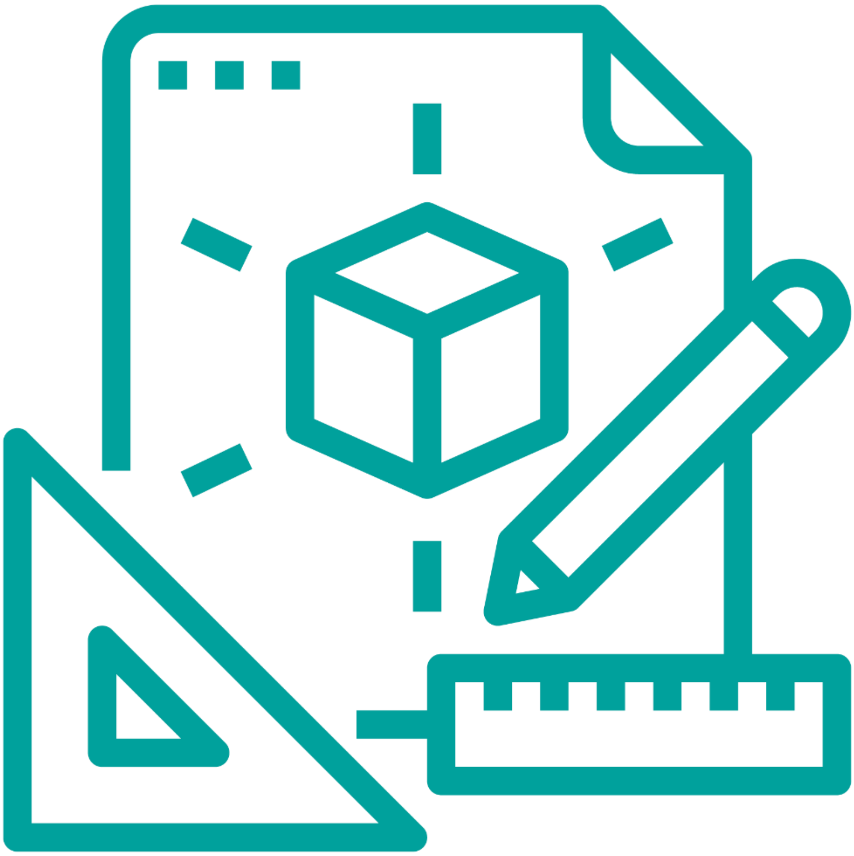
OPENAIR

Operational Network of
Air quality Impact Resources

Best Practice Guide

BP204 | Develop

Data communications procurement



Introduction

Until recently, air quality sensing tools accessible to local governments, researchers, and the wider community were fairly basic. They did not provide real-time data connectivity or include low-cost portable sensors. They used only fixed data loggers (which need data to be manually extracted, a time-consuming process). They often depended on entirely analogue (rather than digital) sensors, such as gas diffusion tubes that changed colour over a period of months when exposed to pollution.

Things changed dramatically with the arrival of the Internet of Things (IoT) and smart cities technologies over the last decade or so. We now have combinations of relatively low-cost technologies that support the direct connection of small sensing devices with data users. Devices can remain actively deployed and produce data across their entire operational lifetimes. This has fundamentally altered how environmental sensing is done, and who can do it.

We can now:

- receive, capture, store, and respond to near real-time data
- deploy distributed telecommunications networks and easily retrieve data from all devices simultaneously
- analyse data and gain real insights to support informed decision-making.

There are currently many options to choose from when considering data communications technologies in support of low-cost sensing.

This resource is intended to help you understand these options, and identify those that are most suitable to your project. Each of the technologies described in this document has strengths and weaknesses, and knowing which option can best meet your needs will depend on your project context and aims.

Who is this resource for?

While this document contains some technical information, it is intended for general use by all parties involved in an air quality sensing project, including:

- smart city project leads
- smart city teams
- procurement teams
- planners
- local government executives
- IT staff
- data custodians
- analysts
- project partners.

How to use this resource

This document is a practical guide to help you understand some of the factors involved in choosing suitable technologies to connect internet connected environmental monitoring systems.

It will give you an overview of some of the technical issues you need to consider when embarking on an air quality sensing project. This guide may also help you make choices that serve purposes well beyond the scope of your project, since telecommunications are a fundamental building block of any smart city initiative.

Figure 1 depicts a basic sensor network, showing environmental sensors connected to gateways via wireless communication. Data from the sensors is then transported to the network or cloud, where it is stored, analysed, and made available to users.

