OPENAIR

Operational Network of Air quality Impact Resources

Sensing device troubleshooting: extended guide

SR303

December 2023

openair.org.au

Table of Contents

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. This extended guide provides a practical framework for troubleshooting issues that can occur with smart low-cost air quality sensing devices and collating useful data from these devices into a database.

Who is this resource for?

This resource is a detailed 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 guide provides an overview of the OPENAIR troubleshooting framework for the operation of smart low-cost air quality monitoring sensing device networks. The **framework diagram** (Figure 1) outlines 12 types of issues that can commonly occur. The diagram contains hyperlinks to related sub-sections within this document, supporting rapid navigation. Alternatively, you can use the Table of Contents at the beginning of this document to go directly to specific topics.

Use the **troubleshooting diagnostic process flow chart** (Figure 2) to narrow down which issues (of the identified types 1-12) you are likely to be dealing with, then navigate to the sub-sections relating to those issues. Each sub-section provides extensive information on each of the 12 common types of issues in the troubleshooting framework, with practical tips to help diagnose, fix, and mitigate the specific issue you are dealing with.

You should familiarise yourself with the most common issues outlined in this document during the early planning stages of your project. Pay particular attention to the risk mitigation advice, much of which relates to procurement decision-making.

Note that many of the potential issues outlined in this document relate to networks requiring more hands-on monitoring, where much of the operational responsibility lies within the organisation. If you plan to have service contracts in place to outsource much of this responsibility, you can use this guide as a reference to ensure that prospective suppliers are aware of the common issues and know how to troubleshoot them.

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.

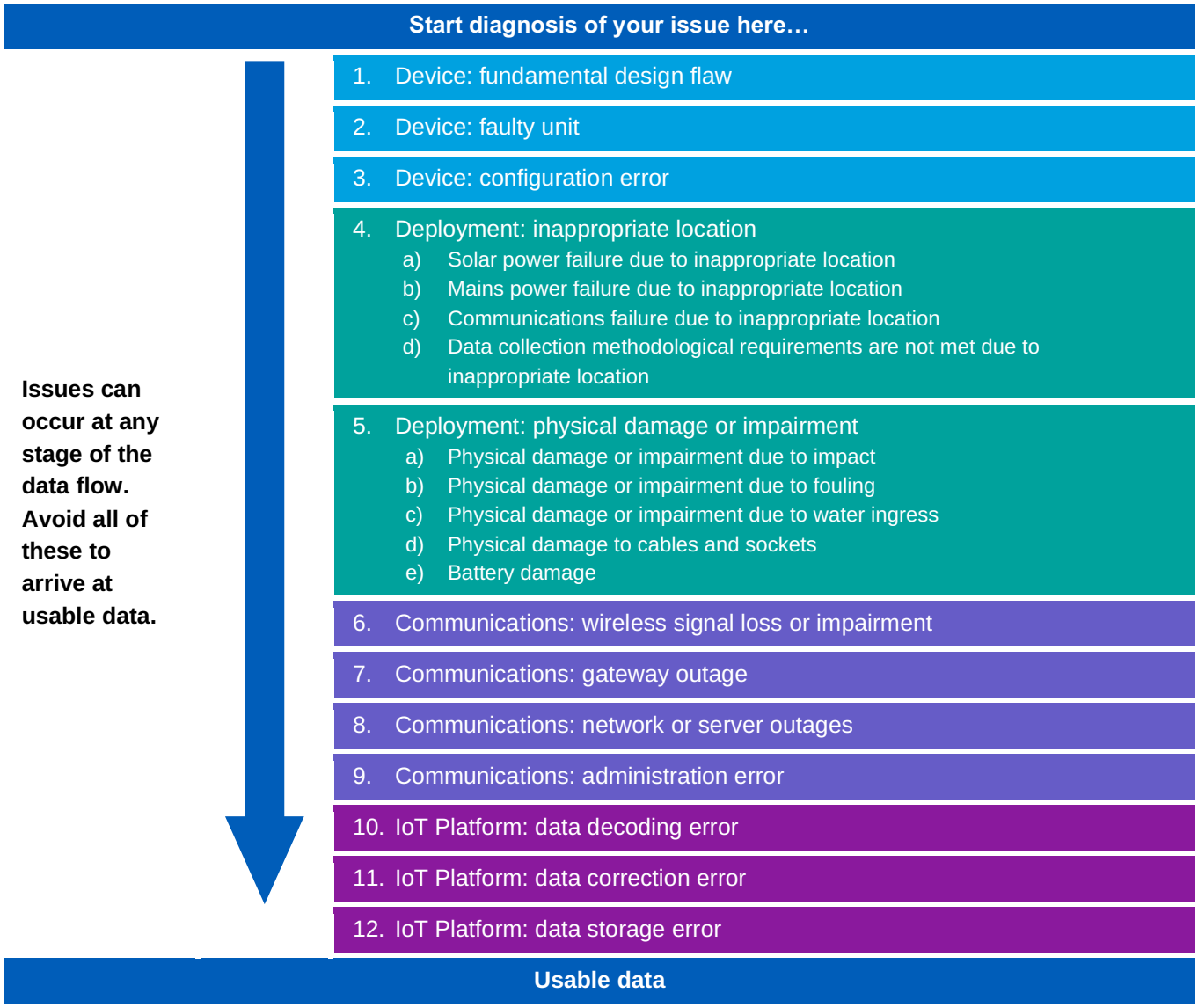

Figure 1. A troubleshooting framework for diagnosing issues associated with the use of smart low-cost sensors for the collection of usable data

Troubleshooting diagnostic process flow chart

Use this flow chart (Figure 2) to help narrow down which issues (of the identified types 1-12 in Figure 1) you might be facing.

