VENTURE Insights

Launching your IoT network strategy

Choosing an LPWAN network for the long haul

May 2020

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

VENTURE Insights

Table of contents

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Executive Summary

Interest and investment in Internet of Things (IoT) solutions is growing in every industry. IoT can cut costs, improve efficiency, and increase the visibility of industrial processes. It is not surprising that many companies and government agencies are now exploring IoT technology and developing use cases.

One option for IoT connectivity is a direct connection to the cellular mobile network. But increasingly, low power wide area networks (LPWAN) are preferred because of their cost, coverage and power advantages. This whitepaper focusses on cellular LPWAN networks that are based on mobile networks.

Different organisations are at different stages of their IoT journey. Typically, they will start by experimenting with IoT devices and networks to develop a better understanding of the technology and its potential. But technology isn't much use until it is applied to real business problems. Organisations must move past awareness raising, testing and trialing to address concrete business issues.

It is natural to test and trial more than one IoT network or platform technology – that's what tests and trials are for. But tests and trials must be accompanied by an early assessment of the strengths and weaknesses of each network technology, to ensure that the network can support the business solutions you are trying to implement. Otherwise, you risk committing to a 'technology trap': a network that doesn't give your IoT strategy room to grow and develop.

The network criteria you need to consider include:

1. The scalability of infrastructure and platforms as the device network grows
2. The coverage the network can provide, and on what timeframe
3. The security and reliability of both network and platforms, as IoT use cases become more critical to the organisation's business
4. Two-way operation to make it easy to upgrade device firmware and control devices.
5. A clear technology roadmap and global vendor support.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Figure 1: Buyer criteria for a long-term IoT strategy

Scalability

The first feature you want is scalability. A scalable network can support ten, a hundred, a thousand, or a hundred thousand devices, but the cost of adding and operating a new device doesn't rise. In fact, economies of scale mean it will probably be cheaper to add and operate each device as your device fleet grows. Further, a scalable network means that adding more devices doesn't cause radio interference between devices and doesn't slow down your data transfer. Finally, a scalable network will allow you to add new kinds of devices for new solutions smoothly, and without disrupting your older devices.

In contrast, a network that doesn't scale constrains IoT growth. It gets more expensive as you roll out and manage your solution to new geographies, and it will become more expensive as you deploy new devices and solutions.

Coverage

The second feature you want is coverage. Checking the coverage of your candidate networks is something you should do at the test and trial stages of your IoT strategy development.

A network with established coverage allows you to roll out an IoT based solution without costly investment in new network infrastructure like towers, antennas and backhaul connections. It speeds up roll out because roll out isn't dependent on getting that new infrastructure in place and finding suitable and accessible locations. Finally, it lowers overall capital cost because you can minimise the need for alternative solutions in blackspot areas.

Carrier cellular networks have these advantages, and more. You don't need to get into how they operate, and you don't need to maintain or operate them. Instead, you have the certainty of knowing they will be there, and how much they cost. Carrier cellular networks can even extend your coverage internationally through roaming agreements, to support export or international transport businesses.

In contrast, a network that lacks coverage requires in-fill investment. This slows down deployment. And it adds cost because remaining blackspots require even more investment, or the deployment of a different solution in blackspot areas. In addition, these new network builds will need to be managed on an ongoing basis to ensure network reliability, adding cost.

Security and reliability

The third feature you want is security and reliability. These aren't the same thing, but they are closely related. A secure network protects you by protecting your IoT solution from unwanted scrutiny and malicious attack. A reliable network also protects you, but from service disruption. Networks are secure and reliable when they natively provide encryption and other forms of security, and they use the best quality spectrum and infrastructure.

In contrast, networks are insecure when they either lack security measures entirely, or have security added as an afterthought. They are unreliable when they lack dedicated, managed spectrum, or they don't use infrastructure backed by an experienced network operator and world-class technology vendors.

Two-way network

The fourth feature you want is a two-way network. Devices send data, but sometimes it is necessary to send data back to the device, if it is controlling something or maybe because the device needs a re-configuration or a firmware upgrade. But not all networks can do this. A one-way network means you cannot upgrade the firmware on your devices or use your network to go beyond data collection into more sophisticated solutions that use IoT to control business processes.

Open, global standard

The final feature you want is an open, global standard. Your supplier should be able to explain how their network will be developed and kept up to date as IoT advances, and how the technical standards that the network is based on will be extended to meet new needs. And they should have the internal resources to ensure that happens.

Sinking investment into networks that don't meet these criteria will cut off a lot of the potential of IoT for your organisation.

This might not be apparent early in the IoT development cycle. But it will become apparent as you start integrating IoT more and more into your business processes and attempt to deploy more sophisticated solutions. And the only way out at that point is costly write-offs of your network investment and starting all over again.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Cellular LPWAN solutions aren't the only ones in the market. There are non-cellular networks too. So it's reasonable to ask what makes cellular networks the best long-term choice for your IoT strategy.

