

Part 1: What ARE YOU TRYING TO DO?

Anatomy of IoT

Collect your data

Process your data

Use your data

Monitor & control

Analyse & understand

Predict & maintain

IoT in action

Build your own IoT canvas

Part 2: MAKING THINGS HAPPEN

STEP 1: Digitise your things

STEP 2: Connect your things

STEP 3: Manage your things

STEP 4: Secure your things

Partners

Connectivity selector

IoT checklists

Glossary

INTRODUCTION

This guide aims to strip the Internet of Things (IoT) down to what really matters –and explain it in plain language.

- If you're new to IoT –start at the beginning and you'll be up to speed in no time.
- If you already know a bit –jump to the section you want to know more about.

IOT IN A NUTSHELL

At its most simple, IoT is a way of collecting data from things in the physical world. This data can then be analysed into insights that can make business processes more efficient, give us more control over our homes, warehouses, worksites, cars and buildings –and even create completely new business models.

Right now, IoT is turning hundred-year-old industries digital and creating completely new ones. If it's not affecting your industry yet, it soon will be. But hey, if someone's going to disrupt your industry, it might as well be you.

So, let's get started.



Part 1:

WHAT ARE YOU TRYING TO DO?

“If I had an hour to solve a problem, I’d spend 55 minutes thinking about the problem and 5 minutes thinking about solutions.” – Albert Einstein

A common mistake in IoT is to start building a technical solution and then trying to find a problem it can solve – it happens more often than you’d think. Instead, you should start by clearly defining what you want to achieve. Until you’ve done that, don’t even start looking at the technology.

START WITH YOUR WHY

Here’s a friendly hint: if you can’t put yourselves into one of these categories, there’s a danger you’re wasting your time.

<p>1 ASSET EFFICIENCY Make the most of what you’ve got</p> <p>Know where your assets are and how much they’re being used.</p> <p>E.g. Know which rubbish bins need emptying and where they are so you can plan your pick up route.</p> <p>Know which meeting rooms are actually being used and which are empty.</p> <p>Know how much each vehicle in your fleet is used and exactly where it is right now.</p>	<p>2 PROCESS EFFICIENCY Optimise everything</p> <p>Monitor and optimise to increase efficiency and productivity while reducing down-time.</p> <p>E.g. Compare the fuel consumption of each vehicle and driver in your fleet.</p> <p>Monitor elevator usage and schedule predictive maintenance to avoid down-time.</p>
<p>3 New Product / Service Innovation Disrupt an industry</p> <p>Technology-first businesses and start-ups that unlock new possibilities using IoT.</p> <p>E.g. Fitness trackers. Pet trackers. Child trackers.</p>	<p>4 Legacy Product / Service Innovation Bridge the gap between the past to the future</p> <p>Unlocking new value from existing industries.</p> <p>E.g. Products > services. Sales > subscriptions.</p>

ASK YOURSELF:

What’s the problem I want to solve or opportunity I want to take?

Common answers are:

Utilisation: I want to use my assets more.

Availability: I want to make sure things are working when they should be.

Efficiency: I want to reduce waste and increase production.

Safety & Security: I want to keep my people safe and my operation secure.

What are my current processes?

What would be affected?

What KPIs will I use to measure success by?

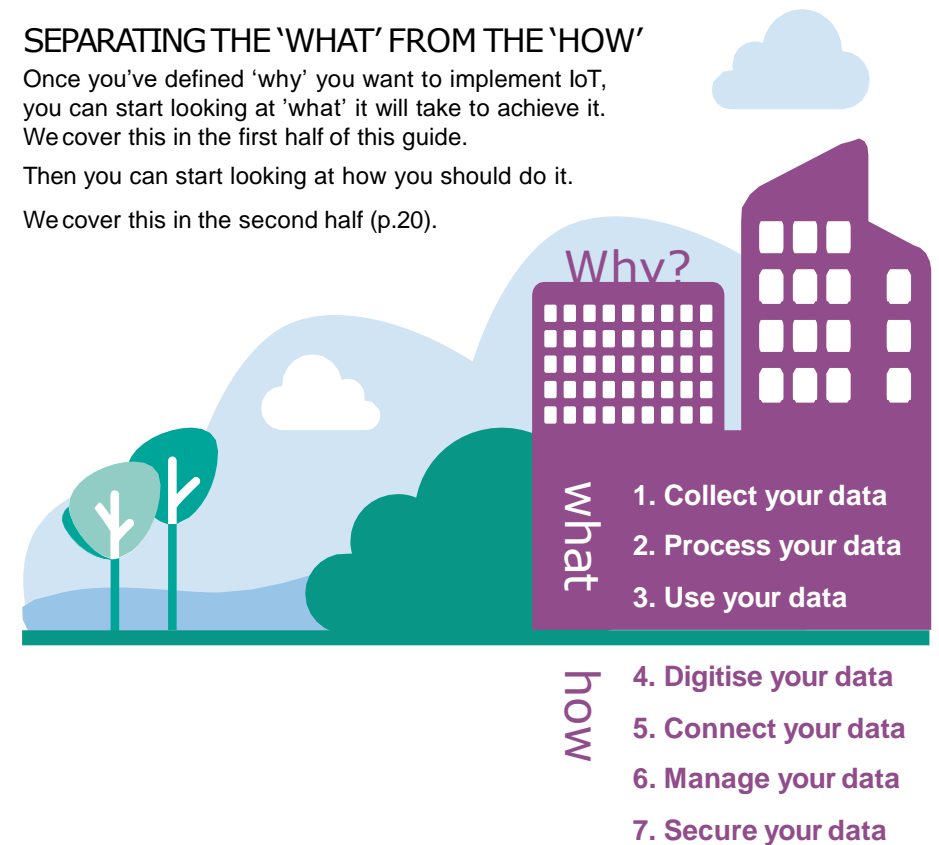
It’s well worth talking to an expert at the ‘why’ stage to help you understand the possibilities.

SEPARATING THE ‘WHAT’ FROM THE ‘HOW’

Once you’ve defined ‘why’ you want to implement IoT, you can start looking at ‘what’ it will take to achieve it. We cover this in the first half of this guide.

Then you can start looking at how you should do it.

We cover this in the second half (p.20).



ANATOMY OF IOT

The 3 main parts IoT are:



THINGS

What's a thing? Well, it could be pretty much anything really. It could be a building, a vehicle, a toaster. It could be a plant, an animal... it could be you! It could even be a traffic pattern or the way a crowd moves – anything that generates data that can be connected and collected can be part of the Internet of Things.

IoT creates a “phygital” world where physical things have digital twins. The thing is in the real world and its twin is the digital data it generates on a dashboard or feeds into a system.



BUSINESS LOGIC

This is the brain of an IoT system. Its where data from things is turned into meaningful information. Once the data has been collected, the business logic sets the rules. It defines what data should be extracted and what insights can be drawn. It also defines what data outputs should trigger further actions or generate alerts or warnings.



USERS

Once you've got the data and insights, the way you use them depends if you're a person or machine. If you're a person, you will probably want a dashboard that presents insights and alerts and lets you see patterns and trends. That way you can see it on your computer screen, phone, tablet – even your watch. Machines on the other hand can consume data directly from protocols, algorithms or APIs. And when you can combine data from multiple sources, you can get some very powerful insights. That's the power of open data and APIs.



