March 2021

Guide to the effective deployment of IoT on construction sites

Capturing learnings from the Weather Ledger project

About this guide

This guide has been designed to provide broad and practical guidance to help construction industry professionals understand how to go about using IoT on construction sites and how to avoid potential pitfalls and deliver a successful IoT project.

Developed through learnings gathered from the deployment of IoT devices at 5 live construction sites as part of The Weather Ledger project (IFS 45147) this guide also draws on other experience, expert input, best practice and standards.

This guide defines successful IoT deployment as: being straightforward to install, trouble-free, reliable, secure, trustworthy, and resilient. It securely collects and sends valuable data and is supported by robust contingency measures delivered in a cost effective manner.
The guide covers the fundamental aspects for achieving best practice when it comes to the Planning, Procurement, Deployment Operation and Recovery (see table below) of IoT devices and their associated infrastructure in a construction site context. Where applicable, weather measurement is used as the reference use case, following learnings from the EHAB Weather Ledger Project.

This guide has been authored by the Connected Places Catapult, in collaboration with project partners led by EHABITATION (EHAB) Ltd, contributions from BAM Nuttall, EHAB, Digital Catapult, Ferrovial and Clyde and Co. who are joint project partners for The Weather Ledger project.

Partners working together

EHAB · CATAPULT Connected Places · Innovate UK · CATAPULT Digital · CLYDE&CO · ferrovial construction · bam nuttall

How to use this guide

This guide has been designed to support each stage of an IoT project on construction sites from planning a site, procurement of IoT devices through to deployment, operation and then recovery at the end of the project. You can choose to read this guide from start to finish, or just reference the stage you are at in the construction process.

- **You might want to go straight to the checklist to get a complete overview of what things you need to think of and use this as a handy reference guide.**
- **You might want to reference the Definitions and Explainers if you are not familiar with some technical terms such as what IoT and LoRa actually means.**

Quick start

If you are planning what to do first, reference the **Planning** stage on **page 11.**

If you are looking at procurement of IoT devices, go to the **Procurement** stage on **page 15.**

For information on how to set up IoT on site, refer to the **Deployment** stage on **page 20.**

When you are looking after an IoT set up that is operational, you can reference the **Operation** stage on **page 23.**

For those that are at the end of a project, you can reference the recovery phase on **page 24.**

Glossary and resources

Go to **page 25** for a Glossary to help with any keywords we have referenced.

You can go to **page 27** we have provided a useful checklist that helps prompt what needs to be thought about at each stage of a project.

Contents

Introduction

The guide has been produced based on the learnings derived from the real world experiences and activities that have taken place as part of Innovate UK Transforming Construction challenge funded project 'The Weather Ledger'., that The project was using IoT (Internet of Things) and DLT (Distributed Ledger Technology) to automate the collection of weather related clauses in standard NEC construction contracts: **The Weather Ledger**.

Weather affects almost every project in the construction industry, with approximately 20% of overall build budget lost due to weather delay, which is only set to get worse as a result of climate change with a projected 17% increase in rain and 20-90% increase in flooding. The project set out to help reduce these impacts providing a digital approach to improve weather risk management.

Deployed across 5 active construction sites around the UK in major infrastructure projects HS2, Dawlish Warren (Network Rail), Harrow on the Hill Underground Station (TFL), Stubbington Bypass (Hampshire County Council) and Houghton Brook (Environment Agency). IoT devices were utilised to collect localised real time weather data to automate weather compensation events and support pro-active weather risk management.

With a major driver in the industry to improve construction productivity, IoT is seen as a key tool in helping solve real world construction productivity challenges. This guide has been created from capturing the learnings from the Weather Ledger project in order to provide practical guidance so that others in the Construction Industry can best harness the benefits of the Internet of Things.

Overview: IoT Deployment stages and key activities

This guide breaks down the stages of IoT deployment into the following stages:

Planning	Strategising the deployment, site considerations including infrastructure required to support deployment, considering the outcomes you want to achieve from your IoT deployment and the information you require to achieve that outcome, including whether IoT is the right solution for meeting your information requirements
Procurement	Making sure the IoT devices meet the information requirements and the guiding principles, considerations for selecting IoT devices based on the guiding principle
Deployment	How to deploy IoT devices on site including power supply, connectivity, siting, positioning, protection and security
Operation	Monitoring the device and how to ensure the device is operating as expected and maintained
Recovery	Construction sites are by their very nature a temporary activity. Care must be taken at the end of a given project to recover and recondition any hardware for reuse on future projects. The data however is bound to the building site itself and must be carefully separated and stored as part of the site handover process

Who this guide is for?

