IoT NOW

ANALYST REPORT

SMART ENERGY

Will IoT technologies complement smart grid investments?

Analyst Report

Prepared by Beecham Research

Yiru Zhong,
principal analyst,
Beecham Research

IoT technologies support power and utilities sector transformation

The concept of a smart grid in the power and utilities sector took shape at around the same time as the Machine-to-Machine (M2M) sector began its own transformation journey towards Internet of Things (IoT). The official characteristics of a smart grid were defined in the United States at the end of 2006 while the European Union set up a smart grid task force in 2009 to drive the necessary research and development efforts. According to the US Department of Energy, a total of US$7.9 billion of private and government funding were invested in 99 smart grid projects with 228 utilities over a six-year period of 2010 and 2015. The European Commission Directorate-General Joint Research Centre on the other hand committed €5 billion between 2002 and 2016 in 950 smart grid projects

At around the same period, the M2M sector was growing out of a cottage industry between 2005 and 2007 to one where M2M modules manufacturers began to acquire assets to establish technology and market share leadership between 2008 and 2010. The M2M sector was optimistic that the power and utilities sector, particularly the distribution network operators, will drive connection volume and revenue significantly between 2010 and 2020 because millions of electricity smart meters have to be deployed globally within the decade. Reality was far from expectations; the sense of urgency within the M2M sector was not matched by the power and utilities companies.

The M2M sector's expectation that EU regulations will obliged EU member states to deploy smart meters did not materialise in the same scale and timelines. Instead, the power and utilities sector embraced IoT technologies at their own business priorities. Their sense of urgency in relying on IoT technologies became more acute as they face adapt or die scenarios from five key disruptive influences. These 5 factors create new market entrants, which makes a traditional monopolies or oligopolies incapable of responding to competition. IoT technologies enable power and utilities companies to address these five factors in a do-or-die scenario.

De-carbonisation: Decarbonisation describes the act of reducing the carbon footprint in existing energy sources. Power generating companies are primarily the electricity actors to implement this by increasing the use of renewable energy sources. In the European Union, member states agree to a 20-20-20 climate and energy package of achieving 20% reduction in greenhouse gas emissions from 1990 levels, to generate 20% of energy from renewables, and 20% improvement in energy efficiency by the year 2020. The European Commission reported that EU member states are on track to achieve this target by 2020 as the latest figures revealed that EU as a group were estimated to have 16.4% of renewables in their final energy consumption in 2015.

This is a disruptive factor to power companies because capital expenditure is required to reduce reliance on traditional energy sources such as nuclear and coal to integrating renewables such as solar, hydro, and wind power. These greenfield investments require significant financial outlay that power companies need to fund even as they receive government funding. The European Commission estimates that €379 billion is needed annually to support its 20-20-20 climate and energy targets. The intermittent nature of renewable energy sources requires additional investment by transmission systems and distribution network operators too. Both research and development and field tests are required to consider how the electricity grid will integrate ▶

renewables into the grid for a stable, balanced and resilient system. Further downstream at the consumer level, renewables, especially residential renewables such as solar panels and energy storage, will increase the interactivity between consumer and grid. Transmission and distribution grids are not traditionally used to two-way electricity flows with the residential consumer.

Decentralisation: Through the 20-20-20 climate and energy targets in the European Union, decentralisation of energy sources or distributed generation becomes a viable solution to address the energy efficiency target. Decentralisation is the act of generating energy in areas closer to consumption sites, away from such large nuclear or coal plants. With renewables and energy policies, smaller scale power generation communities such as co-operatives that run wind or solar farms become new stakeholders in a traditional energy grid.

By siting community windfarms close to the source of consumption, the traditional flow of electricity from a massive generation company through transmission lines and distribution substations is disrupted. Transmission systems operators must now manage much more interactivity with the grid, making current objectives of balancing its transmission grid more complicated because there are new generation companies to be integrated into the grid. Distribution network operators on the other hand are also challenged to have to accommodate additional more sites.

