Demande d'approbation du Projet de Lecture à Distance, Phase I d'Hydro-Québec Distribution

Dossier R-3770-2011

Mémoire du RNCREQ

Présenté à la Régie de l'énergie

26 octobre 2011

Rédaction

Christian Martel, analyste, Centre Hélios

Philip Raphals, expert-conseil, Centre Hélios

Collaboration

Me Annie Gariépy, avocate

Philippe Bourke, directeur général Regroupement national des conseils régionaux de l'environnement du Québec

Cédric Chaperon, chargé de projet en énergie et changements climatiques, Regroupement national des conseils régionaux de l'environnement du Québec

Table des matières

1) Préambule....4

1.1) Présentation du RNCREQ....4

1.2) Structure du document....5

2) Enjeux....5

2.1) L'importance d'une vision d'ensemble....5

2.2) Risques....10

2.2.1) Risques reliés à la maturité technologique....10

2.2.2) Risques reliés à l'évolution des normes....12

2.2.3) Risques reliés à l'espérance de vie des composantes de l'IMA....13

2.2.4) Risques reliés à la sécurité....15

3) Les analyses économiques....18

3.1) Les analyses de l'Union de consommateurs....18

3.2) Analyse économique et financière du Projet LAD....19

3.2.1) Comparaison entre le Scénario IMA et le Scénario de référence....19

3.2.2) Analyse du Scénario IMA....20

3.2.3) Analyse du Scénario de référence....20

3.2.4) Comparaison des scénarios....23

3.2.5) Impact tarifaire du Projet LAD....24

3.3) Analyse financière et économique du Projet R-3770....28

4) Conclusions....28

4.1) Le Projet R-3770....28

4.2) La mise en place d'un réseau intelligent....30

ANNEXES

1) Préambule

Ce document constitue la preuve écrite du RNCREQ dans le dossier R-3770-2011.

1.1) Présentation du RNCREQ

Les seize (16) conseils régionaux de l'environnement (CRE) interviennent en faveur de la protection et de l'amélioration de l'environnement à l'échelle de chacune des régions administratives du Québec. Par leurs actions, ils cherchent à favoriser l'intégration des préoccupations environnementales dans les processus de développement régional.

Pour eux, ce développement doit se faire dans le respect de la capacité de support des écosystèmes. C'est une condition essentielle au développement durable.

Les CRE sont des organismes autonomes, issus du milieu, reconnus comme interlocuteurs privilégiés du Gouvernement sur les questions environnementales. Ils regroupent un nombre croissant de membres d'horizons divers poursuivant des objectifs communs. Ce réseau unique constitue un acteur influent dans le domaine de l'environnement au Québec.

En tenant compte des réalités locales et régionales, les CRE privilégient l'action, la concertation, l'éducation, l'information, la sensibilisation et la veille environnementale, pour atteindre leurs objectifs. Ils défendent des valeurs fondamentales comme la solidarité, l'équité et le respect.

Fondé en 1991, le Regroupement national des conseils régionaux de l'environnement du Québec (RNCREQ) a quant à lui pour mission de contribuer au développement et à la promotion d'une vision nationale du développement durable au Québec, de représenter l'ensemble des CRE et d'émettre des opinions publiques en leur nom. Le RNCREQ œuvre dans la plupart des grands dossiers environnementaux (changements climatiques, matières résiduelles, gestion de l'eau, énergie, forêts, agriculture, etc.).

En regroupant et représentant l'ensemble des régions du Québec, le RNCREQ facilite les échanges d'expertise entre les régions, assure la diffusion de la vision particulière des CRE et encadre les relations avec les intervenants politiques, sociaux, économiques et environnementaux au niveau national.

Comme en témoigne leur mission, les CRE se sentent interpellés de multiples façons dans la mise en œuvre du développement durable par le gouvernement du Québec. Rappelons en outre que dans le cadre de l'entente de partenariat formel qu'il a conclue avec les CRE depuis bientôt 15 ans : «*le gouvernement du Québec reconnaît que les Conseils régionaux de l'environnement ont le mandat de contribuer au développement d'une vision régionale de l'environnement et du développement durable et de* ***favoriser la concertation de l'ensemble***

des intervenants régionaux en ces matières».

«*La ministre du Développement durable, de l'Environnement et des Parcs reconnaît les CRE comme* ***interlocuteurs privilégiés du gouvernement du Québec en région pour la concertation en matière d'environnement et de développement durable*****».**

1.2) Structure du document

Dans la section 2, nous introduisons certains enjeux soulevés par le présent dossier.

Dans la section 3, nous regardons les analyses économiques présentées par le Distributeur au soutien de sa demande.

Dans la section 4, nous présentons une discussion et des conclusions.

2) Enjeux

Le RNCREQ considère important d'analyser les différents aspects et enjeux soulevé par ce projet.

2.1) L'importance d'une vision d'ensemble

Comme nous allons le voir, il existe un important consensus à l'effet que les entreprises de services publics qui développent d'abord une vision d'ensemble de leurs attentes et objectifs réussissent mieux l'implantation des IMA, comparativement aux entreprises qui vont de l'avant, à la pièce, sans axes directeurs basés sur une telle vision.

Par exemple, le consultant McKinsey & Co. a publié en 2010 une synthèse des enjeux principaux reliés au déploiement de réseaux électriques interactifs – intelligents, sous le titre, « McKinsey on Smart Grid »[1]. Il explique que la technologie est encore jeune, au point où, en 2010, aucun système d'IMA à fonctionnalité complète n'avait encore été déployé à échelle aux États-Unis :

> The course of worldwide smart grid adoption has been halting and complex, with progress varying from country to country. Underlying technologies remain expensive, and the smart grid business case assumes significant changes in customer behavior. A business model is emerging, especially for customer applications, while regulators, utilities, and third-party service providers define their roles and set technology standards.

[1] McKinsey on Smart Grid Summer 2010, http://www.mckinsey.com/en/Client_Service/Electric_Power_and_Natural_Gas/Latest_thinking/ McKinsey_on_Smart_Grid.aspx.

> Many core systems remain unproven, and as we go to press, not a single full-feature AMI system has been stably and fully deployed in the United States at scale.

Il reconnaît que les incertitudes sont importantes, avec des risques importants d'erreurs :

> The smart grid is facing the near-term disruptions characteristic of the introduction of any truly transformative technology. For the actors in the electric power industry, the course forward is uncertain, and the likelihood of early missteps is high.

Cela dit, il ne recommande pas de simplement attendre, mais plutôt d'apprendre des expériences des autres pour maximiser les bénéfices et minimiser les risques.

Un des chapitres-clés de l'étude de McKinsey s'intitule « Best practices in the deployment of smart grid technologies ». Ce chapitre commence en soulignant le danger qui accompagne la mise en place des systèmes IMA/compteurs intelligents :

> The first stage of deployment of a smart grid rollout is generally in the deployment of smart meter technology. Here the record of utility companies has been mixed — unsurprising given the level of complexity involved. Some utilities have had to interrupt their rollout of smart meters to reassess the technology selected, and some have switched vendors. Still others have incurred hundreds of millions of dollars in cost overruns due to systems integration issues. And some utilities have failed to realize the expected benefits from smart meter projects because of change-management issues. [2] (Nos soulignés)

L'étude présente ensuite un tableau de « meilleurs et pires pratiques », reproduit ci-dessous.

Exhibit 1

The do's and don'ts of smart grid deployment

Where to do it	What to do – 10 best practices	What not to do
Vision and business case	**1** Define a smart grid vision and the road map to get there **2** Build a compelling business case tailored to technology maturity and the regulatory environment **3** Develop a capability-driven regulatory case articulating stakeholder costs and benefits, and addressing technology obsolescence and security concerns	• Pursue stand-alone projects when each becomes a positive business case • Assume technology is a static choice and business-case framework of one service area will work in another • Translate internal business case into a regulatory filing and assume regulators and stakeholders will understand it
Implementation	**4** Set up program architecture that considers risk and industry maturity **5** Select technologies for the long term and use pilots strategically **6** Pursue true strategic sourcing to optimize providers capabilities while minimizing risk **7** Maintain significant business focus on IT integration activities	• Assume a narrow approach to systems integration will succeed • Map technology to current needs or fail to test technology marketing claims • Use a procurement-led process that fits other categories of spend where functionality is well known • Assume clear business requirements will lead to successful IT integration
Operations and change management	**8** Employ lean operations techniques to accelerate cost-effective technology deployment **9** Actively define end-state business processes and change required to deliver **10** Set up cross-functional governance across all key business units	• Scale up current capabilities and assume an unrealistic learning curve • Plan on capturing the benefits in the business case without significant change management • Lead the project from either an IT or single business unit perspective

[2] Best practices in the deployment of smart grid technologies , Anjan Asthana, Adrian Booth, and Jason Green , p. 24-25.

La première recommandation formulée par McKinley est donc de définir d'abord une vision du réseau intelligent et le chemin pour y arriver (« *Define a smart grid vision and the road map to get there* »). Il compare les bénéfices de cette approche gagnante avec la poursuite de projets indépendants, où chacun doit présenter sa justification financière individuellement (« *Pursue stand-alone projects when each becomes a positive business case* »)[3].

Cette deuxième approche (« *What not to do* : Pursue stand-alone projects when each becomes a positive business case») décrit précisément celle retenue par le Distributeur :

> « *Chaque nouvelle fonctionnalité qui répond à un besoin réel du Distributeur ou de ses clients fera l'objet d'un examen spécifique dans lequel les bénéfices et les coûts d'implantation seront analysés. Une demande d'autorisation distincte, lorsque requise, sera présentée à la Régie* ».[4]

Par ailleurs, le projet de LAD du Distributeur présente plusieurs des aspects identifiés par ces experts comme étant importants à éviter :

- Des éléments du Réseau intelligent seront introduits à la pièce, à mesure que cela peut se justifier financièrement;
- L'hypothèse que les compteurs, routeurs et collecteurs ne soient pas remplacés avant 15 ans présuppose que le rythme d'avancement technologique ralentira beaucoup;
- Le Projet reporte à plus tard l'intégration de l'IMA et des nouveaux compteurs aux différentes fonctionnalités du réseau intelligent;

McKinley n'est pas le seul à souligner l'importance d'une planification globale avant de déployer l'implantation d'un réseau « intelligent ».

Dans une revue électronique de l'industrie, *Smart Grid News,* la firme Accenture, qui est par ailleurs la firme retenue par le Distributeur pour l'accompagner dans son Projet LAD, présente une série de brefs articles synthétiques qui exposent les points saillants de projets de réseaux intelligents[5]. De l'avis du RNCREQ, ces points saillants sont des applications pertinentes au projet présenté par le Distributeur.

Dans un de ces articles, un directeur senior d'Accenture, Michael Burck, insiste sur l'importance d'un *roadmap,* dans le titre même se son article : *Start with a Fully Baked Smart Grid Roadmap and Then Develop Your Data Management Framework*[6]. Ce titre fait référence à un vieil idiome de la langue anglaise, *half-baked*, défini par Merriam-Webster comme suit :

---

[3] Ibid.

[4] HQD-1, doc. 1, p. 18.

[5] http://www.smartgridnews.com/artman/publish/Accenture-smart-grid/

[6] *Start with a Fully Baked Smart Grid Roadmap and Then Develop Your Data Management Framework*, Michael Burck, 2010.jun,, Smart Grid News, http://www.smartgridnews.com/artman/publish/Business_Strategy/First-Things-First-Start-with-a-Fully-Baked-Smart-Grid-Roadmap-and-Then-Develop-Your-Data-Management-Framework-2443.html

> ***Half-baked***
>
> ***a*** **:** *poorly developed or carried out <a half–baked idea> <half–baked research>*
>
> ***b :*** *lacking adequate planning or forethought <a half–baked scheme for getting rich>*
>
> ***c :*** *lacking in judgment, intelligence, or common sense*

Ainsi, il met en garde contre la tentation d'aller de l'avant avec un projet qui est « *half-baked* », c'est-à-dire sans une planification adéquate. Il écrit :

> « *Developing a successful framework for smart grid data management starts with a roadmap which establishes an effective, cost-efficient approach toward smart grid implementation. ...*
>
> *At each stage of developing the Smart Grid data framework, it's important to provide a link to the company's Smart Grid vision and identified business values to achieve both internal and external stakeholder alignment.* » (Nos soulignés)

Comparons l'approche du Distributeur avec celui de Southern California Edison (SCE), un des leaders nord-américains dans le domaine. Déjà en 2007, SCE avait développé un *Smart Grid Roadmap,* qui a été mis à jour périodiquement, sous sa direction Advanced Technology. La version la plus récente articule comme suit la *value proposition* de son plan de Réseau intelligent[7] :

> **1.3. Smart Grid Value Proposition**
>
> Key objectives of SCE's smart grid development strategy include pursuit of technologies that provide significant customer value that exceeds the cost of implementation, as well as identifying best fit solutions to meet policy objectives that may not have direct operational benefits. Smart grid technology projects will likely involve a mix of both incremental and replacement investments that not only expand existing capabilities, but also build new capabilities.
>
> reducing greenhouse gas emissions and increasing grid security, safety and reliability. These benefits are often difficult to quantify, may vary widely in their justification of various smart grid technologies, and are multi-faceted in terms of who receives benefits from them. Benefits may not only accrue to SCE customers, but also to California residents or our broader society. In addition, these benefits need to be considered within the context of the portfolio of smart grid technologies to be deployed at different times over the next twenty years and beyond.

[7] Southern California Edison, Smart Grid Strategy & Roadmap, pages 7-8.