This guide have been designed for project delivery personnel from IoT and construction companies, but also other stakeholders looking to utilise IoT data in the construction sector, with a view to strategically planning their deployment with favourable outcomes in mind.
This includes the following users:

User	User Story	Planning
Construction Data Analytics SME's	"I want to utilise IoT data that provides a reliable, trustworthy single source of truth so that my construction data analytics solutions are trusted and secure"	Reliable, trustworthy data analytics solution
IoT company	"I want to ensure my IoT devices are deployed correctly so that it is reliable and provides a quality service for my clients"	Quality service, Reduced risk, Credibility
Construction Site Manager	"I want to utilise IoT to gain insights to help me manage my construction site with a high level of quality and a minimum level of disruption"	Gaining insights from IoT, Understanding deployment best practice, Minimising disruption, Quality, Lower costs
Legal / Contracts manager	"I want to use smart contracts and know Ii will be provided with a reliable, trustworthy source of data"	Trusted data
Construction Project Manager	"On a day to day basis I want to use IoT data to know how localised weather conditions may be affecting the safe working environment on site so that I can ensure the wellbeing of my staff"	Improved H&S
Structural Engineer	"I want to understand the onsite weather conditions so that I can determine whether parameters such as concrete cure times are within approved parameters "	Improved quality of the built structures

Principles that guide effective deployment of IoT in construction

The following is an overview of the key principles that should be considered to guide a successful IoT deployment. The subsequent sections of this guide describe how these can be implemented across the lifecycle of an IoT project.

1. Good Data Management

Ensure appropriate controls are in place to provide reliability and data integrity that is appropriate to its intended use.

Data access, and recovery and therefore the controls that need to be in place are highly dependent upon the purpose of the deployment and how critical the data is that is being collected.

The accuracy and reliability of IoT data plays an important role in being able to effectively respond to events in a timely manner. Several sources need to be accessed and compared to ensure that received data from the IoT devices are trustworthy and reliable.

Backup processes and procedures should be in place to ensure that if and when there is data loss at some point within the chain it can be recovered, validated and ingested without the risk of spurious or duplicate records.

2. Robust Testing and performance

Ensure that the performance of the selected IoT devices satisfy the specific requirements of the deployment.

Select IoT devices that have been tested by an appropriate and accredited third party test laboratory (accredited to ISO 17025) to support the verification of performance against manufacturers claims.

3. Self sufficiency and simplicity

Ensure that the IoT device can be installed and operated with minimum effort for non-technical people (ideally 'out of the box' by users without requiring a site visit from a third party). In most instances, once a sensor is deployed, it is difficult, time consuming and disruptive to upgrade or replace a device. A device that is self-contained (e.g. serviceable, stores data, self-powering) and simple to use as possible (plug and play) is recommended.

4. Proactive/ Dynamic Maintenance

Ensure that the IoT device reports health data regularly, securely capable of reporting important factors like battery level, signal reception, data storage, data transfer loss etc. Ideally IoT devices should be capable of sending alerts if its health data drops below the predefined thresholds. This feature can be helpful to mitigate any problems before any potential failure such as loss of data.

Human monitoring onsite in remote locations is costly and arduous. In the absence of an established interface, if a device goes offline, there is no chance of connecting to it. In this case, it either has to be retrieved for repair, recalibrated or replaced depending on the nature of the problem.

5. Security and resilience

Ensuring the design and operation of the system is implemented following a security minded approach and that resilience of the system is considered by ensuring that any potential single point of failure in the system is appropriately mitigated and that integrity is maintained through the life of the system. This should include the timely deployment of security updates as these arise with minimal disruption.

Deployment stages and key criteria

The following describes the key project stages (**Planning**, **Procurement**, **Deployment**, **Operation** and **Recovery**) and measures that should be followed, with reference to the five key principles of good IoT deployment.

Part 1: Planning – how to plan an IoT project

Description:

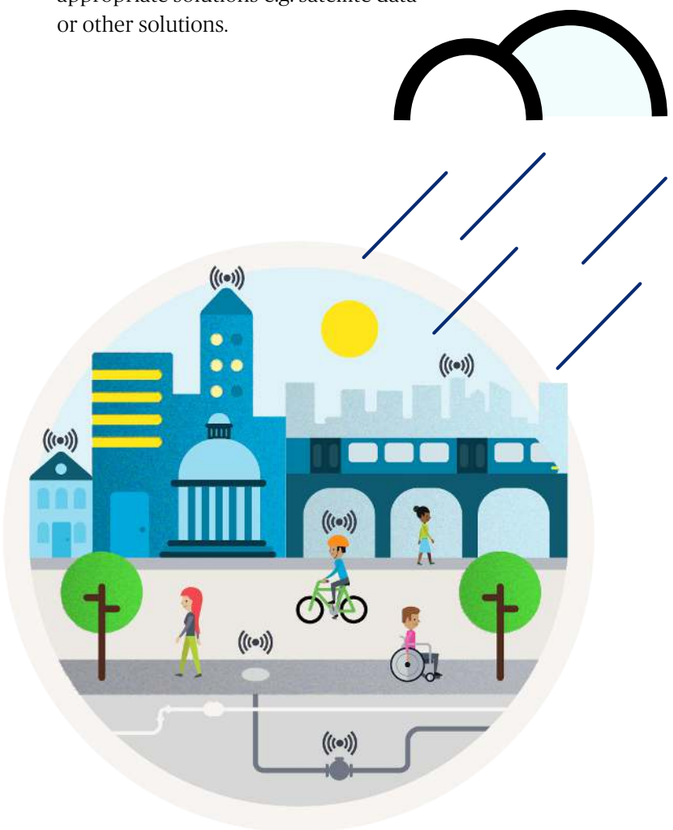
The key activity at this stage is to strategise the deployment including defining what parameters the IoT devices will need to collect and at what interval. This should consider any site specific requirements such as where the IoT devices will be located and considering what power and connectivity will be available to inform selection of the most appropriate IoT devices.