Location
59.274155
17.789203



Speed
76 km/h



Fuel consumption
39.5 L / 100 km



Driving hours
3:14



Break due
1:16



Humidity
31%



Temperature
21°C



Occupancy
71 employees
12 guests



COLLECT YOUR DATA

The starting point of IoT is to turn physical into digital. This is generally done by sensors that are built into or attached to things. In simple terms, anything that measures something and is connected, can generate digital data which can be collected. This could be the temperature of a room, the location of a rubbish container, or how full the rubbish container is right now.

In general terms, sensors let you do 3 things:

SENSE

Things in the environment that can be measured: e.g. temperature, pressure, humidity, luminosity, motion, and proximity.

REACT

Sensors can be set to react to pre-defined scenarios. At one end of the scale they can send a message that their battery is flat. At the other end of the scale is a power grid adapting output based on the real-time demands of a city.

TRANSFORM

In most scenarios, even after digitise, things still have limited capability to process what's captured. They can do simple things like filtering, simplifying, correcting and transforming data; but you need to connect your things to the cloud, edge or local computing where the heavy processing happens.



PROCESS YOUR DATA

Welcome to the brain of your IoT system. This is where data is turned into meaningful information. The business logic will be your guideline at this stage. It will implement the rules, make decisions, and manage your things and users.

RULES ENGINE

Your rules engine is the set of instructions you define to create real-time actions for incoming data. The business logic is implemented within this engine. The easiest way to define the rules engine is to use IFTTT (IF This Then That) technique.

Recipe

if this then that

Trigger

Action

If [energy demand is high] then [generate more power]

If [beer levels are low] then [automatically order more]

If [battery level is low] then [send an alert]



Location
63.257329
10.860739

INTERNET OF SHEEP
INorway in 2017, carried out the world's largest Narrow- band IoT pilot. They put sensors on 10.000 sheep to enable farmers to track them on their mobile phones. This made it easy to locate them even in difficult terrain or weather conditions. If sheep could speak, they'd thank us.

AGGREGATE

Now you need to bring together the 3 Vs of big data:

Volume:

how much data will you collect?

Variety:

what types of data will it be?

Velocity:

how quickly do you need it?

In some situations, it could be a small packet of system status data, such as a water level measurement that is sent twice a day. At the other end of the spectrum is an autonomous vehicle that is sending data from multiple sensors inside and outside the car that are combined with other traffic data sources remotely and sent back in the form of instructions – every few milliseconds.

UNDERSTAND

In situations like the autonomous car, complex analytics are required. Multiple data sources are combined, calculations are made, and data is transformed into patterns which can be used as inputs for other systems. In other situations, it's a simple alert to your phone that there's a water leakage at your house.

INFORM

Fed by the rules engine, data is sent when certain criteria are met. This could be a time: send data once every minute or it could be a trigger: send data if the temperature of cold-chain cargo reaches a certain level or if smoke is detected.



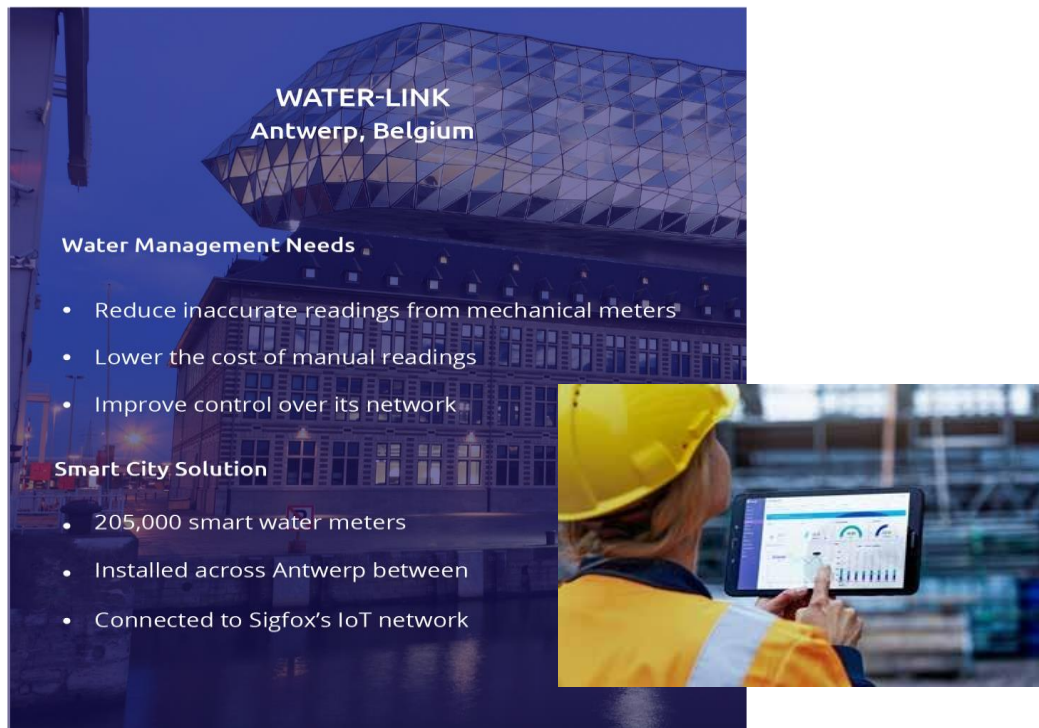
USE YOUR DATA

IoT can put your world on a dashboard, which gives you real-time information to make informed decisions. But it can also send data directly to your other digital systems via an API – which makes really big things possible.

The ways IoT can be used can generally be separated into three areas:

MONITOR & CONTROL

Monitoring is the foundation of IoT: being able to see what's happening in the physical world through digital data sent from devices. Companies can continue to monitor how people use their products so they can make them




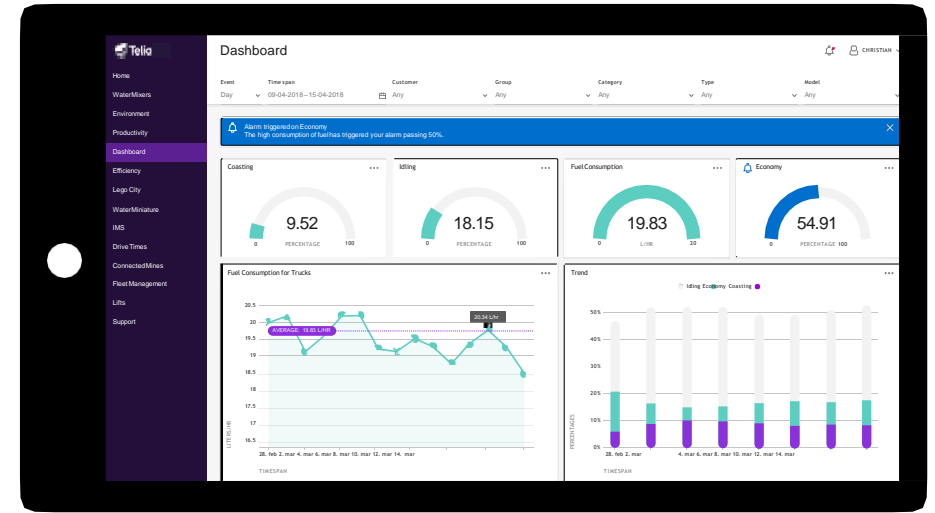
WATER-LINK
Antwerp, Belgium

Water Management Needs

- Reduce inaccurate readings from mechanical meters
- Lower the cost of manual readings
- Improve control over its network

Smart City Solution

- 205,000 smart water meters
- Installed across Antwerp between
- Connected to Sigfox's IoT network

better. This is being used today in the white goods, electronics, and automotive industries.

