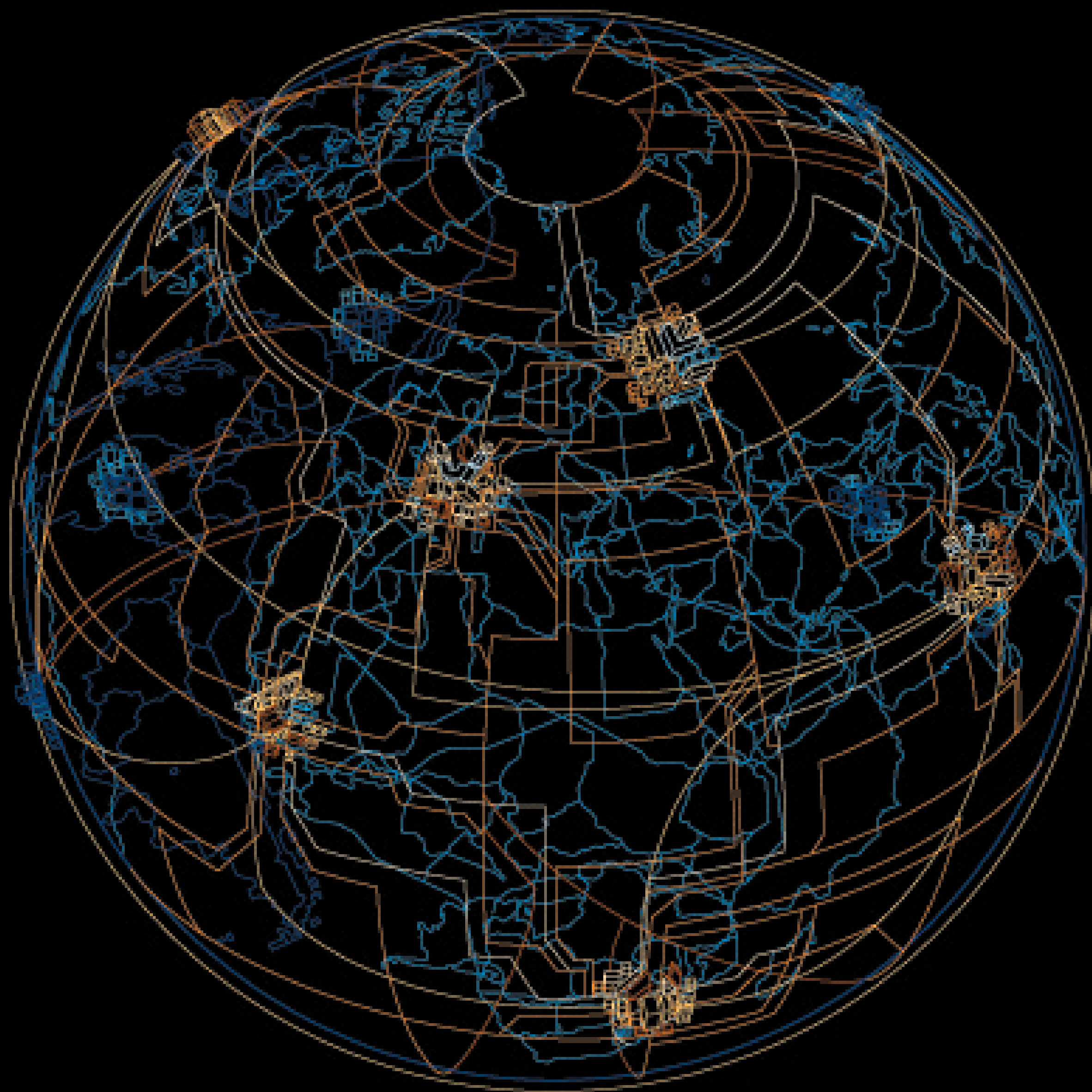

White paper

Smart grid
Beyond smart meters

Power and productivity
for a better world™

ABB

Executive summary

Smart grid: a combination of software, communications control technologies, and equipment in the field designed to operate the power grid more efficiently and reliably.

The smart grid is a growing sector of the economy, but more importantly, it is the key to modernizing our electric power infrastructure. This paper explores several trends in smart grid technology and deployment that are likely to characterize the sector in the near term.