The overall impact of decentralisation is creating competitive pressures traditionally monopolistic organisations such as generation companies. The more frequent touchpoints into the grid requires traditional stakeholders to have more up to date information shared across a variety of users to make sure the grid remains balanced, stable and resilient.

Deregulation: De-regulation affects the power and utilities sector in two well established ways. The first type of de-regulation is the demolishment of vertically integrated utilities where generating assets must be separated from the transmission, distribution and retail entities of the operations. This is a more readily accommodated de-regulation with relatively minimal impact on overall grid efficiency or even lower energy costs to the consumer. The second type of de-regulation is the introduction of competition to retail utilities; customers are free to switch their energy supplier just as they are free to switch their mobile or broadband provider. The actual impact on this is mixed; the average churn rate for electricity customer is about 13% in the UK, in what is a highly competitive retail market in Europe. UK's electricity customer churn rate at 13% compares poorly to the average churn rate for mobile services between 25-27%. The power and utilities sector however anticipates that more policy changes are imminent to catch up with the new services and requirements that a full smart grid scenario will require.

Three changes in policies are required at a minimum. The first is to ensure that support incentives are in place to transition towards a cleaner energy system. The European Commission for example is committed to ensure that energy efficiency proposals support the behaviour necessary to achieve the 20% energy efficiency targets, to ensure that the electricity wholesale market can support new grid services such as demand response, and to ensure sustainable business conditions for new business models because of a smart grid system.

This is a disruptive factor to the power and utilities sector because those forward-looking companies are keen to proactively engage in the shaping of these policies development to create the best practices for the rest of the industry.

Digitalisation: Digitalisation is a catch-all phrase of using IT and communications technologies within an IoT system to convert an analogue grid network to a IP-connected grid that provides data and insights to the wider energy ecosystem. This could be as simple as investing in next generation communications networks, upgrading analogue low bandwidth networks. It could also be about enabling connectivity of previously remote and unconnected devices/objects so that the companies can start measuring the status of their assets in the field at greater interval and allowing for others in a control operations room to remotely manage and make better informed decisions.
This is a disruptive factor to traditional power and utilities companies because new investments are necessary to digitalise the grid. In an already long list of investment priorities, these IT-based spending may not make it to the top five must have projects. The benefits, however, of digitalising the

grid is democratisation of data that will open new revenue streams in the future.

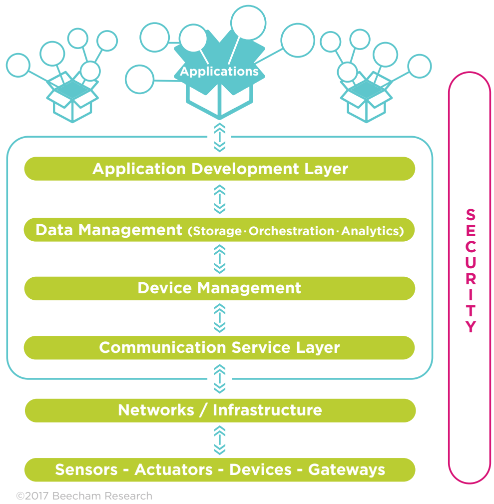
Democratisation: Democratisation is about the dispersion of both proprietary and public data that have been aggregated and anonymised to create new business models. Within the traditional grid, for example, a transmission system operator may invest in a data management platform to aggregate all its operational data into a single point so that various types of users can access the relevant section of insights to make better decisions. New entities can also be formed through the act of making wholesale data publicly available. A start up renewables energy supplier in Denmark, Vindstød, entered the market in 2012 because the Danish regulator opened all energy information that provided transparency of the energy system immediately. With a greenfield approach in selecting only the latest digital technologies, Vindstød could combine digital sales and customer processes to customers and utilise the democracy of previously opaque information to succeed in the marketplace. By the end of 2016, Vattenfall acquired the start-up for an undisclosed amount.

Through these five disruptive factors, the power and utilities sector face an ever-increasing urgency to meet competition by becoming smarter in the way they work and by offering a service level that matches end-user expectations. The sense of "transform now or face irrelevance" drives investment priorities where IoT technologies are being incorporated into existing operational investment projects.

