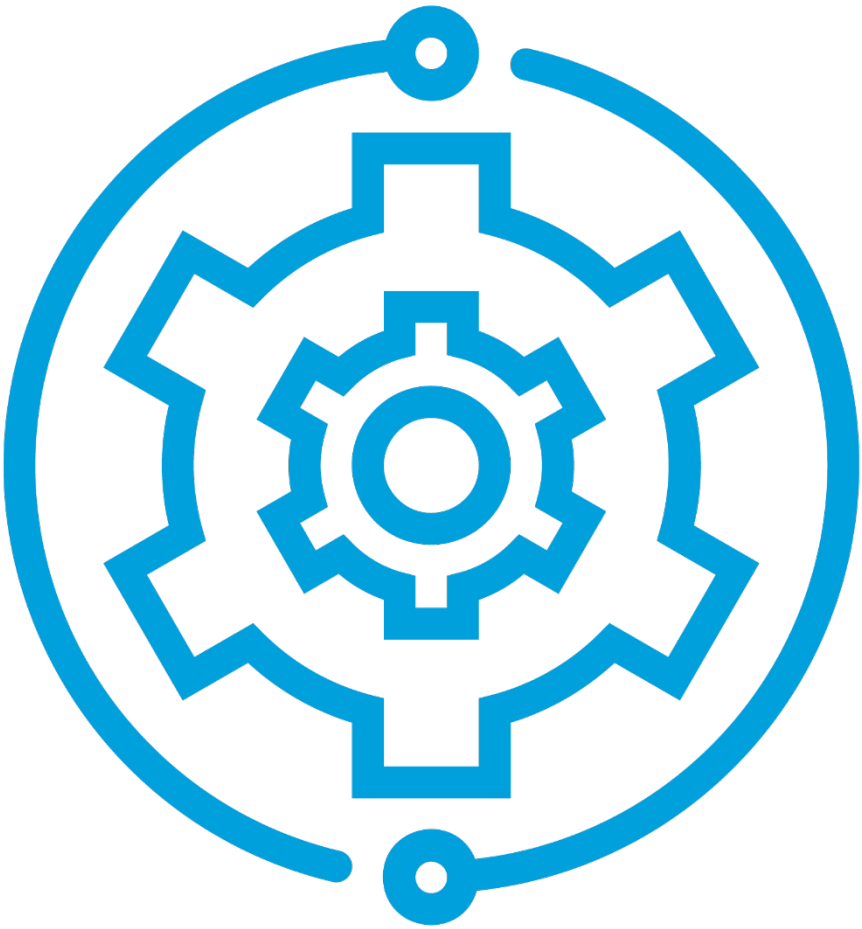
OPENAIR

Operational Network of
Air quality Impact Resources

Best Practice Guide

BP305 | Implement and operate

Sensing device troubleshooting: common problems and how to fix them



Introduction

Air quality sensing devices need constant monitoring and oversight in order to function correctly and reliably. Devices require ongoing maintenance, and are never 'set-and-forget'. The larger the network of devices, the more likely that one of the devices will have a technical issue or complication that requires attention at some stage during your project's lifetime.

Troubleshooting refers to the process of diagnosing the nature and cause of an issue, and how to address it. If you identify an issue with the data your sensing devices have gathered, it will fall into one of two categories: either you have data missing, or your data looks incorrect or strange. The cause of this might be that something is wrong at the level of a device or the way it is deployed, or there might be an issue with communications or your IoT platform.

Who is this resource for?

This chapter is a practical tool to assist anyone tasked with establishing, designing, implementing, or operating a smart low-cost air quality sensing device network. It is written with local government in mind, but may be useful to a broader range of users.

How to use this resource

This OPENAIR Best Practice Guide chapter introduces a framework of common issues that can arise with smart low-cost air quality sensors and the provision of useful data into a database. It includes some practical information to help diagnose common issues, fix them, and mitigate against reoccurrence.

This resource is designed to be useful at the start of your project planning to help you allocate resources effectively. It can also be used as an ongoing reference guide as you move through your project design and implementation phases.

For more in-depth guidance on this topic, please refer to the OPENAIR supplementary resource *Sensing device troubleshooting: extended guide*, which goes into more detail about the twelve types of common issues, what the symptoms of each issue look like in the data, how to fix them, and how to minimise or mitigate the risk of these issues occurring.

A framework for troubleshooting

The collection of usable air quality data relies upon a stack of co-dependent technologies that are integrated with one another to form a larger modular system. Issues can occur at any point in that system, and may not be directly associated with a device. Data flows through a series of layers (the device, the communications network, the data platform, and so on), and at each layer, everything must be in good working order. Failure or issues at any point can result in loss of data or poor-quality data.

Figure 1 charts the flow of data through a sequence of steps to create a troubleshooting framework for diagnosing issues. Potential errors or issues can arise at each step in the sequence. For usable data to be collected, each step in the process must be followed. If an issue arises, it will be occurring at one (or more) of these steps. Troubleshooting is an exercise where you first identify where in the system an issue is occurring, and then how to address it.