1. Deployment strategy

1.1 At this stage you should firstly define the outcome you are looking to fulfil from your IoT deployment and what information you need to support this. For example this includes what parameters you are collecting, the sampling intervals you need data to be reported (e.g. is it 1 or 15 minute, hourly etc), or report data when a particular event happens or a parameter passes below or above a predefined threshold, so that you can ensure the IoT devices you select are programmable to supports this.

1.2 It is important to determine whether it is essential to report data at all times during operation (frequency of reporting impacts on battery consumption). Consider whether you need a way of recovering data if it is not being collected all the time.

1.3 Consideration should also be made of whether IoT provides the right solution for the information you require or whether alternative data capture solutions may be more appropriate by engaging with the market to consider appropriate solutions e.g. satellite data or other solutions.



2. Deployment location and site context

2.1 You need to define an appropriate, secure location on site to support deployment (see Deployment), mark this out on site plans/models at the pre-planning phase considering the position and location of IoT devices to avoid them being moved through the works.

2.2 This will include a location for sensors, the IoT gateway, which is what the sensors talk to using wireless connectivity and power. This may also require a location for batteries and solar panels where reliable permanent power is not available. Note that site generators are not defined as a reliable source as they may be switched off or run out of fuel.

2.3 The size of the project may impact on the number of locations that you need to deploy depending on the use case. For weather sensors, large infrastructure projects (e.g. linear infrastructure such as rail, road, utilities) for example may require sensors to be deployed at multiple site locations in order to sufficiently capture localised weather events.

2.4 Consideration should be given to identify whether the device might be required beyond the construction programme such as for ongoing site weather monitoring in coordination with the client. As well as being a potentially cost effective approach, this may impact on the specification, location of the device and handover process (see part 5: recovery) subject to client requirements.

3. Power & Connectivity

3.1 Determine what power and connectivity is available or will be immediately available. Secure and reliable power and connectivity shall be planned for in advance of installation of IoT devices to ensure they can operate from day one.

Why?
Anecdotal evidence - a deployment of IoT sensors on a recent project was unsuccessful because the power supply was only available during working shifts and therefore intermittent however the IoT hub required continuous power to function correctly. It is therefore important to ensure the provision of power that will meet the needs of the IoT deployment.

3.2 For connectivity, this should either be wired or wireless. Wired solutions are very reliable while wireless can provide more flexibility for deployment. Depending on availability, wireless connectivity should be provided through either:

- Low Power Wide Area Networks (LPWAN) such as LoRaWAN, Sigfox, NB-IoT,
- Cellular (2G/3G/4G/5G) or
- WiFi

LPWAN solutions are specifically designed for connecting IoT devices with low power, they can provide wider and deeper network coverage. Most IoT devices using LPWAN can last a couple of years in the field without a battery charge. In the absence of LPWAN, onsite WiFi or cellular can be used.

Ahead of deployment, you should firstly identify if there is connectivity via any of these networks at the site location using existing coverage maps such as:

- WiFi connection to construction site network
- Low Power Wide Area Networks (LPWANs) such as:
  LoRa gateways https://www.thethingsnetwork.org/mapintheUK
  Sigfox: https://www.sigfox.com/en/coverage

- Mobile coverage (2G, 3G, 4G and 5G) can be checked via mobile network operator's coverage map.

3.4 It is advised that you test the connectivity on- site, using a field test device. This is due to the fact that if a site is at the boundaries of two cells it may experience some connectivity issues. Therefore by testing the reception signal and choosing a network with better reception you can connect your device to a more reliable network.

3.5 If there is no Low Power Wide Area Network coverage on site, a local IoT gateway connected using mobile connectivity (i.e. 3G/4G/5G) may be required for the sensors to connect to. In general, IoT devices connected to cellular networks or WiFi consume more energy than when they use LPWAN connections.

4. Cyber Security

4.1 Consider whether a security minded approach is required, based on the security triage process described in ISO 19650-5 based on the sensitivity of the site and the information that will be processed. Where from this it has been determined that a security minded approach is required, this should be deployed in accordance with ISO 19650-5. This should include ensuring the deployment will align with the site's security management plan and any specific mitigation measures.

