GSGF>>REPORT

SMART_METER_SECURITY_SURVEY

AUG_2016

THE GLOBAL SMART GRID FEDERATION (GSGF: HTTP://WWW.GLOBALSMARTGRIDFEDERATION.ORG/)

The Global Smart Grid Federation (GSGF: http://www.globalsmartgridfederation.org/) is committed to creating smarter, cleaner electricity systems around the world. By linking the major public-private stakeholders and initiatives of participating countries, the federation shares best practices, identifies barriers and solutions, fosters innovation, and addresses key technical and policy issues. These and other activities help member organizations initiate changes to their country's electric systems to enhance security, increase flexibility, reduce emissions, and maintain affordability, reliability, and accessibility of electricity.

The Global Smart Grid Federation also works with the International Smart Grids Action Network (ISGAN: http://www.iea-isgan.org/) as well as with national and international policymakers to address the broad challenges of deploying smarter grids. This nexus provides bidirectional communication and collaboration, which envisions accelerated deployment of smart grids around the world and facilitates consensus-building within the international community to address concerns related to electricity systems and climate change.

EXECUTIVE SUMMARY

The Work Group on Cyber Security was formed by GSGF in May 2015 to examine security issues in various segments of the smart grid eco-system. This report discusses such issues in smart meters and the associated advance metering infrastructure. It is expected that the global smart meter deployment would cross 800 million by 2020. Several geographies including North America and Europe have achieved a significant portion of their targets already. Smart meters will provide a platform to utilities for optimizing their overall infrastructure, improving efficiency and managing demand-supply in a better way. While these are significant benefits, it is also understood that as software and communications become more pervasive, systems will become prone to previously alien issues – security being one of them.

In this report, we attempt to provide a global picture of the smart metering rollout while illustrating the nuances in system architecture. We then point out several challenges from a privacy and system security standpoint that must be addressed at the design and rollout phase. The objective is to highlight the fact that security and reliability can't be isolated from each other. For a system to be dependable, security is just as important as reliability.

WORK GROUP PARTICIPANTS

Country	Members
Australia	Guo Chen, Andy Zhao
Belgium	Steven Frere
Denmark	Helle Juhler-Verdoner
France	JP Mennella
India	Reji Kumar Pillai, Hem Thukral, Shailendra Fuloria (Chair)
Ireland	Michael Callan, Lee Hayward, Jon Longstaff
Israel	Mati Epstein, Erez Koren, Gabriel Mazooz, Amit Slutzky, Yehonatan Kfir
Japan	Yuichiro Shimura, Yoshiko Kawai
Korea	Gun Hee Lee
Netherlands	Johan Rambi, John Post, Igor van Gemert, Carlos Portes Montela
Turkey	Murat Sirin

TABLE OF CONTENTS

1 INTRODUCTION

The current electricity infrastructure in most countries emerged several decades ago when local generation and distribution facilities were merged into national or regional power grids. Electricity is produced by a small number of large generators, fed into a high-voltage transmission grid that transports it over long distances, and then stepped down at substations into medium-voltage distribution networks until it finally reaches the customer's homes and businesses. The electricity meter at the customer premises records consumption and the customer is billed once per billing cycle. This is now changing.

In the last decade, most countries have committed to adopt changes in technology to enable them to meet targets on sustainability and ensure security of energy supply. This is changing not only the physical infrastructure of the power infrastructure but also the regulatory environment that governs the system and ultimately the relation between the utility and the customer. Smart meters are looked upon as one of the means that will help transform the energy delivery network into a two-way information system; it can signal price changes to the customer who in turn will be able to set rules so that heavy-load appliances such as dishwashers, air conditioners, electric cars etc. can be used when the tariff is cheapest. This will make demand elastic to the supply and in turn result in a 'demand response' that will help utilities manage peak demands as well as fluctuating generation resources like solar and wind. Peak demand shaving will help governments meet energy security goals and will also save utilities money, as customers on day-night tariffs are typically paying less than the wholesale cost of energy during the peak[1]. However, smart meters also raise several serious security issues which we discuss in this report.

The American Recovery and Reinvestment Act started the move towards the deployment of the new 'smart grid'. The European Union's response in 2009 was a Directive requiring all Member States to conduct an economic assessment of smart metering; states who find it to be beneficial must ensure full rollout by the year 2022 with 80% completion by 2020.

Several other countries have subsequently enacted legislation mandating adoption of smart meters as part of broader clean energy initiatives. In 2008, the United Kingdom mandated that 53 million smart electric and gas meters be deployed in homes and businesses by 2020. In China, the government released its smart grid plan (Special Planning of 12th Five-Year Plan (2011–15) on Smart Grid Major Science and Technology Industrialization Projects) in May 2012, calling for massive investment in smart grid technology. As part of the plan, the State Grid Corporation of China (SGCC) announced that it would deploy 300 million smart meters by 2015 and close to 435 million meters eventually[2].

Many countries have deployed a significant number of smart meters and are now trying to leverage the platform to deploy services such as outage management, distribution management, home automation etc. that will improve the reliability indices of the utility as well as ensure efficient use of manpower. While utilities can realize substantial benefits from smart meters and associated platforms, there are also concerns from a security standpoint with a risk of widespread fraud if a security vulnerability is industrialized. Manipulated meter readings can lead to substantial revenue loss for the utility. Presence of features such as a remote connect/disconnect switch can lead to a strategic vulnerability if an adversary is able to get the ability to turn off power from millions of households. Regulation and universal standardization would need to be just right – lack of it can lead to interoperability issues thus limiting the overall benefits a consumer and the industry can get from the ecosystem.

The rest of this report is organized as follows: In Section 2, we talk about the global smart meter deployment scenario and roadmap and Section 3 discusses various smart metering and associated infrastructure that are being implemented across these countries. Finally, through Section 4, we discuss the various security and privacy challenges that are associated with these architectures and how the rollout projects are addressing them.

2 SMART METERS: DEPLOYMENT AND ROADMAP

It is anticipated that almost 800 million smart meters would have been installed globally by 2020. While Europe leads the penetration rate – growing from 15% in 2010 to 85% in 2020. When the rollout is complete, China would see the largest install base with over 435 million meters followed by the United States with 135 million meters.

