

Advanced Metering: ecosystem, security threats and counter measures

By Mohit Arora
Systems Engineer
Freescale Semiconductor Inc.

Today, the vast majority of meters installed around the world are simply dumb devices. Utility Companies are on the move to modernize their meter readings and data collection systems with advanced metering infrastructure (AMI). Utilities are upgrading their legacy metering and data-exchange infrastructure to tap into this new capability.

The deployment of AMI and automated meter reading (AMR) capabilities in the power distribution system has the potential to save energy suppliers and their consumer's significant amounts of money in the near term. The energy suppliers can benefit by more efficient meter reading,

fewer truck rolls (i.e. fewer maintenance personnel dispatch events), outage location identification, remote connect/disconnect etc.

Energy consumers will also have new opportunities to reduce their energy costs by taking advantage of real-time energy pricing, off-peak rates, and various programs that will be possible with the two-way communication networks between the utilities and their customers.

Utilities, regulators and customers see the benefits in making the customer connection more intelligent and responsive to system needs. The AMI (also known as smart grid) requires a combination of different technologies that rely on network connectivity, posing significant security issues that must be addressed from the beginning.

Advanced metering technologies: the ecosystem

Since the time the electromechanical meter was invented more than a century back, there has been very slow progress except in the last few years with the introduction of AMR and AMI.

Moreover, with the recent downturn in the economy, there has been an increased focus on energy conservation fueling the growth of Smart Metering technologies like AMI/smart grid.

AMR is generally regarded as the reading of a utility meter by a means that does not require physical access or visual inspection of the meter. Normally, within an AMR system, the meter data is passed from the meter to the utility via communication network. AMR is a one way communication.

AMI offers a more sophisti-

cated two-way communication system that collects, measures and analyzes energy usage from network-connected devices such as electricity meters, gas meters and/or water meters. The AMI includes software, hardware, communications, customer-associated systems and meter data management (MDM) software. With AMI/AMR, utility companies can introduce time of use rates, demand response features like peak load pricing as well as outage detection and assessment thereby providing customers means of saving energy and cost.

As an example, the consumer can implement home area network (HAN) to connect with all the smart devices. These devices can include computers, smart thermostats, air conditioning, home security systems, intelligent appliances or any other digital device. Inter-