Planning section summary

- ✔ Define your deployment strategy including what information do you actually need and the number of IoT devices
- ✔ Define a clear location for deployment, marked up on site plans/ models and ensuring the location is suitable so that it will not be disturbed based on site programme
- ✔ Check power and connectivity on site to determine suitability and consider what infrastructure might be needed
- ✔ Determine if there are any specific mitigation measures that need to be implemented based on the site's security

An off-grid IoT set-up

"One of the learnings we found from the Weather Ledger is that the British summer does not always offer enough sunlight to provide a totally off-grid IoT set-up."

Using Atmos 41 Sensors from DecentLab with LoRaWAN gateways and solar panels to trickle charge the batteries, this setup appeared to give us enough power and uptime, but later, in the midst of a UK winter we found that the solar panels weren't providing as much power as the original design had estimated, causing issues of data loss. As a result we now look at more resilient power, ensuring there is a means of recovering any data loss and having status flagging up where there are problems. When using solar panels in the UK. Assume only one hour of sunlight per day in the winter and ensure that this is sufficient to replenish the battery.

Part 2: Procurement - how to procure the right infrastructure

Description:

The key activity at this stage is to select IoT devices that are sourced with specifications and attributes that support their intended use, with access to on-demand support and assistance when needed.

As with all sensor solutions the intention should be to eliminate any single point of failure. Points of failure could be the sensor, the radio interface, the radio backhaul, the fixed backhaul or the back end platform. Care should be taken to ensure that wherever possible there are backup and duplicate systems in place, particularly where the sensors provide particularly critical information. This should be in the form of extra sensors, extra radio base stations running over different networks and then robust, load balanced and duplicated back end systems. All of these systems should have automatic alarming processes in place so that if and when something does go down an appropriate action may be taken.

1. IoT Sensors Selection

1.1 Firstly source IoT devices that suit the required parameters and sampling intervals and also the intended communications protocol e.g. LoRaWAN or SigFox compatible IoT devices.

A device that is self-contained (e.g. serviceable, stores data, self-powering) and simple to use as possible (plug and play) is recommended.

1.2 If the sensor is to be battery powered it is essential that the battery can be replaced by the end user as opposed to having to replace the whole sensor or return it to the supplier for reconditioning. If the sensor is to be battery powered the battery status should be regularly reported so it can be determined when replacement is required.

1.3 It is recommended that at least two or three sensors are selected per sampling point, in order to avoid being reliant on a single point of failure and this also allows calibration of results.

1.4 Source the device from a manufacturer where live assistance and supporting documentation is provided. This will ensure support can be provided should any issues occur with the device (e.g. battery failure).

1.5 It is advisable to select a device with higher specification to prevent unexpected failures. So for example: ensuring that the battery capacity is more than sufficient, the enclosure has an Ingress Protection (IP) rating that exceeds the needs of the site (e.g.IP66) and that any memory for local storage exceeds the expected requirements just in case it is not possible to get to the sensor as quickly as one would like (e.g. because of COVID lockdown)

2. Accuracy

2.1 The accuracy of the sensor should be considered, this should be determined from specifications with calibration certificates provided by the supplier. Note that accuracy should not be mistaken for display accuracy (e.g. a manufacturer may quote that a display can be accurate to two decimal places yet this doesn't necessarily mean the sensor is accurate to this level of detail)

3. Performance Verification:

3.1 It is recommended that the performance of IoT devices (e.g. accuracy) are independently verified by sourcing IoT devices certified by a third party accredited testing laboratory (in accordance with ISO 17025).

3.2 It is also recommended that suppliers are able to provide suitable references from other deployments to verify credentials.

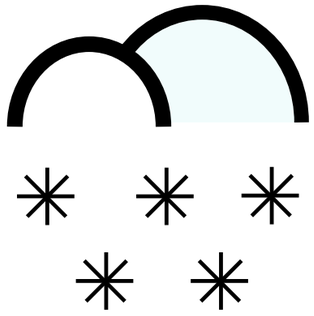
3.3 Where planning to deploy sensors that are particularly critical, it is recommended that third part field testing data should also be obtained.

Why?
Many IoT devices may have performance data based on testing in a lab, however field testing is important to ensure testing should be carried out in real-life scenarios. These measures protect against potential device failures that could otherwise jeopardise critical data being recorded.

4. Data Storage:

4.1 Select sensors that store data, or find an alternative means to collect data on site and store it (even if a human has to go there and retrieve it if the device goes offline). If it is critical to obtain every data packet, it is recommended that data should be stored locally.

Why?
Not all IoT devices store data, they may only collect it and send it. If the network is offline, the sensor does not know the payload was not received. For example, if an IoT gateway goes offline during a weather event, a weather sensor may not report this event and it will appear as though it has not happened.



