TAILORING IOT ARCHITECTURE FOR UTILITIES

Within the utility industry, the IoT concept has found its way into distribution operations and information technology (IT) organisations through seemingly benign business requests. The reality is that these requests should require departments to contemplate more about the future of their enterprise architecture, rather than merely addressing present-day issues.

In an interview with Metering & Smart Energy International, Roy Pratt, chief architect and technology strategist at BRIDGE Energy Group, shares his insight into taking an architectural approach to the design and implementation of Internet of Things (IoT) technologies in utilities and why it's critical to their future success.

MSEI: Can you provide a detailed explanation of what it means to take an "architectural approach" to the design and implementation of IoT in the utility context?

RP: It is of the utmost importance that utilities take a disciplined, architectural approach to doing IoT. IoT is not something you want to allow to just happen and grow organically, through adding IoT devices and systems to your network haphazardly, without direction or planning. What I mean by 'architectural approach' is the application of some structured enterprise architecture framework ie. TOGAF, USDA, DoDAF, etc. to help a) define the vision for IoT in your organisation; b) analyse the business model that supports that vision; c) design the information/ data architecture and 4) incorporate the IT governance needed to keep it all together.

In many cases, IoT technology is almost too easy to 'bolt' onto existing legacy applications, operational systems and data sources without doing the architectural work. A disciplined architectural approach makes sure that the technology fits with existing systems and applications by evaluating the ramifications to the current organisational business model, technology environment, and data repositories.

So – it's really the application of a structured architectural approach that we at BRIDGE advocate. Practitioners will promote certain frameworks – some may be stronger in certain aspects than others, but the key is that the right one is chosen to provide the organisation with the best results for their type of business.

The framework chosen must be recognised as sound, proven, but most importantly, it should be familiar to the enterprise architecture team that must use it. It should ideally have the supporting tools, standards and processes needed to go along with that framework. You don't want to be figuring out IoT and figuring out a new framework at the same time.

MSEI: Which enterprise architecture frameworks are most commonly used by utilities for IoT?

RP: While we don't advocate any one framework, the two most common frameworks that we come across in utility architecture work are TOGAF (well over 50% utilities that we work with) and USDA. In our experience, most utilities have adopted and are using some form of TOGAF. Utilities also use a variety of others such as DoDAF and MODAF. These are related frameworks and are commonly used by utilities, their IT departments and many of the technology services companies supporting utilities.

What are the pillars upon which IoT architecture is built?

RP: The first is to find a proven, familiar framework to be followed. Second – begin the IoT architecture process with the end goal in mind. Explore the questions that you are trying to answer through architecture work – before you begin. This provides a map of where you are going. Having these questions upfront allows you to frequently revisit them throughout the architectural process to ensure that the framework is forcing you to look at the key things that need to be addressed. Scalability, reliability, performance and security are some of the key things that need to be addressed with IoT systems.

Utilities also need to consider the uniqueness of IoT technologies. Enterprise architects are used to architecting all types of systems, devices and technology. However, you have to keep in mind that there is generally some uniqueness to that new system or that new device that your architectural approach may not have taken into account previously. The uniqueness of IoT devices and systems includes factors such as third party trusted security that you should look at. Often, these devices aren't within your technology domain; they're just some device out in the network that may be shared device outside your security authority.

Also tying in with the 'uniqueness of IoT devices' is the niche functionality of these devices. Many IoT devices are limited to one or two functions, so you may not be able to apply some of your typical system-level thinking to these devices. Their communication protocols, data structures, and integration adapters will likely be as unique as the devices themselves and be new to your technical staff.

Moreover, scale and volume need to be factored in – from pilots to large-scale rollouts, IoT devices may come into the organisation as a proof-of-concept, pilot, or test. The next thing you know a production implementation is approved and the number of devices can blossom to thousands or tens-of-thousands very quickly.

> *"IoT is not something you want to allow to just happen and grow organically, through adding IoT devices and systems to your network haphazardly …"*

Lastly, an important concept to mention is the autonomy of IoT devices. IoT devices can be virtual or physical devices over which you have little to no control. You may be connecting to that device because of a service it offers in providing a video or audio feed or temperature reading, etc. So, there are many unique features of IoT devices and you need to ensure that this is considered when going through your architectural approach and framework.

MSEI: What in your experience works particularly well when designing an IoT architecture? In other words, what are the key elements of success when designing and implementing IoT architecture for utilities?

RP: There are not a lot of utilities doing this yet. BRIDGE's approach and discussions with many utilities is that they need to be proactive when it comes to IoT. Typically the tools we use in advocating an architectural approach use TOGAF as the primary enterprise architecture framework. We also use a lot of standards support from places like CIM. Standards are starting to define and put some structure to the IoT devices out there.

MSEI: Can you expand on the significance of an IoT platform within the overall IoT architecture?

RP: IoT platforms bring together all of the pieces of related technology to build on an IoT ecosystem. An example is OpenFMB. This is a reference architecture in a framework for distributing information and control with IoT devices. OpenFMB leverages common internet standards to distribute data and control across IoT field devices. Instead of having a master-slave environment, it enables devices in the field to actually communicate with each other without having to go back to a central device. The purpose is to try and shorten the communication time between devices and relieve the amount of data that must go back to the utility for decisions to be made.

