PP40010882

www.electricenergyonline.com

Electric Energy T&D MAGAZINE

MARCH-APRIL 2017 Issue 2 • Volume 21

Envisioning the 21st Century Grid: Powering the Future with Distributed Energy Resources

Electric Energy T&D MAGAZINE

Publisher:
Steven Desrochers:
steven@electricenergyonline.com

Editor in Chief:
Terry Wildman:
terry@electricenergyonline.com

Account Executives:
Eva Nemeth: eva@electricenergyonline.com
Murrae Gomola: murrae@electricenergyonline.com

Art Designer:
Anick Langlois: alanglois@jaguar-media.com

Internet Programmers:
Johanne Labonte: jlabonte@jaguar-media.com
Sebastien Knap: sknap@jaguar-media.com
Tarah McCormick: tarah@jaguar-media.com

Electric Energy Magazine is published 6 times a year by: Jaguar Media Inc.
834 Montée Masson
Terrebonne, QC Canada J6W 2C6
Tel.: 888.332.3749 • Fax: 888.243.4562
E-mail: jaguar@jaguar-media.com
Web: www.electricenergyonline.com

***Electric** Energy **T&D** Magazine* Serves the fields of electric utilities, investor owned, rural and other electric cooperatives, municipal electric utilities, independent power producers, electric contractors, wholesalers and distributors of electric utility equipment, manufacturers, major power consuming industries, consulting engineers, state and federal regulatory agencies and commissions, industry associations, communication companies, oil & gas companies, universities and libraries.
Post Publication mail agreement #40010982
Account #1899244

POWERPOINTS

DistribuTECH or Bust!

Well another year has come and gone and with it the annual DistribuTECH Conference and Exposition. It also meant travelling to San Diego aboard my least favourite airline. I can't believe an Airbus 320 could hold so many people although I was a bit suspicious when I saw a crowbar at the end of each row and the rope ladders were neatly coiled by the doors. Five hours with my knees up under my chin in the econo economy section was just about as much as I could take. I'm glad San Diego is such a fabulous city making my misery melt away very quickly.

I always like riding in the Toyota Prius hybrid taxis. I was totally impressed by the quality and performance of the vehicles and was amused when I saw on the dashboard readout that the car at one point was averaging 100 miles per gallon. Many of my colleagues, including myself, were also lusting after the new Tesla and other performance EVs of which we saw a good many on the streets.

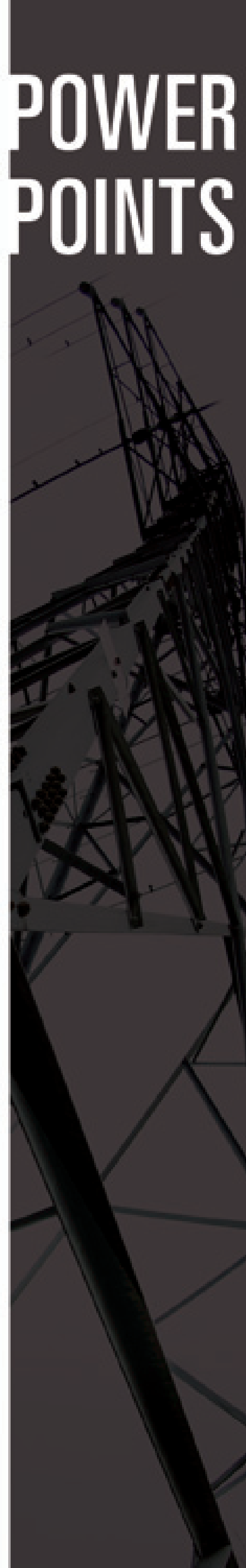
Some years ago, the White House stated that cars running on hydrogen, the universe's most abundant element, would be a popular form of transport. That optimism changed under Steven Chu, the Nobel Prize-winning physicist who was President Obama's first secretary of energy. "We asked ourselves, 'Is it likely in the next 10, 15 or 20 years that we will convert to a hydrogen-car economy?'" Dr. Chu said then, "The answer, we felt, was no."

Rather than hydrogen, a lot of attention was being apportioned to battery electric vehicles, particularly those made by Tesla Motors.

DistribuTECH 2017 was awesome. Apparently a record-breaker for attendance. There are always 'themes' that resound about the place every year and 2017 was no different. A few years ago it was Big Data and Little Data; last year was Microgrids, distributed energy resources (DER) and distributed energy resource management systems (DERMS) and this year is the Internet of Things (IoT). Microgrids, DER and DERMS were still hot-button topics.

A microgrid is a localized grouping of distributed energy resources and loads (such as distributed generators, storage devices, or controllable loads) that normally operates connected to and synchronous with the traditional centralized grid (Macrogrid). It can also disconnect and function autonomously as physical and/or economic conditions dictate.

IoT is increasingly on the lips of conversations in the workplace and outside of it. It's a concept that has the potential to impact how we live and how we work. What is the 'Internet of Things' and how is it likely going to impact us, if at all?



Let's start with understanding a few things.

Broadband Internet is seeing real growth and availability. The cost of connecting is falling, more devices are being created with Wi-Fi capabilities with on board sensors, technology costs are going down, and smartphone penetration is occurring at blistering speeds. All of these things are creating a 'perfect storm' for IoT.

So, what is the Internet of Things?

Stated simply, this is the concept of basically connecting any device with an 'on' and 'off' switch to the Internet (and/or to each other). This includes everything from cellphones, washing machines, headphones, lamps, coffee makers, wearable devices and so on. This also applies to components of machines. For example, a jet engine of an airplane or the drill found on an oil rig. Analysts claim that by 2020 there will be over 26 billion connected devices. The IoT is a giant network of connected 'things' (which also includes people). The relationship will be between people-people, people-things, and things-things.

Why would anyone want so many connected devices talking to each other?

Examples of what this might look like could include:

- Perhaps you are on your way to a meeting; your car could have access to your calendar and already knows the best route to take.
- If traffic is heavy your car might send a text to the other party notifying them that you will be late.
- Your alarm clock wakes you at 6 am and then notifies your coffee maker to start brewing.
- If your office equipment knew when it was running low on supplies and automatically re-ordered more.

On a larger scale, the IoT can be applied to things like transportation networks: 'smart cities' which can help us reduce waste and improve efficiency for energy use. This would help us understand and improve how we work and live.

In fact, the IoT allows for virtually endless opportunities and connections, many of which we can't even think of or even fully understand the impact going forward. It opens the door to a lot of opportunities but also to many challenges.

Security is a huge topic that is often discussed. With billions of devices being connected together, what can be done to make sure their information stays secure. Will someone be able to hack into your toaster and gain access to your entire network? It's no secret the IoT opens up companies all over the world to more security threats. This is exacerbated by the issue of privacy and data sharing. This is really a heated topic so one can only imagine how the conversations and concerns grow when numbers escalate into the many billions of connections. On top of this, many companies specifically are going to be faced with the massive amounts of data that all of these devices are going to generate. Companies need to figure out a way to store, track, analyze, and make sense of the vast amounts of data that will be produced,

For now the best thing we can do is educate ourselves about what the IoT is and the potential impacts that can be seen on how we work and live.[1]

1 Jacob Morgan – Keynote speaker, author and futurist

Sensor Company Acquires Innovation Incubator Awardee, Launches Next-Generation "Connected" Building Technology

March 2017

When researchers at the Energy Department's National Renewable Energy Laboratory (NREL) helped install a peel-and-stick energy-metering system in a Wells Fargo branch bank, they weren't sure exactly what they would learn.

After all, the system from Whisker Labs an Oakland, California, startup was the first "beta-ready" technology to emerge from the Wells Fargo Innovation Incubator (IN2). As part of the five-year, $10 million program, select companies that have successfully met technical project-based milestones in the laboratory have the opportunity to test and demonstrate their products in a real-world environment within Wells Fargo's commercial real estate portfolio. The June 22 pilot installation at a branch in Aurora, Colorado, was designed to allow NREL to evaluate technology performance and demonstrate the benefit of this less-invasive submetering system in a commercial building.

"We wanted to see how it performed under real-world load profiles versus how it did in the lab, a unique opportunity as part of the IN2 program," said Meghan Bader, a program manager with NREL's Innovation and Entrepreneurship Center.

In the midst of the beta demonstration, Earth Networks announced on December 5, 2016 that it had acquired the startup. The company, which operates the world's largest weather observation networks, will create a new division for the energy-sensing hardware and software infrastructure.

"Our breakthrough device and software platform unlocks the full potential of a smart home by collecting and analyzing health intelligence data from both legacy 'unconnected' appliances and optimizing newer 'connected' appliances and devices," said Bob Marshall, chief executive officer of Earth Networks, based in Germantown, Maryland.

The successful exit affirms the purpose and value of the incubator.

"Through the IN2 program we were able to successfully test the technology within the NREL Systems Performance Lab," said Richard Adams, director of NREL's Innovation and Entrepreneurship Center. "Using NREL's laboratory, we were able to characterize the performance of the 'stick-on' power meters with typical appliance loads. The accuracy of the measurements relative to reference meters indicates potential suitability to applications such as measurement and verification, as well as fault detection and diagnostics of building equipment."

ENGIE and Schneider Electric Collaborate to Digitize the Energy Sector

March 2017

Schneider Electric, the global specialist in energy management and automation, and ENGIE, a global energy player committed to be leader of the energy transition in the world, have signed a Memorandum of Understanding (MoU) to explore and deploy new digital solutions for operational efficiency of renewable assets (wind and solar PV), leveraging Supervisory Control and Data Acquisition (SCADA), Historian and related application software powered by Schneider Electric's Wonderware brand.

Asset management, SCADA obsolescence management, remote monitoring and diagnostics and cybersecurity in a complex ecosystem will also be investigated as part of the agreement.

ENGIE and Schneider Electric welcome this collaboration as a major joint initiative in the digitization of the energy sector.

"*ENGIE's objective is to develop remote supervision and control of its global renewable energy production assets, and possibly other energy assets as well, to optimize their performance. We are working in close collaboration with Schneider Electric with a shared vision of the challenges of an energy world that is decarbonized, digitalized and decentralized,"* specified Didier Holleaux, Executive Vice President of ENGIE.

"Schneider Electric leverages its software solutions to address and solve customer needs in new and efficient ways, which will now benefit to ENGIE, a great business partner of Schneider Electric over the past decade. Our combined technology and industry expertise can help identify new opportunities on how to better serve the energy market, while providing greater access to affordable, clean energy," said Philippe Delorme, Executive Vice President, Building & IT, Schneider Electric.

Schneider Electric is already a ENGIE's strategic partner for real-time monitoring and management of its European wind and solar power installations. This partnership demonstrates ENGIE's ambition to accelerate its digitization globally to lead the energy transition.

Northern Pass line: Hydro-Québec has no intention to abandon the project

March 2017

With a view to openness and transparency, we contacted the journalist Jean-Nicholas Blanchet to explain once again Hydro-Québec's participation in the Northern Pass line project. Mr. Blanchet's conclusions from our conversation remain erroneous. Hydro-Québec has absolutely no intention to abandon the project.

Hydro-Québec wishes to reiterate the position we shared with numerous Québec media:

- Hydro-Québec will not pay for the line in the U.S.
- Hydro-Québec will make sure this project is profitable for Quebecers.

We firmly believe in the strength of our alliance with our American partner, Eversource. We intend to submit this project to the request for proposals the state of Massachusetts will be issuing soon. This project will benefit both Québec and the New England states.

Year to year, Hydro-Québec seizes business opportunities on export markets, which form a large part of its profits, for the benefit of Quebecers as a whole.

PG&E Delivered Second Best Reliability in History in 2016, Despite Challenging Weather

March 2017

Pacific Gas and Electric Company (PG&E) delivered excellent electric reliability in 2016 with the average customer experiencing one outage during the year. PG&E's sizable investment in its electric infrastructure and its robust commitment to integrating innovative technology continues to pay dividends for its customers.

In 2016, the average duration of power outages for a PG&E customer was 109 minutes. That was up slightly from 96 minutes in 2015, but still represented the second-lowest total in history and reflects a 35 percent improvement over the past decade. The slight decline in year-over-year reliability can mostly be attributed to stormy El Nino weather early in the year.

"It's our job to provide safe and reliable power to our customers, and I'm proud to say that that is exactly what the men and women of PG&E delivered in 2016. The hard work of our employees coupled with the investments we continue to make to create a smarter, more reliable grid benefit all of us," said Pat Hogan, senior vice president, PG&E Electric Operations.

What's behind the solid electric reliability performance in 2016? The integration of advanced communications and control technologies throughout the electric grid continues to enhance the resiliency of the system and helps identify and restore power outages more quickly. In the last five years, PG&E has invested $15 billion to enhance and harden its electric transmission and distribution system assets. A wide range of factors, from the operation of new distribution control centers to the building of a smarter energy infrastructure to advances in forecasting and emergency planning, all contributed to reliability progress.

New Distribution Control Centers

Since 2014, PG&E has opened three state-of-the-art electric distribution control centers that manage more than 140,000 miles of electric distribution power lines throughout Northern and Central California. The third of these - in Rocklin in Placer County - opened in 2016. These facilities are the nerve centers of the grid that delivers energy to the homes and businesses of more than 16 million Californians. The Rocklin, Fresno and Concord centers have enhanced electric reliability for PG&E customers while incorporating clean, renewable energy into the grid.

Smart Grid

PG&E continues to install advanced automated technology on power lines throughout its service area. This technology can automatically "self-heal" the grid by re-routing the flow of electricity around a damaged power line and effectively restore power to the majority of impacted customers within minutes. These systems have been installed on more than 25 percent of PG&E's electrical distribution circuits, helping the company avoid more than 160 million customer outage minutes and saving more than 1.6 million customers from a sustained outage since the program began in 2012. Other advances, such as line sensors that help pinpoint the specific location of an outage, continue to be integrated into the system.

Advance Forecasting

PG&E's meteorology team has developed a Storm Outage Prediction Model (SOPP) that incorporates real-time weather forecasts, historic data and system knowledge to accurately show where and when storm impacts will be most severe. This model enables the company to pre-stage crews and equipment as storms approach to enable rapid response to outages.