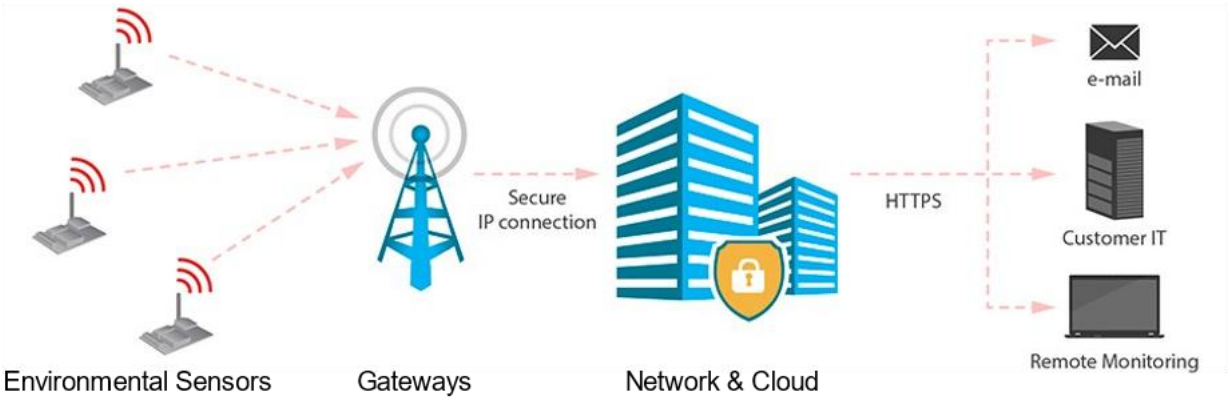


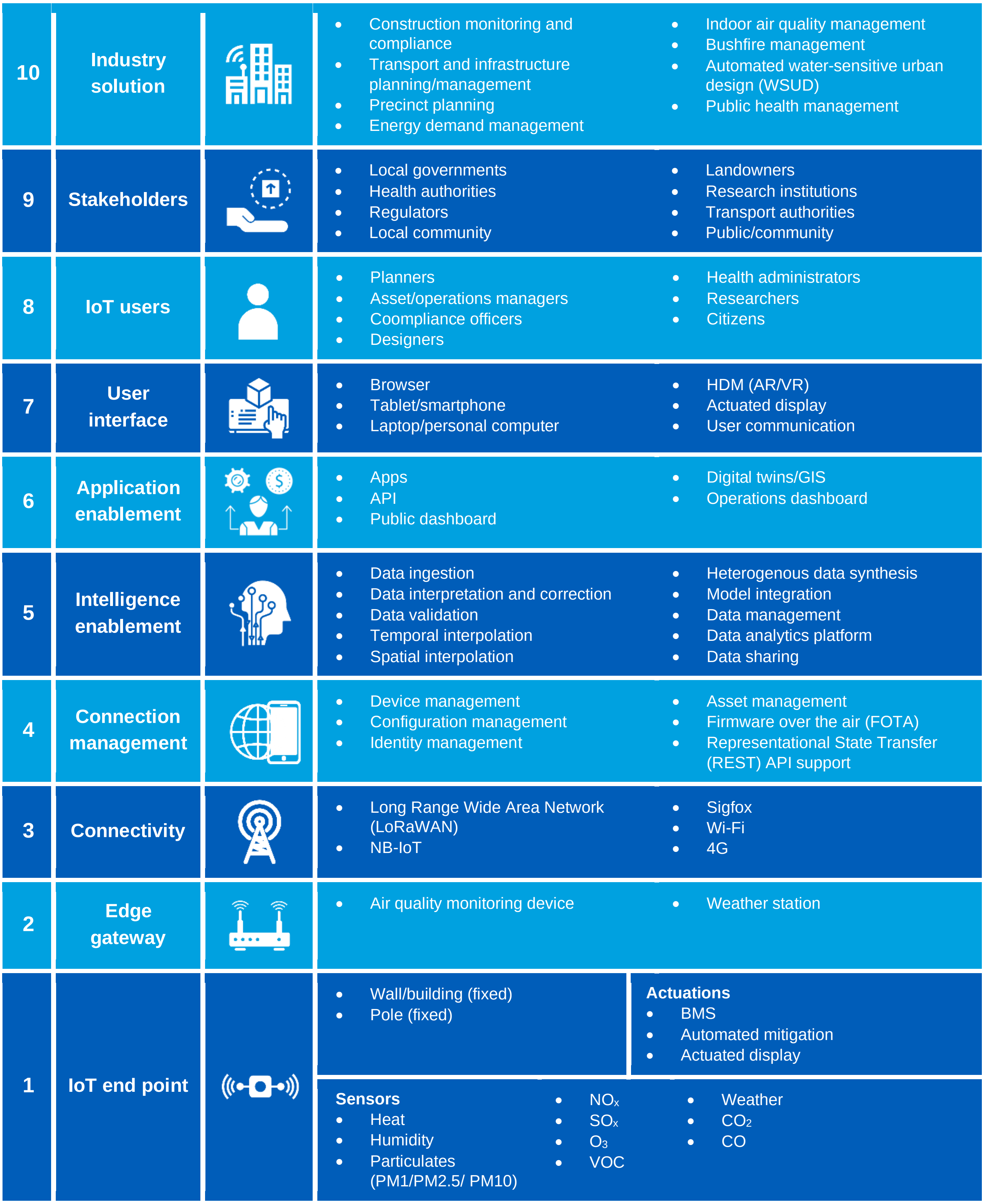
Figure 1. Basic sensor network. Figure source: (Stoces et al., 2016)

In any remote-sensing project, there are two factors to consider in terms of ‘connectivity’:

- the connection between the sensor and the internet
- the connection between the user and the internet.