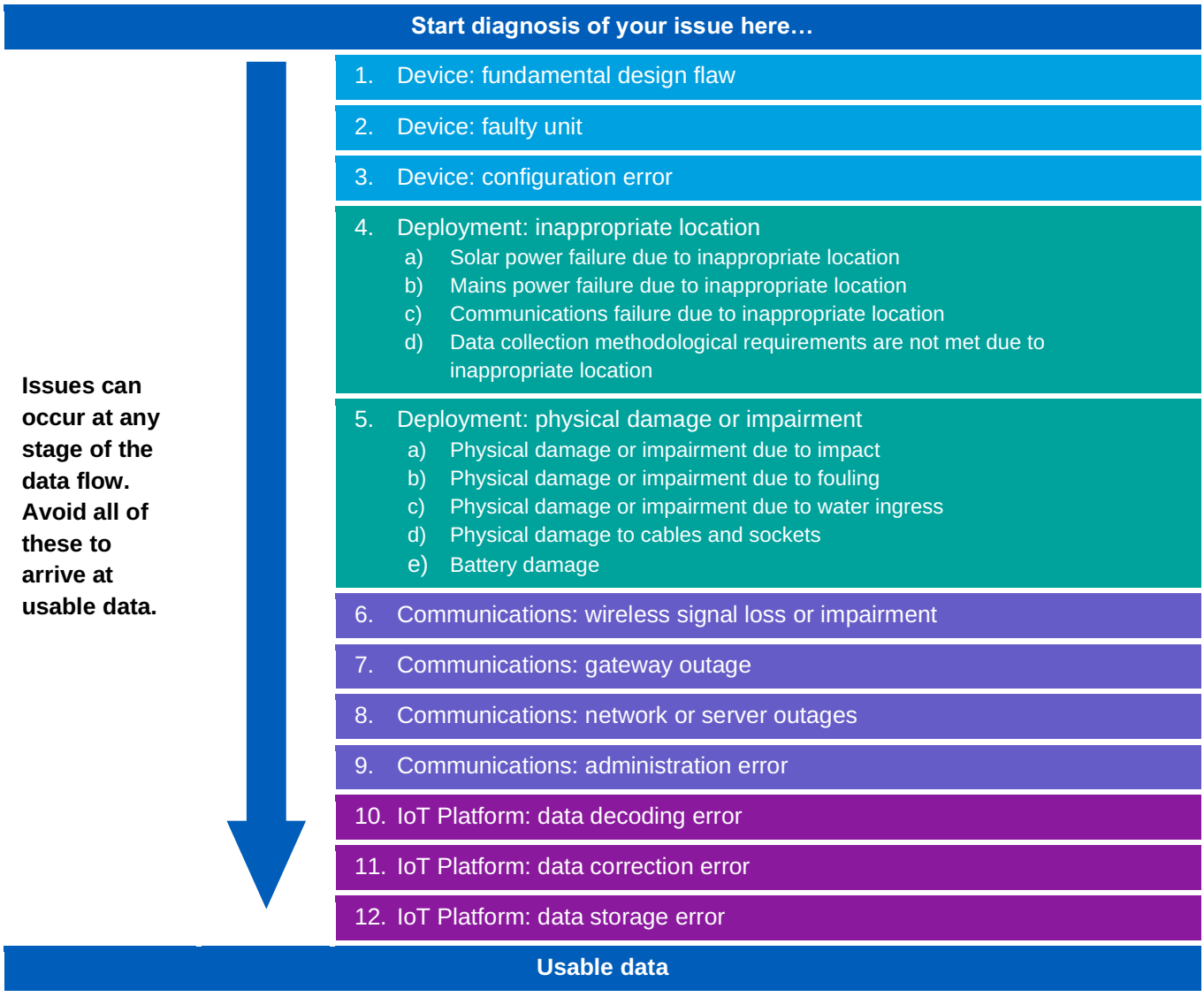


Figure 1. A troubleshooting framework for diagnosing issues associated with the use of smart low-cost sensors for the collection of usable data

An overview of troubleshooting issues

1. Device: Fundamental design flaw

What is happening?

It is possible for a commercial device to have some fundamental aspect of its design that prevents the collection of usable data, or otherwise impairs data quality. This might be anything from the design of the

housing (e.g. it traps too much heat, creating a positive bias on temperature readings) to the choice of components (e.g. the battery is not large enough to cater for long periods of low solar collection in winter). The result will be some kind of impairment, either to data quality, or to device functionality.

How can you fix it?

Once you identify this issue, there is nothing you can do to fix it. You either need to find a way of dealing with the impaired function (e.g. accept lower-quality data and apply correction factors to compensate), or you need to decommission and replace the device with a different product.

2. Device: Faulty unit

Individual devices can have faults on arrival, so always test new units prior to deployment. Image source: Creative Commons

What is happening?

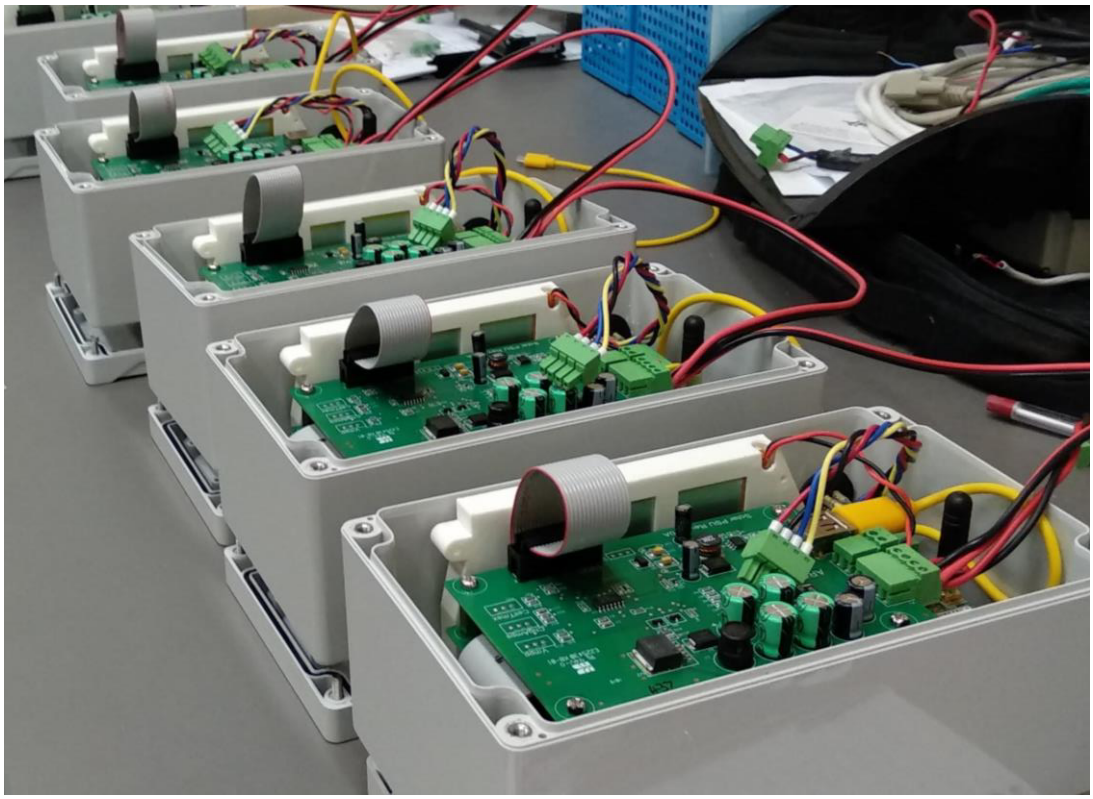
A specific device may have a fault, either physical (hardware) or in its programming (software); examples include:

- hardware faults include damaged seals, electrical faults, damaged wiring, or assembly error
- software faults include incomplete flashing of firmware, or firmware bugs.

How can you fix it?

A fault with a specific device may or may not be fixable. Permanent damage to integral hardware (e.g. from water ingress) generally means that the device is a write-off. Damage to modular components can often be addressed (e.g. a seal or battery replacement). Firmware can also be reinstalled or debugged, and this can sometimes be done by the vendor remotely (using 'over the air', or OTA, updates), meaning that you might not even need to recall the device from the field.

3. Device: Configuration error



Devices are usually pre-configured in a batch by the vendor, prior to shipping. Image source: The ARCS Group

What is happening?

Sensing devices generally have a number of configurable settings that relate to the function of onboard sensors, data processing, and data communications. These settings should be optimised for your project and data use requirements. It is possible for settings to be inappropriately configured, which may result in data that does not meet your needs (e.g. high intermittency), or in complete loss of data transmission.

How can you fix it?

You need to reconfigure your device(s). Devices with 'over the air' (OTA) reconfiguration functionality allow you to remotely update settings without having to physically access the device. This is an extremely useful design feature that is worth considering as a priority during your procurement decision-making. Devices that lack OTA functionality will need to be directly accessed. Some devices have near-field communications technology (e.g. Bluetooth) that require you to have a laptop or smartphone within a few metres, meaning that you won't need to organise access at height. For others, you will need a direct physical connection.

4. Deployment: Inappropriate location

4a) Solar power failure due to inappropriate location

Even partial shading of a solar panel can result in incremental reduction in battery voltage and eventual power failure. Image source: UTS

What is happening?