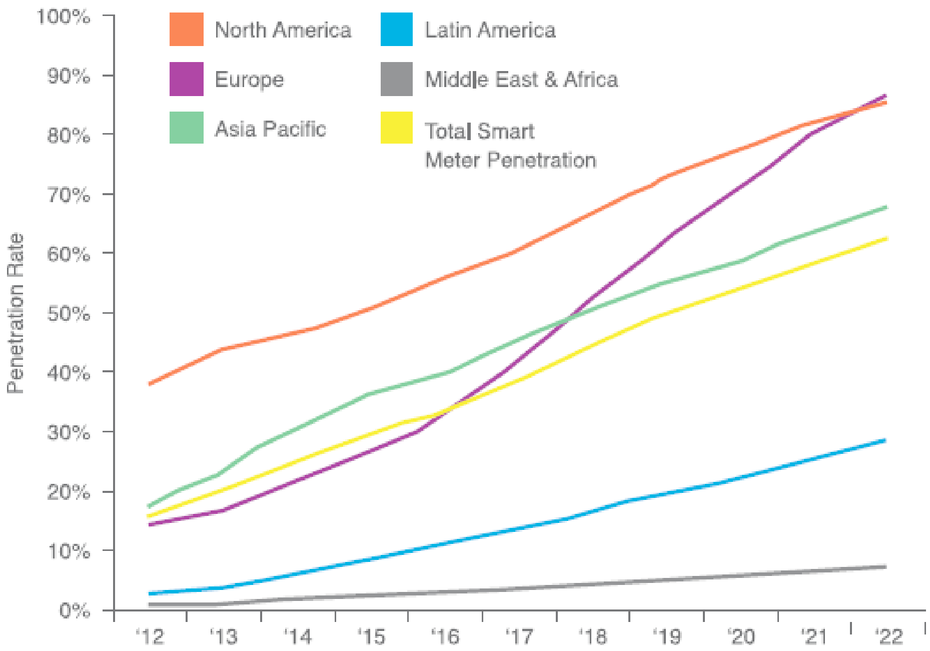


Figure 1: Smart Meter penetration rate (Source: Navigant Research)

The US was one of the first countries to adopt a smart grid and a smart metering charter through the Energy Independence and Security Act (EISA) of 2007 and the American Recovery and Reinvestment Act (ARRA) through which the country committed to transform the existing electricity infrastructure into a smart grid. The Edison Foundation's Institute for Electric Innovation suggests that more than 50 million smart meters have already been deployed / replaced in the US till date[3]. Pacific Gas and Electric (PG&E) already completed 100% rollout of 5.14 million smart meters in 2013 itself. Customers can now participate in PG&E's SmartRate plan, a voluntary critical peak pricing (CPP) rate plan that will help manage system load during hot summer days, and receive notifications of when they are moving into higher-priced electricity tiers. South California Edison (SCE) which has rolled out roughly 5 million smart meters also offers similar critical peak pricing voluntary programs to its customers. Utilities such as Oncor, Alliant Energy, Arizona Public Service, Center Point Energy, Central Maine Power Company have also achieved 100% rollout.

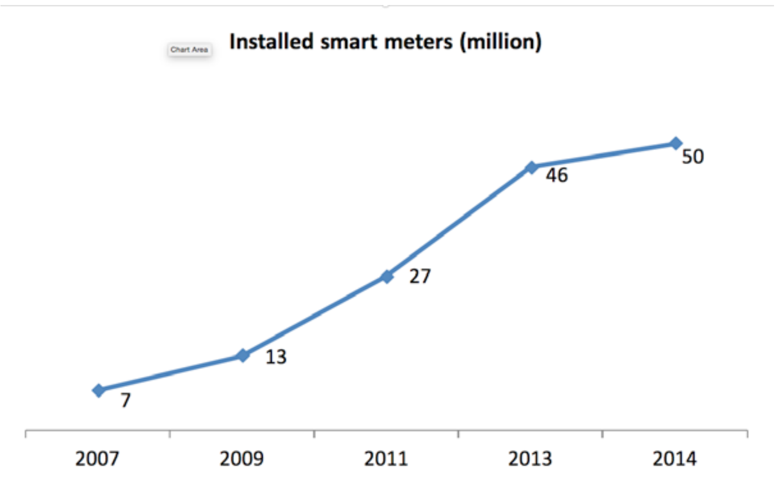


Figure 2: Smart meter installation in the US

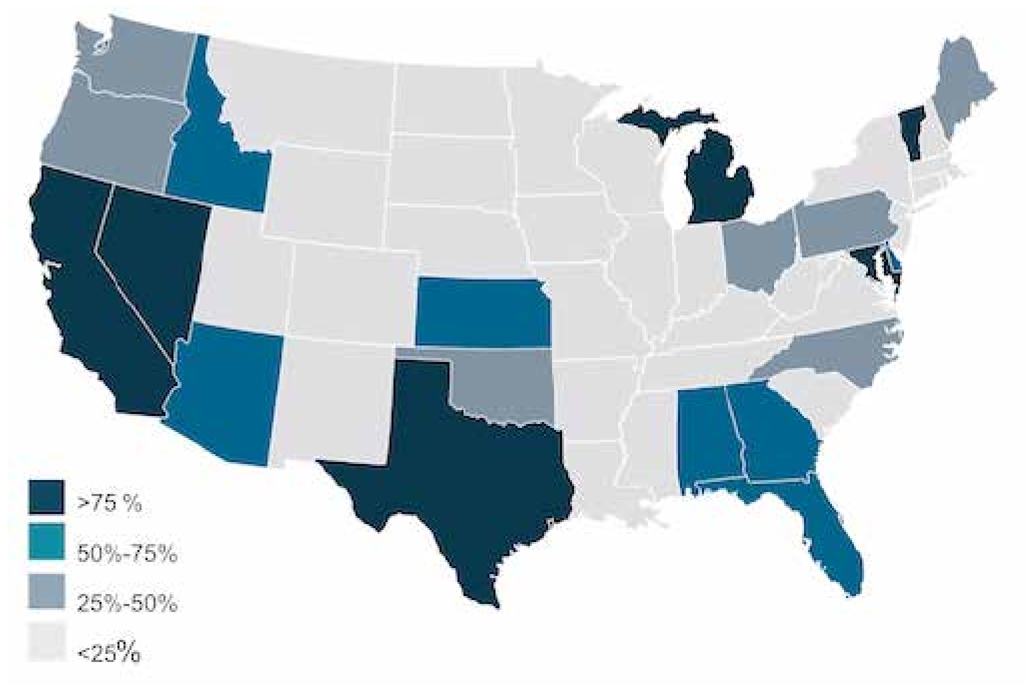


Figure 3: Smart meter penetration in the US (Source: GTM Research)

The UK government expects that the roll-out of smart meters will play an important role in Britain's transition to a low carbon economy and help meet some of the long-term challenges in ensuring an affordable, secure and sustainable energy supply.

The Smart Metering Program, being led by the Department of Energy and Climate Change (DECC), is aimed to have around 53 million smart meters by 2020. Energy suppliers are responsible for planning, delivering and installation of smart meters for their customers and are free to plan the roll-out in a way that suits their business and the needs of their customers, subject to the requirement to complete the roll-out of 53 million smart meters by the end of 2020. The rollout has accelerated since 2013 with 1.3 million smart meters installed by the 9 major energy companies till mid-2015[4].

Despite a relatively low starting point, policy at the EU and national levels is pushing smart meter initiatives ahead quickly so as to meet the EU's 2020 energy efficiency targets. The Energy Services Directive (2006/32/EC) identified smart meters as one of the main ways to achieve an improvement in energy efficiency. The Electricity Directive (2009/72/EC) mandates that at least 80 percent of consumers must have smart meters by 2020 subject to positive economic assessment of the long-term costs and benefits, to be carried out by each member state. The EU's smart-meter rollout is underway. By mid-2011, an estimated 42.3 million smart meters had been installed in the EU, mainly as the result of large rollouts in Italy, Sweden, Finland, and Denmark[5].

