Keywords: energy measurement, smart grid, security, electricity, network, IT, metrology, communication, powerline, RF, wireless, smart energy, environment, conservation

APPLICATION NOTE 5536

Energy Measurement and Security for the Smart Grid - Too Long Overlooked

By: David Andeen, End Segment Manager, Smart Grid
Jan 25, 2013

Abstract: It may sound trite, but it is definitely true: the smart grid has the potential to completely transform the energy industry. However, smart meters and grid management alone will not ensure the success of the smart grid. Unlike traditional IT networks, smart grids require consideration of energy measurement and security. To completely optimize this technology, smart grid designs must focus on energy measurement and security. This tutorial considers the benefits of both energy measurement and security and how they make machine-to-machine networks different from traditional IT.

A similar version of this article appeared in Chinese on *EE Times China*, January 7, 2013.

Introduction

As smart meter rollouts continue globally, consumers, design engineers, and utilities discuss how the smart grid will transform the entire energy industry. Smart meters already allow utilities to save money by accessing meter data without sending someone to physically read the meter. Utilities, factories, and consumers are now pushing for more conservation and alternative fuels. New business models encourage peak demand reduction through incentives such as time-of-use pricing to reduce consumption during maximum demand periods. Distributed resources, such as electric vehicles and various forms of solar and wind generation, are maximizing renewable resources and leveraging the available resources to accommodate peak demand. All of these developments will also lead to more big data analysis within smart grid. With smart meters, utilities go from one or fewer meter reads per month to six to 96 meter reads per day. All of the data generated from smart meters offer the opportunity to better understand usage patterns, waste, and other factors that utilities have yet to uncover.

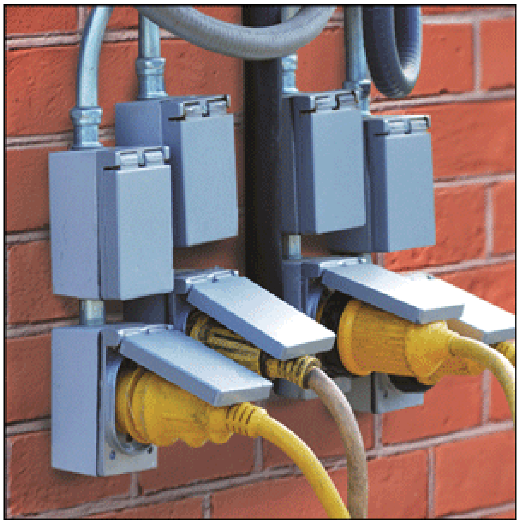
But in the end, smart meters and grid management alone will not ensure the success of the smart grid. To completely optimize this technology, smart grid designs must focus on energy measurement and security.

Energy Measurement Actually Saves Energy

Unfortunately, with so much emphasis today on the future management of smart grid technology and its roots in telecom infrastructure (for more on this, see the Appendix: Smart Grid vs. Telecom—A Tale of Two Networks), one can easily forget that energy measurement and security are essential to the system's success. After all, a network concerned with electricity management must both measure its critical commodity *and* also protect the valuable infrastructure that delivers it. Enter energy measurement.

Smart meters measure industrial and consumer energy consumption with a feature called "metrology," utility-grade energy measurement. These smart meters are already part of a massive machine-to-machine utility network in several locations including Italy, California, and parts of Scandinavia. But, are utilities the only ones with a keen interest in measuring energy consumption? Of course not. The benefits of broad-based energy measurement can extend to the vast number of users and providers on the grid.

As a personal example, last year my electricity bill progressively increased over the course of October, November, and December. In late December, my electric dryer broke down. Fortunately, my wife and I were able to immediately purchase a new one, which was critical in the middle of winter. In retrospect, the dryer motor burnout caused excessive energy consumption, which explained my higher monthly electricity usage, the resulting bill, and eventually the financial burden of immediately purchasing a new unit.



Energy measurement can assist in situations such as mine. Applying energy measurement to a variety of applications, such as consumer devices and industrial motors, offers tremendous benefits: reduced electricity consumption; usage patterns that signal maintenance requirements or even the replacement of critical assets; and better educated users or systems operators who can make more informed decisions about consumption and system performance. In the case of my dryer, accurate measurement of the motor's electricity consumption would have immediately shown that the device was consuming more energy with time. Like the "check engine" light on your automobile, energy measurement records usage patterns, and thus give an indication of device health and operation well in advance of failure. That usage pattern would have provided enough time for me to repair the clothes dryer or to simply find a new one (on sale!).

The energy consumed, or wasted in the case of my faulty clothes dryer, is small compared to the potential benefits of accurate energy measurement in an industrial setting. Manufacturing environments, where motors account for 54% of electricity use,[1] make for higher-stake situations with uptime requirements and production targets. A 100hp motor with a 2.5% voltage imbalance, for example, will consume an estimated additional $476 in electricity per year.[2] Add to this the additional wear and tear on equipment, which results in additional maintenance and earlier replacement costs. You quickly understand the enormous potential benefits of energy measurement in a smart grid system for industry. Now take the logic a step further. Multiplying the cost of electricity and maintenance across all motors used globally represents a massive opportunity for energy conservation and savings.