Cellular mobile operators in Australia operate two main cellular LPWAN technologies: NB-IoT and LTE-M. "Cellular" means that they are delivered by the same infrastructure as the mobile phone system, with one big difference – they have a much bigger range than the mobile phone range, covering around twice the area nationally. And because cellular LPWAN technologies share the same 700Mhz spectrum as the 4G mobile network, they have excellent in-building and in-ground coverage as well. These cellular LPWANs compete with other, non-cellular LPWANs, principally LoRaWAN and Sigfox.

But cellular LPWANs have capabilities that make them stand out as a long-term network choice:

1. Cellular LPWANs are highly scalable, designed to support scenarios with hundreds or thousands of devices per mobile tower. This gives your strategy room to grow.
2. Cellular geographical coverage, particularly Telstra's, is second to none. This means you won't need lots of in-fill solutions to get the coverage you need.
3. Cellular LPWANs have built-in, carrier-grade security. And unlike their competitors, they don't share spectrum with other kinds of operators, having dedicated spectrum that guarantees unimpeded access to bandwidth. This means you can count on the security and reliability of cellular LPWAN communications.
4. Cellular LPWANs are truly two-way networks. You can control and maintain devices as well as get data from them, without the expense of costly truck rolls..
5. Cellular LPWANs are backed by some of the biggest technology companies in the world, and the world's biggest technical standards organisations. They're around for the long haul.

Finally, an IoT system is more than the network. It requires devices and platforms to collect, manage and analyse data to generate the insights that inform and control business processes.

Telstra's cellular LPWAN networks will interface natively with any IP-based platform, so the customer can choose whether to use a Telstra device management or data management platform or a platform from someone else.

A long-term investment in IoT requires a technology partner that will be around for the long haul. Telstra has been delivering networks and solutions to Australian customers for over a century, longer than any other technology company still in the market.

And Telstra can help you design, test and trial secure and reliable IoT solutions that scale and have instant wide area coverage, giving you plenty of room to grow and evolve your IoT strategy. With a workforce of over 20,000 technology and business experts, Telstra can also provide end-to-end professional support and ensure that you get the most out of your IoT strategy.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Launching your IoT strategy

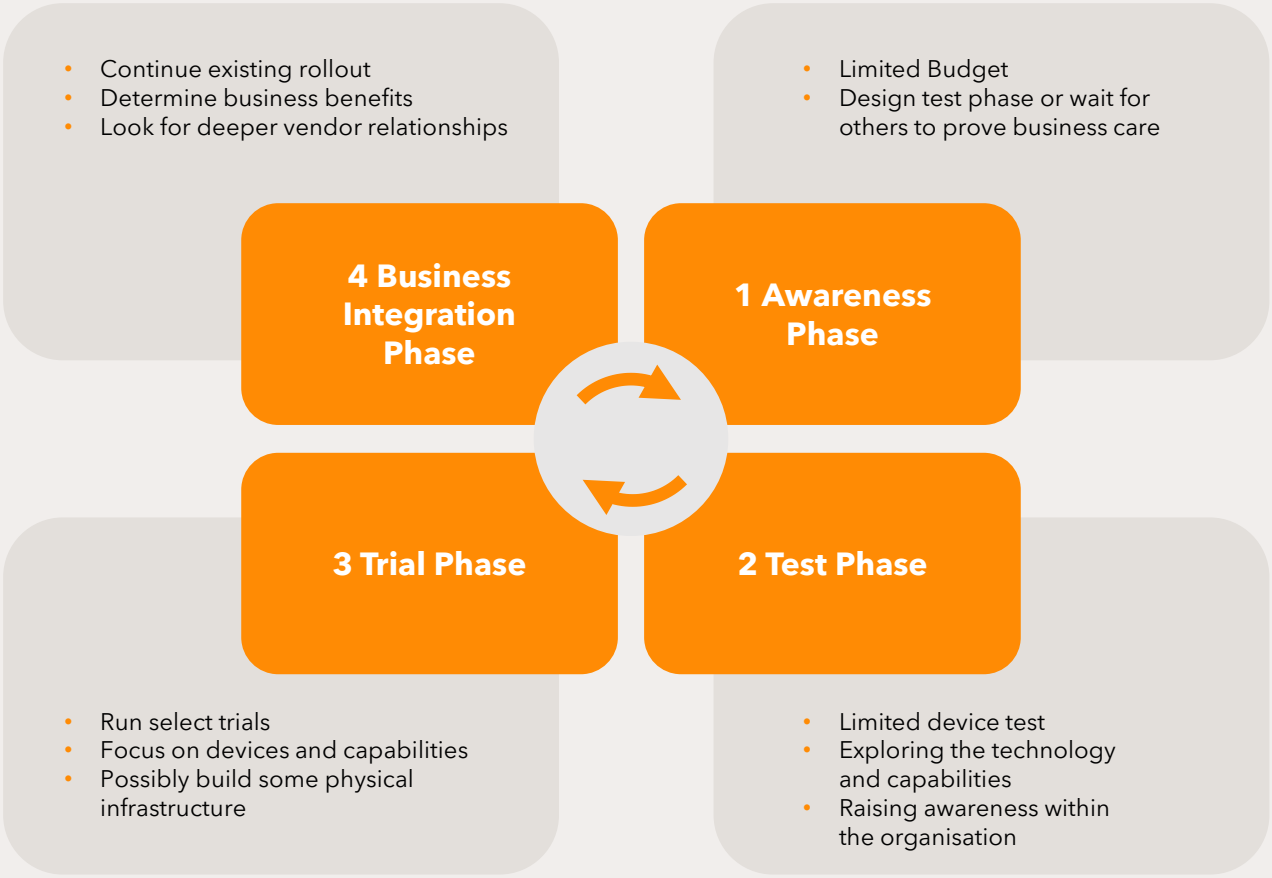
All IoT strategies depend on a low-power wide-area network (LPWAN) that can support and connect IoT devices. Choosing that network is part of the process of developing and implementing an IoT strategy that supports your organisation's business processes and delivers positive return on investment. It is crucial to choose a network that gives you options for future use cases and does not cut off the long-term potential of IoT.