The next step up is to send instructions back to the device so you can control it remotely. This could be to activate a heating system or a fire prevention system or even to turn a sensor on or off when it's needed. Smart buildings are an example where information from how many people are in the building and how many are expected can be used to adjust the temperature and proactively keep it comfortable.

ANALYSE & UNDERSTAND

This is where things really start to get interesting. When you combine the data from your sensors with other data sources, you can start to optimise your operation and priorities your resources.

This means you can drive costs down, increase your productivity, and reduce your environmental footprint.

PREDICT & MAINTAIN

The next level is not just to know what's happening, but to anticipate what's about to happen. It's the key to just-in-time maintenance & inventory management as well as maximising uptime and resource planning.

Thanks to machine learning and statistics, a large set of data can produce valuable predictive analysis. Whether it's data from your washing machine or traffic patterns at different times, the IoT solution can make insightful predictions. Use cases include predictive health-care, predictive maintenance, proactive business models and supply/demand forecasts.

IOT IN ACTION

TRANSPORTATION

By combining data from vehicles and their surroundings, transport operators can increase the efficiency or just their vehicles, but their entire fleets.

Real-time fleet management lets them optimise asset utilisation and route planning. Eco driving helps drivers to reduce fuel costs and emissions. Predictive maintenance helps to reduce vehicle downtime and increase profitability.

LOGISTICS

With the ability to track vehicles, cargo and assets in real time; logistics operators can optimise route planning, deliveries and asset utilisation. They can also deliver a better customer

PUBLIC TRANSPORT

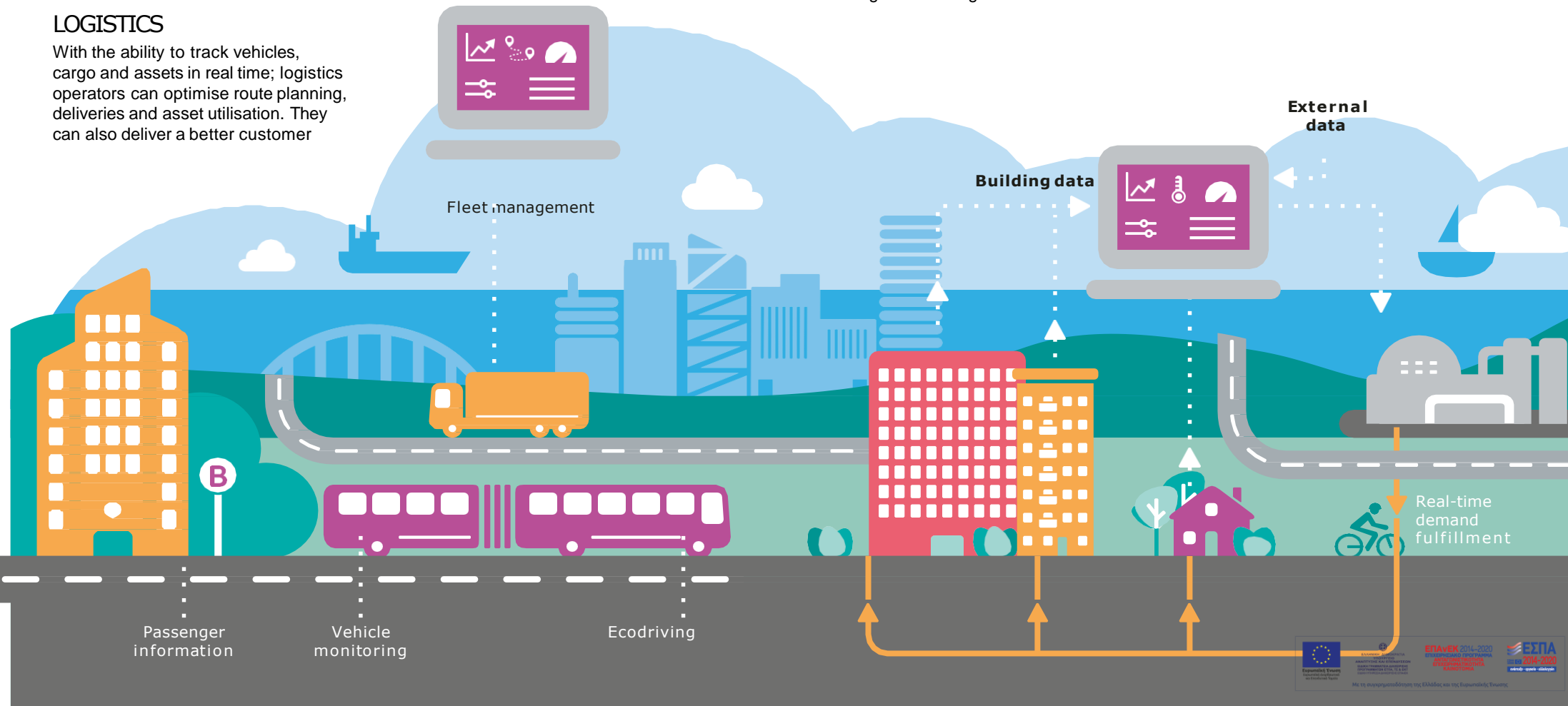
Connected public transport goes far beyond onboard WiFi. Public transport operators are using real-time fleet management to make their services more reliable and providing passenger information to make them more predictable. At a higher level, crowd analytics is emerging as an important tool for understanding underlying commuter needs and measuring and identifying new routes.

HEALTHCARE

One of the main promises of connected healthcare is “home instead of hospital”. Patients are able to monitor themselves from home while healthcare providers monitor them from a distance. This means greater independence for patients and lets healthcare providers focus on the patients that need help the most. IoT data from wearables also unlocks ‘big data’ possibilities that enable health providers to analyze large data sets and gain new insights.

UTILITIES

At one end of the scale, utilities are using Automated Meter Reading (AMR) to monitor power, gas and water meters across broad geographic areas. At the other end of the scale, they are integrating data from multiple sources in real time to understand needs and provide real-time demand fulfillment for energy grids and district heating.



MANUFACTURING

“Optimise everything” is the catchcry of industry 4.0. With real-time visibility of what’s happening, real-time optimisation has become possible. The impact can be seen from predictive ordering and automated supply chains to production management and predictive maintenance.