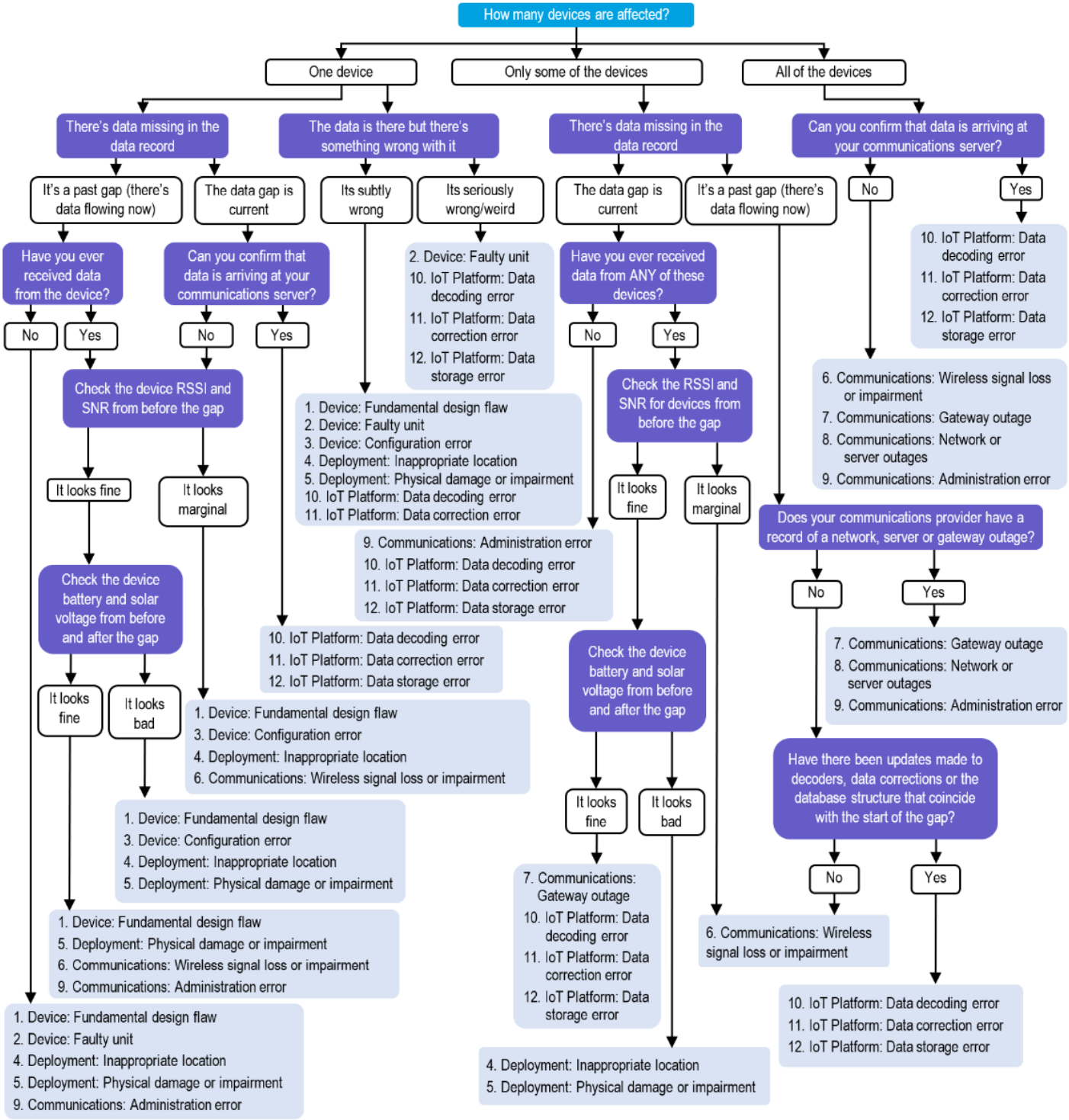

Figure 2. Process flow chart for troubleshooting diagnosis

A detailed typology 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.

What does this look like?

This issue can impact data quality and a diverse range of device functions, meaning that there are no clear symptoms.

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.

How can you mitigate this risk?

This risk should be addressed during the technology procurement stage. You should be clear about the specific needs of your project, in terms of data quality and practical requirements. You can check the track record of devices: 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.

2. Device: faulty unit

What is happening?

A specific device may have a fault, either physical (hardware) or in its programming (software).

Examples of hardware faults include:

- a damaged seal that leads to water ingress
- a fault within a specific electrical component
- damaged wiring
- a device that is wired incorrectly due to human error during assembly.

Some examples of software faults include:

- an error occurred when the device had its firmware uploaded, resulting in incomplete flashing
- a bug in a firmware update that impairs functionality.

What does this look like?

Generally speaking, these types of fault result in a loss of signal from a device, due to it becoming inactive. In cases with firmware bugs, data may arrive but look extremely strange, or fail to be correctly interpreted.

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.

How can you mitigate this risk?

This is a quality control concern for the vendor. The only way to mitigate this risk is to choose a product or vendor with a highly regarded profile and good testimonials. Pay attention to warranties, and be clear about what they do and do not cover. For larger networks, it is a good idea to include a support package as part of an ongoing service agreement. This might include a 'return to base' service, where faulty devices can be assessed and refurbished by the vendor.

3. Device: Configuration error

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.

The main configurable device settings to be aware of are:

- **Reporting interval:** The period between data reports sent by a device. This can generally be altered to meet the needs of your project. Shorter reporting intervals provide higher definition data, however, this increases power demand, which can lead to power loss issues or shortened battery life.
- **Sampling rate:** The period between sensor measurements taken by a device. One transmitted data report may be calculated from many samples. For example, a device might sample every two seconds, then transmit a reading every 15 minutes that is formulated as a mean of 450 samples. Only some devices have configurable sampling rates.
- **Calibration settings:** These will vary by device and sensor types, but relate to the processing of raw sensor data within a device. They can subtly impact data quality.
- **Communications settings:** The types of communications settings that can be configured will vary by device and communications type. Most of them boil down to altering the balance between how likely a device is to maintain reliable communications on the one hand, and power management on the other. Common communications settings include transmission power

(basically, how loudly the device communicates), and spreading factor (basically, how many times the device repeats its message in a given transmission). Maximising these settings will increase the reliability of communications in a marginal location, but also increase power demand, which can lead to power loss issues or shortened battery life.

What does this look like?

Inappropriate device configuration can result in a wide variety of issues, meaning that there are no clear symptoms that indicate it. Poor configuration of communications and basic device functionality tends to impact the reliable transmission and capture of data packets (i.e. you will see a loss of communications, or very intermittent data capture).

Settings that relate to data collection (e.g. sampling rate and reporting interval) will impact data quality. Data quality can only be assessed relative to your data use case – the data either supports or does not support your use case. For example, a sampling rate that is too low may result in more 'noisy' data (i.e. greater standard deviation around your average).

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.

How can you mitigate this risk?

You should take the time to understand your data requirements (e.g. reporting interval) and the practical constraints of your network design (e.g. communications 'black spots' in an inner city environment), and discuss these with your technology vendor, who should be able to help you optimise configurable settings on your devices to ensure reliable functionality in your chosen environment. A vendor should be an expert in configuring their own device for optimal performance, so this is something that you need to feel confident about at the point of procurement.

