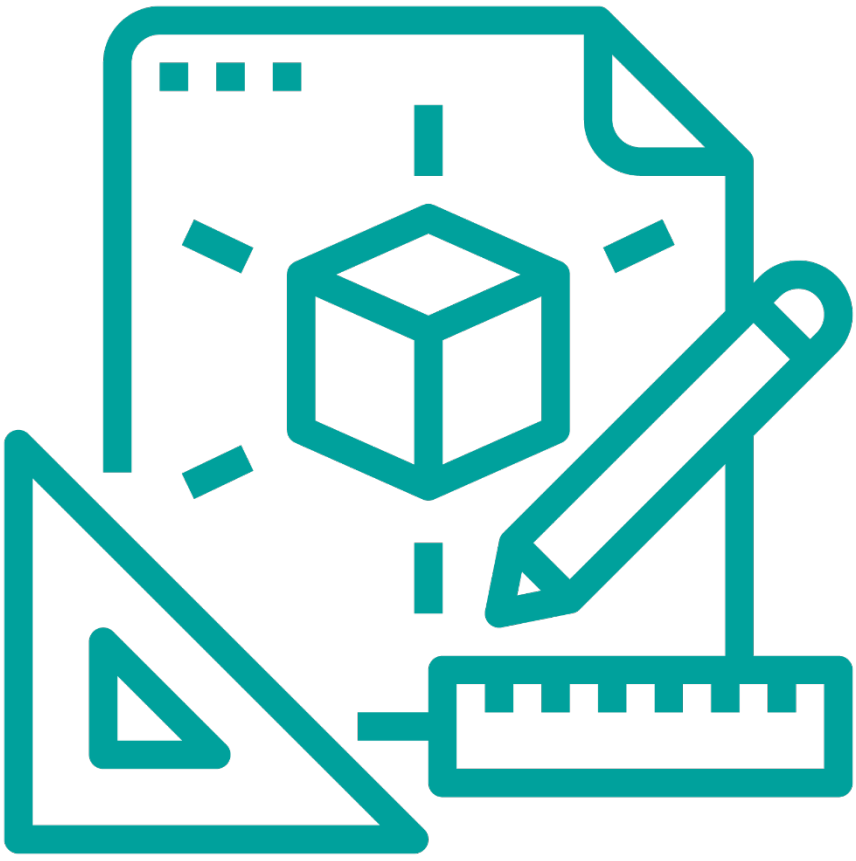
OPENAIR

Operational Network of
Air quality Impact Resources

Best Practice Guide

B207 | Develop

IoT reference architecture for smart air quality monitoring



Introduction

When we establish a smart sensing network we need to collect, manage and store data and make it available for one or more end uses. Different layers of technology are brought together, including hardware components, communications infrastructure, and various platforms and databases, as well as more advanced data analytics and visualisation capacity. These technology components form a complete integrated system that we call an 'architecture' or 'technology stack', through which data flows. Various users access and make use of that data at different layers of the architecture.

A *reference architecture* is a generic framework or structure that describes how *components* of an IoT architecture come together and relate to each other. It describes the type of technology and functionality at the various layers of a technology stack while avoiding specific mentions of products or vendors, which may quickly become dated. Reference architectures are useful as a guide for designing your own tailored solution because they provide you with a map of all the parts and functions you are likely to need.

This Best Practice Guide chapter will introduce you to an IoT reference architecture developed for low-cost air quality monitoring and provides a generic and high-level framework that is adaptable and applicable to develop a specific IoT solution for your project. The framework we have developed for the OPENAIR project is based on the more general IoT Reference Framework v1.0 developed by the IoT Alliance of Australia (Internet of Things Alliance Australia, n.d.).

How to use this resource

This Best Practice Guide chapter provides an overview of the IoT reference architecture and a framework to assist with the development of an IoT systems architecture that meets the needs of your air quality monitoring project.

What is the purpose of this reference architecture?

- To establish a common language or 'terminology' to facilitate discussions amongst the air quality sensing community and stakeholders.
- To help you to understand and articulate the structure and functional needs of your prospective IoT solution relative to a more generic template.
- To support you in the design of a detailed IoT solution for your project.

There are two types of reference architecture referred to in this chapter: 1) simplified reference architecture, and 2) full reference architecture.

Who is this resource for?

This resource aims to assist people involved in the strategic planning of an air quality monitoring project. It is also intended to be a practical tool for people responsible for designing and implementing an IoT solution for a specific air quality monitoring project such as:

- Enterprise architects
- Data architects
- Technology architects
- Solution architects
- IT project managers
- IT procurement managers

It is also intended as a general reference for:

- People leading new air quality monitoring projects
- Council executives
- Smart City project leads
- Planners
- Environmental managers

An expanded version of this resource, with additional detail, can be found in the OPENAIR supplementary resource *A reference architecture for smart air quality monitoring: detailed guide*.

