde	7
I.3.2 Estimation du marché des smart grids	10
<u>I.4</u> Conclusion	12
Développement des services liés aux smart grids	
Introduction	13
II.1 Les acteurs de l'industrie du système électrique intelligent	13
II.2 la chaîne de valeur du système électrique intelligent	14
II.2.1 Le système électrique	15
II.2.2 Consommateur.....	16
II.2.3 L'agrégateurs : un nouveau métier pour le marché électrique	17
<u>II.3</u> Le développement des véhicules électriques.....	18
II.3.1 Electromobilité et intégration au réseau	18
II.3.1.1 Le « Vehicle-to-grid » pour limiter l'impact des pics de consommation.....	19
II.3.1.2 le Smart Garage	20
<u>II.4</u> Construction d'offre de services du stockage pour les réseaux de distribution du futur. . 21	
II.4.1 La valorisation du stockage distribué : une approche « multifonction ».....	21
II.4.2 Services du stockage à valeur « distributeur »	22
II.4.2.1 Lissage des transits de pointe (SD1).....	22
II.4.2.2 Réglage local fin et dynamique de la tension (SD2)	23
II.4.2.3 Soutien au réseau en fonctionnement dégradé (SD3).....	23
II.4.2.4 Renvoi de tension en poche locale (SD4).....	23

Sommaire

II.4.3 Services du stockage distribué à valeur « producteur décentralisé».....	24
II.4.4 Services du stockage distribué à valeur « consommateur »	24
II.5 Intégration des EnR dans les smart grids.....	25
II.6 Normalisation dans les réseaux électrique intelligents	25
II.6.1 Normes de transport et de distribution	26
II.7 Conclusion	27

Calcul technico-économique

Introduction	28
III .1 Analyse coût-bénéfices	28
III .1-1 Description	28
III.1-2 Les étapes pratiques de L' Analyse Coût-Bénéfices.....	29
III.1-3 Objectifs de l' Analyse Coût-Bénéfices :	31
III.2 Méthodes analytiques de planification	31
III.2-1 La fonction de coût.....	32
III.2-2 Les dépenses en investissements	32
III.2.2.3 coût des pertes.....	33
III.2-3 La gêne économique.....	34
III.2-4 Le gain	35
III.3 Etude de cas ou application :.....	35
III.3-1 Calcul du coût de la variante "V0".....	35
III.3-2 Calcul du coût de la variante "V1".....	35
III.3-3 Calcul Le gain	36
III.4 Autre impacte des smart grids	37
III.4-1 Détecteur de défaut	37
III.6. CONCLUSION	38

Sécurité informatique

Introduction	39
IV.1 Définition	39
VI.2 Mécanismes de sécurité	40
IV.3 Risques, menaces et politique de sécurité.....	40
IV.3.1 Risques.....	41
IV.3.2 Menaces	42
IV.3.3 Politique de sécurité	42
IV.4 Analyses des vulnérabilités des smart grids.....	42

Sommaire

IV.4.1	Méthode d'analyse MEHARI	43
IV.4.1.1	Présentation de la méthode MEHARI.....	44
IV.4.1.2	Démarche de l'analyse	44
IV.4.1.3	MEHARI appliquée au comptage évolué, compteur intelligent.....	45
IV.5	sécurité du comptage numérique évolué.....	46
IV.5.1	Les communications dans les compteurs communicants.....	46
IV.5.1.1	Protocole de communication TCP/IP.....	47
IV.5.1.2	Unicité de l'adresse IP d'un compteur communicant.....	49
IV.5.2	Sécurité par Infrastructure à clef publique.....	50
IV.5.2.1	Rappel sur la cryptographie.....	50
IV.5.2.2	Chiffrement à clef publique, asymétrique	50
IV.5.2.3	Algorithme RSA pour le cryptage des données du compteur	51
IV.5.2.3.1	Principe.....	51
IV.5.2.3.2	Programmation sur le langage C	52
IV.5.2.3.3	Programme de cryptage	54
IV.6	Conclusion	55
	Conclusion générale	56

Liste des figures

Figure 1.1 : Evaluation de la taille du marché mondial en milliards de \$ par ans.	12
Figure 2.1 : Les industries impliquées dans le smart grid.	14
Figure 2.2 : Représentation de la chaîne de valeur d'un système électrique intelligent	16
Figure 2.3 : Interactions Agrégateur-Autre acteurs, dans les smart grids	17
Figure 2.4 : Schéma de l'architecture du système de régulation envisagé par AC Propulsion	19
Figure 2.5 : Une illustration du stockage pour le lissage de la charge	22
Figure 2.6 : Architecture des normes de réseau intelligent selon la CEI 62357	26
Fig.3.1 : Les étapes pratiques de l'Analyse Coût-Bénéfice	30
Figure 4.1 : Objectifs de la sécurité d'informations d'un système	40
Figure 4.2 : Infrastructure à analyser pour la sécurité dans le smart grid	43
Figure 4.3 : Démarche de sécurité par MEHARI	45
Figure 4.4 : Correspondance entre modèle OSI et protocole TCP/IP	48
Figure 4.5 : Exemple d'adresse IP d'un compteur	49
Figure.4.6 : procédé de chiffrement des PKI	51

Introduction générale

Introduction générale

Le concept traditionnel des réseaux électriques est dans une phase de dépassement. Il ne s'agit pas uniquement de changer les lignes, les interrupteurs, les transformateurs, mais également l'électronique, l'informatique et le mode de communication. Tels que nous les connaissons, ces réseaux se transformeront en réseaux intelligents. Les smart grids sont ces infrastructures nouvelles qui permettent une gestion bidirectionnelle en temps réel de l'électricité et des informations associées, grâce à l'utilisation des technologies numériques. Ce mix innovant permet non seulement une meilleure intégration des énergies renouvelables, mais également un acheminement et une gestion de l'électricité de manière plus efficace sur l'ensemble du réseau.

Le nombre d'applications qui peuvent être employées sur le réseau intelligent une fois la technologie de communications déployée se développe aussi rapidement que les entreprises inventives peuvent les créer et les produire. Le déploiement de tel système requiert un effort important de recherche-développement et des investissements considérables. Les rapports de certains économistes estiment que ces cinq dernières années les recettes de l'industrie des smart grids avoisineront les 13 milliards de dollars et que le taux de croissance tourne autour de 23%.

Alors que les réseaux intelligents poursuivent leur déploiement, la nécessité d'une sécurité accrue sur les réseaux se fait de plus en plus pressante et les géants de l'informatique comme IBM, Oracle, et Cisco se positionnent sur ce nouveau marché.

En effet, le marché associé à la sécurité est immense : Pike Research a récemment publié un rapport selon lequel, la cyber-sécurité devrait représenter un marché de \$21 milliards entre 2010 et 2015 avec un revenu annuel de \$3.7 milliards en 2015 [1]. Les investissements relatifs à la sécurité devraient correspondre à 15% de l'investissement total dans le Smart Grid [2]. L'Amérique du nord devrait être la part la plus importante du marché avec un revenu de \$1.5 milliards, cependant d'autres régions comme l'Asie pacifique (\$1.2 milliards) et l'Europe (\$784 millions) devraient voir leur part grandir rapidement.

Concernant la consommation de l'énergie électrique, il est utile de traiter les aspects économiques liés à l'intégration de ces Smart Grids dans les réseaux électriques. Un aspect particulier attire l'attention, et il s'agit d'évaluer les capacités de ces systèmes intelligents à réduire les coûts d'investissements occasionnés par l'insertion de la production d'énergies

Introduction générale

renouvelables aux réseaux de transport et de distribution. Un autre aspect qui attire l'attention est lié à la sécurité informatique, car ces mesures de sécurité sont conçues pour protéger le réseau électrique contre les attaques par les terroristes et les pirates, ainsi que le renforcement de sa résistance contre les catastrophes naturelles et les menaces involontaires telles que les pannes d'équipement et les erreurs des utilisateurs.

Ce travail a pour objectif de présenter deux aspects économiques et sécurité informatique des projets smart grids.

Le mémoire est structuré comme suit :

Le premier chapitre traite de la croissance de l'industrie des smart grids. Dans ce chapitre on va se baser sur le visage des smart systèmes dans le monde et la croissance de marché des smart grids ;

Le deuxième chapitre traite le développement des services liée aux smart grids ;

Quant au troisième chapitre, il traite le calcul technico-économique. Dans ce chapitre on va parler sur une méthode analyse cout-bénéfice et on va faire une petite application sur l'investissement des équipements des smart grids (compteur intelligent) ;

Dans le dernier chapitre, on va parler sur la sécurité informatique.

Une conclusion générale clôturera ce travail.

Introduction

Les avancées technologiques actuelles permettent d'engager une mutation du système électrique de nature à rendre active la demande des consommateurs. L'industrialisation pour une mise en œuvre à grande échelle, les coûts associés aux solutions proposées, ainsi que le facteur humain lié aux comportements des consommateurs constituent autant de freins majeurs au déploiement des réseaux intelligents dits smart grids (SG).

Un réseau électrique intelligent est un réseau qui est capable d'intégrer au meilleur coût les comportements et les actions de tous les utilisateurs qui y sont reliés : producteurs, consommateurs ainsi que ceux qui sont les deux à la fois. L'objectif est d'assurer au système électrique une grande pérennité et rentabilité, avec des pertes faibles et avec des niveaux élevés de sécurité, de fiabilité et de qualité de la fourniture.

I.1 Historique du développement des smart grids

L'histoire des réseaux et des systèmes électriques conventionnels permet de comprendre les raisons de leur développement actuel, leur mode de fonctionnement mais aussi leur limitation par rapport à un avenir énergétique en pleine évolution. L'arrivée des énergies locales essentiellement renouvelables a donné lieu à des adaptations pour permettre l'insertion de ces énergies dans le système électrique initialement non conçu pour les accueillir.

Historiquement, les réseaux électriques ont une architecture centralisée et une communication unidirectionnelle du producteur au consommateur. Le déploiement des smart grids accompagne la modernisation des réseaux et des infrastructures vers une architecture décentralisée. L'objectif est d'intégrer une multitude de sources d'énergie renouvelable de toutes tailles, et de permettre de nouveaux modes d'utilisation et de stockage de l'électricité (véhicules électriques). A l'intérieur de ce réseau électrique évolué, le consommateur final disposera des outils et services lui permettant de connaître sa consommation et d'interagir en temps réel. L'approche est donc orientée vers une demande « active », grâce à des compteurs intelligents (smart meters) et des échanges bidirectionnels.

L'évolution du réseau électrique a été très lente; il a longtemps été conçu autour de sa fonction première : couper, protéger, transformer, évoluant pour « seulement » devenir plus compact, plus performant grâce à une technologie de mieux en mieux maîtrisée. Cette évolution a rarement été suffisante pour en justifier le remplacement sur le terrain.

Ce n'est que depuis 20 ans que l'adjonction de fonctions de communication a progressivement transformé ce matériel : on peut désormais le commander à distance et, de ce fait, agir de manière dynamique sur le réseau électrique pour en optimiser les performances ou pour assurer une meilleure continuité de service. Par ailleurs, il s'est transformé en capteur d'informations relatives au matériel lui-même ou au courant qui le traverse. Ainsi, des algorithmes particuliers permettent de traiter ces informations et de leur donner un sens par rapport aux appareils alimentés par les réseaux : l'analyse d'un courant permet par exemple de surveiller la performance d'un procédé industriel ou de détecter les premiers signes de faiblesse d'une machine, annonciateurs d'une défaillance prochaine.

Le protocole de Kyoto élaboré en 1996, en imposant des limites aux émissions de CO₂, a inévitablement contraint l'évolution des réseaux électriques aux critères suivants:

- Moins de pollution au niveau de la production par le développement et le recours aux énergies renouvelables,
- Moins de pertes d'énergie,
- Moins d'unités de production grâce à un meilleur lissage de la demande,
- Une meilleure utilisation de l'énergie,
- Une consommation réduite, chaque fois que possible [3].

I.2 Les visages des smart grids dans le monde

Un certain consensus se forme sur ce que constitue le smart grid. Cependant, les priorités du smart grid varient d'une région à l'autre ou d'un distributeur à un autre. Notre intérêt a été porté sur des pays divers ; à savoir : Européens, USA et émergents comme la Chine et l'Inde.

I.2.1 Cas des pays de l'Europe

La Commission européenne soutient de nombreux projets de recherche et de développement sur les technologies des smart grids. Dès 2005, elle leur a dédié une structure, la plate-forme smart grid (ETP smart grid – EuropeanTechnology Platform), qui coordonne les fonds des programmes cadres de recherche et développement. Cette plateforme a été renommée smart grids Forum en juin 2009. De très nombreux projets ont été financés par ce biais ; une large proportion d'entre eux était dédiée à l'étude de l'intégration de production renouvelable et diffuse dans les réseaux.

Les démonstrateurs de recherche ciblés sur l'intégration des énergies renouvelables et la production distribuée étaient des actions importantes du 5^{ème} et 6^{ème} de Plans-Cadre de Recherche et de Développement(PCRD). Ainsi, sur la période allant de 2002 à 2006, le 6^{ème}

PCRD a soutenu plus de 60 projets sur la thématique « réseaux intelligents et intégration des énergies renouvelables » pour un montant total d'investissement de l'ordre de 190 millions d'euros. Au-delà des aspects technologiques, les projets couvraient des aspects socioéconomiques, législatifs et de gestion des réseaux [4].

En juin 2009, 14 grands gestionnaires de réseaux d'électricité européens (dont RTE et ERDF) ont présenté au smart grids Forum une initiative commune de recherche, développement et démonstrateurs (RD&D).

Cette initiative, EEGI (European Electricity Grid initiative), représente plus de 30 projets pour un budget prévisionnel de 2 milliards d'euros.

Parallèlement, en 2009, la commission européenne a mis en place la Smart Grid Taskforce, un groupe de travail rassemblant tous les acteurs concernés par les smart grids (régulateurs, gestionnaires de réseaux, producteurs d'électricité, fournisseurs d'énergie et équipementiers). Son objectif est d'élaborer un jeu de recommandations pour l'intégration des technologies de smart grids dans des conditions favorables pour les utilisateurs des réseaux [5].

Les initiatives européennes se sont focalisées sur l'intégration des énergies de sources renouvelables dans le mix de production, avec la perspective d'augmenter l'implication des utilisateurs finaux dans la gestion du système, au travers de politiques de gestion de la demande et du déploiement d'infrastructures de comptage communicant.

L'année 2009 fut le théâtre d'une foultitude de colloques, salons ou conférences sur les enjeux du smart grid. On dénombre aujourd'hui 90 projets pilotes dans le monde. Avec deux typologies de projets : ceux qui sont très orientés réseau et ceux axés sur le client final. Ces expérimentations sont en effet indispensables tant à la validation des nouvelles technologies qu'à l'étude des comportements des usagers. Programmées sur une durée moyenne de trois à cinq ans, elles s'inscrivent dans une démarche partenariale matérialisée par la mise en place généralisée de consortiums industriels [6].

I.2.2 Cas des USA

Les Etats-Unis sont actuellement à la pointe des technologies vertes et ce pays a engagé la transformation de son vétuste système électrique en "smart grid", un réseau truffé d'informatique et calqué sur l'architecture d'Internet. L'Amérique prend ainsi une avancée rapide dans ce domaine, qui attire des investissements colossaux et des géants comme IBM, Google, Cisco, Accenture General Electric ou Siemens. Les smart grids sont censés faire baisser la demande d'électricité de 10 %, intégrer dans le réseau les sources décentralisées d'énergies renouvelables et résorber les pics de consommation générateurs de pannes et de

pollution. Ces technologies pourraient ainsi éviter des coupures de courant qui coûtent chaque année 80 milliards de dollars aux Etats-Unis et réduire la facture énergétique du pays de 150 milliards de dollars par ans.

Les critères mis en exergue justifiant le projet smart grid sont la fiabilité et la sécurité de l'alimentation. Le blackout de 2003 était l'un des plus sévères d'une série qui a révélé la fragilité du réseau américain à supporter les demandes de pointes, pour cela une attention particulière est accordée pour le contrôle des pointes de la demande. Les USA ont adopté les projets de smart grids par un projet de loi dès 2007 et accordent à cette industrie et à sa mise en œuvre le tiers du budget alloué au financement de l'énergie. En termes de régulation et de réglementation, il a été développé et implanté des standards groupés en six volets : - sécurité informatique, - courbes sémantiques, modèles et logiciels, - visualisation et surveillance permanente du réseau, - gestion de la demande, - stockage de l'énergie et – électrification du transport.

I.2.3 Cas de la Chine

La croissance économique remarquable de la Chine lui a permis de doubler ses capacités de production d'électricité entre 2004 et 2008. La production d'énergie renouvelable connaît un essor important qui se fait dans des centres importants qui se connectent directement au réseau de transport.

Le réseau chinois est dorsal, et nécessite la concentration de tous les efforts pour favoriser un transport d'électricité efficace. La Chine envisage la construction d'un gigantesque smart grid pour une valeur avoisinant les 60 milliards d'euros. Il est remarquablement différent des réseaux Américains et Français, ce dernier est très centralisé et le smart grid chinois s'inscrit dans un contexte d'accélération des besoins énergétiques.

I.2.4 Cas de l'Inde

Les smart grids en Inde ont été mis en œuvre pour améliorer l'efficacité énergétique. Il y a l'exemple d'équiper les postes électriques de systèmes de relevé automatique dotés de capacités de mesures électriques avancées. Pour le transformateur, le système surveille le niveau d'huile et la température.

La communication s'effectue par le biais de réseaux cellulaires avec un système central de contrôle et d'acquisition de données. Il convient aussi de minimiser les pertes d'énergie estimées à 30% sur le réseau indien actuel. Le blackout septembre 2012 avec ses effets économiques désastreux, a donné à réfléchir d'une manière concrète à l'accélération de

la mise en œuvre du projet smart grid avec un questionnement sur sa capacité à éviter la récurrence de cet événement redoutable [7].