4. Deployment: inappropriate location

There are several types of issues relating to the inappropriate location of a device:

a) Solar power failure due to inappropriate location

b) Mains power failure due to inappropriate location

c) Communications failure due to inappropriate location

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

4a) Solar power failure due to inappropriate location

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. This can be broken down into sub-issues:

- The location may receive too much shade at certain times of the year (e.g. during winter months, when the sun is low in the sky and days are short; or during summer months, when deciduous tree canopies create shade).
- The optimal aspect for the solar panel is not practically achievable (e.g. another piece of infrastructure, such as a street sign, is positioned on the north side of a street pole, meaning that the solar panel cannot be pointed north). Aspect can have a significant impact on panel function.

What does this look like?

A device suddenly ceases communication, either indefinitely, or for a period of many days or weeks. In some cases (generally dependent on the design of the system[1]), the device may come back online. During a rainy winter, you may see multiple offline periods or 'long-period intermittency' in your data.

The first thing to check to confirm this issue are the records of battery and solar voltage in your data record for the period leading up to loss of communications. Devices have a lower threshold for battery voltage, below which they will cease to function (check with your vendor to confirm what this is). If solar power failure is your issue, you will see a rapid decline in battery voltage, and some evidence of reduced panel voltage across the same period. Note that even a relatively small reduction in panel voltage over the period of a week or so can be enough to push battery voltage below the critical threshold.

This problem may overlap with solar panel fouling, where dust, snow, bird droppings, or leaves obscuring part or all of the panel cause a significant drop in its performance. It is possible for fouling to occur in summer months and not cause power loss, only for it to become a problem over the winter when the days are shorter and the sun is at a lower angle.

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? A panel that has good morning sun exposure but poor afternoon exposure can be offset to point north-east, maximising exposure to the available morning sun. You may need to look at rearranging the configuration of other items on the pole, or shifting your device to a different height, to achieve the optimal aspect. Even a small increase in daily solar exposure may be enough to fix your issue.

[1] Devices with battery protection and the ability to automatically re-establish a communications network connection are generally able to come back online following critical power failure without any manual intervention.

- **Move the device.** If optimising panel aspect is not enough, consider options for a nearby location that has more solar exposure. For cities with 3D digital twins, you may be able to directly model this. Be careful that you do not compromise your study requirements by shifting the data collection location too far from your point of interest.
- **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. A larger battery can store more solar power and allow the device to operate for a longer period with low solar exposure. A larger panel can ensure complete recharging over a shorter exposure period.
- **Shift to mains power.** A final option is to shift to mains power for more reliable supply. Check its availability at the existing location, and speak with your device vendor to see if this can be supported.

How can you mitigate this risk?

You should also consider shaded locations combined with overcast weather and mid-winter sunlight. To mitigate the risk of solar power failure, ensure that the solar panel and battery system are designed with appropriate tolerance (e.g. that a fully charged battery can power the device for at least three days without a recharge; that the battery can fully charge with no more than three hours of direct sun exposure, etc.).

It is also advisable that a solar-powered device has inbuilt battery protection that causes the device to shut down before battery levels drop too low and cause irreparable damage to the battery. Most well-designed solar-powered devices should have this feature.

Try to think through your solar power needs as early as possible, so that you can discuss them with your chosen device vendor during the procurement process.

Note that 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. Another approach is to ensure that a process is in place to reset devices in such circumstances, and to verify restored functionality.

4b) Mains power failure due to inappropriate location

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.

What does this look like?

This issue will most commonly appear as a periodic loss of communications from a device during daylight hours, with normal functionality resuming each night (though the pattern will vary depending on when power is actually supplied).

Some devices are not able to automatically recover from unexpected power failure, which would result in complete loss of communications with no resuming activity.

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 streetlamp is turned on), and discharging the battery during the day.

How can you mitigate this risk?

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 from the start.

Note that 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 restore themselves, though this may limit you to the more costly end of the spectrum of low-cost devices. Another approach is to ensure that a process is in place to reset devices in such circumstances, and to verify restored functionality.

4c) Communications failure due to inappropriate location

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.

Regardless of the communications technology used, the viability of communications coverage is determined through a combination of signal strength (RSSI) and signal-to-noise ratio (SNR).

- RSSI is impacted by distance from a communications gateway, as well as by line of sight. Depending on the technology used, certain radio frequencies can also bounce off or pass through buildings and trees, though all are blocked entirely by topology.
- SNR relates to the volume of the communications signal relative to the radio background noise, which tends to be higher in urban areas.

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. Adverse conditions can include rainy weather, wet tree canopies, heavy smoke, and busy traffic. There can also be seasonal variation associated with a signal being blocked by summer plant foliage.

A final consideration is the aspect of the device antenna relative to the nearest gateway. For a device positioned close to a large pole, particularly one made from a dense material such as concrete or steel, the pole itself may physically block line of site between the antenna and the gateway. This can occur in an otherwise viable location.

What does this look like?

If a device is installed in a location where the communications coverage is unviable, or the position of the device is causing the signal to be blocked, then you will likely never receive any data from it. You should

go to the location, and conduct a field check for RSSI/SNR using a separate device of the same model to verify this diagnosis.

A device that initially connects but subsequently suffers a communications failure will show a sudden cut-off in the data record, with no apparent voltage issues in the lead-up (such as you would see associated with power failure). The thing to check here is the record of RSSI and SNR in the data record. First, assess these metrics for the entire period that you do have data for. If it looks like the device was operating at marginal levels under normal conditions, then the likelihood that you are now dealing with a communications issue is quite high. Again, a field test of RSSI/SNR is the best approach for diagnostic verification.

Consider weather conditions and the time of day, in case periods of communications loss align with poor weather or heavy traffic. Note that devices can vary in their sophistication: some are able to re-join the communications network automatically after losing connectivity; others are not, meaning that they may stay offline even after the conditions that caused the drop-out have ended. You should be able ask the device vendor about this.

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 boost its transmission power and/or its spreading factor. In simple terms, transmission power can be thought of as how loudly a device shouts its message. The spreading factor can be thought of as how many times (in close succession) a device shouts the same message, which increases the likelihood of it being detected. There are upper limits to both of these settings, and maximising either one of them can have a significant impact on the battery life of a device. For this reason, the aim is always to optimise them for a given location, ensuring that communications are reliable without draining the battery too quickly.
- **Move a device to a new location that has better signal coverage**. This may compromise the data use case and should be carefully considered.
- **Install an additional local communications gateway** to improve signal coverage at the location. This is the costliest option, and only tends to make sense if you are dealing with a large number of devices with communications coverage issues. Note that it is inadvisable to move an existing gateway once it is deployed and you have multiple devices already using it, because there is a high chance that this will create communications coverage issues for other devices.

How can you mitigate this risk?