> Although SCE believes in taking a cost-effective approach to the deployment of smart grid technologies and systems, traditional cost/benefit models may not account for all of the value to be derived from smart grid investment decisions. A substantial portion of smart grid benefits are societal in nature and include achieving national and state priorities such as energy independence,

Ainsi, SCE a identifié dix catégories de bénéfices de son réseau intelligent :

1. ***Provide Customer Benefits*** by improving grid reliability, enhancing customer communications, and by empowering customers to better manage their energy usage and costs.
2. ***Reduce Peak Demand*** through demand management programs and services.
3. ***Increase Energy Conservation & Efficiency*** by enabling integration of customer energy management systems and grid energy management systems; this integration can reduce system losses.
4. ***Reduce Operating Expenses*** by lowering the cost of planning and support functions, operating costs and energy costs.
5. ***Avoid, Reduce or Defer Capital Investments*** by increasing capacity utilization, extending the useful lives of grid assets, optimizing energy procurement practices, and investigating new technologies.
6. ***Increase Utility Worker Safety*** by providing tools and information that allow them to perform their work in a safer manner.
7. ***Improve Grid Resiliency and Reliability*** by reducing the frequency and duration of outages and service interruptions, and by improving power quality, accommodating greater diversity of energy resources, and increasing grid security.
8. ***Reduce Greenhouse Gas Emissions*** by integrating renewable energy resources with the electric delivery system, and promoting the adoption of electric vehicles.
9. ***Promote Energy Independence*** by facilitating electricity-based transportation.
10. ***Promote Economic Growth & Productivity*** by fostering the development of California's clean technology economy, and associated job growth.

La mise en place d'un réseau intelligent créerait en réalité une multiplicité des bénéfices reliés à l'efficacité énergétique, comme le démontre le tableau suivant, tiré de l'étude de McKinley mentionné ci-dessus[8] :

[8] McKinley on Smart Grid, Smart Grid and the Promise of Demand-Side Management, p. 41.

Exhibit 2

Successful demand-side management

Successful DSM optimizes multiple design options across 6 levers

DSM lever	Design options	Description
Rates	• Flat rate • Critical peak pricing (CPP) • Time of use (TOU) • Real-time pricing (RTP) • Interverted block pricing	• Same rate at all times • Extremely high rates during critical peaks • Variable pricing for prescheduled blocks of time • Variable pricing at all times, informed close to instantaneously • Increase rate for higher use customers
Incentives	• No incentives • Provide rebates on bill • Provide cash compensation	• Base case • Debit bill based on degree of behavior change • Provide separate check to encourage behavior change
Information	• None • Event notification • Real time usage • Historical usage • Comparative usage • Device-specific usage • Billing usage	• Monthly paper bills and consumption information • Notification of DR events under way • Consumption at a given moment (e.g., kW, light bulb equivalents) • Consumption compared to previous period of time • Consumption compared against last month's or peers' • Individual device usage in real time; can be paired with above • Real-time billing information
Controls	• None • Programmable communicating thermostats (PCTs) • Smart appliances/plugs • Home energy controller • PHEV smart chargers • DG/S control devices	• No automation of devices to reduce energy consumption • Automated AC control • Automated appliance on/off • Centralized control & automation of major home appliances • Optimized charging of PHEVs • Optimized usage, storage, and later discharging of energy
Education	• No education • Educate by segment • Educate by channel • Educate by positioning	• Base case • Vary by income, consumption behavior, attitudes • Use various means: e-mail, bill inserts, newspaper, etc. • Emphasize different HAN benefits (reduced energy costs and carbon emissions, increased competition with neighbors, etc.)
Customer Insight and verification	• None • Verification of benefits capture	• Base case • Verify DSM (EE, EC, and DR) and economic utility captured by customers

Ainsi, la mise en place d'une vision globale permet une réflexion approfondie sur les coûts et bénéfices réels, sans se limiter artificiellement à des gains associés à la réduction de la main d'œuvre reliée à la relève de compteurs. Il permet également une consultation large, tant à l'intérieur qu'à l'extérieur de la compagnie, sur les objectifs visés, sur la meilleure architecture à mettre en place, et sur les bénéfices éventuels, non seulement pour sa clientèle, mais pour la société en général.

2.2) Risques

2.2.1) Risques reliés à la maturité technologique

La notion de *Maturité technologique* est primordiale car des choix technologiques et des orientations stratégiques s'y rattachent. En outre, il est essentiel de la prendre en considération dans un cadre de planification à court à long terme.

Une technologie peut être jugée mature si elle rencontre les critères suivants :

1. La technologie est en utilisation depuis assez longtemps pour que les problèmes rencontrés aient été éliminés ou réduit à niveau acceptable;
2. La technologie est utilisée à grand déploiement;
3. La technologie est facile à utiliser par les usagers, pas seulement par les experts;
4. Il y a une réduction marquée du nombre de nouveaux brevets et du développement de la technologie;
5. Les avancées au niveau d'une technologie mature sont essentiellement incrémentale et

se limitent en général à de simples améliorations;

6. Les normes sont développées, et si les normes sont matures, elles aussi changent de façon incrémentale, avec des améliorations, mais sans changements majeurs
7. Les prix de la technologie ne baisse plus de façon importante d'année en année;
8. Une technologie, dite mature, a une facilité d'intégration de ses éléments et composantes dans un ensemble ou système dans lequel cette technologie est utilisée.
9. Voici un exemple d'index qualificatif du niveau de maturité basé sur la facilité d'intégration [9]:

Integration Readiness Level

A systematic measurement of the interfacing of compatible interactions for various technologies and the consistent comparison of the maturity between integration points.

Integration – the combining and coordinating of separate components into a seamless unit – interfacing the compatible interactions of various technologies together

	IRL	Definition
Pragmatic	9	Integration is **Mission Proven** through successful mission operations.
	8	Actual integration completed and **Mission Qualified** through test and demonstration, in the system environment.
Syntactic	7	The integration of technologies has been **Verified and Validated** with sufficient detail to be actionable.
	6	The integrating technologies can **Accept, Translate, and Structure Information** for its intended application.
	5	There is sufficient **Control** between technologies necessary to establish, manage, and terminate the integration.
	4	There is sufficient detail in the **Quality and Assurance** of the integration between technologies.
Semantic	3	There is **Compatibility** (i.e. common language) between technologies to orderly and efficiently integrate and interact.
	2	There is some level of specificity to characterize the **Interaction** (i.e. ability to influence) between technologies through their interface.
	1	An **Interface** between technologies has been identified with sufficient detail to allow characterization of the relationship.

où on veut être, dans la mesure du possible, au niveau *pragmatique*.

Plus les choix sont faits tôt dans le développement d'une technologie, plus les risques sont importants :

- difficultés de justifications financières;
- gestion de retards suite aux problèmes des premiers modèles, bogues informatiques des composantes progiciels, etc.;
- dépassement de coûts liés aux problèmes;
- coûts élevés des premières unités.

Dans la présente demande, le Distributeur propose d'installer des compteurs comportant

[9] Gove, R. (2007) Development of an Integration Ontology for Systems Operational Effectiveness. M.S. Thesis. Stevens Institute of Technology et Wikipedia – Mature Technology.

plusieurs technologies que le Distributeur n'a pas l'intention d'utiliser immédiatement. Par exemple, les compteurs incluent des cartes *Zigbee* pour un *Home Area Network,* que le Distributeur n'entend pas activer dans la Phase 1 du présent dossier[10]. Or, le RNCREQ considère qu'il y a un risque réel que, lorsque le Distributeur décidera éventuellement d'implanter des fonctionnalités qui feront appel à cette carte *Zigbee*, elle risque d'être déjà vétuste au niveau du matériel.

Comme nous l'avons vu, étant donné la complexité des systèmes impliqués, une vision globale est essentielle pour que l'implantation d'un réseau intelligent soit couronnée de succès. Le choix de procéder sans établir une telle vision augmente inévitablement les risques reliés à la maturité des technologies en question.

2.2.2) Risques reliés à l'évolution des normes

L'EPRI (*Electric Power Research Institute)* a publié en octobre 2010 un *Smart Grid Executive Summary,* lequel sert un avertissement qui s'applique de façon fort pertinente au choix du Distributeur dans la présente demande :

The Risks

As with any innovation, smart grid investments carry certain risks. Smart grid functional requirements, interoperability and cybersecurity standards are still evolving, and premature technology obsolescence could strand some investments even as transitional technologies need to be replaced before their expected end-of-life. This could become necessary when such technologies become incompatible with adopted standards or cannot meet future requirements for smart grid functionality.

(nos emphases)

L'étude de McKinley, dont on a fait état précédemment, note aussi :

> Do technology choices take into account the long-term priorities set out in the road map? Just as streaming video necessitated significant upgrades to communications networks, future smart grid applications will require greater capabilities, such as low latency for critical grid applications or high bandwidth for interactive customer applications. (nos emphases)

Ce dernier paragraphe suggère que certaines fonctionnalités qui feront partie d'une étape ultérieure de l'implantation d'un réseau intelligent peuvent exiger des caractéristiques qui ne font pas partie des spécifications choisies à l'origine. Par exemple, pour les fonctionnalités qui touchent le comportement du réseau lui-même, la vitesse de réaction est primordiale.

Par ailleurs, ils notent :

[10] HQD-4, doc. 2, p. 12, R. 9a).

> *The NIST smart grid working group has not yet established all the needed standards for smart meters and other smart grid programs.*

Il y a donc un risque de devoir modifier l'infrastructure choisie, une fois les normes pertinentes établies.

2.2.3) Risques reliés à l'espérance de vie des composantes de l'IMA

Comme nous allons le voir dans l'analyse économique à la section 3, l'espérance de vie des composantes de l'IMA est un enjeu majeur dans la rentabilité du Projet LAD.

Dans le Tableau B-4[11] de sa demande, le Distributeur présente les périodes d'amortissement proposées des actifs :

TABLEAU B-4 : DURÉE D'AMORTISSEMENT DES ACTIFS

ACTIFS	DURÉE D'AMORTISSEMENT
Compteurs	15 ans
Poteaux	40 ans
MDMS	5 ans
Frontal d'acquisition	5 ans
Collecteurs	15 ans
Routeurs	15 ans

Il est important de noter que si la période d'amortissement du *MDMS* et du *Frontal d'acquisition* a été prudemment fixée à 5 ans, le Distributeur attribue une période d'amortissement de quinze (15) ans aux *Compteurs*, *Routeurs* et *Collecteurs.* Il justifie cette période d'amortissement en faisant référence à un document préparé par Accenture, *AMI Business Case Research : Smart Meter life expectancy in North America,* qui à son tour fait référence aux périodes d'amortissement appliquées par cinq entités nord-américaines[12]. Un des documents cités, celui de Southern California Edison précise que :

> The generally-accepted lifespan for solid state meters and meters with electronic components is fifteen years, compared to the industry-average lifespan of thirty years for mechanical meters …[13]

Or, le RNCREQ ne conteste pas le fait qu'un compteur électronique aurait normalement une durée de vie fonctionnelle de quinze ans. Cela ne veut pas dire, cependant, que le Distributeur

---

11 *Tableau B-4 : Analyse de risque et mesures de mitigation*, HQD-1, Doc-1, page 58 de 58

12 HQD-2, doc. 1, Annexe A, en liasse.

13 Ibid., p. 6.

ne verra pas la nécessité de les remplacer plus tôt pour des raisons d'obsolescence technologique.

Il est important de reconnaître que le choix d'appliquer une durée de vie de 5 ans pour les actifs informatiques qui sont au cœur du MDMS et du frontal ne veut pas dire qu'après cinq ans ils ne fonctionneront plus. Ce choix vient plutôt de la reconnaissance que, dû à l'évolution technologique, il sera probablement pertinent de les remplacer avec celle d'une nouvelle génération qui n'existe pas encore. Il s'agit d'un raisonnement tout à fait standard pour les actifs d'informatiques, qui devront normalement être remplacés tous les cinq ans environ, considérant la vitesse de l'évolution technologique.

Dans l'éventualité où il faudrait remplacer les logiciels chaque cinq ans, l'utilisation d'une durée de vie de 15 ans pour les compteurs, routeurs et collecteurs dépend inévitablement de l'hypothèse que ces appareils, qui contiennent aussi des éléments informatiques, seront en mesure de supporter les prochaines trois générations d'applications. Cela n'est pas une évidence. Un ordinateur Pentium II acheté en 1998 peut très bien être fonctionnel aujourd'hui, mais il ne pourra jamais supporter les logiciels de cryptage/décryptage qui sont essentiels pour l'opération des réseaux WiFi d'aujourd'hui.

Ainsi, la validité de cette hypothèse ne peut être connue avec certitude. Le très fort coût qui accompagnerait le remplacement de ces actifs avant la fin de leur durée de vie physique aurait des répercussions majeures sur la rentabilité du Projet, comme nous le verrons dans la section 2.2) .

Le Distributeur n'ayant pas encore procédé à l'exercice de la planification de ses besoins pour la gestion de son réseau *Smart Grid*, il ne peut démontrer que les équipements choisis en 2011 auront la capacité de satisfaire ses besoins dans 5 ou 10 ans. La capacité de pouvoir faire des mises à niveau du *firmware* des compteurs, routeurs et collecteurs n'est pas une confirmation que le matériel aura la capacité de supporter les applications qui correspondront au besoins du Distributeur dans 5 ou 10 années.

Historiquement, le coût du GFLOP, la capacité d'un ordinateur de faire un milliard de calculs par seconde, à chuté de façon exponentielle. Le GFLOP est une mesure de capacité informatique et la chute de son coût reflète l'évolution technologique. C'est cette évolution technologique qui motive le changement des actifs informatique plus fréquemment que dans le cas d'une technologie mature.