BUILDINGS

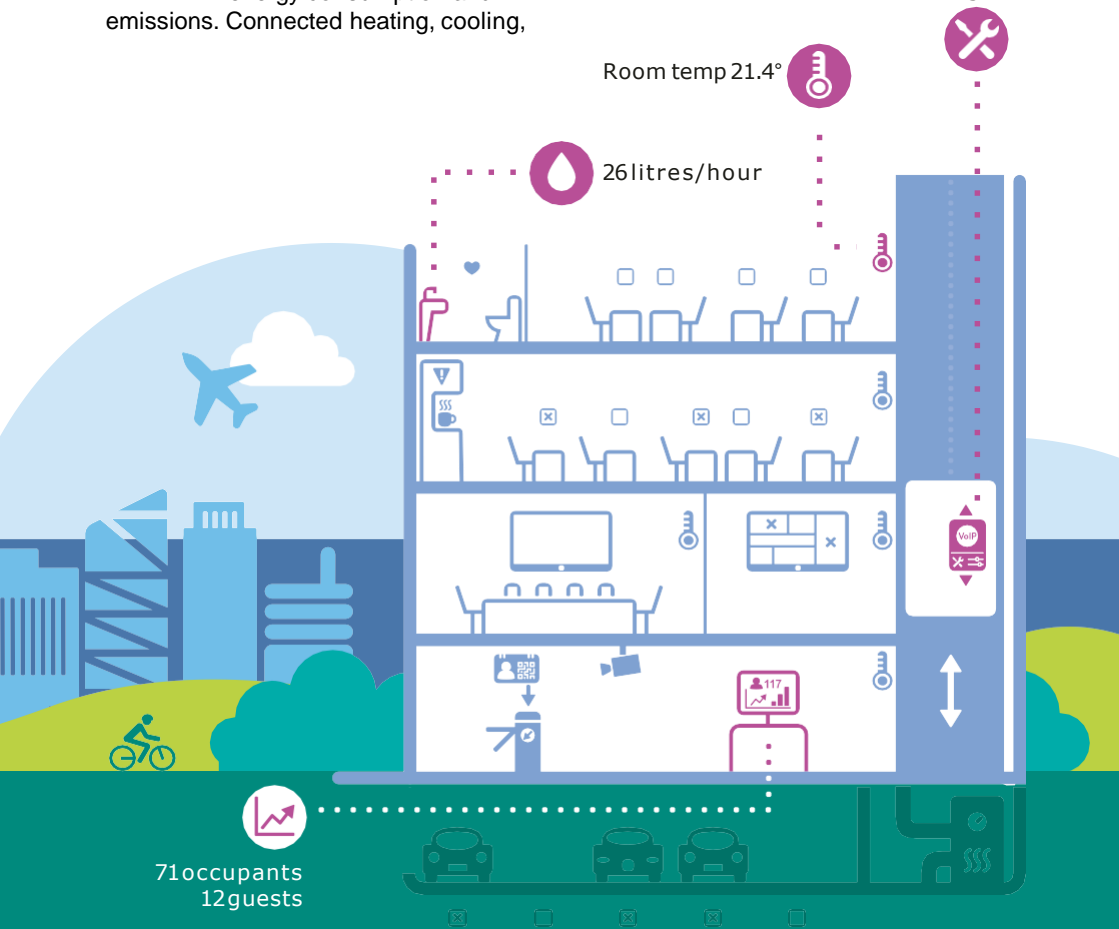
Buildings account for almost 40% of the world’s energy consumption and emissions. Connected heating, cooling,

lighting and space utilisation can make a big difference for the environment, building profitability and the comfort of those who live and work in the building.

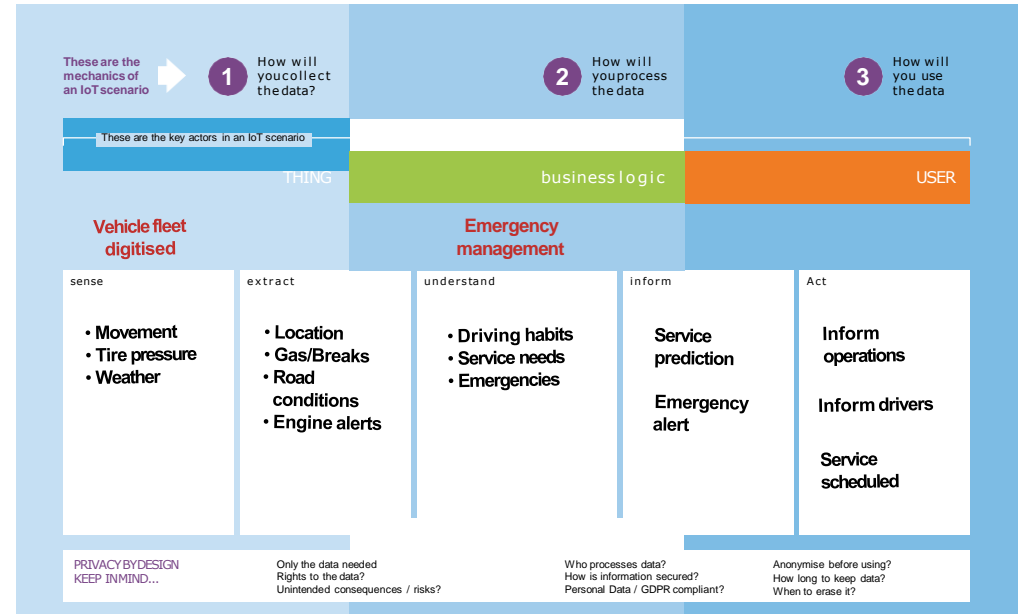
SMART CITIES

When you combine everything above – and add in sensors that optimise public services from street lighting and traffic lights to parking and waste collection – you get smarter, more liveable cities.

Maintenance Due Aug 22



BUILD YOUR OWN IOT CANVAS



YOUR TURN

On the next page is a blank canvas. Start filling it out now and refer back to it as you go. Here’s an example.

We have a vehicle fleet and we’d like to sense their movement, tire pressures, weather conditions etc. By collecting this data and applying business logic, we turn it into information. In this way we can extract location information, acceleration and braking behaviours, road conditions and any engine alerts from the transformed data. With the help of the rules engine inside the business logic, we can understand driving habits and service needs. We can detect emergencies, flat tires, engine failures or critical weather alerts.

Based on the scenario, we inform the operations personnel about the emergency for them to act on it. We might also inform the driver so they’re aware of the upcoming service need. And finally, we can even schedule service with a 3rd party maintenance company automatically so they can organise their resources.

The natural way to fill in the canvas is from left to right, but you can also start with the desired user actions. Usually it might take a few swings between the three sections to perfect your scenario.