THE GRID TRANSFORMATION FORUM

Envisioning the 21st Century Grid

Powering the Future with Distributed Energy Resources

We are speaking with Dr. Ali Ipakchi, Sr. Vice President Smart Grid & Green Power for OATI

EET&D: Distributed Energy Resources (DERs) are having a huge impact across multiple industries. How have they transformed the energy industry, and what is the impact on the grid?

Ipakchi: The growing volume of DERs, especially solar PV and battery storage, are having a significant impact on the power industry. At the bulk power level, PVs are impacting the system load shape, reducing net demand mid-day, and increasing ramping requirements in the early evening. As a result, some regions, such as California, have started experiencing negative market prices for energy in mid-day and higher prices in the evening. This has created opportunities for storage assets to shift demand from evening to mid-day. The intermittency of solar generation has also increased the demand for balancing and regulation services, but where the most impact is occurring is on the distribution grid.

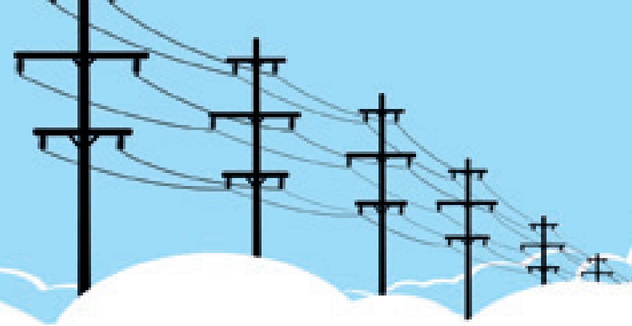
DERs create operational and reliability issues as they impact voltage levels, phase balances, and system losses, as well as create the potential for reverse flows, which challenge protection and control systems. On the other hand, if DERs are properly managed, they can provide enhanced distribution reliability, improved supply economics, and higher levels of system resiliency. As many DERs are owned by end-use customers or aggregators, more attention also needs to be placed on customer services and customer management. Furthermore, with increased levels of customer-side and customer-owned generation, utilities need to adopt their business models with new revenue generating customer services.

Power companies need extended capabilities to manage DERs and to deal with large volumes of data for monitoring, scheduling, dispatch, and control of resources, while maintaining distribution reliability and addressing customer related issues. Distributed Energy Resource Management Systems (DERMS) are able to bring together the functionalities needed for distribution reliability management and combine them with customer side programs and services, while providing capabilities for DER management and scheduling, as well as economic optimization.

Distribution Management Systems (DMS) primarily model the electrical characteristics of the distribution grid. With the emergence of DERs, distribution utilities are no longer just operating the wires, but also managing these resources, most of which are owned by customers. A DERMS needs to manage customer contracts, various tariffs, and, perhaps soon, price-based transactions for the supply of various grid services.

EET&D: In addition to the customer service challenges, what are the engineering challenges? What happens to the grid as more and more DERs are out there?

Ipakchi: On the distribution grid, DER challenges are more localized. For example, you may see a higher penetration of solar PV and electric vehicles in a more affluent neighborhood. The circuit serving the neighborhood may experience reverse flows mid-day and higher peaks in the evening, as more people plug in their vehicles after coming home. There will be impacts on the voltages, losses on the circuit, the loading on transformers, and the substation serving the neighborhood.



If the utility has the ability to monitor and control all of these assets through a DERMS, they can drastically minimize the operational and technical impacts. They can also use the DERs to provide reactive power support and improve voltage on the circuits. Aside from demand response, using behind-the-meter assets is not a common practice in the industry at this time.

Under regulatory pressures, some utilities are considering, or have already undertaken, the non-wires alternative approach to address distribution constraints or transmission congestion issues. Surgically deployed DERs can provide load relief, voltage support, or other services needed to address these reliability issues. Other utilities now consider DERs as a component of their resource adequacy and a source of grid services, including capacity, reserves, and frequency regulation.

EET&D: Why is the ability to forecast down to the end-use level so important, and what are the factors that have to go into those forecasts?

Ipakchi: With high levels of DERs, forecasting distributed generation levels, demand, and dispatchable load at circuit levels has increasingly become an important requirement. Without it, you will only be able to operate in a reactive fashion. A system with good forecasting allows utilities to know where things are going to be in ten minutes, an hour, two hours, four hours, six hours, etc., and enables them to take corrective measures as needed. These proactive measures drastically improve economics, enhance system reliability, smooth out relationships with grid service providers, and improve overall operations.

A good forecast is driven by data. It requires information regarding the capacity of circuit locations of solar panels, electric vehicle chargers and charging patterns, storage assets, and demand response capabilities. Good forecasts can be generated when this information is combined with local weather forecasts and other statistical data.

EET&D: What are the concrete impacts utilities are feeling right now or will feel in the next one to two years?

Ipakchi: The growth of demand-side resources has a fundamental impact on the Integrated Resource Planning (IRP) process. IRP projects supply and demand needs and provides a plan for meeting demand with planned generation resources, while considering transmission and distribution needs. Traditionally, IRP relied on system load forecasts, generation, and transmission planning. As we move forward, utilities will need to take a closer look at what's going on at the demand side, evaluate the growth of DERs, and also assess how much resource flexibility and dispatchability they can have on the demand side.

Another thing that is important is the concept of resiliency. Resiliency is different from reliability. For example, if you're a utility out in the middle of the country, the chances of losing power for a couple of hours, or even a day during a tornado or other severe weather conditions, is something you're trying to prepare for. Resiliency is important in this scenario so that the available DERs, combined with distribution switching, can be utilized to provide power to critical infrastructure, such as the police department, a place to charge cell phones, etc. Distributed resources can be positioned by the utility or by customers through incentives to create a resilient neighborhood or resilient districts. Investing in district energy services is something I highly recommend to all utilities, since it demonstrates customer care and their value for communities.

EET&D: Thank you, Ali. We can't thank you enough for taking time out of your busy schedule to speak with us.

About the Author

Dr. Ali Ipakchi has over 33 years of experience in information technology applications to power systems and electric utility operations. As the Senior Vice President of Smart Grid and Green Power at Open Access Technology International, Inc. (OATI), he is responsible for product design and development as well as business growth in Grid Modernization and Grid 3.0 areas. Prior to OATI, Dr. Ipakchi was Vice President of Integration Services at a leading consulting firm, assisting utility clients with roadmaps, specifications, and implementation strategies for operational and automation systems, particularly in the Smart Grid area. He has also held various senior management positions at leading T&D system vendors supporting power application development and system solutions delivery to the power industry. Dr. Ipakchi has led new business-line and corporate development initiatives. His areas of experience include utility and power systems operations, enterprise and operational IT systems, utility automation, System solutions for distribution, transmission and merchant operations, and for ISO and emerging DSOs. Dr. Ipakchi is co-holder of several U.S. patents on power systems applications. Dr. Ipakchi received his Ph.D. from University of California at Berkeley.

GREEN OVATIONS

Innovations in Green Technologies

Get Active: A New Approach to Energy Management

By Bill Brewer

When it comes to energy and sustainability management, the pressure on organizations has reached a tipping point. Global energy and climate concerns are spelling the end of business as usual. While consumers and shareholders are demanding that organizations be better corporate citizens and increase transparency, governments are establishing more reporting requirements.

At the same time, advances in energy markets and technologies have given companies more control over how they consume energy, where it comes from and how much it costs. And as energy demand continues to rise, utilities and businesses alike are feeling the strain as they are asked to increase efficiency and self-generation initiatives.

In the midst of these changes, many companies have found themselves at a crossroads. Charged with reducing energy costs, risk and impact, they must also maintain their operations and remain competitive. Many organizations face a common roadblock: decision makers and data often operate in disconnected silos, making it impossible to manage the complexity and maximize the ROI of energy and sustainability programs.

These decision makers – who hold titles ranging from procurement officer, to operations manager, to sustainability director – each bring immense worth to the table. But maximizing the value of their efforts requires teamwork, a joint venture to manage energy and environmental initiatives as part of a cohesive strategy. The whole can deliver greater returns than the parts.

So leading companies are changing how they buy, sell, use and track electricity, natural gas and other resources. Combined management of these activities offers a holistic view of their performance as well as access to the data decision makers need to refine their strategies to drive innovation. By following a collaborative approach, organizations can create real-time and long-term savings, and gain a significant competitive advantage in the marketplace.

As businesses embark on their individual journeys in this new energy landscape, three powerful trends have emerged:

Decarbonization

With increasing pressure from consumers, investors and regulators, organizations must commit to significantly cutting carbon emissions over the coming years to reduce their environmental impact. Similar pressures from the European Energy Directive (EED) and Paris Agreement have increased the desire for public disclosure of energy and sustainability practices to increase corporate transparency and accountability.

The move towards decarbonization is already apparent as the renewable energy market is set to grow substantially over the next 15 years. Consider the following data points from the International Energy Agency's World Energy Outlook 2016 report:

- The average cost of wind power has plummeted 60 percent since 2009, falling below $20 per megawatt-hour in many markets.
- Four-fifths of companies are planning to build out their renewables portfolio with multiple types of transactions (e.g., off-site power purchase agreements and on-site installations).
- By 2030, investment in renewable generation is expected to outpace fossil-fueled generation by 60 percent.

One way organizations are reducing their carbon impact is through carbon markets, which place a price on the emitting of carbon in a way that allows less carbon-intensive activity to become economically beneficial. For example, organizations may be required to purchase permits to release a certain volume of emissions from coal-generated power. Permits for natural gas emissions generally require only half the permits of comparable coal generation.

Layer on fully renewable options like wind or solar, and the opportunities for cost savings on energy as well as permits become significant. This is just one approach to meet the environmental challenges of the 21st century.

Decentralization

Electricity is generated primarily by large power plants owned and operated by utilities or other independent power producers. This centrally generated electricity is then distributed across country- or state-wide grids through transmission and distribution lines and substations. However, an increasing number of companies are taking advantage of distributed energy resources (DERs) which can include technologies like on-site solar panels, combined heat and power and fuel cells and batteries.

Renewable energy, particularly solar and wind energy, is the fastest growing source of electricity today. In addition, the cost of renewable generation continues to drop, fueling market growth and its integration into traditional grid networks. Although the continued shift to incorporating renewable energy sources can be challenging, utilities that support customers with this transition will find the benefits outweigh the negatives.

As DER technologies improve and costs continue to decrease, the grid will evolve. The electricity grid of the future will be comprised of many small, decentralized microgrids that give customers greater control over the source of their electricity. Energy will be generated, stored and distributed closer to where it's used, thanks to solar, wind and other renewable energies and storage technologies.

New distributed generation capacity will exceed new centralized capacity by as early as 2018. The end result will be greater energy reliability, which is something all utilities strive to deliver and constituents demand.

This smarter, more decentralized electrical system has the potential to increase overall efficiency, resilience, security and environmental sustainability – all while opening new opportunities for services and business.

Digitization

Smarter, more efficient energy use is also being driven by operational technologies and the Internet of Things (IoT). The IoT has brought unprecedented interconnectivity to everything from the power plant to the plug and improves the generation-to-consumption value chain. Not only will the number of connected devices increase in the coming years, but so will the granularity of the data that these devices produce.

The knowledge gained from IoT presents new ways for utilities to improve customer interactions. For example, when they send invoices, they can include detailed information about energy use – e.g., consumption patterns, historical trends and comparisons to companies with similar operations and footprints. Energy and sustainability teams can combine this data with information from enterprise systems and analysis to:

- Plot and visualize the impact of energy utilization at a portfolio level
- Make changes to loads in real-time to avoid costly peaks
- Make better use and purchasing decisions in response to real-time grid signals
- Run simulations to understand the long-term impact of initiatives against targets
- Improve efficiency by controlling consumption in real-time in response to changes in weather, occupancy and production scheduling

Consumers, too, are increasingly adopting technology that not only maximizes energy efficiency but also automates their behavior for ease of use. For instance, smart thermostats can be programmed for maximum efficiency so they're not heating or cooling an empty house. This new level of automation makes it even easier to use energy responsibly.

Looking to the future

Declining renewable energy costs along with increasing outside pressure have created a unique opportunity: true collaboration between sustainability, energy efficiency and energy procurement teams. The trends driving the move to active energy management are universal and impact businesses in all sectors.

The practical implications are significant. Companies can use data, technology and innovation to develop new strategies to reduce their carbon footprint, improve resiliency and create new cost-reduction opportunities.

So what might an active energy management future look like as businesses move closer to convergence across the domains of energy supply, energy efficiency and sustainability? Here are examples of the impact of this type of convergence:

1. **Energy Becomes an Asset, Not a Cost Center**
   Historically, many companies viewed energy as a fixed cost to maintain ongoing operations. However, as markets decentralize, organizations that tap into the grid can consider partnering with other participants. For example, one company buying energy from one utility isn't the only option. Companies that see energy as an asset can reduce their operating costs and potentially create new sources of revenue that can positively impact profit margin.

2. **Strategic Sustainability Delivers Value**
   As larger firms deploy coordinated strategies and see the business benefits of active energy management, they are turning attention to their supply chains. By supporting suppliers to help mitigate risks and improve resiliency, suppliers can then reduce costs and pass through the savings from improved efficiency.

3. **New Business Models Remove Financial Barriers**
   When companies add up all the explicit and implicit costs of energy such as backup generation, maintenance and training, they may find the actual price of electricity is double or even triple the line item amount on their bill. New business models like energy-as-a-service (EaaS) mean companies can delegate their energy program and spending to a trusted advisor, allowing them to focus on their core business.

Businesses and utilities alike can't afford to wait to act – they must take this opportunity to facilitate energy efficiency, support innovation and increase renewable adoption today. Rather than looking at a carbon-neutral world as a barrier to operations, organizations should focus on the advantages and strategic value active energy management brings.