The IoT development cycle

Organisations moving into IoT do not address all of the business issues immediately. There is a learning curve as they start to understand its technology capabilities and its business costs and potential.

There are four main phases of IoT strategy development in the typical organisation, reflecting this learning curve.

Figure 2. Four phases of IoT development



SOURCE: Venture Insights

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

1 Awareness phase

The first is the Awareness phase. The organisation has a general idea that IoT can deliver benefits, but there is often little linkage between IoT and the wider business needs of the organisation. It may be developing concepts or designing possible tests, and often they are watching peers to see what successful use cases emerge in their sector.

Typical Awareness stage activities revolve around information gathering and industry discussions.

2 Test phase

In the Test phase, the organisation's IT team will typically be conducting limited device, connectivity and coverage tests, exploring the technology and its capabilities. This is the phase where an organisation starts to think about the technology it will use, particularly which LPWAN network they are going to commit to.

Longer term business considerations are not central yet with project managers still focused on getting the network and data platforms to operate.

3 Trial phase

In the Trial phase, the organisation typically starts to invest in IoT devices and connectivity infrastructure for trials of a particular business or industry use case or cases. There will be more focus, particularly on certain use cases, as the organisation tries to identify the 'on-ramp' applications that might have a clear business case. In this phase the organisation will be gathering information about technology capabilities and performance in the field, particularly coverage. It will also be starting to think about how to support the organisation's business processes, for example by generating cost savings.

4 Business Integration phase

The final and most advanced phase is the Business integration phase. In this phase, the organisation starts to measure and manage the business benefits of IoT use cases, apply traditional return-on-investment (ROI) criteria to further builds, and step up their management of their technology vendors. Questions arise about:

- The scalability of infrastructure and platforms as the device network grows
- The coverage the network can provide, and on what timeframe
- The security and reliability of both network and platforms, as IoT use cases become more critical to the organisation's business

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Avoiding the technology trap

The Business Integration phase is where these questions start to impact the effectiveness and affordability of the organisation's IoT strategy. Limited network coverage, difficulty in managing larger numbers of devices, and network reliability issues can make the transition from the Trial to the Business Integration phase painful and disappointing.

This means that the right network strategy must be chosen at an early stage. It is natural to test and trial more than one IoT network or platform technology – that's what tests and trials are for. But tests and trials must be accompanied by an early assessment of the strengths and weaknesses of each network technology across a range of performance criteria.

The network criteria that need to be considered early in the development of your IoT strategy include:

- Cost of operation of networks and platforms, and how those costs vary with scale
- Costs and complexity of managing a fleet of IoT devices
- Incremental costs of expanding coverage as the solution is deployed across the organisation's geographical footprint
- The security and reliability of the network and platforms, and whether these technologies can support future devices and applications critical to business operations, and to employee and public safety.

Regulation must be added to the mix in critical infrastructure industries like gas, water, and power which are subject to national security rules. For example, these rules generally require the ability to upgrade device firmware, and a network and platform capable of delivering these upgrades promptly. Some states require critical infrastructure data to be stored in Australia, which rules out service providers without a local presence. And under our privacy laws, all organisations need to ensure the security of any data that could compromise the privacy of an individual.

A network that cannot deliver these options will restrict the ability of any organisation to deploy IoT solutions efficiently and effectively over the long term. They are a 'technology trap' that can lead to costly operation and stranded assets as the organisation seeks to expand its IoT strategy to include more critical business processes. For these reasons, the organisation's executive team should be questioning the longer-term implications arising out of each of the four development phases.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Long-term requirements for IoT technology acquisition

How to choose your IoT technologies

An IoT solution is not an end in itself. Broadly, the purpose of an IoT solution is to monitor, gain insight into, and/or control business processes. Different processes occur in many different industry verticals, and they extend to the delivery and operation of consumer products as well.

To do this, an IoT system requires devices, a network, and platforms for device and data management. The choice of devices, networks and platforms is important because it determines what scalability and coverage your IoT system will have, both now and in the future.