5. IoT Gateway

5.1 The following is recommended for IoT Gateways:

5.2 Specifying a gateway that is compatible with the IoT devices and will suit the number of intended device.

5.3 The gateway should be within an IP66 rated enclosure where located outdoors.

5.4 An ethernet cabled connection for backhaul is preferred. If the only option is to backhaul data over a cellular network, then ensure that the gateway contains an integrated 3/4/5G modem.

5.5 Ensure that the gateway can be remotely managed.

Why?
This is essential as there may be times when the gateway needs to be restarted, or even require a full firmware update. The majority of commercially available gateways do come with a back end remote management system which will allow for complete management and maintenance of the gateway and even alerting should the gateway go off line. Some vendors will charge for this back end system some provide it free of charge. This should be considered when selecting a gateway.

6. Power supply

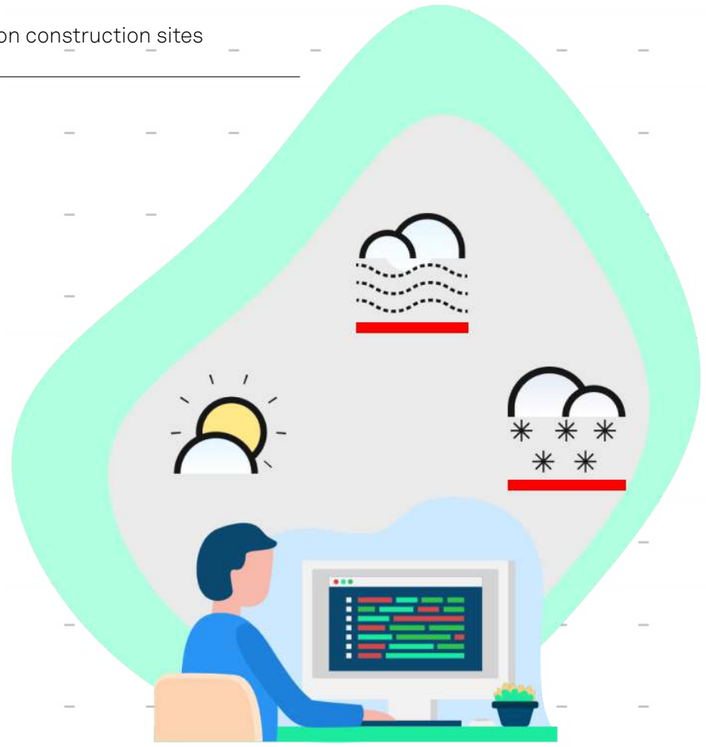
6.1 The IoT Gateway will require a power supply. If there is no permanent power supply on site, a solar panel array will be needed to charge a battery supply.

6.2 A minimum 14 days back-up battery power is recommended to support the Gateway should the solar panel array fail. AGM batteries (absorbed glass mat) are beneficial on construction sites as they do not have to be kept upright and are spill-proof.

6.3 For Solar panel array, a solar control charger will be needed along with battery protection. Their orientation and tilt should be optimised, south facing and tilting 30-40 degrees and avoiding shade (full technical guidance for solar PV installation can be found through the microgeneration certification scheme here: https://mcscertified.com/wp-content/uploads/2019/08/PV-Book-ELECTRONIC.pdf)

6.4 It is recommended that seasonal variation of performance is considered as solar PV output will vary in different conditions. For example what works well in July might not provide sufficient power in November.

6.5 Electrical installation should comply with Building Regulations Part P and the BS 7671 IET Wiring Regulations.



7. Device security

7.1 IoT devices that comply with ETSI EN 303 645 provide a good baseline level of cyber security. This should include:

- Ensure that no default passwords are used and that if IoT devices are pre-configured with passwords then they are unique and any records of these passwords are carefully stored
- Having policies which define actions to be taken in the event of a vulnerability being detected
- Ensuring software/firmware updates are automated and secure
- Ensuring user credentials, keys and other sensitive data is securely stored within the device, secure hardware or encrypted
- Maintaining confidentiality, integrity and authentication for communication to/from IoT devices and services
- Minimising exposure to surface attacks e.g. by disabling unused functions so the device only utilises intended functions
- Ensure software integrity
- Ensure personal data is protected
- Make system resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data (where relevant to deployment)
- Make installation and maintenance of device easy
- Validate input data

7.2 Where sensitive information is to be collected or the site is of a more sensitive nature that the system is designed to meet any additional mitigation measures defined (this should align with the requirements of ISO 19650-5)

8. Lifecycle cost

8.1 Consideration should be given to the lifecycle cost of IoT devices including the cost of the IoT devices, installation, maintenance access and recovery.

8.2 Consider opportunities to reduce the lifecycle cost such as reusing IoT devices at the end of the project or considering how the device might be utilised on the site on a more long term basis for ongoing monitoring.