Smart grid spending is on the rise. IDC Energy Insights sees per annum growth in smart grid spending of 17.4% between 2010 and 2015 reaching $46.4 billion per year by the end of that period. Similarly, Electric Light & Power projects global smart grid spending will reach $65 billion by 2017. Fully 80 percent of this spending will go to things other than smart meters.

Similarly, the top trends in smart grid tend to focus on the utility side of the meter and some do not involve end use customers at all. Meanwhile, areas that require customer involvement are likely to focus on larger commercial, industrial and institutional organizations rather than residential consumers.

The four top trends we discuss here are:

- **Distribution automation** - an umbrella term, along with distribution grid management, for a variety of technologies and applications designed to make power distribution networks more reliable and efficient by introducing a higher degree of automation and autonomy to the system.

- **Analytics and "big data"** – really an extension of the analyses utilities have performed for years, but greatly enhanced by the availability of high speed data communications and advanced computing capabilities. These are vital to harness the flood of data coming out of an increasing number of smart devices being installed across the grid.

- **Demand response** – another decades-old technology that is poised to make a much larger impact thanks to advanced computing and communications technology. Utilities are already able to mitigate system peaks by reducing demand via automated controls. Going forward we could see a proliferation of virtual power plants make demand response operationally equal to generation.

- **Cyber security** – an issue that is growing in importance by the day. There is widespread concern that the response is being outpaced by the threat. It took a year for NERC to implement its latest iteration of CIP requirements. While technological defenses are advancing, recent studies show social media channels can be exploited to gather sensitive information about utility systems.

These areas represent the most often cited in our informal survey of industry analyst reports, trend stories published by leading industry media outlets, and published views of industry observers. This list is far from exhaustive, and should not be viewed as scientific. Other trends identified in our research include the growth of microgrids, the falling cost of energy storage, the implications of wider adoption of electric vehicles, and the next phase in automated metering infrastructure (AMI) rollouts.

In a recent report on utility industry trends, Pike Research described the smart grid as "a large commercial venture" with tens of billions of dollars being invested over the next few years. The commercial venture of smart grid is also growing, and is set to continue doing so despite sluggish growth across the broader economy.

IDC Energy Insights sees per annum growth in smart grid spending of 17.4% between 2010 and 2015 reaching $46.4 billion per year by the end of that period. Similarly, Electric Light & Power projects global smart grid spending will reach $65 billion by 2017. The magazine goes on to note that smart grid spending in transmission and distribution will outstrip spending on smart meters by more than five to one. Likewise, IDC Energy Insights reports that smart grid spending in North America will focus on distribution automation in addition to advanced metering infrastructure.

The purpose of this paper is to highlight some of the trends in smart grid technologies and applications being implemented by utilities across the country. The trends discussed below are drawn from an informal survey of industry analyst reports, trend stories published by leading industry media outlets, and published views of industry observers. This is not a scientific approach, nor is it intended to be exhaustive in its findings. Rather, we are using this sampling of informed opinion as a proxy to identify areas within the smart grid that deserve attention not only from industry players but from regulators, policy makers, and the many other stakeholders that have an interest in the modernization of our power grid.

Smart grid trends

Defining "top trends" in smart grid

Interestingly, of the 10 "top trends" lists we reviewed, only three mentioned consumer issues (e.g., privacy concerns with smart meters) as a trend to watch. Indeed, there was far more consensus around topics that have limited or no consumer contact, such as:

- Distribution automation
- Analytics and managing "big data"
- Demand response
- Cyber security

We will define and discuss each of these in the following sections.

Distribution automation

This is really an umbrella term, along with distribution grid management, for a variety of technologies and applications, some of which have been in use for many years. The main purpose of distribution automation (DA) is to make power distribution networks more reliable and efficient by introducing a higher degree of automation and autonomy to the system. More recently, DA has added some interesting applications that show great potential.

One of these, known as volt-VAr optimization or VVO, deals with the balance between real power and reactive power. Both flow over the same wires, but only real power is used to run our computers, light our streets and cool our buildings. Reactive power is needed to maintain voltage levels and system stability, but it doesn't do the "work" that real power does.

Since there is a finite amount of "capacity" (or "bandwidth" to use a computing analogy) available on transmission and distribution lines, the more reactive power there is flowing on a given line, the less real power is able to get through. Reactive power also requires generation capacity, increases energy consumption, and increased generation emissions.