Smart grid is IoT for the electricity system

The various components of an IoT system, in three simplified segments, are essential to support power and utilities companies in addressing the disruptive forces in their sector. As illustrated in **Figure 1**, the IoT system is made up of objects and sensors at the lowest layer, communications networks and services, middleware of platforms fulfilling at least four functions in connectivity management, device management, data management, and application development layer. Equally importantly and must be front of mind is security provisions; without which would increase threat vulnerability to the grid.

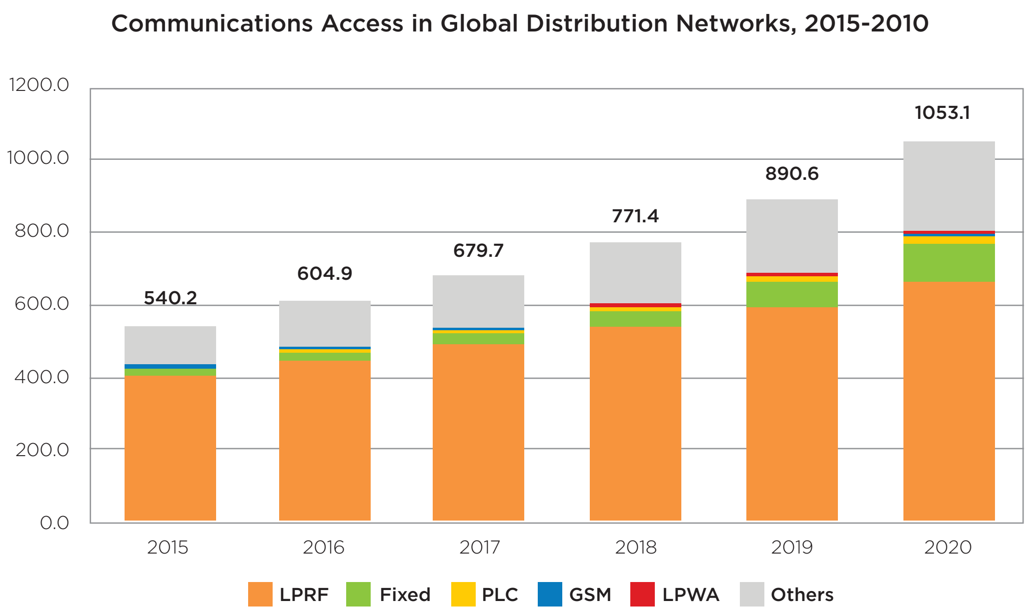
Figure 1. IoT Reference Architecture



In an electricity system, the various objects and machines across the electricity value chain must first be connected to the internet. These objects or machines can be engineering devices from smart meters, invertors or phasers or sensors and aggregators added to add computing power to analogue or simple engineering devices. These objects need to be connected using by a variety of traditional and next generation communication accesses. The legacy telecommunications in the power and utilities sector tended to be power line communications and 2G or GSM connectivity. New communications such as low power wide area access such as NB-IoT, Sigfox and Lora have entered the domain to provide more choices to help connect the grid to become smarter. The third component in an IoT system is the reliance of a middleware layer to bring these disparate components together. The platform layer is also a complex area; those that address connectivity management needs, those that help manage devices in the field, those that bring data together for secure storage, analysis, use and dissemination of data and insights. At the last layer lies the integration with operational technologies, the integration of data with existing enterprise systems and operational systems.

Beecham Research estimated that the number of connections in distribution networks globally reached 605 million in volume in 2016. **Figure 2** ▶

Figure 2. Distribution of connectivity in distribution networks globally



illustrates the distribution of connectivity access in 2016 was predominantly low power radio frequency (LPRF) as it is the existing form of connecting smart meters. Fixed networks, another legacy communication, formed the next biggest access at 3.6%. The next largest access is 2G networks at 1%. By 2020, however, the proportions are expected to change significantly. First, the proportion of LPRF will drop from 75% to only 63%. The reduction will be taken up by fixed networks and power line communications. The growth in access will come from low power wide area (LPWA) access such as 3GPP standardised family of NB-IoT/Cat-M/EC-GSM, and proprietary ones such as Sigfox and Lora. From an initial 1.2million in 2017, the number of LPWA connections will increase to 9million in 2020.