China has become the world's largest market for smart electricity meters as a result of several initiatives by the Chinese national government. The installed base of smart meters in China is expected to grow from 139 million units in 2012 to 377 million units by 2020, reaching 74% market penetration[6]. Reportedly, China's customer base demands smart meters at price points of less than $50 per unit for residences, less than half of the typical price in North American and European smart meter markets[7].

The Ministry of Power in India has been promoting investment in smart grid technologies in recent years to cut Aggregate Technical and Commercial (AT&C) losses, which are as high as 25-30%.. India ranks third in the world for smart grid investment, after the United States and China. India Smart Grid Forum (ISGF), a public-private initiative of the Ministry of Power, worked on the development of cost-effective smart meters in 2011 and worked with the Central Electricity Authority (CEA) for the formulation of functional requirements and technical specifications for smart meters which was published in June 2013. Subsequently, the Ministry of Power advised the Bureau of Indian Standards (BIS) to formulate standards on smart meters. In August 2015, BIS published the new Smart Meter Standard, IS 16444: AC Static Direct Connected Watthour Smart Meter – Class 1 and 2 Specification covering Single phase energy meters; three phase energy meters; single phase energy meters with Net Metering facility and; three phase energy meters with Net Metering facility. Another standard IS 15959: Data Exchange for Electricity Meter Reading, Tariff and Load Control — Companion Specification has been revised and published as IS 15959: Part 2-Smart Meter in March 2016.

The 'Ujwal Discom Assurance Yojna' (UDAY), announced recently in November 2015, has set a target of installing 35 million smart meters by December 2019. Consumers having a monthly consumption of greater than 500 units will get a smart meter in Phase 1 of this initiative. In Phase 2, smart meters will be deployed for consumers with monthly consumption greater than 200 units.

Since the Great East Japan Earthquake in 2011, Japan has taken approaches to rely less on nuclear power and to accelerate promotion of renewable energy and smart grid. the Energy-Environment Council was established to develop the policy response to ensure a safe, stable, efficient, and environmentally-friendly energy system. . The council issued a report in July 2011 which emphasized the need for efficiency and conservation measures as well as supply-side measures, including introducing smart meters and a diversified electricity tariff system[8]. The number of smart meters installed in 2014 nationwide was 3.66 million, and the planned figure for fiscal 2015 was 7.5 million. About 12 million smart meters are planned to be installed annually for 3 years starting 2016. By 2019, Japan would have rolled out close to 48 million smart meters[9].

Korea's push for smart meters is part of the Smart Grid Initiative announced by the Korean central government in 2009. Spearheaded by a demonstration project on Jeju Island, the initiative is intended to help reduce overall energy consumption by 3 percent and cut electricity consumption by 10 percent by 2030[10]. Korea's primary government body responsible for energy policy, the Ministry of Knowledge, plans to replace all household analog meters with smart meters by 2020. Currently, the Korea Electric Power Company (KEPCO) is focused on installing smart meters for residential customers, which make up about 14 percent of national energy consumption. KEPCO plans to roll out smart meters to about half its households (about 10 million units) by 2016[11].

Apart from the US, Canada has been at the forefront of smart meter installations in North America. Canada's power infrastructure must stay advanced to counter challenges of vast distances and hostile terrain separating major power generating resources from consumers[12]. The Canadian smart meter industry spurred into action by the National Clean Energy Fund in 2009, under which $200 million was allocated towards smaller-scale demonstration projects of renewable and alternative energy technologies, including smart grids and smart meters[13]. British Columbia's 2010 Clean Energy Act required BC Hydro, the province's primary electricity provider, to install smart meters for all its nearly 1.8 million customers by the end of 2012[14]. In Ontario, the Smart Meter Energy Initiative was introduced in 2004 with installation targets of 4.3 million homes and small businesses by 2011, which was followed up by a 2010 mandate for time-of-use pricing[15]. With the addition of Hydro-Québec's plan to install nearly four million smart meters in the next several years, Canadian market penetration of households with smart meters should reach two-thirds by 2016[16].

Brazil and Mexico are among the top emerging markets for smart meters due to their rapid economic growth. Brazil's energy regulator, Agência Nacional de Energia Elétrica (ANEEL), had previously maintained that all electricity meters must be replaced by new smart ones. This would have resulted in about 63 million smart meters being rolled out[17]. However, this proposal hit a roadblock and the current plan is to have smart meters only for new installations and optional for existing customers. Mexico is the second-largest potential market for smart meters in Latin America, after Brazil, and is expected to have 21 million such meters installed by 2020[18]. Although Mexico primarily relies on mechanical meters and is behind the United States in smart meter installations, Mexico is seen as an emerging market for smart meters for its commercial customers.

There is no single uniform metering architecture that is followed globally, and for good reason. Countries have their unique requirements and the system is modeled to meet them. For example, the UK has 9 large energy suppliers that provide electricity using the distribution network owned by the Distribution Network Operators (DNO). The meters are owned by the suppliers and not the DNO. In nearby Ireland, it is the network operator that owns and maintains the meters and shares the reading with the energy company. Then there are countries like India where the market is still not fully deregulated and the supplier and network operator are one and the same.

The existing market and system architecture impacts the rollout of smart metering infrastructure. Italy has been the leader where Enel, the dominant utility, launched its `Telegestore' project and has now rolled out more than 32 million digital meters. These devices used narrow-band Power Line Carrier (PLC) Communication to pass on the consumption data to data concentrators, which in-turn pushed the data to Enel's enterprise servers. The meters primarily served the purpose of debt management through prepayment and included features to enable demand response and time-of-day tariff plans. Germany plans to integrate more than 25 GW of wind power into the infrastructure in the next 20 years. The 'Energiegesetz' entitles every customer to choose a 'meter point operator', essentially an energy service company that gets an annual fee for installing and maintaining a meter and can also sell the customer energy management services. This was a bold attempt to introduce competition into the market but did not really pick up. In the Netherlands, grid operators are responsible for installing and reading out smart meters and for offering services associated with market facilitation. The advanced metering infrastructure designed for this purpose has been set down in Netherlands Technical Agreement (NTA) 8130 of the Netherlands Standardization Institute (NEN). Grid operators will be responsible for implementing the requirements and measures and maintaining a reliable advanced metering infrastructure. Acting on the instruction of the grid operators, Netbeheer Nederland will be responsible for developing policy and will oversee correct implementation. In the current architecture, grid operators manage most of the functionality within the advanced metering infrastructure, including the information and communication technology on the smart meter. All systems and devices within the advanced metering infrastructure, from the meter up to and including the P4 interface of the grid operators, are included in the scope. This definition applies to all grid operators. The situation for grid operators that only have gas connections differs from that of other grid operators in that they only maintain a Central System (CS), which is fed via P4 from other Central Systems[19].