BUILD YOUR OWN IOT CANVAS

These are the mechanics of an IoT scenario

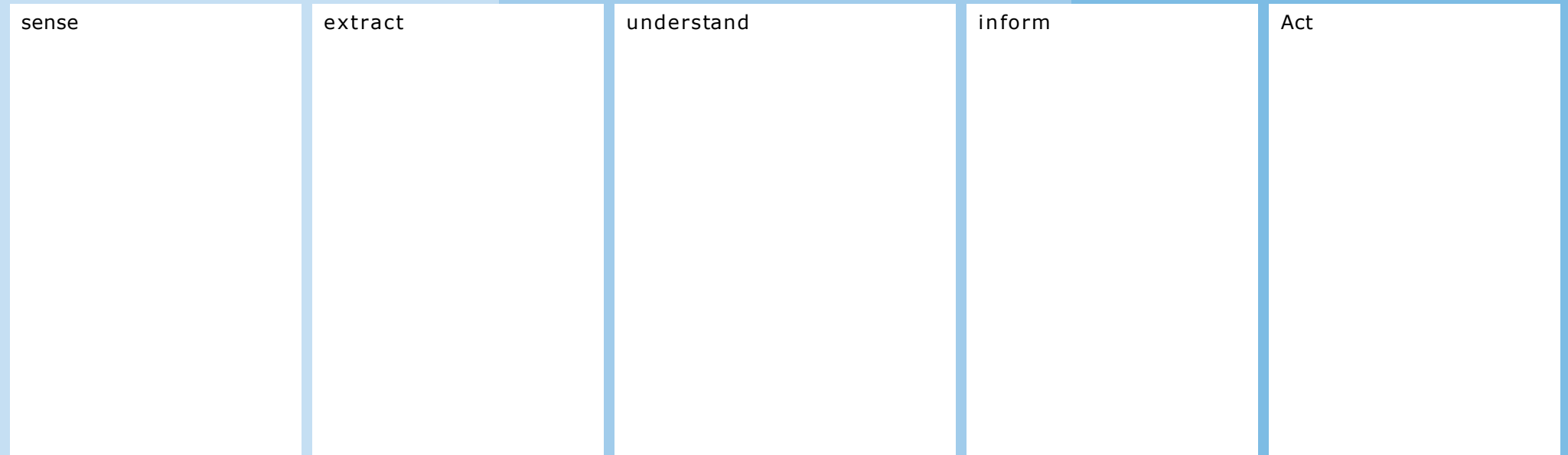
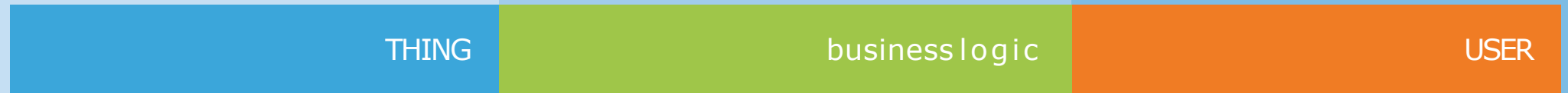


1 How will you collect the data?

2 How will you process the data

3 How will you use the data

These are the key actors in an IoT scenario



**PRIVACY BY DESIGN
KEEP IN MIND...**

Only the data needed
Rights to the data?
Unintended consequences / risks?

Who processes data?
How is information secured?
Personal Data / GDPR compliant?

Anonymise before using?
How long to keep data?
When to erase it?

Part 2:

MAKING THINGS HAPPEN

STEP 1: digitise YOUR THINGS

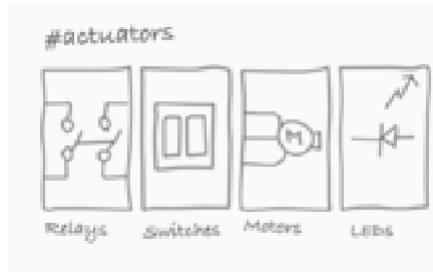
By translating physical forms into digital representations, a 'digital twin' is created. This senses the analog world and shares this data digitally. Let's break this down step by step.

SENSING THE ANALOG WORLD

Sensors are the key to creating the digital nervous system. They make it possible for the 'thing' to start seeing, hearing and feeling. Via sensors, it is possible to measure many parameters such as temperature, pressure, humidity, luminosity, motion and proximity. The information collected is digitised and transformed into data.

ANATOMY OF A DIGITISED THING

The brain of the digitised thing is called the #controller. It is a low power central processing unit (CPU). It includes a random-access memory to run functions, storage to keep the data and a real-time clock module. The controller runs its own micro code. This is called #firmware.



The things can also react autonomously if they have #actuators. As the sensors collect the input, actuators provide the output. Their main components are relays, switches, motor and LEDs.

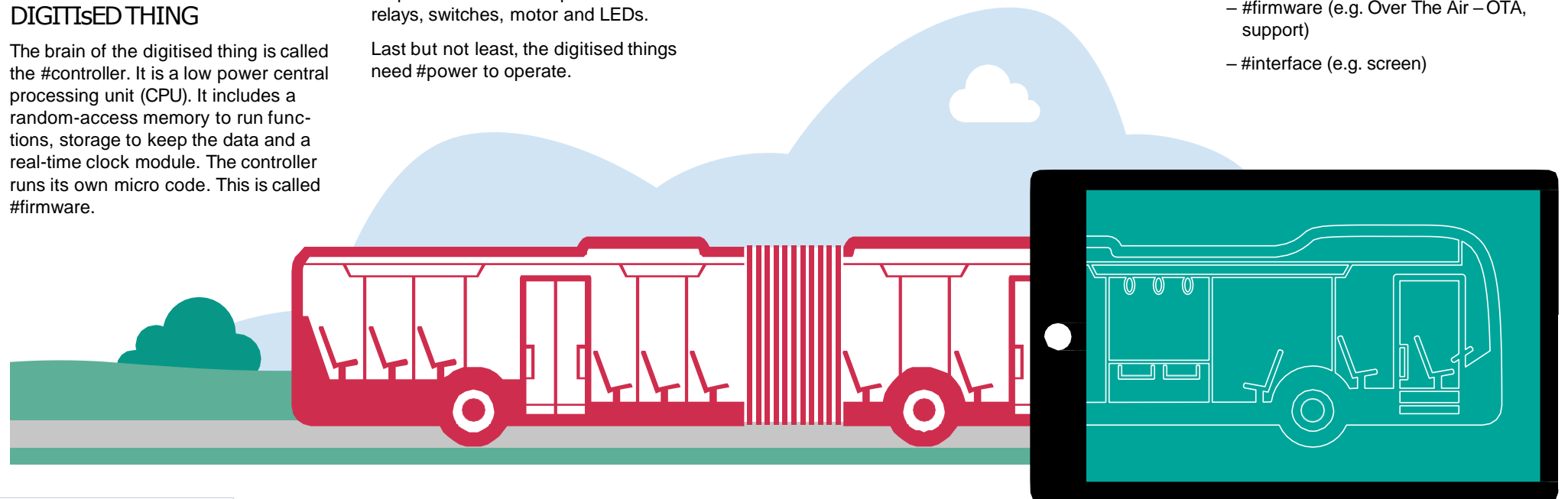
Last but not least, the digitised things need #power to operate.

Interfaces

While some IoT devices might only execute machine to machine communication, others provide Human Machine Interfaces (HMI) to interact with people. Keyboards and touch screens are most common but fingerprint sensors and eye scanners might be also considered as interfaces.

When digitising your things, you should think about:

- #sensors (e.g. sensitive vs robust)
- #power (e.g. battery vs direct power)
- #housing (e.g. design and specs)
- #actuators (e.g. relays, LEDs)
- #communication (e.g. connectivity)
- #data (e.g. real-time vs offline)
- #controller (e.g. storage, clock)
- #firmware (e.g. Over The Air – OTA, support)
- #interface (e.g. screen)





CONNECTION TRADE OFF: RANGE VS BANDWIDTH VS POWER

Ideally, everyone prefers the longest range, highest data bandwidth with minimum power consumption. But more data requires more power and longer range demands even more power. In order to comply with the need for high bandwidth and long-range requirements, the only feasible option is cellular – i.e. 4G LTE or 5G. If your devices will be in constant motion - like an autonomous smart car or tracking device – you will need cellular connectivity. As the number of connected things increases, cellular will be the best solution to overcome density and capacity problems.