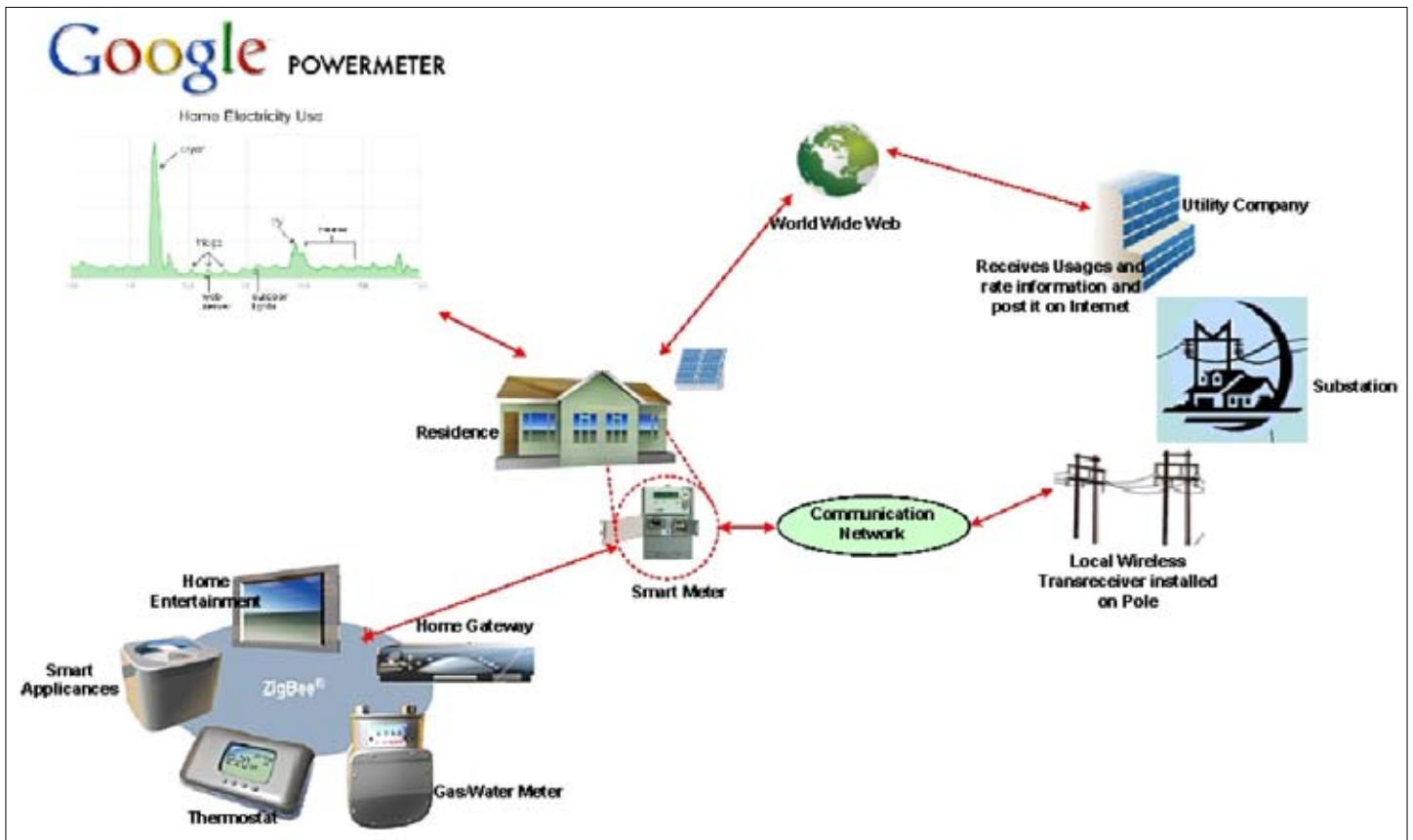


Figure 1: Shown is a smart metering network.