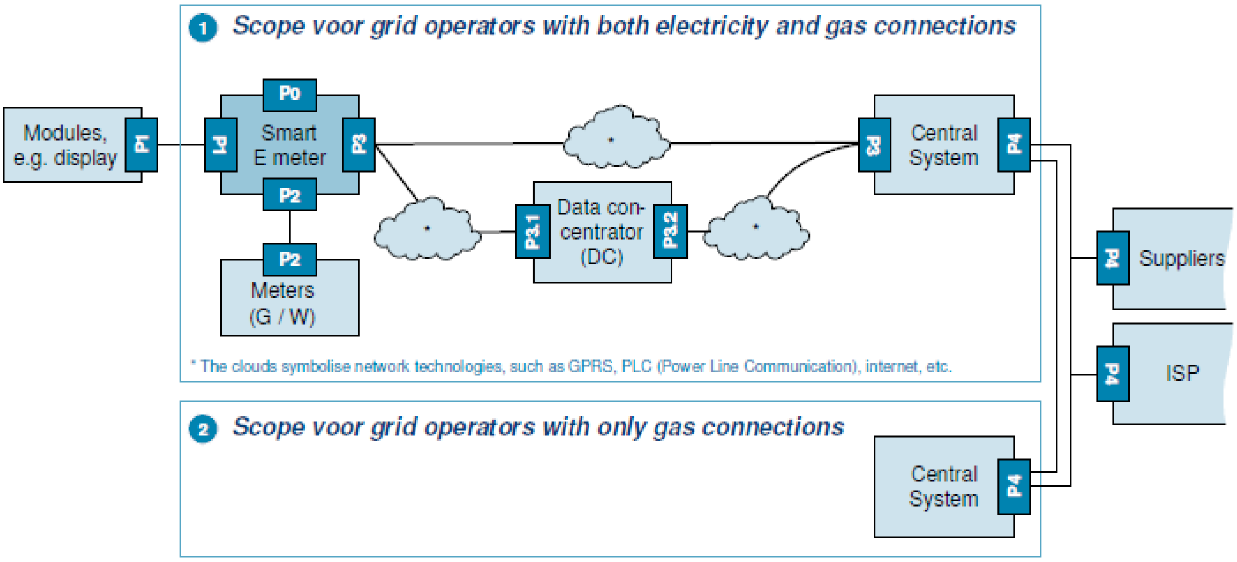

1 Scope voor grid operators with both electricity and gas connections
Modules, e.g. display
P1
P0
P1
Smart E meter
P3
P2
P2
Meters (G / W)
*
*
*
P3.1
Data con-centrator (DC)
P3.2
P3
Central System
P4
P4
Suppliers
P4
ISP
* The clouds symbolise network technologies, such as GPRS, PLC (Power Line Communication), internet, etc.
2 Scope voor grid operators with only gas connections
Central System
P4

Figure: Smart metering requirement scope in Netherlands

The UK has opted for a centralized architecture in which the government will license a Data Communications Company (DCC) to manage all 53 million electricity and gas meters in the country. The idea is that the DCC will act as a thin client and provide a control point from which data will be passed to energy retailers, network operators, the regulator, service companies and customers, as appropriate. It is also expected to keep down the cost of customer switching between retailers so as to protect market competition.

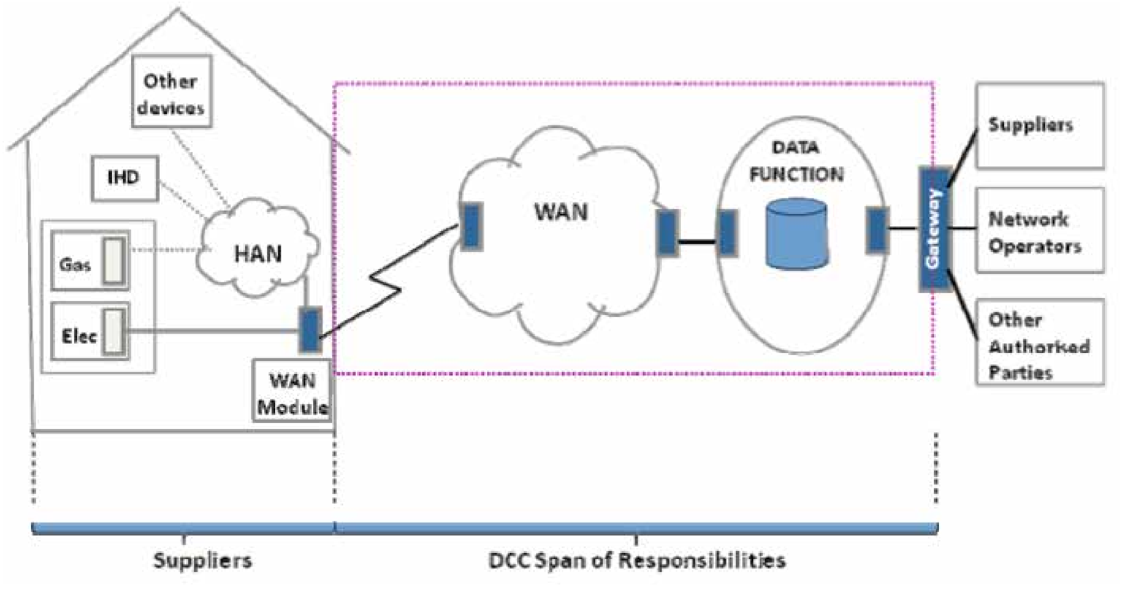


Figure: UK's smart metering architecture implemented through the DCC

Japan, on the other hand, has opted for a distributed architecture. The data from smart meters can be shipped to the energy utility through two mechanisms: In the first option, smart meter data is transferred to the Head End System (HES) and then to the Meter Data Management System (MDMS) both of which are owned and operated by the utility. The utility can share this data with a retailer or a third party with customer's consent. This is typically referred to as 'Route A'. The second architecture entails the transfer of smart meter data to a Home Energy Management System (HEMS) which then transmits it to a third party over the internet. This third party then shares the consumer data with the utility according to predefined agreements. The communication between the meter and in-home devices is referred to as 'Route B'. The one between the utility or HEMS in the home and a retailer or a third party is referred to as 'Route C'.