A simplified reference architecture for low-cost air quality monitoring

The simplified architecture is intended as a reference for a non-technical audience. Its main function is to highlight in a practical sense, the distinct types of products and services that will need to be procured to build a complete system. See Figure 1 (page 3) for details of the simplified architecture.

A full reference architecture for low-cost air quality monitoring

The full reference architecture is organised into 10 layers (Figure 2, page 4): IoT endpoints, edge gateways, connectivity, connection management, intelligence enablement, application enablement, user interface, users, stakeholders, and industry solutions. It also includes four functional cross-layers: operations, security, data governance, and data sharing.

Data users		
User interfaces (laptop, mobile, tablet, etc.)		
Application enablement	**Air quality data applications**	End user business and IoT applications: • data discovery and sharing (e.g. public dashboard; open data portal; custom API) • developer services.
Intelligence enablement	**Analytics and visualisation platform**	A user-facing dashboard that might incorporate maps, customisable graphs, and more advanced data analytics tools (e.g. GIS; digital twins; machine learning/AI).
	Data management and storage *[Data platform]*	Device telemetry (sensor readings) must be structured and stored in a way that is secure, searchable, and accessible. Storage options tend to be cloud-based third-party services (commonly Amazon or Microsoft) that are connected to data management systems, which structure data and manage user access.
Connection management	**Device hosting and management + basic data interpretation** *[IoT platform]*	You will need a contract with a service provider that hosts devices in a digital platform. Device management involves the onboarding and commissioning of new devices and their subsequent management, with alerts in place for failures and errors. Be aware of your basic data interpretation requirements (like humidity interference correction for particulate data, and calibration and drift correction for gas data), and communicate these before proceeding.
Connectivity + edge gateway	**Communications**	You will need a contract with a communications provider that supports the transmission of live data from devices to a central online management location. Your chosen communications solution might involve local government-owned infrastructure (gateways), or you might engage a telecommunications provider and make use of their existing infrastructure.
IoT end point	**Devices** (IoT end point)	Physical digital hardware that produces and transmits data.
The physical world		

Figure 1. Basic components of data architecture for a sensing network

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

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

Architectural layers

Industry solutions

The industry solution layer provides the context for an IoT solution such as industry segment (industrial, consumer, enterprise) and its many implications such as security, regulations, supply chain, etc.

Stakeholders

This layer provides the business perspective of an IoT solution. This layer should clearly indicate all IoT ecosystem stakeholders involved in the IoT solution, such as solution owner/operator (business, enterprise, government) and service provider. Identifying all the stakeholders allows the underlying complexity in any IoT solution to be managed end-to-end, including security, privacy, data integrity, solution resiliency, availability, processes, and resources.

IoT users

This layer identifies the type of IoT users who interact directly or indirectly with the IoT solution. Users can be categorized as primary or secondary. Primary users are IoT solution owners which act upon the information produced by the solution. Secondary users are such as those who operate and manage the solution or have a business interest in the solution. This layer helps the IoT solution owner identify who the real customers are.

User interface

Shows the type of interfaces that need to be supported by the *application enablement* layer. Examples include interfaces that are widely used today such as from mobile apps to the emerging types such as AR/VR devices. User Interface that enables access and or manage of the IoT system and devices.

IoT client devices can be a desktop, laptop, tablet, smart phone, wearables, or purpose-made devices including user communication methods.

Application enablement

The application enablement layer refers to a set of functions and foundational services such as the API enabler, web portal, web and mobile application building and enablement, user interface security, developer services, etc. This layer enables functions that are both business and technical in nature to be accessible to the ‘users’. It can include end user business and IoT applications.

Intelligence enablement

This layer refers to the use of smart technologies to turn air quality data into intelligent and actionable information. The air quality data collected from different devices needs to be analysed, cross referenced, and observed to identify patterns. These smart technologies (e.g., artificial intelligence, machine learning) help to produce insightful outcomes and to derive smart solutions. The intelligence enablement layer includes data platforms, analytics platforms, third party data APIs, data sharing, data management, data governance.

Connection management

The connection management layer specifies a set of the IoT core functions; for example, connection management, which refers to the management of networks, protocols, device/gateway management, ID management, user authentication. This layer forms the final part of what is commonly referred to as the 'IoT Platform'.

Connectivity

The Connectivity layer provides the network connection between endpoint/gateway devices and IoT core platforms. This layer supports connectivity technologies Bluetooth, WiFi, RFID, Ethernet, 6LoPAN, LoRaWAN, Sigfox, LPWAN, 3G/4G LTE, LTE-M (Cat-M1), NB-IoT (Cat-NB1) and other proprietary radio technologies; This layer also represents (Internet) access network for IoT client devices, which could be fixed or mobile broadband, as well as connectivity to ISP.