There are several actions that you can take to mitigate communications coverage issues:

- **Procure communications technologies that are appropriate for your spatial context.** You need to understand your spatial context, and the sorts of challenges that 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’. Your data use case will determine how you need to deploy devices within this context. Communications technologies vary in their coverage, range, and ability to penetrate physical barriers (e.g. tree canopies). You

need to ensure that you choose a communications technology (and corresponding devices) that are appropriate for that context.

- **Ensure you have enough gateways.** It is important to ensure that you have enough gateways to service your study area. It is strongly advisable to have at least two gateways to provide stereo coverage to a majority of your deployment locations, particularly for larger networks (>10 devices). 3G/4G/5G and NBIoT communications in more urban settings tend to have very dense coverage, essentially eliminating this concern. Private local networks (e.g. LoRaWAN or SigFox) rely more on your ability to invest in multiple gateways.
- **Optimise your hardware for marginal communications.** It is possible to optimise your hardware to support devices in locations with more marginal signal. 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 down). You can also optimise device configuration (specifically, transmission power and spreading factor), as already discussed.
- **Conduct on-the-ground signal testing to support your network design process.** Your chosen technologies place constraints on the reliability of device communications in any given location. You should design device network deployments to avoid marginal signal locations. To achieve this, ensure that you undertake thorough on-the-ground signal testing of planned deployment locations prior to device deployment, allowing you to avoid later issues.

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.

There are a large number of considerations relating to this issue, and each use case is different. However, the most common considerations are as follows:

- **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). Materials such as concrete, brick, and steel can pose greater problems in this regard, particularly if 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.
- **Wind fetch.** Another consideration relates to the positioning of wind sensors, which are often integral to an air quality monitoring network. Accurate wind measurement requires a minimum 'fetch,' or distance, that air can move uninterrupted before it hits a wind sensor. There are fixed standards about this for meteorological monitoring, *if* the aim is to record wind speed and

direction that is representative of the general area. However, it should be noted that some data use cases might call for such methodologies to be sidelined. For example, if you wanted to monitor wind in a street canyon, you would – by definition – need to ignore meteorological standards. The bottom line is that the location you choose should meet the needs of your chosen data use case.

What does this look like?

This type of issue can be subtle, difficult to spot, and quite varied in nature. You are unlikely to detect anything from basic visual observation of your data. Statistical analysis is generally required.

One common symptom of deployment methodology issues is a systemic bias in data from one device, relative to mean values taken from multiple other devices in the same area, or in similar deployment contexts. Care should be taken here to distinguish between variations that arise from a genuine deployment issue, and variations that represent a 'true' phenomenon. For example, a roadside sensor mounted on a large steel street pole might report average temperature as two degrees warmer than a sensor in a nearby park that is mounted on a large wooden telegraph pole. You should check that this difference represents a genuine variation in localised ambient temperature, and is not just a result of the roadside device picking up thermal radiation from the steel pole. It may be a combination of both effects, and it can be quite difficult to discern precisely what is occurring.

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.

How can you mitigate this risk?

Mitigation of methodological issues relating to the deployment of your devices relies upon careful and thorough planning of your device deployments:

- **Understand your data requirements.** You must start with a clear understanding of your data use case, which will dictate the attributes of the data you need to collect. You can then develop a deployment methodology that supports those data requirements. Bear in mind that a variety of practical constraints tend to force a degree of compromise on deployment methodology, away from what might be considered a perfect ideal. Your aim should be to find a pragmatic balance between the practical and the ideal that still serves your data use case.
- **Devices that support methodological requirements.** A variety of procurement decisions relating to the design of devices can help to mitigate common sorts of methodological issues, and may be thought of as ways to offset practical constraints of deployment locations. 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.

5. Deployment: physical damage or impairment

Physical damage to (or impairment of) a device can occur in several ways:

a) Physical damage or impairment due to impact

b) Physical damage or impairment due to fouling

c) Physical damage or impairment due to water ingress

d) Physical damage to cables and sockets

e) Battery damage.

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.

What does this look like?

Damage caused by impact can result in a variety of symptoms in the data feed:

- **Loss of communications with no prior symptoms**. While this may be attributed to other power supply issues, or to a broader issue with the communications network, it may also result from direct physical damage to communications hardware (e.g. the antennae, or the communications module).
- **Loss of some but not all telemetry**. This can result from damage to one particular sensor, where the main body of the device remains undamaged. The likelihood of this occurring increases for devices that have sensors deployed as separately mounted external units to the main device.
- **Sudden loss of solar panel power, followed by slow decline of battery voltage, then communications loss**. Most solar-powered devices should report panel voltage as part of their standard telemetry. Even relatively small amounts of damage to a panel can be enough to compromise their operation.
- **Sudden loss of communications, caused by loss of mains power**. While this can be attributed to power supply being turned off, it may also result from physical damage to power cables.

You will need to conduct a physical inspection of a device to verify any diagnosis.

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 entire device back to your vendor for refurbishment.
- **Replace the entire device with a new unit**. This is the more costly option. If you lack spare devices in stock, you may also face a procurement period of weeks or months while you wait for the replacement device to arrive, which could impact your data use case.

How can you mitigate this risk?

Mitigation of this risk all relates to how a device is deployed. Ideally, these decisions should be made when a device is first deployed, however, you may also make changes to a deployment following an incident to avoid future damage. The following tips should assist you:

- 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.
- Make devices as inconspicuous as possible in locations where vandalism is a concern. A simple approach can be to 'hide' a device on the far side of a pole, relative to the main angle from which it would be viewed.

5b) Physical damage or impairment due to fouling

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. Here are some tips to consider for each type of fouling:

- **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 the accuracy of a sensor and ultimately renders it unusable. Ironically, this tends to occur in the most polluted environments, where reliable sensing is likely to be most valued.
- **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.

What does this look like?

Fouling can result in the following common symptoms:

- A complete loss, or dramatic reduction, of solar panel voltage output.
- A concurrent decline in battery voltage, perhaps over several days or weeks, ultimately resulting in a loss of communications.
- A slowly building bias or inaccuracy in sensor telemetry, evident over many months (this is especially the case when there is particle deposition within a sensor, or obstructed ventilation).

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.

How can you mitigate this risk?

You can mitigate the risk of fouling in the following ways:

- **Schedule regular maintenance.** To detect fouling before it starts to impact your data, 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. You might also have a service agreement with your device vendor for periodic cleaning and refurbishment of devices, which could include installation of new sensor components.
- **Build redundancy into the design.** If you anticipate issues with panel-fouling from the start (e.g. you know that there will be a lot of leaves falling in the autumn), you can choose to use a larger size of panel that has higher margins of tolerance for loss of exposed area. Likewise, you may choose to upgrade a panel to a larger size if panel-fouling proves to be a recurring issue. If bird droppings are a concern, installation of bird spikes may be helpful. Another way of increasing the tolerance of your solar battery system to periodic loss of panel exposure (e.g. from snow or frost) is to use a larger battery that is able to supply power to the device for a longer period before needing a recharge.