I.3 Croissance du marché des smart grids

Selon les analyses, le marché des équipements des réseaux intelligents atteindrait 11 à 22 milliards d'euros d'ici 2014, réparti sur trois segments clés : les applications, les systèmes de comptage intelligents et les applications réseaux, représentant respectivement 2 à 7 milliards, 5 à 9 milliards et 4 à 6 milliards d'euros.

La croissance du marché mondial s'appuiera sur celle des trois régions : les États-Unis qui représenteront en 2014 un peu moins de la moitié du marché total, l'Europe qui représentera à terme environ 40 % et la Chine (environ 15 %).

En Europe et dans les autres économies avancées, l'existence d'infrastructures déjà en place ralentira la croissance du marché des équipements intelligents. À l'inverse, les économies émergées comme la Chine bénéficieront d'un saut technologique. D'autre part, la dérégulation tardive du marché européen entraîne un retard de ce dernier par rapport au marché américain dans le déploiement des compteurs évolués, première étape dans la mise en place du réseau intelligent [8].

Beaucoup de projets ont été réalisés dans les différents pays comme les États-Unis, l'Europe, le Japon.

I.3.1 Les grands projets smart grids dans le monde

La plupart des projets smart grids sont encore au stade de démonstration ou projets pilotes, mais depuis un ou deux ans, des projets de taille et des budgets significatifs (supérieurs à 100 millions de dollars) voient le jour.

On compte actuellement près de 90 projets et démonstrateurs de réseaux intelligents en cours dans le monde. On fait un tour d'horizon de dix projets parmi les plus importants :

- **JAPON : Projets du Ministère du Japon, 786 \$M, début 2010**

Le Ministère de l'économie et de l'industrie japonaise a lancé quatre projets smart grids à grande échelle : Yokohama City, Toyota City, Kyoto Keihanna District et Kita-Kyushu City. Ces projets étudient des systèmes de gestion, via des compteurs intelligents, de l'énergie consommée par les maisons et les bâtiments, et incluent l'intégration des véhicules électriques, des panneaux photovoltaïques et des batteries.

- **INDE : Smart-City-India, 400 \$M, début 2010**

Trois pilotes sont prévus dans les villes de Haryana, Maharashtra et Gujarat avec comme partenaires Hitachi, Mitsubishi, JGC Corp et Toshiba. Ils visent l'intégration des énergies intermittentes et étudient des systèmes numériques de gestion de l'énergie. Les trois projets smart grids sont intégrés dans un projet plus global de ville « intelligente » (qui comprend aussi les transports propres, la gestion des déchets, ou l'approvisionnement en eau potable).

- **ETATS-UNIS :**

- PGEC Smart Grid Demonstration Project, 356 \$M**

Ce projet est financé par le DOE et se focalise sur l'un des constituants potentiels d'un smart grid : qui est le stockage. La technologie visée dans ce démonstrateur est la technologie à air comprimé (CAES). Le stockage est très étudié aux Etats-Unis pour réguler le réseau électrique.

- **Pacific Northwest Smart Grid Demonstration Project, 178 \$M**

Début 2009 : ce projet vise à déployer un réseau électrique intelligent dans 5 Etats et impliquera plus de 60 000 clients particuliers. Les objectifs sont de tester de nouvelles combinaisons de technologies smart grid (comprenant des équipements, des logiciels, et des outils analytiques poussés) pour mieux maîtriser les coûts liés à la distribution d'énergie et mieux incorporer les énergies intermittentes, comme l'éolien.

- **Columbus Southern Power Company Smart Grid Demonstration Project, 150 \$M**

Début 2010 : l'objectif est de mettre en place une infrastructure smart grid fiable, interopérable et intégré pour 110000 clients particuliers dans l'Etat. 13 technologies différentes seront utilisées dans ce projet, comprenant des compteurs intelligents, des systèmes de communication, des véhicules hybrides rechargeables, des systèmes de stockage ou encore des sources d'énergie intermittente.

- New York State Electric & Gas Corporation Smart Grid demonstration Project, 125 \$M, début 2010**

Ce projet est financé par le DOE et vise à réaliser un démonstrateur d'une technologie de CAES (stockage à air comprimé) de 150 MW. Par ailleurs, ce système de

stockage sera intégré dans une infrastructure smart grid pour améliorer la fiabilité du réseau et permettre une meilleure intégration des énergies intermittentes.

- Los Angeles Department of Water and Power, 120 \$M, début 2010

Ce projet vise à tester des technologies de sécurité des systèmes d'information, le cyber sécurité étant un enjeu clé du développement des smart grid. Il vise également à réfléchir à mieux intégrer les véhicules hybrides rechargeables, qui pourront représenter une part significative des véhicules sur les routes.

- First Energy Smart Grid Modernization initiative, 115 \$M, début 2009

En s'appuyant sur différentes technologies du smart grid, telles que des systèmes de gestion de la communication et de l'information, des compteurs intelligents et l'automatisation du système de distribution, ce projet souhaite de moderniser le réseau électrique existant et réduire la consommation énergétique en période de pointe.

- SmartGridCity Boulder, 100 \$M, début 2008

Il s'agit du premier projet smart grid historiquement mis en place avec un budget dépassant les 100 \$M. Les principaux objectifs sont d'identifier les technologies qui sont les mieux acceptées par les consommateurs et qui sont les plus performantes (compteurs intelligents, thermostats communiquant, logiciel de suivi de consommation,...). Le porteur de projet, XcelEnergy, a déjà engagé plus de trois fois la somme qu'il avait prévu initialement, principalement à cause du coût sous-estimé des fibres optiques.

▪ **AUSTRALIE : Australia Smart Grid, 100 \$M, début 2010**

les objectifs de ce projet sont de rassembler des données via le déploiement de technologies avancées de communication et de contrôle automatique à grande échelle pour faire une étude précise des coûts et des bénéfices associés au smart grid. Il est attendu qu'un "Smart Grid" national devrait permettre d'économiser aux ménages australiens 5 milliards de dollars par an (à comparer aux 11 milliards fournis aujourd'hui par les énergéticiens).

Un des premiers constats que nous pouvons faire est l'absence de projets de grande ampleur en Europe. Une des raisons est relativement la bonne qualité de puissance offerte des réseaux électriques dans les pays européens, notamment par rapport à ceux des Etats-Unis

En effet la Chine a prévu d'investir dans le cadre de son plan de relance 7,3 milliards de dollars dans le smart grid. Un premier projet pilote smart grid mené par le State Grid Electric Power Research Institute (SGEPRI), avec Honeywell comme fournisseur principal, va débiter. L'objectif est de mieux maîtriser la consommation énergétique des bâtiments commerciaux. La Chine investit aussi dans l'établissement de grandes liaisons (le Super Grid) pour accompagner au mieux la très forte croissance de la demande en électricité du pays. La Chine est d'ores et déjà le premier investisseur mondial déclaré dans le smart grid.

La majorité des projets qui sont ainsi en train d'être lancés devraient permettre de lever quelques verrous identifiés pour le développement des smart grid à l'échelle industrielle : définition de standards, définition de business model, gestion de l'acceptabilité du public, maîtrise des coûts des technologies, cyber sécurité, ...etc [9].

I.3.2 Estimation du marché des smart grids

Compte tenu des différentes estimations existantes sur le marché, nous nous sommes fixés comme objectif de quantifier les investissements mondiaux dans les smart grids à l'horizon 2030.

De nombreuses études ont été publiées ces derniers temps (IEA, Electric Power Research Institute, GTM Research, McKinsey, Morgan Stanley, Pike Research, Zpryme...) sur les opportunités économiques offertes par le développement du marché des smart grids. Les chiffres publiés varient fortement selon le périmètre de l'étude et les hypothèses d'investissement, selon Electric Power Research Institute (EPRI) et Pacific Northwest National Laboratory (PNNL), le marché mondial des smart grids sur les 10/15 dernières années représente 200 milliards de dollars. Soit environ 13,3 milliards de dollars par ans. La taille du marché est amenée à croître considérablement. En 2008, Morgan Stanley estimait le marché mondial annuel des smart grids à 40 milliards de dollars d'ici 2014 et 100 milliards de dollars d'ici 2030. Avec une répartition du marché très favorable aux équipements réseaux (60 %). Mckinsey estimait en 2010 que le marché annuel en 2014 représenterait entre 15 et 31 milliards de dollars et serait plutôt dominé par les systèmes de comptage (7 à 13 milliards). Le Gimélec estime que le marché mondial devrait atteindre entre 16 et 68 milliards de dollars par an d'ici 2020.

Le plus récent rapport de GTM Research prévoit que l'ensemble du marché européen des technologies smart grids atteindra les 3,1 milliards d'euros en 2012. Ce montant est amené à croître de 120 %, pour atteindre 6,8 milliards d'euros en 2016, répartis entre les

segments de marché que sont le comptage évolué, l'automatisation de la distribution, l'intégration des énergies renouvelables, les véhicules électriques et les systèmes informatiques propres au domaine de l'électricité.

L'institut Pike Research, qui est l'un des plus reconnus et les plus actifs, effectue des évaluations par grandes zones ou pays. Pour 2020, le cumul présenté fait une somme pondérée de plusieurs prévisions dans les différentes régions du monde. Le chiffre de 450 milliards réparti sur une progression linéaire donnerait un résultat proche de 100 milliards d'investissement par ans à l'horizon de 2020.

A noter que Pike a également prévu en 2010, un pic d'investissement dans les smart grids en 2015 à environ 35 milliards de dollars dans l'année.

L'hypothèse d'une baisse des investissements qui amènerait à voir l'évolution des smart grids comme une mise à jour technologique qui aurait donc une fin nous semble très contestable.

C'est à l'image des investissements informatiques dans une entreprise où, très souvent, les prévisions de projets amènent à voir un pic d'investissement à horizon de 3 ans. Après quoi ils devraient décroître une fois ces projets réalisés. Or cela ne se passe quasiment jamais ainsi. D'autres projets, d'autres innovations apparaissent.

Les différentes estimations font apparaître de très fortes variations. Plusieurs indicateurs montrent cependant qu'on est plutôt à horizon 2020/2025 sur un ordre d'idée autour du chiffre de 100 Milliards de dollars. La figure (1.1) montre l'évaluation de la taille du marché mondial en milliards de \$ par ans [10].

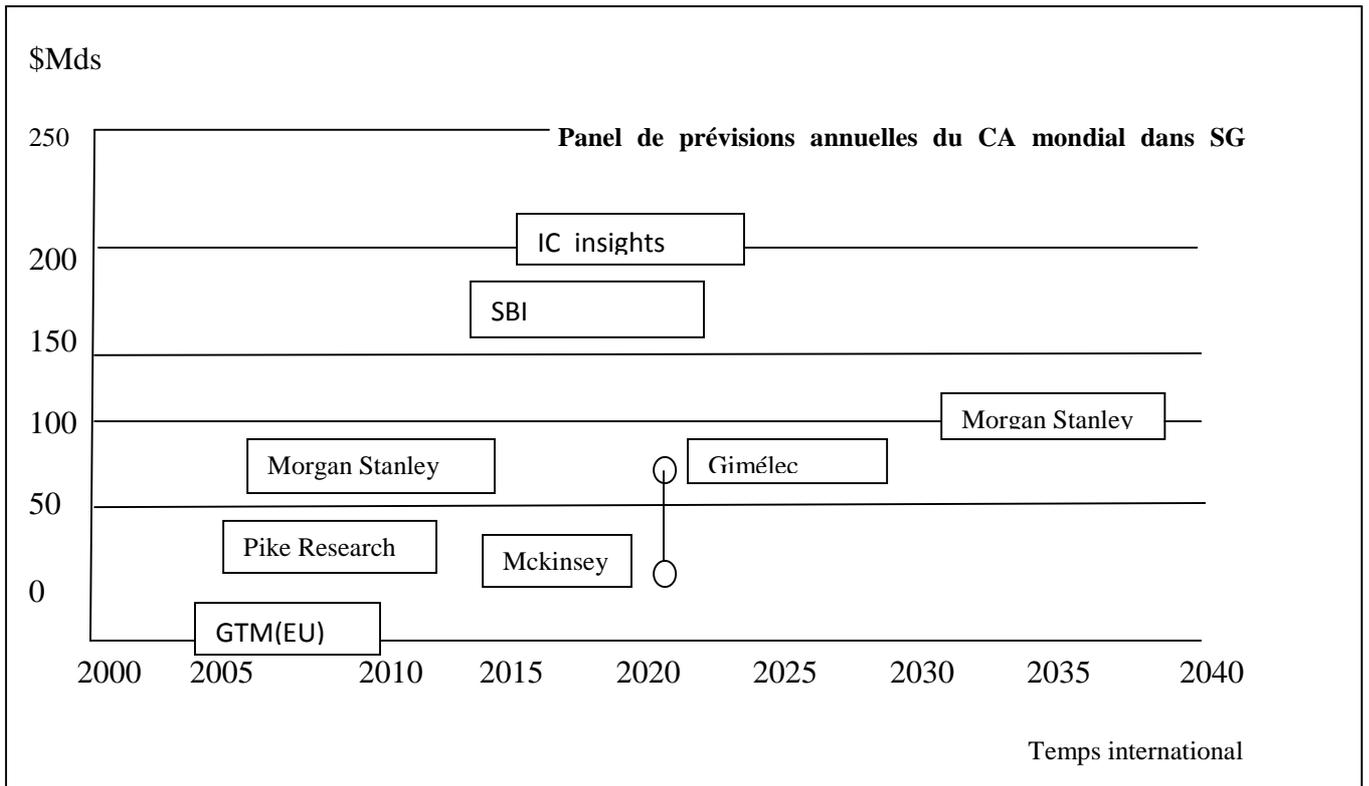


Figure (1.1) Evaluation de la taille du marché mondial en milliards de \$ par an.

I.4 Conclusion

Les smart grids offrent l'opportunité au monde de révolutionner son réseau électrique et énergétique. Avec la technologie de communication et d'information, l'efficacité énergétique, l'optimisation, la fiabilité et la sécurité deviendront les maîtres mots pour décrire le réseau.

Les smart grids ouvrent également la voie à un grand nombre d'applications influençant significativement l'industrie de l'énergie mais aussi l'industrie des télécoms et l'industrie de l'informatique.

Les visages du smart grid diffèrent selon les régions du monde, voir même d'un distributeur à l'autre, selon les facteurs politiques, économiques et environnementaux propres à chaque cas. Malgré tout, on distingue quelques grands courants dans l'industrie, chaque cas ayant aussi ses accents particuliers.

Le marché du smart grid joue un grand rôle dans la croissance et le développement de cette technologie dans les différents pays.

Introduction

Les activités des services continuent de connaître une dynamique forte et d'occuper une place dominante dans la gestion de l'énergie électrique. Dans la distribution de l'énergie, leur part ne cesse d'augmenter. Intégrés dans une économie mondialisée, soumis à des exigences de compétitivité élevées, les services connaissent aujourd'hui de profondes évolutions structurelles et un changement de modèle d'activité liés à des facteurs technologiques, économiques, démographiques et sociétaux. Ces mutations vont, à court ou à moyen terme, exiger des compétences nouvelles pour comprendre les enjeux et y répondre : maîtrise de l'offre /demande, nouveaux modes d'interaction avec les clients, nouveaux modes de facturation...etc. Dans ce contexte de profonde transformation, le secteur des services s'ouvre au-delà de sa sphère traditionnelle, attirant chaque année de nombreux nouveaux acteurs de l'énergie.

Les acteurs traditionnels de la chaîne de valeur sont les premiers concernés par le déploiement des réseaux électriques intelligents. Leur rôle, leur métier et leurs activités seront profondément modifiés : les producteurs pourront, notamment, mieux prévoir la demande en électricité, optimiser l'utilisation des interconnexions et gérer activement la demande, les gestionnaires de réseaux seront assistés dans le développement, l'exploitation et la maintenance de leur système et le fournisseur verra sa relation avec les consommateurs facilitée.

Aujourd'hui, de plus en plus, les distributeurs d'énergie électriques choisissent d'orienter leur stratégie vers des activités de services, notamment en associant une prestation de service à leurs clients. Les fournisseurs d'énergie proposent ainsi des services qui apportent une valeur ajoutée à leur électricité, ce qui leur permet d'augmenter leur chiffre d'affaires (sécurisation des données, protection des dispositifs intelligents, gestion de la demande, offrir des conseils pour mieux gérer la consommation...etc.).

II.1 Les acteurs de l'industrie du système électrique intelligent

La numérisation et la modernisation du système électrique dans son ensemble, auront des conséquences différentes selon les acteurs. Comme le rappelle la Commission de régulation de l'électricité de France CRE [11], alors que les producteurs et gestionnaires de réseaux considèrent ces évolutions comme une possible optimisation de leur métier, les fournisseurs d'électricité et les équipementiers y voient plus un relai de croissance.

Cependant, le déploiement des smart grids permet également d'ouvrir la porte à de nouveaux acteurs et notamment ceux issus du monde de l'informatique (software) et de celui des télécommunications (hardware). La distinction entre ces deux secteurs n'est pas si marquée puisque de nombreux acteurs se positionnent sur les deux secteurs, mais elle permet de couvrir l'ensemble des besoins induits par le développement des smart grids c'est-à-dire de l'architecture réseau, du logiciel et des services.

Plusieurs acteurs sont impliqués dans le développement d'un réseau électrique moderne et d'une nouvelle industrie électrique. Ce développement représente une opportunité d'affaire considérable pour l'industrie électrique, celle du bâtiment, des technologies de l'information et des produits pour le grand public tels que illustrés par la figure (2.1).