About the Author

Bill Brewer is Vice President, Regional Operations – Americas, Schneider Electric. He is responsible for the oversight of Schneider Electric's client energy portfolio for natural gas, electric power, alternate fuels, carbon and renewables. He has extensive experience helping clients develop risk profiles for energy procurement and environmental sustainability strategies. Over the past few years, Bill has helped centralize Schneider Electric's global Sustainability services for clients. He formerly served as a wholesale trader for natural gas and electricity in the western United States for Merrill Lynch and Allegheny Energy. He also served as a portfolio manager, managing a 1,250 MW portfolio of financial and physical generation assets in California and Nevada. He has extensive background in electricity risk management, wholesale energy trading and the underlying fundamental influences shaping the energy markets.

Bill earned a bachelor's degree in Business Administration from Bellarmine University and a master's degree in International Business from The University of New South Wales, Sydney, Australia.

From Research to Action

EPRI's Telecommunications Initiative: Fiber Optics for the Future

By Tim Godfrey and Christine Hertzog

The Electric Power Research Institute (EPRI) recognizes that today's power grids and advanced grid initiatives need reliable, resilient, flexible, and secure telecom networks. Fiber optics networks play increasingly strategic roles as their uses move beyond teleprotection and supervisory control and data acquisition (SCADA). Electric utilities were among the first adopters of fiber-optic communications because its dielectric or non-conducting nature provides increased safety and reliability over copper-based wireline telecommunications.

EPRI's Telecommunications Initiative is examining questions utilities have about fiber-optic networks as part of its six-part research investigation. See the September/October 2016 issue of Electric Energy T&D for more information about the project scope, which will be completed at the end of 2017.

EPRI's collaborative approach brings together utilities and our technical experts to create consensus-based answers to these fiber network questions confronting utilities that are considering deployment or expansion of fiber optic networks:

- What are the best practices for installation, operation, and maintenance?
- What are beneficial uses for fiber networks beyond substation communications?
- Are shared fiber networks workable and what are the best practices and business models?
- What is the fiber lifecycle and the tradeoffs for cable types such as optical ground wire and all-dielectric self-supporting?
- How can we justify cost and secure funding for fiber networks?

Fiber – part of everyone's diet and network?

The research topics in the Strategic Fiber track of the Telecom Initiative are based on a foundation of knowledge about fiber optic fundamentals for utilities. Our researchers documented the basics, such as cable types and their applications, network designs, and variable factors that influence equipment and installation choices. This step helps ensure that all research participants have accurate and consistent knowledge to inform their fiber decisions.

The research is developing an inventory of common utility fiber network uses as well as a review of other deployments that offer options for utilities. While the most universal utility applications include teleprotection and SCADA communications, our research identified five other potential applications that are deployed at utilities and can alter today's fiber cost-benefit analyses and assumptions.

A web of ownership options and legal/regulatory issues impact cost-benefit analyses

Many utilities are challenged with legacy and current decisions about fiber network ownership structures and the related issues of who operates and maintains these networks. Some have in-house resources and budgets that can support full ownership and these network assets, but other utilities face constraints related to staffing, funding, or regulatory policies that make third party ownership and-or maintenance arrangements more feasible.

From Research to Action

Coupled with that are a range of legal and regulatory issues. Since telecommunications service providers have regulatory oversight at federal, state, and local levels, utility fiber decisions are strongly influenced by unique factors that probably change at state borders.

A key finding from our ongoing research indicates that fiber networks solely dedicated to serving utility locations have a much lower frequency of additions, moves, and changes of fiber connections compared to service provider networks. This contributes to a reduction in unintentional outages. That finding has implications for cost justifications, one of the most complex topics within fiber network discussions.

Fiber network investments have both capital and operational funding aspects that must be compared to alternatives involving hybrid or third-party ownership. Our research revealed interesting decision trends regarding capital versus operating expense when third party service providers are involved. Results also emphasize the importance of breaking down siloed perspectives by adopting a strategic analysis approach to fiber network decisions.

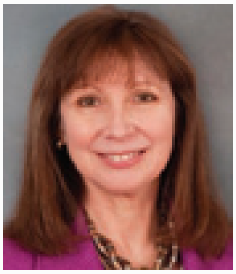
What's next for utility fiber networks?

Two other common challenges were identified by surveys and assessments of Telecom Initiative participants. Utilities with legacy fiber have increasing age-related failures in that equipment, and lack experience in how to proactively plan maintenance tasks and procurements. Workforce issues of understaffing or absence of staff with relevant skills to plan, design, deploy, operate, and maintain fiber optic networks also loom large.

Our final fiber research report will be distributed to participating utilities by the end of 2017, although preliminary results are being shared now. This will not be the termination of our research activity into the roles and recommendations for fiber optic networks in utilities. EPRI's 2018 telecommunications research will include investigation of potential methods for expanding fiber deeper into utility distribution systems to support advanced grid and distribution automation initiatives.

About the authors

Tim Godfrey is a technical executive with the Electric Power Research Institute, specializing in telecommunications. He manages the Telecommunications Initiative, a research project addressing the key challenges utilities face related to the telecommunications infrastructure supporting the smart grid. He holds a BSEE from the University of Kansas and has worked in the area of wireless networking and communications for 20 years. He has 23 granted patents. Mr. Godfrey has participated in IEEE standards development since 1994. He is the chair of the IEEE 802.24 Smart Grid Technical Advisory Group, and the IEEE 802.16 GRIDMAN Task Group.



Christine Hertzog is a technical advisor for ICT and Cyber Security at the Electric Power Research Institute. She was previously the founder of a consulting firm focused on smart grid ecosystems and has an extensive telecommunications background. She authored the Smart Grid Dictionary, and co-authored Data Privacy for the Smart Grid. She has also served in an advisory capacity to innovators, industry associations, and publications. She has an MS in telecommunications from the University of Colorado, Boulder.

The Internet of Things Starts with the Grid of Things – Part 3

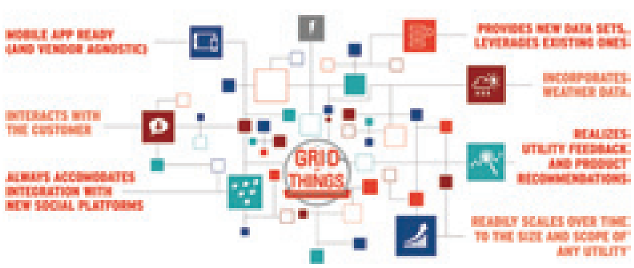
By Peter DiSalvo

When Electric Energy T&D approached us and said they were passing the baton to me, a software developer, for Part 3 of *The Internet of Things Starts with the Grid of Things*, I abruptly said, *"don't you mean you are passing the toast"*?

For those of you that missed Part 1 and Part 2, *The Internet of Things Starts with the Grid of Things* is a five part tell-all editorial series that began with us giving away a big secret:

"I want my toaster to talk to my Utility."
Zac Canders, Co-founder of DataCapable

Part 1 announced the secret. Part 2 complemented it. Part 2 provided a step-by-step manual on how to embrace interoperability. A call to action, to "Become Interoperable". It provided the details on how to collaborate, embrace standards, and create APIs. Part 2 laid forth the argument that to drive the next generation of the utility industry, collaboration and involvement must occur.



The Landscape Is Changing and So Is Software Development

We all agree that the utility industry is changing fast. Fossil fuels are being replaced with green alternatives. Microgrids, renewables, and batteries are now a common theme at every utility around the World. Whether we call it a revitalization (or maybe even a revolution) the current dynamics and state of the utility industry make it an exciting time to be involved. The modularity of today's software and platforms has yielded newfound opportunities for creative and exciting capabilities that previous generations only dreamt of. Each employee is not only part of a company's strategic revenue plan, but can also be part of a much broader vision, *the Grid of Things*. But how?

More importantly, Who...

First, I need to take a step back. The evolution that the Grid of Things series addresses is how the 'toaster' is a simile for something much more meaningful:

> *"The idea of your toaster talking to your utility doesn't make sense. Who would want to skip breakfast just because electricity is a few pennies more that day"? - Peter DiSalvo, CTO and Co-founder of DataCapable*

The 'toaster' in this series is interchangeable with any device in your home. If the call to action, "Become Interoperable", is based on standards and API's then Part 3 is the logical definition of the individuals responsible; the software developers, product managers, and technical experts that are moving device-to-utility communications from the realm of 'possible' to 'inevitable'.

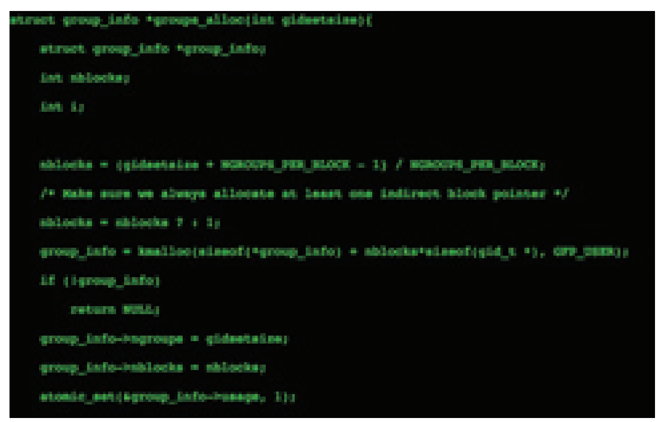


Figure 1: Code is what is driving change in the industry

Building the Grid of Things Requires Passion

"*Why are you a software developer*?" This is the first thing I ask any potential software engineering new hire. And here is why you should too:

Whether it's their first day in the utility industry or a seasoned developer looking for a new role. As a development manager, it's important to build a team that is passionate about software. You need people that are truly passionate about creating applications and solving problems with code, regardless of the use case. The type of people that will create a new app for fun instead of watching a movie on a rainy day.

The Grid of Things isn't a millennial vision...

Generational challenges do exist and the software teams building the Grid of Things must work well together. Working as part of a team means that self-motivation, excitement to solve problems, and learning new skills are keys to the success of the entire organization.

The younger generation is likely to jump from job to job every couple years early in their career. I fall into this category having held 5 jobs in 10 years as a developer. Software development managers can try to mitigate turnover by constantly challenging your team and allowing them to embrace new and exciting technologies. Have an "Innovation Event" once every quarter that allows the team to drop their tasks for the day and build something for fun that can help the business grow.

In contrast, the older generation has foundational expertise that can support processes and technology adoption guidance that will ultimately ensure a company runs smoothly. These seasoned team members have lived through decades of development trends and understand the impact of adopting an immature technology. Leverage these team members to ensure that technology adoption, maturity, and general big picture considerations are analyzed before new technology is adopted. The last thing you want to do is select a technology that isn't the right fit for your solution and won't be supported in a year.

It's also important to recognize that while passion for development is important, it's also essential to encourage and embrace the team's passion for things outside of work. Doing the same thing day in and day out will get tiring for anybody. Working long hours without something to relieve stress or give the brain a break will ultimately burn any team member out.

The Grid of Things Is the Evolution of Technology

The utility industry has figured out how to gather large amounts of data. This is evident with things like smart meter (AMI) data. Most product and service providers have a clear understanding of how to gather, store, and analyze big data. The next big wave of technology involves using the insights gathered from big-data and automating existing inefficient processes within an organization.

This trend is happening across every industry. In 2017, a software developer does not have to be knowledgeable about all fields. There are third party experts for every niche and these experts provide API's for easy integration.

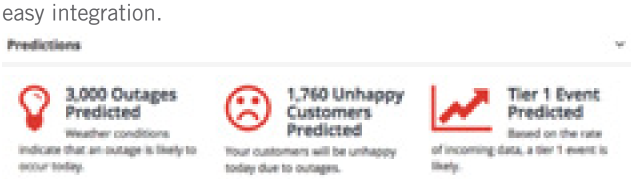


Figure 2: API's can enhance the capability of a software solution and enable predictive intelligence

Gone are the days where a developer has to be the expert

Software companies are turning their areas of expertise into API's for others to use. Companies can focus on the things that they do well and not worry about the rest. Each company can generate revenue on individual pieces of their functionality. For example, a software developer can use an API that's available on the web to run some advanced algorithms that require very specific skills. This functionality would be expensive for a company to build on its own. This modularity opens value for both the business and its customers. Software companies have the liberty to focus on their core capabilities and leverage the expertise of others when needed.

The power of the cloud

Moving software to the cloud is inevitable. The utility industry must accept this. It's an uncomfortable situation for a lot of utilities and vendors because they lack the proper knowledge and expertise to do it the right way. Moving software to the cloud can enable interoperability, accessibility, and if done correctly, enhance security.

The role of standards

Standards are an important aspect of interoperability, collaboration, and adoption. Within in your system, you're free to follow best practices and your own standards, but communication outside your platform should follow well known and accepted standards. Keep in mind:

- Sometimes standards may use outdated or clunky technology to support older platforms and due to a lack of support.
- It's important to get involved with standards bodies and make sure that standards are done correctly with the latest accepted technology. It's hard to motivate a team when they're stuck working on old, boring technology.

The Grid of Things Depends on Collaboration

Each software developer is playing an active role in the Grid of Things vision. API's and collaboration is enabling software platforms and companies to do things that never were imagined before. I personally want each and every one of you to get involved. Send me a note at *Peter@DataCapable.com*.

Collaboration is the most important aspect to advancing technology. Without collaboration, every business would be wasting time rebuilding the same functionality over and over. As we look to the next installment of the Grid of Things, Collaboration will be that key element. How we, the industry, are becoming interoperable. And as hinted in Part 2, it will conclude in an industry first (and extremely exciting) demonstration that's going to require your help.

About the author

Peter DiSalvo is CTO and Co-founder of DataCapable. He is passionate about new and exciting software and pushing the boundary of what is capable with a software platform. His work has been recognized by publications such as Forbes, TechCrunch, Wired, Telegraph, and The New York Times. His experience includes building software for U.S. Navy destroyers, large-scale military unmanned autonomous aircraft, augmented reality language translation apps, and the smart grid. He is a full-stack developer and his experience encompasses technical leadership, graphical user interfaces, API development, android development, and distributed infrastructure development.