5c) Physical damage or impairment due to water ingress

What is happening?

Water ingress refers to any situation where water enters areas of a device where it should not be, usually resulting in permanent physical damage to circuitry and components. Water can create a short in a live circuit, causing localised heat that literally ‘fries’ the fragile electrical components. Water can also cause corrosion of metal, aided by the flow of current.

Water ingress 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.

What does this look like?

Water ingress can result in the following common symptoms:

- Rapid decline of battery voltage, followed by a complete loss of communications that is indicative of the device losing power. This decline would occur against a normal fluctuation of solar panel voltage (if solar is featured).
- Water ingress may also impact a single component. For example, a modular sensor, mounted external to the main device, might suffer water ingress and cease functionality, while the main device continues to function. This would appear as null or zero data reported against telemetry streams associated with that sensor.

It should be noted that visible signs of water ingress can be delayed for weeks or months after deployment of a device. This is because water ingress may take a while to build up to a critical amount that impairs device function. You may also have an issue, such as a damaged seal, that is not a problem during dry weather. It might take six months until a device first experiences heavy rain, and only then will the issue manifest.

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.

How can you mitigate this risk?

You can mitigate against the possibility of water ingress in the following ways:

- **Understand IP ratings.** Pay close attention to IP rating during procurement. This is a global standard that relates to the ability of a device to withstand water ingress. IP ratings are expressed as two numbers, the second of which denotes resistance to water. A water resistance rating of 5 or higher ensures that a device can withstand strong rainfall. Many low-cost sensors have water resistance ratings of 7, which indicates they can withstand full, immersion in water up to 1 metre deep for 30 minutes.
- **Support thorough training of device assemblers and installers.** The most common cause of water ingress is human error, as opposed to poor design or low water resistance. This error tends to occur when seals are being broken and re-established, such as when a battery housing is replaced, or a cable is connected into a socket. The way to mitigate human error is to support 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.

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.

What does this look like?

In cases where cables or sockets are damaged during assembly or installation, the device will never activate or send data, due to a lack of power or data connection.

Routine inspection that involves temporary removal and replacement of a device or device components can result in cables or sockets being damaged. If a device suddenly stops working following an inspection, with no evidence of battery voltage decline or communications issues prior to communications loss, then cable or socket damage is a strong possibility.

In cases where the damage impacts the connection of an external modular sensor into a main device, loss of telemetry from that sensor will result. This might manifest in data reports as zero or null values, or as a flatline improbable value.

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.

How can you mitigate this risk?

You can mitigate the risk of physical damage to cables and sockets in the following ways:

- **Support thorough training of device assemblers and installers. As** with water ingress, the principal way to mitigate damage to cables and sockets is to support 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 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.
- **Choose robust products.** Your choice of product is a major factor in mitigating the risk of cable and socket damage. Some low-cost sensing devices are designed more robustly than others,

with fewer parts able to break or be incorrectly assembled. It can be difficult to determine this type of product quality during procurement. The best advice is to seek testimonials from other users of the product, and reach out to them to check things like the design and build quality, as well as asking whether they experienced any issues with poor-quality design, or flimsy components.

To protect cables from damage by birds, you can encase them in robust conduit. You may also be able to design custom mounting brackets that protect sockets from direct access. Anti-bird spikes may 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. Different types of batteries have different DoD limits. For example:

- Lead-acid batteries (which are large, heavy, and generally only used to support larger, high-performance devices or weather stations) have a DoD limit of around 50%. This means that you should always have the battery at least half-full to avoid permanent damage to the chemical cells.
- Lithium-ion batteries (which are lightweight, energy-dense, and used in many low-cost sensing devices) and nickel-cadmium batteries (which are heavier than lithium-ion batteries, and also widely used for low-cost sensing devices) both have a DoD limit of around 80-90%. This means that far more of their power can be used up before they run the risk of permanent damage.

Regardless of the DoD limit, if it is exceeded, you could experience 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.

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
- short day length in mid-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. In most cases, assuming a 24-hour charge cycle, a battery will function effectively for at least as long as the other components in a device. This means that concerns about rechargeable battery life are generally irrelevant because other, more

critical, parts of a device are likely to start failing before the battery becomes a problem. However, 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.

What does this look like?

Battery damage can result in the following common symptoms:

- Battery voltage drops past a known lower threshold, with the device going offline shortly afterwards. The threshold will vary by device, based on battery type. Device drop-out due to battery discharge does not necessarily indicate permanent battery damage.
- Following device drop-out, a failure to come back online after power supply to the battery is restored (e.g. following a week of good solar exposure) strongly indicates permanent battery damage.

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.

How can you mitigate this risk?

You can mitigate against battery damage in the following ways:

- **Invest in built-in power management and battery protection.** Devices that feature rechargeable batteries should have built-in power management and battery protection functionality. This is an automatic system that shuts down a device before a depth of discharge limit is reached, preventing battery damage from occurring. Smartphones, laptops, and well-designed sensing devices have this technology as standard. Unfortunately, some low-cost sensing devices lack this technology, or if they do have it, it is not effective or optimised. Power management and battery protection should be on your list of technical requirements to inform your procurement of sensing devices.
- **Set up automatic threshold alerts.** An operational mitigation approach involves the use of battery voltage threshold alerts, where a platform alerts you to an issue before it becomes a permanent problem. This requires you to have an IoT platform that can set automatic thresholds relative to device telemetry, and can issue alerts when thresholds are breached. In this case, you need to determine a lower voltage threshold for your device, which should be set slightly above the DoD limit for the battery used. This will warn you when a DoD limit is at risk of being breached. You can then try to work out why power supply to the battery is dropping, which may include a field visit (e.g. allowing you to fix issues with a solar panel).

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**, usually due to some kind of physical blockage of signal in line of site between a device and a gateway. The causes of such a blockage may include:
    - **A new building or other large structure** appears between the device and the gateway. This is generally along a line of site. However, in some inner-city locations, 'normal' signal connection may occur by bouncing off buildings, which means that a blockage may not be in line of site and is impossible to identify.
    - **Summer vegetation growth** (notably deciduous tree canopies) can block wireless signal, particularly in cases where devices and communications gateways are deployed at lower heights.
    - **A small, localised, fixed blockage near the device**. For example, a large new sign installed on the same pole as the device may be positioned such that it blocks the wireless signal.
    - **A small, localised, fixed blockage near the gateway antenna**, caused by installation of a new physical object that creates a radial 'blind spot' in a certain direction (think of this like a whole arc of the compass being knocked out for that gateway's connectivity).