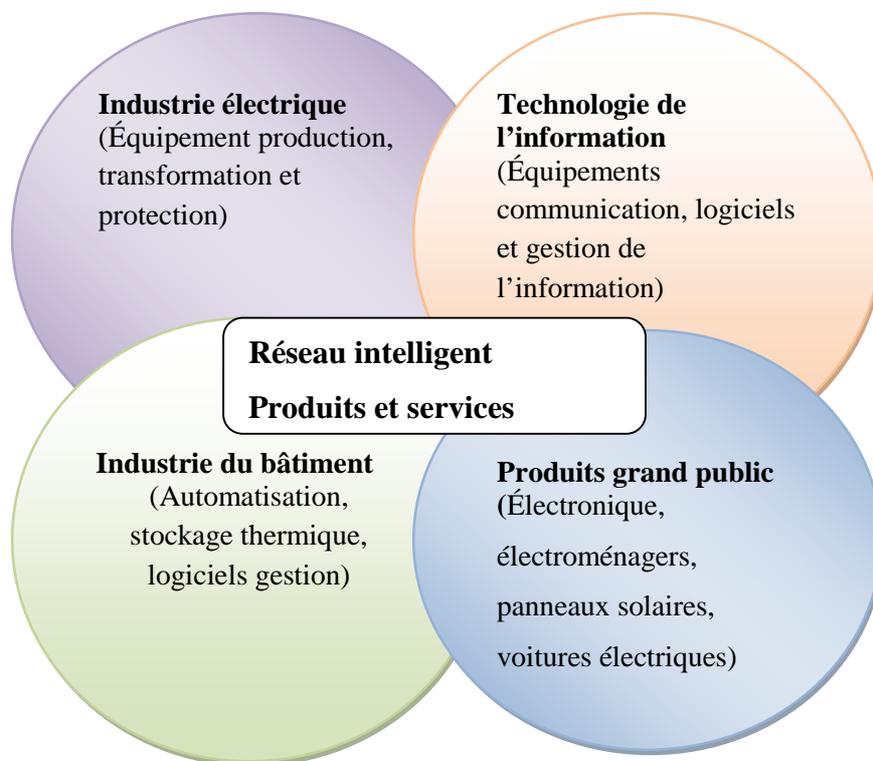


Figure (2.1) Les industries impliquées dans le smart grid [12].

II.2 La chaîne de valeur du système électrique intelligent

Une chaîne de valeur (telle que schématisée par la figure (2.2)) est un ensemble d'activités interdépendantes dont la mise en œuvre permet de créer de la valeur identifiable et, si possible, mesurable. Elle intègre donc toutes les étapes, de l'approvisionnement en matières premières à la consommation finale. Son efficacité repose essentiellement sur la coordination des différents acteurs impliqués et leur capacité à former un réseau cohérent et collaboratif. Les technologies de l'information favorisent un échange de données propice à une organisation efficiente de l'ensemble de la chaîne [13].

II.2.1 Le système électrique

Le système électrique représentant l'ensemble de la chaîne production-transport-distribution et commercialisation de l'énergie électrique est l'un des systèmes critiques parmi les plus complexes et les plus étendus d'un pays. Sa complexité est due principalement aux facteurs suivants :

- le nombre important de composants (i.e. sources, consommateurs, infrastructure matérielle),
- la multitude des phénomènes physiques qui y interviennent (i.e. propagation, effet Joule),
- la diversité et l'emplacement des sources d'énergie par rapport aux zones de consommation,
- l'obligation d'assurer, à chaque instant, un équilibre entre les puissances produites et consommées (aux pertes près), liée aux possibilités limitées de stockage de l'électricité,
- les fortes interactions et les objectifs souvent antithétiques entre le fonctionnement du système électrique, son organisation, les phénomènes sociétaux, politiques et les contraintes environnementales.

Par rapport à ce dernier point, on a pu assister, ces dernières années, à la libéralisation du marché de l'électricité dans de nombreux pays du monde. Cette ouverture a eu un impact important sur l'organisation et donc sur le fonctionnement des systèmes électriques. Avec le développement des smart grids, il s'est induit un objectif principal qui consistait à supprimer le « monopole » sur l'industrie d'électricité. On encourage ainsi l'apparition de plusieurs acteurs au niveau de quelques segments de cette chaîne électrique et donc l'apparition de la concurrence entre ces différents acteurs, élément d'ailleurs indispensable pour le fonctionnement d'un marché libéralisé et une réduction des prix pour le client final.

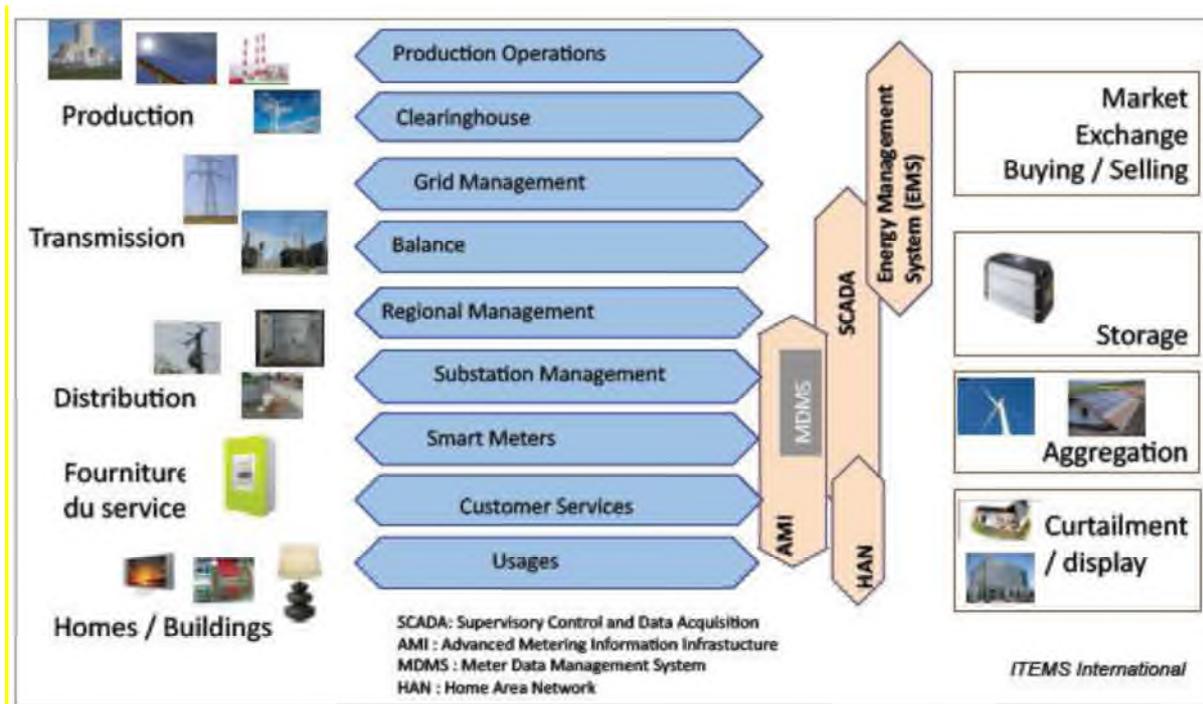


Figure (2.2) Représentation de la chaîne de valeur d'un système électrique intelligent [14].

II.2.2 Consommateur

L'environnement smart grids introduit un nouvel étage d'optimisation de l'équilibre offre / demande au niveau des réseaux de distribution, puisque le consommateur devient une variable d'ajustement par la production décentralisée et par le pilotage des charges. La CRE prévoit ainsi dans son rapport sur les modèles économiques des smart grids, que « l'utilisateur final aura un rôle actif dans le système énergétique et va devenir le centre d'attention des autres acteurs de la chaîne de valeur ».

Les bénéfices pour les consommateurs sont nombreux. En améliorant les connaissances sur la consommation électrique, les consommateurs pourront bénéficier d'offres tarifaires plus diversifiées et mieux adapter à leurs comportements. Ils pourront également s'équiper de nouveaux services d'efficacité énergétique ou de maîtrise de la demande leur permettant de mieux gérer leur consommation mais également de jouer positivement sur les pics de consommation et les pannes dues à une surcharge du réseau. Enfin, les consommateurs pourront espérer un service de meilleure qualité puisque les nouvelles technologies permettront aux gestionnaires du réseau d'anticiper, de détecter et de réparer les pannes mais également de répondre en temps réel aux besoins en électricité

Une partie de ces nouveaux services pourrait s'inscrire dans les démarches de bâtiment intelligent et constituer une alternative aux services proposés par les acteurs

traditionnels du secteur de l'énergie. La montée en puissance de ce marché qui permet d'ores et déjà de piloter son habitat ou d'en contrôler les principales fonctions à distance via Internet représente une véritable opportunité pour de nombreux acteurs.

II.2.3 L'agrégateur : un nouveau métier pour le marché électrique

L'agrégateur est nouveau service dans les smart grids qui assure au réseau un volume d'effacement tout en garantissant aux clients industriels un impact limité de l'effacement sur leur procès ou aux clients tertiaires un impact limité sur le confort des occupants des bâtiments, il est nécessaire de disposer d'une grande flexibilité en agrégeant un grand nombre de sites. C'est le rôle dévolu à l'agrégateurs. En plus de la mise en action de capacités d'effacement, l'agrégateurs doit générer, gérer et valider des scénarios d'effacement sur les différents sites pour optimiser le potentiel, la flexibilité et la fiabilité de son action.

L'état d'un site et sa consommation doivent être connus en temps réel pour permettre la réactivité imposée par les contraintes du réseau électrique. Les automates permettant le pilotage des sites tertiaires et industriels peuvent ainsi être interrogés et pilotés par le système d'information de l'agrégateurs. Les informations ainsi collectées peuvent être complétées par des alertes de dysfonctionnement remontées par les techniciens de maintenance et les refus d'effacement des clients exploitant le site.

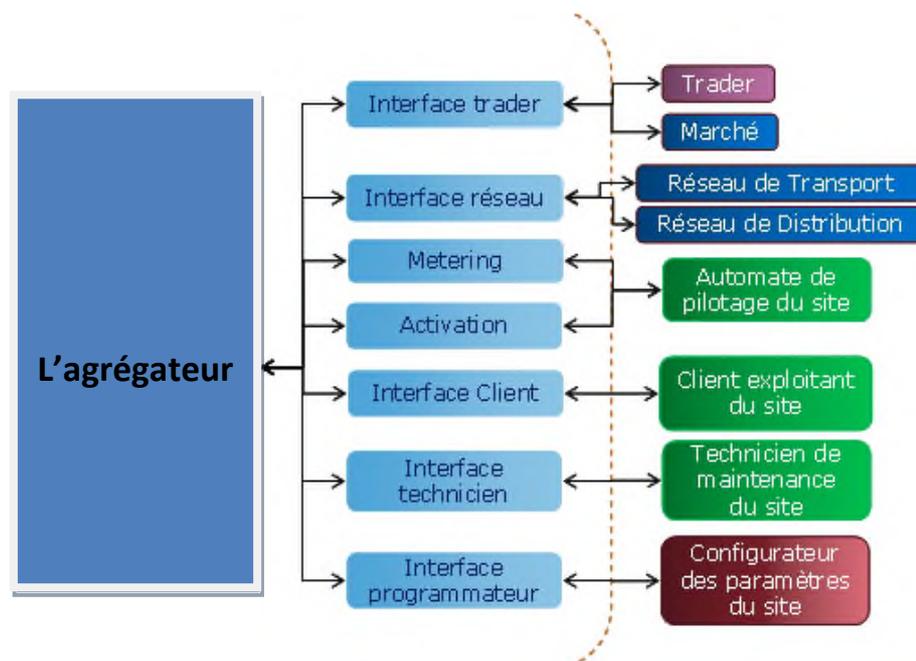


Figure (2.3) interactions Agrégateur-Autre acteurs, dans les smart grids [15].

La naissance du nouveau métier ou de la nouvelle fonction d'agrégateurs d'effacement est une chance importante pour accélérer l'émergence du marché de capacité. Cette nouvelle approche comporte deux caractéristiques principales:

- l'agrégation doit permettre de faire accéder au marché un grand nombre de nouveaux acteurs plus petits ou dont l'engagement d'effacement n'est pas totalement garanti sur l'année en apportant sécurité et disponibilité des installations. Autrement dit, lors des déclenchements de l'effacement par l'agrégateur, le consommateur final garde la possibilité à tout moment de revenir en mode « normal ». Cette option laissée au consommateur implique pour l'agrégateur une importante mutualisation des installations et une forte réactivité des systèmes de pilotage pour compenser toute baisse du niveau d'effacement garanti pour l'équilibre du système électrique ;
- l'agrégation doit être gagnante au plan économique pour les propriétaires des installations incluses dans le plan d'effacement. D'où l'importance de l'existence d'un marché permettant la monétisation de l'effacement.

II.3 Le développement des véhicules électriques

Le développement attendu du véhicule électrique (VE) et de son impact sur le réseau électrique va en faire un acteur majeur du développement des réseaux électriques intelligents. Le succès du véhicule électrique est intimement lié à la mise à disposition préalable des infrastructures de recharge adéquates. En cours de développement actuellement, celles-ci seront de différentes natures (rapidité de la recharge, station d'échange de batterie...). Si le parc automobile glisse progressivement vers la propulsion électrique, la demande en électricité va croître sensiblement et représentera de facto une charge conséquente sur le réseau. L'offre de production devra par conséquent s'adapter afin d'intégrer ces nouveaux besoins et les smart grids seront primordiales pour assurer cette transition (en programmant par exemple le rechargement des véhicules la nuit pendant les heures creuses afin d'éviter des pics de consommation mettant à mal la capacité du réseau).

II.3.1 Electromobilité et intégration au réseau

La coopération entre les secteurs de l'énergie et de la communication pourrait résulter en un profit macroéconomique. Les objectifs premiers des véhicules électriques (réduction des émissions de CO₂) ne doivent pas cacher le fait qu'une coordination intelligente et efficace des différents secteurs pourrait éviter les pics de consommation.

Le programme E-Energy en Allemagne devrait permettre l'intégration intelligente de l'électromobilité à un système global d'approvisionnement en énergie électrique, la consommation d'électricité étant guidée par la production [16].

- 1ère phase : charge de la batterie. Des solutions avancées basées sur les TIC sont nécessaires pour éviter les heures de saturation.
- 2ème phase : stockage temporaire de l'énergie et injection d'électricité sur le réseau pour compenser les effets de fluctuation. Une mise en place de mécanismes de règles et de pilotage à moyenne et basse tension s'avère nécessaire.

II.3.1.1 Le « Vehicle-to-grid » pour limiter l'impact des pics de consommation

Le terme « Vehicle to Grid » (V2G), littéralement « du véhicule vers le réseau » caractérise l'action de **réinjecter l'électricité contenue dans les batteries d'une voiture électrique dans le réseau électrique durant ces fameuses périodes de stationnement**. Le véhicule électrique communique ainsi avec le réseau électrique pour mener à bien cette action.

❖ Les essais d'AC Propulsion

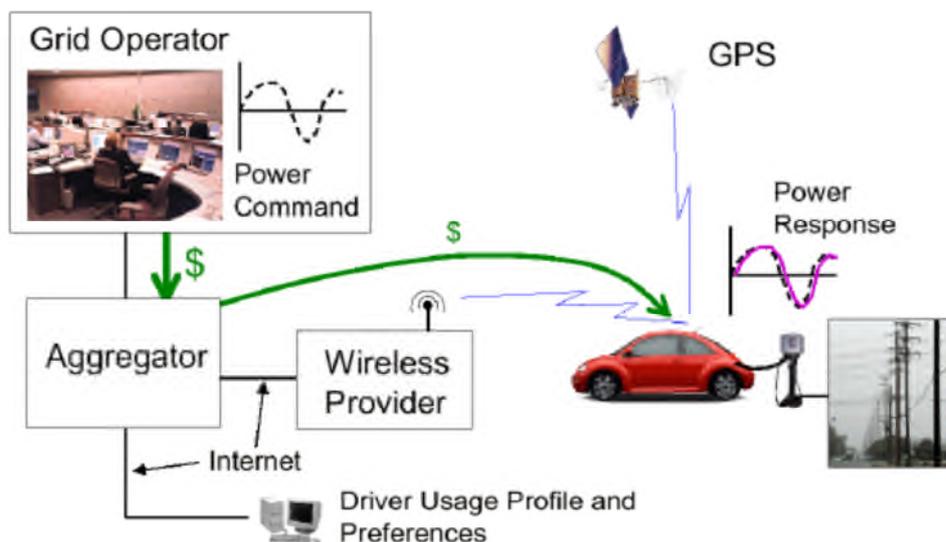


Figure (2.4) Schéma de l'architecture du système de régulation envisagé par AC Propulsion.

Ce projet, présente une analyse détaillée des rouages de systèmes de régulation du réseau électrique et comment la technologie V2G peut les apporter et ce en plus d'un support local pour les résidences. Un véhicule de test a été équipé d'un système électrique bidirectionnel pour prendre de l'énergie au réseau et la stocker dans des batteries et être capable de renvoyer cette énergie au réseau électrique. Le véhicule était aussi équipé d'une connexion Internet sans fil permettant le contrôle à distance de la gestion énergétique.

Les résultats obtenus ont montré que les temps de transmission sans fil convenaient pour respecter les contraintes du système Cal. ISO et que la charge sur la batterie due à l'activité de régulation était sensiblement identique à la charge d'une journée d'utilisation normale de la voiture. De plus, les bénéfices pécuniaires de cette activité de régulation du réseau excèdent les coûts liés à la dégradation de la batterie dans la plupart des scénarios envisagés par cette étude [17].