Devices and networks are primarily hardware. Devices collect data or control actuators of some sort under instructions from the network. The network passes the data back to the platforms, and (if it is capable) may also pass data back to the device (e.g. a control instruction or a firmware upgrade). Devices and networks must be based on the same technology standard to communicate, and there are several standards in the market.

In contrast, device and data management platforms are primarily software applications "in the cloud", and normally interface to the device through the Internet Protocol (IP). Device platforms keep your devices connected, monitor their performance, reconfigure then as required, and perform maintenance like firmware upgrades. Data management platforms take the data that the devices are sending and turn it into actionable intelligence by analysing the data and generating information and insights that you can use to manage and improve business processes.

There are many criteria that are relevant to the performance of these devices, networks and platforms, but the key one is to keep your options as open as possible. This is because IoT use cases are developing fast, and in unpredictable directions. Technology choices that don't give you options constrain your future strategy. Technology choices that give you more options for new kinds of IoT solutions across your operating (or your broader business) supply chain give you more freedom to evolve your IoT strategy as new use cases emerge.

Devices are very specific to the use case you are implementing, leaving you free to choose the right device for each solution. Software like device management and data management platforms evolve from year to year and can be fairly easily upgraded or swapped. But your choice of network isn't so easy to change, because you'll have a device fleet that is designed to connect to that network. This makes it critical to get your initial choice of network right.

Choosing your LPWAN network

Choosing a network for the long-term means choosing a network that can support the solutions you want to deploy in the future. It is impossible to know exactly what solutions you will deploy and where, but there are some network features that will give you more options as your IoT strategy develops.

1. The scalability of infrastructure and platforms as the device network grows
2. The coverage the network can provide, and on what timeframe
3. The security and reliability of both network and platforms, as IoT use cases become more critical to the organisation's business
4. Two-way operation to make it easy to upgrade device firmware and control devices.
5. A clear technology roadmap and global vendor support

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Why you should consider a cellular LPWAN solution

Mobile cellular networks offer a range of IoT network and IoT platform solutions. These solutions work out of the box. They will work just as well for a small IoT test or IoT trial as for a full-blown wide area IoT commercial network.

This whitepaper focusses on the LPWAN connectivity that cellular networks provide. Cellular LPWAN networks and platforms meet all of the long-term requirements for IoT technology acquisition. They have the scalability, coverage, security and reliability to ensure that your IoT strategy can grow and evolve along with your needs and experience.

Cellular LPWAN solutions aren't the only ones in the market. There are non-cellular networks too. So it's reasonable to ask what makes cellular networks the best long-term choice for your IoT strategy.

Australia's main LPWAN technologies

There are four main technologies used for LPWAN IoT connectivity in Australia.

Figure 3: Table of LPWAN network technologies

	CELLULAR		NON-CELLULAR	
	NB-IoT	**LTE-M**	**LoRaWAN**	**Sigfox**
Coverage	around 4M sq km	almost 3M sq km	Smaller	Smaller
Spectrum	Dedicated		Shared	

Cellular mobile operators in Australia operate two main cellular LPWAN technologies. "Cellular" means that they are delivered by the same infrastructure as the mobile phone system, with one big difference – they have a much bigger range than the mobile phone range, covering around twice the area nationally. And because cellular LPWAN technologies share the same 700Mhz spectrum as the 4G mobile network, they have excellent in-building and in-ground coverage as well. Current LPWAN coverage can be viewed on the Telstra Enterprise website.

To view Telstra coverage maps visit https://www.telstra.com.au/business-enterprise/about-enterprise/our-network/iot-coverage-map

Cellular LPWAN technologies also operate on lower power, extending battery life and cutting costs.

Telstra operates two main types of cellular LPWAN network in Australia. In fact, they are the only carrier that currently operates both.

The first network is called NB-IoT. NB-IoT is specialised for low date rate applications like environmental monitoring, agricultural sensing, water and gas metering, and industrial sensors. These devices don't move around. Today, using a Category NB1 device, the maximum peak throughput in a downlink direction is ~20kbps and ~60 kbps in an uplink direction. Typical speeds are lower. NB-IoT has excellent range, and may even work a few metres underground. Battery life, with the right usage pattern, is ten years plus.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

The second IoT network is called either LTE-M (referring to the network) or CatM1 (referring to the kind of device). The LTE-M network is designed for more complex use cases like asset tracking, smart building monitoring and control, and other smart venue applications. CatM1 devices can move around and stay connected to the network. The LTE-M network also differs from NB-IoT in delivering faster data rates. CatM1 devices can even support voice communications, which NB-IoT devices cannot. They can operate in either full or half-duplex mode although Category M1 devices in market today only support half duplex.

A main competitor to cellular networks in Australia is LoRaWAN (Long Range Wide Area Network). LoRaWAN is mainly designed for the same kind of simple devices that NB-IoT is designed for. LoRaWAN providers are expanding their networks, but they do not match the coverage of cellular networks, particularly Telstra's. LoRaWAN operates at a slightly higher 900MHz frequency than NB-IoT and LTE-M, but in an unmanaged spectrum block that is shared with other technologies and service providers.