Renovating T&D Systems – A First Step Towards Implementing a Modern Grid

By Kay Stefferud

Distribution and Transmissions systems are evolving to accommodate increasing amounts of renewable distributed generation (DG) while also dealing with more intense storms, cyber security threats, evolving markets and aging infrastructure. Adapting to these changes requires necessary adjustments to protection schemes, fault detection, outage management, market interfaces, grid topologies, and a host of other considerations.

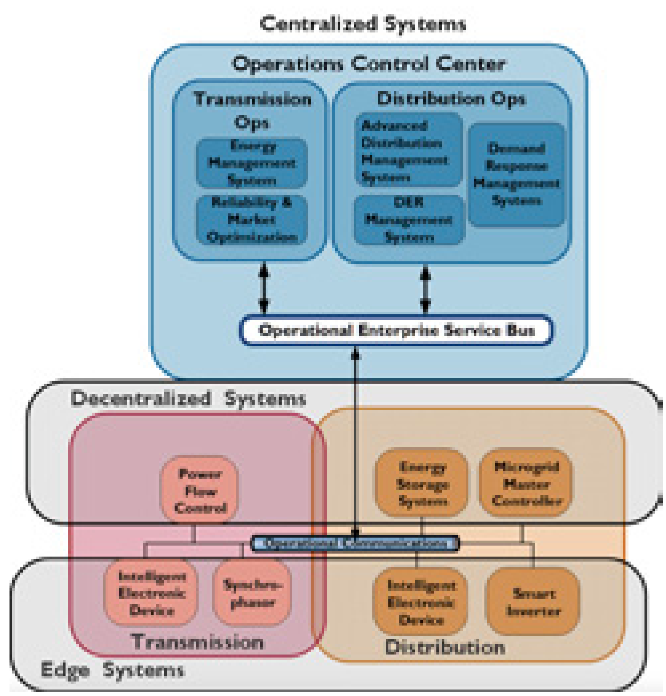
At the same time, advances in communications as well as intelligent grid monitoring and control devices have created tremendous amounts of data reporting details of current grid conditions. Available data can provide operational insight and enable control systems to manage the complexities of two-way power flows, the intermittent nature of wind and solar generation while also better managing storms and proactively identifying equipment which needs to be replaced. Proper management and analysis of available data can provide situational awareness enabling utilities to respond to increasingly dynamic load profiles as well as reverse power flows.

The question is how to incorporate planned and existing T&D equipment, sensors, intelligent control devices and communications systems to effectively integrate DERs, improve reliability, and better manage aging assets. Effective implementation of both an enterprise architecture and a data management strategy can enable the modernization of T&D systems necessary to address the many challenges currently facing electric utilities. This article begins with the rationales for enterprise architecture and a data management strategy, and then presents a solution approach to systematically implement a modern grid.

Historically, power flowed from bulk generation sources to consumers, with baseload generation, peak generation and ancillary services ensuring that energy demands were met. Generation and transmission systems were centrally managed while distribution systems required little active control. The voltage and frequency deadband was large enough to accommodate the small amount of DG that was installed on the distribution system.

Today in increasing portions of the grid these assumptions are no longer valid and with further disruptions possible because of future unknown market mechanisms and future technological changes, more flexible systems are needed. In particular, a system of systems (SoS) architecture featuring distributed and edge controls is needed as well as an effective data management strategy.

As shown, enterprise architecture with new and existing centralized control systems such as Advanced Distribution Management Systems (ADMS) and Distributed Energy Resources (DER) management systems can address increasing dynamic conditions on distribution systems.



Decentralized and edge control systems including field message buses (FMB), intelligent electronic devices (IEDs), smart inverters and energy storage systems can meet timing requirements and reduce the communications bandwidth required for centralized controls. Decentralized and edge control systems efficiently monitor and manage assets leveraging three fundamental advantages. First, edge and decentralized controls can react much more quickly than centralized systems which have a built-in communications delay. Secondly the large number of new devices makes centralized control unwieldly.

For example, with utilities now reporting hundreds of thousands of DERs, centralized control, especially if human operators are needed, is simply not possible even if the necessary communications bandwidth were available. Third, delegating controls such as DER schedules to distributed and edge devices allows for data analysis and management to be distributed to many devices. Doing so reduces the need for large complex centralized systems and large-bandwidth communications networks. Decentralized and edge devices can make decisions using local data based on pre-determined parameters, sending overall results to centralized systems which can then optimize the overall T&D systems.

Distributed and edge controls are both necessary and feasible. For example, edge controls such as smart inverters attached to DG and distributed controls such as community energy storage systems can provide real time control of voltage and reactive power on distribution circuits. Centralized systems can then perform state estimate calculations based on received data.

An architecture using edge, decentralized and centralized processing is an enabling technology necessary to utilize the vast qualities of available data. In addition, data analysis capabilities and data management strategies are needed to leverage the data from sensors and intelligent devices. Data management capabilities include time alignment, operational analysis, data mining and data analytics.

Time alignment is the process of time syncing data points as well as techniques to filter data when too many data points are received and techniques to estimate data points when too little valid data is received.

Operational analysis is the process of integrating raw data from multiple sources into meaningful knowledge. Data fusion transforms raw data into situational assessments, impact assessments and recommended improvements to sensor settings.

Data mining identifies patterns in data using statistics and advanced techniques. It is used to identify factors relevant to outcomes of interest. For example, data mining can be used to identify sensor readings indicating a high probability of an asset failing.

Data analytics will allow the vast amount of data available to be leveraged and effectively applied to address the challenges facing today's grid control systems. Data analysis includes advanced techniques such as machine learning.

Realizing that decentralized control and data techniques can improve and optimize today's increasingly complex T&D systems is the first step in architecting future grid systems. The next step is to define the solutions needed to implement the modernized grid systems. For generation, transmission and distribution utilities, architecture building blocks can be used to transform existing systems into future grid systems which address many challenges including business model challenges, increasing severe storms, aging infrastructure and uncertain future markets.

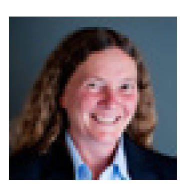
As shown below, enterprise architecture building blocks highlight implementation of the decentralized processing and data management strategy. At the base are hardware based solutions including common IT platforms typically with multiple processors, storage area networks (SANs), firewalls and other cyber security products. Other base solutions are common data repositories and Field or Wide Area Networks (WANs) which are typically based on dual IPv4 and IPv6 protocols. Mid-level architecture blocks include standards-based data models, typically IEC 61850, standard communications protocols such as DNPv3 and standard message formats such as MultiSpeak. Standards-based communications protocols and message formats are a key enabling technology for the Internet of Things (IoT), for devices such as cellular phones, and for apps which run on many types of devices. Using standards-based communications technology will help enable faster implementation of modern grids.

The next level of architecture blocks are application integration technologies including web-based Application Programming Interfaces (APIs) and Graphical User Interfaces (GUIs) with a common look and feel for all applications.

Architecture Building Blocks

After defining architecture building blocks, the next step is to define common architecture details for operational systems. This step defines communications, data and application specific solutions such as IEC-61850 based profiles and web-based service interface definitions, integrated firewalls/intrusion detection and prevention systems, and protocol translators for communicating with legacy equipment. Adaption of enterprise architecture using the steps outlined here can be used to integrate increasingly large numbers of DGs, improve operational efficiency and adapt to new markets using data analysis and management techniques, standardized data definitions/protocols and cyber secure communications.

About the author



Kay Stefferud is Director of Implementation Services for EnerNex. She is a collaborative, versatile and results-oriented system engineer, who has 30 years of technical, program and team leadership experience in dynamic, rapidly-evolving environments. She uses her analytical problem solving skills in architecture development, requirements specification, procurement, design, test and system deployment. Kay has full project experience from concept development to system installation and training. Kay's projects include specifying, designing, and testing microgrids, assessing the impacts of distributed energy resources including solar PV systems, and developing enterprise architectures and innovative energy solutions.

LoT's Role in Embracing the Future of the Grid

By Stewart Ramsay

There are a great many people in the market that suggest that the electric transmission and distribution network has outlived its usefulness and that as a country we should no longer be investing in the grid. While that may be a goal for many, I believe that it is a goal that is neither practical, nor realistic in the foreseeable future. There are a host of reasons why we will continue to be dependent on our network, not least of which is the role that it has played and will continue to play in increasing the percentage of renewable energy in the mix and its substantial role in helping to significantly lower the costs of renewables. In short, electricity networks have been and should continue to be a major enabler of the growth of our economy. They have seen us through our industrial growth and can provide the same value to the growth of our low carbon, renewable energy economy.

We need the network, though clearly it must change, to adapt and become part of something much larger and more intelligent. Its role has changed from being the sole source of delivered energy, to being an enabler of: new technologies, new capabilities for customers, new markets for energy, and most significantly the enabler for a greener economy, and the networks can only do this through embracing and leveraging IoT.

So, clearly IoT has huge potential for the grid and to bring benefit to customers, the economy and our society overall. It also has potential to be a significant cost and operational burden. Utilities already have a lot of data. Many are awash in data, and having far more data shows up as a cost burden and a liability (if you have the data and don't see what it is telling you…). There are data security and cyber security concerns which I won't cover in this article as they are worthy of deep discussions on their own.

IoT by itself is not the answer. The value lies in what we do with it. Throughout my career I learned a number of things, and one of the most important things I learned was this: Data on its own is worthless.

Leveraging processes, tools and systems to convert the data into meaningful information helps. What matters most is being able to take the data, create information and then use it to create new insights. It is the insights that enable us to make different and better decisions.

Around the globe new technologies are being deployed that allow customers to generate and store energy, to manage the energy use in their homes and businesses and to power their vehicles in new ways. In most cases these technologies are being developed to work in isolation with little consideration of the power that can be unleashed through having a seamless integrated and intelligent system.

More forward thinking utilities realize that we have a unique opportunity to redefine our role and to become the facilitator of an interconnected and intelligent grid. They see the value for customers in having their smarter homes communicating with the utility's systems to use energy more efficiently, expand and improve their quality of life, and to lower their costs of energy. Leveraging these technologies and harnessing IoT can create the ability for customers to trade energy with neighbors, family members or in economic markets. We can leverage this network of interconnected resources to enhance reliability and reduce the cost for all customers regardless of their economic means. If we are not deliberate and thoughtful in embracing IoT, we run the risk of IoT providing value to those customers who can afford new systems and technologies at the expense of those who can't.

In leveraging IoT, the role of utilities extends far beyond being the architect of this new era of customer empowerment. They become central to the customers and their primary relationship in everything having to do with energy and smarter living. This opens new dimensions for the relationship and, with it, new business opportunities. As the interconnectedness (information and electric) grows, the utilities can become a source of knowledge and insight offering strategies to save energy and lower costs. Utilities can be a partner that helps simplify their lives by scheduling necessary maintenance on their appliances; helping customers see when it is time to replace outdated appliances and pointing them to the best sources for purchasing new ones.

Utilities can be the enabler of energy transactions, or undertake those transactions on the customer's behalf, thereby ensuring that they optimize the use of their distributed resources and energy usage. In such a role utilities can ensure that even the least affluent customers are provided energy, and flexibility at the lowest costs in the market.

In an interconnected future utilities are the enabler of reinventing the customer experience, while creating a cleaner more streamlined energy value chain.

So how do we prepare our network and our business for the new role as driver of the new energy economy? We see three keys:

1. **Embrace this new mindset**
   As I listen to our peers in the industry, I realize some of them still see distributed energy resources as a predatory threat. As a result, they resist these technologies and rationalize their actions. We need to recognize that these technologies bring with them the potential to meet societal goals for clean air and GHG reduction. Moreover from a purely pragmatic network view, planned and deliberate integration of these technologies enables us to improve the efficiency of the network, reducing costs to customers while enhancing reliability and security of supply. These technologies are only a threat if we fail to recognize their value in our relationship with our customers. They are a powerful tool in advancing the state of the network and empowering our customers.

2. **See and build the fully integrated grid (electric and data), including customers and their systems**
   Historically, we have viewed the connection to the customer as the end point, the last stop in the delivery system. Our support of customers' quality of life has been limited. While we have engaged in Demand Response and Energy Efficiency programs, we have only recently begun working with customers in supporting intelligent homes (Home Area Networks – HAN), grid connected storage, and intelligent DER control.

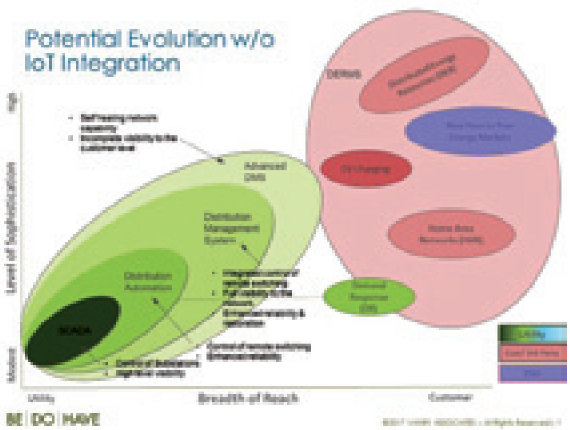
   With advances in end point technologies and IoT capabilities, we now have an opportunity to engage the customers in ways that were never available before. We expect that there will be a wide range of responses among the customers: from those that want simply to have a lower cost, more reliable supply; to those that want to participate in markets selling and buying excess energy. At minimum, we have the opportunity to offer our customers a far higher quality of life at costs below what they are paying now. We can engage with our customers in ways that we have not been able to engage with them since deregulation, and reestablish a strong and trusting relationship. Adopting a strategy of interconnectedness could allow our customers to see that we can provide their energy needs in whatever manner meets their requirements, from managing their energy consumption to optimizing their costs and providing the critical infrastructure that enables them to engage in energy markets.