❖ Publications récentes à l'université du Missouri

Entre 2008 et 2009, des membres de l'Université de Sciences et de Technologies du Missouri ont publié deux articles [19,20] sur l'Optimisation par Essaim Particulaire pour résoudre le problème V2G dans un contexte d'agglomération des véhicules dans un parking. Le problème qu'ils ont cherché à résoudre est de planifier au mieux les charges/décharges des véhicules pour que ceux-ci réalisent un profit tout en ayant une charge suffisante lors de leurs sorties (60% de la batterie). Dans ce système, les véhicules peuvent acheter et vendre de l'électricité au réseau électrique mais aussi entre eux.

La modélisation réalisée avec des parkings de 50, 500 et 5000 véhicules montre que la technique trouve de façon consistante une bonne solution. Les auteurs prévoient donc de continuer leurs recherches et d'affiner l'algorithme pour aussi y intégrer d'autres marchés (régulation, réserve tournante, marche de pics) [18].

II.3.1.2 Le Smart Garage

La fondation Rocky Mountain Institute a développé un groupe de travail appelé Smart Garage co-financé par The Lemelson Foundation et Google, ce groupe réuni des entreprises de premier plan pour travailler sur le future de l'automobile électrique et son intégration dans le réseau. Le groupe de travail a organisé une « charrette »¹¹ en octobre 2008, parmi les participants on peut noter la présence d'IBM, A123Systems, Alec Brooks de Google, Tesla, Nissan, GM, Ford et plusieurs compagnies électriques.

Enfin, Le modèle économique du véhicule électrique si souvent décrié se voit donc renforcé par le développement à venir des technologies « vehicle to grid ». Loin d'aggraver

les pics de consommation d'électricité, les véhicules électriques pourront au contraire les effacer en lissant la production d'énergie électrique. De plus, le « V2G » permettra d'optimiser l'intégration des énergies renouvelables dans le réseau électrique. Constructeurs, fabricants de bornes, énergéticiens et autres acteurs de la filière électrique ont donc tout intérêt à s'entendre et à collaborer pour qu'émerge au plus vite cette « smart » technologie dans le smart grid [19].

II.4 Construction d'offre de services du stockage pour les réseaux de distribution du futur

Les solutions innovantes doivent être développées pour esquisser les réseaux de distribution du futur en intégrant ces évolutions. Le stockage d'énergie est l'une des options envisagées pour les années à venir.

II.4.1 La valorisation du stockage distribué : une approche « multifonction »

Les études de valorisation du stockage disponibles dans la littérature, menées dans des contextes technique, économique et réglementaire donnés montrent qu'une unique application ne suffit généralement pas à rentabiliser l'investissement et l'exploitation d'un stockage. C'est pourquoi, dans les limites des possibilités des technologies disponibles, il faut imaginer des méthodes pour maximiser les bénéfices générés par le stockage réparti, d'une part, et tenter de minimiser ses coûts de mise en œuvre, d'autre part. Deux principes peuvent ainsi être formalisés :

- **Mutualisation des services** : il s'agit d'associer un maximum d'applications pour divers acteurs au sein d'une même unité de stockage. L'objectif est de cumuler plusieurs sources de valeur (notamment économique et environnementale) en vue de favoriser l'atteinte d'une rentabilité. Par exemple, l'utilisation du stockage pour alimenter une poche isolée du réseau de distribution suite à un incident est un service potentiellement porteur d'un fort intérêt technique. Cependant, du moins dans les conditions actuelles, cet usage ne serait sollicité qu'exceptionnellement. Il en résulterait une valeur économique a priori modérée mais des possibilités d'affecter le stockage à d'autres applications en parallèle, de façon à en maximiser l'utilisation. Cette réflexion se fait, cependant, au prix d'une complexité ajoutée dans la construction d'un modèle d'affaires (contractualisation potentielle entre plusieurs acteurs). De plus, elle pose la question de la priorisation des services entre eux de façon à satisfaire au mieux les besoins de chaque partie prenante du smart grid.
- **Mutualisation des matériels** : il s'agit d'aider l'insertion du stockage en combinant celui-ci à des composants existants ou en développement dans les réseaux de distribution intelligents,

comme les convertisseurs statiques ou les infrastructures avancées de contrôle/commande. L'objectif est ici de réduire le coût initial du stockage pour faciliter l'atteinte d'un bilan profitable dans la durée. L'objectif du présent point de ce chapitre est d'étudier l'offre de services du stockage pour les réseaux de distribution d'un smart grid. En dépit des performances élevées, le coût du stockage demeure un frein majeur à son développement massif. Ainsi, pour que le distributeur puisse bénéficier à terme de cette nouvelle option technique, la mutualisation des services doit être examinée. En plus des gestionnaires des réseaux de distribution, il semble opportun d'ouvrir la réflexion à d'autres parties prenantes pour maximiser le potentiel de valorisation.

II.4.2 Services du stockage à valeur « distributeur »

II.4.2.1 Lissage des transits de pointe (SD1)

Le service SD1 consiste à placer une unité de stockage au niveau d'éléments contraints du réseau pour apporter une solution transitoire flexible. La recharge est réalisée aux faibles transits, de façon à disposer d'une réserve d'énergie pour déstocker à la pointe de charge et ainsi minimiser les courants maximaux sur les ouvrages concernés (Figure 2.5). Les transits apparents peuvent être réduits par une action en puissance active et, plus marginalement, par une compensation locale de réactif. Par exemple, passer de $\tan\varphi=0,4$ à $\tan\varphi=0$ réduit le transit apparent de 7%.

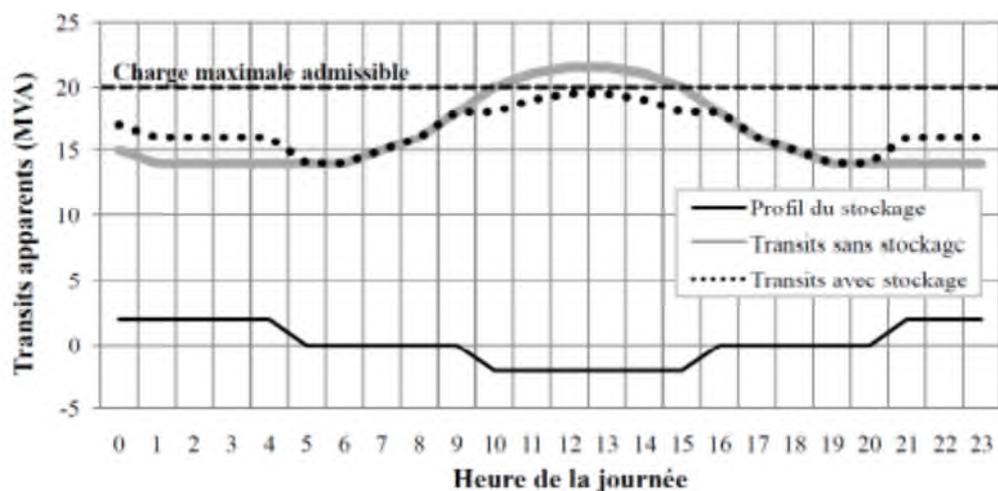


Figure (2.5) Une illustration du stockage pour le lissage de la charge [20].

II.4.2.2 Réglage local fin et dynamique de la tension (SD2)

Les études de planification sont menées de façon à maintenir un niveau de tension satisfaisant pour les utilisateurs. Si une contrainte est identifiée, en parallèle des solutions classiques (renforcement), le stockage distribué est susceptible d'être utilisé comme un nouveau moyen de réglage de la tension dans les réseaux de distribution. Deux déclinaisons de ce service semblent a priori envisageables :

- **Soutien local au plan de tension** : le stockage peut injecter de l'actif ou du réactif sur un départ existant chargé en vue d'assurer un niveau de tension adéquat durant les périodes de pointe (prévention des situations de tension basse). Dans ce cas, il constitue une alternative à des investissements qui devraient être réalisés pour maintenir la qualité de fourniture dans les limites contractuelles ou réglementaires admissibles.
- **Soutien à l'insertion de la production décentralisée** : l'absorption d'actif ou de réactif en couplage direct ou à proximité d'une installation de production décentralisée peut aider à minimiser localement l'impact de celle-ci sur le plan de tension (prévention des situations de tension haute). La solution actuelle, lorsque l'étude de raccordement identifie des contraintes, consiste en un renforcement dont la charge est désormais partagée entre le producteur et le GRD : la valeur du service serait donc répartie entre les deux acteurs.

II.4.2.3 Soutien au réseau en fonctionnement dégradé (SD3)

Cette méthode implique la conservation de marges qui peuvent s'avérer élevées au regard des besoins de la situation normale d'exploitation, et ceci en prévision d'évènements par nature ponctuels et relativement rares. Dans ce cadre, le stockage pourrait apporter un soutien lors d'indisponibilités d'ouvrages (incidents localisés, travaux de maintenance). Il fournirait de nouveaux schémas d'exploitation et viendrait limiter les éventuelles contraintes sur les matériels durant ces situations de fonctionnement dégradé [21].

II.4.2.4 Renvoi de tension en poche locale (SD4)

Avec l'insertion croissante de producteurs au sein des réseaux de distribution, leur contribution à un éventuel service de reprise de charge en cas d'incident (local ou généralisé) suscite l'intérêt [22]. Le stockage d'énergie pour les réseaux intelligents pourrait réaliser (ou contribuer à) un tel renvoi de tension:

- Des unités de stockage mobiles communicantes pourraient être employées ponctuellement.
- Le renvoi de tension en poche locale pourrait être ajouté à l'offre de services d'un stockage stationnaire, par exemple dans une zone où les solutions conventionnelles (bouclage, renforcement) sont difficiles à mettre en place

II.4.3 Services du stockage distribué à valeur « producteur décentralisé »

Cependant, en ce qui concerne le réglage de la fréquence, certains gestionnaires de réseau, notamment en Irlande, exigent déjà que le raccordement de fermes éoliennes s'accompagne de la fourniture de réserve pour le réglage de fréquence. En l'absence de stockage, une telle obligation impose aux producteurs à base d'EnR de dégrader volontairement l'efficacité de conversion de leurs dispositifs : une part du productible disponible se trouve perdue [23].

Effectivement dans les smart grids, afin d'exploiter la totalité du productible disponible instantanément, l'unité de stockage réaliserait une modulation des injections de la source EnR, suivant une caractéristique puissance/fréquence (appliquée par exemple au niveau du point de raccordement) lui permettant de respecter les spécifications du gestionnaire du réseau.

Parmi les autres applications possibles du stockage pour les producteurs décentralisés dans les smart grids, nous retiendrons notamment la valorisation des effacements, qui consiste en un stockage/report d'une énergie qu'il n'est pas possible d'injecter sur le réseau à l'instant où elle est disponible, pour une raison donnée : congestion, taux de pénétration limités, régulation de tension, etc. Par ailleurs, le producteur en collaboration avec l'agrégateur, peut éventuellement rechercher une réduction des perturbations qu'il induit sur le réseau amont, en conformité avec seuils tolérés par le GRD, effectuer des reports d'injection de façon à optimiser la valorisation de sa production (y compris par autoconsommation) ou encore viser, via un stockage massif, la garantie d'un profil de production annoncé à l'avance.

II.4.4 Services du stockage distribué à valeur « consommateur »

La tarification de l'énergie électrique est la résultante d'une part proportionnelle à la puissance souscrite « abonnement » et d'une part proportionnelle à l'énergie consommée. La puissance souscrite n'étant souvent atteinte que très marginalement en pratique, le consommateur réserve un service qu'il a tendance à sous-utiliser.

Le lissage de la pointe consiste à écrêter le profil de consommation d'un client pour réduire la puissance qu'il souscrit et donc le montant qui lui est facturé à ce titre au prix, cependant, d'une consommation d'énergie accrue (pertes dans l'unité de stockage). Pour ce faire, la recharge est réalisée lorsque la consommation du client est faible et le déstockage est synchronisé avec les appels élevés de puissance. Les cas les plus favorables correspondent à des pointes courtes et dont l'occurrence est prévisible à l'avance, de façon à limiter la capacité de stockage à installer [24].

En la matière, les combinaisons effectivement réalisables peuvent être étudiées en tenant compte du point de raccordement du stockage au sein du réseau de distribution via la construction d'une matrice services/localisations. Cet outil de représentation a permis d'identifier des cas propices pour le stockage distribué qui font actuellement l'objet de développements techniques (simulations dynamiques) et économiques (modèle d'affaires) dans les projets « smart grids ».

II.5 Intégration des EnR dans les smart grids

Afin de faciliter l'intégration des EnR dans le système électrique, les réseaux devront être gérés de manière plus réactive, grâce aux technologies de smart grids. Ces technologies regroupent de nombreux outils et systèmes pour la gestion des réseaux (comptage communicant, stockage de l'électricité, modèles de marché, onduleurs et charges contrôlables, etc.). Les nouvelles technologies de l'information et de la communication interviendront également afin d'optimiser les flux d'énergie et, notamment, d'assurer l'équilibre « offre/demande ». En développant l'observabilité, la prévisibilité, le pilotage et la flexibilité, les smart grids permettront de mieux gérer l'intermittence des énergies renouvelables.

- Les gestionnaires de réseaux développent des outils de prévision de la production renouvelable, afin de mieux gérer l'équilibre production/consommation et, ainsi, d'améliorer l'insertion de cette production sur les réseaux. Il s'agit de déterminer quelle part de la puissance totale maximale attribuer aux énergies renouvelables.

-La météorologie joue également un rôle prépondérant pour une meilleure intégration des énergies renouvelables aux réseaux. Les prévisions météorologiques permettent d'opérer des rapprochements statistiques et/ou corrélatifs entre l'aléa météorologique et la production. Ainsi, un faible écart entre les prévisions et la production sera satisfaisant pour maintenir l'équilibre.

- Le stockage de masse et le renforcement des interconnexions apparaissent comme des solutions complémentaires aux FACTS pour améliorer la flexibilité du système électrique. En effet, en offrant la possibilité de lisser la production de pallier l'intermittence des EnR, ils permettront de mieux intégrer les énergies renouvelables au système électrique

II.6 Normalisation dans les réseaux électrique intelligents.

L'ouverture des marchés de l'électricité entraîne une évolution des acteurs et des modèles économiques (commercialisateurs différents des gestionnaires de réseaux, apparition d'agrégateurs, augmentation du nombre des producteurs de faible puissance, subvention par tarif de rachat, etc.) qui nécessite des nouveaux processus de gestion. La normalisation pour

les réseaux intelligents peut favoriser l'accès au marché de solutions nouvelles. Elle permet notamment aux nouveaux produits et services d'acquérir la confiance des gestionnaires et des consommateurs, facteur sans lequel l'innovation pourrait longtemps rester inacceptable.

II.6.1 Normes de transport et de distribution

La Commission électrotechnique internationale présente les couches d'application, les services et les protocoles de normalisation transversaux applicables à la gestion d'un réseau d'électricité, ainsi que leurs interconnexions. Une évaluation approfondie qui a mené à la définition de plusieurs normes et lacunes prioritaires. Dans la figure (2.6), on trouve une description des couches de référence clés.

On note que cette partie du travail est très bien développée dans un mémoire de fin d'études à soutenir en juin 2013 au département de Génie Electrique, traitant de la technologie des projets smart grids [25].

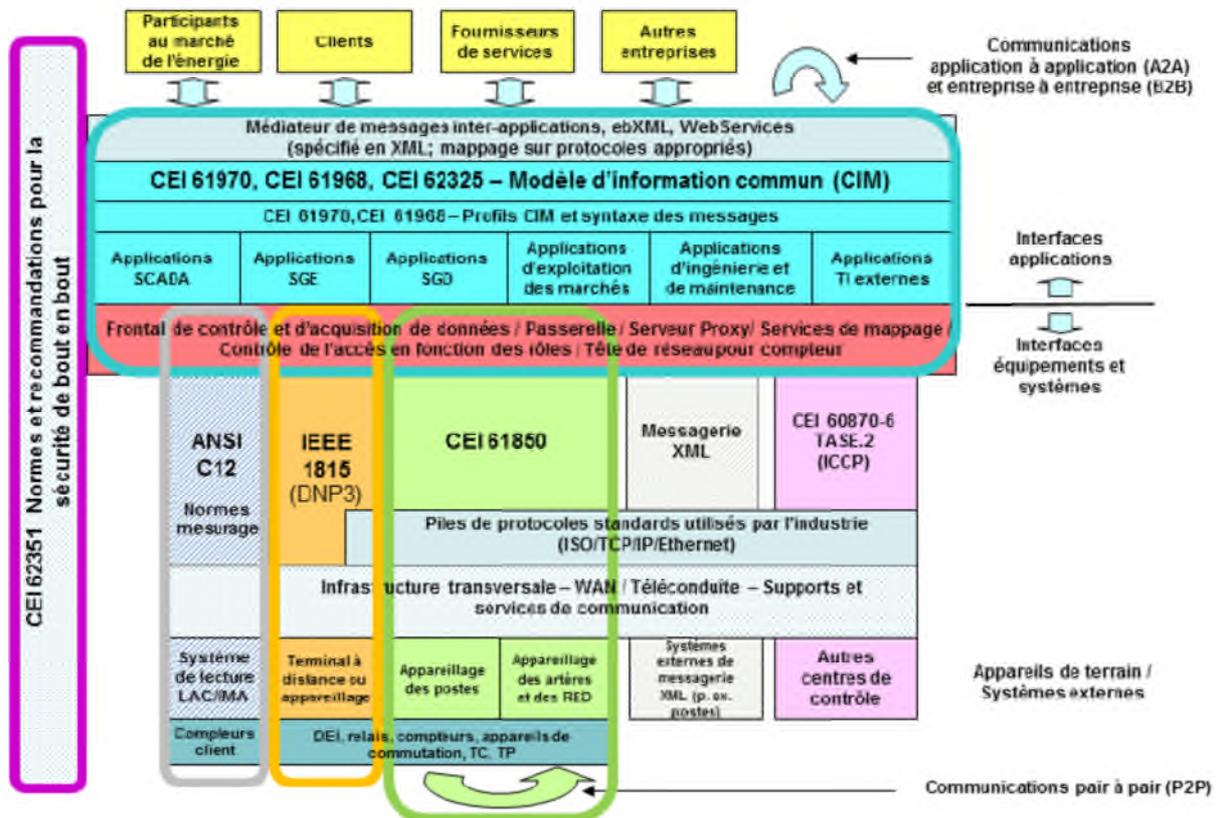


Figure (2.6) Architecture des normes des réseaux intelligents selon la CEI 62357

II.7 Conclusion

Aujourd'hui, la majorité des projets de smart grids sont à l'initiative des opérateurs de réseaux et des fournisseurs électriques. Ceux-ci ont tendance à ne voir les TIC que comme un outil permettant de renforcer la qualité de leur service. De leur côté, les acteurs des TIC sentent un marché très prometteur mais encore difficile à pénétrer. C'est pour cela que l'arrivée des smart grids permet l'entrée de nouveaux acteurs proposant de nouveaux services et produits pour les secteurs de l'énergie mais aussi informatique et des télécoms, dans un contexte réglementaire axé sur la sobriété énergétique, et pour ce dernier point on a défini quelque normative relatif aux système du smart grid. Dans cette optique, nous avons bien insisté sur les parties critiques en développement telle que le véhicule électrique et la technologie V2G, le stockage d'énergie, ainsi le développement des smart grids est dans le développement des EnR.