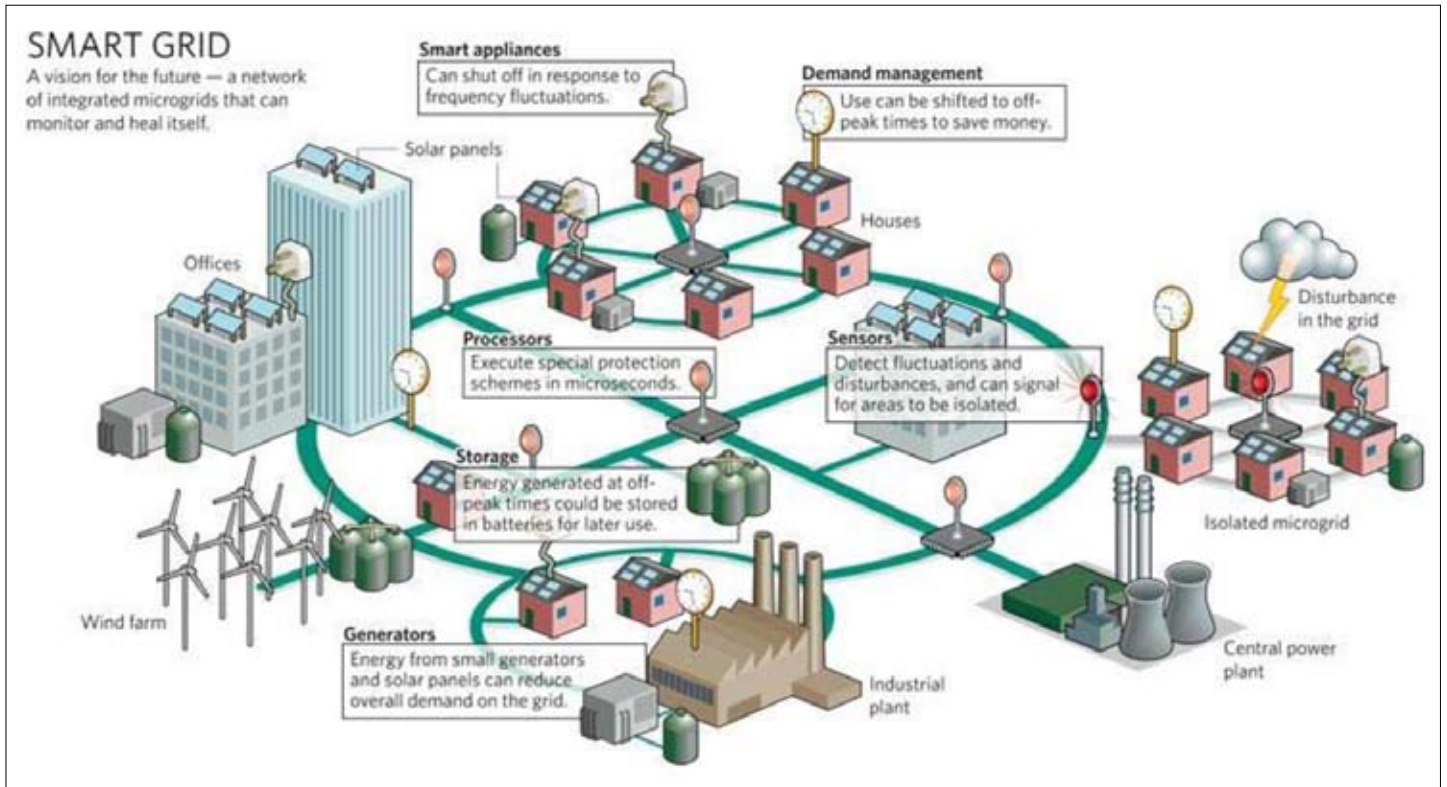


Figure 2: Here's a more futuristic smart grid ecosystem with self-healing capabilities. (Source: photobucket.com)

communication between the devices can be wired or wireless or mixed of both using technologies like Zigbee/Homeplug.

With two-way communications capability, the HAN can measure, verify, dispatch demand response and provide feedback displays to the customer showing billing effects associated with usage of various appliances. A washing machine equipped with smart-metering technology can, for example, be programmed to start wash automatically during non-peak hours so the consumer can take advantage of lower rates. Same applies to other smart appliances like geysers that can be set to turn on automatically at the specified time and thus manage the peak load. Another network topology can be where the home computer (so called home gateway) would talk to the smart appliances and connect to a Smart Meter (**Figure 1**).

When connected to a network smart meters can report measurements directly to the utility company. This can be done with a wireless transceiver installed on power pole that

communicates with Smart meter installed in the consumer home and sends the data to the substation or central database maintained by utility company. Utility company can post this data on the internet so consumers can access their data online to know their detailed usage.

Companies like Google have started to collaborate with utility companies to analyze this online data. Google Power Meter is one such electricity usage monitoring tool that receives information from utility smart meters and in-home energy management devices and visualizes this information for customer in web based graphical format. These applications can provide detailed information showing energy consumption by different appliances like washing machine, refrigerators, TV etc. so customers can analyze and manage their consumption and save cost.

Note that to make this practical, Smart Meter need to be programmed by the utility companies to implement time based metering, with different rates for peak and offpeak usage.

Figure 2 shows a more futuristic smart grid ecosystem with self-healing capabilities. As shown, the network connections can be traced from the customer's premises to distribution substations that control the generation and flow of electrical power.

Smart appliances may also communicate with plug-in hybrid electric vehicle/storage, photovoltaic arrays and wind turbines. Energy generated via Solar panel at off-peak times could be stored in battery for later use. Additional energy generated from the solar panel/small generator can be fed back to the grid reducing the overall demand on the grid.