The device location means that continuous, reliable, year-round power is not achievable from a solar and battery system. This generally means that adequate solar exposure cannot always be maintained, due to the deployment location or configuration.

How can you fix it?

Once you confirm the nature of the issue, organise a physical inspection of the device. The following options can help to fix the issue:

- **Check the aspect of the panel**. Is it optimised to maximise solar exposure for that location?
- **Move the device.** If optimising panel aspect is not enough, consider options for a nearby location that has more solar exposure.
- **Upgrade the battery or the solar panel.** You may be able to avoid needing to move to a new location if you can retrofit either a larger battery, or a larger panel.
- **Shift to mains power.** A final option is to shift to mains power for more reliable supply.

4b) Mains power failure due to inappropriate location

Lighting poles can be ideal locations for deploying devices, but may only have intermittent power supply. Continuous power can be provided to a device by installing a battery that is recharged overnight. Image source: UTS

What is happening?

For mains-powered devices, continuous 24/7 power supply may not be available. This can often be the case for certain street light systems that switch on and off as part of a complete circuit, with no power availability during daylight hours.

How can you fix it?

To support a device that relies upon intermittent mains power, install an external battery and battery-charging control unit that can store power for use at times when mains supply is unavailable. This tends to involve recharging the battery at night (when power to a street light is turned on), and discharging the battery during the day.

4c) Communications failure due to inappropriate location

Growth of summer tree canopy can block wireless signal from a device, and should be considered if you are choosing a deployment location during winter months. Image source: UTS

What is happening?

The device location that has been chosen may have generally poor or unviable communications coverage under optimal environmental conditions, resulting in a device deployment with no communications, or only intermittent communications. Alternatively, a location with initial marginal communications coverage may support a device that communicates reliably during optimal conditions, but becomes intermittent or loses connection entirely during adverse conditions (e.g. rainy weather, wet tree canopies, heavy smoke, or busy traffic).

How can you fix it?

You have three main options for fixing communications issues that relate to deployment location.

- **Reconfigure the communications settings** on a device to improve its ability to reliably transmit data in a location with marginal signal coverage.
- **Move a device to a new location that has better signal coverage**. Keep in mind that this may compromise your data use case, and should only be done after careful consideration.
- **Install an additional communications gateway** to improve signal coverage at the location.

4d) Data collection methodological requirements are not met due to inappropriate location

What is happening?

The device location fails to provide the physical conditions necessary for the collection of robust and reliable data of the quality required to support the stated data use case. In general, this manifests as a small positive or negative bias away from 'true' values for the parameter measured.

Two common considerations are:

- **Thermal interference.** This can result from a thermal mass that is in close proximity to the device (e.g. a wall, large pole, or rooftop) and is exposed to a lot of direct sun.
- **Airflow.** You may wish to ensure that you have good air circulation and mixing in the vicinity of a sensor, as this will tend to provide a more representative sample of the surrounding air. Furthermore, if a sensor is located where airflow is very restricted, it may not pick up small-scale, localised fluctuations in air quality – or vice versa, it may report on trapped pollution in its vicinity that has dissipated in the surrounding area.

A Stevenson shield can protect sensors from thermal radiation and direct sun while maintaining optimal airflow. Image source: UTS.

How can you fix it?

The simplest and most universal fix for this problem is to move the device. This might mean choosing an entirely new location (e.g. more appropriate mounting infrastructure), or it might mean a small change to the micro-siting of the device (e.g. move it further up a pole, or use a different installation bracket that holds it further from the pole).

Another option, which specifically addresses issues of thermal interference, involves retrofitting a Stevenson shield or screen. This is a specially designed housing for an ambient temperature and humidity sensor that optimises airflow, reflects sunlight and direct thermal radiation, and ensures protection from the weather.

5. Deployment: Physical damage or impairment

5a) Physical damage or impairment due to impact

What is happening?

Physical impact of an object with a device can cause a variety of damage that may or may not impair functionality. Damage can include partial loss of telemetry, or loss of power (e.g. if a solar panel or external battery is damaged). It may also result in a damaged mounting bracket becoming unsafe, causing safety and compliance concern if this occurs in a public space. Common causes of impact include collision with a vehicle (e.g. a delivery truck backs into it), and vandalism. Hail can also be a concern.

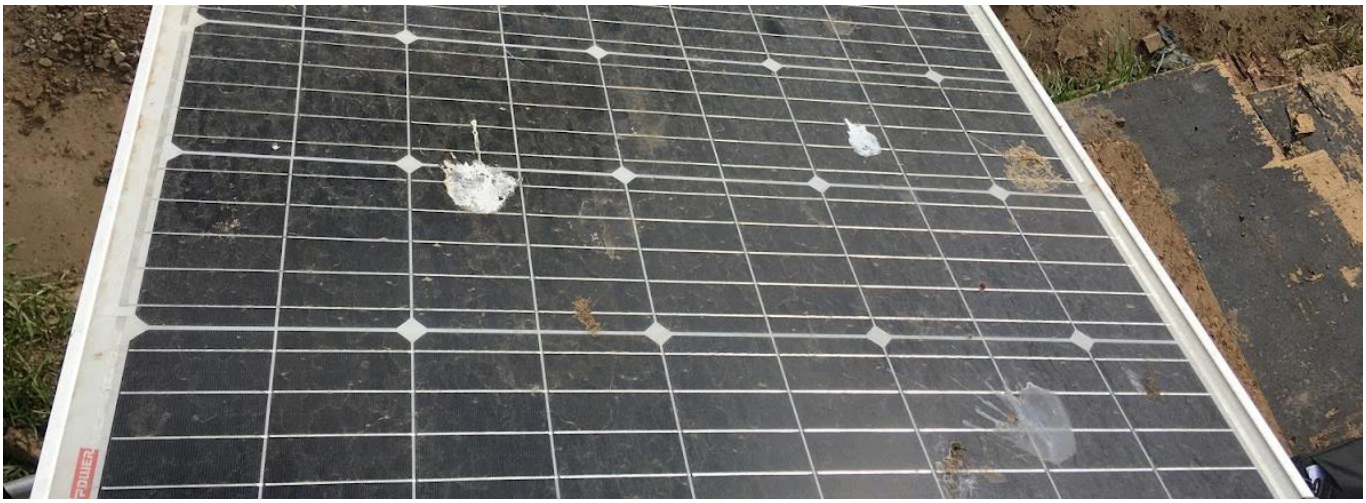
A sensing device solar panel damaged by collision with a delivery truck in the City of Sydney. Image source: UTS

How can you fix it?

Once you identify that physical damage has occurred, try to assess the impact that it is having. Is this something that requires immediate attention, or is it something superficial that you can live with? Assuming you decide to take action, you have two basic options:

- **Repair or replace damaged parts**. This may be as simple as installing a new solar panel or mounting bracket, or it may involve sending the device back to your vendor for refurbishment.
- **Replace the entire device with a new unit.** This is the more costly option, and may result in a significant gap in your data record if procurement and/or shipping of the new unit is delayed.

5b) Physical damage or impairment due to fouling



Even mild fouling of a solar panel can be enough to completely impair its function. Image source: UTS.

What is happening?