Date	Approximate cost per GFLOPS
1961	US $1,100,000,000,000 ($1.1 trillion)
1984	$15,000,000
1997	$30,000
April 2000	$1,000
May 2000	$640
August 2003	$82
August 2007	$48
March 2011	$1.80

Il n'existe aucune raison de croire que cette évolution tire à sa fin. Si la puissance des appareils informatisés continue d'augmenter, les exigences des logiciels augmenteront inévitablement aussi, ce qui crée la possibilité — aucunement évaluée dans la preuve du Distributeur — qu'il pourrait être appelé à remplacer les compteurs qui sont au cœur du Projet bien avant la fin de leur vie utile.

2.2.4) Risques reliés à la sécurité

Au Tableau 9[14] de sa demande, le Distributeur présente les *risques* identifiés et les *mesures de mitigation* proposés, dont ceux qui s'appliquent à la *sécurité des TI et de télécommunication* :

Sécurité des TI et de télécommunication	Respect des normes propres à ce domaine d'activité, dont le chiffrement des données, le contrôle des accès, la signature des commandes, la journalisation des évènements, la surveillance du réseau, la redondance, etc.

Or, cette simple formulation ne représente aucunement l'ampleur de la question de la sécurité dans les IMA.

Une présentation entitulé, *The Four Layers of Smart Grid Security*[15], par Ernie Hayden de Verizon (mai 2011) présente les bien différents aspects de cet enjeu. La présentation est reproduite comme Annexe B.

D'abord, la présentation mentionne l'inquiétude quant à la sécurité d'un réseau interactif-intelligent de la part de plusieurs agences gouvernementales américaines, notamment National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Energy (DOE), Federal Energy Regulatory Commission (FERC), et Government Accountability Office (GAO).

Tel que présenté par Verizon, la sécurité d'un réseau interactif-intelligent comporte quatre couches : la protection physique, la cybersécurité, la protection de l'information privée, et, la gestion et stockage de données.

La protection physique signifie la protection contre le vandalisme, le vol, les modifications, l'injection de *virus,* ou encore la modification du cryptage ou de l'authentification. La protection physique n'inclut pas des dommages accidentel, mais inclut la météo, les tempêtes solaires, les volcans, les tremblements de terre, ainsi que les inondations.

La cybersécurité est le niveau où il y a le plus de vulnérabilités. L'accroissement de la complexité y contribue grandement. La protection se fait par des détecteurs intelligents et des technologies de communications avancées. Cette couche inclut les liens de communications d'un IMA dont le HAN, le NAN (qu'il soit de type RF ou PLC—la communication avec les fils électriques eux-mêmes), ou le WAN. Les réseaux WAN ont tendance à être une agrégation de segments, parfois privés, parfois publique. Aussi, les segments de WAN peuvent être de différente technologie. Par exemple, un segment d'un WAN pourrait être de la fibre optique et le prochain segment un câble coaxial. Dans le cas du WAN, pour les segments qui passent par les réseaux publiques, les attaques sont plus probable, mais cela n'exclut pas les attaques sur les segments privés.

La nature des attaques du type cybersécurité peuvent être sur la protection des informations

---

[14] *Tableau 9 : Analyse de risque et mesures de mitigation*, HQD-1, Doc-1, page 43 de 58

[15] www.us-cert.gov/control_systems/icsjwg/presentations/spring2011/ag_13b_ICSJWG_Spring_2011_Conf_Hayden.ppt

privées, sur d'intégrités des données, ou sur la disponibilité du service.

La protection d'information privée est un aspect qui est rapidement en train de devenir une priorité centrale. Les attaques à ce niveau se catégorises tel que suit :

1. débordement des données – problèmes de qualité de programmation
2. reniflement des données – la captures de données (RF), entre le compteur et le routeur
3. attaque du cryptage des données
4. attaque sur le mot de passe d'une composante ou un système
5. attaque sur le niveau de priorité d'accès (se faire passer pour un administrateur)

La gestion et le stockage de données est un nouveau défi qui vient avec les compteurs de type IMA. Les compteurs intelligents et le réseau électrique intelligent vont générer une grande volumétrie d'information, qu'il faudra stocker, analyser et protéger. Les coûts de ses activités, et les bénéfices concrets qu'ils amènent, n'ont pas été abordés dans la preuve du Distributeur.

Lors de la rencontre technique du 14 septembre 2001, le Distributeur a révélé qu'il serait le premier fournisseur en électricité à inclure un système de sécurité de si haut niveau. Or selon le RNCREQ, il est fort douteux que la solution ultime à la cybersécurité a été trouvée. Les risques continueront de se présenter, et les solutions devront continuer à s'y adapter.

2.2.4.1) Risques d'atteinte à la vie privée

Avec le choix technologique permettant de communiquer les profils de consommation personnels des consommateurs vers le Distributeur en passant par un réseau de communication ouvert, il existe bel et bien un risque d'atteinte à la vie privée, et ce, malgré les meilleurs efforts en matière de cybersécurité. L'histoire et le vécu de la sécurité informatique nous démontrent que tout système de cybersécurité est vulnérable, et que ce n'est qu'une question de temps avant que celui-ci soit compromis.

La proposition du Distributeur de recueillir des données de la consommation de chaque consommateur chaque 15 minutes ouvre la porte à des atteintes de la vie privée encore plus grandes.

La preuve du Distributeur ne justifie pas la nécessité d'obtenir ces profils de consommation d'énergie de clients résidentiels. En fait, cette information n'est requise que par le client résidentiel désireux d'économiser de l'énergie ou des coûts de consommation. Cette information peut être utilisée par des appareils ménagers de prochaine génération, sur un réseau résidentiel HAN, de type *ZigBee* ou équivalent.

Un survol des fonctions sur la Figure 4 du document HQD-1, Document 1 démontre qu'il est possible de mettre en place presque toutes les fonctions en gardant les profils de consommation personnelle, chez le client.

Or, le RNCREQ désire souligner que, le bénéfice le plus important de l'implantation de compteurs intelligents est de fournir au client des informations en temps réel de sa consommation énergétique, pour l'aider à la mieux gérer. Il s'agit, rappelons-le, d'une

fonctionnalité que le Distributeur a choisi de ne pas offrir dans le contexte du Projet[16].

Or, le fait que ces données sont utiles pour le client ne veut pas dire qu'elles sont utiles, ni encore moins nécessaires, pour le Distributeur. Par exemple, pour mieux comprendre la consommation des clients, il serait possible de faire des projets pilotes avec certains groupes de clients, pour des périodes fixées, sans faire de toute la province un laboratoire permanent d'étude de profils de consommation individuels. Et ce, sans parler des coûts reliés à la gestion de ce torrent de données qui représentera les mesures au 15 minutes de tous les consommateurs au Québec.

Dans une réponse à un engagement, le Distributeur a précisé que, selon la *Loi sur l'accès,* il « *ne peut recueillir que les renseignements personnels sur les clients qui sont réellement nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il assure la gestion*[17] ». Il a également indiqué qu'il considère les profils de consommation des clients comme des renseignements personnels. Or, selon les explications du Distributeur, il est difficile de voir en quoi il a réellement besoin de ces profils. La seule utilisation mentionnée est qu'il « *lui procurera une meilleure connaissance des profils de consommation et lui offrira l'occasion de développer des solutions qui tiennent davantage compte de la réalité de sa clientèle*[18] ».

Dans ces circonstances, le RNCREQ questionne sérieusement la proposition du Distributeur de cueillir des données détaillées sur la consommation de chaque client.

2.2.4.2) Risque à la fiabilité de l'approvisionnement des clients

Avec l'inclusion d'un appareil de déconnexion/connexion automatique par télécommande, le Distributeur créera un risque technologique qui n'existe pas actuellement. Cette fonction crée la possibilité qu'un « hacker » puisse déconnecter un (ou plusieurs) client(s) à leur insu, ce qui augmente de façon importante le tort qu'il peut causer et, fort probablement, la tentation de le faire, pour certaines personnes.

L'ancien directeur de la CIA, James Woolsey, qui se concentre maintenant sur les dossiers énergétiques, présente un scénario fictif pour expliquer les risques des réseaux intelligents[19]. Son article, reproduit en Annexe A, décrit l'histoire des réseaux intelligents de la perspective de l'année 2019. Il y a eu une série d'attaques au réseau dont l'auteur est éventuellement identifié comme … un ado. La crédibilité et le sérieux du scénario sont chez l'auteur.

Qui pourrait attaquer la sécurité d'un réseau intelligent ? L'étude de Verizon mentionne, entre autres, le crime organisé. Couplé avec le scénario de Woolsey, qui illustre les risques des réseaux intelligents interactifs, cela ouvre la porte à des scénarios moins spectaculaire, mais probablement plus coûteux à long terme pour les clients.

Selon les informations fournies à la rencontre technique, le compteur proposé par le Distributeur

---

16 HQD-4, doc. 7, page 5, R. 1.6.

17 HQD-3, doc. 2, page 7.

18 HQD-1, doc. 1, p. 32.

19 http://www.altenerg.com/back_issues/index.php-content_id=134.htm

a des moyens de protection s'il est physiquement altéré, mais le système n'a pas de fonctions de protection au cas où la sécurité de ses télécommunications serait compromise. Une fonction de sécurité simple comme un délai de déconnexion de 3 jours, avec affichage et avertissement sonore de la mise en marche de la déconnexion, pourrait mitiger ce problème.

3) Les analyses économiques

Le Distributeur demande l'autorisation de la Régie de procéder avec la Phase 1 du Projet LAD (« *le Projet R-3770* »)[20]. La Phase 1 consiste des travaux préparatoires, de la mise en place des TI de l'IMA, et du remplacement de 1,7 million de compteurs (presque 50 % de son parc) dans la Région 1[21].

Nous utiliserons l'expression « *le Projet LAD* » pour faire référence au projet LAD dans son entièreté (Phases 1, 2 et 3), et l'expression « le *Projet R-3770* » pour faire référence à la Phase 1 du Projet LAD, pour lequel le Distributeur demande l'autorisation dans le présent dossier.

Il est important de souligner que la vaste majorité des informations au dossier concernent le Projet LAD dans son ensemble, et non pas la Phase 1 qui fait l'objet de la demande R-3770.

Il appartient évidemment au Distributeur de choisir le projet qu'il présente à la Régie pour approbation. Cela dit, il lui incombe de produire une preuve complète sur le projet qu'il soumet.

Le *Projet R-3770* représente presque 50 % des coûts du *Projet LAD* (440 469 $ / 997 402 $)[22]. Toutefois, le dossier n'indique pas clairement quel pourcentage des bénéfices escomptés pour le *Projet LAD* est attribuable au *Projet R-3770*.

En fait, une analyse économique et financière est présentée pour l'ensemble du *Projet LAD*, et non pour le Projet R-3770. Dans la présente section, nous présentons quelques observations à l'égard de cette analyse. Il importe se souligner, cependant, que, étant donné l'absence d'une analyse similaire concernant le *Projet R-3770*, la Régie n'est pas en mesure de prendre des jugements éclairés sur la demande déposée devant elle.

3.1) Les analyses de l'Union de consommateurs

Tel qu'annoncé dans le Demande d'intervention du RNCREQ, afin de réduire leurs coûts et augmenter leur efficience, celui-ci s'est entendu avec l'Union de consommateurs afin d'avoir accès à des versions préliminaires de l'analyse préparé par l'analyste de cette dernière, M. Paul Paquin.

Le RNCREQ fait sien plusieurs des constats de cette analyse :

---

[20] HQD-1, doc.1, page 10.

[21] Ibid., p. 7.

[22] Ibid., Tableaux 4 et 11, pages 34 et 46.

- Le rythme de déploiement proposé par le Distributeur provoque une mise au rancart d'un grand nombre de compteurs qui n'ont pas atteint la fin de leur vie utile et dont le coût n'est pas entièrement amorti. La valeur comptable de ces actifs, estimée à 160 M$, sera radiée. Il serait donc important d'essayer de minimiser les coûts de radiation et d'amortissement accéléré.
- L'UC, comme le RNCREQ, questionne la présomption du Distributeur qu'il peut reporter le remplacement des compteurs bien au-delà de leur vie utile présumée de 15 ans. Toutefois, le RNCREQ ne considère pas que la solution explorée par l'analyste d'UC, soit d'arrêter l'analyse en 2027 est une solution adéquate. Le RNCREQ considère qu'il serait plutôt nécessaire d'intégrer les coûts investissements de remplacement dans l'étude de long terme.
- Le RNCREQ s'entend avec l'UC sur l'importance de regarder la valeur cumulative des revenus requis différentiels. Toutefois, le RNCREQ a choisi de le faire avec le taux d'actualisation retenu par le Distributeur (6,099%), qui est plus conservateur que le taux de 10 % retenu par l'UC.
- Le remplacement des frais d'exploitation par des investissements, sur lesquels il retire un rendement, crée un bénéfice pour le Distributeur, mais pas pour la clientèle.

3.2) Analyse économique et financière du Projet LAD

Malgré le fait que sa demande d'autorisation se limite à la Phase 1 (le *Projet R-3770*), la presque totalité des informations présentées par le Distributeur à l'appui de cette demande couvre l'ensemble du *Projet LAD*. Dans cette section, nous examinerons ces éléments.

3.2.1) Comparaison entre le Scénario IMA et le Scénario de référence

La justification économique du *Projet LAD* repose sur une comparaison économique entre le *Projet LAD* et un Scénario de référence, basé sur la poursuite des activités de base de remplacement des compteurs avec des compteurs électroniques dits « standards », avec une relève manuelle par 600 employés à l'aide des MOM

Tableau R-6.2
Ensemble des gains et des coûts d'achat et d'installation de compteurs actualisés (2011) sur 15 ans

M$ (actualisés 2011) période d'analyse 2011-2027	Scénario IMA
Investissements	483,8
gains	(623,0)
Taxe sur les services publics	-
Valeurs résiduelles	(33,1)
Total	**(172,3)**

(pour la clientèle résidentielle)[23].