Then, if you want to decrease the power consumption, but still want to send large amounts of data, you need to sacrifice on range. For indoor connectivity within a few metres, WiFi and even Bluetooth will be enough. To achieve low power consumption but also have long communication range, data bandwidth must be limited. In these cases, Low Power Wide Area (LPWA) technologies like NB-IoT, LTE-M, SigFox and LoRa are suitable.

STEP 2: CONNECT YOUR THINGS

Connectivity is at the heart of IoT. Things, business logic, and users all talk to each other. In today's world, the number of different connection technologies and protocols is overwhelming. This can lead to a lot of frustration when it comes to choosing the communication platform for your solution. Each technology comes with its own benefits and drawbacks.

These three questions will help you to understand which type of connectivity is best for you: How much data will flow? Is mobility key? Is your solution mission-critical?

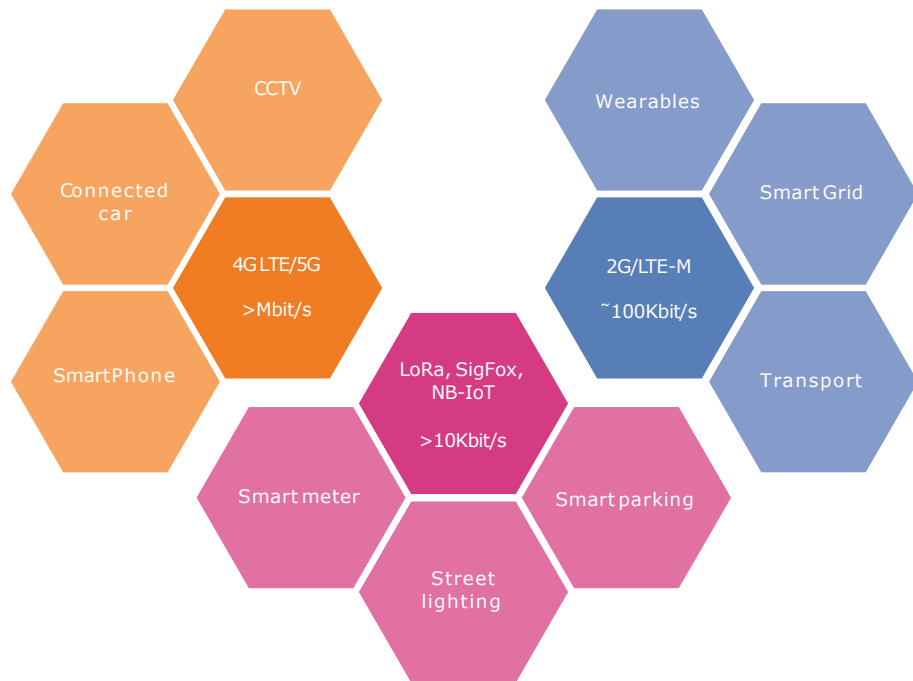
	Location based			Low Power Wide Area					Cellular	
	NFC	BLE	WIFI	SigFox	LORA	NB-IOT	LTE-M	4GLTE	5G	
Range	1m	10m	100m	20km	5-10km	40km	40km	40km	100m-40km	
Data Throughput (up to)	424 kbps	2 Mbps	3 Gbps	0.1 kbps	50 kbps	150 kbps	1 Mbps	1 Gbps	1-10 Gbps	
Licensed/ Dedicated Spectrum	No	No	No	No	No	Yes	Yes	Yes	Yes	
Security	Low	Low	High	Medium	Low	High	Very High	Very High	Very High	
Indoor Penetration	N/A	Very low	Low	High	High	Very High	High	Medium	Medium	
Battery operation	N/A	1-2 months	1-6 months	6-14 years	4-9 years	4-8 years	1 year	1 year	Less than 6 months	

MISSION CRITICAL

If your IoT device serves a mission-critical need, like monitoring a defibrillator or a power grid, it needs to send the data whenever it is needed. Therefore, the connection availability must be very high – preferably telco grade like 99.999%.

POSITION ACCURACY AND LATENCY

Some services may require the exact location of the device and can't tolerate significant delay in the communication. Position accuracy and latency can be crucial, for example precision manufacturing or autonomous vehicles that interact with other cars or roadside infrastructure. By latency we mean, the duration of a packet of data to get from one point to another. Sometimes, the round-trip time is also considered latency.



Gateway or independent

If you have a lot of sensors in a small area – like in a factory or a home – you can connect them all to one gateway and connect that to the Internet. But if your sensors are spread all over town or around the country or overseas, then you need connectivity that connects each of them directly to the Internet. That's why some factories build their own enterprise networks, but distributed ventures use cellular connectivity.

There are several technical design factors to determine between choosing a gateway vs independent network. If you want all your individual IoT devices to connect to Internet directly, they might need more memory and more processing power. Adding a gateway device might also mean more complex and longer development and deployment cycles.

STEP 3: MANAGE YOUR THINGS

As the number of things increases in an IoT solution, so does the complexity of management and maintenance of the network.

Consider trying to find a failed IoT device that needs to be serviced or replaced – inside a high-rise building. You need to have adequate backend systems to locate and identify the correct “failed” device easily. One aspect is remotely accessing your things and getting their operational health status. It is also a major benefit to be able to update the device software #OTA (Over The Air).

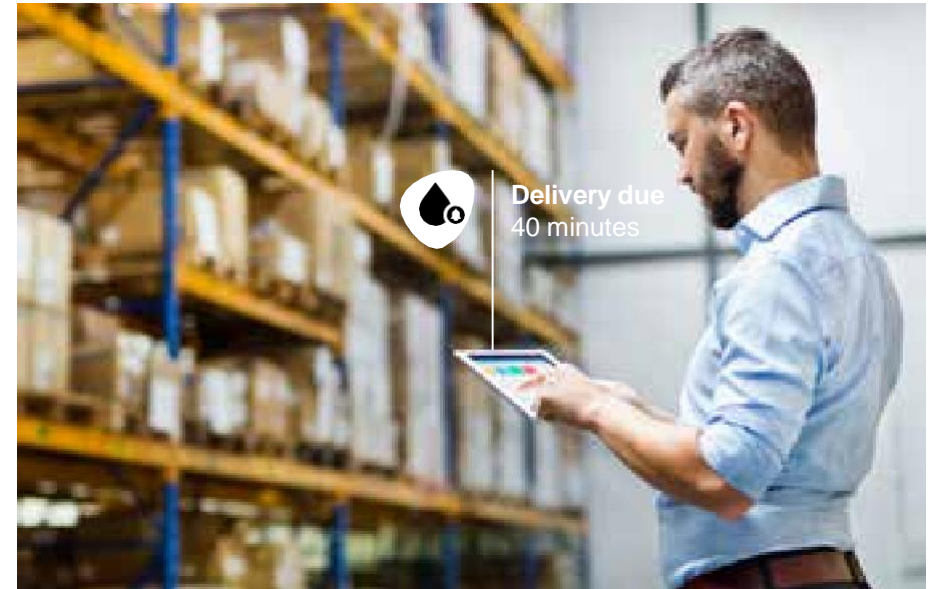
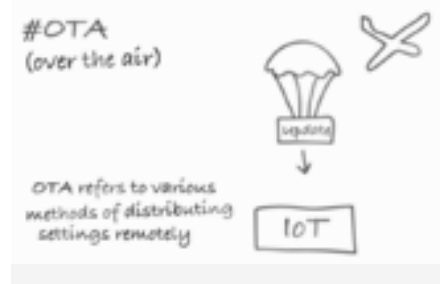
Let’s focus on how an IoT solution is designed, developed, deployed, operated and continuously improved over its lifecycle.