Fouling refers to the build-up of unwanted material on components of a device, resulting in functional impairment. The components that are most impacted by fouling are solar panels, the inside of sensors, and housing ventilation, as described below:

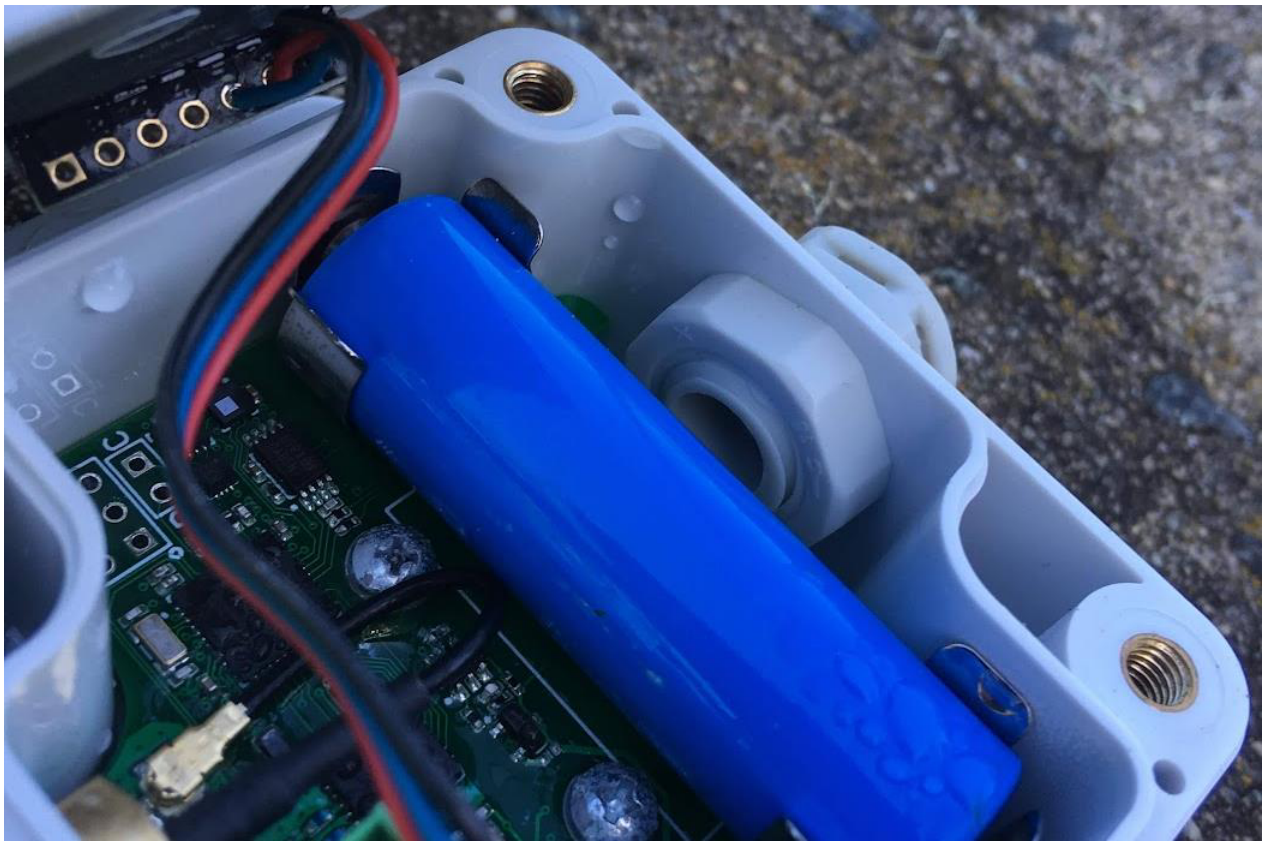
- **Fouling of solar panels.** Solar panels tend to have relatively small margins of tolerance for fouling. Leaves, bird droppings, or spiderwebs can commonly reduce the total area of exposed panel by small amounts that are nevertheless enough to entirely impair panel function. Uniform deposition of dust and particulate pollution on a panel, as well as snow or frost, can also entirely impair panel function.
- **Fouling of sensors.** The inside of sensors can be impacted by the deposition of dust and airborne particulates on receptors, which impairs accuracy and ultimately renders the sensor unusable.
- **Fouling of housing ventilation.** The housing of a device includes ventilation holes designed to ensure airflow over sensors. Spiders and insects can enter these spaces and restrict airflow. This will cause a device to become less responsive to ambient conditions, and may also create a small bias in temperature and humidity readings.

How can you fix it?

The basic fix for fouling involves cleaning and removal of the unwanted material. This is simple for solar panels and external air intakes, but may prove to be more involved for internal components.

Internal fouling is not visually apparent. If it is suspected to be a problem, this is likely based upon detection of systemic inaccuracies or bias in the data. It is therefore advisable to recall the device and send it to your vendor for refurbishment.

5c) Physical damage or impairment due to water ingress



Water ingress can occur through a damaged seal, resulting in permanent damage to internal electronics. Image source: UTS.

What is happening?

Water ingress can result in permanent physical damage to device circuitry and components. It generally occurs because of a damaged seal, or from a poorly or incorrectly replaced housing lid or cover. These issues tend to occur during assembly (e.g. following battery installation) or installation of the device.

How can you fix it?

Water ingress tends to result in permanent irreparable damage to the components that it affects. In some cases, you may be able to replace damaged parts (e.g. a battery or battery terminal). In other cases, you may have issues with small circuitry components that are harder to replace.

Generally, the situation requires returning the device to the vendor, either for refurbishment or proof of issue. If repair or replacement of components is not possible, you may need a new replacement device, in which case you may be able to claim on the warranty.

5d) Physical damage to cables and sockets

What is happening?

Cables and cable sockets can be damaged during assembly and installation of a device by not following correct procedures. Common issues include overtightening, bending of terminal pins, and cables being caught or pinched by tools or tightened brackets, resulting in internal damage to wires. Damage by birds (e.g. cockatoos) is also a common issue.

Cockatoos can damage cables. Image source: Creative Commons.

How can you fix it?

If cable or socket damage is suspected, the first step is to conduct a physical inspection of the device. Disconnect and reconnect all cables, and run a manual reset of the device to confirm whether it is working and sending complete data packets. Often, the issue can simply be a loose connection that can be solved by correctly inserting a cable into a socket. If damage is detected, this will require replacement cables or sockets. The latter may require returning the device to your vendor.

To protect cables from damage by birds, you can encase them in robust conduit. You may be able to design custom mounting brackets that protect sockets from direct access. Anti-bird spikes can also help.

5e) Battery damage

What is happening?

Rechargeable batteries used in solar-battery systems or as mains power backup can be permanently damaged as a result of over discharge, or too many charge cycles. The most common issue with battery damage relates to exceeding the recommended depth of discharge (DoD) limit, which can lead to battery failure. DoD exceedances occur when power supply for recharging the battery drops below planned tolerances for an extended period of time, resulting in a device drawing too deeply on battery reserves.

A battery should ideally be integrated with a charge controller that prevents 'depth of discharge' (DoD) exceedances, avoiding permanent battery damage.
Image source: UTS.

For solar systems, a DoD exceedance can occur due to one or more of the following factors: fouling of the solar panel; damage to power cables; higher than expected shade on a solar panel (e.g. deciduous tree canopy in summer months); prolonged rainy or overcast weather; and short day length in winter.