Le modèle d'affaires de cette chaîne de valeur présente la répartition de l'activité et, notamment, l'origine de ses revenus afin de dégager de la rentabilité d'un tel projet smart grid. Donc, le chapitre suivant va aborder un calcul coût-bénéfice sur un périmètre cohérent et une estimation des montants financiers associés à ces postes de gains et de coûts.

Introduction

L'étude technico-économique des projets énergétiques reste une étape d'une importance capitale avant toute décision de déploiement et de généralisation. Au-delà du coût des technologies, l'heure est à la recherche de rentabilité économique. Pour bien comprendre pourquoi on cherche à valoriser l'étude technico-économique, il faut commencer par déterminer les voies possibles de valorisation de cette filière, ainsi que les acteurs qui y trouveront des bénéfices. Il est donc nécessaire de raisonner par bénéfice: identifier dans un premier temps les méthodes de calcul, déterminer les gains de chaque acteur, avant de rechercher les calculs économiques.

L'évaluation économique consiste à apprécier les avantages et les inconvénients d'une décision. Nous pouvons compter sur plusieurs méthodes qui permettent d'éclairer le décideur au cours de certaines phases du processus de décision. Les méthodes à mettre en œuvre dépendent de la nature du problème à résoudre et de l'information plus ou moins précise (complète) des différents paramètres et éventualités associés à la décision. On trouve beaucoup des méthodes de calcul technico-économiques comme : Méthode de calcul des coûts (target costing) et la méthode Analyse coût- bénéfices (ACB)...etc.

Dans ce travail, nous nous placerons principalement du point de vue de la fiabilité pour les initiatives des Smart Grids, pour cela il existe plusieurs analyses économiques. L'évaluation peut être ex ante (avant incération dans le projet) ou ex post (après sa réalisation). Notre travail est centré sur l'évaluation ex ante, vue comme un outil d'aide à la décision. Les méthodes de l'évaluation économique ex ante sont bien placées pour les projets énergétiques, ainsi on trouve la fameuse méthode «Analyse coût- bénéfices (ACB) » pour évaluer les projets smart grids.

III .1 Analyse coût-bénéfices

III .1.1 Description

L'Analyse Coût-Bénéfices (ACB) vise à identifier et à quantifier les conséquences positives (bénéfices) et négatives (pertes) d'une décision, puis à les exprimer en une unité commune permettant la comparaison : l'unité monétaire. C'est un outil d'aide à la décision qui permet d'évaluer l'intérêt pour la société d'un projet, programme ou réglementation. Il peut être utilisé pour aider à juger et évaluer différents choix stratégiques en termes de leurs conséquences sur tous les groupes de la société affectée par ces décisions.

L'ACB est un outil analytique qui peut aider les décideurs à allouer les ressources de manière socialement efficace. Elle identifie et cherche à quantifier les coûts et les bénéfices d'un programme ou d'une activité, et présente les données disponibles sous une forme structurée. L'une des forces de la méthode est qu'elle fournit un cadre pour analyser les données (et donc les éléments d'une décision) de façon logique et cohérente. L'ACB aide le preneur de décision à répondre à des questions telles que :

- Est-ce que la proposition fournit un bénéfice net à la société toute entière ?
- Devrait-on mettre en œuvre le projet, programme ou réglementation considéré ?
- Devrait-on poursuivre avec le projet ou programme?
- Parmi plusieurs projets alternatifs, lequel devrait être sélectionné ?

Un des intérêts de cette méthode est d'explicitier les hypothèses sous-tendant une décision, d'identifier et de quantifier l'ensemble des éléments pris en compte dans la décision, donc d'améliorer la transparence du processus décisionnel. En fournissant un cadre structuré pour discuter sur des bases communes, elle peut faciliter la concertation entre les différentes parties prenantes d'une décision. Les principes et la pratique des analyses coût-bénéfices sont bien établis aux États-Unis.

III.1.2 Les étapes pratiques de L'Analyse Coût-Bénéfices

On peut décomposer la démarche d'une l'Analyse Coût-Bénéfices en plusieurs étapes organisées comme données sur la figure (3.1):

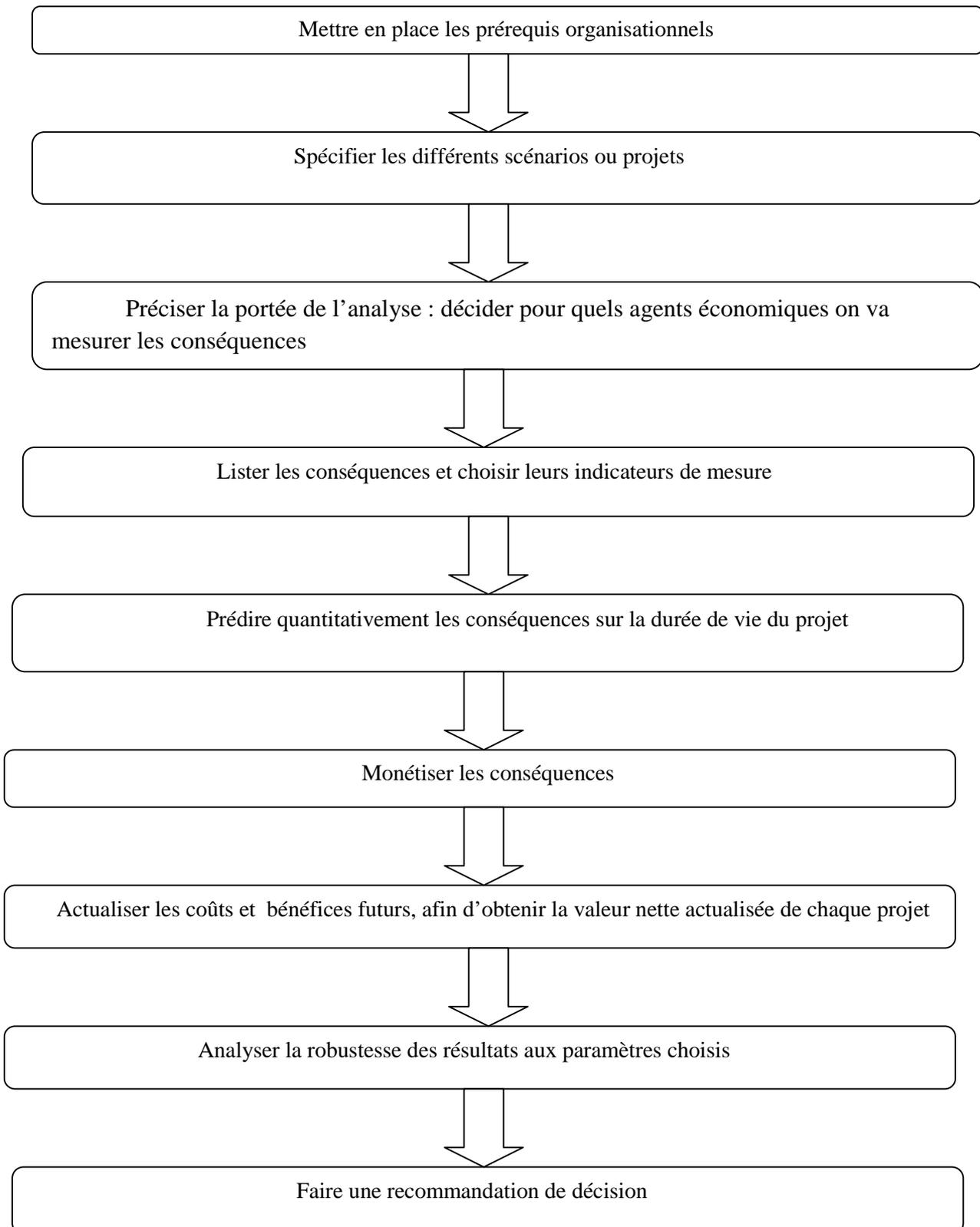


Figure (3.1) Les étapes pratiques de l'Analyse Coût-Bénéfice.

III.1.3 Objectifs de l'Analyse Coût-Bénéfices :

Afin de faciliter son utilisation dans de bonnes conditions. Nous nous focalisons sur des questions relatives à la gestion des risques industriels, et en particulier sur l'arbitrage entre dépenses en matière de prévention et bénéfice social escompté de la réduction du niveau de risque. L'ACB pourrait être envisagé comme un outil méthodologique permettant de comparer différents projets propres à réduire les risques émanant d'un établissement à risque d'accident majeur. Les différents projets conduiraient à différentes solutions de réduction du risque, par exemple en considérant les possibilités de substitution entre prévention du risque à la source et protection des enjeux autour du site. Cette méthode fournit des indications quantifiées sur les possibilités techniques de mesures de prévention et sur leurs impacts, ainsi que sur les conséquences des opportunités de prescriptions foncières et sur le bâti, afin de prendre la mesure des arbitrages possibles.

L'analyse coût-bénéfices permet de :

- clarifier les éléments pris en compte dans l'analyse, et fournir un cadre structuré pour débattre de leur importance relative ;
- intégrer les intérêts des différentes parties prenantes ;
- favoriser la concertation, l'échange d'information, voire même la contestation d'une décision en fournissant un cadre structuré pour comparer les différents composants d'une décision ;
- effectuer une analyse de sensibilité afin de déterminer quelles hypothèses ou données d'entrée ont le plus grand impact sur les résultats de l'analyse ;
- garder une trace des éléments ayant conduit à privilégier une option parmi d'autres à un instant donné. Cette trace peut se révéler précieuse lorsqu'il s'agit de justifier une décision pour plusieurs années [26].

III.2 Méthodes analytiques de planification

La décision d'investissement et son caractère optimal sur le renouvellement d'ouvrages existants ou la création d'ouvrages nouveaux, ne peuvent s'analyser sans tenir compte des conséquences de cette décision à la fois sur les frais d'exploitation (pertes) résultats et sur la qualité du produit distribué. Nous allons définir un critère économique qui consiste à minimiser la fonction «objectif et certains critères de décisions qui aident au choix entre les solutions envisagées lors de traitement de la qualité de service.

III.2.1 La fonction de coût

On distingue trois constituantes principales de la fonction coût :

- les dépenses en investissements I_t ;
- la gêne économique F_t ;
- les frais d'exploitation R_t ;

Le critère économique en question, est celui qui minimise la fonction coût et est définie par

$$\text{Min } E \sum_{t=1}^T \frac{I_t + R_t + F_t}{(1+i)^t} - \frac{V_{T+1}}{(1+i)^{T+1}} \quad (3.1)$$

Où T : est l'horizon de la planification ;

t : est l'indice du "pas de temps";

i : est le taux d'actualisation ;

E : un opérateur désignant l'espérance mathématique.

On considère la période de planification confondue avec la durée de vie de l'équipement sur lequel ou investit.

Cela nous amène à effectuer une hypothèse simplificatrice avec l'expression $\left(\frac{V_{T+1}}{(1+i)^{T+1}}\right)$ de l'équation (3-1) égale à zéro.

La fonction de coût devient :

$$\text{Min } E \sum_{t=1}^T \frac{I_t + R_t + F_t}{(1+i)^t} \quad (3.2)$$

Les constituantes de la fonction coût seront calculées en valeurs actualisées. Par conséquent, on introduit le taux d'actualisation i qui caractérise la politique d'investissement de l'entreprise.

Ce taux permet d'exprimer le facteur de récupération du capital (Amortissements) donnée par: $CRF = \frac{\gamma^n(\gamma-1)}{(\gamma^n-1)}$; $\gamma = i+1$, tel que n est l'année d'utilisation.

III.2.2 Les dépenses en investissements

Dans un réseau électrique, les investissements s'effectuent sur un ou plusieurs ouvrages, dont la durée d'utilisation diffère d'un ouvrage à un autre. Le calcul du coût total s'effectue sur une durée d'étude connue.

Soit I_k , le coût en capital unitaire capitalisé d'un élément k . Le coût d'investissement annuel actualisé d'un élément k est donné par:

$$I_{ak} = I_k \cdot \frac{\gamma^n (\gamma - 1)}{(\gamma^n - 1)} \quad (3.3)$$

Le coût de d'investissement totale d'éléments k sur la période $T = [t_1, t_2]$ de planification est le suivant:

$$C_I(t) = \sum_{t=t_1}^{t_2} \sum_{k=1}^{k'} I_{ak}(t) \cdot \gamma^{-t} \quad (3.4)$$

III.2.2.3 coût des pertes

Dans ce cas le coût des pertes dépend essentiellement des pertes de puissance maximale qui transite dans le réseau.

Les pertes maximales sont données par :

$$P_{\max} = 3 \times R \times I_{\max}^2$$

Le coût annuel des pertes est données par :

$$C_k = (k_p + k_w \cdot \theta \cdot T_a) P_{\max} \quad (3.5)$$

Si l'on désigne par r le facteur d'évolution de la charge l'équation (3.5) devient :

$$C_k = (K_p + K_w \cdot \theta \cdot T_a) P_{\max} \cdot r^n \quad (3.6)$$

Avec R : Résistance de la bobine de compteur en Ω .

k_w : Tarif du Kwh;

K_p : Tarif annuel du kW ;

θ : Facteur de charge ;

I_{\max} : Charge maximale ;

Si on a k' tronçons, le coût total annuel est alors :

$$C' = \sum_{k=1}^{k'} C_k$$

Le coût total des pertes est donnée par :

$$C_p = \sum_{t=t_1}^{t_2} C'_p \gamma^{-t} \quad (3.7)$$

III.2-3 La gêne économique

Le travail développé dans le cadre des smart grids est inspiré de la gêne économique traitée dans la valorisation des mesures techniques et organisationnelles pour améliorer la fiabilité du réseau. Cette gêne est ressentie principalement par l'utilisateur du réseau électrique. Les constituantes principales sont les valeurs caractéristiques de la fiabilité. Ces dernières sont exprimées en termes de nombre de coupures annuelles, de leurs durées et de l'énergie annuelle non distribuée.

-Premières valorisation de la gêne

Elle a été définie comme étant le coût de la défaillance qui croît rapidement quand la coupure se prolonge. Elle est calculée suivant la durée de coupure.

a) Cas de coupures brèves :

Le coût de la défaillance C_d est proportionnel à la puissance coupée et est donnée par

$$C_d = K_p \cdot P_c$$

b) Cas de coupures moyennes :

Le coût de la défaillance est proportionnel à l'énergie non distribuée et est exprimée par :

$$C_d = K_w \int_{T_c} P_c(t) \cdot dt$$

En particulier pour une puissance P_c constante le coût de la défaillance sera :

$$C_d = K_w \cdot P_c \cdot T_c$$

Où T_c est la durée de coupure.

c) Cas de coupures longues :

Le coût de la défaillance est le coût de l'énergie non distribuée est exprimé par :

$$C_d(t) = K_w \cdot (1 + \theta) \cdot P_c \cdot t$$

Dans notre travail, compte tenu de taux d'actualisation, on prend $N = h_f$ et W_n ;

Où W_n : l'énergie annuelle non distribuée ;

P_c : La puissance moyenne par départ ;

h_f : La fréquence moyenne annuelle de coupure.

Le coût total de l'énergie non distribuée est

$$C_w = k_w \cdot \sum_{t=t_1}^{t_2} W_n \cdot \gamma^{-t} \quad (3.8)$$

Le coût actualisé de la gêne économique est alors

$$C_g = C_w + K_p \sum_{t=t_1}^{t_2} P_c \cdot h_f^2 \gamma^{-t} \quad (3.9)$$

Le coût total actualisé est finalement [27] :

$$C = C_G + C_I + C_P \quad (3.10)$$

III.2-4 Le gain :

Le gain est formulé par la différence entre les coûts des deux variantes à comparer. La première variante correspond à l'état actuel d'exploitation, et la deuxième consiste à l'intégration d'un équipement de smart grid (compteur intelligent) au réseau.

$$G = C_{V0} - C_{V1}$$

(3.11)

II.3 Etude de cas ou application :

Dans notre cas, il s'agit de remplacer les compteurs conventionnels par des compteurs intelligents. On considère un réseau où on installe (remplacement) de dix (10) compteurs.

La problématique traitée est résumée sous forme des variantes, à savoir : l'état initial représenté par la variante V0 et l'état avec les compteurs intelligents comme variante V1

III.3-1 Calcul du coût de la variante "V0"

Dans cette variante, il ya aucun investissement engagé.