The Sigfox standard is the fourth main IoT technology. Like LoRaWAN, Sigfox is for the same kind of simple devices that NB-IoT is designed for. It operates in the same shared spectrum as LoRaWAN. It is the simplest IoT technology, and its coverage also depends on whether the Sigfox operator has built infrastructure with sufficient range to cover your area. It has some very limited capacity to downlink to devices, but it is not practical for a true two-way solution.

LoRaWAN and Sigfox are not specified by recognised global standards bodies. LoRaWAN is standardised by an industry alliance. LoRaWAN specifies Lora as one of two physical layer protocols to use for LoRaWAN.
Lora is a proprietary technology owned by Semtech. Sigfox too is a proprietary technology, owned by the company Sigfox.

LoRaWAN and Sigfox have had one big advantage over cellular NB-IoT and LTE-M up to now. They have been around several years longer. As a result, there have been more LoRaWAN and Sigfox devices available at relatively low price points. The current generation of cellular technologies were only standardised in 2016 and rolled forward into the 5G standard in 2018.

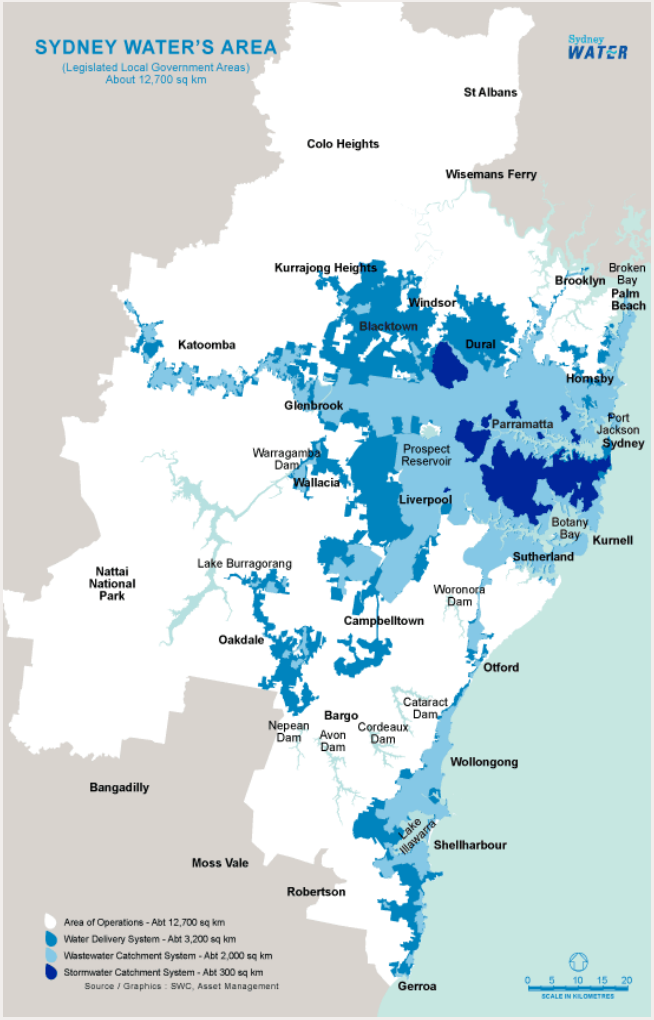
But since then, technology vendors have been making integrated circuits ("chipsets") to support these standards and the stable of cellular LPWAN devices is growing fast.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

IoT Case Study: Environmental overflow detection

Water utilities are leading users of IoT. Sydney Water Corporation provides water services to the greater Sydney area and the regional Blue Mountains, with 1000 pumping stations, 250 reservoirs, and over 40,000 kilometers of pipeline. Traditionally reliant on customer reports to detect faults, particularly sewerage overflows, it wanted to be able to find and anticipate faults instead, using IoT-enabled sensor devices.

After trialing five different network solutions, Sydney Water settled on NB-IoT as a key element of its IoT network strategy. With such a huge asset base to monitor, the scalability of NB-IoT was a decisive factor. Coverage and reliability were even better than expected. In another major plus, the network was available immediately without additional infrastructure investment. The new IoT system has already detected 23
of sewage overflow events in the first nine months (which would once have gone unnoticed for some time).