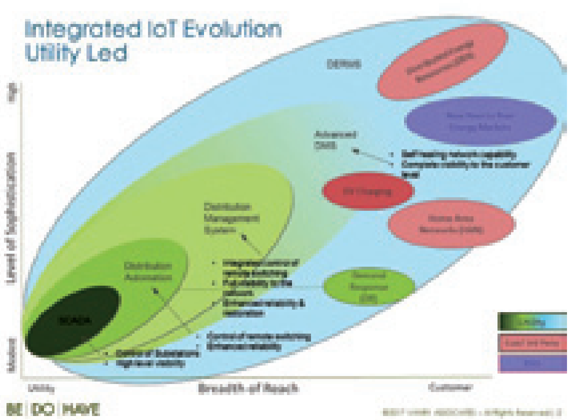
3. **Adopt and adapt new technologies while stewarding the network**
   There is no doubt that integrating distributed energy resources increases the complexity of the network and brings new challenges to the safe and secure operations of the grid. These challenges are coming, regardless of our decisions to embrace technology or not. By being proactive in adopting these technologies, we have a far greater hand in ensuring that we can continue to operate and maintain the network in a safe and reliable manner. Moreover, the utility is the entity that is best positioned to see where and how these technologies can bring the greatest value to the customer base as a whole. By leading, we can ensure that we take steps to avoid the pitfalls of previous decisions, where renewable integration came as a benefit to the affluent customers and at the expense of the less affluent ones. We have the ability to look holistically at the system and optimize the overall investment, using an appropriate combination of grid and non-grid investments. We understand how to leverage the output of new resources to support the grid rather than driving unnecessary investment in it. Over time, we believe that the nature of the grid will be transformed to something that is continually optimized and continuously evolving.

   It is in this third area where we must be most deliberate and thoughtful. As we look to a fully integrated customer-network grid, we recognize that the existing systems can only meet some of the immediate and future requirements. While many utilities are contemplating wholesale replacements of all of their key operational systems, IoT and advances in system technologies have created another form of solution. Over the years, most utilities have made many good system investments. Those systems however do not reach far enough to meet our needs. We do not believe that any one system is capable of meeting all of the needs, particularly when the technologies, policies and regulation continue to evolve. What we need is a system that can evolve with us, leveraging the tools that we have today, and allowing us to add new tools and new capabilities to meet changing demands. Typically, this 'Best of Breed' approach has been difficult to implement as integrating systems has proven problematic.

4. **Move to a "System of Systems" architecture for IT/OT and ET**
   Along with growth in IoT has come growth in capabilities in Systems of Systems. A System of Systems approach allows existing systems, sensors, programs, apps, cloud databases, to integrate seamlessly and effectively. It is in effect the 'universal translator' for IT, OT and External Technology (ET) systems. A SoS is the only practical way to fully leverage the potential being unleashed by IoT. The data that we need to run this future grid will exist in hundreds of different systems installed and owned by others. The notion that we can require standard interfaces is simply not realistic. We need to understand that we will have to work with what shows up, now and in the future, and it is only through a SoS approach that such universal acceptance and integration becomes possible.

Adopting a System of Systems approach could enable a fundamental shift in the potential evolution of Distributed Energy Resource Management Systems (DERMS). On our current course, DERMS appear to be emerging ad hoc in many locations. If we look holistically at what is in the best interest of all customers we might view that a more integrated DERMS (one that is amalgamated with the operation of the network) would produce the lowest cost and most reliable interconnected network.





5. **Build a durable strategy for communications infrastructure**
   In the world of IoT, communications will become even more critical. Today utilities rely on a multitude of communications media. This is likely to continue into the future as many of the sources of data will reside outside of the utilities and outside of their control. We will need to look realistically at the sources of the data and the most effective means of communications. We need to look at this pragmatically and over multi-year time horizons. The longevity of the communications paths need to align with the longevity of the data sources. Many utilities invested in end point devices that use cellular technology. Cellular has proven reliable and valuable in most cases. The concern that we now see is that cellular carriers are moving away from older 2G and 3G systems to 4G and 5G. Thus, utilities are forced to upgrade their fleets of end point devices due to the loss in communications infrastructure. While this may not require that utilities invest in their own communications infrastructure, it does suggest that communications infrastructure needs to be looked at as an integral part of the investment decision and the life cycle of all technologies, including communications, should be considered.

IoT holds great promise for customers and for utilities. Done well it can bring great benefits in lower costs, greater reliability, enhanced quality of life, and lower impacts on the environment. Done piecemeal, we run the risk of seeing significant investments with lopsided benefits. We owe it to all of our customers to embrace IoT in a pragmatic manner that brings benefits to all.

About the author

Stewart Ramsay is the Managing Executive of Vanry Associates, a global consulting firm specializing in strategy, leadership and executive coaching. Mr. Ramsay has more than 30 years of experience in leadership, operations, engineering and consulting roles in the global utility and technology industries.

Preparing for the Cost of IoT Deployments

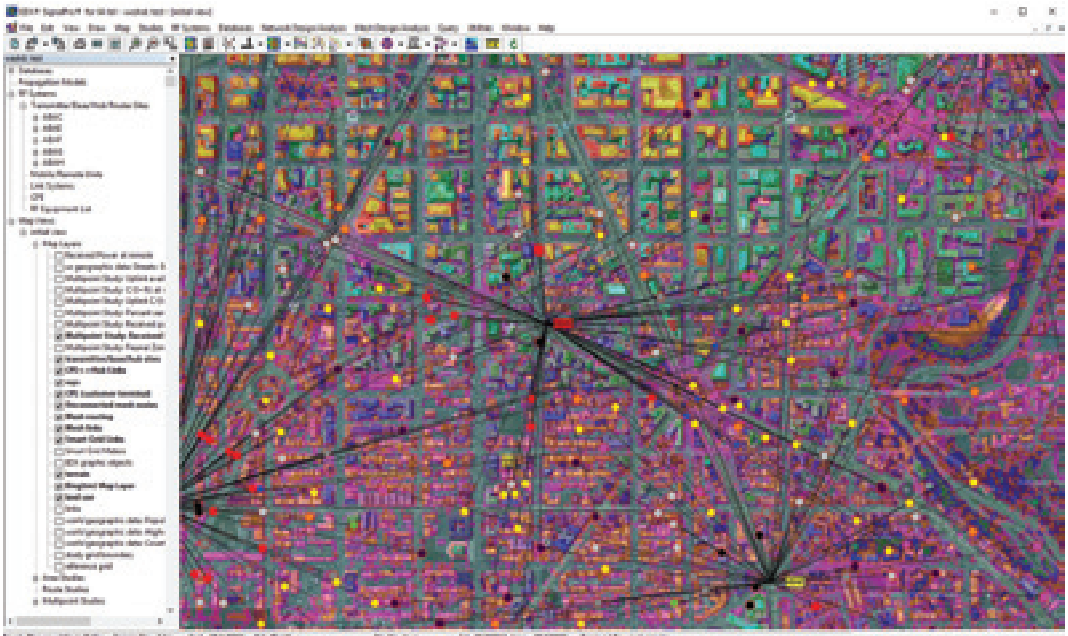
By Bob Akins

By many estimates, there is expected to be 35 billion IoT devices by 2020. So here's a good question; how much are these deployments going to cost? Of course, an individual business or government agency may be dealing with a small deployment made up of hundreds of devices only covering a small geographic region, but still; the question remains. And unfortunately this can be an overwhelming question even for the small IoT deployments because of the complex nature of these networks. Let's not forget that we're talking about networks made up of devices that are always on, always connected and always generating and transmitting vast amounts of data that can that can potentially be made up of any number of devices, technologies and system architectures. Aside from the obvious factors when estimating the cost of an IoT deployment, there are many others to consider. Perhaps many of them are overlooked because in many ways, we're not used to thinking about them, just as we're not used to such complex networks. But when we start considering these often overlooked factors, we get a more realistic picture of our network deployment costs.

For enterprise, IoT presents exciting opportunities to streamline operations, lower operating costs, manage fleet and much more. But these enterprises face the challenge of attempting to estimate the cost of IoT deployments while realizing this can vary greatly by the type of devices used and where the system is deployed. Furthermore, the factors that go into deploying an IoT network and the level of analyzation regarding performance, is often times outside the scope of what a business is used to when dealing with their business operations and expenses.

Similarly for vendors, the complex nature of these deployments may well be outside the scope of typical network deployments. One of the main challenges is realizing that each deployment is different from the next and the network design methodology that worked for Customer A may not translate to Customer B.

To be sure, the cost of an IoT deployment is an often discussed topic among enterprise, vendors and everyone in between. However, these conversations often take place under the assumption that the system is fully installed and operating. As such, the planning of IoT networks usually revolves around the data acquisition of system performance and traffic, real time reporting of device behavior, along with maintenance, field technician and battery replacements costs. This is not a completely misguided approach. Obviously all of these factors are vital and will play a huge part in the overall system cost.



Link information from base to fixed subscriber units

But let's not get ahead of ourselves. Before we have a functioning network, there are many things that can be done pre-deployment to ensure a properly designed system that not only keeps costs down but also performs optimally.

Furthermore, it is worth noting that things like network loading and the traffic patterns seen in the system will have a huge impact on how the system is performing overall. But, these factors would be in addition to architectural limitations should there be any. This is one of the reasons why we must take every step to ensure a robust system design.

Knowing that each IoT network may consist of any number of technologies and hardwares etc, there are still universal considerations to every network before deploying any type of hardware in any system architecture.

Let's first look at where the network will be deployed. Obviously each geographic region and area that may need to be served by an IoT network will be vastly different. This should be the first consideration when planning a deployment, because the physical characteristics of service areas are at the foundation of how much hardware will need to be employed to ensure coverage. To take into account these physical characteristics, it is beneficial to create a 3D model of the service area which can be done with any number of available database layers. However, given that IoT devices will be at or near ground level, and are greatly affected by buildings, structures, trees and other items at ground level, it becomes imperative to use databases that offer a realistic view of what the environment looks like. In other words, a database must be resolute, accurate and current. There are current and custom wireless network planning databases available that offer many different data layers such as land use, terrain elevation, buildings, land use height and social media data for traffic planning. These databases can be used in sophisticated wireless network planning software that allows you to create 3D models of the environment and then place network devices at various locations in the model to predict system performance.

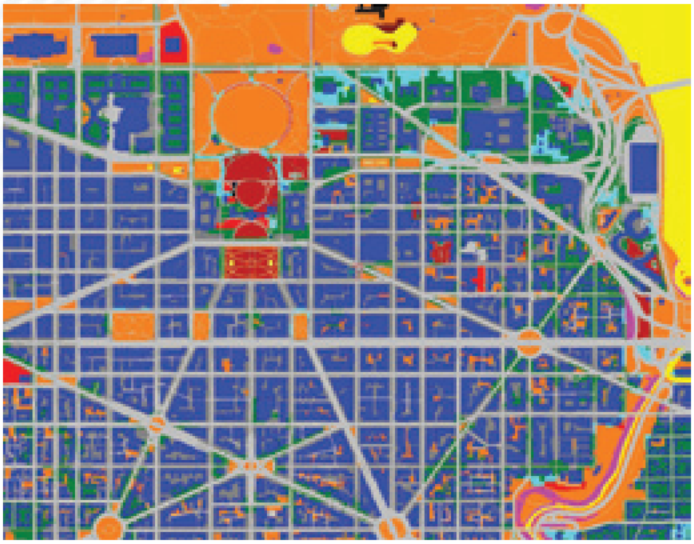
Area study showing system coverage in EDX SignalPro

Using the information learned from the 3D service area model…when can then begin the process of determining how much hardware will be needed. Let's say for example we need to install collectors to serve mobile/end-user units. Using the information from the 3D model of the service area, along with a list of pole and/or asset locations, it can be determined how many collectors will need to be deployed in order to serve these mobile units. Obviously, this will help prevent the over-provisioning of a deployment and keep our costs down. This examination of collector locations can include any number of parameters. In addition to the service area database and tower and pole information, we can also include street vector and intersection information, building data, technical specification such as equipment receive sensitivity and maximum distance and more.

Because each piece of hardware will have different specifications and limitations, it is important to consider these in conjunction with the aforementioned service area characteristics. Think of how some hardware with a given set of specifications may perform in a rural area versus an urban area for example.

When used accurately, this information can also be used to get more in-depth with our network deployments. If our hardware contains any capacity constraints for example, this information can be used in conjunction with the physical characteristics of the service area when assessing collector location. For example, if our collectors have a maximum amount of allowable traffic, or if there are throughput limits on links, then we can account for such constraints and either relocate a collector or add another as necessary. These types of calculations will help ensure that we have designed a balanced and scalable system.

As such, these constraints become a vital component of our planning not only for the initial deployment, but also in ensuring optimal data flow. In turn, this keeps maintenance and back-end costs down as well as ensuring that the system is scaleable and will be able to accommodate system expansions and new users.



Clutter Database from EGS Technologies – depicting land use in Chicago

Another way to help ensure a successful deployment plan, perhaps particularly for startups, would be to get some real world measurements of your devices' behavior in the field. A small test site and pilot system allows for measurements that can be used in deployment models, which can be fine-tuned using this real-world information.

This level of system design is much more effective than ad hoc type estimates followed by costly field measurement, testing and device relocation iterations. Furthermore, a properly designed system will reduce installation time, thereby keeping costs down further.

All of this is not to say that every situation can be planned in advance, nor can any deployment model account for every variable our networks may encounter. Given the complex nature of these networks, coupled with the complex nature of service areas, it is clear that not all conditions that may present themselves can be accounted for. But with planning, we can minimize the risks and keep initial costs as well as post-deployment costs down.

For vendors planning a deployment…it is important to have the right tools at your disposal. This will allow you to keep your costs low, provide lower bids and get more deployment jobs. In addition, this will potentially save back end fees for maintenance and trips to the field.

For businesses looking to deploy an IoT network… it is vital to work with a vendor who has the capability to capture the data analytics measuring system performance. But as demonstrated here, the design of a system starts much before any device is mounted. The modeling of system behavior beforehand will help ensure the system is operating properly and there are no extraneous costs. Imagine for example a system with an uneven traffic flow that is putting too much traffic on one device, thereby draining its battery rapidly and unnecessarily costing more in maintenance fees. It is important to know the right questions when selecting a vendor for your deployments. The issues raised here serve as a good starting place to ensure the vendors you consider are using the proper tools and will provide you with a reliable, redundant, low cost network.