1) Le coût d'investissement est :

$$C_I = 0$$

2) Coût des pertes :

Les pertes ne sont pas prises en considération.

$$C_p = 0$$

3) Coût de la gêne économique :

Dans ce cas la puissance consommée par les dix (10) utilisateurs de compteurs intelligents est de :

$$10 \times 4 \text{KVA} = 40 \text{ KVA.}$$

Le montant de la fraude est estimé à 10% de la consommation totale ;

Et le montant des factures non payées est estimé à 10% de la consommation ;

Et le préjudice financier des branchements illicites est de 5% de la consommation ;

$$C_{V0} = 8409,6 \text{ €}$$

III.3-2 Calcul du coût de la variante "V1"

1) Coût d'investissements :

Dans notre cas d'étude, les dépenses en investissement correspondent à la mise à disposition et l'installation de 10 compteurs intelligents dans la durée de vie de chaque composant est estimée à 20 années. Le prix d'achat d'un compteur tiré des documents EDF est estimé à 240€ et le coût de l'installation est de 54€. En considérant un taux d'actualisation autour de 4%, Et le tarif d'un kWh est de 0,12€ ; Le coût de revient investi sur un seul compteur intelligent est de :

$$I_k = 295€ \text{ Et donc } I_{ak} = 21,70€$$

Le coût de d'investissement annuel d'éléments k 'sur la période T = [t1, t2] de planification est le suivant:

Année	1	2	3	4	5	6	7	8	9	10
Investissement	208.00	200.00	192.31	184.92	177.80	170.96	164.39	158.07	151.99	146.14

11	12	13	14	15	16	17	18	19	20
140.52	135.11	129.92	124.92	120.12	115.50	111.05	107.15	103.02	99.06

Le coût de d'investissement totale d'éléments k 'sur la période T = [t1, t2] de planification est le suivant:

$$C_I = 2950€$$

2) Le coût des pertes : elles sont exprimées par l'équation (3.7) et supposées nulles.

$$C_{pertes} = 0$$

3) Le coût de La gêne économique :

Suite à l'installation des compteurs intelligents on réduit la fraude de 3% et les branches illicites de 2% et les facteurs non payées de 5%

Le coût de la gêne économique est :

$$C_G = 5045,76€$$

Le coût total de la variante V1 est :

$$C_{V1} = 7995,76€$$

III.3-3 Calcul Le gain :

Dans ce cas le gain est égale à la différence entre les deux variantes V0 et V1

$$G = C_{V0} - C_{V1}$$

$$G = 8409,6 - 7995,76 = 413,84\text{€}$$

Cette application à une échelle réduite renseigne sur l'intérêt de l'installation des compteurs intelligents. Dans la littérature, on a mentionné le cas de l'Italie qui s'est engagé à lutter contre la fraude de l'électricité et à engager un projet d'installation de 30 millions de compteurs de ce type. L'ENEL certifie que le coût d'investissement a été amorti par l'argent récupéré de la fraude.

III.4 Autre impacte des smart grids

III.4-1 Détecteur de défaut :

Dans certaines publications récentes [28], on trouve comme mesures techniques engagée pour améliorer la fiabilité du réseau et par conséquent la satisfaction du consommateur, on trouve l'installation des indicateurs de défauts. Ce dernier permet de réduire le temps de recherche de défaut et par conséquent la durée des coupures. Il a un impact direct sur le préjudice ressenti par le client et un impact indirect ressenti par l'entreprise exprimé en termes d'énergie non distribuée.

$$\text{END} = t_c \cdot P$$

La diminution de facteur t_c implique la diminution de l'énergie non distribué, et par conséquent celle de l'énergie non distribuée donc aussi la diminution de la gêne économique.

III.5 Conclusion

Au cours de ce chapitre, nous avons spécifié l'importance d'une étude technico-économique dans la prise de toute éventuelle décision des projets d'investissement énergétique, la méthode utilisée dans notre étude est la méthode d'analyse du coût/bénéfices. Cette dernière, comme son nom l'indique est relativement simple, l'ACB compare les coûts et les bénéfices associés à une décision, laquelle est jugée économiquement souhaitable si les bénéfices attendus sont remarquables.

Nous avons effectué une étude analytique où nous définissions un critère économique pour minimiser la fonction coût, puis un calcul sur le gain. Cependant, nous avons manipulé un exemple sur une expérience de route pour la généralisation des compteurs intelligents appliquant l'étude économique sous dessus. Ceci montre bien le gain apporté par ces dispositifs intelligent aussi bien du côté consommateur que du gestionnaire, pour le premier lui permet de maîtriser mieux sa consommation, et pour le second de répondre activement pour le premier.

Enfin, l'étude technico-économique pour les projets smart grids est d'une importance capitale pour assurer leur rentabilité. Cependant, l'investissement dans le compteur intelligent doit être considéré sur une période très longue (20 à 25 ans) et les acteurs de la chaîne de valeur doivent s'accorder pour savoir comment se répartit les charges de cet investissement

Introduction

Les systèmes d'information (SI) dans les smart grids reposent en partie sur des systèmes qui stockent, traitent et transmettent de l'information. Ces derniers peuvent être, pour les plus sophistiquées, des ordinateurs mais aussi des périphériques informatiques, des téléphones, des compteurs, des capteurs...etc. Ses systèmes sont majoritairement reliés par des réseaux locaux à l'intérieur de leur organisme d'appartenance voir reliés aux réseaux internet. Certains SI offrent des services, parfois vitaux ou essentiels, sur lesquels repose l'économie de la gestion d'énergie électrique. Ainsi de multiples informations risquent d'être accessibles de presque n'importe quel point des connections du smart grid. Les enjeux de la sécurité dans les smart grids, ne sont pas d'accroître les opportunités de gain mais de limiter les possibilités de pertes.

A ce titre, les informations dans les smart grids constituent une ressource stratégique, une matière première. La protection de ce patrimoine contre les malveillances doit par conséquent être un souci permanent d'organisation.

Selon le rapport d'*EPRI*, « La sécurité informatique est un thème critique dans les smart grids dû au potentiel croissant des attaques cybernétiques. Les attaques proviennent non seulement par des acteurs en relation, comme à partir des employés mécontents, l'espionnage industriel, mais aussi par des Hackers expérimentés dans le domaine d'électrotechnique pour pénétrer un réseau, puis ils accèdent aux logiciels de gestion, et changent les conditions de charge, de commande et de régulation pour déstabiliser le réseaux de manière imprévisible.» [29].

IV.1 Définition

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité:

1. **disponibilité D:** demande que l'information sur le système soit disponible aux personnes autorisées.
2. **Intégrité I:** demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.

3. **Confidentialité C**: demande que l'information sur le système ne puisse être lue que par les personnes autorisées.

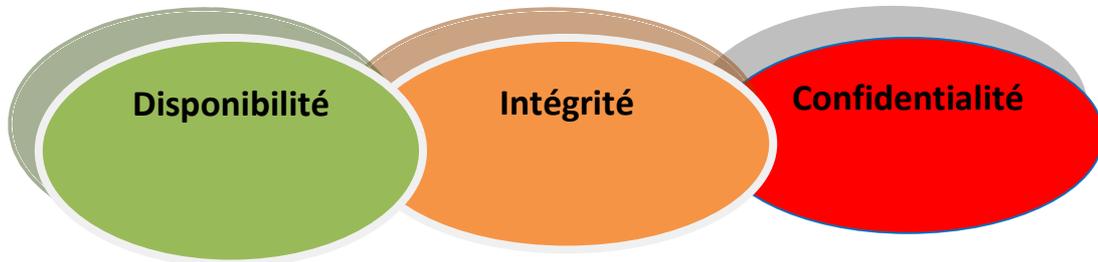


Figure (4.1) Objectifs de la sécurité d'informations d'un système [30].

VI.2 Mécanismes de sécurité

Les trois propriétés (confidentialité, intégrité et disponibilité) peuvent être assurées totalement ou partiellement par des mécanismes de sécurité. Nous définissons ci-dessous les mécanismes les plus importants de la sécurité :

- **Autorisation** : action par laquelle on permet, ou on interdit, à un utilisateur un ensemble d'actions sur des informations.
- **Authentification** : reconnaître (avec certitude) un utilisateur.
- **Cryptographie** : l'art d'écrire des secrets pour les rendre inintelligibles à des tiers.
- **Chiffrement** : il vise à assurer la confidentialité d'informations en transformant un texte en clair en un cryptogramme (ou texte chiffré) à l'aide d'une clé de chiffrement. Nous allons traiter ce mécanisme dans une partie spéciale avec un algorithme en appui pour un chiffrement asymétrique (PKI).
- **Clé** : information (secrète) utilisée pour chiffrer ou déchiffrer un texte chiffré.
- **Signature** : information contenue dans un message servant à garantir son authenticité et intégrité [31].

IV.3 Risques, menaces et politique de sécurité

Risques et menaces sont deux concepts fondamentaux pour la compréhension des techniques utilisées dans le domaine de la sécurité. Le *risque* est une fonction de paramètres qu'on peut maîtriser à la différence de la *menace* qui est liée à des actions ou des opérations émanant de tiers. Dans un smart grid, la sécurité concerne non seulement les éléments physiques (modems, routeurs, commutateurs...) mais aussi les éléments logiques, voire

volatils, que représentent les données qui circulent dans les infrastructures de communication. Le responsable de la sécurité doit analyser l'importance des risques encourus, les menaces potentielles et définir un plan général de protection qu'on appelle *politique de sécurité*.

IV.3.1 Risques

Les risques se mesurent en fonction de deux critères principaux : la vulnérabilité et la sensibilité. La vulnérabilité désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau intelligent est un point facile à approcher. Un élément de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible : le compteur communicant, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau de communication (cet exemple sera manipulé dans une partie de ce chapitre).

On peut classer les risques en deux catégories : structurels, ils sont liés à l'organisation et la démarche d'un gestionnaire de sécurité ; accidentels, ils sont indépendants de l'entreprise. Enfin, selon les niveaux de sensibilité et de vulnérabilité, c'est distingué quatre niveaux de risques dans les smart grids, selon qu'ils sont acceptables, courants, majeurs ou inacceptables.

- Acceptables. Ils n'induisent aucune conséquence grave pour les entités utilisatrices du réseau. Ils sont facilement rattrapables : pannes électriques de quelques minutes, perte d'une liaison...
- Courants. Ce sont ceux qui ne portent pas un préjudice grave. Ils se traduisent, par exemple, par une congestion d'une partie du réseau. La mauvaise configuration d'un équipement peut causer la répétition des messages émis, un opérateur peut détruire involontairement un fichier de configuration...
- Majeurs. Ils sont liés à des facteurs rares. Ils causent des préjudices, mais ils peuvent encore être corrigés. Un attaquant isole un client. La conséquence se traduit par le remplacement de l'ensemble du matériel, mais, tous les logiciels et les données avaient été sauvegardés et archivés dans les serveurs centraux.
- Inacceptables. Ils sont, en général, fatals pour le réseau lui-même. Ils peuvent entraîner son dépôt de bilan. Exemple : la pénétration des réseaux de gestion avancée de l'énergie EMS, ainsi des préjudices peuvent atteindre les clients.

IV.3.2 Menaces

On peut également classer les menaces en deux catégories selon qu'elles ne changent rien (menaces *passives*) ou qu'elles perturbent effectivement le smart grid (menaces *actives*).

Les menaces passives nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même.

Les menaces actives nuisent à l'intégrité des données et à la sécurité du réseau lui-même. Elles se traduisent par différents types d'attaques : modifier ou détruire des informations, d'empêcher une partie du réseau intelligent de fonctionner, de rejouer un scénario après en avoir modifié certains aspects. Parmi les menaces actives, on distingue celles liées aux infrastructures de supervision et gestion SCADA (pour les centrales de production et les réseaux de transport), les menaces aux infrastructures de comptage évolué AMI dont le compteur communicant est le maillon remarquable, ainsi que les menaces liées aux autres services.

IV.3.3 Politique de sécurité

La définition d'une politique de sécurité pour les smart grids nécessite d'abord l'analyse des systèmes d'informations ainsi que les informations qui circulent ou qui sont stockées (analyse de leur importance pour le gestionnaire, analyse du coût que représenterait la perte de données ou d'un équipement) et celles des menaces qu'on peut objectivement envisager. Les priorités et les stratégies influent sur le choix des procédures internes que devront respecter tous les utilisateurs. Il faut définir les mécanismes de protection à mettre en œuvre (les outils antivirus, les pare-feu, les *patches* ou programmes de correction des systèmes et des applications utilisés) puis tous les outils de surveillance (depuis l'audit jusqu'au journal historique et la détection des intrusions). Nous ne détaillerons ici que les aspects de la sécurité directement liés au réseau, le contrôle d'accès physique aux bâtiments, sécurité des systèmes de télégestion SCADA...

IV.4 Analyses des vulnérabilités des smart grids

Il existe de nombreuses méthodes d'analyses de risques. Outre le domaine de la sécurité des systèmes d'information que nous abordons ici, les domaines de gestion d'infrastructure des réseaux SCADA, des infrastructures à comptage évolué AMI ou encore les domaines de gestion d'énergie électrique EMS, ont recours à des analyses de risques.

Considérons en premier lieu les vulnérabilités liées à la phase de développement du smart grids. Ces vulnérabilités sont dues à un défaut de spécification ou de conception

(comme par exemple l'oubli d'un cas d'utilisation extrême dans les infrastructures AMI, l'absence d'interdiction dans l'accès à des données sensibles) ou à une erreur de développement. Ces vulnérabilités sont donc introduites dans les composants avant que ceux-ci ne soient disponibles ou utilisés. De plus, si un composant contient une vulnérabilité, cette vulnérabilité sera présente sur tous les systèmes comportant ce composant dès la mise en service de ce dernier. Cette caractéristique est très intéressante et permet d'étudier l'évolution de l'état des vulnérabilités dans le temps.

Bien que ces domaines soient très imbriqués, la démarche générale d'une analyse de risque peut se résumer dans les trois étapes suivantes :

- Identifier les menaces auxquelles devra faire face le système ou l'organisation (quels types d'attaquants, mais aussi quels phénomènes.
- Identifier les vulnérabilités des infrastructures des smart grids face à ces menaces ;
- Estimer les conséquences qui résulteraient de la réalisation des menaces et de l'exploitation des vulnérabilités.

A partir de ses trois points principaux, nous allons définir une méthode d'analyse de risque adaptée aux systèmes d'informations dans les smart grids en général, c'est bien la méthode MEHARI.

Infrastructure smart grid	Donnée	Mécanismes de sécurité
AMI	D, I, C	1, 2, 3, 4, 5
DMS	D, I, C	3, 4
EMS	I, C	2, 3, 4, 5
SCADA	D, I	2, 3, 4, 5

Table (4.1) Infrastructure à analyser pour la sécurité dans le smart grid [32].

D disponibilité, I intégrité, C confidentialité

1 à 5 niveaux de sécurité.

IV.4.1 Méthode d'analyse MEHARI

Nous avons décidé d'appliquer ou du moins, essayé d'appliquer, la méthode MEHARI à notre étude.

Cette méthode est intéressante pour le cadre de la sécurité des projets smart grids. C'est pourquoi nous nous sommes limités à la définition de l'existant, à une recherche adaptée

et à une rapide analyse en fonction des recommandations de la norme ISO 17999:2005, référence sur la gestion de la sécurité informatique dans les infrastructures énergétiques. L'analyse par une méthode d'audit n'était pas obligatoire dans notre mémoire. Cependant, il nous apparaissait intéressant d'essayer de prendre en main un outil complet d'analyse de la sécurité des smart grids.

IV.4.1.1 Présentation de la méthode MEHARI

La méthode MEHARI (Méthode Harmonisée d'Analyse des Risques) a été développée par le CLUSIF [31] pour cerner les risques liés à l'informatique et à l'information. Cette méthode fournit un cadre, des procédés et des bases de connaissances permettant de se pencher sur plusieurs points tels que:

- Les enjeux majeurs de sécurité pour la distribution automatisée de l'énergie électrique et notamment les dysfonctionnements potentiels des systèmes informatiques et la gravité engendrée.
- Les vulnérabilités, en évaluant la qualité des mesures de sécurités en place,
- Les risques de manière à définir les mesures les mieux adaptées à mettre en œuvre.

L'objectif de cette méthode pour la sécurité des smart grid consiste à minimiser les risques encourus du fait de son système d'information. Cela signifie que la sécurité est l'absence de risque inacceptable.

IV.4.1.2 Démarche de l'analyse

Toute démarche d'analyse de risque commence à :

- Partir des enjeux majeurs, et analyser, pour chacun, comment il pourrait être attaqué, puis prendre les mesures en conséquence.
- Partir des vulnérabilités et les réduire toutes jusqu'à ce que les risques deviennent acceptable.
- Partir des situations de risque combinant les enjeux et les vulnérabilités et procéder à une analyse de risque.