For mains power systems, a DoD exceedance can occur if a circuit is damaged or turned off for an extended period. For example, a sports field closed for three days over Christmas might have power to light poles switched off for long enough to completely drain a device's battery.

Another battery failure concern relates to charge cycles. All battery types have a maximum number of charge cycles associated with their expected operational lifespan. If you have a modular device where you can replace other components as they wear out, battery life and replacement may also become a concern.

How can you fix it?

If a battery has suffered permanent damage, it cannot be restored. You will either need to install a replacement battery, or procure a replacement device. Some smart low-cost sensing devices are designed to take standard consumer-grade batteries (e.g. AA or AAA), making replacement simple. Others take industrial batteries that might be hardwired into the device, meaning that you will likely need to return the entire device to the vendor for refurbishment. You should also be aware of warranty breaches if you break the seal on certain compartments of a device.

Higher performance devices tend to include power management and battery protection technology that shuts down the device before a DoD exceedance can occur, avoiding the risk of permanent battery damage. You may wish to prioritise this as a technical requirement for your device procurement.

6. Communications: Wireless signal loss or impairment

NOTE: This issue bears close similarity to '*Communications failure due to inappropriate location*', which has already been discussed. However, it is useful to distinguish between the two.

The former issue relates to a decision made about a device deployment location during the planning stages of a project, where the location is inappropriate because it does not support viable communications. The emphasis in that case is on better deployment planning.

For wireless signal loss or impairment, the focus is subtly different. If the original decision about the deployment location was sound, and that wireless signal at that location was viable when the device was deployed, then any subsequent issue that arises is due to *changes* to that original situation that have occurred during the operation of the device. We therefore dedicate a separate troubleshooting category to this concern.

What is happening?

Devices that transmit data using wireless communications technology can fail to communicate with a local communications gateway due to a loss (or impairment) of wireless signal at any point between the device and the gateway. This issue can occur with any communications technology that uses local gateways (including Wi-Fi, LoRaWAN, SigFox, 3G/4G/5G, NBIoT, or Cat-M1).

Wireless signal loss or impairment can occur for two main reasons:

1. **Wireless signal strength reduces to marginal or non-viable levels** due to some kind of physical blockage of signal in line of site between a device and a gateway, or to adverse atmospheric conditions. Examples include:
    - a new building or other large structure appears between the device and the gateway
    - summer vegetation (notably deciduous tree canopies)
    - a small, localised fixed blockage near the device (e.g. a large new sign)
    - a small, localised fixed blockage near the gateway antenna
    - Heavy city traffic that results in intermittently blocked signal over rush hour periods

Heavy bushfire smoke in Parramatta, NSW. Smoke can attenuate wireless signal strength, resulting in lost communications.
Image source: UTS.

- Rain, mist, or heavy smoke that attenuates signal strength through the air for certain radio technologies.

2. **Signal-to-noise ratio (SNR) changes** due to increased background noise in the area. This can result from installation of new wireless technologies (using similar electromagnetic frequencies as those being used by your device) in the vicinity of the device or the gateway.

How can you fix it?

There are several ways to fix a wireless signal issue:

- **Identify the root cause of the issue and remove it**. This is easiest when the blockage is physical and very localised to either the device or a gateway, as you are more likely to have jurisdiction to move it.
- **Move a device to a new location that has better signal coverage**. This may compromise your data use case, however, and should only be done after careful consideration.
- **Reconfigure the communications settings** on a device to improve its ability to reliably transmit data in a location with marginal signal coverage.
- **Raise the height of an existing private gateway using a mast**. The height of a gateway can make an enormous difference to signal coverage.
- **Install an additional communications gateway** to improve signal coverage at the location.

3. Communications: Gateway outage

A communications gateway can fail for a wide range of reasons, resulting in partial or complete loss of network communications. Image source: UTS.

What is happening?

The communications gateway ceases normal function, causing a loss of communications between devices and the communications server. This results in a data gap for the period that the gateway function is impaired. A gateway outage can occur for several reasons, including: scheduled maintenance, loss of power to the gateway due to accidental shut-off or issues with solar-battery systems, physical damage to the gateway, changes to gateway firmware; changes to server settings that cause the gateway to lose connectivity with the server, or suspension of service due to unpaid invoices.

How can you fix it?

Fixing a gateway outage can require a range of actions that depend on the cause of the problem. If you suspect that there is an outage, the first step is to contact your communications service provider. They likely have access to operational data that you do not have, meaning that they can probably confirm the issue and its cause, and rectify it.

Loss of power or physical damage are local issues that your vendor may not be able to identify. You may need to arrange a physical inspection and address obvious issues (e.g. turn power back on, or make on-site repairs). More serious hardware faults may mean that the entire gateway needs replacing or refurbishment.

4. Communications: Network and server outages

A server can experience an outage for several reasons, resulting in a data gap for all devices in your network. Image source: Creative Commons.

What is happening?

Most types of communications networks can experience a temporary outage that impacts all gateways and devices in the network. A network outage (particularly with mobile networks that have high use) is generally associated with network congestion, which often coincides with large public events, such as Christmas or Mother's Day. A server outage causes a loss of communications between gateways and your IoT platform. This results in a loss of data for the period that the outage occurs.

A server outage may result from planned or unplanned maintenance and updates; a programming error or misconfiguration of the server by the service provider; power failure to the server (non-cloud-based servers only); an exceedance of server resource consumption (i.e. data storage and processing); or a cybersecurity attack that targets and compromises the network or server.

How can you fix it?

For the most part, network and server outages are not under your direct control. One exception is Wi-Fi that relies upon an internal network within your organisation, in which case you should contact your own IT department for assistance. For all other cases, you will need to engage with your external communications service provider for assistance.