- **Adverse weather**. Rain can attenuate signal strength through the air, particularly for low-power technologies like LPWAN. It can also create wet vegetation that forms a physical barrier, and blocks communications signals.
- **Heavy city traffic** can result in intermittently blocked signal over rush hour periods.

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.

What does this look like?

Complete wireless signal loss results in a complete loss of communications from your device. Impaired signal results in an intermittent data record that is full of gaps (a 'Swiss cheese effect').

Most devices report signal strength (RSSI) and signal-to-noise ratio (SNR) as part of their standard telemetry. Root causes of wireless signal loss can occur suddenly, leaving no trace of issues in the telemetry record. However, there is a good chance that you can see reduced RSSI and/or SNR in the telemetry record leading up to signal loss or a period of intermittency. This data is the strong indicator of a wireless signal issue.

Complete loss of communications and intermittent communications can both occur as a result of power supply issues, as already discussed. It is therefore helpful to confirm that there are no abnormalities in solar panel or battery voltage in the lead-up to the core symptoms you observe.

This issue also tends to impact devices individually, except in case of adverse weather and heavy traffic (which can impair signal strength for all devices in a network for the period where changed conditions occur). If you have no adverse conditions, and you are seeing multiple devices lose signal or suffer highly intermittent signal, then the chances are good that you are not looking at a wireless signal issue, but an issue further up the data stack (which will be discussed in a later section of this guide).

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 (e.g. move a sign further up a pole so that it is no longer right in front of your device). It will likely be impossible for blockages occurring elsewhere in the urban environment (e.g. a new billboard), or for environmental causes (such as weather). Likewise, increased signal noise tends to result from technologies over which you have no direct control.
- **Move the device.** If you can't remove a blockage, move your device so that the blockage is no longer a problem. This may be as simple as a small adjustment (e.g. move the device one metre up a pole), or it may require a whole new location. This may not be an ideal solution because it can be time-consuming and costly, and it may negatively impact your data use case (e.g. you might need the device to remain in its current location because you need to collect data there).
- **Reconfigure the communications settings on a device** to boost its transmission power and/or its spreading factor. In simple terms, transmission power can be thought of as how loudly a

device shouts its message. The spreading factor can be thought of as how many times (in close succession) a device shouts the same message, which increases the likelihood of it being detected. There are upper limits to both of these settings, and maximising either one of them can have a significant impact on the battery life of a device. For this reason, the aim is always to optimise them for a given location, ensuring that communications are reliable without draining the battery too quickly.

- **Raise the height of an existing private gateway, using a mast**. The height of a gateway can make an enormous difference to signal coverage, particularly in cases where signal blockages are occurring at a fairly low level in the urban environment (e.g. summer vegetation growth). Installing a mast generally requires engineering design and approvals, and installation can be costly. The cost of such an upgrade should be weighed against the cost of installing an additional gateway elsewhere.
- **Install an additional private communications gateway** to improve signal coverage at the deployment location. This is a costly option, and only tends to make sense if you are dealing with a large number of devices with communications coverage issues. Note that it is inadvisable to move an existing gateway to a new location once it is deployed and you have multiple devices already using it, because there is a high chance that this will create communications coverage issues for other devices.

How can you mitigate this risk?

There are several actions that you can take to mitigate the risk of wireless signal loss or impairment:

- **Procure devices that use communications technologies with a high tolerance to changing local conditions.** Communications technologies vary in their ability to penetrate physical barriers (e.g. tree canopies, walls, vehicles), bounce off solid surfaces (i.e. lower dependence on line of site), and be heard above background noise (e.g. low-powered communications technologies like LoRaWAN are more susceptible to low signal-to-noise ratio than 4G). 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. If your use case demands it, you may wish to offset this risk by choosing technologies that have higher tolerances to changing conditions.
- **Ensure that each device is serviced by at least two gateways.** This is called the ‘stereo gateways rule’, and ensures redundancy at the level of wireless signal coverage. 3G/4G/5G and NBIoT communications in more urban settings tend to have very dense coverage, essentially eliminating this concern. Private local networks (e.g. LoRaWAN or SigFox) rely more on your ability to invest in multiple gateways.
- **Ensure that private gateways are installed in an optimal position** that maximises their coverage. If your device network uses private gateways for communication (e.g. Wi-Fi, LoRaWAN, or Sigfox), choose gateway deployment locations that are as high as possible off the ground. The rooftops of tall buildings that are owned by your organisation, or by a close partner, are ideal. Aim to install a gateway on as tall a mast as possible. Ensure that a gateway antenna is not obstructed by any nearby objects, including the mast itself (the antenna should protrude

above the top of the mast). Your gateway vendor should provide detailed guidance for optimising installation.

7. Communications: Gateway outage

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** (a limited offline period that should be planned for ahead of time).
- **Loss of power** to the gateway due to accidental shut-off of the mains supply circuit. For gateways powered by solar-battery systems, power loss can result from physical damage or fouling of a solar panel or power cables, or from reduced solar exposure due to short days, cloudy weather, or increased shade.
- **Physical damage** (e.g. water ingress, lightning strike, hail, bushfire, birds, or vandalism). Poor gateway design or build quality increases the risk of this occurring.
- **Changes to gateway firmware** that cause the gateway to lose connectivity. This may be due to an incomplete firmware update, or a bug associated with a firmware update.
- **Changes to server settings** that cause the gateway to lose connectivity with the server.
- **Suspension of service** due to unpaid invoices.

What does this look like?

A gateway outage may result in some or all of the devices in your network losing connectivity at the same time, or reporting intermittently.

A small network that uses a single gateway will see a global loss of communications from all devices.

For networks that use multiple gateways, a single gateway outage may not cause widespread loss of communications across your whole network. However, it may still result in the following symptoms:

- A single gateway outage can lead to a loss of stereo coverage for some devices. If a device is suddenly reliant upon a single gateway for reliable communications, it may become susceptible to intermittent data reporting, particularly if its connection with the remaining active gateway is marginal. This intermittency may be evident in a cluster of devices in close proximity.
- Outlying areas of your device network may be serviced by single gateways. A gateway outage would cause complete loss of communications for multiple devices in these areas.

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.

NOTE: Some gateways may not be sophisticated enough to automatically resume standard operations once the cause of an outage is resolved. This may mean that the outage continues until more active measures are taken. You may need to engage your communications service provider for assistance.

How can you mitigate this risk?