All the HAN devices are connected to a Smart Controller/Meter through a network such as Zigbee or mesh wireless. Collector nodes communicate with the utility through common communication mechanisms including the Internet.

Smart devices, especially the appliances can shut off automatically in response to fluctuations (i.e due to disturbance in grid) and can signal to the substation to isolate the area or shut off power.

These smart grid technologies are now in the process of being deployed. The operation and control of the current power grid depends on a complex network of computers, software and communication technologies that, if compromised by hackers, could be used to cause great damage, including extended power outages and destruction of electrical equipment. Therefore, known vulnerabilities in these systems must be mitigated to increase the security and success of the smart grid.

Security threats

Future smart grid or advanced metering is heavily going to rely on different communication technologies, be it wired or wireless. Increased level of automation between different smart grid components is going to imply increased computer controlled electronics and software that may increase the chances of potential cyber attack.

A cyber attack has the unique attribute that it can be launched through the public network from a remote location anywhere in the world. The Wall Street

Journal has already reported that cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. Potential consequences of successful cyber attacks can include the destruction of generators, power outages or even grid instability. This is a serious thread that government worldwide is starting to pay more attention.

There have been a couple of studies that have identified several methods for attacking wireless devices used in AMI networks. Since these wireless devices are outside the utility's physical security perimeter, they are at high risk of being compromised. One of the study done by Goodspeed documented how attackers can extract data from the memory of these devices including keys used for network authentication and how the device memory can be modified by an attacker to insert malicious software.

Other vulnerabilities in AMI devices include insecure data buses, serial connections or access to debug port remotely.

Except the physical tampering of the meter to change characteristics, most of the known vulnerabilities are associated with the communication media and communication protocols as power grid gets connected to the Internet, which has inherent security weaknesses. Each communication path is a potential attack path for a knowledgeable attacker. There are many potential entry points physically unprotected. Wireless networks can be easily monitored by attackers and may be susceptible to Man-in-the-Middle attacks.

The next section is going to focus on some of the techniques that can be deployed to secure the communication channels making smart grids more secure and reliable.

Securing the communication ports

Here are some of the recommended techniques that can be implemented to secure the com-

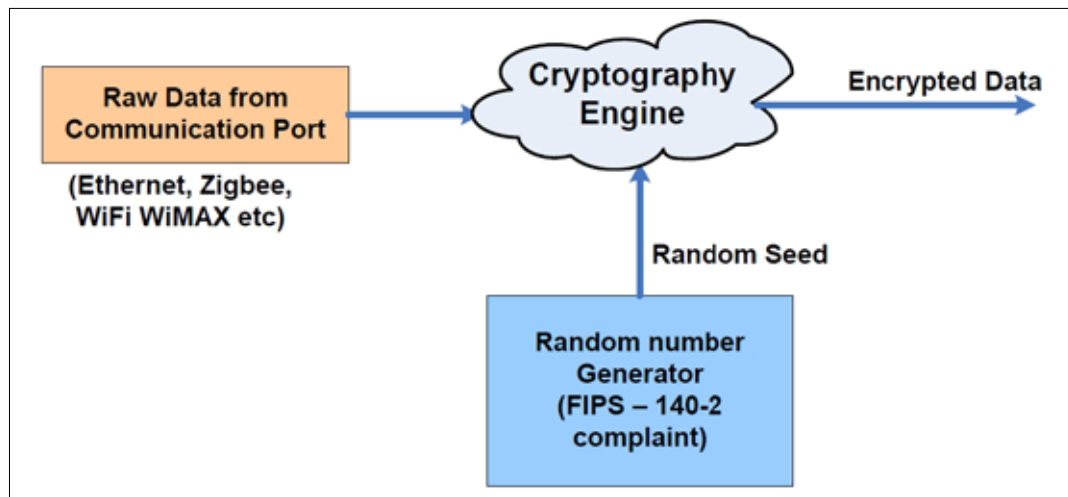


Figure 3: Shown is data encryption using NIST-compliant random number generator.

munication channels in a Smart Grid Ecosystem:

Using secure communication protocols—There are many data exchange protocols used between entities within the power grid. Some of these protocols such as TCP/IP, HTTP and FTP are widely used in the global Information Technology domain. These are not very secure and are vulnerable since the data transferred is in the clear that can easily be eavesdropped by the hacker.