These two types of connection involve very different sets of requirements and considerations. To create and deliver a successful project, however, *both* types must be addressed. This guide will focus mostly on **sensor device connectivity** (with some brief notes about user connectivity at the end).

Figure 2 illustrates where these two different connectivity types (and needs) are situated within the wider telecommunications framework. This figure depicts the IoT Alliance Australia (IoTAA)’s reference architecture for all IoT projects, and shows the end-to-end architecture as well as the telecommunications context. (IoTAA, n.d.)



10	Industry solution		• Construction monitoring and compliance • Transport and infrastructure planning/management • Precinct planning • Energy demand management	• Indoor air quality management • Bushfire management • Automated water-sensitive urban design (WSUD) • Public health management
9	Stakeholders		• Local governments • Health authorities • Regulators • Local community	• Landowners • Research institutions • Transport authorities • Public/community
8	IoT users		• Planners • Asset/operations managers • Coompliance officers • Designers	• Health administrators • Researchers • Citizens
7	User interface		• Browser • Tablet/smartphone • Laptop/personal computer	• HDM (AR/VR) • Actuated display • User communication
6	Application enablement		• Apps • API • Public dashboard	• Digital twins/GIS • Operations dashboard
5	Intelligence enablement		• Data ingestion • Data interpretation and correction • Data validation • Temporal interpolation • Spatial interpolation	• Heterogenous data synthesis • Model integration • Data management • Data analytics platform • Data sharing
4	Connection management		• Device management • Configuration management • Identity management	• Asset management • Firmware over the air (FOTA) • Representational State Transfer (REST) API support
3	Connectivity		• Long Range Wide Area Network (LoRaWAN) • NB-IoT	• Sigfox • Wi-Fi • 4G
2	Edge gateway		• Air quality monitoring device	• Weather station
1	IoT end point		• Wall/building (fixed) • Pole (fixed) **Sensors** • Heat • Humidity • Particulates (PM1/PM2.5/ PM10) • NO_x • SO_x • O_3 • VOC	**Actuations** • BMS • Automated mitigation • Actuated display • Weather • CO_2 • CO

Figure 1. Full reference architecture for low-cost air quality monitoring (adapted from IoTAA, 2022)

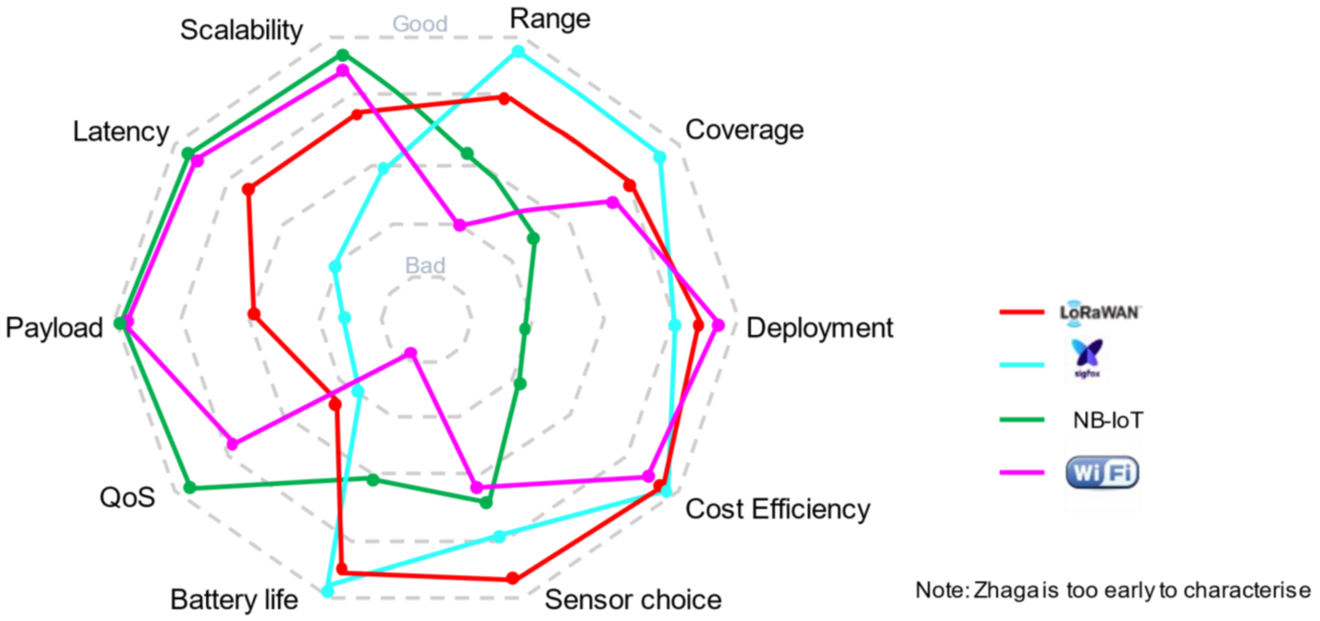
Sensor device connectivity

Sensors can be placed in a wide range of settings, from comfortable, well-connected local government office buildings to remote field locations in harsh environments. Given this wide range of possible locations, connectivity needs will vary significantly.