Procurement section summary

- Provide resilient power including:
- Where off-grid solar powered gateway solutions are being used, size the PV array comfortably above demand including at times of lowest solar output (e.g. winter) with minimum 14 days back-up battery power

Consider lifecycle cost:

- Consider IoT devices lifecycle cost of IoT devices including installation, maintenance and recovery costs

IoT Gateways:

- Ensure the Gateway is compatible with and suitable for the number of IoT devices required
- Select a Gateway with Ethernet (if suitable for site) or contains an integrated 3/4/5G mode

Select sensors that:

- meet the information requirements defined at the planning stage e.g. type and interval of data
- have batteries that are easily replaceable where needed
- can store data in the event of a power or connectivity failure
- are sourced from manufacturers with live assistance
- have verified performance e.g. third party testing by an accredited laboratory to ISO 17025
- comply with baseline security defined in ETSI EN 303 645 including provision of patch management during their life

Site set-up

> **“We learnt the importance of defining a fixed location on site where the device will not be disturbed and to maintain integrity”**

The Weather Ledger Pilot involved deployment of IoT devices over five active construction sites. The IoT devices were deployed in a few ways on site such as a dedicated pole or mounting to a pole on temporary site buildings that were due to be there for the life of the project. The key thing is ensuring it is in a location that is not likely to be distrubed and allows the integrity to be maintained.

Part 3: Deployment - how to set up IoT on your site

Description:
the key activity at this stage is to install IoT devices in the appropriate place on the construction site, avoiding risk factors, complying with recognised standards, and protecting against any potential tampering and security breaches.

1. Siting and positioning

1.1 Sensors and IoT Gateways should be sited in a location that supports the intended functionality and does not compromise performance. They should be mounted to scaffolding, a separate pole, or any other type of structure that has adequate clearance to capture the relevant information and away from large objects, structures or potential activities that might interfere with functionality. Specific guidance should be followed appropriate to the type of sensor based on manufacturers recommendations and as below.

2. Specific considerations for weather sensors

2.1 Consideration should be made as to how the local environment may impact upon the sensor and provide potential false readings and ensuring they are mounted at a location that aligns with the following:

Sensor type	How to use
Air temperature and humidity sensors	• Placed at 1.25 metres above ground • Ideally at a horizontal distance that is twice the height of the nearest object (e.g. 40 metres away from a 20 metre high building) • Sited at a location ideally above natural landscaping. (e.g. grass) Avoid rock/ concrete and dark-colored surfaces, roofs, or irrigated landscaping • Located away from surfaces that heat quickly (e.g. dark surfaces) or surfaces that cool quickly (e.g. concrete) • Positioned away from any nearby potential sources of heat such as buildings or mechanical end electrical equipment • In a position where free circulation of air can occur
Wind sensors (Anemometer)	• Mounted at 10 metres above ground in a clear unobstructed location or as high as possible given the local circumstances • Sited at a horizontal distance of 10 times the height of the nearest obstruction, or as far from obstructions as practical given the site, with maximum exposure of the anemometer to the commonest wind directions • When placed at roof level, the sensor should be placed as high above the roof structure as it safely and economically can be (preferably 2-3m above the highest point), to avoid potentially turbulent air below • When placed on the side of a mast (rather than at the top), the sensor should be placed on a horizontal boom extending outwards from the mast, at a distance of 3 times the mast diameter
Rain gauge (also known as an udometer or pluviometer)	• Ideally mounted at a height of 1.25 to 1.85m above the ground • Ideally located at a horizontal distance of 4 times the height of the nearest obstruction • Ensure the gauge is mounted level to the ground, away from any horizontal surface that can introduce rain-splashing or surrounding snow buildup

3. Security and protection (from tampering, protection from damage from construction activities)

3.1 Position the device away from the main construction area or anywhere which carries a significant risk of damage to the device.

3.2 To prevent tampering, ideally place the device in hard-to-access or cordoned off areas. Where increased level of trust is required this could be located in an area maintained by a trusted party with no vested interests in the data. This achieves a higher level of security.

3.3 Having multiple sensors can also mitigate against tampering or vandalism to one sensor, as data from other sensors can be aggregated and gaps in data collection identified. Data can be compared to another authoritative source (e.g. the Met Office for weather data) for validation purposes.

3.4 A configured alerting system can help identify deviation from the data norm, with human checks ensuring greater validity of data.

4. Calibration

4.1 A copy of the calibration certificate/s should be requested from the supplier to confirm measurement parameters are within manufacturers defined parameters and calibrated in accordance with British (BS), European (EN) or International (ISO/IEC) standards as relevant including the following as relevant:

Sensor / measurement instrument	Standard
Rain gauge	• BS EN 17277:2019 Hydrometry. Measurement requirements and classification of rainfall intensity measuring instruments
Anemometers	• IEC 61400-12-1:2005(E) "Wind turbines - Part 12-1: Power performance measurements of electricity producing wind turbines, First edition 2005-12/ Annex F "Cup anemometer calibration procedure"

Note: this list can be expanded in future iterations.