5. Communications: Administration error

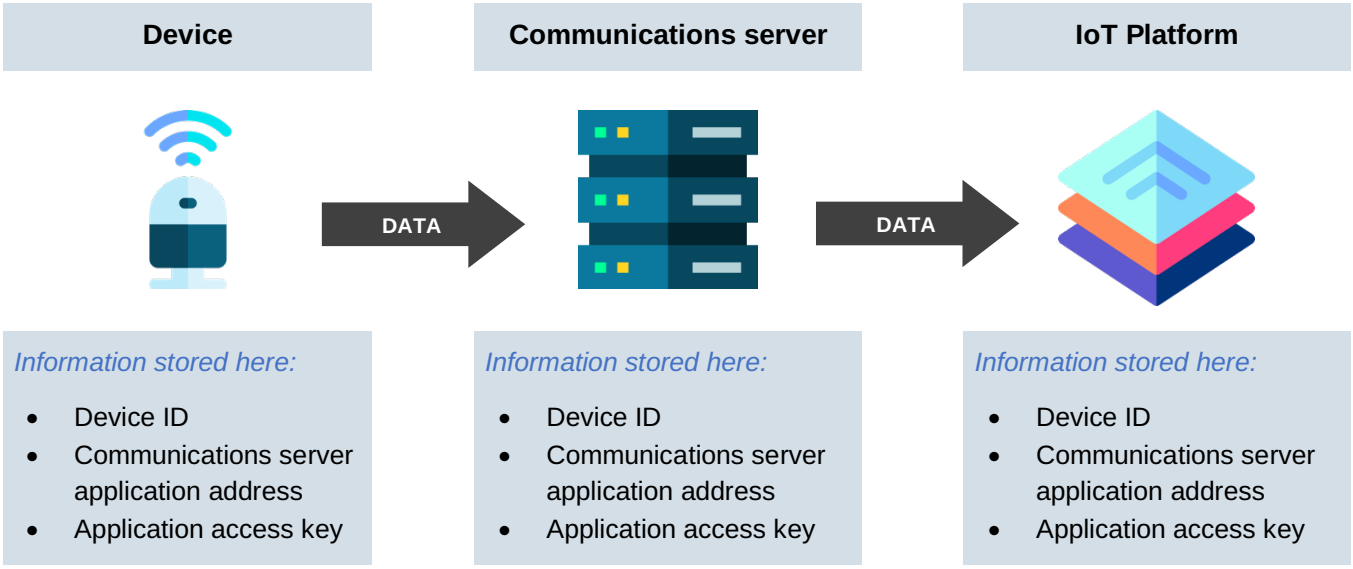


Figure 2. A diagram showing the flow of data from a device to an IoT platform, via a communications server. If the information stored in each location does not match, an administrative error occurs. Graphic source: Freepik.

What is happening?

An administrative error can result in a communications failure. Data flows from a device, through a communications server, and into an IoT platform – Figure 2 illustrates this in detail. In each location, critical information needs to be registered. If there are any discrepancies in this information between the three locations (generally resulting from human error), a communications failure occurs. Errors can impact single devices (e.g. a single device identification code is wrongly entered) or whole groups of devices (e.g. an IoT platform has the wrong server application access key).

How can you fix it?

If a device is not being 'seen' by your communications server or by your IoT platform, then a check of all the codes and keys in the device, the server, and the IoT platform is a useful first response. Depending on the nature of your service contract, your device vendor may take responsibility for undertaking these checks and fixing the issue. In some cases, your vendor may even pick up and fix an issue without you even being aware of it. However, if you are taking a more DIY approach, you will need to do this yourself.

Unfortunately, correction of an error in a device generally requires a direct physical connection to be made with that device, meaning a trip into the field, access at height, and various access approvals. This is why acceptance testing should occur prior to deployment, because it picks up on these issues while access to the devices is still quick and easy. Corrections in a server or IoT platform are easier to make.

6. IoT Platform: Data decoding error

Raw data from a sensing device arrives as a string of alphanumeric characters that comprise a 'data packet'. This string must be decoded to extract discrete pieces of information. Errors can occur in this process. Image source: Creative Commons.

What is happening?

A data packet arriving in an IoT platform from a device is composed of a string of compressed information. The data packet must be decoded, and errors can occur in the decoding process. A decoding module contains a map of the data packet associated with a specific device type, and is able to slice it up into discrete pieces of information. One piece might relate to a temperature reading, and another to battery voltage.

Data decoding errors can result from a variety of more fundamental issues:

- The decoding module can be incorrectly set up, impacting all devices of a certain type.
- Updates to device firmware can result in changes to the structure of a data packet. If a corresponding change is not made in the decoding module, a decoding error will occur.
- Updates made within an IoT platform can impact the functionality or integration of decoders.

How can you fix it?

Contact your IoT platform vendor for assistance in the first instance. If things look complicated, then you may also need to connect them with the device manufacturer to help support collaborative problem-solving.

Decoder modules are hosted within IoT platforms. The platform owner writes and integrates decoders into the platform, and is best-placed to diagnose and fix a decoder error. This task is generally easiest in cases where one provider has developed the devices and the platform as a single ecosystem. In cases where a platform provider is hosting third party devices, a decoder will be written by the platform provider based upon that device's documentation. In this scenario, there is room for error in the device documentation (generally related to it being out of date relative to device firmware updates). The result will be that a platform provider may struggle to diagnose and fix the issue on their own, instead requiring the active assistance of the device manufacturer.

7. IoT Platform: Data correction error

What is happening?

Decoded sensor data often requires the application of 'correction factors' to improve data quality. Certain types of data require certain types of correction. The main types of data correction for air quality monitoring applications are temperature interference correction; humidity interference correction; regionally specific correction factors that account for variables like salt, dust, pollen, or biogenic VOCs; and calibration drift correction.

Devices deployed in coastal locations might have correction factors for salt aerosols. Image source: UTS.

In smart monitoring networks that handle near-real-time sensor data, correction factors can be applied to data streams as they arrive, ensuring that live data shown on a platform is corrected, and resulting in a corrected data record in your database. This approach is in contrast to a more manual approach, where corrections are applied to a static data set. Our focus here is on errors in live correction factors.

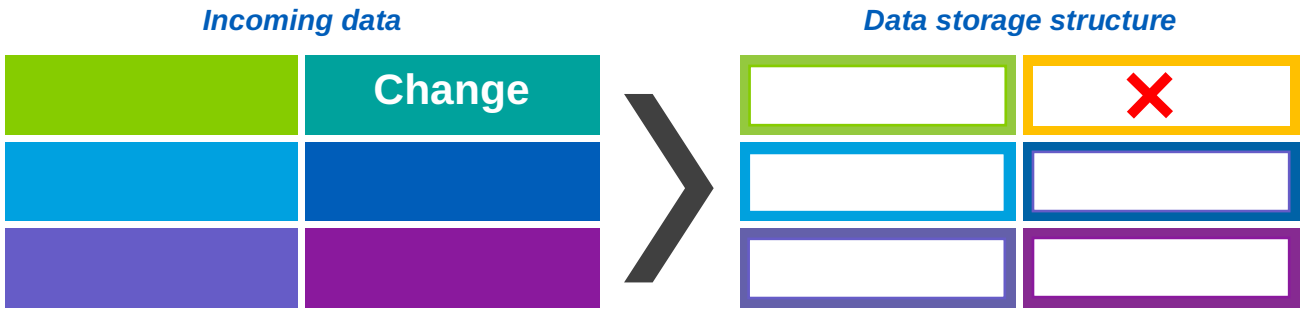
Correction factors can be implemented with errors (e.g. a misplaced decimal point), due either to human error at the point of implementation, or to errors in supporting documentation. Errors can also occur if correction factors are updated during the operation of your sensor network (e.g. based on new insights). Please refer to the OPENAIR Best Practice Guide chapter *Data interpretation: correction and harmonisation* for further information about correction factors.

How can you fix it?

Correction factor errors will generally be detected by someone (usually outside of the platform provider organisation) tasked with data quality control or analysis, possibly several months after a system goes live. The IoT platform provider should be contacted, and a meeting arranged between their developers and the person who detected the issue. Ideally, there should be detailed documentation about actually applied correction factors to which both parties can refer. The IoT platform provider should then be able to fix the issue, ensuring that future corrected data in your database is accurate.

While correction factor errors may go undetected for some time, the good news is that they can be retroactively adjusted, meaning that past data can be made usable for analysis. This is contingent upon you storing raw device data in your database, alongside any corrected data.

8. IoT Platform: Data storage error



A change in the structure of incoming data can result from updates to devices or decoders.