For an urban building, connectivity may simply involve an ethernet connection or wireless internet connection (using Wi-Fi or Bluetooth). In public spaces, suburbs, and more remote locations, 'wide-area' wireless options are typically needed (which include LoRaWAN, Sigfox, Wi-Fi, mobile phone technology, or NB-IoT). Each of these options should be considered on a case-by-case basis.

Technical considerations

Figure 3 maps the top ten factors to be considered in terms of sensor device connectivity (and Table 1 describes these ten factors in more detail). This 'spider diagram' shows the relative strengths and weaknesses of the four main wireless technology options (LoRaWAN, Sigfox, NB-IoT, and Wi-Fi). There are other emerging technologies now available (such as Zhaga), but scale, maturity, availability, and pricing make these four the most likely (and feasible) choices in the current market.



Note: Zhaga is too early to characterise

Figure 3. Spider diagram comparing four wireless network technologies (LoRaWAN, Sigfox, NB-IoT, and Wi-Fi)

Table 1. Top ten telecommunications factors to consider

Factor	Description
Range	Given that each of these technologies is a form of radio communication, 'range' describes the maximum distance the signals can travel between the sensor and the network antenna. This is a variable distance that depends on many factors, including the antenna location, sensor location, and urban and rural terrain.
Coverage	Coverage is a measure of how widely deployed a technology is (or, if you are building your own network, how easy it is to cover the required area). If you are planning to use a particular telecommunications company's mobile phone network (e.g. NB-IoT), then you need to know whether NB-IoT is available in the sensor deployment area. If there is no network coverage where you need it, you will have to choose an alternative option, such as LoRaWAN.
Deployment	This term refers to the relative ease (or difficulty) of using and deploying sensors and other network equipment to support your project, if relevant.
Cost efficiency	Cost efficiency is a metric to measure and compare all the costs associated with procuring and operating an end-to-end service, based on the chosen telecommunications solution.
Sensor choices	This refers to the number – and range – of sensors available in the market that are designed to connect to the wireless technology you select for your project.
Battery life	Most air quality sensors are deployed in the field, which means that using mains power is usually not practical or feasible. For this reason, most sensors run on batteries. Battery life refers to how long the battery will last under normal operating conditions.
Quality of service (QoS)	QoS is a metric to measure how available the network is, calculated according to the percentage of total time that the end-to-end service functions as intended. If the service is not operational for one day out of ten, this would be described as a QoS of 90%. Typically, telecommunications networks have a QoS of between 99% and 99.999%. This may seem like a very small difference, but it is actually the difference between *days* of outage per year versus *seconds* of outage per year.
Payload	Payload is the amount of data that can be carried between the sensor and the data storage location. Typically, the bottleneck for data flow is the communications link between the sensor and the network, so from a telecommunications network perspective, this is a vital parameter. Note that although sensor telemetry data involves small payloads, remote sensor management and software updates require significantly higher payloads.
Latency	Latency is the time it takes for any action to cause a reaction. For example, if a sensor is requested to send data, latency is how long it takes the sensor to respond to that request and start sending the data. Generally, lower latencies are more desirable.

Factor	Description
	Environmental data, in general, does not require low latency. If sensor data takes a minute instead of a second to be transmitted, this will typically have minimal or no impact on the usefulness of the data.
Scalability	Scalability is a measure of how large a sensor network can practically become before it stops working efficiently. Some technologies can support millions of sensors, while others can support only tens or hundreds. It is important to make sure your chosen technology can support the maximum projected number of sensors for the life of the project.

Beyond these top ten factors, there are several others to consider in making a well-informed decision about sensor connectivity to meet your specific user requirements. These include:

1. **Access to locations** (e.g. street level, inside commercial premises, or upper levels of buildings). The chosen locations for sensors are very important for the environmental measurements you want to make. They are also important from an operational perspective. You need to know if and how you can access the sensor locations, if necessary. Consider security access keys or alarm codes, available access hours, and anything else that may hinder your access to the sensors.
2. **Capacity** (e.g. number of end points, clustering of access points for backhaul aggregation). The number of sensors to be deployed plays a big role in deciding how best to design a telecommunications solution. If sensor numbers are small (less than a hundred), you may choose to manage the sensors using internal resources. If larger sensor numbers are anticipated, an outsourcing management model is likely to be more attractive. The software tools used will also differ for small and large deployments. Scaling up to larger deployments can be costly and complex. For local government sensor networks for environmental monitoring, sensor numbers are typically small.
3. **City site access** (e.g. buildings, poles, bus shelters). Sites must be chosen with a consideration of power supply needs, radio signal strength, physical security to minimise accidental or malicious damage, and creating minimum visual impacts that affect community amenities.
4. **Planning for peak usage periods** (e.g. bandwidth, number of access requests during busy times). When defining the telecommunications needs for your project, it is vital to consider performance during peak usage periods particularly if the data communications system is carrying data for several applications and systems.
5. **Backhaul capacity and performance** (e.g. fibre and mobile strategy). Wireless communications base stations usually are connected to the internet via fixed communications types such as fibre optic cables. This is known as “backhaul”. Backhaul capacity is a key consideration. Information from sensors is often stored in the cloud, which uses network capacity and affects performance. It is important to understand these traffic loads, and ensure that the communications backhauls have sufficient capacity to meet the needs of both sensors and users.