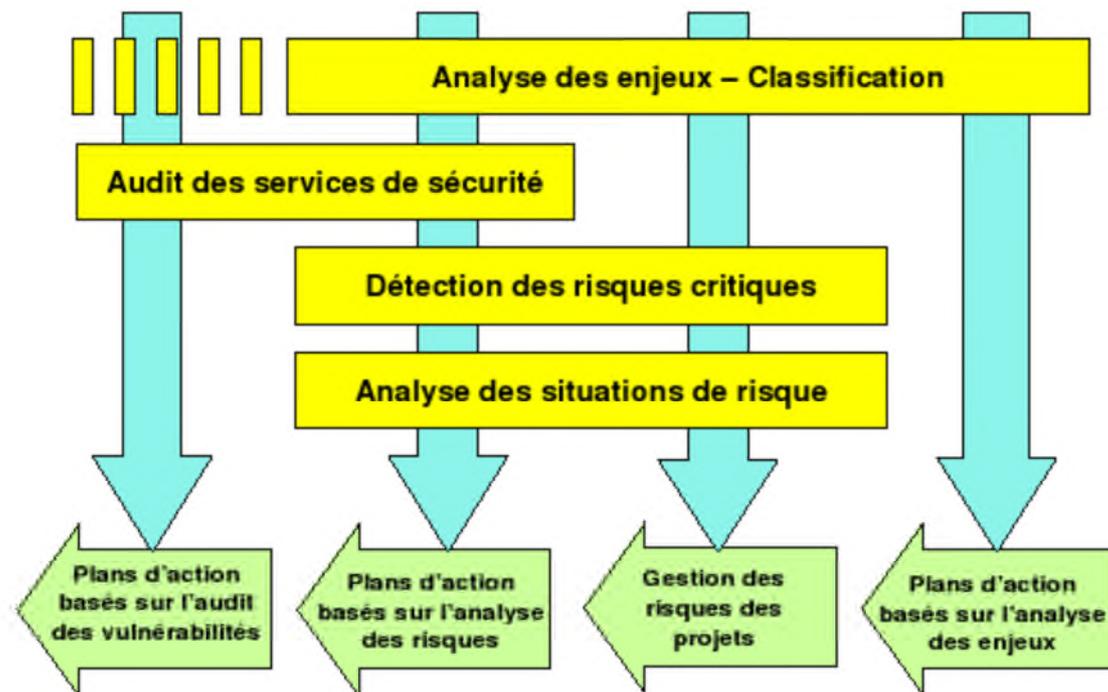


Figure (4.2) Démarche de sécurité par MEHARI [33] ;

Les vulnérabilités des systèmes d'information relatifs à un smart grid avec cette méthode sont relatives à la :

- Cohabitation de nouvelles et anciennes applications
- Interconnexion de différents SI de plus en plus entre les différents acteurs
- Ouverture des SI vers l'extérieur (internet)
- Télémaintenance, télé relève et infogérance
- Mobilité, nomadisme, connexion à distance, GPS...

IV.4.1.3 MEHARI appliquée au comptage évolué, compteur intelligent

Il s'agit donc de répertorier les actifs/ressources dans un compteur, d'identifier les dysfonctionnements redoutés liés à ces ressources, d'évaluer la gravité de ces dysfonctionnements et ensuite de classer les ressources en vue d'être utilisées pour l'analyse de risque. Pour cela la méthode intègre un questionnaire pour un groupe de client et de gestionnaires permettant de réaliser l'audit. Cet audit permettra d'avoir une vision globale de la qualité de la sécurité du compteur et de mettre en évidence ses faiblesses.

Enfin, le module d'analyse de risques permet :

- Soit en partant de la base de connaissance des situations de risques de MEHARI,
- Soit en partant de situations de risques mise en place par le fournisseur de ses dispositifs,

- Soit des deux, de déterminer si oui ou non, un risque est acceptable et ainsi de mettre en place un plan de sécurité pour le risque étudié. La méthode inclue les recommandations de la norme ISO 27002. On fait l'objet d'une étude de cryptographie des données.

On s'inspirant à partir d'un rapport d'audit sur la sécurité du compteur intelligent Linky publié par la CRE [34], où c'est remarquer la présence des vulnérabilités liées à la confidentialité des données envoyées par le GRD au niveau du compteur. A ce titre, nous allons appliquer la cryptographie asymétrique pour assurer la confidentialité des données échangées.

IV.5 Sécurité du comptage numérique évolué

Advanced Metering Infrastructure **AMI**, ce système de comptage évolué est l'un des concepts clés des réseaux intelligents puisqu'il permet de communiquer sur les données de consommations avec les équipements en aval et en amont du compteur intelligent, (ce dernier nous allons le développer dans un point spécial vu son rôle critique dans la sécurité AMI).

Ces systèmes intègrent des équipements et des logiciels permettant de compter, de communiquer et d'analyser les consommations des clients. D'une manière générale, ils permettent de relever de manière détaillée et régulière les consommations et favorisent les offres de facturation intégrant des coûts horaires différenciés. A ce titre, vu le flux important de données, leurs concentration et leur disponibilité sur un réseau, d'où de nouvelles menaces apparaissent car derrière tous ces échanges et partages, il y a toujours un modèle économique pouvant être déviant, soucieux de valoriser toute information.

Les systèmes de comptage évolué appelés également comptage communicant permettent d'affiner le comptage, de réaliser des opérations à distance (en particulier la relève) et de mieux maîtriser le réseau. Toutefois la sécurité des systèmes d'information SSI pour ses systèmes reste un risque majeur pour leur un fonctionnement intégral. Dans cette partie, nous intéressons à la sécurité informatique au niveau du compteur communicant et de son environnement.

IV.5.1 Les communications dans les compteurs communicants

Nous allons survoler l'aspect technique du compteur intelligent, tant que ce dernier est abordé en détail dans l'autre travaille de recherche par nos camarades travaillant sur « l'aspect technique des smart grids », nous nous intéressant donc au côté communications.

Une communication est décomposée en un certain nombre de transactions. Chaque transaction se traduit par une émission de l'émetteur vers le récepteur. Au gré de

l'enchaînement des transactions, les systèmes appelant et appelé jouent tour à tour le rôle d'émetteur et de récepteur.

Cette architecture constitue le modèle de référence OSI (Open system interconnection) et est capable de supporter la majorité des besoins de communication de données des compteurs communicants. Il est décliné en sept couches (figure 4.4) :

- couche Physique : elle décrit les caractéristiques physiques de la communication ;
- couche Liaison de données : elle spécifie comment les paquets sont transportés sur la couche physique ;
- couche Réseau : elle résout le problème de l'acheminement de paquets à travers un seul réseau ;
- couche Transport : elle assure que les données arrivent dans l'ordre correct ;
- couche Session : elle définit l'ouverture des sessions sur les machines du réseau ;
- couche Présentation : elle définit la manière dont les données vont être représentées ;
- couche Application : elle est l'interface utilisateur/logiciel et fait parvenir les requêtes à la couche de présentation [35].

IV.5.1.1 Protocole de communication TCP/IP

a) Principe

La suite Internet Protocole ou suite TCP/IP est un ensemble de protocoles de communication utilisé principalement par le **réseau Internet**. Les deux couches de protocoles les plus importantes sont Transmission Control Protocol (TCP) et Internet Protocol (IP). La correspondance entre le modèle OSI et le protocole TCP/IP est donnée sur la figure 4.

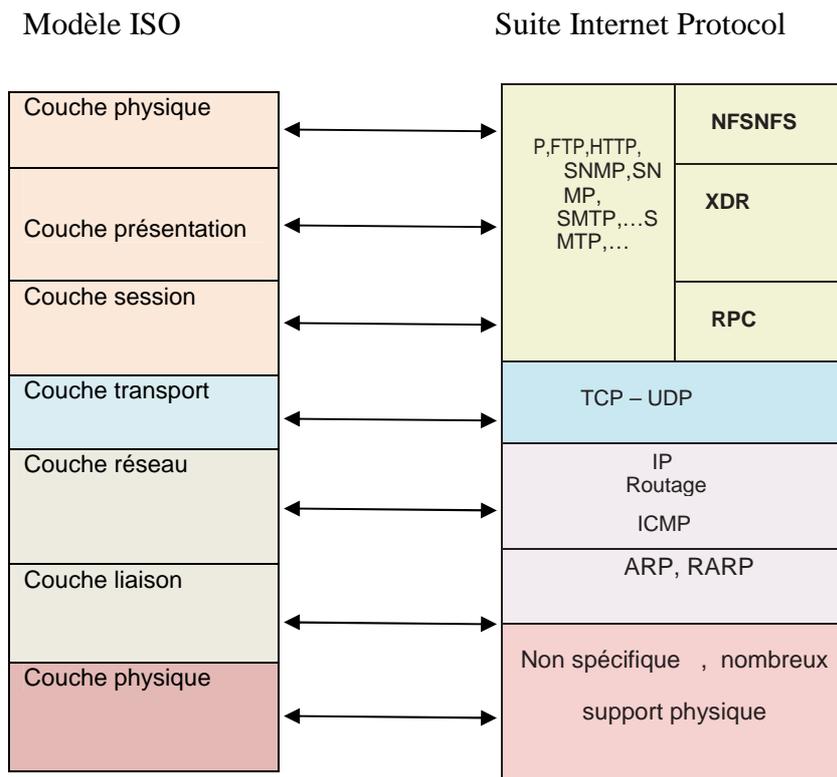


Figure (4.3) Correspondance entre modèle OSI et protocole TCP/IP

La plateforme du compteur intelligent utilise se model de communication avec les serveurs du distributeur d'énergie. Du niveau 7 de l'application, au niveau 4 du transport, l'information circule dans ce que l'on appelle un " message ", au niveau 3 elle se nomme " packet ", puis " frame " au niveau 2 et " signal " au niveau 1.

b) Caractéristiques de TCP/IP

Le succès de TCP/IP pour le comptage évolué vient d'un choix technique adapté, s'appuie ensuite sur des caractéristiques intéressantes :

1. C'est un protocole ouvert, les sources (C) en sont disponibles gratuitement et ont été développés indépendamment d'une architecture particulière, d'un système d'exploitation particulier, d'une structure commerciale propriétaire. Ils sont donc théoriquement transportables sur n'importe quel type de plate-forme des compteurs.
2. Ce protocole est indépendant du support physique du réseau. Cela permet à TCP/IP d'être véhiculé par des supports et des technologies aussi différents qu'une ligne série, un câble coaxial Ethernet, une liaison louée, un réseau token-ring, une liaison radio (satellites, wireless), xDSL, ATM, fibre optique, liaison en courant porteur en ligne CPL...etc.
3. Le mode d'adressage est commun à tous les clients, quelle que soit la plate-forme qui l'utilise. Si

l'unicité de l'adresse est respectée, les communications aboutissent même si les hôtes sont aux antipodes.

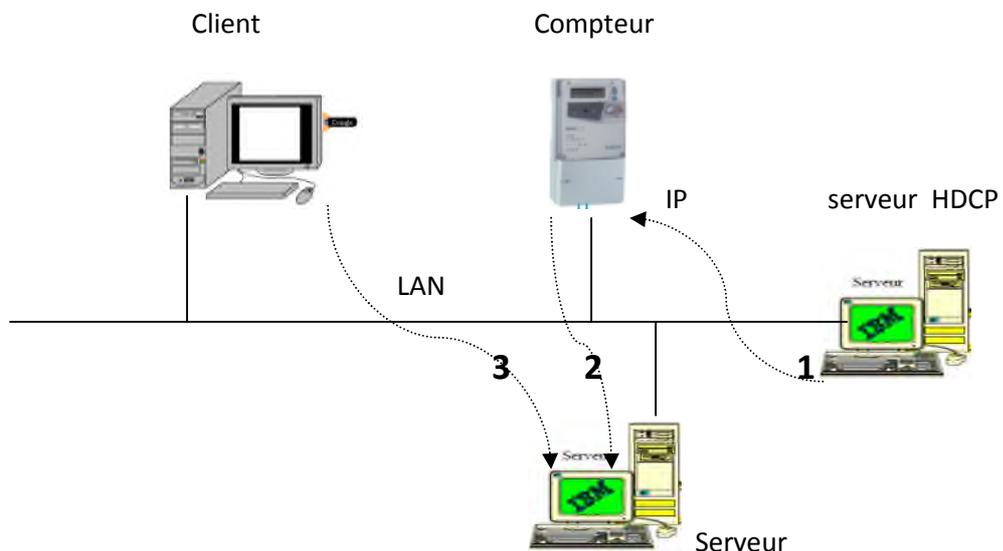
4. Les protocoles de hauts niveaux sont standardisés ce qui permet des développements largement répandus et interopérables sur tous types de compteurs intelligents [36].

IV.5.1.2 Unicité de l'adresse IP d'un compteur communicant

Un système de communication doit pouvoir permettre à n'importe quel compteur de se mettre en relation avec n'importe quel serveur. Afin qu'il n'y ait pas d'ambiguïté pour la reconnaissance de chaque compteur d'un client, il est absolument nécessaire d'admettre un principe général d'identification. Lorsque l'on veut établir une communication, il est intuitivement indispensable de posséder trois informations :

1. Le nom de du propriétaire du compteur,
2. Son adresse,
3. Le réseau auquel il est raccordé.

Les adresses IP (version 4) sont standardisées sous forme d'un nombre de 32 bits qui permet à la fois l'identification de chaque boîtier et du réseau auquel il appartient. Le choix des nombres composants une adresse IP n'est pas laissée au hasard, au contraire il fait l'objet d'une attention particulière notamment pour faciliter les opérations d'identification.



Nom du compteur	Adresse IP
SLB761MA12345678	10.485.234.5

Figure (4.4) Exemple d'adresse IP d'un compteur [37].

IV.5.2 Sécurité par Infrastructure à clef publique

IV.5.2.1 Rappel sur la cryptographie

La cryptographie est un procédé qui permet de rendre un message inintelligible, de protéger des données. Ainsi, tout message ou donnée que l'on souhaite protéger d'un œil indiscret peut se voir modifier par un algorithme cryptographique. Dans la littérature consacrée, nous retrouvons différents termes et usages : cryptage, chiffrement, cryptanalyse, signature.

IV.5.2.2 Chiffrement asymétrique à clef publique

Une infrastructure à comptage évolué AMI, est basée sur un nombre important de compteurs intelligent associés aux serveurs des gestionnaires, ainsi l'authentification de chaque client est impérative. Dans cette section nous proposons l'utilisation et la distribution des clefs dites public pour pouvoir échanger des donnée, faire de la télégestion. Le chiffrement asymétrique utilise des paires de clés asymétriques : une publique et une privée.

Une infrastructure de gestion de clés, (PKI – *Public Key Infrastructure*) permet de mettre en œuvre des systèmes de chiffrement asymétrique. Les principales fonctions supportées sont:

- la génération d'un couple unique de clés (clé privée – clé publique), son attribution à une entité et la sauvegarde des informations nécessaires à sa gestion, archivage des clés, procédures de recouvrement en cas de perte par l'utilisateur ou de demande de mise à disposition par les autorités judiciaires;
- la gestion des certificats numériques, création, signature, émission, validation, révocation, renouvellement des certificats;
- la diffusion des clés publiques aux clients qui la solliciteraient et qui seraient habilités à l'obtenir;
- la certification des clés publiques (signature des certificats numériques).

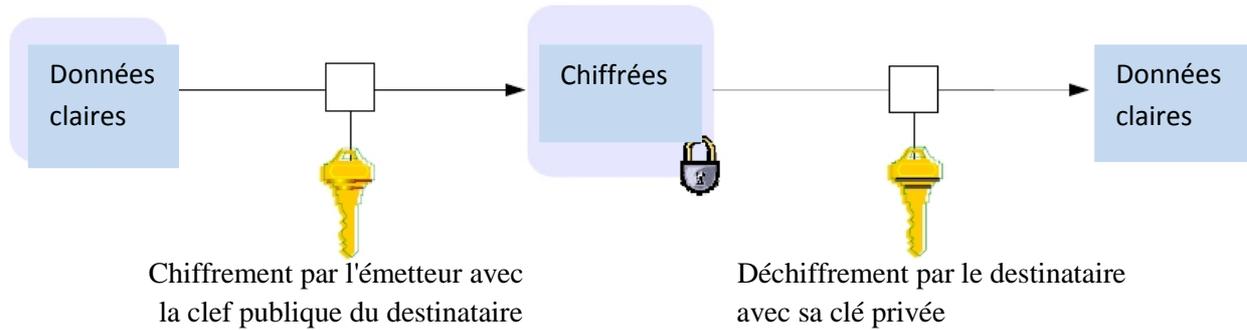


Figure (4.5) procédés de chiffrement des PKI [38].

IV.5.2.3 Algorithme RSA pour le cryptage des données du compteur

IV.5.2.3.1 Principe

Nous avons choisi parmi les algorithmes de chiffrement celui de RSA publié par Rivest, Shamir et Adelman en 1977 [39]. Il est facile de fabriquer de grands nombres premiers p et q pour fixer les idées, 100 chiffres. Etant donné un nombre entier $n=p \cdot q$ produit de 2 grands nombres premiers, il est très difficile de retrouver les facteurs p et q . Intuitivement: la donnée de n est la clé publique : elle suffit pour chiffrer. Pour décrypter, il faut connaître p et q , qui constituent la clé privée. Sécurité dite « calculatoire » : système inconditionnellement sûr.

Théorème. Soient p et q deux nombres premiers, et posons $n = p \times q$.

Soit e est un entier premier avec $(p - 1) \times (q - 1)$, alors il existe un entier $d > 0$ et un entier m tels que $e \times d + m \times (p - 1)(q - 1) = 1$.

Notons au passage que si on choisit d positif et inférieur à $(p - 1)(q - 1)$, alors d est unique.

On note a^k le nombre a élevé à la puissance k , c'est-à-dire le nombre a multiplié par lui-même k fois.

Pour tout entier $a > n$ premier avec n , le reste de la division de $a^{e \times d}$ par n est égal à a .

Schéma :

1. On choisit p, q deux « grands » nombres premiers
 2. On calcule $n=p \cdot q$
 3. Un entier e est choisi tel que premier avec $(p-1)$ et $(q-1)$
 4. L'entier d tel que $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$ est calculé, avec l'algorithme d'Euclide
- le couple d'entier (n, e) représente la clef publique
L'entier d représente la clef privée.