DEVICE MANAGEMENT

Scaling an IoT solution is all about control. As the number of connected devices increases, bulk-actions and automation become essential. You need to be able to carry out device provisioning, remote configuration, management of firmware and software updates, and remote troubleshooting.

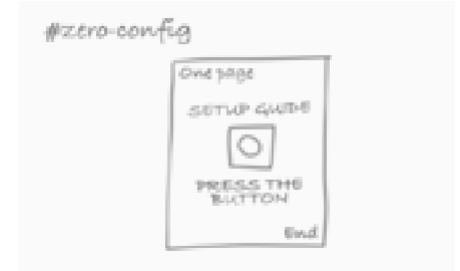
USER MANAGEMENT

Whether it is a public use or enterprise-wide deployment, you need to think about who has access to which features. This requires a wide range of user authentication, access and other security and privacy scenarios.



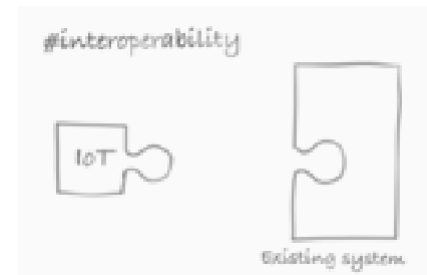
INTEROPERABILITY & APPLICATION ENABLEMENT

Next phase is integrating the IoT solutions with existing systems, management tools and the rest of the wider IT-ecosystem. Application enablement and interoperability are the fundamentals. Built-in application programming interfaces #API, software development kits #SDK, and gateways are the key to the integration of 3rd party systems and applications. Well-defined external interfaces can cut specific integration efforts from months to just a few days.



EASE OF DEPLOYMENT

At the moment you activate your devices, will they immediately start sending live data? This depends how you have configured them. If your devices are #zero-config networking compatible, your deployment will be faster and easier.

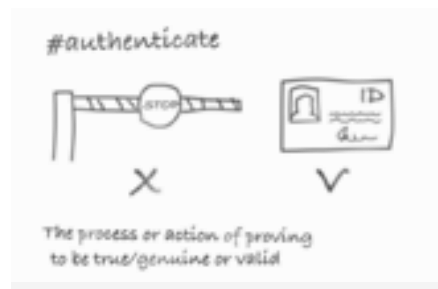




STEP 4: SECURE YOUR THINGS

More and more IoT infrastructures carry sensitive data about systems and individuals. Sometimes it is Personally Identifiable Information (PII) like a person's health records or financial credentials.

Whether it is the device itself which stores the data, the connection protocol which makes the information exchange possible, or the management software console at the headquarters - they all need to be designed with security and privacy in mind. Never take it for granted.

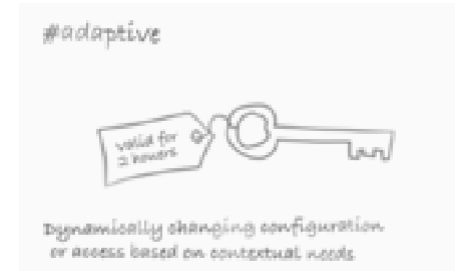


USERS AND SECURITY

For example, do the things in your network just communicate with each other or do they also provide an interface to people? If they do, how will you #authenticate users? Will you let them enter user credentials or will you invest in biometric alternatives? You need to develop a holistic plan that includes all aspects of security.

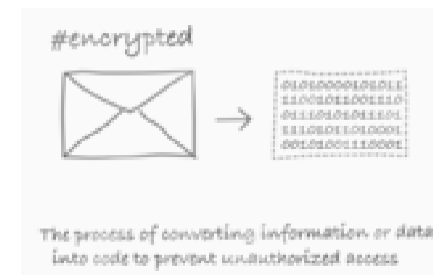
DATA AND SECURITY

Do you store data on the thing itself or send it directly to central cloud storage? In either option, you need to protect your data from a security breach. This starts with the physical housing design – especially if your things are accessible to the public. Depending on your data, you may also consider integrated circuits which automatically store their data #encrypted. So even if they are extracted from the device board, their contents cannot be read or decrypted easily.

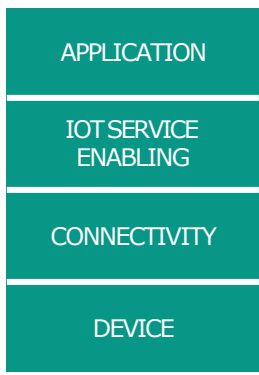


CONTEXT AND SECURITY

Situational context can add a 'common sense' layer to security. For example, making keys and locks function only during working hours is nothing new. But when your smart door lock communicates with the delivery person's mobile to generate a one-time-key when they are at your door, that's a good example of #adaptive security.

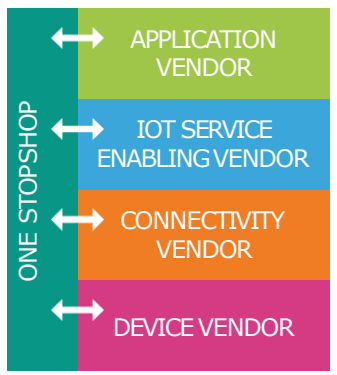


SINGLE VENDOR



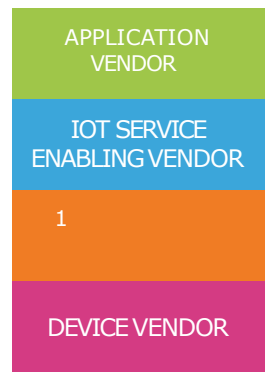
A single supplier/partner provides a customised end-to-end solution. This often suits small and medium enterprises (SMEs) who have less complex legacy to integrate into and don't have the time or resources to manage the integration themselves, and companies with single straightforward use cases - e.g. fleet tracking.