As objects are connected, power and utilities companies can begin to accumulate data to be analysed for insights to make better decisions about operations and in the future, consider monetising their data-centric investments. The following examples illustrate how connectivity, platforms and analytics support power and utilities to address the 5D disruptive forces.

***Generation** companies address decarbonisation and decentralisation forces*

Generation companies such as RWE and EON in Europe are early adopters of integrating renewable energy sources to the grid. The investment priorities at this stage of the electricity grid is to rely on IoT, specifically adding sensors to increase instrumentation to better achieve renewables integration interconnection points within the generation plant and the rest of the grid. The deployment challenge in these initiatives relate to the management and control of operational technologies, suggesting that the role of the middleware in platforms becomes the most important. Without a platform layer, generation companies' key success metrics of balancing investments while integrating RES and optimising opex spending would be affected.

***Transmission** systems operators address decentralisation, digitalisation and democratisation forces*

Transmission systems operators (TSOs) are increasingly relying on IoT platforms to aggregate existing data to better utilise existing aging assets. The investment priority at this stage is to invest in ▶

such a way that existing assets can be extended to fulfil its remit for reliability, stability and resilience of their grid. This means increasing instrumentation and deployment data management platforms that allow TSOs to aggregate available data and to apply analytics to provide better inputs for pre-emptive operations and maintenance activities or better workflow planning for mobile workers. National Grid in the UK deploys IBM Watson to pull data together to enable engineers and non-technical business users to use the same information to address their individual work requirements.

***Distribution** network operators address all five Ds forces*

Distribution network operators (DNOs) are the most active users of IoT technologies amongst the other grid stakeholders. This adoption of IoT technology may coincide with an investment schedule that relies on IoT technologies to achieve their business outcomes. For example, DNOs are tasked with deploying smart meters globally. Even in the case of Europe where the deployment of smart meters is no longer as clearly mandated, DNOs around the world are investing in distribution automation. Together with these operational investments, various IoT components are included. This means that DNOs are considering connectivity and platform requirements as well as integrating cybersecurity elements to these projects.

***Retail** invests for decentralisation, digitalisation and democratisation forces*

Retail utilities are not directly deploying IoT technologies. They however benefit from IoT technologies being adopted by the rest of the grid and even their consumers. First, they are using the results of having increased instrumentations that generate more data that is converted to intelligence for various uses. In the case of retail utilities, their customer facing functions are improved by being able to offer relevant information to their customers who expect instantaneous information. Second, retail utilities also expect to utilise increased instrumentation within residential homes, where IoT devices such as smart meter, smart thermostats and small-scale generation assets such as solar panels and residential energy storage facilities to increase the instrumentation necessary for consumers to manage their own energy production and consumption. Retail utilities hope that smart homes services can be the salvation of new services that create customer loyalty and minimise churn out of their contracts.

The current investment patterns among traditional power and utilities companies are common in the pursuit of data and insights to improve business as usual operations. While they aspire to utilise IoT technologies to support their transformative goals, they do face three main implementation challenges.

Three IoT adoption challenges

The first is in the selection of an appropriate IoT technology, whether it is communications or platforms. The second is integration, with enterprise and operational applications, of data, and with the increased number of interconnections and interactivity with third parties in a smart grid scenario. The final adoption challenge is security assurance, where power and utilities companies already struggle to keep up with a rapidly evolving security threat landscape. Mistakes in these three main challenges result in financial penalty for downtime and any associated public relations fallout.

Selection of communications access: The emergence of new communications discussion such as the progress towards 5G and the increasing prominence of Sigfox, Lora and other low power wide area networks such as the standardised NB-IoT in 2017 meant that power and utilities companies have many choices. The selection of these new protocols over existing communications topology such as power line communications and traditional use of low power radio frequency raises questions on which access is better suited for which operation requirements.