If a corresponding change is not made in the data storage structure, then some or all of the data will fail to enter storage.

Figure 3. Changes to incoming data can result in data storage errors. While this is not the only type of data storage error that can occur, it is the most common.

What is happening?

Data arriving from a sensor network into an IoT platform must be correctly entered into a database, otherwise it will be lost. There are several things that can go wrong at this stage:

- Databases are often structured using various fields and lists. The structure of incoming data may fail to match the structure of your data storage, resulting either in a failure to store that data, or in it being stored incorrectly. Such errors can occur as a result of device firmware updates, or decoding or correction factor updates that alter the structure of the incoming data. Note that some databases use *unstructured* data storage, either in parallel with (or instead of) *structured* data storage. This can avoid loss of data, and for this reason it is good practice to store raw, unstructured data.
- Other types of data storage error relate to disruption of the data storage solution itself, and to issues with the integration of that solution with the IoT platform. Data storage can be directly disrupted due to a server outage, exceedance of storage capacity, scheduled maintenance, programming errors and bugs, cybersecurity attacks, or failure to pay invoices (resulting in suspension of service). Integration of data storage with an IoT platform can fail due to coding errors, which might result unexpectedly from maintenance or platform software updates.

Figure 2 (above) illustrates the most common type of data storage error.

How can you fix it?

An IoT platform refers to data in a database, meaning that a storage error will show up as no data record in your IoT platform. Therefore, in order to diagnose this problem, you should ideally have access to a user interface for your communications server. Here, you should be able to check to see if data is being received and forwarded by the device in question. If you don't see data, you likely have an issue with communications, or with the devices themselves. If you do see data packets arriving, then you can confirm that the issue lies downstream, in the IoT platform. At this point, you could be looking at a decoder error, a correction factor error, or an error in your database. Regardless of which it is, your

action should be the same: raise the issue with your IoT platform provider. They should be able to pinpoint the cause of the issue, and fix it.

Risk mitigation tips by project stage

At each stage of a project, there are measures you can take to mitigate the risk of future issues arising. Familiarise yourself with these measures, and build them into your project plan. These recommended mitigation measures have been grouped according to the stages of the OPENAIR Impact Planning Cycle. Refer to the OPENAIR factsheet *The Impact Planning Cycle at a glance* for a description of the Impact Planning Cycle.

Identify

Project initiation and strategy development phase

Develop a strong business case and a data use action statement. Be clear about the type and quality of data that you need to collect, who will use it, and what it will be used for. This clarity, early on in your project, will inform all of the design decisions that you make later. Risk mitigation measures invariably require additional time, effort, and expense to implement. For each one, you need to understand how critical it is to supporting your business case and data needs.

Develop

Technical requirements and procurement

Invest in quality devices. Check the track record, seek testimonials, speak to other users, and check to see if any independent performance assessments have been published. For larger procurements, you may also choose to purchase two or three devices, and co-locate them with reference equipment for a test period to rule out obvious issues prior to full investment. In addition to data quality and reliability, pay attention to physical attributes (e.g. IP rating, robustness, housing design, physical materials used, mounting brackets, and ease of assembly). Pay attention to warranties, and be clear about what they do and do not cover.

Pay attention to device features and functions. A variety of procurement decisions relating to the features and functions of devices can help to support your specific data use case. For example, if accurate ambient temperature readings are important, you can ensure that devices feature Stevenson shields to mitigate thermal interference. In humid environments, a heated air intake for particulate sensing can reduce humidity interfering with the accurate measurement of pollutants. Pay attention to functional attributes (such as ‘over the air’ updates, automatic device recovery, in-built power management, and configurability options).

Choose appropriate power solutions. Think through your solar power needs as early as possible, so you can discuss them with your chosen device vendor during the procurement process. Consider shaded locations and the possibility of fouling from leaves and dust, as well as overcast weather and mid-winter sunlight. Ensure that the design of the solar-battery system has tolerance to support your devices through these conditions. For mains power, consider including an external battery to support devices when power is switched off. All devices that feature rechargeable batteries should have built-in power management and battery protection functionality.

Consider automatic recovery. Not all low-cost devices will be sophisticated enough to restore normal operations following power failure. One approach is to procure devices that have the capacity to automatically recover themselves.

Use configurable settings. Procure devices that can be configured to meet your needs, with set-up support. Ensure that devices can support your desired reporting interval and sampling rate, and that communications settings can be configured to support reliable connectivity (if you plan to deploy devices in locations where signal strength might be marginal). Speak with a prospective vendor, and be clear about the level of support they provide for custom configuration of devices. Understand that you may need to iteratively tweak settings to optimise them, and that this may require extended support.

Collect device documentation. Obtain detailed device documentation as early as you can in the procurement process. If you are building a more modular, integrated system, access to thorough and detailed documentation should be a technical requirement for device procurement – check what is available, and be wary of products that have minimal available documentation. Getting hold of this information early is helpful. This gives your communications service provider, IoT platform provider, and database manager sufficient time to develop integration software and data management structures prior to going live, avoiding rushed work and reducing the chance of mistakes.

Choose the right communications technology. You should understand your spatial context, and the sorts of challenges this might create for communications coverage. Undulating terrain, dense vegetation, and high-rise buildings can all create complex environments with a lot of communications 'black spots'. High-rise urban settings are at a higher risk of wireless signal loss (or impairment) resulting from changing conditions than low-rise or rural settings. Communications technologies vary in their coverage, range, and ability to penetrate physical barriers (e.g. tree canopies). You need to ensure that you procure a communications technology (and corresponding devices) that are appropriate for the spatial context of your deployment locations. If you choose to invest in private local communications gateways, procure high-quality products with a proven track record.

Ensure adequate communications coverage. It is important to ensure that there are enough gateways[1] to service your study area. It is strongly advisable to have at least two gateways to provide stereo coverage to a majority of your device deployment locations, particularly for larger networks (>10 devices). You can also ensure that private gateways are installed in an optimal position that maximises their coverage (e.g. choose gateway deployment locations that are as high as possible off the ground; aim to install them on as tall a mast as possible; and ensure that a gateway antenna is not obstructed by any nearby objects, including the mast itself). Your gateway vendor should provide detailed guidance for optimising installation.

Choose the right communications servers. Use a communications server that is cloud-based to remove the risk of a server outage due to power failure. You can also consider using a private communications server. Many communications service providers have commercial options for either public or private servers. Public servers have large numbers of users, and are more likely to experience outages and congestion. Private servers will cost you more to use, but come with a range of service guarantees. They reduce the risk of outages, remove the risk of network congestion, are likely to have

[1] A gateway is an antenna that transmits and receives signals from devices (e.g. a Wi-Fi router is a gateway, as is a 4G telecommunications mast).

less scheduled downtime, and can mitigate against the risk of cybersecurity attacks and overconsumption of resources.

Optimise your hardware for marginal communications. It is possible to optimise your hardware to support devices in locations with more marginal communications coverage. Devices can be chosen with larger antennae, stronger transmission power, and greater battery capacity. Private local gateways can also be installed optimally (e.g. with a tall mast and no nearby objects in line of sight), or sub-optimally (e.g. too low). You can also optimise device configuration (specifically, transmission power and spreading factor).