Remote Monitoring

"When access to site can be limited, the ability to remotely monitor the IoT set-up including monitoring of battery status and any anomalies in the reporting of data was a key requirement for the project"

As part of the Weather Ledger project, IoT devices equipped with a warning mechanism were able to report on the percentage of data loss, as well as battery information and other possible issues that could be affecting the quality and integrity of their data. This allows for the routine monitoring of any potential issues that might impact on the loss of data, with an expectation that some level of data loss might occur (e.g. up to 5%). The use of status alerts can help to manage this situation to flag up any issues should they occur. It also is a way of providing evidence to show the level of data integrity the system is providing.

Deployment section summary

- ✔ Mount sensors and gateways in a suitable secure location away from large objects, structures or activities that might risk interference with functionality, result in damage or potential tampering or theft
- ✔ Mounted sensors in a location in line with specific guidance for the type of sensor e.g. locating temperature sensors away from sources of heat
- ✔ Obtain copies of calibration certificates to confirm performance against relevant standards (e.g. BS EN 17277:2019 for rain sensors, IEC 61400-12-1:2015 for anemometers)

Part 4: Operation - how to operate a resilient system

Description:

the key activity at this stage is to ensure various aspects of the deployment are properly set up so that maintenance and repair can be done seamlessly, with consideration to physical and cyber security measures, and adequate human checks and balances.

1. Human checks and balances are important in ensuring the system as a whole is working properly, and that the data flow and frequency are not interrupted by unexpected events. A combination of onsite and remote offsite monitoring measures helps provide a robust end to end solution.
2. An individual/s will need to be made responsible for monitoring in case any alerts/alarms are triggered to identify any faults such as battery failure.
3. The use of an IoT device monitoring platform, where alarms can be set for changes in device status is recommended.
4. Monitoring the frequency of the device (IoT sensor) sending messages helps identify whenever it, or the gateway potentially goes offline and helps build reliability.
5. It is recommended that consideration is given about other ways of recovering data if it is not being collected all the time and how any maintenance will be managed if needed (i.e. what to do if it breaks). This should include considering issue/fault repair time particularly if the device is providing 'contract critical' data.

Operation section summary

- Ensure there is a process in place for monitoring the system to check for faults (e.g. battery failure) either on-site or remotely

Part 5: Recovery - how to recover devices at project closure

Description:

At the end of an IoT project, it is important to then demount any IoT devices for their re-use or recover any data the device may hold

1. Agreement should be made to ensure IoT devices can be recovered from site and utilised as part of future projects, returned to the supplier or where at their end of life returned for recycling or refurbishment.
2. IoT devices should be checked for any wear and tear in accordance with manufacturer guidance and repaired/ reconditioned where needed for future use.
3. Where IoT devices store data, data should be recovered from the device and handed to the responsible party (e.g. construction information manager) and existing data cleaned from the device.

Recovery section summary

- Ensure there is an agreement for recovering IoT devices at the end of the project for re-use, refurbishment or recycling as relevant. This should include the recovery of any data for handover to the responsible party.

Glossary

Distributed Ledger Technology (DLT)

Refers to a type of database which is spread over multiple locations (i.e. a distributed database) and which can be used like a digital ledger to record and manage transactions.

Internet of Things

Is defined as: Infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

The internet of Things, or "IoT" for short, is made up of devices – from simple sensors to smartphones and wearables – connected to the internet and communicating with each other.

IoT Gateway

An internet of things (IoT) gateway is a device that connects IoT devices, equipment systems, sensors and the cloud. By connecting the IoT devices in the field and a centralized cloud, the IoT gateway can offer local processing and storage solutions, as well as the ability to autonomously control field IoT devices based on data input by sensors. IoT gateways also receive information from the cloud, which then goes to the device itself. This means that all the information moving from an IoT device to the cloud, or vice versa, goes through the connected IoT gateway.

LPWAN:

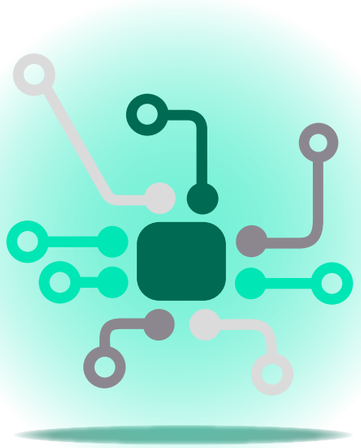
A low-power wide-area network (LPWAN) or low-power wide-area (LPWA) network or low-power network (LPN) is a type of wireless telecommunication wide area network designed to allow long-range communications at a low bit rate among things (connected objects), such as sensors operated on a battery.

LoRA

LoRa is a wireless technology that offers long range, low power and secure data transmission for M2M (Machine to Machine) and IoT applications.