ONE-STOP-SHOP



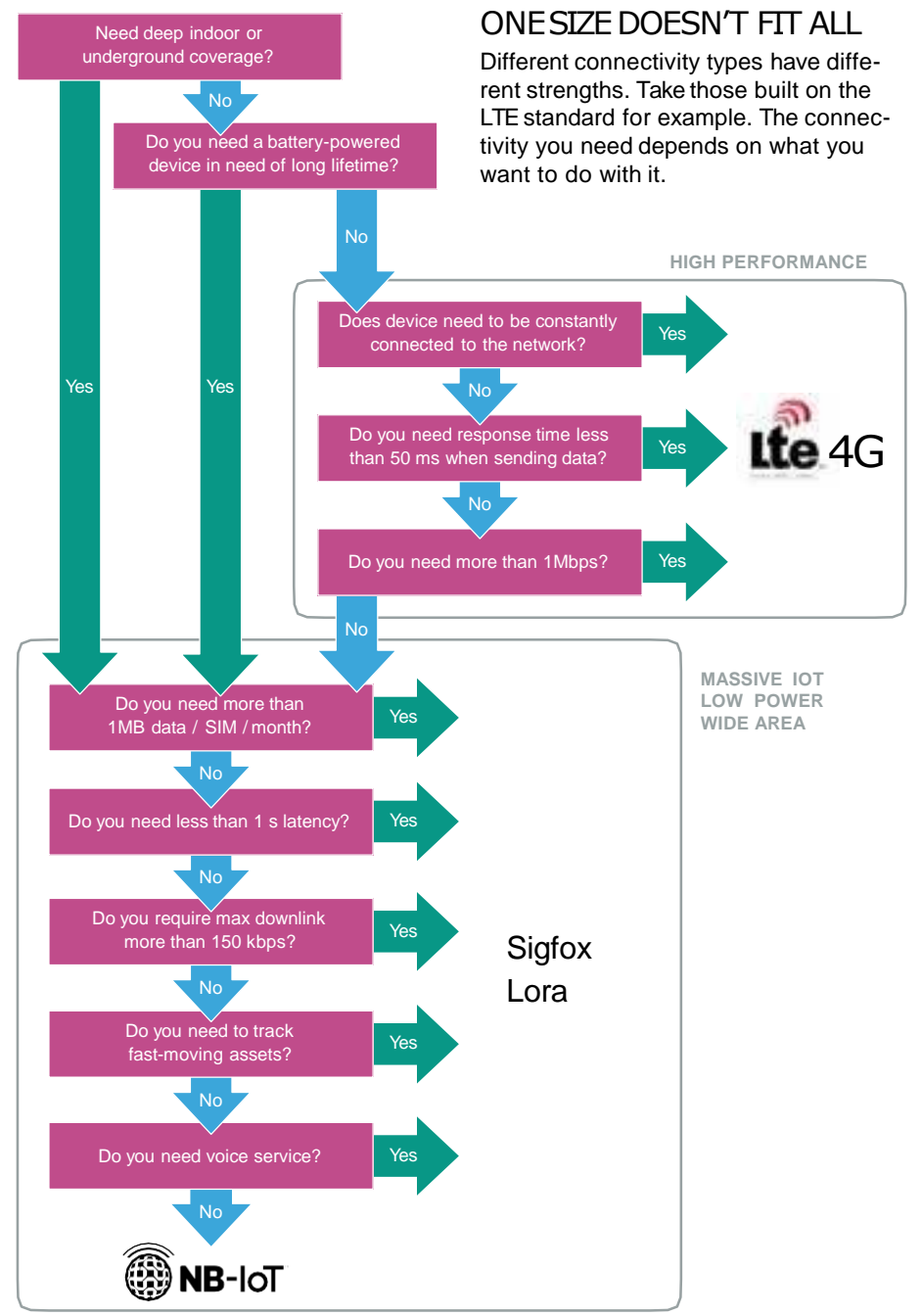
A specialist IoT partner integrates a solution of best-of-breed partners for each part of your ecosystem. This approach provides simplicity and flexibility without single vendor lock in.

MULTI VENDORS



This approach provides greater control, but it also requires the expertise and resources to manage, control and integrate different solutions.

ONE SIZE DOESN'T FIT ALL
Different connectivity types have different strengths. Take those built on the LTE standard for example. The connectivity you need depends on what you want to do with it.



IOT CHECKLIST

START WITH THE WHY
<p>What problem are you solving? (e.g. process efficiency, asset efficiency, innovation...)</p>
<p>Who will use the IoT solution? (e.g. things, users, patterns, 3rd parties...)</p>
<p>What insights will be useful for them? (e.g. monitor, control, analyse, understand, predict, maintain...)</p>
<p>Which things can collect the data? (e.g. machines, devices, buildings, animals, plants, patterns...)</p>
<p>What physical qualities do they have? (e.g. size, casing, power, interface...)</p>

THE BUSINESS LOGIC – PROCESS THE DATA
<p>What are you trying to understand? (e.g. situation, trends, patterns, out of boundaries...)</p>
<p>How will you set your business rules? (e.g. IFTTT, complex algorithm, machine learning...)</p>
<p>What are the characteristics of data? (e.g. volume, variety, velocity, sources personal data / GDPR...)</p>
<p>What are the contextual differences? (e.g. time, place, situation...)</p>
<p>How will the data be managed? (e.g. interoperability, application enablement, APIs, libraries...)</p>

THE THINGS – COLLECT THE DATA
<p>How will it be digitised? What will it sense? (e.g. temperature, pressure, movement, sound, humidity...)</p>
<p>How will it react? (e.g. switches, motors, valves, buzzer, LEDs...)</p>
<p>Who will it talk to? (e.g. people, things, systems...)</p>
<p>What data will it extract? (e.g. units, limits, boundaries, baseline, contextual...)</p>
<p>How will they get connected? (e.g. range, bandwidth, consumption, accuracy, latency...)</p>

THE USERS – USE THE DATA
<p>What are the touchpoints? (e.g. applications, HMI, screen, conversational, chatbots, who will see the data, what changes in routines/processes, KPIs...)</p>
<p>How will users interact with the System? (e.g. real-time, ad-hoc, on-demand...)</p>
<p>What will you monitor, analyse or predict? (e.g. situations, behaviors, values, patterns...)</p>
<p>What types of actions are there? (e.g. notifications, alerts, triggers, execution, events...)</p>
<p>How will security be ensured? (e.g. user-device security, authentication, encryption rules...)</p>

GLOSSARY

Actuator: hardware piece of a device for moving and controlling other parts

Adaptive configuration: dynamic configurations changing based on the contextual needs

API (Application Programming Interface): a set of subroutine definitions, communication protocols, and tools for building software

Auditing: conducting an official inspection of the changes of an object – like a thing, network, or service

Authentication: the process or action of proving or showing something to be true, genuine, or valid

Authorisation: the action of giving official permissions

Availability: the probability that an item will be operable and ready to go any time

Power consumption: total amount of power needed to operate the thing for a certain period

TCO: sum of operations and total cost of ownership

Controller: the brain of an IoT device

Data rate: amount of data to be sent or received i.e. speed per second over the network connection

Density: the portion of the potential connections in a network that are actual connections

Encryption: the process of converting data into a code, especially to prevent unauthorised access

Firmware: embedded software which runs on the IoT device controller

Interface: a system or device which enables two different entities to interact with each other

Interoperability: interfaces that are flexible enough to work with other entities

Latency: how much time it takes for a set of data to get from one point to another i.e. responsiveness

Library: a group of functions, routines and variables which accelerate software development

Mission-critical: service or system whose failure or disruption will result in the failure of essential operations

Mobility: maintaining connection qualities while being transported to another location

OTA (over-the-air): methods of distributing software and configuration settings to devices wirelessly

Position accuracy: the degree of closeness of the indicated readings to the actual physical position

Sensor: hardware piece of a device which detects (senses) qualities of the physical environment

Simulation: an imitation of the operation of a real-world process or system

SLA (Service Level Agreement): contract between the client and provider about service qualities

Traffic capacity: the amount of data that can be transmitted across a link when there is no congestion

Zero-configuration: a set of technologies that automatically configure settings