6. **Power supply strategy** (e.g. efficiency and availability). Most smart low-cost sensors are battery-powered. The battery life is determined by the way you configure and use the sensors. For example, if you ask a sensor to report every 10 seconds, the battery life will be much shorter than if it is reporting every hour. The amount of information reported will also affect battery life, so it is likely that a trade-off will be needed between battery life and information demands. If sensors are mains-powered, consider if the available mains power is reliable enough for your needs.
7. **Regulatory requirements and obligations** (e.g. relevant telecommunications law and regulations). If you build and operate your own sensor network, it may seem attractive to provide access to other users (outside your organisation) to help pay for the cost of this infrastructure. The Australian Government's *Telecommunications (Interception and Access) Act (1979)* has very strict rules and obligations that may apply in this situation, and it is important to understand these prior to offering services to external clients. *("Telecommunications (Interception and Access) Act (1979) ", 1979)*
8. **Management and operations**, including:
    - network operations centre
    - IP address management
    - performance monitoring
    - policy and fair use enforcement
    - content filtering (if any)
    - software updates and patching
    - fault reporting and resolution
    - spare parts reserves
    - preventative maintenance, such as battery replacement
    - intrusion prevention and security
    - change management.

Wi-Fi

Many of the readily available low-cost air quality sensing devices use Wi-Fi. Wi-Fi networks are commonly installed in public and corporate buildings. Public Wi-Fi networks are also quite common in town/city centres, often provided by the city itself, or by telecommunications service providers. The key features of Wi-Fi are described in Table 2.

Wi-Fi has some drawbacks, however. Using Wi-Fi significantly constrains options for device deployment (since you are restricted to locations with reliable and strong Wi-Fi signal), and generally requires access to a mains power supply (since Wi-Fi has a high-power demand that generally rules out batteries and solar power). There are exceptions to this, and solar/battery/cellular modem kits are available for some sensor types to eliminate the need for mains power and a Wi-Fi network.

Table 2. Key features of Wi-Fi

Issue	Description
Range	Wi-Fi range is typically limited to less than 100 metres, and is useful either within an office building, or – when outdoors – close to a Wi-Fi hotspot. Note that the range is affected by which version of Wi-Fi you use. Wi-Fi operates in several different radio frequencies; the lower the frequency, the wider the range.
Coverage	Wi-Fi coverage within a corporate building is usually very good. Coverage of public Wi-Fi is very patchy. Care must be taken when considering the use of Wi-Fi, as network coverage may vary depending on network usage and weather conditions. Deploying sensors as close as possible to a hotspot is recommended.
Deployment	Wi-Fi-connected sensors are easy to deploy, and special technical skills are not required.
Cost efficiency	Wi-Fi is very cost-effective.
Sensor choices	There are several environmental sensors available that support a Wi-Fi interface. They do not all support the different operating frequencies of Wi-Fi, so make sure to choose compatible ones.
Battery life	Wi-Fi consumes considerable power, and is therefore not usually battery-operated. Mains power is generally required for Wi-Fi-connected devices. This means that Wi-Fi is not the best option for very remote sensors.
Quality of service (QoS)	QoS depends on many end-to-end delivery and use factors, and not just on the sensor connection. Wi-Fi networks are typically quite suitable for this kind of sensing project. QoS may not be guaranteed, but short outages can probably be tolerated without major project implications.
Payload	Wi-Fi offers a very large payload for data transfer, well beyond the needs of environmental sensing.
Latency	Because Wi-Fi devices are typically mains-powered, power consumption is not limited, thus latency is very low.
Scalability	Although Wi-Fi does have limitations in terms of the number of devices that can be connected, this device limit is well beyond the needs of most environmental sensing projects.

Table 3 summarises some of the distinctive *applied* features of Wi-Fi, in terms of device location, cost models, community participation, and functional constraints. All of these factors should be considered when selecting a telecommunications network for your air quality sensing project.

Table 3. Some applied features of Wi-Fi

Feature	Description of application
Device location	In general, use of Wi-Fi requires devices to be deployed on properties with reliable Wi-Fi connections (e.g. local government-owned buildings). Local government-managed public Wi-Fi may expand your options.
Cost and pricing model	For local government-supported projects, Wi-Fi will essentially be free (since the project can use existing Wi-Fi networks).
Community participation	Wi-Fi can be a good option to support community-hosted devices. However, you should consider the practicalities and ethics of relying on private internet connections to run your project. Note that lower socio-economic groups may have difficulty maintaining continuous connectivity throughout the life of your project, and this may disrupt data collection. For this reason, local government-run public Wi-Fi may be a better solution.
Device functionality constraints	Mains power is required (due to the high-power demand of Wi-Fi). Wi-Fi supports high bandwidth data transfer. This means it will support high reporting rates (e.g. every 30 seconds), as well as more sophisticated 'edge computing' associated with high-performance device options (generally outside the 'low-cost' definition). Most non-technical use cases will not require these functions.