Les résultats annuels des deux scénarios sont reproduits aux tableaux 1 et 2, sur la prochaine page[24].

Selon le Distributeur, pendant les quinze (15) ans qui correspondent à la période d'amortissement des nouveaux compteurs, les gains actualisés du *Projet LAD*, par rapport au Scénario de référence, sont de 172 M $, tel que l'indique le Tableau R-6.2, reproduit ci-dessus[25]. Il s'agit d'un bénéfice moyen d'environ 11 millions $ par année (172 M$/15).

3.2.2) Analyse du Scénario IMA

L'Analyse du scénario IMA mentionné ci-dessus comporte une ligne « Réduction de coûts et revenus », qui mène une réduction de 243 millions $ sur les 20 ans analysés (124,4 M $ actualisés). Cette ligne est ventilée dans une réponse à la Régie, comme suit[26] :

Le tableau R-7.1-B détaille l'écart apparaissant à la ligne « Réduction de coûts et revenus » selon la demande de la Régie.

R-7.1-B : RÉDUCTION DE COÛTS ET REVENUS

Réduction de coûts et revenus période 2012-2031 M$ actualisés	
Interruption / Remise de service à distance	(96,1)
Activités clientèle	(17,4)
Mise en conformité	(11,0)
Total	**(124,4)**

La source des valeurs n'est pas précisée, ni la signification précise des expressions « Activité clientèle » et « Mise en conformité ». En ce qui concerne la réduction des coûts de 96,1 millions $ pour « Interruption/Remise de service à distance », rien n'indique que le Distributeur aurait tenu compte de la réduction des revenus qui en découlerait, étant donné que les frais appliqués aux consommateurs qui subissent une interruption de service devront éventuellement être réduite pour refléter la réduction du coût pour le faire. Le montant de 96,1 millions $ devrait donc être retranché pour tenir compte de la modification éventuelle des Frais d'interruption de service (art. 12.5e des *Tarifs et conditions du Distributeur),* afin de refléter le coût de fournir ce service.

3.2.3) Analyse du Scénario de référence

Plusieurs éléments de l'Analyse du Scénario de référence soulèvent des doutes et des questionnements. Sur la base de l'information dont il dispose actuellement et sous réserve

[23] Ibid., p. 38.

[24] HQD-3, doc. 2, pages 1 et 2 de l'Annexe A.

[25] HQD-2, doc. 1, p. 16, réponse 6.2.

[26] HQD-4, doc. 1, page 12.

d'obtenir de plus amples clarifications, le RNCREQ formule les observations suivantes.

L'élément le plus grand dans le Scénario de référence, qui compte à lui seul pour 45 % de l'ensemble de ses coûts, est la Masse salariale de la relève. Il est prévu que ce poste devrait augmenter de 40,7 M $ en 2012 à 71,4 M $ en 2031, soit une augmentation annuelle de 3 %.

Tel que mentionné plus haut dans la section **Error! Reference source not found.**, depuis quelques années, les compteurs électroniques installés par le Distributeur sont en réalité des compteurs AMR, lus à distance par le biais d'un MOM.

> « *Jusqu'à 160 000 compteurs, essentiellement résidentiels, sur le total de 3 476 000 compteurs walk-by actuels, pourraient être lus dans un mode drive-by. Toutefois, ces compteurs ont été introduits pour une autre raison dans le parc des compteurs, soit dans le but de faciliter la lecture des compteurs difficiles d'accès. Le Distributeur installe maintenant ce type de compteur lorsqu'il y a une nouvelle intervention sur le compteur (nouvelle installation, programme d'étalonnage)* »[27]. (Nos soulignés)

Ce passage explique pourquoi, au moment de sa rédaction en 2005, il n'était pas possible de se prévaloir de la capacité de lecture à distance de compteurs électroniques :

> « *Actuellement, ces 160 000 sont disséminés dans toute la province.*
>
> *Pour avoir recours au mode de lecture drive-by il faudrait, en plus des compteurs, se munir de véhicules équipés de la technologie permettant de faire la lecture à distance (à bord du véhicule). Ce mode de lecture ne peut être rentable que si les compteurs sont installés de façon concentrée, ce qui n'est pas le cas des 160 000 compteurs actuels*[28]. »

Dans le présent dossier, le Distributeur confirme que les compteurs électromécaniques seront remplacés par des compteurs électroniques dont la relève peut être effectuée par radiofréquence par le biais d'un MOM[29]. Le nombre de compteurs de ce type (à 900 MHz) déjà en service s'élève à 730 882, dont la vaste majorité (625 540) installée dans les dernières cinq années[30].

Selon le Distributeur, les compteurs électroniques comptent maintenant pour plus de 20 % de ses compteurs[31]. Évidemment selon la stratégie de remplacement de compteurs, tel qu'indiqué au Tableau B-1[32], le pourcentage de compteurs AMR augmentera inexorablement au fil des ans. Quoique les employés doivent toujours aller de quartier en quartier pour faire ces lectures, la productivité des employés ne peut qu'augmenter avec la pénétration croissante de compteurs électroniques RF et la diminution correspondante du pourcentage du parc qui requiert la lecture manuelle[33]. Éventuellement, la pénétration des compteurs électroniques atteindrait

---

[27] R-3579-2005, HQD-14, doc. 5, page 18.

[28] Ibid.

[29] HQD-4, doc. 4, p. 4.

[30] HQD-4, doc. 12, p. 7, Tableau R-1.12.

[31] HQD-2, doc. 1, p. 5, Tableau R-1.3.

[32] Ibid.

[33] HQD précise que « la relève de compteurs se fait toujours manuellement par quelque 600 employés à l'aide de MOM », sans

inévitablement un niveau où l'achat de véhicules munis de la technologie de lecture serait rentable.

Tout cela démontre que, en suivant la stratégie de remplacement des compteurs qui constitue le Scénario de référence, la Masse salariale devrait inévitablement diminuer, plutôt de s'augmenter à 3 % par année.

Le Distributeur explique son choix de ne pas réduire les coûts de la masse salariale de la relève dans son Scénario de référence comme suit :

> "*Une baisse de coût ne se concrétise que dans un scénario de déploiement massif concentré sur une courte période. Or, le scénario de référence prévoit un remplacement du parc sur une période de 20 ans, principalement en fonction de l'âge des compteurs, avec des compteurs électroniques comme ceux déjà acquis par le Distributeur depuis quelques années. La technologie de ces compteurs relative à la relève ne permet qu'un gain marginal étant donné que le releveur doit quand même sillonner toutes les routes du Québec*"[34]. (Nos soulignés)

Le RNCREQ s'inscrit en faux contre la logique présentée par le Distributeur dans cette réponse. Selon notre compréhension, la baisse de coût dépend du niveau de la **pénétration** des compteurs RF dans une région donnée, et non pas sur la vitesse à laquelle cette pénétration aurait été déployée. Qui plus est, le temps requis de parcourir toutes les routes du Québec dans un camion est forcement beaucoup moins élevé que le temps requis pour le faire à pied, entrant dans chacun des demeures.

Il est donc évident que, dès que la pénétration des compteurs RF dans le parc atteint un certain niveau, il y aura des gains importants à l'égard du coût de la relève — gains qui ne sont pas représentés dans le Scénario de référence présenté par le Distributeur. Cela dit, le RNCREQ reconnaît que ces coûts ne diminueront pas aux niveaux minimaux prévus avec la technologie IMA.

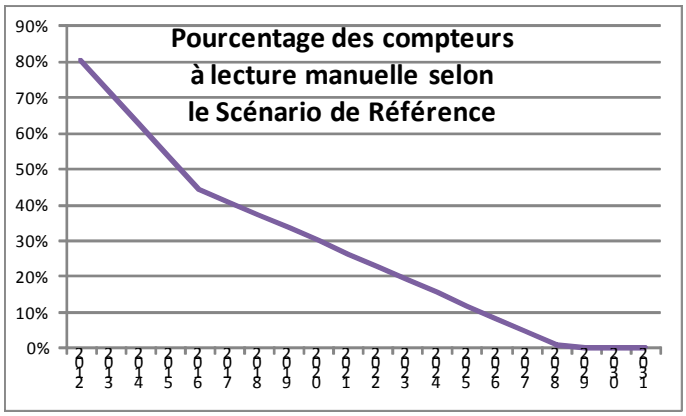
Afin d'explorer les implications de ce constat sur l'analyse économique faite par le Distributeur, le RNCREQ a, dans un premier temps, adopté la prémisse conservatrice selon laquelle, en 2011, 90 % du parc de compteurs requiert une lecture manuelle, nous réduisons ce chiffre chaque année en fonction du nombre de compteurs installés, selon le Tableau B-1[35].

---

mentionner la capacité de lecture RF des compteurs électroniques. HQD-1, doc. 1, p. 38.

[34] HQD-4, doc. 4, page 4-5, R. 1.6.

[35] HQD-1, doc. 1, Annexe B, page 57.



Malheureusement, le RNCREQ ne dispose pas en ce moment des données nécessaires pour modéliser l'évolution des coûts selon ce scénario.

En l'absence de ces informations, nous avons dans un premier temps choisi d'appliquer l'hypothèse très conservatrice que nombre d'employés travaillant dans la relève diminue à environ 3 % par année, soit l'équivalent de l'inflation prévue. Ainsi, dans un premier temps, nous avons présumé que la Masse salariale Relève demeurera stable en dollars courants, pour refléter une diminution graduelle des effectifs requis.

Avec cette hypothèse, la Masse salariale Relève diminue à 815 M $ sur la période 2012-31, et le coût total en dollars courants diminue de 2 416 M $ à 2 136 M $. Actualisé au même taux, cela donne une valeur actualisée de 1 238 M $. Tenant compte des valeurs résiduelles, et incluant les coûts de l'infrastructure TI (qui est requis pour le Scénario IMA, mais pas pour le Scénario de référence), la différence entre les deux scénarios se réduit à seulement 68 M $, sur 20 ans, où seulement 3,4 millions $ par année en moyenne.

Si, par contre, les coûts de la relève diminuent par 2 % par année, dus à l'automatisation graduelle de la lecture du parc de compteurs électroniques, les bénéfices économiques du Projet LAD disparaissent entièrement.

3.2.4) Comparaison des scénarios

Selon le RNCREQ, vu strictement d'un point de vue financier, le *Projet LAD*, et forcement aussi le *Projet R-3770*, comporte un très faible niveau de rentabilité :

- Le bénéfice moyen prévu par le Distributeur sur les premières 15 années du Projet est de seulement 11,5 million $ actualisés par année (172,3 M $/15[36]), sur un investissement de presque un milliard de dollars.

[36] HQD-2, doc. 1, p. 17, Tableau R-6.2

- Le bénéfice moyen sur les premières 20 années du Projet est de seulement 14,5 millions $ actualisés par année (289,7 M $/20[37]).

Rappelons que, tel que défini par le Distributeur, le Projet R-3770 ne comporte aucun bénéfice important pour le consommateur, autre que le bénéfice économique escompté. Dans ce sens, il se distingue de la vaste majorité, sinon la totalité, des projets AMI et Réseau intelligent ailleurs, qui se justifient en grande partie par des bénéfices réels offerts aux consommateurs, comme celles identifiées par Southern California Edison, décrites plus loin.

Étant donné l'ensemble des risques technologiques décrits plus haut, le RNCREQ conclut que le bénéfice escompté est loin d'être suffisant pour compenser les investissements et les risques.

3.2.5) Impact tarifaire du Projet LAD

Le Distributeur a aussi évalué l'impact du Projet LAD sur les revenus requis, sur une base annuelle. Comme l'indique le Tableau 1 sur la prochaine page, son analyse démontre que l'impact annuel sera à la hausse pendant les années 2012 à 2017 inclusivement, avec des impacts à la baisse ensuite.

Le tableau 1 démontre que, quoique l'impact sur les revenus requis devient négatif en 2018, l'impact **cumulatif** du *Projet LAD* sur les revenus requis demeure positif jusqu'en 2026. Cela implique que, jusqu'en 2025, les augmentations tarifaires totales dues à l'implantation du *Projet LAD* demeurent plus élevées que les réductions tarifaires cumulatives qui découlent de ses gains.

Si le Projet LAD va de l'avant, les hausses tarifaires dans les années 2012-17 constitueront pour les consommateurs un investissement qui sera récompensé par une réduction tarifaire pour les années subséquentes. Il prendra huit ans (de 2018 à 2026) pour repayer l'investissement. **Ainsi, selon les chiffres du Distributeur, le consommateur ne verra pas de bénéfice net avant 2027.**

Cette analyse est faite en dollars courants. Si on applique aux consommateurs le même taux d'actualisation nominal utilisé par le Distributeur, soit de 6,099%[38], le « payback period » dure **jusqu'en 2029**, comme l'indique le tableau 2.

Ainsi, l'impact net sur l'ensemble des consommateurs est négatif pendant quinze (15) ans, si on ne tient pas compte de l'inflation ni de la valeur temporelle de l'argent, ou pendant dix-sept (17) ans, en utilisant le taux d'escompte du Distributeur. Évidemment, l'utilisation d'un taux d'escompte plus élevé que 6,0999% ferait en sorte que l'effet cumulatif sur l'ensemble des consommateurs demeurera négatif encore plus longtemps.