SOURCE: Sydney Water, Telstra, Venture Insights

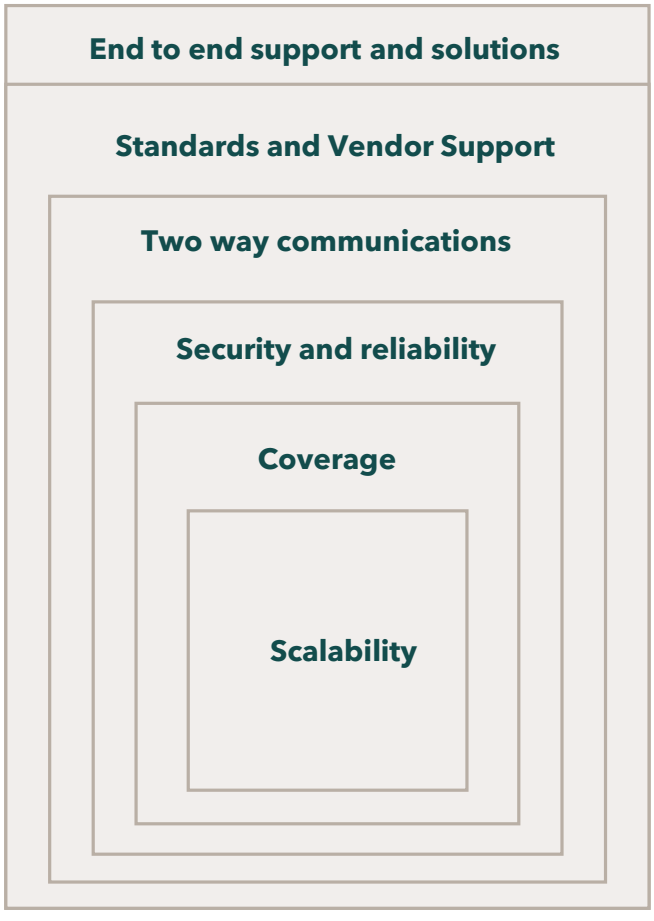
IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Summary - Benefits of cellular LPWAN

Earlier, we identified several features that IoT technologies need to have in order to prepare your organisation for a future where your IoT strategy has evolved to encompass more and more of your business processes:

1. The scalability of infrastructure and platforms as the device network grows
2. The coverage the network can provide, and in what timeframe
3. The security and reliability of both network and platforms, as IoT use cases become more critical to the organisation's business
4. Two-way operation to make it easy to upgrade device firmware and control devices.
5. A clear technology roadmap and global vendor support.

Figure 4: IoT technology features



So let's see how cellular technologies stack up against those criteria.

Scalability

Cellular LPWAN technologies are purpose-built to support very large numbers of IoT devices, in the tens of thousands on a single mobile tower. They achieve this by using dedicated spectrum without interference and by using sophisticated traffic management which is built into these technologies. Data traffic from devices is managed carefully to avoid interference and data loss. All devices and networks using NB-IoT and LTE-M/CatM1 technologies have these capabilities out of the box because they are part of the standards that define them.

In contrast, LoRaWAN and Sigfox used shared spectrum where other technologies may operate, which can cause interference problems from other users of the spectrum.

As IoT advances, literally millions of devices will be put in place in urban and regional Australia. Only cellular LPWAN technologies, specifically NB-IoT and LTE-M/Cat-M1, are specifically engineered to handle really big networks without interference. Non-cellular technologies are suitable for smaller-scale and low-density community networks, and in low risk and non-critical applications. But they can be a useful test bed to grow your knowledge about network, platform and applications. The operational data they generate can inform your development of a scaled and secure network strategy.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Coverage

Telstra's NB-IoT and LTE-M networks use exactly the same towers and antennas as standard 4G mobile services. Telstra operates more than 8,900 4G sites across Australia. But the cellular LPWAN networks have much greater range standard 4G mobile and cover over double the area of mobile coverage. Your experience of standard 4G mobile therefore isn't an indication of cellular LPWAN coverage performance. LPWAN coverage is much better.

All of this, combined with the size of Telstra's existing 4G network, makes Telstra the clear IoT coverage leader. Its NB-IoT network has the largest coverage of any IoT network in the country, reaching almost 4 million square kilometers across Australia. LTE-M coverage is somewhat less than NB-IoT, at around 3 million square kilometers.

One advantage of the Telstra network is immediately apparent. The chips that power cellular LPWAN devices on the Telstra network increasingly support both NB-IoT and LTE-M. This means that cellular LPWAN devices can leverage the best qualities of both technologies. For example, a low data rate device can normally use NB-IoT to send data, but the LTE-M network can be used to download a large firmware update to the device in a much shorter time, reducing power consumption. This flexibility is not available to LoRaWAN or Sigfox, or to Telstra's cellular competitors who don't operate both NB-IoT and LTE-M.

The second advantage is that an organisation can immediately begin to test their IoT use cases without investing in network build and monitoring. This allows the organisation to focus on the business outcomes of the trial from the start.

This cellular LPWAN network coverage extends across both regional and urban markets, providing a seamless network for both static and mobile IoT devices covering 99.5% of Australians. The extent and depth of this coverage is highlighted by the fact that most LoRaWAN networks actually use 4G networks to carry data between their base stations and their central office (adding extra complexity and technical risk in the process).

In contrast, LoRaWAN and Sigfox operators have a much smaller network of sites. In addition, they are constrained by tough radio emission standards for their 900MHz shared spectrum that limit their output power to only one watt EIRP[2]. They also operate using simpler antennas that can have less efficient output power, unlike cellular base station antennas that focus radio waves tightly in the horizontal direction to maximise range.

The result is that non-cellular networks do not match cellular LPWAN coverage and are less useful for mobile applications like logistics management and stock tracking because their coverage is patchier and less reliable.