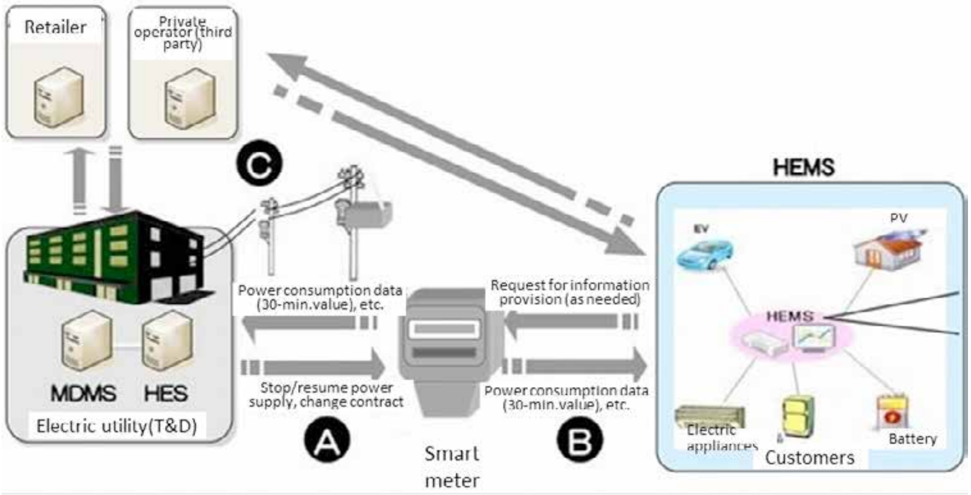
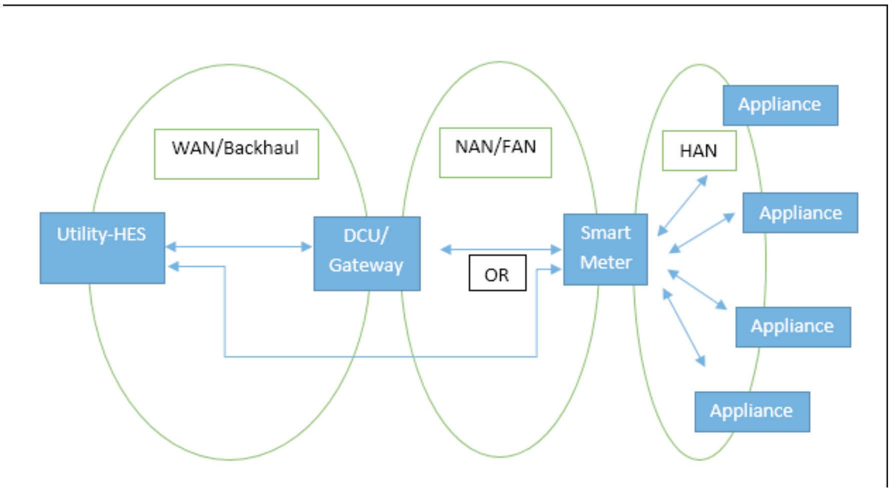

Retailer
Private operator (third party)
C
HEMS
EV
PV
HEMS
Power consumption data (30-min.value), etc.
Request for information provision (as needed)
Stop/resume power supply, change contract
Power consumption data (30-min.value), etc.
MDMS
HES
Electric utility(T&D)
A
Smart meter
B
Electric appliances
Customers
Battery

Figure: Smart meter architecture in Japan[20]

The AMI architecture is still evolving in India with a typical scenario as shown in the following figure:



There are no restrictions on the use of communication technologies in any segment of the infrastructure. A sample of technologies being discussed for each leg can be summarized as:

Technology/Protocol	Last Mile/NAN/FAN	HAN	Backhaul/WAN and Backbone
Wireless	6LoWPAN-based RF mesh, ZigBee, Wi-Fi	6LoWPAN-based RF mesh, ZigBee, Wi-Fi, Bluetooth, Z-Wave, NFC, ECHONET	Cellular, Satellite, LPWA, Long Wave Radio, TVWS, Private Microwave Radio links (P2P and P2MP)
Wired	PLC, Ethernet, Serial interfaces (RS-232, RS-422, RS-485), DSL	PLC, Ethernet, Serial interfaces (RS-232, RS-422, RS-485)	Optical Fiber, Ethernet, PLC, DSL

The most common features we see being implemented globally are:

- Daily collection of consumption data (typically 30-minute interval and register data)
- Collection of meter events
- Meter service switch / valve with remote disconnect / reconnect functionality
- Remote meter configuration
- Remote meter firmware upgrade
- Meter security services which support device authentication, encryption of data, role based access and validation of digital signatures prior to execution of remote commands or firmware upgrades

Having discussed the common features and architecture, we next discuss the security and privacy landscape across meter deployments.

4 SECURITY AND PRIVACY LANDSCAPE

It has been well established that systems fail not only due to technical reasons, but more so because the responsibilites and incentives to protect them are not well defined[21]. Most smart metering projects involve the following:

- In most countries, the Distribution System Operator (DSO) or the Distribution Network Operator (DNO) has been typically responsible for maintaining the reliability of the distribution network. In smart metering projects, they will also be responsible for the overall reliability of the new infrastructure that is rolled out.

- The electricity Suppliers/Utilities typically use the distribution network to ensure a reliable supply of power to the end consumer. They maintain the billing system and other associated systems for customer relationship management, payment portals and enterprise IT management.

- The energy regulator typically has the responsibility of maintaining checks-and-balances to ensure that the energy market and overall infrastructure works efficiently.

The finer details of the architecture vary across countries. For example, the meter at the consumer's premises is owned and maintained by the network operator in some and by the energy supplier in others. Such nuances will determine the roles and responsibilities of the stakeholders when it comes to security. If Alice guards a system while Bob pays the price of failure, we can predict that such a system will eventually fail[22]. The complex supply chain in the overall eco-system further demands that roles and responsibilities for security and reliability must be defined clearly upfront. For example, in the UK, the meter ownership rests with the energy supplier but customers can switch from one to the other (just like you can switch between your mobile network operators or internet service providers). How do we fix liability when a vulnerability is discovered in a meter that a particular supplier inherited from another? In such a complex eco-system, the role of the energy regulator would span further than ensure ethical market practices – it would also have to assure the overall security design across the industry. This will be a step change for all stakeholders but will have to be taken nonetheless to ensure that the electric system continues to work in a dependable manner.

The network operators as well as the energy suppliers will have to conduct frequent Vulnerability/Threat/Risk assessments on their systems to ensure that they understand the system risks as it evolves and appropriate mitigation actions are planned. NERC-CIP Version 5 has already introduced a new standard (NERC-CIP-010-1) to mandate such audits at a defined time interval. The energy regulator must play a significant role in ensuring that such activities are monitored at a defined frequency.

Incident response and management is another critical area where it is critical to have pre-defined responsibilities for all stakeholders in a complex socio-technical system such as the power infrastructure. The US utilities are mandated through NERC-CIP-08-V5 to have in place a well-defined process to identify, classify and respond to cyber incidents. There must be a clearly defined incident management team and an incident handling procedure that they must follow at times of crisis. While other geographies like Europe and India are working on similar mandatory standards, they are yet to evolve to a mature state. This is absolutely critical for the dependable functioning of the multi-stakeholder modern electricity infrastructure where information sharing between multiple principals during crisis would be inevitable.

In 2014-15 India Smart Grid Forum (ISGF) and NCIIPC (National Critical Information Infrastructure Protection Center) together conducted a survey of 7 leading utilities in India to understand the cybersecurity culture and level of preparedness in each organization, commencing from the senior most management, to the actual ground / operational personnel, including those in departments not traditionally associated with cyber security such as Legal or Human Resource Development. The top 10 findings and recommendations of the exercise are now published. More such exercises would be needed globally to identify the cybersecurity postures of utilities and provide them a foundation to lay out their roadmap. The top 10 findings and recommendations are mentioned in Annexure A.