Related to improved management of reactive power is the concept of conservation voltage reduction. If reactive power flows are reduced, the system can accommodate lower distribution line voltages without violating voltage constraints. Lower voltages further reduce demand and losses, improving efficiency of the grid.

Utilities have long sought to minimize reactive power flows through the use of capacitor banks and special transformers operating autonomously on the grid. Now, with the help of increased computing capacity and high speed communications, it is possible for these devices to be coordinated across an entire utility distribution system. Where previously the actions of one device might have an adverse impact on another part of the system, now the grid as a whole can be optimized. The result is an improvement of 3-4 percent in system-wide efficiency.

VVO is a prime example of an advanced smart grid technology that provides benefits to the system as a whole, but does not touch the utility customer directly. Fault detection, isolation and restoration (FDIR) does both. As the name implies, FDIR is aimed at managing outages to reduce the length of time customers are without power. FDIR uses a combination of automated circuit breakers, reclosers and other equipment to detect an outage (e.g., a line taken out by a downed tree during a storm), isolate the faulted section of the line, and reroute power so the impact of the outage is minimized and those who can still receive power are quickly re-energized.

FDIR can be applied system-wide, or on a very limited basis—even on a single feeder—as part of a low cost pilot program. In fact, this is one of the virtues of DA generally that make it appealing for utilities. DA projects can be highly targeted, and even small investments can yield measurable value. AMI installations, by contrast, tend to produce the greatest value when the meters are deployed over the largest area, which not only implies greater cost, but also more time before the full impact of the investment can be realized.

Analytics and "big data"

First we should be clear that utilities have been performing "analytics" for decades. Since the advent of the spreadsheet, grid operators have used various measurements and operational data to perform studies on system performance, load modeling and outage scenarios among other things.

Today, modern computing capabilities are making use of the flood of data that utilities receive from smart devices on the grid to produce ever more sophisticated analyses that would have been unthinkable just a few years ago. It isn't just smart meters—data from substations, remote sensors and even specific pieces of equipment like transformers are now being used in a wide range of applications.

One example is condition-based maintenance. Transformers are the heart of the transmission and distribution system, but until recently utilities could only perform maintenance on a schedule provided by the manufacturer, much like changing the oil in a car every 3,000 miles. This time-based maintenance happened whether the given unit needed it or not. Now timely operational data from individual transformers allows grid operators to get a better picture of the actual condition of a given piece of equipment, and schedule maintenance according to its specific needs rather than a generic schedule.

Analytics can also uncover hidden trends and other useful information by combining data streams from different sources. One as yet untried example reported by Public Utilities Fortnightly involves plotting the location of different types of trees near power lines. Some species are more likely to fall in high winds, so the theory goes that by identifying areas with high concentrations of vulnerable trees, you could focus pruning work on those areas.

As the amount of data utilities take in increases, advances in computing and communications technology will enable those organizations to glean actionable information from it. The availability of data also can prompt new applications.

Demand response

Like analytics, utilities have been responding to system peaks by reducing demand at certain customer sites for decades. It has been known by different names—load curtailment, “interruptible” rates, and now demand response (DR)—but the concept is the same. Utilities can manage periods of high demand by either generating more power or reducing load. Since the “cheapest megawatt is the one you don’t use,” demand response programs have been effective at meeting system peaks and even deferring the need for power plant construction.

As smart meters have been introduced, there has been an increasing expectation on the part of many customers with regard to DR. However, DR can have a substantial impact even if residential customers are not involved.

Industrial plants and other large users of electricity have a ready business case for participating in demand response programs, and the actions of a handful of steel mills, cement plants or institutional campuses can have the same impact as thousands of residential customers. Smart grid technologies are also making it possible for utilities to expand their demand response activities in novel ways.

One example is the concept of the virtual power plant. The idea is simple: aggregate a variety of utility customers and present their collective demand reduction to the grid operator as a dispatchable resource. The combined load reduction can be invoked in the same way and with the same effect as ramping up a power plant to meet the peak demand, only without the fuel cost, maintenance and emissions.

Going forward, we expect to see demand response play a larger role in utility operations. Residential customers will come into the fold if there is a compelling value proposition and participation in the given program is easy. Smart meters and home automation networks can enable some of the advanced demand response programs. Over the near term, however, we expect demand response to focus on the lower-hanging fruit of commercial and industrial customers that have greater exposure to energy costs. Typically, these customers also already have smart meters that capture demand and interval data for time-of-use and other rate structures.