IoT platforms will continue to mature as the technology matures and proliferates. You should expect IoT platforms to pull in your standards, drivers and interfaces and your data structures, management tools and security tools into one place. Bringing all these elements together will enable the creation of a high quality IoT system faster, cheaper and more reliably.

Architects and developers should be wary about getting stuck with proprietary platform technology that is not sufficiently based on open standards, leaving you trapped in a virtual 'cul-de-sac.' Open standard platforms can be provided by multiple vendors in the market.

MSEI: What are the pros and cons associated with building versus buying an IoT platform?

RP: There are two sides to this coin:

If you absolutely know what you want and know what a certain platform can do; then

> *The rollout of IoT architecture requires IT and OT skillsets as well as executive level management to steer the utility's vision for IoT in the organisation.*

buying an IoT platform is probably the way to go because the required functionalities are already integrated.

However, if you are just starting out and trying to understand how to exploit IoT technology and how it is integrated with the rest of your systems, I recommend building your IoT platform. When you build an IoT platform and put it together yourself, you understand its strengths and weaknesses at a lower level of capability and dependency of the components in that platform.

MSEI: Who is responsible for the design and implementation of IoT architecture?

RP: Chief technical officers, chief digital officers and chief information security officers are the individuals within an organisation that need to provide executive level support for designing, developing, building and rolling out IoT architecture. When it comes to understanding and exploring IoT technologies, you will generally have a group of enterprise architects that are familiar with real-time communications in these distributed environments. These individuals may reside in the IT (Information Technology) department or OT (Operational Technology) department, but it really depends on the utility. Utilities may have one technology department (IT and OT together), but most times, you'll find that these two functions are separate – IT which deals with enterprise, back office and shared services and OT that deals with operational technology systems such as supervisory control and data acquisition (SCADA) systems, outage management system (OMS) and the utility's advanced metering infrastructure (AMI) etc.

BRIDGE has found that a majority of IoT architecture and technology is most easily understood by many of the OT folk who are familiar with distributed communications. The downside in the OT organisation is typically in the areas of structured approaches and data architecture and security – that's where a combined organisation that leverages data architects and security architects from IT is really important. When you look at the key functions aside from understanding IoT devices at system level and understanding last mile communication, which is a very strong OT quality, you need to understand data architectures extremely well – what devices can do, how they do it and what type of data they will be sending in. You must be intimately familiar with how these devices fit into the security architecture.

OT departments typically deal with hundreds or thousands of devices. Folks in IT are used to working with tens of thousands of devices and are much better at handling the scale of IoT devices. IT personnel know for example that with monitoring systems and configuration management systems are needed to help manage the size and scale that's involved in IT operations and processes which is very similar to the size and scale of devices you would be dealing with in IoT.

Ultimately, the rollout of IoT architecture requires IT and OT skillsets as well as executive level management to steer the utility's vision for IoT in the organisation.

MSEI: Can you expand on the importance of flexibility and scalability when designing an IoT architecture?

RP: Scalability and flexibility go hand in hand. However, scalability is the primary driver, because flexibility is really constrained by the niche service functionality of the IoT device in general.

For example, once you have architected an IoT humidity sensor in the network, the functionality of that IoT humidity sensor is not likely to change very much. As long as it exists, the device is only going to perform the functions of a humidity sensor and is not going to do much else. You're not going to re-programme its functionality, so many of these IoT devices and systems are very niche and are not meant to be changed – they're meant to be changed out. On the other hand, you may have scaled from a couple of hundred IoT humidity sensors in a pilot or proof-of-concept, to a million very quickly, because they are cheap, easy to implement and ubiquitous.

Flexibility really comes into play when architecting the core systems and applications that the devices will be talking to ie. outage management systems and asset management systems. Outage management systems in utilities used to only talk to the IVR system and the CIS system – that's where they received all their input from. Flexibility became important with AMI systems being introduced, and AMI systems, like IoT, provided a whole lot more volume and frequency of data input regarding whether power was on or off at a particular endpoint. Prior to that, OMS systems did not have a clue what was going on at that endpoint. So we have been able to make OMS systems much better, but again, the key there was the flexibility of that OMS system and being able to incorporate services coming in from new IoT devices or AMI meters out in the field.

MSEI: Where have utilities typically gone wrong with regard to implementing IoT-enabled technologies? What are the common pitfalls to avoid when adopting and implementing an IoT architecture?

RP: Many utilities are testing IoT technology right now – they are just starting to recognise the platform architectures that are out there and what vendors are offering.

The pitfalls to avoid would include allowing the organic growth of IoT to occur without a structured architectural approach. IoT is a whole new branch of architecture, just like existing core systems such as meter data management (MDM) and distributed energy resource management systems (DERMS). Thus, utilities need to take a similar architectural approach to implementing IoT. Finally, utilities need to recognise the uniqueness of IoT devices and systems in their architectural approach and frameworks. Adhering to these guidelines will help utilities avoid some of the major pitfalls when implementing IoT technologies.

Utilities are keenly interested in IoT and the impact it has on business models and grid modernisation plans. Utilities are evaluating IoT as part of new business models as well as part of their push to become distribution system operators, integrating a myriad of distributed energy resources and devices.

Furthermore, IoT technology is a key component in utility grid modernisation plans – which really speak to IoT at the edge of the utility grid. This is where the utility is looking to add new devices or additional devices or intelligence at the edge of the distribution network integrating batteries, switches, sensors , inverters and other smart technologies – that's really IoT for the utility. MI