THE SMARTER OPTION

Phil Beecher *draws on last year's Journey to IoT Maturity report to discuss whether security can go hand in hand with the development of smart utilities*

The energy sector is undergoing a huge transformation, becoming reliant on highly connected communications infrastructures, with millions of endpoints, including a wide range of smart grid devices, such as smart meters and distribution automation devices.

Rapid digital transformation is happening across many sectors – and the energy and utilities industry is not unique in this respect. Huge resources are being invested in smart initiatives to transform the sector, making it more intelligent, innovative and fit for a more sustainable and cleaner future.

In the US, the Biden Administration has successfully introduced the Infrastructure Investment and Jobs Act (IIJA), which includes investment of at least $80-billion into energy and utilities, and described as a: "once-in-a-generation investment in our nation's infrastructure". Funds have been allocated for upgrading the country's grid infrastructure in a move to facilitate the expansion of renewables and clean tech solutions, and making it more resilient to extreme climate events.

But with change comes great responsibility. Evolving decades-old systems into highly connected intelligent infrastructures with millions of devices and endpoints comes with the added danger of significantly increasing the risks. Energy services are a key component of a country's critical infrastructure and the growth of communications networks risks making utilities increasingly vulnerable to attack. Ensuring the communications infrastructure is resilient to cyber attacks must be a key consideration.

Evolving decades-old systems into connected infrastructures with millions of devices and endpoints also increases the risks

Internet of Things (IoT) technology offers huge opportunities across many sectors, not just energy and utilities, which in some regions have benefitted from smart grid initiatives such as smart metering for a decade or more.

In our first state of the nation IoT report published back in 2017, when there were far fewer pilot projects and implementations, we surveyed IT decision makers in the US and UK to find out their attitudes to the technology. Five years later we published a second study so that we could compare attitudes and adoption patterns among smart cities, smart utilities and industrial IoT (IIoT) adopters.

IoT is a bigger priority than ever. More than nine in 10 respondents said that they need to invest in the technology over the next 12 months to remain competitive. The fact that IoT can help them to become more agile is a key driver for adoption. This equips adopters to meet volatile operating conditions, and during the serious economic and geo-political disruptions that we are seeing today.

Early adopters it seems have gained confidence from digital transformation projects that have offered quick wins and as smart solutions have matured. Companies are more likely to be building on their early successes and evolving towards more ambitious strategies. In addition, respondents feel that having an IoT strategy is a must-have, rather than a nice-to-have.

Plans to roll out initiatives have also evolved in the last five years, with projects around security and surveillance, distribution automation and advanced meter infrastructure all up on the previous study.

While newer initiatives, such as electric vehicle charging and connected street lighting are taking the technology even further.

As adopters become more comfortable with this tech, security and data privacy challenges that might have given them pause for thought five years ago are now better understood, and so less of a concern. Respondents ranking security as one of their top challenges fell by more than half in our latest study.

THE GROWTH OF COMS NETWORKS RISKS MAKING UTILITIES INCREASINGLY VULNERABLE TO ATTACK

With industry reports suggesting that IoT devices are being subjected to a growing number of cyber threats, this shift is interesting in the current threat environment and increase in attacks on critical infrastructure. The US Government Accountability Office (GAO) stated recently that: "nations and criminal groups pose the most significant cyber threats to US critical infrastructure, according to the Director of National Intelligence's 2022 Annual Threat Assessment. These threat actors are increasingly capable of attacking the grid."

Each new device connected to a smart grid could present an opportunity for would-be attackers. With an increase in the number of distributed energy resources (DER), such as solar PV panels, wind turbines, fuel cells, battery storage units and electric vehicles/chargers, this further increases the threat surface and so presents new challenges within the sector.

If not 'secure by design' and properly managed, the rapid roll-out of smart meters can increase the risks opening up new attack vectors that can be used to launch a cyber attack to disrupt systems causing power outages or even physical damage. Threat actors can take advantage of vulnerabilities such as inadequately secure communications protocols in smart metering or distribution automation systems.