Procure onboarding support. Procure devices with good registration and onboarding support. Vendor services vary considerably. Some vendors are responsible for device registration and onboarding, while others will ship you unregistered devices with factory settings. Vendors that provide registration and onboarding support should, at least in theory, have well-developed, rigorous processes in place. By procuring devices that come with this kind of support, you can reduce your own level of responsibility, and rely upon the experience and competence of a third party. At the end of the day, better services cost you more, but carry less risk and lead to better outcomes.

Procure operational support. Negotiate appropriate service and operational support agreements with vendors. For devices, this might include a 'return to base' service (where faulty devices can be assessed and refurbished by the vendor). For communications, this might include managed gateways, or service level agreements (SLAs)[2]. For platforms, this might include device management, software updates, and general troubleshooting. Establish your responsibilities versus those of the vendor. Be clear about the type and level of support available (how much, in what form, availability, response times, etc.).

Device deployment planning

Ensure power reliability. Be clear about the reliability of power supply in a given location. When choosing deployment locations that rely upon mains power, find out who manages that power and whether it is continuous or intermittent. Avoid intermittent power, or plan for inclusion of a battery system. For solar-powered devices, assess direct solar exposure at each location, and consider upgrades to panels or batteries for specific devices if it looks like exposure will be marginal at certain times.

Do on-the-ground signal testing. Ensure that you undertake thorough on-the-ground communications signal testing for all planned deployment locations prior to device deployment, helping you to avoid later issues. You should design your device network to avoid locations with marginal signal.

[2] SLAs are legal agreements with service providers that ensure a guaranteed minimum level of service. You will pay more for a service with an SLA, however, they reduce risk and your own direct responsibility for risk minimisation. Only certain services will offer SLAs. SLAs for communications technologies reduce the likelihood of gateway, network, or server outages, guaranteeing a maximum amount of communications downtime per year. Communications SLAs are only available with some technology options – for example, you can get an SLA with 4G, but not with LoRaWAN. SLAs for platforms relate to the amount of guaranteed availability and normal functioning of the platform.

Implement and operate

Network deployment

Establish your own device onboarding process. If you opt for a more in-house approach to device registration and onboarding (as opposed to outsourcing this to a service provider), you should write up a detailed, step-by-step process before you begin. Assign clear roles, establish single sources of truth for metadata, and create a system for tracking and verifying every stage in the onboarding process. This will help you avoid common device administration errors that result in failure to communicate. Even if you are outsourcing device onboarding, it is still highly advisable for you to establish your own in-house process for working with that provider on a device-by-device basis.

Support thorough training of device assemblers and installers. Errors made during the assembly and installation of devices can result in physical damage (including broken seals, cables, and sockets), failure to correctly connect and activate (e.g. power cable incorrectly connected), and installations that create methodological issues (e.g. too close to a large thermal mass), not to mention safety and aesthetic concerns. These types of errors can be prevented by thorough training of device assemblers and installers. If you are deploying a larger number of devices, develop clear, detailed materials that include step-by-step instructions. It is also advisable to arrange supervised test assemblies and installations, where you can run through everything with staff or contractors to ensure they are across all the important details. To support these activities, it is also necessary for you to run test assembly and deployments of devices as soon as you acquire the hardware. Get to know the complexities and idiosyncrasies of the products. Identify potential issues, and come up with methods to avoid them.

Avoid high-risk micro-siting of devices. Micro-siting refers to the specific details of how a device is positioned and installed at a location. Avoid deploying a device facing a road on poles that are very close to the roadside. Avoid deploying a device in locations with delivery truck parking. If you cannot avoid such a location, deploy at a height that is above the height of most vehicles. Install devices at a height that minimises the chances of vandalism, and make devices as inconspicuous as possible in locations where vandalism is a concern.

Take practical measures to prevent physical damage. The risk of certain types of physical damage to devices and gateways can be mitigated. Examples include bird spikes, a rain and hail guard, and deployment in a hard-to-reach location (to prevent vandalism).

Take practical measures to prevent loss of power. Accidental shut-off of mains power is a common cause of gateway and device outages. You can help prevent this by hardwiring power supply (i.e. don't provide an off switch), and labelling switches and fuse boxes clearly (e.g. with a label that says 'DO NOT SWITCH OFF', and including a contact phone number).

Network operations

Schedule regular maintenance. It is recommended that you implement a maintenance and servicing regime for your sensor network that includes physical inspection of devices and solar panels on a regular, recurring basis. External fouling can be checked for and cleaned away. Physical damage can be checked for and addressed. You might also have a service agreement with your device vendor for periodic cleaning and refurbishment of devices.

Set up automatic device management alerts. This is where a platform alerts you to an issue before it becomes a problem. It requires you to have an IoT platform that can set automatic thresholds relative to

device telemetry, and issue alerts when thresholds are breached. Examples include lower threshold alerts for battery and solar voltage.

Track and manage device firmware. Your devices may have updates made to their firmware while you are using them. Updates may be actioned 'over the air' (OTA) by a service provider, or you may need to manually apply them yourself by physically connecting to a device. Either way, keep a record of updated documentation that captures firmware updates, and ensure that there is a process in place for tracking the date, time, and version of updates for each device. You must ensure that updates and supporting documentation are communicated to your IoT platform provider to support decoder updates.

Manage and analyse

Data processing and storage

Document data processing. Ensure good documentation of all data processing. This includes keeping detailed technical records of device firmware, data decoders, and correction factors, and ensuring that these are shared with all parties. This helps to mitigate and address various issues that can arise with the decoding, correction, and storage of data.

Ensure that there is a process in place for all data processing updates. There is a good chance that updates will need to be made to the way that you decode, correct, and structure data during the operation of your sensor network. These types of changes can create errors in data interpretation and storage. Avoid ad hoc approaches to these changes by anticipating and planning for them.

Store unstructured data in addition to structured data. Some data storage is what we call 'unstructured', meaning that any data arriving in the database can be stored regardless of its structure – there are no distinctions made. With unstructured data storage, you can point any new data at your database, and it will be captured. Unstructured data on record can always be correctly structured at a later date. This prevents outright data loss from structured data errors.

Associated OPENAIR resources

Factsheets

The Impact Planning Cycle at a glance

This factsheet presents an overview of the OPENAIR Impact Planning Cycle, a simple, practical framework designed to assist local governments with impact planning for a smart air quality monitoring project.

Best Practice guides

Data interpretation: correction and harmonisation

This Best Practice Guide chapter provides guidance on correction and harmonisation of data produced by smart low-cost air quality sensors. It introduces several types of correction factor that may need to be applied to raw sensor data, and explores how data formatting and labelling should be harmonised with a project data schema to support effective data management and sharing.

Supplementary resources

Sensing device troubleshooting: extended guide

This resource presents an extended systematic list of problems that can arise with smart low-cost air quality sensors and the provision of useful data. It includes practical information to help diagnose, fix and mitigate each type of issue.

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: 20231026 BP305 Sensing device troubleshooting: common problems and how to fix them Version 2 Final


OPENAIR
NSSN
NSW Smart Sensing Network
UTS
Institute for
Sustainable
Futures
NSW
GOVERNMENT
POWERED BY THE
DIGITAL
RESTART
FUND