In cellular or GSM, power and utilities companies already must deal with telecommunications operators deciding to eventually shut down their 2G/GSM networks. In the United States and most parts of Asia, mobile operators have announced that they will decommission their 2G networks. Existing business customers can either take their business somewhere else or take a strong stance and demand that the networks be continued. Whatever the outcome, power and utilities companies do not want to have to deal with such possibilities again.

This demand that networks be in business for the duration of their customers means that there is uncertainty towards the longevity of such start-ups as Sigfox and Lora in offering low power wide area networks. Power and utilities companies are then further given a choice of using standardised communications access by 3GPP on NB-IoT/Cat-M/EC-GSM. Each of these low power access addresses a similar but also different requirement.

Selection of platforms: If the number of communications access is considered one too many, then power and utilities companies face an even more complex choice in selecting a platform. Add to this complexity is the current organisational structure within power and utilities companies, that there may be two different groups of budgets, the IT and the operations team, each of which have their preferences of using their traditional vendors in IT or industrial vendors. They have a limited internal resource/knowledge of what makes the "optimal choice". They also have limited resources to investigate vendor's claims. To test any platforms will incur IT and human resources, both of which are scarce resources that can be better utilised in core tasks. Finally, they also have a rapid time to market to ensure applications are not only deployed quickly but also deployed first time right. The financial penalties for applications downtime can go up to millions in many cases.

The first-time right requirement for platform selection is especially crucial to the power and utilities sector because very often the integration of the middleware requires man hours for piloting, testing and rollouts. It is in this very wide nature of the middleware layer that makes the selection choice very crucial. In the case of industrial control systems such as those in the energy grid, power and utilities companies tend to have many brands of industrial equipment that proprietary and have very closed concepts of application programme interfaces (APIs) and integration protocols for easy interoperability. Despite efforts from industrial vendors that they are interoperable, the level of openness does not reach down to the type of programmable logic controllers distributed throughout the facilities. Platforms and expertise from an IT perspective can overcome these integration problems more easily and can support power and utilities' time to market better. The crucial element here is that power and utilities companies often do not realise the laborious extent until a platform is being deployed.

Integration with applications, data and third parties: Many of the examples of power and utilities companies adopting IoT have reflected an operational difficulty to extend their tests or trials out to more operational applications, or to more sites – for example, increased number of residential households in the trial for virtual power plants, or to more types of third parties, such as local authorities, electric vehicle owners or aggregators. This difficulty is in parts due to the proprietary nature of industrial equipment, where API libraries that can speed up integration remain limited. Similar to the risk of selecting the wrong platform, the act of integrating a software or application to the rest of the grid must be done as smoothly as possible to avoid disruption of operations.

Security provision: The third and increasingly important challenge is the incorporate cybersecurity considerations into any IoT and operational investments. The deployment challenge is made more complex when both IT and operational security needs must be accommodated and traditionally both domains work relatively independently of each other. This divergence is dangerous. First, security breaches can enter the operational domain via the enterprise IT space. The recent ransomware is only a recent but prominent example. Secondly, the business case for additional security investments is already difficult. By leaving out the benefits accruing to one of the two domains diminishes the value of such investments. Finally, as the threat landscape becomes more sophisticated, the defence must be made more holistic to avoid any weak links. It is this continuous requirement to not only prevent, detect and respond to threats, but it is also important to see the whole picture of both IT and operational domains together. Increasingly, there is convergence of IT and operational security solutions to address exactly this ▶

requirement, relying on information sharing on threat intelligence and automation, analytics and artificial intelligence to provide the relevant insights for security specialist teams to monitor their company's real-time security posture.