De plus, il y a lieu de questionner certains éléments du budget prévisionnel :

- Est-ce que le budget annuel pour le maintien de la cybersécurité est raisonnable?

---

[37] HQD-1, doc. 1, p. 39, Tableau 7.

[38] HQD-2, doc. 1, Annexe C, pages 2 et 3.

Tableau 1.

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
revenus requis différentiels	**51,820**	**95,811**	**85,678**	**57,425**	**28,498**	**11,887**	**-7,968**	**-17,791**	**-29,058**	**-37,405**	**-44,434**	**-51,536**	**-59,203**	**-65,195**	**-71,203**	**-76,340**	**-88,106**	**-98,625**	**-102,626**	**-100,857**
revenus requis différentiels (cumulatifs)	**51,820**	**147,631**	**233,309**	**290,734**	**319,232**	**331,119**	**323,151**	**305,360**	**276,302**	**238,897**	**194,463**	**142,927**	**83,724**	**18,529**	**-52,674**	**-129,014**	**-217,120**	**-315,745**	**-418,371**	**-519,228**

Tableau 2.

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
revenus requis différentiels	**51,820**	**95,811**	**85,678**	**57,425**	**28,498**	**11,887**	**-7,968**	**-17,791**	**-29,058**	**-37,405**	**-44,434**	**-51,536**	**-59,203**	**-65,195**	**-71,203**	**-76,340**	**-88,106**	**-98,625**	**-102,626**	**-100,857**
revenus requis différentiels (escomptés)	**51,820**	**90,303**	**76,111**	**48,080**	**22,489**	**8,841**	**-5,586**	**-11,755**	**-18,096**	**-21,955**	**-24,581**	**-26,871**	**-29,094**	**-30,197**	**-31,084**	**-31,411**	**-34,168**	**-36,049**	**-35,355**	**-32,749**
revenus requis différentiels (escomptés) (cumulatifs)	**51,820**	**142,123**	**218,234**	**266,315**	**288,804**	**297,645**	**292,059**	**280,304**	**262,208**	**240,254**	**215,673**	**188,801**	**159,707**	**129,510**	**98,426**	**67,014**	**32,846**	**-3,203**	**-38,558**	**-71,307**

- Est-ce que le budget pour le renouvellement des systèmes de cybersécurité sera adéquat ?
- Est-ce que le budget d'entretien pour des éléments du NAN tient compte du besoin de changer périodiquement les piles sur l'ensemble des routeurs et collecteurs?
- Est-ce que le budget prévisionnel tient compte de la réduction des frais d'interruption, qui devra normalement suivre la réduction du coût de cette activité ?
- Est-ce que le budget prévisionnel tient compte de la croissance du nombre de clients ?

Jusqu'ici, le RNCREQ n'a pas pu résoudre ces questions à sa satisfaction. Prises individuellement ou ensemble, elles soulèvent des doutes quant à la rentabilité escomptée.

Finalement, il faut aussi ajouter à cette analyse deux incertitudes majeures, toutes les deux reliées au remplacement des compteurs. Premièrement, il y a la question de remplacement des compteurs à la fin de leur vie utile. Un document d'Accenture, déposé par le Distributeur à l'appui de sa demande, présente un extrait d'un document déposé par Southern California Edison devant la PUC de la Californie, qui dit :

> "*The generally-accepted lifespan for solid state meters and meters with electronic components is fifteen years, compared to the industry-average lifespan of thiry years for mechanical meters ... This shorter lifespan of the AMI meters will require more frequent replacement of meters and network components than we currently experience, <u>including a large "bubble" beginning fifteen years after the AMI implementation, where many, if not all, AMI meters will again have to be replaced</u>*"[39]. (nos soulignés)

Or, questionné par le RNCREQ[40] et par la FCEI[41] sur la raison pour laquelle le remplacement prévu des nouveaux compteurs vers la fin de la décennie 2020 n'est pas représentatif du rythme d'installation originale (avec un large « bubble »), le Distributeur nous renvoit à sa réponse 1.5 à la DDR #1 de la Régie de l'énergie :

1.5 Veuillez élaborer sur les avantages et les inconvénients d'introduire à l'intérieur d'un intervalle de 5 ans seulement, un parc de 3,75 millions de compteurs en tenant compte des besoins de maintenance et des remplacements futurs des ces compteurs.

Réponse :

Le Distributeur prévoit étaler le remplacement des compteurs de nouvelle génération sur plusieurs années afin de réduire l'impact inévitable d'un remplacement massif au terme de leur vie utile. Pour ce faire, le Distributeur se basera sur ses connaissances en gestion d'un parc de compteurs et son expérience déjà acquise et celle à venir en gestion d'un parc de compteurs de nouvelle génération.

---

[39] HQD-2, doc. 1, Annexe A, page 6.

[40] HQD-4, doc. 7, page 36, R. 20.1.

[41] HQD-4, doc. 4, page 5, R.1.9.

Une somme de 250 M$ en dollars courants est prévue à même l'analyse économique pour le remplacement des compteurs à compter de 2027.

Par ailleurs, la technologie permettra au Distributeur d'avoir une connaissance plus précise de son parc, ce qui contribuera favorablement à la gestion de son renouvellement. Le centre d'exploitation du mesurage, par exemple, pourra suivre en temps réel des lots de compteurs virtuels.

Enfin, le Distributeur pourrait vraisemblablement obtenir une dispense de Mesures Canada pour les travaux d'échantillonnage requis par la réglementation, et ainsi alléger sa charge de travail à cet égard dans le contexte d'un remplacement de l'ensemble du parc de compteurs sur une courte période.

Voir également la réponse à la question 1.4.

Selon le RNCREQ, cette réponse ne dispose aucunement des préoccupations soulevées par le document de Southern California Edison.

Doit-on comprendre que les « connaissances en gestion d'un parc de compteurs » et « l'expérience déjà acquise et celle à venir en gestion d'un parc de compteurs de nouvelle génération » dépasse celles de Southern California Edison à un tel point que cette contrainte majeure ne s'appliquera pas au Distributeur? Sans d'autres preuves plus convaincantes, l'analyse économique devra, selon le RNCREQ, être modifiée pour tenir compte du remplacement des compteurs, routeurs et collecteurs à la fin de leur vie utile. De toute évidence, une telle modification aura l'effet d'anéantir totalement les bénéfices escomptés du Projet LAD.

Cela dit, la deuxième incertitude à l'égard du remplacement des compteurs, qui a des implications encore plus grandes, concerne la question de l'obsolescence technologique, discutée à la section 2.2.1) ci-dessus. Cinq ans est bien long, et dix ans est une éternité dans l'évolution des produits informatisés. De toute évidence, l'évolution technologique qui rend possibles les réseaux intelligents est encore à ses débuts.

L'analyse économique proposée pour le Projet LAD présuppose que les compteurs, routeurs et collecteurs qui en font partie ne seront pas remplacés avant la fin de la décennie 2020. Si le rythme des avancées technologique s'estompe, cela peut très bien être vrai. La durée de vie de ces équipements, au niveau de leur fonctionnalité, n'est pas contestée.

Mais la question n'est pas là. La vraie question est la suivante : **Quelle est la probabilité que, bien avant l'année 2027, le Distributeur puisse vouloir remplacer son parc de compteurs « de nouvelle génération » qui serait devenu vétuste, dû aux avancées technologiques qui auraient lieu dans les prochains dix ans?**

Selon le RNCREQ, cette probabilité n'est pas de 100 %, mais bien plus élevée que 0 %. **Il y a donc une réelle possibilité que, dans les faits, HQ Distribution remplace ces compteurs avec une technologie plus performante, avant le délai de quinze ans.**

Malheureusement, si cela arrive, les gains économiques escomptés pour le Projet LAD seront remplacés par des pertes. Rappelons que, en utilisant le taux d'escompte d'HQD, l'impact

tarifaire cumulatif devient positif seulement en **2029.** Il est donc évident que tout remplacement technologique hâtif fera disparaître ce gain. Plus ce remplacement est hâtif, plus les pertes conséquentes seront importantes.

Lorsque la Régie a demandé au Distributeur s'il était prêt à s'engager à assumer toutes les pertes associées à la non-réalisation des gains anticipés, et s'il offre des garanties à sa clientèle, en termes tarifaires, relativement à la non réalisation des gains anticipés, il n'a pas répondu directement à la question[42]. En l'absence d'une telle garantie, il faut comprendre que ce sont les consommateurs qui ultimement seront appelés à payer si les gains escomptés n'apparaissent pas, comme l'indique par ailleurs une réponse antérieure à la Régie :

> « *Malgré tous ces efforts et l'application des meilleures pratiques de gestion de projet, dans le cas d'un éventuel dépassement des coûts du projet LAD au-delà des taux de contingence prévus, le Distributeur présentera à la Régie les explications requises et demandera la récupération de l'ensemble des coûts dans ses tarifs conformément au cadre réglementaire applicable* ».[43]

Selon le RNCREQ, il s'agit d'un pari à refuser, car les risques sont très importants par rapport aux gains escomptés.

3.3) Analyse financière et économique du Projet R-3770

À la section 10.2 du document HQD-1, doc. 1, le Distributeur a présenté les coûts du Projet R-3770 (la Phase 1 du Projet LAD). Toutefois, à la connaissance du RNCREQ, il n'a présenté aucune analyse financière et économique du Projet R-3770 pour lequel il demande l'autorisation.

Selon le RNCREQ, une analyse financière et économique est un élément essentiel pour l'autorisation du Projet. Le Distributeur n'ayant pas cru bon de présenter une telle analyse pour la Phase 1 du *Projet LAD*, le RNCREQ est d'avis que la Régie n'est pas en mesure de l'autoriser.

4) Conclusions

4.1) Le Projet R-3770

Le Distributeur justifie le « *Projet LAD* » sur la base des gains d'efficience à l'égard des coûts de la relève des compteurs. Quant au « *Projet R-3770* », pour lequel il demande l'autorisation de la Régie dans ce dossier, aucune analyse économique particulière et détaillée n'a été déposée

---

[42] HQD-4, doc. 1, p. 9, R. 5.1.

[43] HQD-2, document 1, page 28-29.

en preuve. Selon le RNCREQ, le Distributeur ne s'est simplement pas déchargé du fardeau de preuve qui lui incombait afin de démontrer que le *Projet R-3770* pour lequel il demande l'autorisation est justifié.

Pour les raisons explicitées dans la section 3.2.5) , le RNCREQ est d'avis que la démonstration de la justification économique du Projet LAD n'est pas non plus acquise.

Rappelons les objectifs énoncés, qui sont de trois ordres :

6. La pérennité du parc de compteurs;
7. La réalisation de gains d'efficience provenant de l'automatisation de la lecture de la consommation, de même que de l'interruption et de la remise en service à distance; et
8. La possibilité d'évolution technologique permettant éventuellement d'offrir de nouveaux services aux clients et de mettre en place des mesures de gestion de réseau[44].

Or, le RNCREQ est d'avis que :

1. La pérennité du parc de compteurs serait aussi garantie par le Scénario de référence, où les compteurs continuent d'être remplacés au besoin;
2. Les gains d'efficience provenant de l'automatisation de la lecture sont petits, par rapport aux investissements proposés, et sont assujettis aux risques majeurs détaillés dans la section précédente,
3. Quoiqu'il soit vrai que la mise en place des équipements visés par le *Projet R-3770* ouvre la porte à une certaine évolution technologique, il risque également de fermer certaines portes, dans la mesure où le matériel acheté et installé pourrait ne pas être optimal pour les fonctions qu'on voudra éventuellement offrir.

Ce constat nous ramène au point fondamental de la section 2.1) , soit l'absence d'une vision globale du réseau intelligent à déployer.

La comparaison faite par le Distributeur entre son Scénario IMA et son Scénario de Référence n'est pas, selon le RNCREQ, suffisamment rigoureuse pour justifier un projet de cette envergure.

Malgré tous les efforts déployés, il demeure possible que les avancées technologiques des prochaines années obligeront le Distributeur à une mise à niveau de ses infrastructures avant la fin de leur durée de vie utile. Il est donc impératif, pour le RNCREQ, de déployer une approche prudente, où l'implantation d'une infrastructure technologique est précédée par une planification des besoins futurs et l'inventaire des spécifications techniques requises pour combler ces besoins.

La décision de remplacer 20% du parc des compteurs du Distributeur longtemps avant la fin de la durée de vie de ces derniers, afin de les remplacer avec une autre technologie qui n'a pas encore atteint un stade de maturité technologique, est en soi une démonstration que l'hypothèse voulant que les nouveaux compteurs soient en place pendant 15 ans est risquée. Rappelons que les compteurs électroniques en place ne seront pas remplacés pour des raisons

[44] HQD-1, doc. 1, page 7.

de défectuosité, mais simplement parce que, à peine quelques années après leur installation, une meilleure technologie est apparue. Selon le RNCREQ, il est impossible d'exclure la possibilité que le Distributeur soit tenté de devancer le remplacement des compteurs une fois de plus, devant une nouvelle solution technologique encore plus attrayante, ayant pour résultat de démolir la rentabilité escomptée du Projet.

Il faut aussi ajouter le risque technologique, soit le fait que, même si la solution choisie est maintenue, les besoins au niveau de matériel informatique au cœur des équipements (compteurs, routeurs et collecteurs) dépasseront les capacités des équipements d'aujourd'hui. Bien que les compteurs de nouvelle génération de type IMA que veut acquérir le Distributeur aient une capacité évolutive par le biais de sa programmation, cette capacité est limitée par le matériel du compteur au niveau de la mémoire disponible et de la puissance de traitement de l'information.