What is LPWAN?

LPWAN stands for 'low-power wide-area network'. This type of wireless network is specifically designed to support long-range, low-data transfers (between a device and a gateway) that require very little battery power consumption. Other wireless technologies, such as Wi-Fi and the mobile phone network, are *not* low-power networks. LPWAN is an umbrella term that describes characteristics of LoRaWAN, Sigfox, NB-IoT, LTE-M, and other wireless networks.

LoRaWAN

LoRa – the 'long-range, low-power' Internet of Things (IoT) platform – was invented a decade ago, and is now implemented in well over 100 million devices worldwide, accelerating the global adoption of IoT.

LoRa is a wireless technology, just like the more commonly used Wi-Fi, Bluetooth, or LTE. As is the case with any technology, there are advantages and disadvantages to LoRa. It enables low-cost, battery-powered devices to send data over long distances. However, for sending data with higher bandwidths, LoRa is not a suitable option.

LoRaWAN builds on LorRa by defining a standard protocol for a higher-capacity, long-range, low-power IoT network of LoRa nodes. It takes advantage of LoRa strengths, and optimises battery life and quality of service for LoRa nodes. The protocol is fully bi-directional, which allows for reliable message delivery (called 'confirmations'). It includes definition of end-to-end encryption for security and data privacy, over-the-air registration of end nodes, and multicast capability. This approach ensures interoperability of the various LoRaWAN networks and devices.

See Table 4 for an overview of LoRaWAN's key features.

Table 4. Key features of LoRaWAN

Feature	Description
Range	LoRaWAN range is highly dependent on context and environment (its range is 5km in urban areas, but in rural settings it can achieve a 15km line-of-sight range). There is a special long-range version of the transmitter that – under ideal conditions – can extend the urban range to hundreds of kilometres.
Coverage	LoRaWAN coverage depends on the way the service is provided. If a local government area (LGA) deploys its own gateways, then coverage is defined by the LGA's gateway locations (and depends on what the LGA chooses to deploy). If you purchase a service rather than gateway equipment, then the service provider will provide the necessary coverage for your needs. In either case, achieving suitable coverage is relatively simple and low-cost.
Deployment	LoRaWAN-connected sensors are easy to deploy, and only limited special technical skills are required.
Cost efficiency	LoRaWAN is very cost-effective. There are a range of pricing options available, from pay-per-device-connected to pay-for-data (on a very limited basis, some services are initially no-cost).
Sensor choices	There are many environmental sensors available that support a LoRaWAN interface. In the low-cost sensor market, a LoRaWAN interface is the most common choice for sensor manufacturers.
Battery life	LoRaWAN is specifically designed to support long battery life. Under ideal circumstances, the battery life can be up to 10 years. In reality, most batteries will probably last about 5 years.
Quality of service (QoS)	QoS depends on many end-to-end factors, not just on the sensor connection. LoRaWAN networks are typically quite suitable for environmental sensing projects. QoS may not be guaranteed, but short outages can probably be tolerated without major project implications. Some service providers do offer a defined QoS (but keep in mind that this will cost more).
Payload	LoRaWAN offers a payload ideally suited to transferring environmental sensor data. The amount of data sent – and the regularity of data transfer – will affect battery life. In other words, the more often you send data, the shorter the battery life.
Latency	As LoRaWAN is optimised for long battery life, latency is sacrificed. Latency is higher than it would be using Wi-Fi, for instance.
Scalability	Although LoRaWAN does have limitations on the number of devices connected, this device limit is well beyond the needs of most environmental sensing projects. Thousands of sensors can be connected without significant performance reduction.

The are two main approaches to choosing LoRaWAN networks - “open” (via The “Things Network” or privately operated by a telecommunications provider. Some of the relevant considerations for these options are described in Table 5.

Table 5. Description of LoRaWAN options: open (via The Things Network), or private/proprietary

LoRaWAN option	Cost and pricing model	Community participation	System Performance
Open LoRaWAN - The Things Network	There is an upfront cost for gateways and their installation, plus recurring operations costs payable to a service provider. There are no ‘per device’ costs. As such, most costs are ‘capex’ (capital expenditure), with set/predicable ‘opex’ (operational expenditure). Cost-effectiveness is reliant upon a critical mass of devices (a minimum of about 20).	Excellent for community participation. The Things Network (TTN) is an open-access global grassroots community that has been developed specifically to empower community engagement with IoT. Anyone can create a TTN account and start adding and managing their own devices.	Signal is often attenuated by poor weather, and periodic device dropouts are not uncommon. However, being open access, other gateways in the vicinity (owned by other people) provide backup connectivity, and help to reduce the risk of dropouts for any given device. LoRaWAN (of any variety) allows for two-way communications with complex functionality.
Private or proprietary LoRaWAN	A per-device subscription model that tends to replace gateway procurement and operation charges. Commercial packages vary. Your upfront ‘capex’ may be lower, but ongoing operational costs for proprietary LoRaWAN may increase as you expand service use.	Not conducive to community participation. The 'per device’ connection fee is a barrier to DIY community involvement. Furthermore, access to the services is not generally designed for open public access.	The onus is on the provider to ensure the LoRaWAN network meets performance expectations. These can be specified in a procurement agreement.