The future of energy companies relies on finding new business models

Despite the appreciation of how IoT can improve power and utilities' business outlook, the flow of investment into IoT is relatively slow. According to Beecham Research's studies, the automotive sector is the largest sector with IoT connections. The operational reason for the power and utilities sector for not taking on a bigger piece is because the companies are constrained in making the business case. The value of IoT enabled smart grid is in the positive externalities that are often not included in a Transmission systems operator's or a generating company's business case. The IoT community has a long way to help power and utilities companies make that wider business case for additional investments. The case studies illustrated so far show that investments are related to business as usual scenarios. These are mostly related to cost issues; of process optimisation and minimising both capital and operation expenses. While the sector aims to monetise data, the relative regulated nature of the sector and a lack of understanding on data security and privacy adds to the constraints to turning insights into a revenue stream.

Power and utilities companies are investigating how emerging technologies can help with these 2 objectives. Blockchain has captured the sector's imagination in a way that is contrary to how the financial services have embraced it. However, the nature of blockchain technologies does address several of the disruptive forces facing this sector. For example, the distributed ledger nature of blockchain allows for integrating solar credits in renewable energy sources. It also provides the settlement mechanisms in the trading of credits. Finally, blockchain also allows internet of energy to eventually integrate any third parties linking to the grid, building towards a true self-healing energy grid.

Blockchain initiatives in the energy sector however are related to operations and cost optimisation issues. For utilities looking for ways to create a revenue stream through transformation is the importance of privacy technologies. Blockchain might be one of them but other technologies that allows utilities to build a reputation of trust could be another way forward. Considering that utilities, together with telecommunications companies, have a direct and recurring billing relationship with the consumers, this is an area to explore. As society moves towards greater digitalisation and intelligence, the B2C element of IoT is the area that needs to be further developed. IoT policies around individual privacy, for example those related to e-privacy and General Data Protection Regulation in the European Union, have deep influence on the direction of smart homes and the role of utilities in the development of smart living, of home domains, car or mobility domains, office domains and within an urban space domain.

Retail utilities have the potential to lead in this initiative, of using their billing relationship with the consumer, of their aggregated knowledge of residential energy consumption, to begin to offer a connected living proposition. It can lead in the development of a new trust metric that treks how the retail utilities has been at protecting data security and privacy assurance. This will require new technologies that captures and enables audit of how an IoT device has been manufactured securely, its app and data storage are secure, and privacy notices comply with GDPR requirements. The smart homes domain is a natural place to start exploring this.

Retail utilities can utilise their user experience investment to allow consumers to manage and monitor their privacy settings. Using privacy technologies as simple as more transparent cookies management in anticipation of the GDPR implementation, retail utilities, through their web interface for laptops and mobile screens, enable consumers to see what they have enabled for data to be shared and tracked on demand. This technology enabled control for consumers is essential to build up trust where the auditable nature of the solution also gives the retail utilities a trail in which to demonstrate it is doing what it says it is doing. This trace gives both parties a metric to measure against any trust measurement, which would make retail utilities a rather relevant place in a connected living scenario. ■

Conclusion

IoT technologies are being considered as complementary to power and utilities investment into smart grid. In the simplest terms, power and utilities companies need to connect their objects and machines to have the insights and intelligence necessary to fulfil the smart grid vision. In the next step, the industry is relying on IoT technologies to address the disruptive factors to remain relevant in a digital world. The selection of existing IoT technologies is time consuming with significant financial risks. It is thus important to understand your requirements clearly to find the optimal technology partner.

beecham research

Shaping the IoT future

About Beecham Research

Beecham Research is the leading market analyst and consulting firm specialising in the development of the rapidly-growing IoT market worldwide. Based in London (UK) and Boston (USA), we have been studying this market for 16 years and are recognised internationally as industry thought leaders with deep knowledge of the market dynamics and technology at every level in the value chain including IoT services, platforms and solution security.

Beecham Research clients span components and hardware, network operations, system integration, application development, distribution and enterprise adopters. Industry sectors where we have particular experience include Energy, Healthcare, Manufacturing, Retail, Smart City, Smart Farming, Smart Home and Transportation. The company is also the leading analyst firm in satellite IoT, low power wide area, and is also working in the wearable technology market.

Beecham Research has been actively researching the IoT platform market for nearly a decade. More recently, as part of our developing support for enterprise users, we have designed a series of tools to aid IoT platform selection.

www.beechamresearch.com