Edge gateway

The edge gateway layer represents: 1) the *aggregation point* for a group of sensors and actuators to coordinate the connectivity of these devices to each other and to an external network such as a connectivity network; 2) a *protocol gateway* that performs protocol conversion between devices and the core platform; and/or 3) an *edge computing gateway* that performs a subset of functions from layer 4, 5 and 6 above, such as data storage, analytics, and ML.

IoT endpoint

IoT endpoint layer represents endpoint devices that can be remotely managed. These endpoints can either be a simple, stand-alone device such as wearables or sensors, or complex product that has a single or multiple endpoints embedded in it. The IoT endpoint layer can be further expanded into an architectural functional stack comprising: hardware such as sensors and actuators, IO devices, MCU, operating systems, hardware abstraction layer, firmware, etc.

Functional cross layers

There are four supporting functions that cut across the reference architecture layers: operations, security, data governance, and data sharing.

Operations

An IoT system must be operated across all layers of a reference architecture, from physical devices all the way up through various platforms, databases, and applications. Operational functions include monitoring performance, conducting planned maintenance and upgrades, troubleshooting, and resolving issues, and managing settings and users. At each architectural layer, operational needs should be considered. It is important to ensure that IoT system operations for your project align with the overall IT operations and service management framework (e.g., ITIL, IT4IT) of your organisation.

WHAT IS IOT SYSTEM OPERATIONS?
IoT system operations are where IoT initiatives become “operationalised”—or integrated into an organisation’s standard procedures and day-to-day operations.

Security

An IoT system is theoretically open to attack from internal and external threats or unapproved data access at any layer of the data architecture, making security a cross-cut consideration from top to bottom of the technology stack. Security requirements are established based on a specific risk assessment and risk appetite defined by your project and organisation.

It is important to ensure that the security of your chosen IoT system aligns with the broader IT security strategy and policy of your organisation.

WHAT IS SECURITY?
Security is the protection of technology and data assets from internal and external threats, based on a risk assessment and risk appetite.

Data Governance

An IoT system requires end-to-end oversight and control over the management and flow of data across the layers. This can include:

- *Data lineage*—provides the ability to trace data from its origin to destination.
- *Data quality*—ensures the monitoring, maintenance and improvement of data accuracy, completeness, consistency, timeliness, validity and uniqueness.
- *Metadata management*—metadata describes data, and it has its own management requirements. Metadata within a smart sensor network can include: contextual information relating to sensing devices and their deployment, information associated with the interpretation of raw sensor telemetry, information associated with the format, exchange and storage of data, information

associated with data users and access privileges, and information associated with the display and analysis of data.

Data governance is about the end-to-end oversight and control over the management and flow of data.

Data Sharing

An IoT system is composed of layers that exchange or share data *internally* with other components of the architecture. Each layer also has the potential to share data *externally* with other systems and users. Thus, data sharing is something needs to be managed at every level of the data architecture to ensure that only appropriate data will be open to the public and that more sensitive data will be shared exclusively with approved recipients. A data sharing policy, plan and supporting set of guidelines and/or procedures is required to operationalise the appropriate assessment, sharing and if necessary, the de-sensitising of data.

It is important to ensure that the data sharing functionality and settings applied to your project align with any pre-existing data management and sharing policies within your organisation.

WHAT IS DATA SHARING?
Data sharing is a process of making data available to individuals or organisations based on terms and conditions.

References

Internet of Things Alliance Australia. (n.d.). *Internet of Things Alliance Australia*.

Associated OPENAIR resources

Best Practice Guide chapters

IoT system operations

This Best Practice Guide chapter provides guidance on the technical operation of an air quality monitoring network as a complete IoT system (comprising multiple devices, communications systems, software/platforms, databases, and digital services). Effective operation of these systems ensures a reliable supply of air quality data, and ensures that data is stored, accessed, and used in accordance with the needs of a project and organisation.

Cybersecurity for smart air quality monitoring networks

This Best Practice Guide chapter provides guidance on key cybersecurity considerations for local governments establishing smart low-cost sensor networks and supporting platforms and services.

Sharing air quality data

This Best Practice Guide chapter provides guidance on the sharing of air quality data. It explores the process by which a local government might assess data to determine its shareability, and presents a series of practical options for implementing data sharing.

Supplementary resources

A reference architecture for smart air quality monitoring: detailed guide

This resource is an extended, stand-alone guide to the OPENAIR reference architecture for smart air quality monitoring. The reference architecture is a framework that identifies the various technical components of a complete air quality sensing network, and shows how devices, communications, platforms, databases, and user interfaces integrate and support the flow and management of data. It is a generic reference that can help local governments to design and implement their own technical solutions.

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: 20231108 BP207 IoT reference architecture for smart air quality monitoring
Version 1