Ainsi, malgré la capacité de mettre à jour à distance les logiciels d'opération des compteurs, la capacité de leur matériel informatique d'opérer ces mises à jour risque de devenir inadéquate pour supporter les logiciels de cryptage, nécessitant leur remplacement ou mise à jour physique, dont le coût n'est pas prévu dans le Projet. Par ailleurs, afin de préserver l''intégrité physique des compteurs et garantir la précisions des mesures de consommation d'électricité à être facturée, ceux-ci sont scellés, selon les exigences de la loi. Cette contrainte complexifie toute mise à jour du matériel faite *in situ*. Il existe donc un risque réel que le matériel qui serait acquis d'ici 5 ans dans le cadre du Projet ait besoin d'être remplacé bien avant 2027[45].

Considérant ce qui précède, le RNCREQ considère que le projet, tel que présenté dans la phase 1 du dossier R-3770-2011, ne présente pas les qualités requises pour être approuvé par la Régie. Il recommande conséquemment à celle-ci de rejeter la demande du Distributeur.

4.2) La mise en place d'un réseau intelligent

Le RNCREQ demeure convaincu que la mise en place d'un Réseau intelligent, y compris une infrastructure de mesurage avancée, pourrait apporter des bénéfices importants aux consommateurs d'Hydro-Québec et à la société québécoise en général. Toutefois, il constate que le Projet R-3770 sous étude ainsi que le Projet LAD dans sa globalité sont inadéquats pour réaliser ces bénéfices.

L'approche du Distributeur, qui consiste à concevoir et faire approuver un projet dans l'unique but de réduire les coûts associés à la relève des compteurs va à l'encontre des meilleures pratiques reconnues par des acteurs majeurs, tels McKinley, Accenture et EPRI. Il y a un consensus très large à l'effet que, pour un projet aussi structurant que celui-ci, il est d'une importance capitale d'établir une planification globale de l'implantation d'un réseau intelligent plutôt que d'amorcer une mise en œuvre à la pièce.

D'une part, cette planification globale aidera à s'assurer que les différents intérêts affectés par le

[45] HQD-3, doc. 2, p. 13, Figure E-6.

réseau intelligent, tant à l'intérieur de l'entreprise que dans la société en général, sont respectés. D'autre part, elle aidera à éviter que des investissements importants soient faits en infrastructures sans que ces équipements permettent de combler les besoins auxquels elles seront éventuellement appelées à répondre.

Par ailleurs, cette planification globale permettra de mettre en application l'un des 16 principes de la *Loi sur le développement durable*, à savoir que les décisions doivent se prendre avec le souci d'assurer l'efficacité économique (« *l'économie du Québec et de ses régions doit être performante, porteuse d'innovation et d'une prospérité économique favorable au progrès social et respectueuse de l'environnement* »). Selon le RNCREQ, il serait risqué à ce stade-ci de débourser des sommes aussi importantes pour de nouveaux appareils de mesures sans avoir la certitude qu'ils pourront éventuellement répondre aux besoins (notamment lorsqu'on voudra mettre en service les autres fonctionnalités).

Ainsi, le RNCREQ considère que si la mise en place d'une IMA était justifiée par les nouvelles fonctionnalités qu'il permettait, dans le cadre d'un projet intégré de Réseau intelligent, ses risques pourraient être acceptables. Notamment, nous référons aux extraits de Southern California Edison et de l'étude McKinley, à la fin de la section 2.1 **Error! Reference source not found.**de la présente, qui démontrent que la mise en place d'un réseau intelligent peut créer de bénéfices importants pour toute la clientèle et pour la société en général, notamment en permettant la mise en place de nouveaux outils d'efficacité énergétique.

Le RNCREQ demeure très optimiste quant aux bénéfices qui découleront éventuellement de la mise en place d'un réseau intelligent au Québec. Il invite Hydro-Québec à entamer une réflexion sérieuse à cet égard, avant de soumettre une proposition étoffée à la Régie de l'énergie.

ANNEXE A

R. James Woolsey:

The Future U.S. Energy Picture ?

Guest Column

The Future U.S. Energy Picture?

In March, at a workshop convened by Sandia National Laboratories and the University of California, San Diego, leaders from academia, government, and the private sector gathered to discuss key energy policy issues.

At the workshop, attendees were asked a question about what the future U.S. energy picture might look like.

Below is R. James Woolsey's response to the question. Mr. Woolsey was Director of the Central Intelligence Agency and is Chairman of the Advisory Board of the Clean Fuels Foundation.

"Imagine it is ten years from now. U.S. energy policy has changed dramatically for the better in response to the intersecting priorities of economic security, environmental and climate security, and national security. Describe the underlying principles and long-term goals that drove that change. What does the U.S. and the world energy picture look like as a result?"

Report of March 2019: The 2009 Plan for a "Smart" Electricity Grid

Plans had been completed ten years ago—in March 2009—for hundreds of billions of dollars in investment to make the electricity grid smarter and more capable of carrying the stranded electricity, produced by solar plants in the southwest and wind farms in the Great Plains, to population centers on the coasts. Central control of electricity demand was to be a major aspect of this new grid, and there were to be a great many other "smart" improvements.

By September 2009, however, a series of cyber attacks on the grid during the summer had a devastating effect, creating dozens of serious regional electricity brownouts and blackouts. For some weeks, authorities were certain the sophisticated attacks had come from, at first, China, then Russia, then Hezbollah cyber-cells in Lebanon.

In September, however, an eighth-grader in Burbank, California, confessed that he and a group of friends had grown bored with video games during the summer and had decided to bring down major parts of the grid for various periods of time. Under questioning by authorities, the group protested that it would have been easy for them to have taken the grid down for months, and that "you guys" should feel lucky they had only taken portions down for days.

The eighth-grader added that the Supervisory Control and Data Acquisition (SCADA) systems that control the grid, using commercial off-the-shelf software over the Internet, were so easy to hack that he and his friends soon got bored with that as well, and several new, more challenging video games had temporarily led them to set aside their grid shutdowns.

The young witness said to his astonished interrogators, "If you dorks can't even deal with us, how are you going to deal with Chinese, Russian, or Hezbollah cyber-dudes? You aren't building a smart grid. It's headed towards being an ODAV grid—we normally don't spell that out for the rents and other old peeps, but it stands for 'Ostrich-Designed, Awesomely Vulnerable.'" (Editor's Note: 'rents' is slang for parents and 'peeps' is slang for people.)

An urgent national re-evaluation of the planning for the smart grid project followed.

The administration learned that the combined incentives of electricity deregulation and electricity companies' consequent total focus on the quarterly bottom line—together with utilities' lawyers' warnings that they risked liability if they acknowledged any security problem that they didn't fix immediately—had destroyed most of the incentives to make the grid secure.

It was also a classic tragedy-of-the-commons problem: if any utility spent the money to fix vulnerabilities, chances were that the blackout of a still-vulnerable neighbor utility—if the neighbor were taken down by cyber or other attacks (e.g. on transformers)—would black them out as well.

When the utility executives were asked why they had fought so hard in the summer of 2008 against increased authority for the Federal Energy Regulatory Commission to be enabled to order security improvements that would apply to all utilities, they looked guiltily at one another—and shrugged.

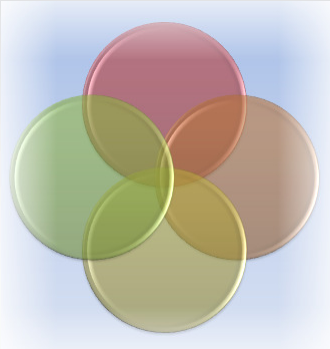
As a result of these events, the administration re-structured the smart grid program to emphasize security as well as renewables and distributed generation, including co-generation. They also adopted a feed-in-tariff. Consequently, over the last decade the rapid growth of clean, distributed, secure electricity and the accelerating move, led by battery improvements, in the electrification of transportation and in electricity storage has brought the U.S. to a position of world leadership in bringing about far greener, and far more resilient, energy systems.

Rumor has it that most of the former Burbank eighth-graders now work for a highly-classified office within the U.S. National Security Agency with two responsibilities: designing U.S. retaliatory steps to deal with any attempted foreign cyber-attacks and periodically functioning as a Red Team to keep U.S. utilities on their toes. e

ANNEXE B

Four Layers of Smart Grid Security
3 mai 2011

The Four Layers of Smart Grid Security



ICSJWG – 2011 Spring Conference
Dallas/Addison Marriott Quorum by the Galleria
Dallas, Texas

Ernie Hayden CISSP CEH
Managing Principal – Energy Security
Global Energy & Utility Practice
May 3, 2011

© Verizon 2011 – All Rights Reserved

Ernie Hayden CISSP CEH

- **Cybersecurity Expertise – Critical Infrastructure and Energy/Utility Domain**
- **CISO Roles**
  - Seattle City Light (NERC CIPs, Smart Grid Security, PCI DSS, FERC Dam Safety)
  - Group Health Cooperative (HIPAA, PCI DSS)
  - Port of Seattle (DHS/TSA, TWIC, PCI DSS, State of Washington Data Breach Laws)
  - Alstom ESCA (FERC Appendix G, Post 9/11 Focus)
- **Committees**
  - NERC Smart Grid Task Force
  - NIST Cyber Security Working Group – High Level Requirements Subcommittee (NISTIR 7628) and Testing and Certification Subcommittee
  - Cloud Security Alliance, Data Lifecycle Security Domain (Leader) for Version 2
- **Certification**
  - Certified Information System Security Professional (CISSP) – ISC^2
  - Certified Ethical Hacker (CEH) – EC Council
- **Other**
  - Instructor – Information Systems Cyber Security Certificate Program, University of Washington
  - CEO – Advanced Sensor Design Company for Hydro Electric Generators
  - Maintenance Manager – Trojan Nuclear Plant
  - Author, Speaker -- Various

© Verizon 2011 – All Rights Reserved

verizonbusiness

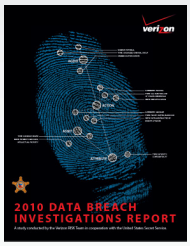
Energy and Utilities

- Energy Solutions
- Utility Solutions
  - Implement Smart Grid
  - Enable End-to-End Security
  - Enhance Customer Service
  - Increase Efficiency and Sustainability

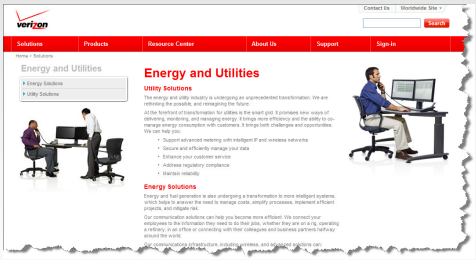
think forward | blog

BLOG | ABOUT THE BLOG | COMMENT POLICY | TERMS OF USE

http://www.verizonbusiness.com/Thinkforward/blog/



New DBIR Published April 19,2011



http://www.verizonbusiness.com/solutions/utility/

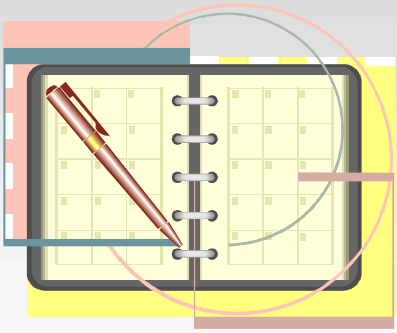
© Verizon 2011 – All Rights Reserved

History of Verizon Security Services

© Verizon 2011 – All Rights Reserved

Today's Agenda

- Intro to "Smart Grid"
- Who's Worried and Why?
- Psychology of Security
- "Layers" of Concern
  - Physical Layer
  - Cyber Layer
  - Privacy Layer
  - Storage Layer
- Just What To Do?
- Question & Answer



© Verizon 2011 – All Rights Reserved

WARNING!!!!

FUD* AHEAD….

* = FEAR, UNCERTAINTY AND DOUBT

© Verizon 2011 – All Rights Reserved

Objectives of Smart Grid

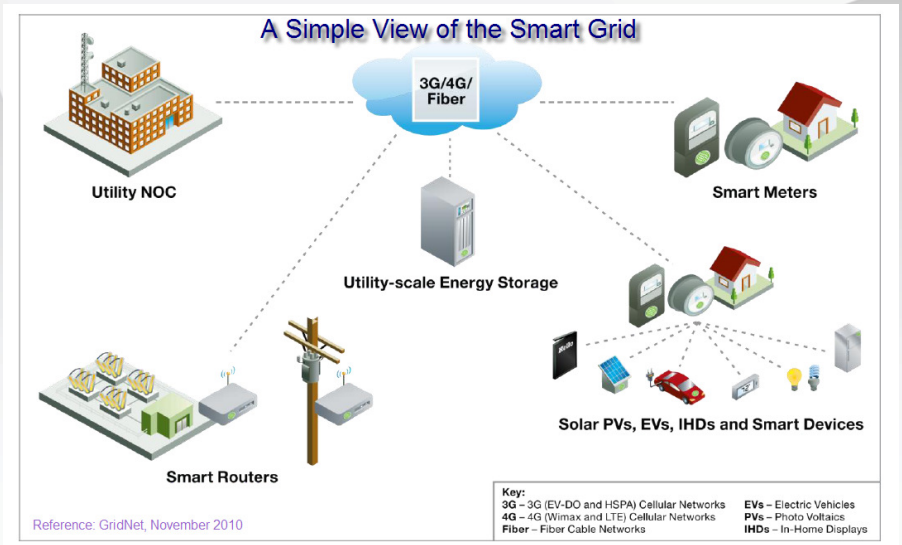
- ***Energy Independence and Security Act of 2007*** **(EISA)** directs federal and state agencies to implement programs that advance the implementation of the "Smart Grid."
- **EISA describes the "Smart Grid" as follows:**
  - *a modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth*
- **Goal:**
  - *The goal is to use advanced, information-based technologies to increase power grid efficiency, reliability, and flexibility, and reduce the rate at which additional electric utility infrastructure needs to be built.*

© Verizon 2011 – All Rights Reserved

What's a "Smart Grid?"