Cyber security

The smart grid is only one area where cyber security has become a kind of elephant in the room. It is being addressed (e.g., with NERC’s critical infrastructure protection protocols), but many within the industry and outside it are worried that the response is being outpaced by the threat. It took a year, for example, for NERC to implement its latest iteration of CIP requirements.

The issue of cyber security in smart grids extends well beyond smart meters, but much of the public’s attention has been focused on the vulnerability—whether perceived or real—of those devices. In fact, there are two aspects of cyber security that should be understood as we implement smart grid technologies. The first is that the nature of the threat has changed, and it continues to evolve. A comparison of the SQL Slammer virus discovered in 2004 and the Stuxnet virus of 2010 puts this in stark terms.

The first was created by a high school student and while it infected computers within critical infrastructure facilities, it did not specifically target them. The second was a highly sophisticated, precisely targeted bug that by all accounts was designed to attack particular programmable logic controllers used at an Iranian nuclear research facility.

Security experts say that large, highly visible denial-of-service attacks like those that have crippled commercial web sites are now giving way to much more insidious attacks that seek to gain a foothold on a given system and remain below the radar, collecting information that can be used in further attacks. Meanwhile, motives are changing as well. “Hacktivism” (e.g., as demonstrated by the group known as Anonymous) is as much a threat to utility IT systems now as terrorism, perhaps more so.

The second key aspect of cyber security is that with the proliferation of digital devices and online services comes an increase in potential points of entry for cyber attacks. Even systems physically separate from the internet are at risk if, for example, an employee plugs his web-enabled smart phone into his workstation to recharge the battery. Stuxnet was delivered via a USB storage device used by an unwitting consultant.

Social media channels have also opened up new pathways for would-be attackers to gain valuable information. In one sobering experiment, security researchers set up a bogus social media persona using a photo of a pretty model. Within two months, "Robin Sage" had collected sensitive information from a variety of highly placed military and government officials. The exercise showed that social engineering is still one of the most useful tools in the attacker's arsenal.

How serious is the cyber threat for utilities? Opinions vary, but they tend to skew toward the pessimistic end of the spectrum. Pike Research, for example, says that a major cyber security failure in the utility industry is "nearly inevitable." Indeed, it's likely that at this point in time almost every major utility has experienced cyber attacks of varying levels of sophistication. It seems more of a question of when, not if, a utility suffers a serious breach.

In terms of resources being dedicated to the problem, IDC Energy Insights projects a 9% cumulative average growth rate in cyber security spending through 2014, rising to $558 million. That's double the analyst's projected growth rate for utility IT spending in total, but protecting utility systems may be as much a question of methods as resources.

Some security experts, such as Red Tiger Security's Jonathan Pollet, suggest that IT system operators should move beyond purely defensive measures and begin to collect information on the individuals and groups most likely to threaten their systems. This more "offensive" approach may seem like something from a spy thriller, but it serves to illustrate the evolving complexity of cyber threats.

Other trends worth watching

The trends we've covered so far—distribution automation, analytics, demand response and cyber security—represent only some of the most-discussed in the industry. There are many other areas within the smart grid arena that are generating excitement, and we've noted a few of them.

- **Microgrids** – The market for small free-standing grids is being driven largely by military applications now, but as microgrids are better able to be integrated with utility operations, we may see more of them in the near future. There is already a compelling business case for microgrids in remote locations—wind and solar are cost-competitive with diesel generation in such instances, even without government subsidies.

- **Energy storage** – IDC Energy Insights says Li-Ion batteries have "won the storage race" and predicts costs will reach $600/kWh this year for grid scale applications. As storage becomes cheaper, it will act as an enabler for more solar and wind to be integrated to the grid, as well as enhancing overall system resilience.

- **Electric vehicle adoption** - Opinions are mixed. Some industry observers see 2012 as a make or break year for electric vehicles, while others predict robust growth. A proliferation of chargers (both home and commercial) will drive the need for more sophisticated grid monitoring, condition assessment, and predictive maintenance, especially on distribution transformers.