4.1 Fraud

Detecting and preventing meter fraud has been a challenge for energy suppliers ever since electricity began to be sold as a commodity. In the early days, when metering technology was primitive, a lighting strike often demagnetized the meters and made them ran faster than normal. Often, utilities quietly chose not to repair them. Soon the customers began to realize that they were being ripped off, and the economic climate during the Great Depression further motivated unhappy customers to seek ways to cheat their utility. The 1930s saw a wave of fraud cases[23,24,25]. The industry responded by installing feeder meters that record the electricity supplied to a few dozen houses so it can be balanced against individual consumption; the National Electric Code was modified to have the meter installed outside the customer's house where utility staff could easily read it and inspect it for tampering; anti-tampering mechanisms included wired lead seals; and electricity theft was made a criminal offence. As for consumer protection – against unreliable meters and the bigger threat of monopolistic behavior by the utilities – regulation was introduced; the view emerged that electricity could be most efficiently distributed as a regulated local monopoly.

Fraud is still an unsolved problem in many parts of the world (especially in developing countries). Energy companies will be OK with occasional, opportunistic fraud; what will be of concern is any means through which fraud can become widespread in a way that non-tech savvy consumers can exploit a technology in smart meters in a way that they report a reduced consumption.

4.2 Over the air upgrades

The industry generally believes that the firmware running in smart meters will have to be upgraded during its normal life-span, which could be up to 15-20 years. A technically similar mechanism could also be used to update meter configurations to modify business logic/ tariff plans, alarm and alert, network functionality, communication features and much more. A scenario where a person physically plugs-in his laptop to install new firmware in each of the millions of meters a country might have rolled out is considered infeasible for reasons of cost as well as limited manpower. 'Over the air upgrades' where the smart meter can be programmed with new firmware remotely is thus an attractive option. However, this much wanted feature does come with its share of potential risks. If proper security measures are not taken, an attacker can patch a meter with his own malicious firmware. The utility can cope if this attack leads to a localized compromise of a single meter. However, if the attack can be propagated to a larger install base, it can lead to serious problems; as we have already agreed, manually updating firmware isn't easy from a cost as well as manpower standpoint.

Designing a security system that stands the test of time for the next 15 years or more is a non-trivial task. Not only does one need to consider things like Moore's Law which will make it easier to factor large prime numbers over time, but also complex issues like secure key management over the entire life cycle of the meter. What happens if the key used to sign firmware upgrades is compromised? Security architectures outlining how such an event might be mitigated is beyond the scope of this document; we merely want to point out to the fact that this is a genuine problem which must be addressed at the design stage itself. Shipping out millions of meters without putting proper security controls and hoping to add security sometime during the lifecycle would be no more than wishful thinking.

4.3 Remote connect/disconnect

It is seen that moving customers from credit to prepayment meters reduces household energy use by almost 10% (a factor that was helpful in countries like South Africa, which suffered a supply crisis during the nineties). The same effect has been noted in Northern Ireland, which has a majority of prepayment meters, as well as in Russia and Brazil. The energy price suddenly becomes salient when people can no longer pay for electricity painlessly by monthly direct debit, but have to go to a vending station and either use their ATM card or hand over cash. Even prosperous people to whom the cost was of no real consequence would suddenly pay attention to how much they used. Prepayment is nonetheless of interest to investor-owned utilities, because of debt management. When a credit customer fails to pay their bill, the routine is to get a court order and send a team to replace their meter with a prepayment one. This is expensive, and the utilities prefer smart meters so that they can turn any meter into a prepayment one remotely.

In addition, with remote connect/disconnect becoming ubiquitous, the utility now has the option to remotely switch off the electricity supply to a consumer in case of non-payment of bill, meter being tampered, consumption exceeding the sanctioned load or in case of a pre-determined demand response event.

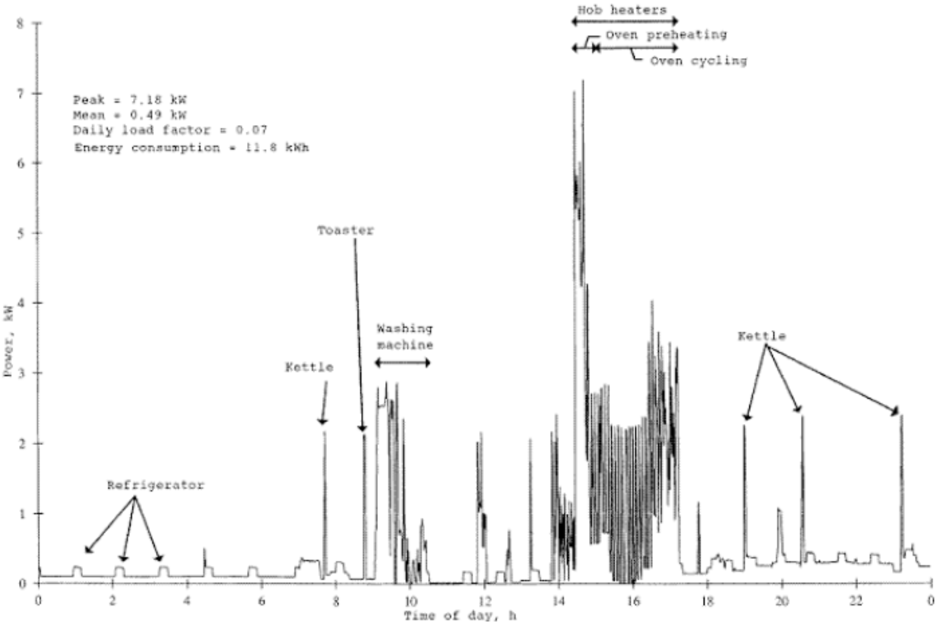
This functionality of remote connect/disconnect can however lead to serious strategic vulnerabilities – an attacker who can gain a head-end can remotely turn off the meters it can talk to. An attack on a higher level system can be even more devastating. Again, it will require well thought of security architectures to ensure that such a scenario does not happen and even if it does, there are built-in mechanisms which can let the utility wrestle back control of its meters from the attacker[26]. This is why appropriate security controls are required at a broader level (not just smart metering!). These security controls are both, technical and procedural in nature, and require the Chief Information Security Officer (CISO), in cooperation with the senior management, to show the way forward in securing the security landscape of the utility.

4.4 Privacy landscape and challenges

The Privacy Working Group of NISTIR 7628 mentions in its charter: 'The Smart Grid brings with it many new data collection, communication, and information sharing capabilities related to energy usage, and these technologies in turn introduce concerns about privacy.' A smart meter directly interfaces with the end user and is perhaps the most important component in the smart grid eco-system from a privacy standpoint.