About the author

Bob Akins joined EDX Wireless in 2012 and has worked with utilities, smart grid vendors and consultants world-wide as they plan, deploy and optimize AMI, distribution automation, M2M and other wireless networks. In his role, Mr. Akins is active in the support of system integrators as well as in the product development of network planning solutions.

A Vision of the Customer-Centric Grid

By Bradley Williams

Electric utilities recognize the need for new distribution network technologies to accommodate sustainable growth and customers' growing interest in grid-connected, customer-owned technologies such as solar rooftops and home/building energy management systems, and smart devices such as appliances. As policies that concern these technologie – customer choice, emissions reductions, weather-related outage response – begin to unfold around the world, a fundamentally different approach to the electric distribution grid is needed.

Utilities must re-examine near-term and long-term plans for distributed energy resources (DER) technology integration and determine whether their current enterprise systems are able to support the needed changes. Moving forward, utilities will need an integrated approach to address DER planning that includes future customer demands, grid operations, asset management, and workforce enablement.

As utilities move to supplying energy and providing differentiated services based on customer needs, they need a long-term technology plan. Utilities will want to ensure that current technology investments and upgrades act as stepping stones to support the programs they want to offer and the expectations of future customers.

The most successful and forward-looking utilities will start with a strategic vision for the technology that brings together the customer, grid, asset, and workforce operations. By filling today's needs with technologies that can incrementally accommodate a variety of future scenarios, utilities can maintain an important role as the electric grid changes from one-way power delivery to a complex, multi-directional system of inputs and outputs offering customer convenience, greater reliability, and adherence to emerging international environmental goals.

Defining the Customer-Centric Grid

Typically, the term 'customer centricity' means putting the customer at the center of the focus of your business, with an understanding that creating meaningful customer value and really putting customers first engenders the most – and the longest-lasting – business value.

The evolution of the customer experience means customers now want from their utility providers the same instant access to the most up-to-date information on the platform of their choice that they receive from other service providers. Additionally, the customer has historically been a more passive consumer of the product provided by the utility, whether that is electricity, natural gas, or water. But with the immense growth of grid-connected, customer-owned distributed energy resources and technologies, in particular, this is no longer the case with electric utilities. Active customer participation is putting the customer at the center of the grid equation like never before, and a fundamentally different approach to the electricity distribution grid is needed to accommodate this change.

The Customer-Centric Grid and DER Lifecycle Management

Distributed energy resources (DER) lifecycle management is one way in which we can illustrate customer-centricity. The DER lifecycle management process starts with the customer, and ensures that he or she remains engaged throughout the entire lifecycle.

Start with customer engagement and enrollment. Utilities will identify customers with DER and qualify them into the right programs. Utilities may have specific programs with specific prices tailored for customers with DER assets. Utilities need an integrated customer information system (CIS) with a customer engagement solution, and service order management, to manage the following procedures:

1. **Integrate distribution network planning**. Utility professionals need to perform a comprehensive network planning and modeling exercise to integrate DER assets. It starts with a network model and inventory of network assets. Capacity and impact planning on existing systems with an integrated distribution management system and outage management system enables utilities to perform capacity and impact planning.
2. **Make use of the granular load forecasting and analytics**. Grid operators have to account for load models from the customer to the system level. Any reverse feedback on the feeders and circuits can have a negative impact on the distribution system. Utilities are looking for an integrated network model that combines device-level data and advanced analytics to develop a much-improved forecast.
3. **Validate customer connection points**. Asset registration and connection is an important step to ensure an ongoing record of each DER device. Utility professionals need to be able to take care of the whole process associated with asset commissioning and decommissioning.
4. **Prepare your asset operations for ongoing DER management and maintenance**. Utility professionals will need to keep tabs on the health of DER devices, and manage configurations and upgrades. An integrated mobile workforce management system with asset management can identify, fix, and restore a DER device much faster. Utilities can offer new services with integrated mobile workforce solutions that constantly track equipment as well as keep the network model up to date.
5. **Review your billing systems and settlement processes**. Customers need accurate billing based on the granular metering and device data to settle DER consumption. For instance, utilities need accurate data for settling net metering, critical peak, and time-of-use prices. Customer operations and IT require an integrated view of billing, metering, and customer engagement solutions.

The Customer-Centric Grid and Future Technology Investments

The future utility will be one that is flexible, and can offer new customer programs or support new business models as they are needed. Investments in technologies that align with a strategic vision of the future utility will provide current and future benefits, including:

Long-term business planning including transformation. Prevent dead-end investments in applications that will clearly need to be changed out in the future. Focus instead on business planning and strategic vision to include DER in the technology landscape. This can also include enabling incremental responses to growing customer demands.

Performing while undertaking digital transformation. Give staff time to drive digital transformation while gaining experience with new procedures and business processes while there is still a relatively small amount of customer-owned energy technologies, DER and demand response on the system.

Analyzing risk carefully and early on. Lower the cost and risk of pilot programs. Planners can have a fully tested real-life technology structure within which to design, offer, and evaluate the results of a wide variety of possible offerings. They can gain experience not only with the technology itself, but with the business process changes that will inevitably accompany the widespread adoption of DER. As the most successful pilots transition smoothly into permanent programs, there is no loss of momentum while staff members struggle to scale up technologies that work well only when the number of participants is small.

A Customer-Centric Focus for the Future

While DER lifecycle management is but one way to illustrate the customer-centric approach to the future grid, it illustrates in detail the customer engagement in every step. Ultimately, if the utility has successful incorporated all the lifecycle steps discussed in the example above, it will be able to circle back to its customers with new information, new programs, and new models for continuing engagement. It becomes a win-win, both for the DER customer and for the utility.

While DER and other customer-initiated technologies may seem more like new challenges to be overcome, they offer excellent opportunities to bring the needs of your customers back to the center of your business. A customer-centric business focus stimulates increased business value now and long into the future.

About the author

Bradley Williams is vice president of industry strategy, Oracle Utilities. Williams is responsible for Oracle's smart grid strategy as well as utility solutions for outage management, advanced distribution management, mobile workforce management, work and asset management, and OT analytics. Williams has spent the past 30 years driving innovation in the utility industry in roles including T&D power system engineering, technology development, asset management and industry analyst.

The Internet of Things: Will Utilities Lead, Follow or Get Out of the Way?

By Ryan Gerbrandt

Throughout the smart grid era, utilities have evolved their approach to communications, achieving in AMI networks some of the first scalable and business case driven IoT deployments. Is the industry ready to lead in the increasingly interconnected IoT era?

The internet of things, more commonly known as IoT, is a concept whose definition is emerging. Futurist Jacob Morgan, in a 2014 Forbes piece, described it as "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other.)" IEEE, which invites input on the subject, currently defines IoT as "a network of items -- each embedded with sensor -- which are connected to the Internet." Fundamentally, IoT is the communication between two devices – not just the transfer of data, but data that is understood at some level by some form of intelligence among the devices.

ATMs, developed in 1974, were among the first smart devices included in IoT. It did not take long for this new "talkable" technology to take hold in our culture. By 2015, there were 2.6 billion smart phones worldwide, according to a November 2016 Ericsson Mobility Report, which predicts 6.1 billion devices by 2022. The number and type of devices poised to be IoT participants is constantly expanding: TVs, coffee makers, washing machines, thermostats, headphones, lamps, cars, bridges, buildings, roads, wearable devices and much more.

IoT in the Utility Industry

AMI was one of the earliest examples of IoT in utilities. Today, it is among the most widespread examples. As of 2015, U.S. electric utilities had roughly 64.7 million smart metering infrastructure installations according to the U.S. Energy Information Administration. With nearly 88 percent of these installations being for residential customers, utilities' use of AMI continues to transform many of their key business processes, especially those related to the way they engage with end customers. Today utilities are poised for even greater IoT growth as digital control infrastructures and new low-cost digital sensors permeate networks – and may introduce additional connectivity from beyond the utility enterprise.

As the rollout of AMI revealed, utilities face the challenge of not only capturing and storing large new data streams, but also figuring out how to identify actionable business intelligence from this data. The rise of AMI and other smart grid applications saw utilities building out various purpose-built networks, leaving many struggling to make sense of it all amidst a "data tsunami" often worsened by siloed devices that couldn't readily share or understand each other's information.

Terabytes Ahead

The AMI data challenge is only a small taste of things to come. In the area of vehicles alone, Gartner, Inc. predicts that by 2020, there will be a quarter billion connected vehicles on the road, enabling new in-vehicle services and automated driving capabilities. As distributed generation, energy storage, and other grid edge resources including EVs proliferate, the growth in data and the need for tools to make sense of it is growing exponentially. How will all this equipment communicate securely and meaningfully -- and over what communications networks?

Utilities learned important lessons including how to deliver mission critical communications across different terrains and how to balance access, privacy and security. These utility challenges helped shape the communications platforms we have now. The utility industry has come to appreciate the complexity and importance of integrated communications.

The future of IoT communications will not be shaped by one particular communication platform or technology. No device-specific or single technology approach fits the variety and complexity of the smart grid era or the coming era of IoT. Communications – by its very definition – is the foundational, unifying approach. It must not only deliver access to data but provide a format for it to be understood, for intelligence to be applied to it at multiple points in the devices and perhaps in its very architecture. In practical terms, communications will need to sit on a unifying platform that can seat a variety of forms of information from many technologies across an enterprise. It must match the best communication technology to specific business case requirements and be scalable to new and smarter tools.

Analyze This

As the maturing smart grid era evolves toward IoT, a variety of brands and types of meters and other devices will need to be able to talk and listen to one another and where networks need to be secure yet accessible. Today, for many utilities, communications between smart devices faces ongoing challenges.

As of 2015 there were 4.9 billion devices within the internet of things and that number is expected to reach or even exceed 50 billion by 2020. The sheer projected growth in endpoints alone makes having a unifying platform increasingly important for effective IoT communications. Utilities ultimately need devices that can communicate within each area of a network, both to each other and to a central host. And as communications networks connect globally, compliance with global standards and protocols will matter more than ever, as will the need for systems based on open standards.

Analytics take communications to the next level, applying advanced intelligence to extract value from data that communications has delivered. Will the rise of analytics follow the model set by smart grid – a gradual recognition of the need to move away from device-specific, embedded approaches and toward unifying, "take all comers" approaches? It remains to be seen. Just as AMI and smart grid began with device-specific, purpose-built platforms, the evolution of analytics shows similarities. Utilities are monitoring and analyzing distributed assets like solar PV using a variety of approaches. Smart lighting is seeing increased adoption, in many cases using proprietary and use-specific tools to monitor and manage them.

Ready to Lead?

Utilities learned critical lessons during the lead up to today's IoT era that are relevant and applicable to almost all other industries facing communications challenges. The progress that utilities have made in AMI network communications has helped build the groundwork for future platforms that will support a modern grid with increasingly distributed and renewable supply sources, from solar panels to wind farms.

Utilities have the opportunity to take leadership positions in the IoT era. From integrated home energy management to microgrids that will interconnect and isolate in real time, IoT will bring an era in which utilities will find themselves overseeing communications that reach across their enterprises and into the homes and workplaces of their customers, interacting along the way with intelligence from transportation and municipal and private services of many kinds. The communications platform will play an increasingly pivotal role in enabling utilities to operate and control all their smart grid and IoT devices, ideally on a unified management platform. With IoT, millions of endpoints are coming, each delivering potentially vast quantities of data from multiple vendors, types, models, firmware versions, protocols, and communications technologies. With a unified approach to utility communications, built on the lessons utilities have already learned – about security, about privacy, about access across siloes, about engagement with consumers – utilities can be equipped to not only survive but lead in the Internet of Things era.

About the author

Ryan Gerbrandt is a career electric utility industry professional. After specializing in utility communications systems, network operations, SCADA, HVDC controls and system protection for Manitoba Hydro, he joined Trilliant in 2007. He pioneered the processes and best practices being implemented in Trilliant smart grid deployments and today, as senior vice president for global solutions.

THE BIGGER PICTURE

BY DR. TIM SHAW

It Must be Working - the LEDs are Blinking!

In my line of work I get the occasional opportunity to come in and examine the results of plant cyber security implementation programs within various organizations. And one general impression I have come away with is that the quality and effectiveness of those programs is invariably directly proportional to the skill-set and expertise of the team responsible for planning and implementation.

I suppose the response from some of you, to my beginning statement, would be a resounding “well duh!”. I guess it should be obvious that a more experienced and talented team would produce better results. And yet surprisingly often I have witnessed plant cyber security programs that have been staffed in a hap-hazard manner, seemingly by whomever didn’t run away screaming when the topic was raised. All too often the team officially consists, at least on paper, of a large number of personnel and consultants with wide-ranging expertise. But the reality is that most of those people never actually participate or have little time to get involved. And so the actual planning and implementation often falls to a handful of plant engineering staff who may have limited access to corporate IT people if they have questions (and know how ask nicely.) As could be predicted, the net result of this is usually a cyber security program that takes much longer to complete than expected, ends up squandering funds and manpower on stuff that provides no cyber security benefit and leaves the plant’s automation systems still vulnerable to cyber compromise. And even worse, the plant and project team usually think they are properly protected.

In prior articles I have discussed the differences between IT cyber security and industrial automation cyber security and the fact that IT ‘best practices’ do not always translate well (or can downright dangerous) in an industrial automation environment. So it is usually not a good idea to let IT be in charge of planning and executing a plant cyber security program. And yet the IT department may have the only available expertise for things essential for a cyber security program such as Ethernet switches and routers and firewalls. Plant engineering and automation personnel have had to become familiar with some things that used to be the exclusive province of IT such as Ethernet networks, because most I&C gear today comes with an Ethernet port. But there is a difference between being ‘familiar with’ and being an expert or even just being reasonably knowledgeable. I have worked with plant engineers and instrument techs whose understanding of Ethernet switches was limited to: ‘if the little lights are blinking then it must be working’. They had no idea of the various settings that could impact the way the switch worked (including stopping it from working) such as QoS (quality of service) or VLAN parameters. They didn’t know that someone could get into the switch via telnet and mess things up from elsewhere on the network, of which the switch was a part. They didn’t know that you could prevent that from happening by setting a password on the switch.