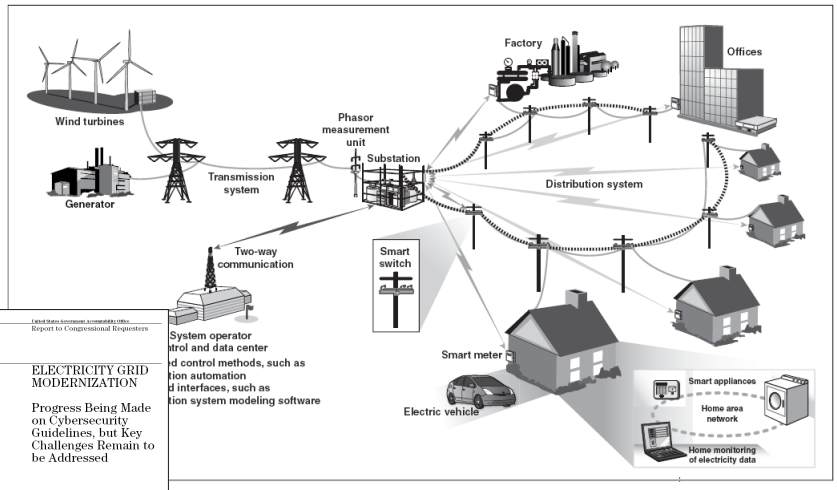
US Department of Energy

© Verizon 2011 – All Rights Reserved

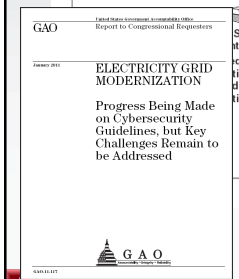


© Verizon 2011 – All Rights Reserved

Figure 2: Common Smart Grid Components



Source: GAO analysis.


GAO

Report to Congressional Requesters

ELECTRICITY GRID MODERNIZATION

Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed

GAO

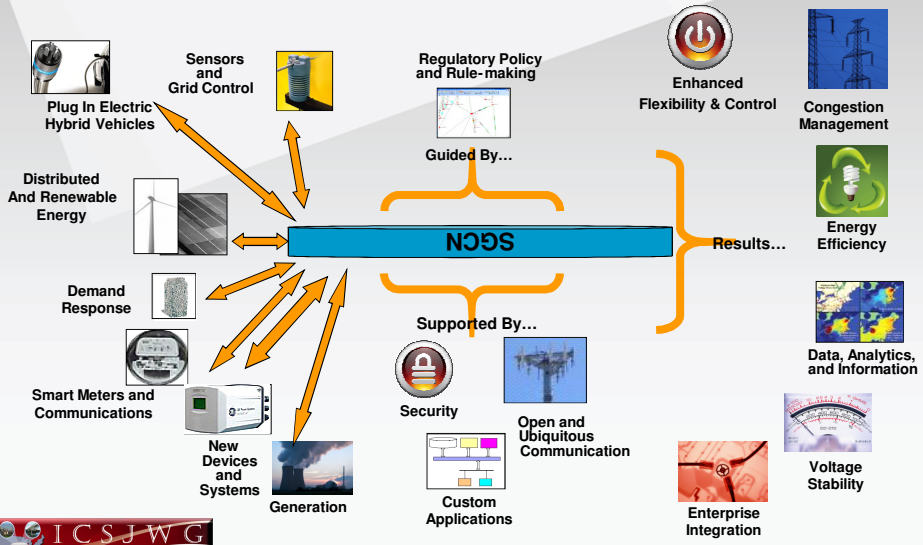
GAO-11-117

GAO Report – Released January 2011

http://www.gao.gov/products/GAO-11-117

© Verizon 2011 – All Rights Reserved

Another View – Smart Grid Communications Network



© Verizon 2011 – All Rights Reserved

Who is Worried?

High-Level Security Concerns from US Federal Government

- **Acknowledged by:**
  - National Institute of Standards and Technology (NIST)
  - Department of Homeland Security (DHS)
  - Department of Energy (DOE)
  - Federal Energy Regulatory Commission (FERC)
  - Government Accountability Office (GAO)
  - Selected State Public Utility Commissions

www.willhackforsushi.com

© Verizon 2011 – All Rights Reserved

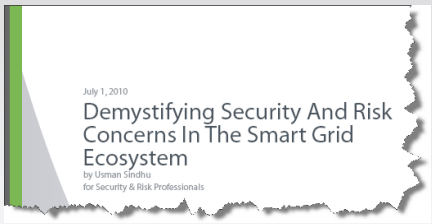
DOE and NIST Concerns

- **Additional Risks to the Grid Include:**
  - **Increasing Complexity of the Grid**
    - »Introduce Vulnerabilities
    - »Increase Exposure to Potential Attackers and Unintentional Errors
  - **Interconnected Networks Can Introduce Common Vulnerabilities**
  - **Increasing Vulnerabilities to Communications Disruptions and Introduction of Malicious Software**
    - » Denial of Service
    - »Compromise the Integrity of Software and Systems
  - **Increased Number of Entry Points and Paths for Potential Adversaries to Exploit**
  - **Potential for Compromise of Data Confidentiality, Including Breach of Customer Privacy**

© Verizon 2011 – All Rights Reserved

Forrester – "Demystifying Security and Risk Concerns in the Smart Grid Ecosystem"

- **Obvious but Still Important…**
- ***"Security always has been and always will be a paramount concern in any IT network. But, what makes smart grid security issues more daunting <u>is the pervasive and massive deployment of these networked components</u> ranging from thousands of smart sensors and other IT-enabled components"***

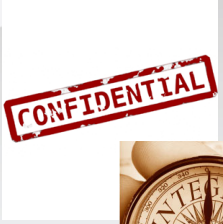


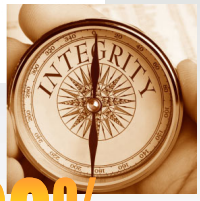
Prediction for U.S. by 2019 → 100M Meters → 100 Petabytes generated during the next 10 years

© Verizon 2011 – All Rights Reserved

Psychology of Security

- **"Protect the Data"**
- **CIA**
  - Confidentiality
  - Integrity
  - Availability
- **Sometimes Also Included:**
  - Non-repudiation
  - Authentication/Authorization



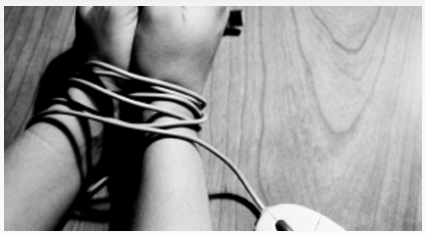


99.9999%

© Verizon 2011 – All Rights Reserved

Psychology (2)

- **Psychology of Attackers – Why Do It? Motivation?**
  - Get Attention
  - Joke/Hoax/Prank
  - Sense of Power & Prestige
  - Make Money – Greed! Revenue! Includes Fraud
  - Revenge
  - Hate
  - Win at All Costs
  - Make Money
  - Corporate Espionage
  - Politics – Fulfill the Agenda



© Verizon 2011 – All Rights Reserved

How Much is that Exploit in the Window?

- **$50,000: A zero-day exploit for Microsoft Windows 7**
- **$20,000 to $30,000 each: Other zero-day exploits**
- **$5,000 and up: Bots that allow users to self-generate botnets**
- **$1,000-$5,000: Customized Trojan program, which could be used to steal online account information**
- **$50: Credit card number with PIN**
- **$10-$100: Change of billing data, including account number, billing address, Social Security number, home address, and birth date**
- **$50: Driver's license**
- **$50: Birth certificate**
- **$10: Social Security card**
- **$2-$5: Credit card number with security code and expiration date**
- **$2: PayPal account log-on and password**

Mother's Maiden Name ($3)
Social Security Number ($3)
Date of Birth ($0.5)
Mother's Date of Birth ($1)
Driver's License Number ($8)
Background Report ($15)
Credit Balance Report ($25)

Everything Has Value!

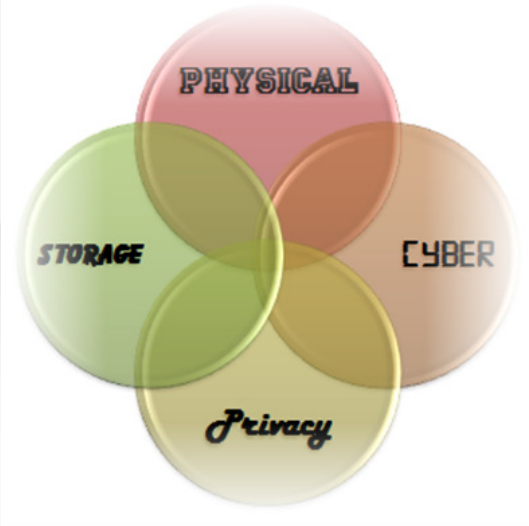
© Verizon 2011 – All Rights Reserved

Who Are the Hackers?

- **Who are they?**
  - Petty Criminals
  - "Script Kiddies"
  - Experimenters / Technicians
  - Disgruntled Employees
  - Your Competition
  - Organized Crime
  - Terrorists (Religious, Environmental, Political)
  - Nation States

© Verizon 2011 – All Rights Reserved

"LAYERS" OF CONCERN



© Verizon 2011 – All Rights Reserved

Physical Layer Security

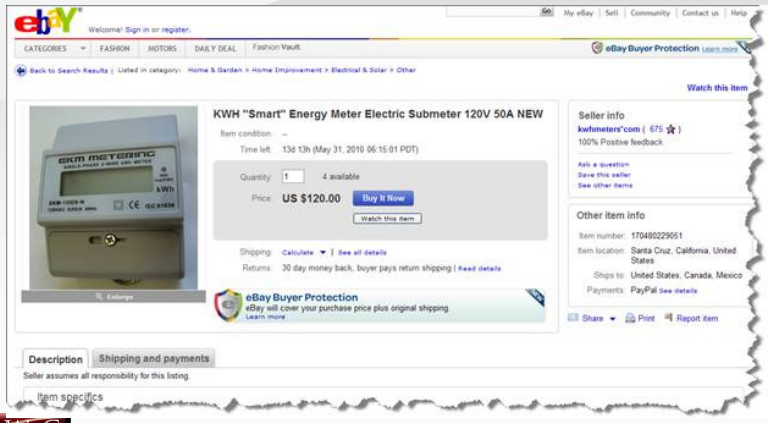
- **Natural Disasters**
  - Snow Storms
  - Hurricanes
  - Solar Flares
  - Geomagnetic Storms
  - Earthquakes
  - Flooding
  - Volcanoes
- **Recognize that Location of the Smart Grid Components Can Be Affected by the Surrounding Environment**

© Verizon 2011 – All Rights Reserved

Physical Layer Security (2)

RESPONSE: METER "LAST GASP" ALERTS WHEN DISCONNECTED

- **Steal the Meters – Sell the Devices**



© Verizon 2011 – All Rights Reserved

Physical Layer Security (3)

- **Tamper with the Meter**
  - Cause Meter to Stop Reading - Disconnect
  - Cause Meter to Mis-Read (or Reverse)
  - Inject Malware
  - Modify Encryption
  - Modify Authentication Mechanism

Proof of Concept

Black Hat BRIEFINGS AND TRAINING

IOActive™ COMPREHENSIVE COMPUTER SECURITY SERVICES

- July 2009 – Black Hat Conference
- IOActive, Seattle InfoSec Firm
- **Proof of Concept** – 24 Hours Caused 15,000 of 22,000 Home Smart Meters Taken Over by Malware/Worm

© Verizon 2011 – All Rights Reserved

“Distraction Attack”

- **Diversion to Roll Maintenance Trucks**
  - Chaos and Costly
  - Unavailability of Crews for “Real” Problems
  - Preparation for “Next Phase” of Attack

© Verizon 2011 – All Rights Reserved

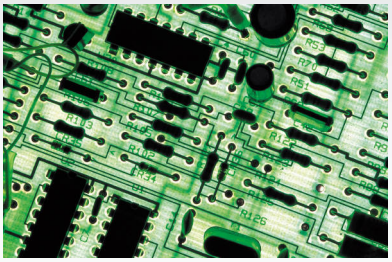
Physical & Cyber

- **Opening the Meter**
  - Accessing Exposed Ports and Connectors
  - Intercept Data Between Microcontroller and Radio
- **Infrared Port Attack/Hack**

© Verizon 2011 – All Rights Reserved

Cyber Layer Security

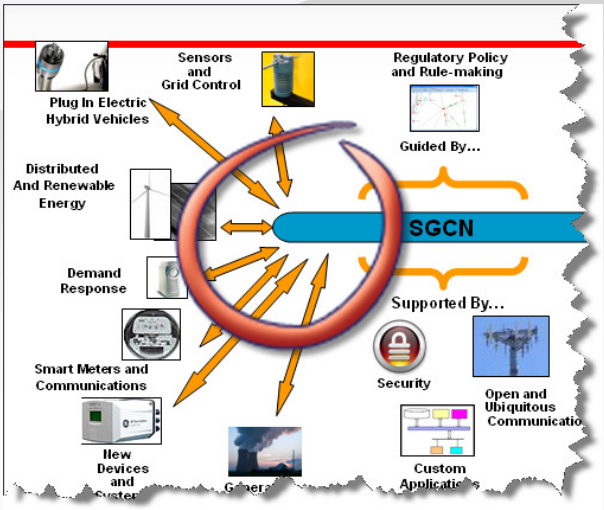
- The Biggest Opportunity for Trouble
- "The Last Mile" Issues
- Remember – Added Complexity Causes Concerns