Sigfox:

Sigfox is a narrowband (or ultra-narrowband) technology. It uses a standard radio transmission method called binary phase-shift keying (BPSK), and it takes very narrow chunks of spectrum and changes the phase of the carrier radio wave to encode the data.



Next Steps

This guide has been developed by learning from real world application but we are keen for this learning not to stop here. We hope you found this guide useful for your IoT project and we are keen to learn from you. If you would like to provide any feedback on this guide or share learnings from your IoT project we are happy to hear from you so that this guide can evolve. Please get in touch with the City Standards Team **info@cp.catapult.org.uk**

Checklist

Planning

- ✔ Define your deployment strategy including what information do you actually need and the number of IoT devices
- ✔ Define a clear location for deployment, marked up on site plans/models and ensuring the location is suitable so that it will not be disturbed based on site programme
- ✔ Check power and connectivity on site to determine suitability and consider what infrastructure might be needed
- ✔ Determine if there are any specific mitigation measures that need to be implemented based on the site's security

Procurement

Provide resilient power including:

- ✔ Where off-grid solar powered gateway solutions are being used, size the PV array comfortably above demand including at times of lowest solar output (e.g. winter) with minimum 14 days back-up battery power

Consider lifecycle cost:

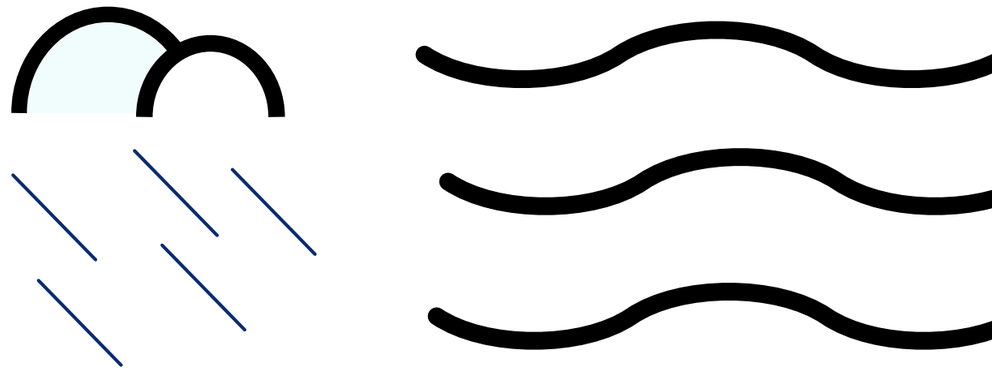
- ✔ Consider IoT devices lifecycle cost of IoT devices including installation, maintenance and recovery costs

Select IoT Gateways that:

- ✔ Are compatible with and suitable for the number of IoT devices required
- ✔ Have Ethernet (if suitable for site) or contains an integrated 3/4/5G mode

Select sensors that:

- ✔ Meet the information requirements defined at the planning stage e.g. type and interval of data
- ✔ Have batteries that are easily replaceable where needed
- ✔ Can store data in the event of a power or connectivity failure
- ✔ Are sourced from manufacturers with live assistance
- ✔ Have verified performance e.g. third party testing by an accredited laboratory to ISO 17025
- ✔ Comply with baseline security defined in ETSI EN 303 645 including provision of patch management during their life



Deployment

Sensors and IoT Gateways:

- ✔ Mounted in a suitable secure location away from large objects, structures or activities that might risk interference with functionality, result in damage or potential tampering or theft
- ✔ Mounted in a location in line with specific guidance for the type of sensor e.g. locating temperature sensors away from sources of heat
- ✔ Obtain copies of calibration certificates to confirm performance against relevant standards (e.g. BS EN 17277:2019 for rain sensors, IEC 61400-12-1:2015 for anemometers)

Operation

- ✔ Ensure there is a process in place for monitoring the system to check for faults (e.g. battery failure) either on-site or remotely

Recovery

- ✔ Ensure there is an agreement for recovering IoT devices at the end of the project for re-use, refurbishment or recycling as relevant. This should include the recovery of any data for handover to the responsible party.

References and other sources of information

1. BS EN 17277:2019 Hydrometry. Measurement requirements and classification of rainfall intensity measuring instruments

2. IEC 61400-12-1:2017 Wind energy generation systems - Part 12-1: Power performance measurements of electricity producing wind turbines

3. ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

4. ISO 19650-5 Information management using building information modelling – Part 5: Security-minded approach to information management

5. ISO 17025 General requirements for the competence of testing and calibration laboratories

6. The Things Network https://www.thethingsnetwork.org/map

CATAPULT
Connected Places

Sajed Amirinia
sajed.amirinia@cp.catapult.org.uk

Gavin Summerson
gavin.summerson@cp.catapult.org.uk

cp.catapult.org.uk

Follow us on Twitter
@CPCatapult

Email us
info@cp.catapult.org.uk