But lack of sufficient expertise and domain knowledge can be a problem for the IT folks as well. In one such instance, as their major task in a plant cyber security program, the corporate IT group was assigned the responsibility for implementing a network intrusion detection system (NIDS) to monitor message traffic entering and exiting the plant and passing between the various systems and LAN segments within the plant. Such systems look at all messages in real-time and analyze them both individually, and as part of a series of message exchanges, in order to detect malicious message traffic. To do this, depending on the underlying technology being used, often requires the development of ‘rules’ and ‘signatures’ that guide the analysis process. Those rules and signatures are protocol specific and the IT world has extensive experience in building up rules for commonly used protocols like http (web browsing) and ftp (file transfer) and smtp (email). The problem of course is that industrial automation systems and devices make use of a lot of uncommon protocols (at least uncommon in IT circles) such as EtherNET/IP and ProfiNET and Modbus/TCP.

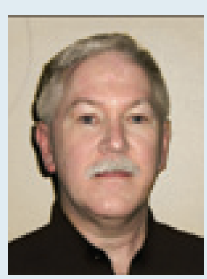
And so in this instance the NIDS was configured with rules and signatures for all the protocols familiar to the IT folks, but in effect it was nearly blind to message traffic to and from and among the automation systems. If you want to send a malicious command to an automation system or maliciously manipulate parameters in such a system or device, you are going to speak to the system or device in a protocol it understands – probably one of those industrial protocols I was just mentioning. So watching for and analyzing that kind of message traffic is rather essential for cyber security in a plant environment. But hey, the LEDs were all blinking, so it must have been working, right?

Sometimes the best of intentions, coupled with lack of sufficient knowledge and inadequate training, can produce results that seem to be successful, at least on the surface, but are actually a failure. In another instance a plant engineer had been advised that a firewall needed to be installed at a certain point in the plant network to comply with some regulatory requirements. The IT department shipped him the firewall and the engineer installed it as directed. To the relief of the engineer, shortly after the firewall was powered-up all of the systems and equipment on both sides of the firewall seemed to return to their normal operation. (And yes, the LEDs were all blinking on the firewall's front panel.) To the plant engineer this was the definition of success and it was only during a cyber security audit the following year that it was discovered that the only rules in the firewall were the factory defaults of 'allow everything going in' and 'allow everything going out'. (For those not conversant with firewalls 'rules' are conditions to check in a message in order to decide to let a message pass through or to block it from passing through the firewall.) So rather than actually functioning as a firewall the device was merely an expensive space-heater with blinking LEDs. The engineer thought that the IT folks had the firewall all setup and configured and the IT folks thought the plant personnel knew about setting up firewalls. A friend of mine used to call that 'mutual mystification' and I believe that term describes it nicely. In that case even if the IT department had tried to pre-configure the firewall prior to shipping it to the plant it probably would only have been configured with rules associated with the commonly used IT protocols and not with any for the industrial protocols used at the plant. And even if the plant engineer had realized the need to put rules into the firewall and was well aware of the industrial protocols being used, he did not have the training and skills to develop the necessary rules and configure them into the firewall.

Lack of experience and appropriate expertise can also lead to situations which start as a success but end up as a failure. In another instance a plant had worked with corporate IT to design and build a portable media anti-virus (AV) scanning station and had put in place work procedures that required all portable media (but especially USB 'thumb drives') to be AV scanned prior to being used in any plant automation system. Most AV software makes use of unique code/data fragments extracted from captured malware (and generally called 'signatures') to identify the presence of such malware on the portable media. The problem is that new and constantly changing malware requires such signatures to be regularly updated in order for the AV scanning function to be effective. When corporate IT setup the scanning station they ensured that the latest and greatest AV signatures were loaded. But they also assumed that the plant personnel would be responsible for keeping the AV signature library updated. It turned out that the one plant engineer who was instructed in how to perform updates left the company a few months later and no one else took over the task because the engineer in question had never trained his replacement or formally documented the procedure. A subsequent cyber security audit discovered that the AV signatures were over a year out of date, which means that for over a year the effectiveness of the AV scanning had been dropping and dropping. But, when media was inserted into the scanning station the LEDs still started blinking, so it was presumed to be working.

So why bring up all these examples? In every one of these cases the people involved were trying to do the right thing and even thought they had done a good job, But, because of a lack of communication and coordination among the various groups supporting the cyber security implementation program, and a lack of applicable technical expertise, the actual results were less than stellar. In each case sited the result was a lack of any cyber security benefit from the labor and monies expended and a false sense of being cyber secure. And it really didn't have to happen that way. If appropriate personnel resources had been allocated and if necessary expertise had been made available at the right points in the program, even if that required going outside the organization – possibly to a knowledgeable vendor, then all of these examples of failure could have been examples of success. Staffing a team tasked with establishing a plant cyber security program requires management commitment and a recognition of both the diverse skill-sets needed and the amount of time each individual assigned to the team must be prepared to devote to the effort. It is important to consider where your organization may have technical weaknesses in critical areas, and to be prepared to seek-out external resources to shore up those weaknesses. As I said back at the beginning, this stuff is pretty obvious. It may fall into the category of project management 101. And yet time and time again organizations look for false shortcuts and cost savings that will end up costing them more in the long run. I have many more such tales I could relate to you, but the LED on my laptop has stopped blinking and so that will have to be the subject matter for a future column.

ABOUT THE AUTHOR



(William) Tim Shaw (PhD, CISSP, CIEH, CPT) has been active in industrial automation for more than 35 years and is the author of Computer Control of BATCH Processes and CYBERSECURITY for SCADA Systems and co-author of Industrial Data Communications. Tim has contributed to several other books, and is a prolific writer of papers and articles on a range of technical topics. Tim has been directly involved in the development of several DCS and SCADA system products and regularly teaches courses for the ISA and the University of Kansas on a range of topics from cyber security to process automation. Inquiries or comments about this column may be directed to Tim at timshaw4@verizon.net.

SECURITY SESSIONS

By Justin Lowe and Sean Duffy

Is Your C-Suite Prepared for the Cyber Future?

With cyber threats to the electric utility landscape increasing, what is the role of the utility C-suite in ensuring preparedness and what steps can be taken to enhance effectiveness? The reality is, effective coordination is often hampered in many utility C-suites by the inherent tensions that exist between those who take an alarmist position regarding cyber security and those who are more complacent. This discord is creating a need for a more holistic-focused approach to better understand and manage risks.

Cyber security is often times handled by small, disparate security groups that only work on a targeted subset of critical assets, leaving a larger set of unregulated components and assets across an organization exposed. In addition, C-Suite executives are often unaware of the role state-elected officials play in their own future cyber protection plans and the need for state regulators to gain assurances that public utility companies are taking necessary steps concerning cyber security.

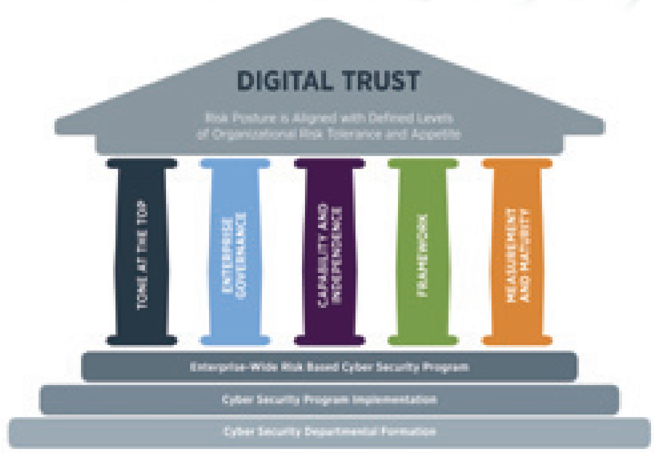
Therefore, it is critical for C-suites to recognize the need for a holistic enterprise oversight program due to the changing nature of the cyber security landscape under their domain. They must ensure appropriate defenses are in place, as well as an effective governance framework and performance metrics are being utilized appropriately.

Key Steps in a Holistic Approach

Many organizations spend too much time focused on compliance, only implementing a handful of requirements, which can sometimes leave gaping holes in their perimeter. C-suite leaders will benefit from going beyond run of the mill health checks and gap assessments, and looking beyond just IT and operations to enhance their organization's security posture.

The first key element to a holistic approach that leaders should be establishing is a baseline cyber security framework. Once the framework is in place, it must be accepted by the organization. Next, a more in-depth evaluation is needed to assess business systems, customer data, IT systems, operational technology (OT) systems including SCADA, physical security and all places where privacy-related information is stored.

Don't make the mistake of letting these risk assessments sit on a shelf and collect dust once conducted. This happens when assessments are not able to be implemented because they are performed by the wrong people, so it is vital to ensure that those doing the assessments have functional experience. The most important thing for leadership to remember is to make sure the implementation strategy fits their organization, otherwise nothing will change.



The Five Pillars

In order to properly build a risk-based cyber security program, utility leaders should use these five pillars to measure and evaluate the strength and maturity of their organization's cyber security:

Tone At The Top –
Conversations and Communications

This first pillar focuses on the need for the C-suite to assess the organization's readiness for change, the appetite for risk and the approach to Organizational Change Management (OCM). All of these factors should be considered carefully, with management being prepared to take on responsibility for proper cyber security and the establishment or enhancement of a cyber security framework.

At the heart of this work is the need for an executive team to be committed to the change, and communication of that commitment across all business units and employees in the organization. If leadership commitment is misunderstood by the organization, it could hinder success. The organization must assess how much and where they are willing to absorb risk, and the resource pool (people and funding) that can be committed to mitigate it. The C-suite must take active interest in the messaging to ensure consistency and commitment. This is the foundation of OCM and necessary to implement new standards of operation.

Enterprise Governance –
Organization And Defined Outcomes

The executive team needs to provide effective governance to the cyber security effort in order to maintain organizational commitment and alignment within the overall strategy. Proper accountability and monitoring should be in place to check if defined goals and outcomes are achieved. The authority to perform identified functions has to be clearly in place, documented and communicated.

Education of the executive team, board and other senior and mid-level management should also be in place to ensure proper engagement and accountability to perform and guide their organizational efforts to complete cyber security tasks. Additionally, roles must be clearly defined and operating protocols in place to provide clarity to the cyber security framework. Finally, results-focused cyber security reporting should be put in place in which the frequency and structure of the reports are reviewed and agreed upon by all parties – and these reporting standards should be updated as the framework matures.

Capability And Independence –
Authority, Personnel and Tools

Another key role for the executive team is the selection and training of cyber security personnel. They need to have the right tools, executive support and have organizational independence in terms of reporting structure – similar to auditing teams. They should have ownership and leadership of the cyber security function with C-suite backing that allows them to have enterprise authority to issue standards, incident handling leadership, and access to manage and mitigate risks with the premise that this is an expected and non-optional part of doing business. The executive team should also create and formally approve a charter for the authority of the cyber security function.

Policy Process And Procedure Framework –
Structural Framework and Program Operations

An essential part of cyber security is having multi-year implementation plans in place. The executive team should oversee and formally approve policy. Also, continued review and program updates should be scheduled to ensure that proper implementation of policy remains timely and effective. Executives need to make sure that the framework standards and policies are clear and complied with enterprise-wide.

External operational assessments of risk coverage, risk remediation and cyber security operations will help to ensure that practices are effective and in-line with organizational expectations. Security control implementation and selection, reference architecture and system security plans should all be reviewed on a regular basis to ensure relevancy and effective use.

Measurement And Maturity – *Program Monitoring, Assessment and Reporting*

The executive team should assess whether it has the information and data to confirm the focus of the organization's cyber security program is in line with expectations and ensure the appropriate level of due diligence to gather the data is evident. It is important for the C-suite and cyber security leadership to agree on metrics, frequency of operations results and program reporting reviews.

Constant vigilance and continuous improvement is needed for a program to be successful. If the proper metrics and review mechanisms are in place, the organization will have an objective assessment and real understanding of the state of their cyber security program and clarity of where improvements are truly needed.

Ultimately, the five pillar approach prioritizes risk that support the protection of the entire enterprise, not just to achieve compliance with a specific mandate such as NERC CIP. This approach consolidates cyber security efforts across the organization with a lower total cost, helping to eliminate costly redundancies that occurs when multiple parts of the utility build ad hoc cyber security mechanisms.

Having the C-suite back the implementation of an organizational cyber security framework, like the five pillars, increases the likelihood of success in implementing a holistic security program. When the entire organization, from executive ranks to the front line, are fully engaged with a security first mindset, a utility is well on its way.

ABOUT THE AUTHOR

Justin Lowe is a cyber security expert at PA Consulting Group. Justin has more than 15 years of experience in cyber security and OT security, and the challenges of addressing security issues across the energy sector. Justin also led the development of Security Best Practices for SCADA and control systems for the UK Government's Centre for Protection of National Infrastructure. And most recently, Justin led the development and implementation of a cyber security program for a newbuild nuclear power plant and the implementation of a cyber security program for a major utility.

Sean Duffy is a cyber security expert at PA Consulting Group. Sean's experience includes: managing risk and security components of large engagements including governance (NERC & NIST), strategic visioning, and solution design and implementation; supporting clients in managing change in their organizations by developing goals, strategies, and an implementation plan to address changes needed to leverage new solution; managing legal and compliance requirements for complex information and operational technology engagements; and, leading cyber incident response planning, education & training and recovery efforts for clients.

Their findings are based on a new report from PA Consulting Group titled, "Is Your C-Suite Prepared For the Cyber Future?"