IoT Case Study: firefighting equipment

The Regional Fire Service Foundation is using Telstra's Track and Monitor Cat-M1 Tracking Units to locate bushfire recovery support pods which are being used in bushfire remediation programs. The recovery pods have an assortment of high value equipment stored within them, and the Foundation needs to easily locate them. The pods will be deployed in regional and remote areas, which requires mobile, wide area IoT coverage to be available immediately. Telstra's CatM1 network fits the bill. The total deployment will be to 200 recovery pods.

SOURCE: Venture Insights

[1] Radiocommunications (Low Interference Potential Devices) Class Licence 2015

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Security and reliability

Telecommunications networks have always been engineered to resist disruption, and to recover as quickly as possible from 'acts of God' like bushfires and cyclones. This ranges all the way from physical security like hardened tower and exchange sites, right up to sophisticated traffic monitoring software to detect malicious attacks.

This extends to cellular LPWAN technologies like NB-IoT and LTE-M/CatM1. Further, NB-IoT networks can operate on dedicated spectrum in the so-called 'guard bands' at the edges of mobile phone spectrum blocks. This spectrum is not used by mobile phone and mobile broadband services to avoid interference with other mobile networks. However, LPWAN is low-power, so it can happily operate in these guard bands without interfering with anything else. This guarantees that cellular LPWAN networks get unimpeded access to spectrum and can't be interfered with by other technologies. This security and reliability isn't something the customer needs to configure, because it comes built-in.

LoRaWAN and Sigfox networks have security systems too, including encryption of data transmissions and other security protocols. But these technologies face another, different issue. They operate in shared spectrum in the 900MHz band, and it is difficult for them to manage interference because they are required to share the bandwidth with all comers . This is a reliability issue that is inherent to using shared spectrum. In contrast, cellular networks operate on dedicated spectrum that they fully control, so interference is not an issue for them.

Two-way communications

NB-IoT and LTE-M/CatM1 are natively two-way technologies, just like the cellular mobile technology they are associated with. This is important for a lot of applications. If you want to control a device remotely it's essential. Also, upgrading the firmware on devices over the air is much easier and cheaper than a truck roll. There are other advantages too. Suppose a daily sensor reading on a water main suggests a possible leak. It is then easy to tell the sensor device to start sending hourly updates to keep a closer eye on things.

The LoRaWAN and Sigfox standards also support two-way communications, in theory. But not every network in fact does so. Sigfox allows for only very limited downlink communications. This restricts them to simple devices that you don't need to update frequently. And when you want to update, you need a truck roll to each device, adding to the costs of operating the network.

Standards and vendor support

Finally, each kind of network needs a technology roadmap backed by a large vendor community to provide device and infrastructure support, and to develop the underlying standards to add new capabilities that meet new needs.

Cellular LPWAN technologies like NB-IoT and CatM1 are part of the same standards process that determines standards for 4G and 5G. The standards organisation responsible is the 3GPP, the biggest standards-writing organisation in the telecommunications industry.

As noted earlier, NB-IoT and CatM1 were originally created as part of the 4G standard. In 2018, they were included into the 5G standard. This means that NB-IoT and CatM1 will be around for long time. When 4G is replaced by 5G (and maybe 6G), the standards for NB-IoT and CatM1 will still be supported. Further, this means that there is an orderly process to add new capabilities to these standards that are backward compatible with older versions. This will ensure that investments in cellular LPWAN technologies and devices will never be stranded by advances in the standard.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Cellular LPWAN standards are truly open. A lot of suppliers claim to use open standards, but not all of them really do. How can you tell? A network technology is not really open unless it is supported by a recognised, open standards-making process. NB-IoT and CatM1 are true globally recognised open standards and are supported by the world's biggest telecommunications technology vendors.

Devices based on these open standards can be moved between networks. For early versions of these cellular LPWAN devices, that might require swapping a SIM card. More recent versions of cellular LPWAN devices use a software SIM (an "eSIM") which can be updated over the air. Either way, you're not locked into any single cellular provider.

Cellular LPWAN standards are supported by the world's biggest telecommunications vendors, the same ones who supply all of the world's 4G and 5G equipment. This is a powerful ecosystem of vendors, telcos and device-makers, all driving cellular IoT development for the long haul. This ecosystem is many times bigger than the ecosystem for rival networks and will deliver falling costs and greater capability over time. Cellular IoT standards are living standards, with a steady stream of upgrades to meet the evolving needs of customers.

Case study

A medical supplies company needed a solution to track expensive hospital treatment chairs valued at over $5,000 each, which are rented to hospitals, retirement villages and aged care organisations. Telstra was able to provide a mix of Bluetooth trackers (for urban areas) and CatM1 (for regional areas), providing a comprehensive solution across the entire footprint of operation. The customer has also deployed Telstra's Track and Monitor Mobile App onto their drivers' tablets so they know when the chairs are dropped off at customer sites. Full deployment will be to around 1,000 chairs over about 18 months.