© Verizon 2011 – All Rights Reserved

"Last Mile"

- Broadband Power Line Systems
- Power Line Carrier Systems
- Public Switched Telephone Network (PSTN)
- Cat5/6 Network Connection
- Radio Frequency
  - WiMax
  - ZigBee
  - 6LoWPAN
  - 802.11x
  - Cellular (CDMA/EVDO, GSM, LTE)



© Verizon 2011 – All Rights Reserved

Second Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements – Feb 2010

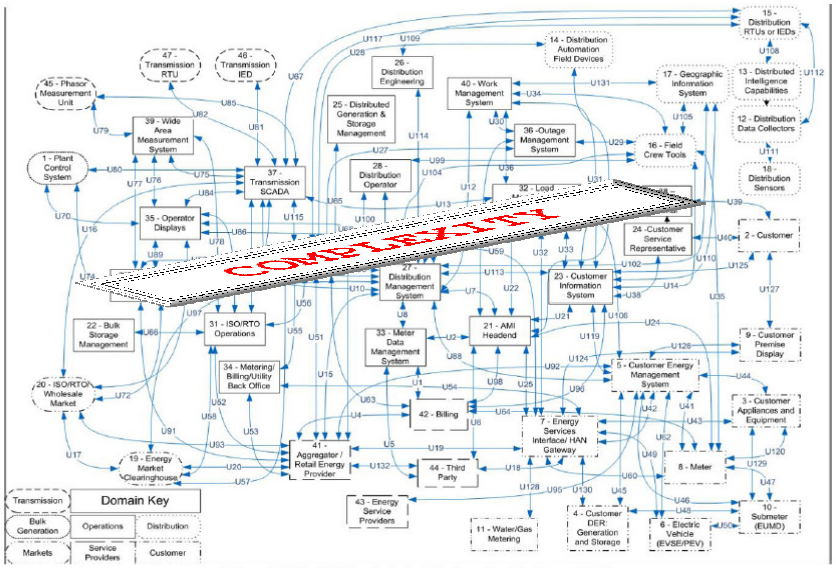
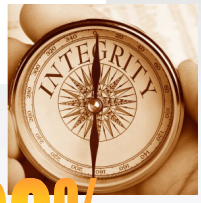


Figure 2.1 Unified Logical Architecture for the Smart Grid

© Verizon 2011 – All Rights Reserved

Cyber Attacks

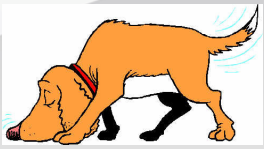
- **Remember C I A**
  - Confidentiality Attacks
    - »Reading, "Sniffing" the data
  - Integrity Attacks
    - »Changing the Data
  - Availability Attacks
    - »Denial of Service – Prevent Use of Service



99.9999%

© Verizon 2011 – All Rights Reserved

Confidentiality Attacks

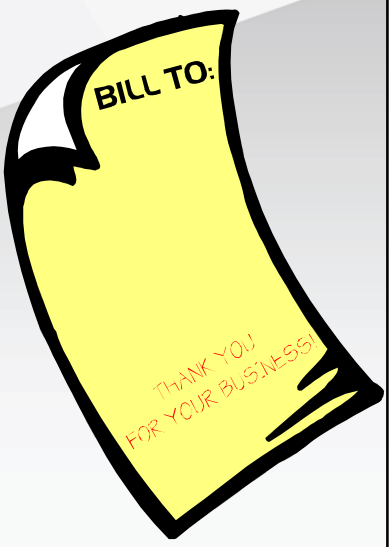


- **Buffer Overflow**
  - Inject Data that is too "Big" for the Meter/System
  - Predominantly Caused by Bad Software Development
- **Snooping / Sniffing**
  - Reading / Capturing the Data between Meter and Collector and Vice Versa
  - Also Internal to Meter Between Microcontroller and Radio
  - A Reason for Encryption – "Cleartext is Bad"
- **Hacking the Encryption**
  - Some Protocols Easy to Break
  - Causes – Weak Keys, Weak Protocols, Weak Initialization Vectors
  - Man-in-Middle Attack
  - "Bit Flipping" Attacks (Weak Integrity Functions)
- **Breaking Into Password Storage on Devices**
- **"Race Condition" Exploits**
  - A race condition is of interest to a hacker when the race condition can be utilized to gain privileged system access.

© Verizon 2011 – All Rights Reserved

Integrity Attacks

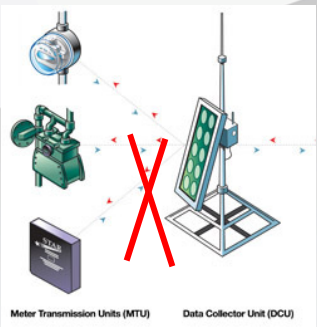
- **Key: Change the Data**
- **Replay Attacks (Man-in-the-Middle)**
- **Why?**
  - Change the Bill (Up or Down)
  - Modify Usage Data
  - Use Data for Fraud
  - Use as Alias
    - »"Gee Officer, I wasn't home that night!"



© Verizon 2011 – All Rights Reserved

Availability Attacks

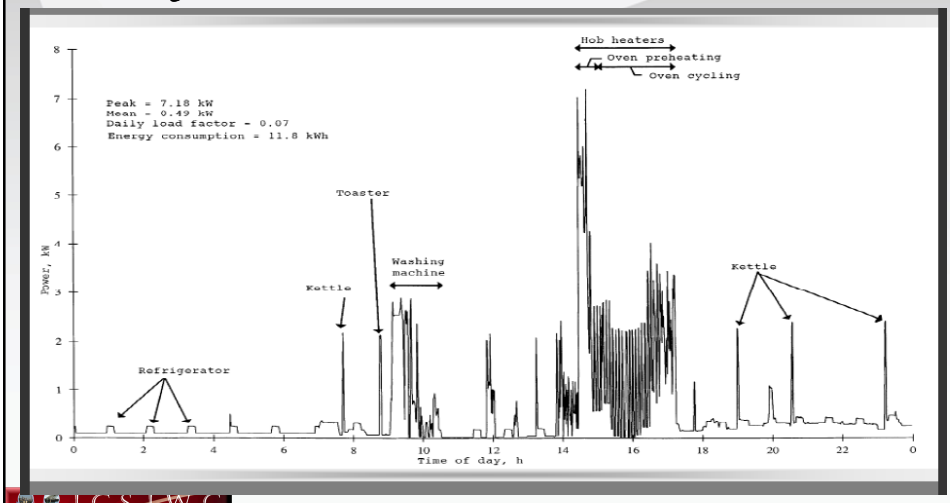
- **Denial of Service (DoS) Attacks**
  - Examples: Georgia Cyber War, Estonia Cyber War
- **Spoofing**
  - Pretending You are Another Meter
- **Meter Authentication Weaknesses**
  - Manipulate Meter to Collector
  Or
  - Manipulate Collector to Meter
- **Name Resolution Attacks**
  - Meter Name Cache Poisoning
  - Denial of Service Attacks Against DNS Servers
  - Reroute Meter Traffic to Another Meter or Collector or Network
- **Hold Ransom**
  - Before Super Bowl?
  - Over a Community/Neighborhood?
- **Wartime Reserve**
  - Chipset Backdoor "Pre-Attack" in Smart Meters



http://www.aclaratech.com/AclaraRF/PublishingImages/starsystem_th.jpg

© Verizon 2011 – All Rights Reserved

Privacy Attacks



http://www.dora.state.co.us/puc/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf

© Verizon 2011 – All Rights Reserved

Privacy Attacks (2)

- Determine Lifestyles
- Determine Best Time to Rob
- Use Info to "Sell" Services (e.g., "I'm here to fix your broken refrigerator, Ma'm!)

http://www.baystatetech.org/graphics/major-app.jpg

© Verizon 2011 – All Rights Reserved

STORAGE ISSUES

A Paradigm Shift

Microsoft Clip Art Online

www.smartgridnews.com

Today's Environment	The Future Smart Grid
Analog Meters or Simple Digital Meters Manually Read or Use "Drive By" Reading	"Smart" Digital Meters & "Smart" Sensors
Read Monthly (or Less Frequently)	Automatic Reading
Minimal Data Accumulation	Read Every ~15 Minutes or More Frequently
Simple Data Fields – KWH Used Since Last Reading	"Data Avalanche!" – Numerous Data Fields and Classes

Microsoft Clip Art Online

Microsoft Clip Art Online

Circuit Breaker ENHayden - Used with Permission

Relays – ENHayden -- Used with Permission

Microsoft Clip Art Online

www.smartgridnews.com

© Verizon 2011 – All Rights Reserved

Types of Data – Data Classes*

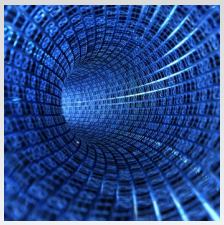
- **Electric/Operational:**
  - Represents electrical behaviour of the grid from intelligent network and smart meter devices
- **Asset Condition/Health:**
  - Represents the condition, health, and behaviour of the assets Meter Use
  - Includes data on total power usage and demand values, such as average, peak, and time of day
- **Events:**
  - Consists of asynchronous event messages from Smart Grid devices (e.g., fault detection events)
- **Metadata:**
  - Holistic view of all Smart Grid data, thus allowing for organization and analysis of other data classes
  - User Usage (Privacy Impacts):
    - » Includes a representation of the user's electric use that can be used to determine actions that could be viewed as private

*Initial Points from Accenture, *http://www.accenture.com/NR/rdonlyres/E1F7B159-1B75-4D42-BEA6-3A4CCAB1D564/0/Accenture_Utilities_POV_SmartGridDataMgmt.pdf*

© Verizon 2011 – All Rights Reserved

Is it an Avalanche? Tsunami?

- **Example #1:**
  - United Kingdom* – 44M Homes → 88M data entries per year
  - Under a new, 2-way, Smart Grid, new meters would create 32B data entries per year. (363 times *more* data per year!)
- **Example #2:**
  - Pacific Gas & Electric*:
    - » 170 MB of Data per Smart Meter per Year
    - » 100,000 Meters → 17 Terabytes per Year
    - » Prediction for U.S. by 2019 → 100M Meters → 100 Petabytes generated during the next 10 years
- **Example #3:**
  - Austin Energy**:
    - » Moving from monthly to hourly reads increases data handing >730 times
    - » Phase 1 Roll Out of 500,000 meters → Yearly data storage from 20TB to 200TB (with disaster recovery redundancy)



http://obiblog.files.wordpress.com/2008/08/data-pic.jpg

1 Petabyte is 1000 Terabytes!

References:

*http://redtape.msnbc.com/2009/10/would-you-sign-up-for-a-discount-with-your-power-company-in-exchange-for-surrendering-control-of-your-thermostat-what-if-it.html and

**http://neuralenergy.blogspot.com/2009/06/smart-meter-data-management.html

© Verizon 2011 – All Rights Reserved

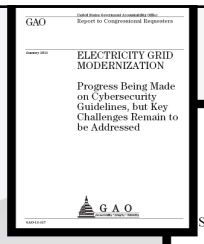
Storage Considerations

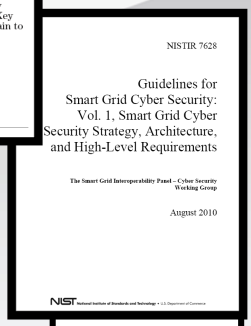
- Costs for More Data Centers and Storage
- Error Handling
- Data Analytics and Business Intelligence Resources
- Security of Data – Static and Dynamic… Stored or in Transit
- Privacy of Data – Consider EU Privacy Laws
- Consumer Education Requirements
- Auditing, Reporting, Regulatory Impacts

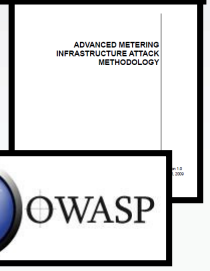
© Verizon 2011 – All Rights Reserved

What To Do?

- #1: DON'T GIVE UP!
- #2: DON'T IGNORE THE THREATS!
- #3: LEARN AND STUDY – DO THREAT MODELING
- #4: INCLUDE SECURITY, IT, UTILITY OPERATIONS IN PLANNING AND SOLUTION DEVELOPMENT
- #5: WORK WITH SECURITY EXPERTS & CONSULTANTS
- #6: ASK HARD QUESTIONS
- #7: BUILD DEFENSE-IN-DEPTH IN EVERY PHASE OF YOUR SMART GRID SOLUTION
- #8: INCIDENT RESPONSE SET UP, PRACTICED
- #9: STORAGE – PLAN, IDENTIFY CONTINGENCIES, LOOK OUTSIDE THE BOX
- #10: INCLUDE SECURITY EARLY, OFTEN


GAO
Report to Congressional Requesters
ELECTRICITY GRID MODERNIZATION
Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed


NISTIR 7628
Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
The Smart Grid Interoperability Panel – Cyber Security Working Group
August 2010


ADVANCED METERING INFRASTRUCTURE ATTACK METHODOLOGY

OWASP

© Verizon 2011 – All Rights Reserved

QUESTIONS? OBSERVATIONS?

© Verizon 2011 – All Rights Reserved

Ernie Hayden CISSP CEH
Managing Principal – Energy Security
Global Energy & Utility Vertical
Verizon Business
206-458-8761
ernest.hayden@verizonbusiness.com

© Verizon 2011 – All Rights Reserved