Once you recognize the importance of well-managed energy measurement, you look for solutions to implement it. Here is where a smart energy meter and measurement system becomes crucial. Maxim Integrated provides several energy-measurement and motor-diagnostic solutions for energy condition monitoring. The 78M6610, 78M6613, 78M6631, and MAX78638 deliver accurate, four-quadrant electricity measurement with custom firmware. They provide valuable measurement data for monitoring and measuring efficient solar-panel inversion, motor health in an industrial application, and energy consumption in lighting and computing applications. Ultimately, the investment in energy measurement solutions shrinks compared to the savings in preventing equipment failure and ensuring system uptime.

Grid Security—Essential, Yet Not Fully Appreciated

The smart grid also requires complete security 24/7. Most consumers, even industrial and utility operators, underestimate the importance of this. Endpoints such as smart meters, industrial motors, consumer devices, and widely distributed automation equipment all consume *and* control electricity. Meanwhile, applications for grid-connected devices continue to increase as smart grid operators are taking advantage of "smart" networks to correct power factor, optimize voltage, accurately locate faults, and reduce repair time to ensure uptime.

Cyber attacks, theft of IP, disruption to productivity—all these threats are rising in both smart grid and industrial-control systems. Only complete security measures, optimized for a smart grid, can thwart these severe threats and ensure maximum operational uptime, whether a simple home clothes dryer or a sophisticated, distributed industrial complex. Unfortunately in many cases the severity of the security risk is not fully appreciated and only minimal security measures exist. In one conversation, a utility professional told me that "barbed wire, a padlock, and high voltage were the only protections" on his utility's substations. Other less-informed operators trust the innate security measures in hardware and fail to recognize the greater threat posed by cyber attacks through software.

The most effective security solutions secure the entire life cycle of a product through hardware *and* software. Because potential security breaches can happen at all phases of device operation, from purchase to manufacturing to operation to decommissioning, grid security has far-reaching applications.

When purchasing a product that will function on a smart grid, the purchaser must be assured that a reliable channel exists for buying silicon and other critical computation devices. This is essential to avoid counterfeit products. In manufacturing, strong authentication techniques prevent third parties, such as manufacturing contractors, from stealing keys and later using those keys to pirate electricity or infect the grid with a virus. In field use, secure key storage and multiple layers of encryption secure data across communication channels. Secure bootloaders prevent viruses and malware from loading into a system. Hardware techniques monitor physical security, enabling responses to tamper events. Devices and sensors not under constant surveillance explicitly need such comprehensive secure protection.

The most effective security is designed and integrated into the system or grid itself. Maxim offers a complete array of secure products, such as the MAXQ1050, MAX36025, and MAX71637 that meet the security needs of the smart grid. Integrated here is basic authentication for multilayer schemes involving split keys, asymmetric encryption, secure bootloaders, and various physical tamper protection mechanisms.

Summary

It may sound trite, but it is definitely true: the smart grid has the potential to transform the energy industry completely. This is exciting and deserves our engineering attention. But in all this management euphoria, it is easy to overlook the often-hidden, but critical roles of measurement and security for the grid. And that is where quality meter design is proving most valuable. If we continue to focus on energy measurement and security to truly harness this technology, then we must appreciate how smart meters are going to enable the smart grid.

Appendix: Smart Grid vs. Telecom—A Tale of Two Networks

When we talk about the smart grid, we often focus on its enormous potential to become a self-healing electricity grid that will reduce energy consumption and transform our energy infrastructure. How was such a revolutionary technology designed and created? What was its impetus?

The telecom infrastructure network with its brilliant architecture and technological maturity is the basis for today's smart grid. Conversations on this topic often bring up networking and big data, which provide the ability to aggregate and analyze tremendous amounts of information and make useful decisions with it.

True, telecom and the smart grid share the same core, high speed, and interoperable communication layers. But, there is a hugely important and fundamental difference between these networks: the smart grid is truly a machine-to-machine network. Traditional telecom endpoints result in a human-to-machine interaction, with telephones, computers, and now smartphones. The endpoints of a machine-to-machine network consist of sensors, functional machines, or both. These machines are often not under immediate human control and, therefore, cannot necessarily express or report the status or the health of the network. As an example, industrial sensors often lie in inaccessible places, far removed from the central system, without access to upgrades, and not under any human surveillance. With no human intervention between the system and remote devices, smart grid system designers must deeply consider both the sensing functions and security of such a distributed network.

References

1. U.S. Department of Energy, Energy Efficiency and Renewable Energy, https://www.energy.gov/eere/amo/motor-systems.
2. *Energy Tips, Motor Systems*, U.S. Department of Energy, Motor Systems Tip Sheet #7, September 2005, https://www.energy.gov/sites/prod/files/2014/04/f15/eliminate_voltage_unbalanced_motor_systemts7.pdf.

Related Parts		
78M6613	Single-Phase AC Power-Measurement IC	Free Samples
78M6618	Octal Power and Energy Measurement IC	Free Samples
78M6631	3-Phase Power Measurement and Monitoring SoC	Free Samples
MAX36025	DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption	
MAX71637	Single-Phase and Three-Phase Secure Energy Metering Microcontrollers	
MAX78638	Three-Phase Energy Measurement and Motor Diagnostics Device	
MAXQ1050	DeepCover Secure Microcontroller with USB and Hardware Cryptography	