NB-IoT

Narrowband Internet of Things (NB-IoT) is a mobile communications standard that is already widespread, and is available in Australia from the major telecommunications companies. NB-IoT is an extension of the 'long-term evolution' (or LTE) cellular communication standard, and uses existing mobile communications infrastructure (i.e. antenna locations and mobile phone infrastructure), as well as previously unused frequency bands. This is what makes this offering so efficient for wireless carriers, resulting in relatively low prices for users.

Unlike 5G or LTE, NB-IoT (with its low bandwidth) is specifically designed for low data volumes, such as two-way transmissions of telemetry data and control information by environmental sensors. In addition, NB-IoT offers optimised, low-energy consumption and – by operating at low frequencies – excellent building penetration. NB-IoT thus paves the way for applications where IoT deployment previously failed due to a lack of economic viability or technical challenges.

Unlike LoRaWAN, NB-IoT is a licensed mobile standard, featuring all of the security and privacy features of mobile networks (including data integrity, confidentiality, and secure authentication). Moreover, with NB-IoT, the provider is able to guarantee reliable transmission quality. Refer to Table 6 for the key features of NB-IoT.

Table 6. Key features of NB-IoT

Feature	Description
Range	NB-IoT range is approximately the same as mobile phone range (i.e. several kilometres from mobile phone towers).
Coverage	NB-IoT is a service offered by the major telecommunications companies in Australia. It is built upon existing mobile phone infrastructure, so there is coverage across almost all of Australia.
Deployment	If sensors are compatible with the company's service offering, deployment is simple. A SIM card is required, and the process is similar to registering a mobile phone with a service provider. This service makes it very easy to support a single sensor – or a small number of sensors – with low upfront costs.
Cost efficiency	NB-IoT is a relatively low-cost option for connectivity, but it is likely to be more costly than LoRaWAN or Wi-Fi.
Sensor choices	There are several environmental sensors available that support a NB-IoT interface. The service provider will need to approve any environmental sensor connected to their network, and confirm that the device is supported.
Battery life	Through careful device configuration, battery life can be up to ten years, but in practice it is more likely to be five years.
Quality of service (QoS)	QoS depends on many end-to-end factors, not just on the sensor connection. The connectivity service offered by operators (such as Telstra, Optus, or Vodafone/TPG) includes some QoS service guarantees, and this is currently similar to mobile phone performance.
Payload	NB-IoT offers a payload ideally suited to transferring environmental sensor data. The amount of data sent – and the regularity of data transfers – will affect battery life (the more often you send data, the shorter the battery life). Some service providers may charge based on data transferred, and not just for device connectivity.
Latency	As NB-IoT is optimised for long battery life, latency is sacrificed. A slightly higher latency should be expected than with Wi-Fi, for instance.
Scalability	The NB-IoT technology is designed to support very high numbers of connected sensors. Thousands of sensors can be handled without significant performance reduction.

Table7 summarises some of the distinctive *applied* features of NB-IoT.

Table 7. Some applied features of NB-IoT

Feature	Description
Device location	Highest flexibility in terms of location, since the signal is carried through existing cellular infrastructure. Good option for covering large areas, such as distributing a smaller number of devices across a whole local government area.
Cost and pricing model	A 'per device' fixed recurring fee is calculated according to data use. No investment required in additional infrastructure (e.g. gateways).
Community participation	Not conducive to DIY participation because of the fees associated with connection. However, due to widespread and reliable coverage, it can be a good option where a community stakeholder is hosting a device, and local government retains management responsibility.
Device functionality constraints	NB-IoT will have a useful life of about 10 years. Currently, the services offered by the major telecommunications companies can be expensive per device, but prices will likely drop over time. Negotiation may be possible if there is a promise of future service usage growth.

Sigfox

Sigfox was the first service provider to use LPWAN techniques to connect devices – such as sensors – to the internet. Sigfox technology wirelessly connects battery-operated devices and sensors to the internet in a range of regional, national, and global communication networks, and is widely used in Australia.

Sigfox was created in 2010, with the goal of connecting objects in the physical world to the digital world. Sigfox offers end-to-end, one-way-only connectivity, sending small data packets (100 bits per second) from sensors – via the Sigfox network and the cloud – to digital third-party sites and applications. Refer to Table 9 for a summary of the key features of Sigfox.