A typical modern meter has two nested units: a core metrology unit which is tamper-resistant, factory-sealed, and exports a read-only database of readings; and a communications unit, sealed by the utility, that talks to the head-end and maybe to customer equipment, and also implements secondary metering functionality such as tariffs and prepayment functions. The energy management itself may or may not be centralized. In a decentralized architecture, the meter communicates with the utility once per time period[1]. It sends the energy usage in each billable time segment of the previous period and receives the prices for each slot in the next period (in the event that they were due to change). The meter may also receive real-time requests from the utility to shed load. The actual management is performed on the customer's premises, either by manual intervention or by a separate system under his/her control: this might be a wall-mounted display device replacing the current thermostat, or a local device that communicates with her home computer, laptop or mobile phone. It might well involve a third-party specialist company for energy management. In the centralised architecture, the meter passes detailed usage and home appliance information to head end, which in turn provides the customer with a web interface to manage energy use. Several US smart metering pilots and the UK have adopted this mechanism whereby half-hourly meter readings are gathered.

Smart meters vastly increase the amount and granularity of consumer data as related to the nature and frequency of energy consumption and generation, thereby opening up more opportunities for general invasion of privacy. Studies have shown that it is possible to identify some of the appliances through load monitoring. Such data might appeal to advertisers and law enforcment agencies alike.



The legal ownership of Smart Grid energy data is the subject of much discussion. Various regulators and jurisdictions have treated the issue of who owns energy data differently. However, regardless of data ownership, the management of energy data that contains or is combined with personal information or otherwise identifies individuals, and the personal information derived from such data, remains subject to the privacy considerations described in this report. It should be the responsibility of the custodian of energy data to ensure that the information gathered from multiple components of the smart grid is safeguarded[27]. From a privacy standpoint, it is important to clearly outline what data is gathered and how often. It is equally important to clearly identify mechanisms and duration of data retention as well as documented access control policies to this data.

In Europe, citizens have the right, under section 8 of the European Convention on Human Rights, to respect for the privacy of their family life. European privacy law was principally expressed in the IT sphere via the Data Protection Directive according to which personally identifiable information may be collected for the purpose of performance of a contract or enforcement of a legal obligation, but it may be processed only in so far as it is adequate, relevant and not excessive in relation to these purposes. This directive is now being replaced with the General Data Protection Regulation (GDPR) with a view to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU[28].

It is expected that after the GDPR is in place, the utilities will have to conduct a utility-to-customer Privacy Impact Assessment

[1] For example, the network companies and suppliers in Ireland are provided with actual meter reading(s) (usually 4 actual reads a year) or estimated meter reading(s) every two months and bill their customer on that basis. In Turkey, the consumption data is gathered on a monthly basis but instant data such as reactive index, maximum demand power, battery alert can be taken.

(PIA). A PIA is a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information. PIAs also define the measures that may be used to mitigate and, wherever possible, eliminate the identified risks. The privacy risks might be mitigated by policies and practices that are instituted throughout the implementation, evolution, and ongoing management of the eco-system. Some European countries like Netherlands have adopted a proactive role in ensuring that a PIA is done before and during the entire system management lifecycle[2]. They describe privacy-sensitive data as information that identifies or describes an individual and includes at least the following:

- Personal information, such as name, sex, age, etc.;
- Connection information, including address, town/city, connection type and EAN code, as this information can be traced back to a specific location and specific person(s);
- Consumption information ('measurement data') at the level of detail of quarterly, daily or weekly readings, as this can contain information about the private sphere;

Monitoring information, provided that this contains the kind of details or is sent with such a frequency that information about the private sphere can be derived.

The underlying principle being that information which is not required for billing purposes and despensing regulatory functions will not be communicated or stored. Information will be stored in one place as much as possible and will be deleted once no longer required for the above functions. It is the responsibility of the grid operator to take measures which ensure that collected data will be sufficient, relevant and not excessive and that no more data will be processed than is necessary.

Other European countries such as Ireland have also declared a Privacy by Design approach to smart meter rollout. The Irish Commission for Energy Regulation (CER), which is responsible for the National Smart Metering Program conducted a Privacy Impact Assessment in 2013 with an objective and published a whitepaper in July 2015 that identifies the data that will be collected from the meters[29]:

- Interval consumption data (normally at 30-minute granularity)
- Register values (cumulative and limited Time-of-Use registers)
- Events (Tamper, Outage, Voltage, Quality, Security, Clock Sync etc)

It will be interesting to see how much of the declared privacy by design approach actually gets implemented in deployment. The 'Meter-ON' project which constatnly monitored the progress of 8 smart metering projects across Europe did not note specifically about how privacy by design was being implemented in these projects. Other smart metering projects across India are also, at the moment, not looking at the privacy aspect arising out of fine grained data collection at all.

Also, it is important to note that data-collection is but one part of the overall privacy landscape. It is equally important to clearly articulate access control policies for such data – something which we did not find mentioned explicitly in most smart metering projects. Depending on the system architecture, the network operator or/and the energy supplier may be the custodian of this data. In many countries, regulation requires that meter data needed for billing purpose be stored for a prolonged period of time (7 years in Ireland for instance). It is however not yet clear whether all other data gathered from meters would also have to be (or should be) stored for such a prolonged duration. It is also important to note that information rests in more than one place in the entire infrastructure: meters, the head-ends and the back-end systems. We are yet to see how some of the guidelines on minimizing data retention in multiple parts of the eco-system and destroying it once no longer needed is being implemented in the rollout projects. The 'Meter-ON' project report does mention that out of the 8 projects reviewed, 7 had elements of security and they did so by "…the use of the cyber security mechanisms defined in the communication protocol used". However, any explicit information about where and how this data is being stored, the Confidentiality, Integrity and Availability requirements and how the role based access control is implemented and monitored is still missing. Most of the Privacy Impact Assessments highlight the importance of explicit consumer consent before the custodian of their data decides to share it with any other principal. Many of the project rollouts don't mention if they intend to share this data with anyone else and if so, what the mechanism to gather consent from consumers is.

[2] The Dutch First Chamber, in 2009, had declined to approve smart meter rollout on the grounds that the mandatory nature of rollout was inconsistent with their view of citizen's privacy and security.

5 CONCLUSIONS

The smart meter deployment would be one of the largest projects of its kind at a global scale with more than 500 million meters being rolled out in the next few years. While this will certainly help utilities know their customers and infrastructure better and make the overall system more efficient, there are important security concerns that should be factored in at the design and deployment phase to ensure that the electricity delivery system continues to be reliable. Security is hard – security for embedded systems is harder; but given the overall impact on the society, not having security controls in place is simply not an option.

In this report, we have surveyed the global smart metering deployment scenario and pointed out the associated security and privacy challenges. It will require that all involved parties—the equipment vendors, the network operators, the energy companies and the regulators come together to ensure that security and reliability are treated together and that the proper target is the sum of the two, namely dependability. Electricity should continue to be supplied out of the wall socket, regardless of the attempts of either Murphy or Satan to interrupt the supply[30].