Smart meters are typically part of a bigger and more complex infrastructure that involves multiple parties, including utilities, grid operators, services operators and customers. They are designed to not only collect and send billing information back from customers to utilities, but also can indicate usage patterns which can be an attractive target for hackers as they disclose sensitive and personal information, including when premises might be unoccupied.

Managing large volumes of data is technically difficult, particularly when regulators interpret the data used by many IoT systems as sensitive or personal information. Those that fail to protect this data risk running into compliance issues that can result in financial penalties and reputational damage.

In our latest study, data privacy regulation was listed as the second highest (political, economic or social) challenge, with more than a third of IT decision makers placing it in their top three. Further, concerns surrounding big data have also increased over the last five years, with around one in five

respondents (up from 11 percent) placing it in their top three challenges for IoT project rollouts.

New data regulations, including the GDPR and the California Consumer Privacy Act (CCPA), have come into force since the first report in 2017, possibly driving up these concerns. Stricter data protection laws put the responsibility for protecting confidential data and information firmly in the hands of those organisations collecting, analysing and storing it.

With the sector facing an ever-greater number of cyber threats and with energy security now a high priority among policy makers and nations due to geo-political turmoil putting energy supplies at risk, the spotlight is firmly on the need to protect our energy infrastructure and the smart networks that it is increasingly reliant upon.

In a recent poll conducted by Wi-SUN Alliance among senior professionals at utility companies, energy security is seen as one of the most important issues in relation to smart/IoT technology development over the next year. But this must happen alongside government funding and initiatives to help drive smart utilities, according to utilities professionals. This is already happening with the US's IIJA investment plans mentioned earlier. In the UK, the Energy Secretary recently outlined steps to strengthen the country's long-term energy security as part of its plans for affordable, clean and, importantly, homegrown power and green energy.

For smart utilities to grow and prosper, but in a way that ensures the highest levels of energy security and protection from cyber threats, we must ensure that the right technology is in place. Designed and built with security in mind from the start, smart systems and connected devices can provide the intelligent monitoring and granular controls that utilities and other providers need to be agile and responsive, and to ensure they are delivering efficient and reliable services.

One of the most important parts of any smart utilities project is choosing the underlying network communications infrastructure. Secure, resilient and responsive communications can open up the possibility of exciting new innovations and collaborative opportunities.

Mesh networking topologies, which can provide peer-to-peer connectivity between devices without routing through a central point, are increasingly favoured among IT decision makers, according to our IoT report. The number exclusively using star networks dropped from 21 percent in 2017 to 12 percent in 2022, while those using hybrid networks, combining mesh networks and star, rose from 58 percent to 68 percent.

Open standards are another critical enabler of innovation and collaboration in a smart utilities' context. We found the number of IT decision makers who believe open standards are either "very important" or "absolutely crucial" rose from 79 percent in 2017 to 84 percent in 2022. Why? Because networks built with open standards can be relied upon as secure. IEEE and IETF data encryption standards and certificate-based device authentication greatly reduce communications network vulnerabilities and minimise the risk of data theft and system sabotage, for example.

There is huge potential for smart technologies and IoT to drive value and success for energy and utilities providers. Those who are able to harness this potential via secure and open standards-based networks will be the winners in the race to a smarter and more resilient industry.

But security and data privacy must remain a priority at every stage of the process, baked in from initial design to implementation and beyond as systems continue to evolve in the future. Get these right, and the benefits that smart utilities can deliver are huge ●

Phil Beecher is President and CEO of Wi-SUN Alliance. Since 1997, Phil has played a key role in the development of communications standards including Bluetooth, wi-fi and various IEEE standards and the specification of test plans for a number of Smart Utilities Network standards, including Advanced Metering Infrastructure (AMI) and Home Energy Management Systems.

It is vital to protect our energy infrastructure and the smart networks it is reliant upon

Picture credit: Wi-SUN