Table 9. Key features of Sigfox

Feature	Description
Range	Sigfox range depends heavily on the environment: about 5km to 10km in urban areas, and about 40km line-of-sight in rural settings.
Coverage	Sigfox coverage is very good. The Sigfox service provider in Australia has already deployed a significant number of base stations, so coverage in most populated areas is decent.
Deployment	Sigfox-connected sensors are easy to deploy, and only limited special technical skills are required.
Cost efficiency	Sigfox is very cost-effective. The service model is a pay-per-connected-device model.
Sensor choices	There are some environmental sensors available that support a Sigfox service. As the service only offers one-way communication, not all sensors can be supported. It is important to check very carefully that Sigfox can provide the service you need for the chosen sensors.
Battery life	Sigfox is specifically designed to support long battery life. Under ideal circumstances, the battery life can be up to 10 years, but in reality, batteries will probably last about 5 years.
Quality of service (QoS)	QoS depends on many end-to-end factors, not just on the sensor connection. Sigfox does not offer QoS guarantees. With only one-way communication, it is not possible to send an enquiry to a sensor to check its status, so the condition of the sensors may not be well understood at any given moment.
Payload	Sigfox offers a payload ideally suited to transferring environmental sensor data. The amount of data sent – and the regularity of data transfers – will affect battery life (the more often you send data, the shorter the battery life). Keep in mind that Sigfox only supports one-way communication.
Latency	As Sigfox is optimised for long battery life, latency is sacrificed – so a high latency should be expected.
Scalability	Sigfox supports many thousands of sensors without significant performance reduction.

Table 10 summarises some of the distinctive *applied* features of Sigfox, in terms of device location, cost models, community participation, and functional constraints.

Table 10. Some applied features of Sigfox

Feature	Description
Device location	Coverage up to about a 20km radius from a gateway (this depends on the topology and built environment). This option tends to be best for a region that can be serviced by existing Sigfox service.
Cost and pricing model	A per-device subscription model. Your upfront 'capex' may be lower, but ongoing operational costs may increase as you expand service use.
Community participation	The 'per device' connection fee is a barrier to DIY community involvement. Furthermore, access to the services is not generally designed for open public access.
Device functionality constraints	Signal is often attenuated by poor weather, and periodic device dropouts are not uncommon. Sigfox has very limited bandwidth, and only allows one-way communications. It is not possible to control devices via the radio interface.

USER CONNECTIVITY

Users of environmental sensors – and the data they produce – can be based in the office, in the field, at home, or anywhere in between. How users access the information generated by your air quality sensor network will vary significantly. In the office, using a desktop or laptop computer would be typical, and these computers tend to be ethernet- or Wi-Fi-connected, leveraging existing corporate IT infrastructure. As long as that IT infrastructure has adequate capacity and stability, the user can reasonably expect to get very good performance – even with rich, high-resolution graphical representations of data. This sets the standard for users' expectations.

When using a mobile device (such as a smartphone or tablet) outside the office, achieving a similarly high performance requires a very good mobile network connection. Sufficient bandwidth is crucial to be able to download allocated data. When developing any user interface applications, care must be taken that mobile network performance will be adequate to meet user needs. For this reason, it is likely that a premium 4G (or even 5G) service would be needed, as well as devices that support these services.

What is Zhaga?

There is an emerging sensor connectivity standard being developed by a global group of companies in the lighting industry who call themselves the Zhaga Consortium.

This consortium has standardised components of LED luminaires to help bring IoT to outdoor lighting fixtures. See Figure 4.

The specification they have developed, known as **Zhaga Book 18**, makes it easy to upgrade LED fixtures by adding or changing 24V modules that provide sensing and communication capabilities.

Some sensors are becoming available that support this connectivity, but it is most likely too early to leverage this standard for local government environmental monitoring projects.

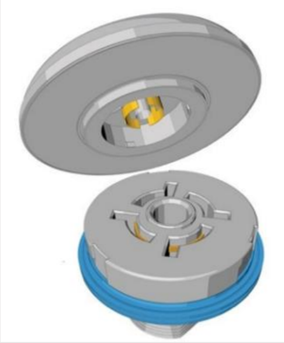


Figure 4. Zhaga modular lighting module and interface. Figure source: (Zhaga, n.d.)

References

IoTAA. (n.d.). *IoT Alliance Australia*. https://iot.org.au/

Stoces, M., Vanek, J., Masner, J., & Pavlík, J. (2016). Internet of Things (IoT) in Agriculture - Selected Aspects. *AGRIS On-line Papers in Economics and Informatics*, *8*(1), 83-88. https://doi.org/https://doi.org/10.7160/aol.2016.080108

Telecommunications (Interception and Access) Act (1979) (1979). https://www.legislation.gov.au/Details/C2017C00192

Zhaga. (n.d.). https://www.zhagastandard.org/

Further information

For more information about this project, please contact:

Peter Runcie

Project Lead, NSW Smart Sensing Network (NSSN)
Email: peter@natirar.com.au

This Best Practice Guide section is part of a suite of resources designed to support local government action on air quality through the use of smart low-cost sensing technologies. It is the first Australian project of its kind. Visit www.openair.org.au for more information.

OPENAIR is made possible by the NSW Government's Smart Places Acceleration Program.

Document No: 202301108 BP204 Data communications procurement Version 1 Final