Guest Editorial 1

Orange Button℠ is Making Solar (even more) Affordable

By Aaron Smallwood

In 2016, the U.S. passed 1 million solar installations, and that number is estimated to pass 2 million by the end of this year. Exponential growth is everywhere in the solar industry, which now powers 1 percent of the country's energy – a ten-fold increase from five years ago. [1]

Since 2010, the compound annual growth rate of solar installations is 58 percent, driven largely by falling prices (70 percent decrease since 2006) and rising demand. Despite falling prices and increasing demand, soft costs remain a stubborn speed bump for residential installations – making up 63 percent of total installation cost. [2]

Orange Button℠ Program Year One

Part of the U.S. Department of Energy-funded *https://energy.gov/eere/sunshot/sunshot-initiative* SunShot Initiative, Orange Button℠ is driving the creation and adoption of industry-led open data standards for rapid and seamless information exchange across the solar value chain, from origination to decommissioning. Standardizing data will reduce soft costs by making it easier to share solar data and speeding up processes.

SGIP, the SunSpec Alliance, kWh Analytics and the National Renewable Energy Laboratory (NREL) are leading the Orange Button℠ program. Orange Button℠ kicked off in early 2016 by recruiting participants to create a scoping study, develop industry-driven use cases, and define market requirements used to inform the (under development) solar data taxonomy. The DOE was pleased with the progress after one year—giving it a "green" status in a recent report.

The Orange Button℠ program is focused on all areas of the solar project value chain, including finance, operations and management, deployment, real estate and grid integration. With input from the Orange Button℠ Requirements Working Groups representing each of these areas, the program created market requirements that defined what data should be included in the solar data standard. The goal is not to build from scratch but to use existing standards where appropriate.

Orange Button℠ Program Year Two

Year Two is another busy year for the program. SGIP is facilitating a handoff of the Orange Button℠ requirements to the industry teams led by the SunSpec Alliance who are building the solar data taxonomy, as well as coordinating solar industry awareness and education. In addition to building the solar data taxonomy, the SunSpec Alliance teams are developing Application Programmatic Interfaces (APIs) and an Orange Button℠ conformance test framework.

In Year Two, kWh Analytics an industry leader in risk management software, continues the development of a cloud based solution that will translate disparate file formats into the new Orange Button℠ data format. The purpose of this solution is to lower barriers to adoption and to accelerate use of the Orange Button℠ taxonomy. The National Renewable Energy Laboratory (NREL) is leading the development of the Solar Data Exchange Platform, a comprehensive catalog for solar data that connects standardized data access to the solar industry to advance the solar marketplace.

Benefits of Orange Button℠

If the management of solar data is streamlined, it can boost the bankability of solar projects, thereby attracting investment. But for that to happen, developers, asset operators, utilities, financiers, solar companies, entrepreneurs and more must work together to define a solar data taxonomy that meets the needs of the participants in the solar project lifecycle.

When adopted, Orange Button℠ will enable asset operators to report performance data to owners and investors without having to customize it for each owner's needs – driving lower costs. Asset owners could receive standardized performance data from all of their investments, eliminating the need for to manually compile multiple formats into a single performance view for portfolio management. Solar developers will be able to utilize a single taxonomy to perform handoff to asset operators, keeping them from wasting time to meet each operator's individual data needs.

There are many ways that standardized data can benefit solar. Another example is if software vendors incorporate the standardized taxonomy into their financial management products, Orange Button℠ can enable exchange of data between systems that currently require manual manipulation to complete.

All of this leads to increased bankability of solar projects, more efficient solar data transactions, and further acceleration of (even more) solar.

In 2017 and 2018, the solar industry will have opportunities to become more familiar with Orange Button℠ and the benefits it can bring. Orange Button℠ program partners will host informational webinars, publish industry updates, review and comment on the taxonomy, and interested solar industry stakeholders can become an Orange Button℠ tester or early adopter.

For more information about Orange Button℠ and how you can get involved go to *http://www.sgip.org/orange-button/*

References

1 Source: SEIA/GTM Research *U.S. Solar Market Insight Q4 2015*
greentechmedia.com/research/ussmi
Lawrence Berkeley National Laboratory, *Tracking the Sun*

2 Source: SEIA/GTM Research *U.S. Solar Market Insight Q4 2015*
greentechmedia.com/research/ussmi
Lawrence Berkeley National Laboratory, *Tracking the Sun*

ABOUT THE AUTHOR

Aaron Smallwood is VP, Technology at SGIP. He is responsible for leading SGIP's Program Management Office and working with member committees and groups in advancing SGIP's technology strategy and agenda.

Aaron has been in Information Technology for 20 years and in the utility industry for the last 15 years. As Director of IT Operations at the Electric Reliability of Council of Texas (ERCOT), Aaron was responsible for the multi-data center IT operations of ERCOT's real-time grid and market systems, deregulated retail market systems, Enterprise Data Warehouse, systems integration, and market settlement systems. In other roles at ERCOT he led business/technology alignment, IT strategy development, program financial management for the Texas Nodal Market Implementation, IT stakeholder relationship management, and the IT divisional project office.

Prior to ERCOT, Aaron was responsible for managing the relationship between IT and utility business units at Aquila, Inc., working with utility and IT leaders to ensure that IT services were aligned with business objectives and that IT was positioned to support their needs.

http://www.sgip.org/orange-button/
Orange Button at sgip.org

http://sunspec.org/sunspec-osdx/
SunSpec Open Solar Data Exchange

http://www.orangebuttondata.org/
Orange Button Data Orange Button Data

Teaming to Mitigate Risk – The Utility Executive and Board Imperative

Guest Editorial 2

By Donald Racey and Ellen Smith

Recent examples of lower probability, high-consequence events affecting the electric utility industry are reshaping the way utility executives and board members must look at risk and the associated costs of mitigating risk. Events such as the 2011 nuclear disaster at the TEPCO Fukushima Daiichi facility in Japan, the 2013 sniper attack on the PG&E Metcalf, Calif., substation and the 2015 cyber-attack on the Ukrainian electric grid, are just a few incidents that reflect non-traditional events which compound the already complex task of mitigating the risk of damage to critical electric assets from traditional sources such as severe weather, seismic events and fire, to name a few.

As a result, these new and emerging risks from unconventional sources are introducing a paradigm shift in the way utility executives address risks, old and new. Industry teaming is one new approach electric utility executives are considering.

It is critical to first form the proper level of understanding and urgency among the utility company board and C-suite executives to generate the increased focus and support that the business needs to address these new risks. Replacing damaged assets that have very long lead times, high capital cost and are critical for providing reliable service to customers must be understood as a top priority. Advances in technology require better education at all organizational levels and across organizational silos with regard to physical and cybersecurity threats, particularly as Internet of Things ("IoT") technology and interconnected devices become more integrated, accessible and understood as imaginable threats and no longer "Black Swan" events. Business leaders need to have specific knowledge and should ensure regular business updates with respect to "critical" assets and systems – those for which a failure could create significant customer outages and/or high expenses. Specifically, the company definition of "critical" needs to go well beyond the narrow definition that NERC CIP utilizes and which may not reflect actual assets that have high consequential risk.

Electric utilities are not the only industry segment that is taking notice. Insurance underwriters of electric utilities, for example, have taken action by reexamining their approach to policy design, pricing and risk-tolerance strategies. Underwriters are evolving in how they assess risk and quantify damage from the potential loss of long lead time critical assets such as high voltage power transformers that can cost well over a million dollars and can take up to two years or more to manufacture and transport.

Insurers are also considering the changes required to long-term business interruption coverage triggered by such events. Cyber-specific insurance is a rapidly growing offering and is becoming an increasingly important part of business risk management, alongside the utility's property & casualty and business interruption policies. "The greatest concern for insurers, however, is that the risk itself is not constrained by the conventional boundaries of geography, jurisdiction or physical laws." (Lloyd's Emerging Risk Report – 2015). Still being determined is how each type of insurance policy interacts and responds to a cyber vector attack that damages or destroys physical property and leads to significant operational downtime and financial impact.

Meredith Schnur, Senior Vice President of the Professional Risk Practice at Wells Fargo Insurance, describes the challenge of "understanding the totality of a company's insurance program, as more than one insurance policy could be triggered as a result of a cybersecurity incident." Relative to physical damage to utilities' operating technology and assets, Ms. Schnur adds, "Most cyber liability policies exclude liability arising out of any injury relating to bodily injury or property damage; cyber is a pure financial loss risk transfer product. One would assume the property policy would cover property damage arising out of a cybersecurity incident, when in fact, there are only a few property insurers who address this exposure under their existing policies. First-party business interruption loss arising out of a cybersecurity incident is evolving as we speak, but today, in the U.S., the coverage is not as robust as it needs to be to protect power and utility types of risks."

Every electric utility is responsible for bearing the entire risk of loss and the cost of replacing an asset, should that be required. Historically the electric utility industry leaned toward asset optimization versus industry standardization, creating a diverse and often utility-specific set of equipment designs. As there were no driving industry utility company-specific efforts for standardization, the current installed base of high voltage electrical equipment across the United States does not readily lend itself to a common stocking one-size-fits-all approach. This industry dynamic has presented an expensive and difficult 'sparing' model for critical assets. Due to this, many utilities have some critical operating assets that do not have spare replacements available in storage, and often any spares held are not maintained or secure. The current, replace-or-fix-upon-failure strategy and independent business self-supply models remain risky and present a threat to the U.S. electrical grid system's overall reliability and emergency recovery time.

Most of the bulk electric power grid was built around traditional, coal and nuclear base load power generation plants. Many of these older plants face the risk of retirement with renewable (wind, solar) and natural gas fuel plants replacing them. This adds new technical risks to assets remaining on the system and makes customers more vulnerable to grid instability and potentially long interruptions from a catastrophic event. According to the Energy Information Administration ("EIA"), 94 coal-fired power plants closed in 2015, with the capacity of nearly 14,000 megawatts. Another 41 coal plants are scheduled to close in 2016, with a combined capacity of more than 5,000 megawatts. Additionally, since October 2012, U.S. nuclear plant owners have closed or announced closure of 14 reactor units at 11 plant sites. All indications suggest that given the age of the U.S. coal fleet, nuclear plant closures, the transition to natural gas, and the growth of renewables and distributed generation, the U.S. electric grid will undergo enormous changes in the decade ahead. This will require electric utilities and transmission owning entities to evaluate their current asset management and critical spare strategies and make adjustments in their approaches.

Since many critical assets have been in service for many years, warranty protections are no longer in place, adding to the potential risks and costs if a significant event damage any of these. It is unreasonable to assume or expect that individual electric utilities will be prepared by maintaining a complete, duplicate inventory of very expensive critical spares. Industry teaming may be an approach to alleviate these concerns.

General Electric's ("GE") Aeroderivative Lease Pool program in the power generation space is an example of an industry teaming model. Participants pay an annual membership fee that offers an alternative to investing in expensive capital spare components while providing a guarantee on asset availability should an unplanned need arise. This program provides the dual benefit of standardizing critical asset types across the industry and reducing costs associated with expensive one-off replacements.

Another approach to risk mitigation and asset management strategy for electric utilities is the formation of Grid Assurance, LLC. Grid Assurance was developed through a collaborative effort of several utilities and was formed with the purpose of providing member companies a cost-effective way to improve the resilience of their bulk electric system assets as a whole, by offering access to an inventory of critical, long lead time equipment stored in secure warehouses and readily deployable to respond to a major system failure. The companies currently involved are American Electric Power, Berkshire Hathaway Energy, Duke Energy, Edison International, Eversource Energy and Great Plains Energy.

The chief executive officer of Grid Assurance, Mike Deggendorf, said, "Grid Assurance was formed to provide an industry-led solution to the emerging risks to resiliency. These are emerging and catastrophic events that need a new risk mitigation capability. Grid Assurance is focused on increasing the capacity and capability to quickly recover from these events with the substantial cost savings that comes from pooling of resources."

By partnering with the Grid Assurance organization, utilities become part of a team working together to plan and develop a strategic asset reserve base. Additional services could emerge, such as pre-engineering, raw material stocking and options for prioritized allocation of emergency manufacturing slots with key suppliers. Additionally, Grid Assurance will perform ongoing logistics planning and will maintain expertise in large asset transportation, including intermodal transportation for inbound and outbound inventory. Where appropriate, it will also arrange for subscriber access to specialized transportation equipment (e.g., Goldhoffers, Schnabel cars, deck barges, dedicated boats, low boys, and cranes). Grid Assurance will manage its inventory so that manufacturer warranties are preserved.

Utilities have often been viewed as slow to adapt to change, yet today's risks require boards and C-suite executives to challenge the status quo and adapt to these rapidly changing and adverse scenarios. Lisa Barton, Executive Vice President for AEP Transmission states, "There are clearly new, emerging risks for which the industry needs to prepare. Balancing the increased capacity for grid recovery, with the cost to customer and risk to the shareholders, is the challenge. Our customers, regulators and shareholders expect us to prepare for these risks, and Grid Assurance effectively balances all of these issues."

Forward-looking utility executives will recognize the need to balance the complexities of leading and surviving in the current, more challenging and risk-laden world. Industry teaming should be considered a key component of a utility's risk mitigation strategy. Participation in such groups should also be welcomed by utilities' insurers as a risk mitigation factor and should be integrated into policy renewal efforts.

With each passing day, the U.S. electric utility client base becomes more reliant on a dependable, resilient and efficient electric power grid. The ability for electric utilities to immediately respond and restore critical electric power service is essential and will require innovative approaches and collaborative efforts across the industry to ensure maximum success.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

ABOUT THE AUTHORS

Ellen S. Smith, P.E. is a Senior Managing Director at FTI Consulting, based in Boston. She works within the Economic Consulting segment, specializing in business advisory and litigation support services. Ms. Smith's areas of expertise include matters involved in power reliability related damages, utility regulatory strategy, emergency response and strategic communications. She is currently providing advisory services with respect to all aspects of utility operations for a client who is going through restructuring. Prior to joining FTI Consulting, Ms. Smith was the Chief Operations Officer and Executive Vice President at National Grid, in Waltham, Massachusetts.

Donald Racey is a Managing Director in FTI Consulting's Economic Consulting segment and is based in Pittsburgh. He is part of the Energy, Power and Products industry practice. He has more than 20 years of experience leading large-scale operational transformation engagements. He specializes in the design, development and implementation of Operational Excellence, Process Improvement and Merger & Acquisition Integration programs.

ADVERTISERS INDEX