There are several actions that you can take to mitigate the risk of gateway outages and their impact:

- **Invest in quality hardware.** If your chosen sensing devices require you to invest in private local communications gateways, procure high-quality products with a proven track record.
- **Install multiple gateways for redundancy.** According to the 'stereo gateways rule', multiple gateways reduce the chance of completely losing communications with some or all of your devices.
- **Check if there are service level agreements (SLAs) in place.** These are legal agreements with communications providers to provide a guaranteed minimum level of service. If an SLA is available, it means that your service provider is doing everything they can to reduce the chances of gateway outages, which removes the responsibility from you. SLAs are only available with some technology options – for example, you can get an SLA with 4G, but not with LoRaWAN. You will pay more for a service with an SLA.
- **Run private gateways with managed services and active support.** You can buy, install, and manage private gateways yourself (the lowest-cost option), or you can buy gateways and establish a managed service contract with a communications provider. A service contract should include active monitoring of your gateways, meaning that you will be alerted as soon as an outage occurs, helping you minimise any data loss. The service should also include active troubleshooting support to get things back on track.
- **Take practical measures to prevent loss of power.** Accidental shut-off of mains power is a common cause of gateway 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 saying 'DO NOT SWITCH OFF', and including a contact phone number). The risk of loss of solar power or battery damage can be mitigated through a variety of measures, as already discussed.

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

8. Communications: network and server outages

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 causes a loss of data for the period that the outage occurs. A server outage may result from:

- **Planned or unplanned maintenance and updates**, including software updates to the server or other network architecture, and network hardware upgrades (above the level of individual gateways).
- **A programming error or misconfiguration** of the server made by the service provider.
- **Power failure** to the server (this is only a factor for servers that are physically based in a single location, as opposed to virtual, cloud-based servers).
- **Server resource consumption** (i.e. data storage and processing) exceeding capacity as a result of poor management.
- **A cybersecurity attack** that targets and compromises the network or server.

NOTE: Updates to a communications network or server may confuse the devices that connect to it, requiring them to be manually reset or updated. If this follow-up is not done, then you may see devices locked in an offline state, even after network communications are restored.

What does this look like?

A network or server outage will result in a complete loss of communications from all devices in your network, with no prior indications of an issue (unless you are informed of scheduled downtime for maintenance purposes).

It is not uncommon for an outage to occur without you being aware of it at the time. If you see a universal gap in your data record, you should contact your communications service provider. They should be able to confirm if the data gap coincides with a known network or server outage.

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.

How can you mitigate this risk?

There are several actions that you can take to reduce the risk of network or server outages, or to reduce their impact if they do occur:

- **Use a dedicated private communications server**. Many communications service providers have commercial options for 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 less scheduled downtime, and can mitigate against the risk of cybersecurity attacks and overconsumption of resources.
- **Use a communications server that is cloud-based**. This removes the risk of an outage due to power failure, because cloud-based hosting is not reliant upon any single location.
- **Check if service level agreements (SLAs) are in place.** These are legal agreements with communications providers to provide a guaranteed minimum level of service. If an SLA is available, it means that your service provider is doing everything they can to reduce the chances of network and server outages. SLAs are only available with some technology options – for example, you can get an SLA with 4G, but not with LoRaWAN. You will pay more for a service with an SLA.

9. Communications: administration error

What is happening?

An administration error relating to the connection of a device with a communications server can result in a device failing to communicate. To understand what is happening in this case, we must first review how a device is registered to communicate with a server.

A device is programmed with a specific address and access key that are unique to a dedicated application within a user account on the communications server. A unique identification code for the device is, in turn, registered within the server application, meaning that the application can recognise and form a connection with the device. This kind of connectivity relies upon the correct information being entered at both ends of the system (in the device, and in the server), and applies to all communications technologies that are commonly used to support IoT devices. It is possible for the server application address and access key to be incorrectly entered into a device. It is also possible for the device identifier to be incorrectly entered into the server. In either case, the result is a failure of a device to connect with the server.

Another possibility for an administration error is at the level of an IoT platform, which is the next level up from the communications server in most data architectures. Each device in a network is registered as a

virtual object within an IoT platform. That virtual object is associated with the device's unique identification code, and with an address and access key for the communications server application with which the device is communicating.

If any of these details is incorrectly entered in the IoT platform, then the platform will be unable to form a connection with the device in the communications server, and no data will flow into the platform. If the error lies in a device identification code, only the connection with that device will be affected. However, if the server application address and application access key are incorrectly entered, then no data from any devices in the network can reach the IoT platform.

What does this look like?

Administration errors that affect communications are an all-or-nothing affair: either everything is perfect, or the smallest error at any point in the system results in a complete loss of connection.

All of these kinds of administration errors tend to be the result of manual human error made during the initial set-up of a new device network. They are generally the fault of the person who managed the onboarding of devices (usually the device vendor). You are most likely to identify this type of error during acceptance testing of a device, a critical step in the activation and deployment process (please see the OPENAIR Best Practice Guide chapter *Air quality sensing device activation and deployment* for further information).

Errors can also occur during network operations as a result of maintenance updates at the level of a device, communications server application, or IoT platform (e.g. if the update accidentally resets or erases critical information). This will then manifest as loss of communications with a device.

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.

How can you mitigate this risk?

Fundamentally, mitigation of the risk of human error comes down to having a clear and rigorous process, and ensuring that everyone on the team is familiar with it, and agrees to follow it.

- **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.

- **Establish your own device onboarding process**. If you opt for a more in-house approach to device registration and onboarding, you should write up a detailed, step-by-step plan 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. 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.

10. IoT Platform: data decoding error

What is happening?

Sensor data arriving in an IoT platform will be in a raw and relatively unprocessed format[2]. Raw data needs to be 'decoded' to unpack various separate pieces of information, and make it more human-readable and shareable. Decoding occurs within the IoT platform, usually with a dedicated decoding module assigned to each device type (make/model/version) in a network. It is possible for this decoding to go wrong, resulting in either a failure to decode, or incorrect decoding.

A data packet that is received from a device comprises a string of compressed information. 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. Environmental telemetry received in this way then needs to be interpreted, from some internal reference value (often a voltage reading specific to a particular sensor) into a universal unit of measurement associated with that telemetry (e.g. '°C' or 'micrograms/m^3').

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

- **Error at setup.** The decoding module can be incorrectly set up from the outset, meaning that all devices of a certain type will share the same problem.
- **Firmware update error.** 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.
- **Platform update error.** Updates made within an IoT platform can also impact decoders (either their internal functionality, or their integration with the platform itself).

What does this look like?