SOURCE: Venture Insights

End-to-end support and solutions

It is also important to look beyond the cellular LPWAN network. Telstra plays in all of the wireless network technologies that your IoT strategy might need may need: Bluetooth, Wi-Fi, cellular LPWAN and satellite. By giving you managed access across all of these technologies, Telstra can cover any network scenario you might encounter.

Beyond these connectivity technologies, an IoT system is more than the network. It requires devices and platforms to collect, manage and analyse data to generate the insights that inform and control business processes.

Telstra's cellular LPWAN networks will interface natively with any IP-based platform, so the customer can choose whether to use a Telstra device management or data management platform or a platform from someone else. But there are good reasons to choose Telstra as a platform partner.

First, a long-term investment in IoT requires a technology partner that will be around for the long haul. Telstra has been delivering networks and solutions to Australian customers for over a century, longer than any other technology company still in the market. You can count of Telstra being around.

Second, Telstra can help you design, test and trial secure and reliable IoT solutions that scale and have instant wide area coverage, giving you plenty of room to grow and evolve your IoT strategy. With a workforce of over 20,000 technology and business experts, Telstra can provide end-to-end professional support and ensure that you get the most out of your IoT strategy.

Finally, Telstra has the related technologies to support your journey. Apart from its superior network, Telstra's connection, device and application management platforms are available to deliver a full end-to-end solution for your IoT use cases.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

Conclusion

Your IoT strategy is a long-term investment. It makes sense to get it right from the outset.

Whatever phase you have reached in your IoT journey, decisions you are taking now will affect your ability to evolve and develop your IoT strategy in the future.

This means that you should choose your LPWAN technology with the future in mind. The test and trial phases of your IoT strategy should include careful consideration of your potential long-term needs and your technology choices should ensure you retain the flexibility for your IoT strategy to evolve and develop. Choose an LPWAN technology that :

1. Is scalable
2. Has extensive coverage
3. Is secure and reliable
4. Supports two-way connectivity
5. Has long-term vendor and standards support.

These network criteria can be applied to any LPWAN network. However, cellular LPWAN networks perform strongly against all of the criteria, and should be contenders for any IoT strategy, particularly in Australia where coverage is such a crucial differentiator.

IMPORTANT DISCLOSURES ARE PROVIDED AT THE END OF THIS REPORT
© 2020 Venture Insights Pty Ltd. All rights reserved

About Venture Insights

Venture Insights provides a subscription research service covering the media, digital and telecommunications industries in Australia, NZ and Europe, with a special focus on new disruptive technologies.

For more information go to www.ventureinsights.com.au or contact us at info@ventureinsights.com.au

This whitepaper has been developed for Telstra and included a range of interviews with independent industry IoT professionals, Telstra's broad IoT management team and Venture's own insights into the IoT marketplace.

Important notice: By accepting this research note, the recipient agrees to be bound by the following terms of use. This research note has been prepared by Venture Insights Pty Ltd and published solely for guidance and general informational purposes to authorised users under the terms of a licence agreement between Venture Insights Pty Ltd and its subscriber. You need to be expressly authorised to use it, and it may only be used for your internal business purposes and no part of this note may be reproduced or distributed in any manner including, but not limited to, via the internet, without the prior permission of Venture Insights Pty Ltd. If you have not received this note directly from Venture Insights Pty Ltd, your receipt is unauthorised. If so, or you have any doubt as to your authority to use it, please return this note to Venture Insights immediately.

This research note may contain the personal opinions of research analysts based on research undertaken. This note has no regard to any specific recipient, including but not limited to any specific investment objectives, and should not be relied on by any recipient for investment or any other purposes. Venture Insights Pty Ltd gives no undertaking to provide the recipient with access to any additional information or to update or keep current any information or opinions contained herein. The information and any opinions contained herein are based on sources believed to be reliable but the information relied on has not been independently verified. Neither Venture Insights Pty Ltd nor its officers, employees and agents make any warranties or representations, express or implied, as to the accuracy or completeness of information and opinions contained herein and exclude all liability to the fullest extent permitted by law for any direct or indirect loss or damage or any other costs or expenses of any kind which may arise directly or indirectly out of the use of this note, including but not limited to anything caused by any viruses or any failures in computer transmission.

Any trade marks, copyright works, logos or devices used in this report are the property of their respective owners and are used for illustrative purposes only. Unless otherwise disclosed, Venture Insights has no affiliation or connection with any organisations mentioned in this report. However, the information contained in this report has been obtained from a variety of sources, including in some cases the organisations themselves. In addition, organisations mentioned in this report may be clients of Venture Insights.

The recipient hereby indemnifies Venture Insights Pty Ltd and its officers, employees and agents and their related entities against any direct or indirect loss or damage or any other costs or expenses of any kind which they may incur directly or indirectly as a result of the recipient's use of this note.

© 2020 Venture Insights Pty Ltd. All rights reserved

DAVID KENNEDY
david.kennedy@ventureinsights.com.au

NIGEL PUGH
nigel.pugh@ventureinsights.com.au

Level 8
333 George Street
Sydney, NSW 2000

Level 6
90 Collins Street
Melbourne, VIC 3000

www.ventureinsights.com.au