REFERENCES

1. 'Smart Meter Security: A Survey', Ross Anderson and Shailendra Fuloria

2. Clean Energy Act, B.C. Reg. 368, S.B.C. 2010, c. 22, section 37.

3. The Edison Foundation, Institute for Electric Innovation, 'Utility-Scale smart meter deployments: Building blocks of the evolving power grid ', http://www.edisonfoundation.net/iei/Documents/IEI_SmartMeterUpdate_0914.pdf

4. Department of Energy and Climate Change, 'Smart Meters, Great Britain, Quarterly report to end June 2015', https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/459467/Smart_Meters_Quarterly_Statistics_Report_Q2_2015.pdf

5. "The Smart Grid in Europe 2012–2016," Van der Zanden, August 16, 2011.

6. PV Magazine, "Smart Meter Market Is Hotting Up in China," May 13, 2013.

7. Greentech Grid, "Some Snapshots of China's Smart Grid," June 25, 2013.

8. Institute of Energy Economics, Japan, "Japan Energy Brief," January 2012, 10–12.

9. Ministry of Economy, Trade and Industry "Challenges and measures for promotion of smart meters" December 2014, http://www.meti.go.jp/committee/summary/0004668/pdf/015_03_00.pdf

10. "South Korea's Smart Meters Program Averts Nuclear Need," Han, March 12, 2012.

11. "South Korea to Install Smart Meters," Han, February 28, 2012.

12. Global Market for Smart Electricity Meters: Government Policies Driving Strong Growth, https://www.usitc.gov/publications/332/id-037smart_meters_final.pdf

13. Northeast Group, LLC, Brazil Smart Grid: Market Forecast (2012–2022), April 2012.

14. St. John, "Brazil's Opt-In Smart Meter Future," August 21, 2012 St. John, "Brazil's Smart Grid Market to Reach $36.6 Billion," April 6, 2012.

15. PR Newswire, "Mexico Smart Grid Market to Reach $8.3 Billion," October 11, 2011.

16. Natural Resources Canada, "Backgrounder: The Clean Energy Fund," May 2009.

17. Navigant, "The Installed Base of Smart Meters," November 11, 2013.

18. Ontario Energy Board, "Smart Meter Initiative: Determination to Mandate," June 24, 2010.

19. Netbeheer Nederland, 'Privacy and Security of the Advanced Metering Infrastructure', Sep 2010

20. Ministry of Economy, Trade and Industry "Challenges and measures for promotion of smart meters" December 2014, http://www.meti.go.jp/committee/summary/0004668/pdf/015_03_00.pdf

21. https://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf

22. 'Security Engineering: A Guide to Building Dependable Distributed Systems', Ross Anderson

23. Los Angeles Times archive, 'Rancher Pleads Guilt in Theft of Electricity', Oct 30, 1931.

24. The Montreal Gazette, 'Electricity theft charged in court', Mar 22, 1934.

25. The Palm Beach Post, 'Theft of electricity is charged in court', Jan 18, 1933.

26. 'Who controls the off-switch?', Ross Anderson and Shailendra Fuloria, SmartGrid Comm, 2010

27. NISTIR 7628 Volume 2

28. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

29. http://www.cer.ie/docs/001021/CER15139%20Data%20Access.pdf

30. ‘Security Economics and Critical National Infrastructure’, Ross Anderson and Shailendra Fuloria, Workshop on Economics of Information Security, UCL, 2009

ANNEXURE A: TOP 10 FINDINGS AND RECOMMENDATIONS OF THE SURVEY UNDERTAKEN BY ISGF AND NCIIPC

S. No.	Finding	Recommendation
1	Many organisations do not have formal Information Security Policy.	Organisations must take steps towards formulation of comprehensive Information Security Policy. Sub-policies and procedures specific to key operational areas should also be prepared. Organisation needs to establish a formal mechanism by means of which all stakeholders (Employees, contractors etc) are required to read and acknowledge the relevant portions of the relevant policies.
2	Many organisations do not have an independent Information Security Audit mechanism.	Regular internal and external audit for the cyber security must be conducted. The auditors must be considered to be changed on a regular basis.
3	Organisations are yet to undertake a detailed Vulnerability/Threat/Risk (VTR) analysis of their Critical Information Infrastructure (CII) and necessary measures to address the same. At present, this is being done as an ad-hoc approach in most of the organisations.	It is essential that at least for CII, the organisations must undertake thorough V/T/R. Organisations should identify CII and corresponding incoming and outgoing dependencies. Process for obtaining approval for notifying CII and approval of the Sectoral Statutory body for CII notification needs to be initiated.
4	Risk assessment & mitigation process are yet to be established and/or reviewed regularly by many organisations. The acceptable residual risks are also to be clearly evaluated and business continuity plan need to be appropriately tuned.	In order for the magnitude of the problem to be understood by the Senior most management, it is essential that a mechanism for evaluating and approving residual Information Security risk be evolved in a manner similar to that existing for Financial or Operational risk. In effect, it is imperative that the Information Security risk be owned by the organizations.
5	Organisations are having ad-hoc Cyber Security Incident handling mechanisms.	Incident management procedures need to be augmented. Some suggestions (indicative but not exhaustive) are: a) Formal definitions of "cyber security incidents" be developed and circulated to all personnel handling IT or ICS systems. b) Incident management processes must be clearly spelled out with responsibilities of individuals and steps for orderly response to a security incident. c) Incident management drills. d) Sensitisation of users and basic training to understand and implement good cyber hygiene
6	Automated mechanisms for monitoring inbound and outbound traffic for malicious/unauthorised activities have not been implemented.	Monitoring of inbound and outbound communications is required to be conducted to observe for unusual or unauthorized activities. Automated mechanism may be implemented for monitoring inbound and outbound traffic, as they provide effective monitoring. It is also recommended that documentation for the monitoring process may be maintained.
7	For disposing Critical Digital Assets (CDA), they are simply forwarded to Waste Management companies. Mechanisms for ensuring data leak prevention for CDA have not been considered.	In order to ensure that no data is inadvertently being leaked outside the organization, policies for disposal of Critical Digital Assets (CDA) must be formulated. Physical destruction of CDA may be considered as a part of organisation's disposal process.
8	Organisations do not have strict control over usage of mobile devices such as removable USB media, Mobile phones etc.	Organisations must define proper usage, access control and security Procedure/guidelines for the mobile phones/smart-phones and portable media, as they are amongst the foremost source of malware infection and system compromise. They may also adopt the procedure for blocking the unauthorised removable media (e.g. USB device) on systems.

9	a) Organisations do not IT security SLA (Service Level Agreement). b) Procurement standards do not include system hardening.	a) Organisations must have IT security SLAs for operational requirements with outside agencies. This will enforce the other organisations to consider security with the service they are providing. b) It is recommended that system hardening may also be included in the procurement standards of the organisation. It will help in making systems secure by design.
10	Many organisations do not conduct Information security awareness trainings.	Organisations should undertake regular security awareness training for its employees. Effectiveness of security awareness training needs to be reviewed once a year at a minimum. Practical exercises may be included in the security awareness training that simulates actual cyber attacks.