The outcomes of data decoding errors can include:

- **No decoding occurs** (no data is visible within the IoT platform).
- **The data packet is incorrectly 'sliced up'** into its constituent sections of information. For example, the order of appearance in the data packet might be mixed up, so that the data section

[2] Noting that the amount of data pre-processing at the level of the communications server will vary by technology and vendor.

relating to humidity is assigned to temperature, and the data section relating to temperature is assigned to humidity. It is even possible to mix parts of two adjacent data sections together. These types of error can produce highly incongruous telemetry outputs.

- **A section of a data packet can be incorrectly interpreted** (e.g. a misplaced decimal place could present 'parts per billion' as 'parts per million'), resulting in telemetry outputs that may be outside of an expected range by orders of magnitude.
- **Failure to store decoded data.** A decoder might be correctly selecting and interpreting data, but failing to deliver the output to the platform (due to a bug in its code that impacts its functionality or integration). No data will be stored or displayed.

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.

How can you mitigate this risk?

One way to mitigate this type of risk is to choose a single, proprietary-managed sensing solution, where one provider manages all devices, decoders, and your IoT platform. However, such a choice has a long list of pros and cons associated with it, and is one of the major decisions for your ongoing business case and smart city strategy. It is by no means a simple mitigation decision.

If you choose a more modular, integrated technical solution (where you are connecting devices from one or more manufacturers into a platform from a separate provider), there are measures you can take to mitigate against the risk of decoder errors:

- **Obtain detailed device documentation as early as you can in the procurement process.** If you are building a more modular, integrated system, then access to thorough and detailed documentation should be a technical requirement for device procurement. Getting hold of the information early is also helpful, as it gives your IoT platform provider sufficient time to write a decoder prior to going live, avoiding rushed work and reducing the chance of mistakes.
- **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.

- **Choose well-established, stable products.** Products (devices or platforms) that have a degree of market maturity are less likely to require updates that could result in decoder errors.

11. 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 correction.** Gas data requires the application of a temperature correction factor because the function of chemical gas sensors is directly influenced by ambient temperature.
- **Humidity correction.** Particulate data can require correction factors for humidity because water droplets can register as particle pollution inside optical sensors.
- **Regional variables.** Regionally specific correction factors that account for variables like salt, dust, and pollen aerosols, or biogenic VOCs, may be applied. State regulatory authorities may supply these correction factors upon request.
- **Calibration drift correction.** Some sensor types (notably, chemical gas cells) exhibit performance drift over their functional lifetime, linked to degradation. This results in 'calibration drift', which can be corrected using a temporal 'calibration drift correction' factor.

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 factor implementation.

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.

What does this look like?

Errors in correction factors or their application tend to result in a subtly inaccurate data output that can be quite hard to detect. Such inaccuracies can only really be picked up after several months of data have been collected, and tend to come to light as a result of data quality control activities that compare the outputs of multiple sensors. Please see OPENAIR Best Practice Guide chapter *Data interpretation: Quality control* for further information about these processes.

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 (a highly advisable form of best practice).

TIP: It is very important to keep a register of correction factors, including all details of updates made (changes, date and time, person responsible, etc.). Speak with your IoT platform provider about this. An updated correction factor will result in a sudden shift in data on record, and it is vital that people looking back on data in the future can connect that shift to a change in correction factor.

How can you mitigate this risk?

There are several actions that you can take to reduce the risk of correction factor errors occurring:

- **Ensure good documentation of correction factors** (precisely what has been implemented), and ensure that this documentation is shared with all parties.
- **Ensure that there is a process in place for correction factor updates**. If your project relies upon the application of data correction factors, then there is a good chance that updates will need to be made during the operation of your sensor network. Avoid ad hoc approaches to these changes by anticipating and planning for them.
- **Choose well-established, stable products.** Products (devices or platforms) that have a degree of market maturity are less likely to have correction errors associated with them.

12. IoT Platform: data storage error

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 in this case, resulting in a failure to store data.

One type of data storage error relates to *structured* data storage. Data arrives from a device in a data packet that can be divided into a series of discrete pieces of information. Each data point can then be processed (corrected, harmonised, etc.) and associated with metadata, before being entered into a database. The outcome is a data record with a particular structure that relates to your project data

schema (see OPENAIR Best Practice Guide chapter *Data labelling for smart air quality monitoring* for more on this topic).

Structured data storage requires that there is a specific structure for the data to exist within, inside the database. This structure should precisely mirror the structure that is inherent to the incoming data. If this is not the case, then the data will fail to be correctly stored (this is essentially a 'round peg, square hole' scenario). Either there will be no new data entry made, or data will be mixed up and assigned to the wrong fields within the database.

An example of a problem occurring in this context might be the addition of a new device type to your network, without necessary updates being made within your database for storing its data outputs. Data might successfully flow all the way through to your IoT platform, and get successfully decoded and converted, only to hit a brick wall and disappear before it can be captured in a database.

Data storage errors relating to structured data can occur as a result of any upstream changes to data processing, including device firmware updates that alter the structure of a data packet, and updates to a decoder or to correction factors that alter the structure of the decoded and corrected data output.

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, exceeding 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.

What does this look like?

Data storage errors typically result in no data storage occurring, which will appear as a gap in your data record. As these errors are most common for newly onboarded device types, what you will see is no data stored against new devices of that type. This sort of universal issue (impacting all devices of one type) should rule out all issues that are specific to individual devices and their deployment.

It can also be possible for data storage errors to result in data being mixed up and stored against the wrong fields in the database, producing extremely incongruous records.

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, which is upstream from your IoT platform (in terms of data flow).

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.

How can you mitigate this risk?

There are several actions that you can take to reduce the risk of data storage errors occurring:

- **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.
- **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 process data during the operation of your sensor network. This will create knock-on effects for how your data is stored, requiring updates to be made to the structure of your database. 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 due to the kind of structured data error described above.

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[3] 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 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)[4]. For platforms, this might include device management, software updates, and

[3] 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).

[4] 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

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.

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

---

4G, but not with LoRaWAN. SLAs for platforms relate to the amount of guaranteed availability and normal functioning of the platform.

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 Guide chapters

Air quality sensing device activation and deployment

This Best Practice Guide chapter provides guidance on activating and deploying smart low-cost air quality sensing devices.

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.

Data interpretation: quality control

This Best Practice Guide chapter provides guidance on the quality control of data produced by smart low-cost air quality sensors. Data quality control helps to isolate trusted data that can then be used to support chosen activities. This chapter explores approaches to cleaning static data sets to prepare them for analysis, and approaches to operational verification and quality control of live data streams.

Data labelling for smart air quality monitoring

This Best Practice Guide chapter provides guidance on data labelling for smart air quality monitoring. It provides advice on developing and implementing a project data schema (which defines all of the telemetry and metadata that will be used in a project).

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 chapter 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: 20231204 SR303 Sensing device troubleshooting: extended guide Version 2 Final