The unsecured protocols should get replaced with Internet Protocol Security (IPSec), Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Secure Shell (SSH). IPsec uses encryption technology to provide data confidentiality, integrity and authenticity between participating peers in a private network. TLS is standardized by IETF, and is a protocol intended to secure and authenticate communications across public networks by using data encryption. These protocols are designed to prevent eavesdropping, message forgery and interference.

Another protocol is SSH. It is a program to log into another computer over a network and execute commands on a remote machine. For example SSH could be used to log into the power grid switching equipment remotely in order to monitor the status or to deliver the commands. It provides strong authentication and secure encrypted communications between two

hosts over an insecure network. It is a replacement for rlogin, rsh, rcp, rdist and telnet. SSH protects a network from attacks such as IP spoofing, IP source routing and DNS spoofing.

Cryptography for data protection—Almost all secure protocols (including the one mentioned) require one or other cryptography techniques to encrypt the data. One of the popular cryptography algorithms is the Advanced Cryptography Standard (AES) used in symmetric key cryptography. It is fast in both software and hardware, is relatively easy to implement, and requires little memory.

AES is pretty good to protect classified information. The implementation of AES in products intended to protect national security systems must be reviewed and certified by NSA prior to their acquisition.

AES supports three keys: 128bits, 196bits and 256bits. Higher key length offers better security.

Using 128bit AES cipher, communication between individual meters and meter data collections can be encrypted, preventing eavesdropping of potentially sensitive customer or metering system information. This would allow data to be never in the clear, thus protecting data integrity, making it difficult if not impossible to snoop in and modify the data by a hacker. This prevents

man-in-the-middle attacks, which could target specific homes or spread throughout the smart grid network.

Higher level of security for control and commands—Symmetric key cryptography is good for bulk data but may not offer highest level of security that can be offered by using asymmetric key cryptography such as Elliptic Curve Digital Signature Algorithm that can be used to encrypt any control/commands like remote disconnect/connect real time pricing changes etc. This ensures higher level of authentication for the commands to control grid equipments.

Key exchanges based on Elliptic Curve Cryptography (ECC) can offer high level of security.

ECC can also be used by wireless networks like Zigbee to offer digital certificates to exchange information between Zigbee nodes/devices within a smart grid ecosystem.

Key generation and storage for cryptography algorithms—Almost all security passwords and cryptography keys rely on random seed.

The use of pseudo-random number to generate secret keys can result in pseudo-security. It is important that random seed generated should be truly random to avoid pattern analysis attempts.

National Institute of Standards and Technology (NIST) recommends using FIPS-140-2 compliant random number generator

for high level of security. Raw data from communication port is encrypted using truly random seed (**Figure 3**). It is highly recommended that a random generator be implemented in hardware as software-generated random numbers are not considered as secure and can easily be hacked.

Also note that random seed generation should not be part of any memory maps registers or software readable, and should only be available to the cryptogra-

phy engine. It would be also be a good idea to erase the keys during any tampering events.

Secure debug and client-server authentication—Debug port manipulation is one of the known hackers' ways of executing unauthorized program code, getting control over secure applications and running code in privileged modes.

Debug ports such as the IEEE standard 1149.1 (AKA JTAG) pro-

vides a hacker with all the means required to break the system's security mechanisms and get control over the OS. Unauthorized debug port usage should be strictly forbidden to properly secure the system.

Secure system often includes an option of providing an authentication key that allows access to debug system. This can either be built into the hardware debug system on the processor or it can be implemented through

software within the application. To offer a higher level of security while allowing debug, it is advisable to use the highest level of security where server authentication is required to allow debug access. By doing so, the server can both monitor any attempted debug access and manage the access keys as well.

Note that similar rules must apply when doing a remote debug into a smart grid control equipment.