- **Automated Metering Infrastructure (AMI)** – Far from being defeated by consumer backlash, smart meter installations continue to move forward at investor-owned utilities as well as at municipals and smaller utilities. The fact remains that AMI networks effectively provide a network of sensors that can be leveraged in a variety of ways that have nothing to do with billing. For example, a major benefit is reduced "truck rolls" for services such as on-demand meter reads. Also, outage management systems can use AMI networks to identify who has power and who doesn't, and also to provide time estimates for restoration. Service like that could counter critics' arguments that smart meters only benefit the utility.

This last point is important in that smart grid investments often involve technologies that are interrelated. Building capability in one may well pave the way for others. Similarly, technologies that improve the efficiency of the power grid often also increase reliability.

Reliability concerns and government programs boost smart grid implementation

Reliability – back where we started

Since the development of electric power systems at the end of the 19th century, the entities charged with operating them have had one overarching goal: keeping the lights on. This is as true today as it was in Edison's time. Reliability is also at the heart of the smart grid, especially when it comes to investments in technologies on the utility side of the meter.

The reason is simple: power outages are costly, disruptive, even deadly events. As long as there are storms, there will be localized blackouts, but large cascading outages are another matter. In most cases they stem from a combination of factors, some of which are attributable to human error, but others can be addressed with smart grid technology, provided we learn the lessons that history teaches.

In September 2011, nine million people in Southern California lost power as the result of a blackout that, according to a federal report on the incident, bore a keen resemblance to the massive Northeast Blackout of 2003. Two items in particular—an inability for grid operators to see what was happening on neighboring systems and the proclivity for automated safety measures to actually make things worse—were cited in the report. It also noted that grid operators failed to heed warnings, and that network models were not updated to reflect the current deployment of equipment.

Technology can't mitigate every human shortcoming, and to be sure, most wide-scale power outages can be blamed at least in part on mistakes made by people. But the smart grid offers a variety of solutions—many of them already proven in the field—that can help to minimize the grid's exposure to and mitigate the effects of human error. That many of these technologies and applications can be implemented without the need for consumers to change their behavior is a fact that often gets lost in the debate over the handful of technologies that do touch them. That debate should not prevent us from realizing the many benefits that the smart grid has to offer on the utility side of the meter.

Government's role

The US federal government has already done much to support the development of smart grid technologies and applications. The most visible initiative was the funding made available under the American Recovery and Reinvestment Act of 2009, which covered a wide range of technology development and utility programs to roll out smart grid technology. Many of these programs were already in the works, but the additional support allowed them to be implemented faster and/or on a wider scale than anticipated.

Given the current economic outlook, it is unlikely that there will be an appetite in Washington for further spending of this kind. Still, there are things government can do. The challenge is that there is no single government agency in charge. FERC oversees the transmission grid, DOE has authority to mandate energy efficiency policy, and the EPA can mandate clean air policy, but individual states drive distribution system policy and reimbursement, which has the most direct impact on the smart grid.

So, each state develops its own rules on AMI investments, renewable portfolio standards, decoupled rate structures, deregulation of markets, etc. In addition, each state public utility commission interprets these statutes, so there is even further variation in how the laws are applied. As a result, there is a high level of uncertainty around the smart grid both from a compliance standpoint, but also from a cost recovery standpoint.

One example of this uncertainty lies in how state legislatures and public utility commissions treat societal benefits from smart grid investments. Reliability, consumer engagement, reduced carbon footprint, integration of renewable generation—all of these require investments. If the traditional utility or the "wires" company is making the investment, the question for that utility then becomes whether there is a clear return and a rationale for taking on the implementation risk.

Obviously this is a multi-faceted problem, but to the extent that government—whether at the state or federal level—can reduce uncertainty about how smart grid investments will be treated, it will create a more hospitable environment for investment.

There is also a need to educate end users of electricity about the importance of modernizing our power grid, and about the many benefits that a smart(er) grid will deliver not only for the utility, but for customers as well. Ultimately, the interests of these two groups are aligned around the desire for a safe, reliable and sustainable supply of electricity. Government can help by supporting, endorsing and amplifying industry's education efforts.

Conclusion

Despite a sluggish US economy, smart grid spending remains on the rise. The newest trends in smart grid technology, surprisingly, are not centered on AMI, but rather non-consumer applications. Smart grid is the key to modernizing our electric power infrastructure, increasing reliability and facilitating integration of renewable energy onto the power grid.

Contact us

ABB Inc.

1455 Pennsylvania Avenue NW
Suite 1130
Washington DC, 20004

Phone +1 202 638 1256

www.abb.us/smartgrids