Signature RSA :

Opération de chiffrement, en inversant les rôles de e et d

Le message émis est le couple (M, Md [n])

Tout le monde peut vérifier la signature par possession de la clef publique

Service de non répudiation

→ Sécurité *calculatoire* : repose sur la difficulté de factoriser n

IV.5.2.3.2 Programmation sur le langage C**a) Utilisation de la bibliothèque RSA**

Bien que l'algorithme RSA soit relativement complexe à mettre en œuvre à cause de la taille conséquente des nombres qu'il nécessite (plusieurs centaines de bits), l'utilisation de la bibliothèque RSA nous fournit une interface très simple d'utilisation permettant de faire abstraction de tout ces mécanismes complexes.

Pour faire simple, ici, nous allons créer un projet de type "Console" en C++. Le code minimal s'affiche:

```
1 #include <iostream>
2
3 using namespace std;
4
5 int main()
6 {
7     cout << "Hello world!" << endl;
8     return 0;
9 }
```

Pour utiliser RSA, vous devez inclure l'entête <rsa.h> :

```
1 #include <rsa.h>
```

b) Création et affichage d'une paire de clés :

Pour utiliser l'algorithme RSA, nous devons instancier un objet de type *Rsa*, à partir duquel nous pourrions appeler la méthode *Rsa::genererCles()* qui permet de générer les clés publique et privé.

```
1 #include <iostream>
2 #include <rsa.h>
3
4 using namespace std;
5
6 int main()
7 {
8     Rsa rsa;
9     rsa.genererCles(1024);
10 }
```

```
11     return 0;
12 }
```

Ici, *1024* représente la taille de la clé en bits. Plus précisément, il s'agit de la taille en bits du nombre semi-premier généré. *1024* est un bon compromis entre la fiabilité et le temps de génération des clés.

Les clés sont maintenant créées. Nous pouvons les afficher ainsi :

```
1 #include <iostream>
2 #include <rsa.h>
3
4 using namespace std;
5
6 int main()
7 {
8     Rsa rsa;
9
10    // Generation d'une paire de clés
11    rsa.genererCles(1024);
12
13    // Recuperation de chacune des clés
14    string clePrivee = rsa.clePrivee();
15    string clePublique = rsa.clePublique();
16
17    // Affichage des clés
18    cout << "Cle privee : " << endl;
19    cout << clePrivee << endl;
20    cout << "Cle publique : " << endl;
21    cout << clePublique << endl;
22
23    return 0;
24 }
```

Voici les deux clés, générées aléatoirement, affichées à l'écran :

Clé privée :

```
1a77ae29fa556dd62e031f2b112a3842d04d83ee92b60f1fe07f580308d9ed3ffcfbdfdf0d04611a
18692774a7e004ea98342472cf0a824cfd9ca9c863f686214ad7cd28ca4706f3e06e53d0dbb56ae
b9ca9edd48e5b348fef8e89dc5d0a1e51db364b2d5d3bc4eaaeccf5c7a1a3726b643fb5700f68e44
24d5db0dc548d27-275cb581574b8ff711ea6a888288900dd9182ea4ab3d159ad701203c207d7075
05d2f77eb32b764d64c1fa1d0e902a6326c4007c2465c87de62f3ecd3652b8e1972e8d31e39317c1
784573b2d2e7585a93402a871e9655dd1ac27aef4006d4f851ed3c671d4e5aff9734eea596c8e74b
37ed941a704d7dce6ad1b477099067d
```

Cle publique :

```
1a77ae29fa556dd62e031f2b112a3842d04d83ee92b60f1fe07f580308d9ed3ffcfbdfdf0d04611a
```

```
18692774a7e004ea98342472cf0a824cfd9ca9c863f686214ad7cd28ca4706f3e06e53d0dbb56ae
b9ca9edd48e5b348fef8e89dc5d0a1e51db364b2d5d3bc4eaaecf5c7a1a3726b643fb5700f68e44
24d5db0dc548d27-9186d8de759f8d62d009a97479f8be466f9c9649ec5676f970b656d3245be5bc
4973d49567f4713a91df58bb0c97228313c0cfc4e98f04e8baf23bfbe4e306c5
```

Ces clés sont composées de deux grands nombres chacune, séparé par un '-'. Nous pouvons constater qu'elles ont une partie commune : le premier grand nombre. Il s'agit du fameux nombre à 1024 bits semi-premier affiché en base 16.

IV.5.2.3.3 Programme de cryptage

Nous allons maintenant créer le programme qui va crypter le message avec la clé publique. On ne régénère pas de clé, nous utilisons celle qui nous est fournie. Voici la façon dont on importe la clé publique dans l'objet RSA :

```
1 #include <iostream>
2 #include <rsa.h>
3
4 using namespace std;
5
6 int main()
7 {
8     Rsa rsa;
9
10    // Recopie de la cle publique dans le programme
11    string clePublique
12="1a77ae29fa556dd62e031f2b112a3842d04d83ee92b60f1fe07f580308d9ed3ffcfbdfdf0d04611a"
13 "18692774a7e004ea98342472cf0a824cfd9ca9c863f686214ad7cd28ca4706f3e06e53d0dbb56ae"
14 "b9ca9edd48e5b348fef8e89dc5d0a1e51db364b2d5d3bc4eaaecf5c7a1a3726b643fb5700f68e44"
15 "24d5db0dc548d27-
169186d8de759f8d62d009a97479f8be466f9c9649ec5676f970b656d3245be5bc"
17 "4973d49567f4713a91df58bb0c97228313c0cfc4e98f04e8baf23bfbe4e306c5";
18 // Import de la cle publique dans l'objet RSA
19    rsa.clePublique(clePublique);
20
21
22    return 0;
23 }
```

Il ne reste maintenant plus qu'à crypter notre message secret et à le transmettre à l'autre programme.

```
1 // Cryptage du message secret
2 string messageSecret = " Votre consommation annuelle est de : ** **
3 ** ** ***";
4 string messageCrypte;
5 messageCrypte = rsa.chiffrerAvecClePublique(messageSecret);
6 // Affichage du message crypte a transmettre
7 cout << "Message crypte : " << endl;
8 cout << messageCrypte << endl;
```

Ce qui donne, avec ‘votre consommation annuelle’, le message crypté suivant.

Message crypte :

```
5f4eaa0321fcfe7b87499115b180f04fa9328ea3592e260acc033d677beca854179357d0063e1bed
e8724cc1637e514ed319f4c75f9f716ac20e579e80a40e7ce5f3774a5ddb2dbf7a16438e7021e6
106b72cb499825b0ac68966061f1529a913ec163983c33334ed9c9afc4bb4debb6b3015489fb3cf1
538645329143a6
```

Pour retrouver notre consommation annuelle, nous allons devoir créer le programme de décryptage. Après exécution, le message décrypté est:

Votre consommation annuelle est de : ** ** ** ** **

IV.6 Conclusion

La sécurité informatique est omniprésente dans les smart grids à cause des menaces qui pèsent sur le SI de celui-ci. Avec la superposition des infrastructures de communication et de gestion, (scada, AMI, EMS...) et l'interconnexion de différents réseaux de communication (LAN, WAN, GPRS, Wifi et surtout Internet) la sécurité informatique dans les smart grids constitue la priorité pour le déploiement de ses réseaux intelligents.

Les responsables de sécurité des smart grids doivent mettre en place des méthodes organisationnelles, telles que MEHARI que nous avons appliquée dans ce chapitre pour dévoiler les vulnérabilités des compteurs communicants.

Ensuite, se référant à un rapport sur la sécurité des données des compteurs intelligents Linky, nous avons constaté le manque de la confidentialité dans ces derniers.

A ce titre, avec l'aide de nos camarades du département informatique, on a pu développer un algorithme de chiffrement asymétrique RSA pour crypter les données échangées dans les compteurs.

Enfin, on peut prévoir que l'utilisateur reste l'un des maillons faibles de la chaîne de valeur des smart grids, et en conséquence qu'il faut lui faciliter au maximum la tâche, en délocalisant le noyau de la sécurité (accentuer l'aspect gestion des habilitations et diminuer le nombre d'identifiants) et rendre tout le processus transparent pour lui.

Conclusion générale

Les réseaux d'énergie électrique sont aujourd'hui à l'aube d'une révolution technologique et économique dont l'avènement des smart grids est un marqueur important. L'ouverture à la concurrence du marché de l'énergie électrique et les décisions en matière de politique énergétique relative au changement climatique sont les deux raisons originelles et principales de cette révolution. Ces dernières années, l'arrivée à maturité du système électrique en termes de croissance ainsi que le fort développement des technologies de l'information constituent les deux catalyseurs principaux des changements majeurs survenant dans le système électrique, notamment dans les réseaux de distribution.

Ce mémoire a pour objectif de traiter plusieurs questions relatives aux futurs modèles d'affaires dans les réseaux électriques et leurs choix d'investissement face aux incertitudes liées à l'émergence et à l'insertion des 'smart technologies' (comptage avancé, gestion active de la demande, effacements diffus, stockage diffus, nouveaux outils de conduite des réseaux...), ainsi suite à cette émergence induisent de nouvelles vulnérabilités d'où une étude sur la sécurité et nécessaire.

La thématique des « réseaux et systèmes électriques intelligents » est identifiée dans de nombreux pays comme un axe prioritaire de recherche et de démonstration, les exemples de déploiement massif étant traités au chapitre I où on a vu que le nombre de projets en ce domaine est en constante augmentation de par le monde, selon le contexte et le pays.

Suite au développement des smart grids apparaît de nouveaux services et acteurs, ce développement représente une opportunité d'affaire considérable pour l'industrie électrique. Comme l'ont exposés au chapitre 2 ; l'industrie électrique, celle des TIC, du bâtiment et le grand public vont connaître un développement majeur. Ainsi, l'apparition de nouveaux métiers dans la distribution d'énergie telle que l'agrégateur pour agréger des effacements diffus, le stockage pour garantir l'équilibre et réduire les pics de consommation, activités de conseils, enfin le parc véhicules électriques pour la gestion des batteries des véhicules électriques afin d'équilibrer le système dans les grandes métropoles.

Dans le chapitre 3, nous avons souligné l'importance d'une étude technico-économique pour une meilleure connaissance de la structure des coûts et des gains de chacune des catégories d'acteurs afin de garantir un optimum technico-économique pour l'ensemble du système. Nous avons pu valoriser à l'aide de la méthode Analyse Coûts-Bénéfices (ACB), les gains apportés par le déploiement des compteurs intelligents, cela à l'aide d'un modèle calcul techno-économique sur implémentés sous Matlab. Il en ressort de

Conclusion générale

remarquer des gains en investissement pour une période donnée grâce aux coûts amortis par les compteurs déjà installés.

Un des aspects de cette révolution est l'arrivée de plus en plus rapide des technologies de l'information et des télécommunications dans les réseaux d'énergie. Cette insertion massive des TIC crée une vulnérabilité relative sur les systèmes obtenus qui doit être gérée dans le cadre du développement de la sécurité informatique. Cette problématique déjà prise en charge par plusieurs firmes dont IBM, Google et Sisco. Ceci constitue un domaine auxiliaire dans la R&D des smart grid. Parmi ceux-ci, les problèmes liés à la confidentialité des données sont ceux auxquels nous nous sommes intéressés au chapitre 4. En effet, les systèmes supportant le développement des réseaux intelligents sont de plus en plus complexes et interconnectés nécessitant pour leur gestion l'échange d'une quantité importante de données. Ce phénomène est amplifié par l'automatisation croissante des systèmes de production et de gestion. Cette dépendance doit surmonter un défi majeur : la sécurité et la protection des données.

Dans notre travail un intérêt particulier a été accordé aux compteurs communicants, car ils constituent le maillon fort des réseaux intelligents, leur intégration dans les réseaux actuels a un impact immédiat sur le volé financier du distributeur. Relativement à la sécurité informatique, sont jugés préoccupants en raison des possibles atteintes à la vie privée et la confidentialité des données échangées. La mise en œuvre de ces compteurs, constitue une étape essentielle du développement de la nouvelle intelligence des réseaux. Leur généralisation est donc attendue.

Nous proposons comme perspective une étude complète sur la sécurité des systèmes SCADA, ces derniers présentent des vulnérabilités aux niveaux des points d'accès des réseaux de communication.

Une autre perspective de ce travail serait une étude sur les critères économiques à l'avenir incertain pour le déploiement de ces technologies intelligentes.

Bibliographie

Bibliographies

- [1] «Smart Grid Cyber Security Market», According to Pike Research: Business Wire - 21/06/10<http://redirectix.bulletins electroniques.com/X59Ou>.
- [2] "15% of Smart Grid Spending Will Be On Cyber Security": Sustainable Business 28/06/10 - <http://redirectix.bulletins-electroniques.com/eSowm>.
- [3] Julien Monereau «Les réseaux électriques du futur une première approche » Juin 2011.
- [4] Mark Twain LIVRE BLANC « des industriels au service de l'intelligence énergétique ».
- [5] Fairouz Iberraken, Rabah Medjoudj, Djamil Aissani et Klaus Dieter Haim « Les aspects décisionnels des projets Smart Grids basés sur le processus d'analyse de la hiérarchie (AHP) »
- [6] Feuille de route sur les réseaux et systèmes électriques intelligents intégrant les énergies renouvelables (<http://www-anr-pv.cea.fr/home/liblocal/docs/Seminaire2007/MULTISOL.pdf>).
- [7] Fairouz Iberraken, Rabah Medjoudj, Djamil Aissani et Klaus Dieter Haim « Les aspects décisionnels des projets Smart Grids basés sur le processus d'analyse de la hiérarchie (AHP) »
- [8] institut de Montaigne « Pour des réseaux électriques intelligents » rapport février 2012.
- [9] Julien Monereau « Les smart grid, les réseaux électriques du futur », adec technopole , version 2- Juin 2011
- [10] « La chaîne de valeur du marché des smart grids », Juin 2012 hrannou@items-int.eu.
- [11] Commission de Régulation d'Electricité de France CRE, Modèles économiques, septembre 2011.
- [12] D, Publication, « Smart Grid - Activities in Canada » Centre de recherche de Varennes, CTEC Number 2010-087 / 2010-05-27.
- [13] Michael Porter, « L'avantage concurrentiel », 1986.
- [14] ITEMS International, « La chaîne de valeurs du marché des smart Grids », Capenergies-SCS, Jun 2012.
- [15] Dalkia « L'agrégateur un nouveau métier pour le marché d'électricité » <http://www.smartgrids-cre.fr>
- [16] Advisory Meeting «E-Energy German Smart Grid Projects Overview EPRI Smart Grid Demonstration» June 2010 Paris/EDF
- [17] A. N. Brooks. «Vehicle-to-grid demonstration project: Grid regulation ancillary service with a battery electric vehicle». 2002.

Bibliographie

- [18] K. A. Corzine C. Hutson, G. K. Venayagamoorthy, «Intelligent scheduling of hybrid and electric vehicle storage capacity in a parking lot for profit maximization in grid power transactions». Missouri unibversity 2008.
- [19] K. Corzine C. Huston G. K. Venayagamoorthy, «Mitra. Real-time modeling of distributed plug-in vehicles for v2g transactions». 2009.
- [20] G. K. Venayagamoorthy A. Y. Saber. «Intelligent unit commitment with vehicle-to-grid a cost-emission optimization». Journal of Power Sources, 2009.
- [21] Nourai A., « Installation of the First Distributed Energy Storage System (DESS) at American Electric Power (AEP) », Sandia National Laboratories, SAND2007-3580, 2007.
- [22] Monnot E., Malarange G., « The future ancillary services provided by DG », livrable FENIX WP1/Task 1.1, Contrat n°SES6-518272, 2006.
- [23] Duval J., « Contribution de la production décentralisée à la reconstitution du réseau après black-out », EDF R&D H-R12-2007-01328, 2007.
- [24] Courtecuisse V., El Mokadem M., Robyns B., François B., Petit M., Deuse J., « Supervision par logique floue d'un système éolien à vitesse variable en vue de contribuer au réglage primaire de fréquence », *Revue Internationale de Génie Electrique*, Hermès, n°4-5, pp. 423-453, 2008.
- [25] Bouchala et Brahimi «Aspect technique des smart grids» en 2013.
- [26] Valérie Meunier et Eric Mardsen « guide méthodologique ICSI», 2009.
- [27] Medjoudj Rabah, « calcul et évaluation de la fiabilité d'un réseau électrique urbain », 14 Décembre 1994. Bejaia.
- [28] Rabah Medjoudj, Djamil Aissani et Klaus Dieter Haim « Power customer satisfaction and profitability analysis using multi-criteria decision making methods» en 2013.
- [29] Draft smart grid cyber security strategy and requirements, NIST IR7628, Sep. 2009 [Online].
- [30] KIM PAANANEN «Information security smart grid demonstration environmeny», Master of Science Thesis, Tampere University of Technology, Tampere, Finland February 2012.
- [31] Bernard Cousin, « Sécurité des réseaux informatiques », Université de Rennes 1, 2003
- [32] Yilin Mo, Tiffany Hyun-Jin Kim, «Cyber-Physical Security of a Smart Grid Infrastructure», Invited Paper, Jun 2010.
- [33] Eric Papet « Analyse de risque avec la méthode MEHARI », e.papet@dev1-0.com.

Bibliographie

- [34] Club de la Sécurité des Systèmes d'Information Français.
- [35] CRE « Rapport d'Audit sur la sécurité de la vie privée suite à l'utilisation des données issues des compteurs Linky », Avril 2012.
- [36] Olivier ROCHON chef produits segments Commercial et Industriel Technique de l'ingénieur, « Communications dans les comptages d'électricité ». 10/02/2007
- [37] François Laissus, « Cours d'introduction à TCP/IP », Version du 25 février 2009.
- [38] franck david, « Fonctionnement des PKI », Cabinet de Consultants en Sécurité informatique, Franck.Davy@hsc.fr
- [39] Diffie W. ET Hellman M. « E. – New directions in cryptography. IEEE Trans. Inform. Theory», vol. IT-22, Nov 1976, pp. 644–654.